Installing Oracle Database 10g Software

Item: 1 (Ref:1Z0-042.1.4.1)

You are in the process of installing Oracle Database 10*g* on your client computer. You have set the value for environment variable `ORACLE_HOME` to `/oracle/ora10g`.

What does this value specify?

- the directory location for the base of OFA
- the directory location where the Oracle software is installed
- the directory location where the script files of the database are stored
- the directory location where the operating system searches for Oracle executables, such as SQL*Plus

Answer:

the directory location where the Oracle software is installed

---

Explanation:

The `ORACLE_HOME` environment variable specifies the directory location where the Oracle software is installed. In this scenario, `/oracle/ora10g` is the directory where the Oracle software is installed.

The `ORACLE_HOME` environment variable does not specify the directory location for the base of OFA. The `ORACLE_BASE` environment variable specifies the directory location for the base of OFA.

The `ORACLE_HOME` environment variable does not specify the directory where the script files of the database are stored. The `%ORACLE_HOME%/rdbms/admin/` directory specifies the location where the script files of the database are stored.

The `ORACLE_HOME` environment variable does not specify the directory location where the operating system searches for Oracle executables, such as SQL*Plus. The directory where the operating system searches for Oracle executables is specified using the `PATH` environment variable.

Item: 2 (Ref:1Z0-042.1.4.3)

Your Oracle server has four databases SALESDB, FINDB, HRDB, and TESTDB installed on it. The SALESDB database is currently running. You set the ORACLE_SID environment variable on the operating system as follows:

```
C:\> SET ORACLE_SID=TESTDB
```

Then, you try to start the TESTDB database from another SQL*Plus prompt using this command:

```
SQL> STARTUP;
```

What will be the result of this command?

- The command will start the TESTDB database without any alterations to the SALESDB database.
- The command will start the TESTDB database and shut down the already-running SALESDB database.
- This command will return an `Oracle already running, shut it down first` error.
- The command will not start the TESTDB database because the assignment of the ORACLE_SID environment variable is incorrect, and you must specify the specific parameter file when issuing the STARTUP command.

Answer:

The command will start the TESTDB database without any alterations to the SALESDB database.

Explanation:

The command will start the TESTDB database without any alterations to the SALESDB database. Setting the ORACLE_SID environment variable specifies the instance name for the database that is to be started. In this scenario, because there are four databases on the same server you should specify the instance name that is to be started using the ORACLE_SID environment variable. Setting this variable will not affect the instances that are already up and running.

The option stating that the command will start the TESTDB database and shut down the already-running SALESDB instance is incorrect because the SALESDB instance will not shut down as a result of the STARTUP command.

The option stating that the command will return an error is incorrect because the error is generated only if you have not specified the instance name by setting the ORACLE_SID environment variable. If this variable is specified, this error will not be generated.

The option stating that the command will not start the TESTDB database because the assignment of the ORACLE_SID variable is incorrect because the variable is set appropriately in this scenario. Additionally, it is not necessary to specify the specific parameter file when issuing the STARTUP command. If no parameter file is specified, the default SPFILE will be used, if the SPFILE is not available, the default PFILE will be used to start the database.

Item: 3 (Ref:1Z0-042.1.3.1)

While installing the Oracle10*g* database on a UNIX platform you are prompted to run the script file `orainstRoot.sh`, which creates another file `oraInst.loc`.

For which purpose is the newly created `oraInst.loc` file used?

- It is used to set the UNIX kernel parameters for the Oracle database.
- It is used to store information about the users accessing the Oracle database.
- It is used by Oracle Universal Installer at startup to find the inventory location.
- It is used by Oracle Universal Installer to store the home directory and base directory locations.

Answer:

It is used by Oracle Universal Installer at startup to find the inventory location.

Explanation:

The `orainstRoot.sh` script file creates the inventory pointer file, `oraInst.loc`, which is used by Oracle Universal Installer at startup to find the inventory location.

The `oraInst.loc` file is not used to set the UNIX kernel parameters for the Oracle database. The UNIX kernel parameters for the Oracle database are set in the `/etc/system` file on a UNIX system.

The `oraInst.loc` file is not used to store information about the users accessing the Oracle database. Information about the users accessing the Oracle database is present in the data dictionary.

The `oraInst.loc` file is not used by Oracle Universal Installer to store the home directory and base directory locations. No particular file stores the home directory and base directory. These are specified by environment variables.

Item: 4 (Ref:1Z0-042.1.3.3)

While installing the Oracle 10*g* database using OUI, which file storage option will provide you with additional features such as mirroring and stripping?

- File System
- Raw Devices
- Oracle-Managed Files
- Automatic Storage Management

Answer:

Automatic Storage Management

Explanation:

The Automatic Storage Management (ASM) file storage option is a new feature introduced in Oracle 10*g* for automatically managing the Oracle database files. The ASM file storage option also supports features such as mirroring and stripping.

The File System storage option does not support mirroring and stripping. Instead, this storage option only supports storage of the Oracle database files in the operating system file system.

The Raw Devices storage option does not support mirroring and stripping. Raw devices are disk partitions that do not have a file system.

Oracle-Managed Files is not a valid storage option when installing with OUI. Oracle-Managed Files is a feature supported by Oracle to automatically manage the Oracle database files. However, Oracle-managed files do not support mirroring and stripping.

Item: 5 (Ref:1Z0-042.1.3.4)

You want to use the Oracle-Managed Files feature to minimize file management and provide efficient storage for your Oracle database.

Which two initialization parameters are used to configure to use the Oracle-Managed Files feature? (Choose two.)

- DB_NAME
- INSTANCE_NAME
- DB_CREATE_FILE_DEST
- DB_RECOVERY_FILE_DEST
- DB_CREATE_ONLINE_LOG_DEST_*n*

Answer:

DB_CREATE_FILE_DEST

DB_CREATE_ONLINE_LOG_DEST_*n*

Explanation:

The DB_CREATE_FILE_DEST and DB_CREATE_ONLINE_LOG_DEST_*n* initialization parameters are used to configure your database to use the Oracle-Managed Files feature. The DB_CREATE_FILE_DEST initialization parameter specifies the destination for storage of the Oracle datafiles that are created. The DB_CREATE_ONLINE_LOG_DEST_*n* initialization parameter specifies the destination for storage of the Oracle redo log files and control files.

The DB_NAME initialization parameter specifies only the name of the Oracle database and does not need to be changed or configured to use the Oracle-Managed Files feature.

The INSTANCE_NAME initialization parameter specifies only the name of the Oracle database instance and does not need to be changed or configured to use the Oracle-Managed Files feature.

Item: 6 (Ref:1Z0-042.1.4.2)

While installing the Oracle 10*g* database, you have set the NLS_LANG environment variable to AMERICAN_AMERICA.WE8IS08859P1.

What will be the default date format assigned to the Oracle 10*g* database?

- DDMMYY
- DD-MM-YY
- DD-MON-YY
- DD-MONTH-YYYY

Answer:

DD-MON-YY

Explanation:

The default date format assigned to the Oracle 10*g* database will be DD-MON-YY. The NLS_LANG environment variable specifies the language, territory, and character set supported by the user sessions in an Oracle 10*g* database. The format to specify NLS_LANG is <*language*>_<*territory*>.<*character set*>. The <*territory*> portion specifies the default date format, numeric formats, and monetary formats. In this scenario, the value for <*territory*> is set to AMERICA, which signifies that the date format, numeric formats, and monetary format will be according to the American territorial region. Therefore, the default date format assigned to the Oracle 10*g* database will be DD-MON-YY.

All the other options are incorrect because DDMMYY, DD-MM-YY, and DD-MONTH-YYYY are not default date formats for the given territory that is assigned the value AMERICA.

Item: 7 (Ref:1Z0-042.1.1.1)

You are in the process of installing Oracle 10*g* on your host computer. Click the Exhibit(s) button to view the hardware composition of your host computer.

Which action should you take to successfully complete the installation of Oracle 10*g* on your computer?

- Increase the RAM on your computer to 512 MB.
- Increase the virtual memory on your computer to 1 GB.
- Increase the free hard disk space on your computer to a minimum of 2 GB.
- Increase the free hard disk space on your computer to a minimum of 1.5 GB.
- Increase the temporary disk space on your computer to a minimum of 200 MB.

Answer:

Increase the free hard disk space on your computer to a minimum of 1.5 GB.

Resource	Current size
Physical Memory	256 MB
Virtual Memory	512 MB
Temporary disk space	100 MB
Free hard disk space	1 GB

Explanation:

The minimum free hard disk space required for a successful installation of Oracle 10*g* is 1.5 GB. You need to increase the free hard disk space on your computer to a minimum of 1.5 GB.

You do not need to increase the RAM on your computer to 512 MB because the minimum amount of physical memory or RAM required for a successful installation of Oracle 10*g* is 256 MB. However, Oracle recommends that you use 512 MB of RAM for an Oracle 10*g* database.

You do not need to increase the virtual memory on your computer because the minimum amount of virtual memory required for a successful installation of Oracle 10*g* is twice the amount of RAM, which is 512 MB in this scenario.

You do not need to increase the free hard disk space on your computer to a minimum of 2 GB because the minimum amount of hard disk space required for a successful installation of Oracle 10*g* is 1.5 GB.

You do not need to increase the temporary disk space on your computer to a minimum of 200 MB because the minimum amount of temporary disk space required for a successful installation of Oracle 10*g* is 100 MB.

Item: 8 (Ref:1Z0-042.1.3.2)

Your Oracle server is running on a Linux platform. You create a new database NEWDB on this server.

Which file is updated with the Oracle system identifiers (SIDs) when this new Oracle database, NEWDB, is created?

- oratab
- crontab
- catexp.sql
- orainstRoot.sh

Answer:

oratab

Explanation:

The oratab file on a Linux platform is updated with the Oracle SIDs when a new Oracle database is created on the Linux platform. The path where the oratab file is located is /var/opt.

The crontab file on a Linux platform is used for scheduling jobs. This file is not updated with the Oracle SIDs when a new Oracle database is created on the Linux platform.

The catexp.sql file is a script file that creates data dictionary views in an Oracle database to support import and export activities in the Oracle database. This file is not updated with the Oracle SIDs when a new Oracle database is created on the Linux platform.

The orainstRoot.sh script file creates the inventory pointer file while installing the Oracle 10*g* database on a Linux platform. This file is not updated with the Oracle SIDs when a new Oracle database is created on the Linux platform.

Creating an Oracle Database

Item: 1 (Ref:1Z0-042.2.2.6)

Your database is running in the shared server mode. You want to ensure that the memory allocated to the shared pool is completely used by the application users and not by RMAN processes or any other I/O server processes.

Which component of the Shared Global Area (SGA) should be allocated memory to achieve the objective?

- java pool
- log buffer
- large pool
- buffer cache

Answer:

large pool

Explanation:

The large pool should be allocated memory to ensure that the memory allocated to the shared pool is completely used by the application users and not by RMAN processes or any other I/O server processes. Increasing the size of the shared pool, setting up a reserved area, and pinning PL/SQL packages are all effective methods of improving the performance of the shared pool. However, the performance of the shared pool can be negatively impacted by SQL-intensive operations, such as those that occur when using multiple I/O server process and Oracle's Recovery Manager (RMAN) utility. The large pool can be configured manually to allocate memory to I/O server processes and RMAN processes. By doing this, the memory allocated to the shared pool will not be consumed by I/O server processes or RMAN processes. Instead, it will be available to the application processes.

Allocating memory to the java pool will not ensure that the memory allocated to the shared pool is completely used by application users and not by RMAN processes or any other I/O server processes. The java pool is a specific area in the SGA and is used to run Java-specific applications.

Allocating memory to the log buffer will not ensure that the memory allocated to the shared pool is completely used by the application users and not by the RMAN processes or any other I/O server processes. The memory allocated to the log buffer is not used by the RMAN processes. The larger the size of the redo log buffer, the less likely it is for the user server process to experience a wait when trying to place redo entries into the log buffer.

Allocating memory to the buffer cache will not ensure that the memory allocated to the shared pool is completely used by the application users and not by the RMAN processes or any other I/O server processes. The memory allocated to the buffer cache is not used by RMAN processes. The larger the size of the buffer cache, the less likely it is for cached buffers to be moved out of the cache by the least recently used (LRU) list.

Item: 2 (Ref:1Z0-042.2.2.4)

Which background process and associated database component guarantees that committed data is saved even when the changes have not been recorded in the datafiles?

- CKPT and control file
- LGWR and online redo log files
- DBW*n* and archived redo log files
- DBW*n* and database buffer cache

Answer:

LGWR and online redo log files

Explanation:

The log writer process, LGWR, and online redo log files guarantee that committed data is saved even when the changes have not been recorded in the datafiles. The log writer process writes the blocks contained in the redo log buffer of the SGA to the online redo log files. The log writer process also writes the buffers to the online redo log files when a user transaction is committed. LGWR writes the committed data to the online redo log files, thus guaranteeing that the committed data is saved even if it has not been written to the datafiles.

The checkpoint process, CKPT, and control file do not guarantee that committed data is saved even when the changes have not been recorded in the datafiles. Checkpoints help to reduce the time required for instance recovery. A checkpoint is an event that signals DBW*n* to flush the modified data from the buffer cache to the disk, and CKPT updates the control file and datafiles. At checkpoints, the modified blocks from the database buffer cache are written to the datafiles by DBW*n*. The data blocks modified by a transaction will be written to the datafiles even if a transaction has not been committed by the user, and a checkpoint is initiated before the user commits the transaction. The control file is used to record structural changes in the database.

The database writer processes, DBW*n*, and archived redo log files do not guarantee that committed data is saved even when the changes have not been recorded in the datafiles. The DBW*n* process writes the contents of the dirty buffers contained in the buffer cache to the datafiles. The archived redo log files are used for database recovery and are considered offline redo log files.

The database writer processes, DBW*n*, and database buffer cache do not guarantee that committed data is saved even when the changes have not been recorded in the datafiles. The DBW*n* process writes the contents of the dirty buffers contained in the buffer cache to the datafiles. The database buffer cache is the area of memory that caches the database data, containing blocks from the datafiles that have been read recently.

Item: 3 (Ref:1Z0-042.2.7.1)

Which three statements correctly describe the **Manage Templates** option available with DBCA? (Choose three.)

- ☐ It allows you to create a template based on another template.
- ☐ It allows you to create a database with a structure similar to an existing database.
- ☐ It allows you to create a template that contains only the data of an existing database.
- ☐ It allows you to create a template based on all the tablespaces of an existing database.
- ☐ It allows you to create a template that contains only the structure of an existing database.
- ☐ It allows you to create a template that contains the data as well as structure of an existing database.

Answer:

It allows you to create a template based on another template.
It allows you to create a template that contains only the structure of an existing database.
It allows you to create a template that contains the data as well as structure of an existing database.

Explanation:

The **Manage Templates** option available with DBCA allows you to:

- Create a template based on another template.
- Create a template that contains only the structure of the database.
- Create a template that contains the data as well as structure of the database.

The **Manage Templates** option in DBCA is accessed on the **Operations** page in DBCA. DBCA uses templates, which are XML files, when creating databases. Each template can include database options, and other specifics of the database, such as initialization parameters. Using these templates makes it easier to create and clone databases.

Using the **Manage Templates** option in DBCA, you cannot create a database. It can only be used to create a template from an existing template or an existing database. This template can then be used to create the database.

Using the **Manage Templates** option in DBCA, you cannot create a template that contains only the data of an existing database. You can create a template that contains the data as well as structure of an existing database.

Using the **Manage Templates** option in DBCA, you cannot create a template based on all the tablespaces of an existing database. A template based on tablespaces in an existing database cannot be created.

Item: 4 (Ref:1Z0-042.2.4.3)

You are required to create a new database using DBCA. The database is required to store historical data pertaining to the last 20 years for a multinational bank. This data is generally accessed to create reports needed in different quarters of the year. In addition, new data is inserted into the database at the end of every month.

Considering these requirements, which template would be the best template to use to create the database?

- Data Warehouse
- General Purpose
- Custom Database
- Transaction Processing

Answer:

Data Warehouse

Explanation:

In this scenario, it would be best to use the Data Warehouse template because you have a large volume of historical data. This historical data is typically read-only and used generally to produce reports.

The General Purpose template can be used to create this database, but because the data specifically matches the requirements of a data warehouse, you should use the Data Warehouse template to create the database. The General Purpose template combines features of the Data Warehouse and Transaction Processing templates and is usually used when you are creating a database for which you are not sure of the kind of data that will be stored.

The Custom Database template can be used to create this database, but because the data specifically matches the requirements of a data warehouse, you should use the Data Warehouse template. The Custom Database template is generally used for scenarios that are more complex. Using the Custom Database template, you can explicitly define the options for the structure of the database that is to be created.

The Transaction Processing template is generally used in situations where the number of concurrent users is higher and the data is accessed and updated more often, such as OLTP systems.

Item: 5 (Ref:1Z0-042.2.3.2)

You have installed Oracle Enterprise Manager 10*g* Database Control on your computer to manage your production database located on a remote host computer through a Web-enabled interface.

Which component is NOT a component of Oracle Enterprise Manager 10*g* Database Control?

- Oracle Management Agent
- Oracle Management Service
- Oracle Management Interface
- Oracle Management Repository

Answer:

Oracle Management Interface

Explanation:

The Oracle Management Interface is not part of Oracle Enterprise Manager 10*g* Database Control. Oracle Enterprise Manager 10*g* Database Control consists of the following components:

- Oracle Management Agent
- Oracle Management Service
- Oracle Management Repository

All of the other options are incorrect because they are components of Oracle Enterprise Manager 10*g* Database Control.

Item: 6 (Ref:1Z0-042.2.4.2)

You are creating a database using DBCA. Which options can be configured when creating a database using DBCA? (Choose all that apply.)

- [ ] character sets
- [ ] memory sizing
- [ ] database block size
- [ ] connection mode
- [ ] maximum number of users in the database
- [ ] default profile allocation for users

Answer:

character sets
memory sizing
database block size
connection mode

Explanation:

When creating a database using DBCA, you can configure the character sets to be used by the database, the memory sizing option, the database block size, and the connection mode used to connect to the server. When you create a database using DBCA and select the **Create Database** link on the DBCA **Operations** page, a wizard is started. One of the steps of the wizard allows you to set initialization parameter values for these, as well as other parameters. The character sets are specific to the territory of the database and language used by the database. The memory sizing option includes the distribution of physical memory into different components of the Oracle database. The block-sizing option configures the database block size to be used by the Oracle database that is being created. The connection mode configures which connection mode, shared server or dedicated server, will be used to connect to the server. DBCA can also be used to schedule database backups on a regular basis.

You cannot configure the maximum number of users in the database when using DBCA to create a database. However, the maximum number of users in the database can be configured at the database level by using the initialization parameter `LICENSE_MAX_USERS`.

You cannot configure the default profile allocation for users when using DBCA to create a database. This is configured at the database level when users are created or by using the `DEFAULT` profile.

Item: 7 (Ref:1Z0-042.2.2.5)

Your database server is running in shared server mode. Which component is a component of the Program Global Area (PGA) when the database is in shared server mode?

- shared pool
- stack space
- user session data
- memory structures
- cursor state information

Answer:

stack space

Explanation:

In shared server mode, only stack space is a component of the PGA. The other components that are the user session data, cursor state information, shared pool, and memory structures are all part of the System Global Area (SGA). When the database server is running in the shared server mode, the PGA is not a part of the SGA, and the PGA only contains stack space. The other components like user session data, memory structures, and cursor state information are part of the SGA.

The shared pool is not a part of the PGA in shared server mode. It is a part of the SGA.

The user session data is not part of the PGA. It is a part of the SGA.

The memory structures are not a part of the PGA, but rather part of the SGA.

The cursor state information is stored in the SGA when the database is in shared server mode.

Item: 8 (Ref:1Z0-042.2.1.4)

You are using an spfile to start the database. The maximum number of users in your database has been set to 150. Because the number of users has already reached the maximum limit, you are not able to create more users.

Which statement should you issue to increase the maximum number of users in this database and keep the change persistent without affecting users who are connected to the database?

- `ALTER SYSTEM SET LICENSE_MAX_USERS=200;`
- `ALTER SYSTEM SET LICENSE_MAX_SESSIONS=200;`
- `ALTER SYSTEM SET LICENSE_MAX_USERS=200 SCOPE=SPFILE;`
- `ALTER SYSTEM SET LICENSE_MAX_USERS=200 SCOPE=MEMORY;`
- `ALTER SYSTEM SET LICENSE_MAX_SESSIONS=200 SCOPE=SPFILE;`

Answer:

`ALTER SYSTEM SET LICENSE_MAX_USERS=200;`

Explanation:

You should use the `ALTER SYSTEM SET LICENSE_MAX_USERS=200;` statement. To make the changes immediate and persistent across an instance that is using an spfile, you should use the clause `SCOPE=BOTH` or accept the default, which is `SCOPE=BOTH`, if you are using an spfile to start the instance. The maximum number of users in a database is set using the initialization parameter `LICENSE_MAX_USERS`.

You should not use the `ALTER SYSTEM SET LICENSE_MAX_SESSIONS=200;` statement because the parameter `LICENSE_MAX_SESSIONS` does not increase the number of users that can exist in a database. The `LICENSE_MAX_SESSIONS` parameter specifies the maximum number of user sessions that can be created in a database at a time.

You should not use the `ALTER SYSTEM SET LICENSE_MAX_USERS=200 SCOPE=SPFILE;` statement because this will modify the parameter only in the spfile. The modification will come into effect only at the next startup.

You should not use the `ALTER SYSTEM SET LICENSE_MAX_USERS=200 SCOPE=MEMORY;` statement because this will modify the parameter only in memory. The change will not be persistent at the next startup.

You should not use the `ALTER SYSTEM SET LICENSE_MAX_SESSIONS=200 SCOPE=SPFILE;` statement because the parameter `LICENSE_MAX_SESSIONS` does not specify the number of users that can exist in a database. The `LICENSE_MAX_SESSIONS` parameter specifies the maximum number of user sessions that can be created in a database at a time.

Item: 9 (Ref:1Z0-042.2.1.3)

Your database is running in the ARCHIVELOG mode. After an instance crash, you start up the database by issuing the STARTUP command. Instance recovery is initiated by the SMON background process.

Which statements are true about the phases involved in the instance recovery performed by SMON? (Choose all that apply.)

- ☐ The instance recovery will recover data up to the last commit.
- ☐ The information used for instance recovery will be derived from the alert log.
- ☐ The information used for instance recovery will be derived from the control file.
- ☐ The uncommitted changes are rolled back using information in the undo segments.
- ☐ The information used for instance recovery will be derived from the data dictionary.
- ☐ The instance recovery will recover all the data entered into the database before the point of the crash.
- ☐ Only the committed changes stored in the online redo log file are applied to the affected data blocks.
- ☐ The committed and uncommitted changes stored in the online redo log are applied to the affected data blocks.

Answer:

The instance recovery will recover data up to the last commit.
The information used for instance recovery will be derived from the control file.
The uncommitted changes are rolled back using information in the undo segments.
The committed and uncommitted changes stored in the online redo log are applied to the affected data blocks.

Explanation:

The instance recovery performed by SMON goes through the following phases:

- All the committed and uncommitted data from the online redo log is applied to the affected blocks.
- The uncommitted data applied to the data blocks is rolled back using the undo information in the undo segments.
- Information, such as the online redo log sequence number, which is to be used for instance recovery is obtained from the control file.
- The instance recovery thus performed will recover the database only up to the last commit. Any uncommitted data will not be applied to the database.

The information used for instance recovery is not derived from the alert log or the data dictionary. Instead, it is derived from the control file.

The instance recovery will not recover the uncommitted data. It will recover data only up to the last commit.

All the data from the redo log file, whether committed or uncommitted, will be applied to the database. The uncommitted data will be rolled back by applying undo data from the undo segments.

Item: 10 (Ref:1Z0-042.2.1.2)

During your routine monitoring operations on the database, you observe that there is heavy contention on data dictionary tables whenever extents are allocated or freed from a tablespace.

Which action should you take as a measure to eliminate this contention on the SYSTEM tablespace?

- Use local extent management for the SYSTEM tablespace.
- Use bigfile tablespaces in the database to avoid contention.
- Use automatic segment space management for tablespaces.
- Use local extent management for nonsystem tablespaces if not using it already.

Answer:

Use local extent management for nonsystem tablespaces if not using it already.

Explanation:

To reduce contention caused on the data dictionary tables by allocation or freeing of extents, you can use local extent management for nonsystem tablespaces. If you use locally-managed tablespaces, the contention on data dictionary tables is reduced. This is because locally-managed tablespaces do not record free space or extent allocation in the data dictionary.

Using local extent management for the SYSTEM tablespace will not eliminate the contention because the contention is mainly caused by allocation and deallocation of space in the nonsystem tablespace.

Using bigfile tablespaces will not eliminate the contention on data dictionary tables. A bigfile tablespace is mainly used to store a large volume of data thereby avoiding the requirement to create several smallfile tablespaces to store the same data.

Using automatic segment space management will not eliminate contention because automatic segment space management is used to automatically manage values for storage parameters, such as PCTUSED, PCTFREE, and PCTINCREASE, for different database objects. When using automatic segment space management, the free space within the segment and used space is tracked using bitmaps and not by using free lists. Using this technique will not reduce contention on data dictionary tables.

Item: 11 (Ref:1Z0-042.2.2.1)

Which stages of Structured Query Language (SQL) statement processing are performed when you issue a MERGE statement? (Choose all that apply.)

- [ ] The rows inserted are written to the datafiles.
- [ ] The data is fetched and returned to the users.
- [ ] The updated blocks are written to the datafiles.
- [ ] The changes made are recorded in the redo log files.
- [ ] The System Change Number is recorded in the control file.
- [ ] A parse tree is generated for the query if it does not already exist.
- [ ] Blocks of data are retrieved into the database buffer cache if they are not already present.

Answer:

A parse tree is generated for the query if it does not already exist.
Blocks of data are retrieved into the database buffer cache if they are not already present.

Explanation:

When a MERGE statement is issued at the SQL prompt, it undergoes the following stages:

- The PARSE stage in which the query is parsed to check for details, such as the syntax of the statement, privileges on the object, and optimal execution plan.
- The BIND stage in which any variables are assigned values.
- The EXECUTE stage in which the query is actually executed. At this stage, the data required by the user's query is retrieved from the database buffer cache and returned to the user.

The option that states that the inserted rows are written to the datafiles is incorrect because the data is written to datafiles only at checkpoints.

The option that states that the data is fetched and returned to the user is incorrect because the MERGE statement does not undergo a FETCH stage. The FETCH stage is only applicable to the SELECT statement.

The option that states that the updated blocks are written to the datafiles is incorrect because the updated data is written to datafiles only at checkpoints.

The option that states that the changes are recorded in the redo log files is incorrect because the changes are written to the redo log files only when a commit is performed.

The option that states that the System Change Number is recorded in the control file is incorrect because the System Change Number (SCN) is recorded in the control file only on a commit.

Item: 12 (Ref:1Z0-042.2.3.1)

You are a DBA with Startel. You have a set of four databases SALESDB, FINDB, HRDB, and PROD. You also have two listeners, L1 and L2, and an application server, APPS1, located on different locations globally. You have been assigned the task of managing all these components from your office located in New York.

Which two tools should you install to administer these components centrally on the network? (Choose two.)

- Oracle Management Agent
- Oracle Enterprise Manager 10*g*
- Oracle Enterprise Manager 10*g* Grid Control Console
- Oracle Enterprise Manager 10*g* Application Server Control
- Oracle Enterprise Manager 10*g* Database Control Console

Answer:

Oracle Management Agent
Oracle Enterprise Manager 10*g* Grid Control Console

Explanation:

To administer the databases, listeners, and Web application servers centrally, you need the Oracle Management Agent installed on all the host computers and the Oracle Enterprise Manager 10*g* Grid Control Console installed on the centralized computer, which you will use to administer the components located globally. The Oracle Management Agent monitors all targets on the host and sends the monitoring information to the middle-tier Management Service, and manages and maintains the host and its targets. The Oracle Enterprise Manager 10*g* Grid Control Console is used to administer the components located globally.

Oracle Enterprise Manager 10*g* does not provide any help in centrally administering databases located globally. Oracle Enterprise Manager 10*g* is used to monitor and manage your database.

Oracle Enterprise Manager 10*g* Application Server Control is not used for managing databases globally. It is used to manage Oracle Application Server 10*g*.

Oracle Enterprise Manager 10*g* Database Control Console is not used to manage databases globally. It can only be used to monitor and manage a single Oracle10*g* instance at a time.

Item: 13 (Ref:1Z0-042.2.2.2)

Users in your application complain of slow response to queries. Upon analysis, you realize that the queries are being reparsed because they are aged out quickly.

Which component of the Shared Global Area (SGA) should you modify to avoid the reparsing of queries?

- java pool
- large pool
- library cache
- redo log buffer
- data dictionary cache
- database buffer cache

Answer:

library cache

Explanation:

Increasing the library cache component of the SGA will help avoid the reparsing of queries because the library cache contains the parse tree information of queries. The queries are reparsed because they are aged out too quickly from the library cache due to lack of space in the library cache. Adding more space to the library cache will ensure that the parse tree information for the queries is not aged out. Because space cannot be directly allocated to the library cache, the shared pool component of the SGA can be increased, thereby increasing the size of library cache, which is contained in the shared pool.

The java pool is an incorrect option because it does not store the parse tree information for the queries, and modifying it will not help to avoid the reparsing of queries. The java pool is a specific area in the SGA that is used to run Java-specific applications. To run these Java applications, you use the Java stored procedures in the database. The size of the java pool is determined by the `JAVA_POOL_SIZE` parameter specified in the initialization parameter file.

The large pool is an incorrect option because it does not store the parse tree information for the queries, and modifying it will not help to avoid the reparsing of queries. A large pool, when configured, is used to store the session memory information for shared servers and is also used for some RMAN operations.

The redo log buffer is an incorrect option because it does not store the parse tree information for the queries, and modifying it will not help to avoid the reparsing of queries. The redo log buffer is used to record all the changes made to the data blocks in a database. The redo log buffer is used in recovery.

The data dictionary cache is an incorrect option because it does not store the parse tree information for the queries, and modifying it will not help avoid the reparsing of queries. The data dictionary cache is a part of the shared pool, which stores the definitions of recently accessed data objects, such as tables and indexes.

The database buffer cache is an incorrect option because it does not store the parse tree information for the queries, and modifying it will not help avoid the reparsing of queries. The database buffer cache is used to cache the recently accessed data blocks that have been retrieved from the datafiles as a result of user queries on the database.

Item: 14 (Ref:1Z0-042.2.4.1)

You need to create a database similar to an existing database. The data and structure of the new database must be the same as the existing database.

Which action would best obtain the desired results?

- Create a database using the CREATE DATABASE statement. Then, perform a complete database import of the original database.
- Create a template of the existing database using DBCA that incorporates only the structure of the original database. Then, use this template to create the new database.
- Create a template of the existing database using DBCA that incorporates the structure and data of the original database. Then, use this template to create the new database.
- Create a template of the existing database using DBCA that incorporates only the structure of the original database and use this template to create the new database. Then, perform a complete database import of the original database.

Answer:

Create a template of the existing database using DBCA that incorporates the structure and data of the original database. Then, use this template to create the new database.

Explanation:

To create a database similar to an existing database with the same structure and data, use DBCA to create a template with the same structure as well as data from the existing database. Then, use this template to create the new database. When you create a template from an existing database using the structure as well as data, this template will contain all the physical and logical characteristics of the source database. The datafiles, log files, control files, and archive redo logs will all be the same in number and size. The other structures in the database, such as the tablespaces, tables, and user schemas, will be identical to those in the source database.

Using the CREATE DATABASE statement would require more administrative effort. You would need to specify all of the needed options to create the new database with the same options as the original database. Manually creating the database and then performing an import would require more effort than using DBCA to create the database from a template.

Using DBCA to create a template with only the same structure and using this template to create the new database would create the database, but not with the same data as the original database. You would need to rebuild the data in the database.

Using DBCA to create a template with only the same structure and using this template to create the new database followed by a complete database import is not the best choice. This will increase the time needed to create an identical database because you will need to perform a complete database import after the database creation.

Item: 15 (Ref:1Z0-042.2.1.1)

Eric is working as a database administrator with Telstar Corporation. He has been granting SYSDBA and SYSOPER privileges to certain users who must perform certain administrative tasks, such as starting and shutting down the database remotely.

Which file determines the number of users that can be granted the SYSDBA or SYSOPER privilege?

- trace file
- control file
- alert log file
- password file
- system datafile

Answer:

password file

Explanation:

The password file contains information regarding the number of users who can be granted the SYSDBA or SYSOPER privilege. While creating a password file, you can use the ENTRIES clause to specify the number of users who can be granted the SYSDBA or SYSOPER privilege. The password file can also be used to authenticate users who are trying to access the database remotely. The REMOTE_LOGIN_PASSWORDFILE initialization parameter can be set to provide a different authentication mechanism for the database. Setting the parameter to a value of NONE specifies that users should be authenticated by the operating system. Setting the parameter to a value of SHARED specifies that more than one database can use the same password file. Using this method, the user can be authenticated on one or more databases that use the same password file. Setting the parameter to a value of EXCLUSIVE specifies that users are using the password file for authentication.

The trace file option is incorrect because a trace file cannot be used to determine information regarding the number of users who can be granted the SYSDBA or SYSOPER privilege. The trace files in an Oracle database are created for every server process and background process. Whenever the server or background process encounters an error or is terminated, the information regarding the error is written to the respective trace file. The trace file can be used to gather information regarding these server and background processes.

The control file option is incorrect because a control file cannot be used to determine information regarding the number of users who can be granted the SYSDBA or SYSOPER privilege. A control file in an Oracle database contains information about the physical structure of the database. The control file is required whenever you start the database and must be available throughout the life of the instance.

The alert log file option is incorrect because the alert log file does not contain information regarding the number of users who can be granted the SYSDBA or SYSOPER privilege. The alert log file in an Oracle database contains database-wide information about the errors and other important events in the database. The alert log file contains the startup and shutdown times of the database, the default parameters used to start the database, and other important information regarding the database.

The system datafile option is incorrect because a system datafile file cannot be used to determine information regarding the number of users who can be granted the SYSDBA or SYSOPER privilege. The system datafile in an Oracle database is a part of the SYSTEM tablespace. The SYSTEM tablespace is created in an Oracle database automatically upon database creation and constitutes the data dictionary.

Item: 16 (Ref:1Z0-042.2.5.2)

You have created a database using DBCA. Now, you want to change the configurations of the database using DBCA.

Which option CANNOT be configured using DBCA?

- configure the database to enable daily backup
- configure the database to run as a shared server
- configure the database to use the Local naming method
- configure the database to use password file authentication
- configure the database to use Automatic Storage Management

Answer:

configure the database to use the Local naming method

Explanation:

Using DBCA, you cannot configure the naming method for resolving a net service name. The naming method for the database can be configured using the net configuration files or the Net Configuration Assistant.

DBCA can be used to configure the database to enable daily backup. To enable daily backup of the database, you must check the **Enable Daily Backup** check box on the **Management Options** page. While enabling backup, you can specify the time when the daily backup will be performed and the username and password of the user performing the backup.

DBCA can be used to configure the database to run as a shared server. To configure the database to run as a shared server, you must select the appropriate connection mode in the **Connection Mode** tab on the **Initialization Parameters** page.

DBCA can be used to configure the database to use password file authentication by setting the appropriate parameters. You can set the `REMOTE_LOGIN_PASSWORDFILE` parameter to `EXCLUSIVE` or `SHARED` using the **Initialization Parameters** page to enable the database to use password file authentication.

DBCA can be used to configure the database to use Automatic Storage Management. To configure the database to use Automatic Storage Management, you must select the **Automatic Storage Management (ASM)** button on the **Passwords and Storage** page.

Item: 17 (Ref:1Z0-042.2.2.3)

Which activities in the database signal DBW*n* to write the data from the database buffer cache to datafiles? (Choose all that apply.)

- ☐ whenever there is a log switch
- ☐ whenever a user transaction is committed
- ☐ whenever the database is shut down cleanly
- ☐ whenever a table is dropped from the database
- ☐ whenever a tablespace in the database is taken offline
- ☐ whenever the server process cannot find free buffers in the database buffer cache

Answer:

whenever there is a log switch
whenever the database is shut down cleanly
whenever a tablespace in the database is taken offline
whenever the server process cannot find free buffers in the database buffer cache

---

Explanation:

DBW*n* writes data to datafiles whenever there is a log switch, whenever the database is shut down cleanly, whenever a tablespace in the database is taken offline, and whenever the server process cannot find free buffers in the database buffer cache. DBW*n* writes data to datafiles any time a checkpoint occurs. A checkpoint occurs when you shut down the database cleanly, whenever there is a log switch and whenever a checkpoint is forced by the DBA using the ALTER SYSTEM CHECKPOINT statement. Also, an incremental checkpoint occurs when you take a tablespace in the database offline. In addition, when the server process scans the database buffer cache and is unable to find any free buffers, it signals DBW*n* to write the data from the database buffer cache to the datafiles.

DBW*n* does not write data to the datafiles when a user transaction is committed. Modified data blocks are written to the redo log buffer only on a commit.

DBW*n* does not write data to the datafiles when a table is dropped from the database. When dropping a table from the database, only the redo is written to the redo log buffer.

Database Interfaces

Item: 1 (Ref:1Z0-042.3.3.1)

You issue the following ALTER TABLE statement:

```
SQL> ALTER TABLE MASTER SET UNUSED COLUMN CODE;
```

Which statements regarding the CODE column of the MASTER table are true? (Choose all that apply.)

- Values can be inserted into the CODE column.
- The CODE column is permanently dropped from the table.
- The CODE column can be dropped later.
- The CODE column will not be displayed if you issue a SELECT statement against the MASTER table and use an asterisk in the select list.
- The CODE column will not be displayed if you execute the SQL*Plus DESCRIBE command to view the structure of the MASTER table.
- The data contained in the CODE column of the MASTER table is cleared, but the empty CODE column remains in the structure of the MASTER table.

Answer:

The CODE column can be dropped later.

The CODE column will not be displayed if you issue a SELECT statement against the MASTER table and use an asterisk in the select list.

The CODE column will not be displayed if you execute the SQL*Plus DESCRIBE command to view the structure of the MASTER table.

Explanation:

In the given scenario, the CODE column can be dropped later, the CODE column will not be displayed if you issue a SELECT statement against the MASTER table and use an asterisk in the select list, and the CODE column will not be displayed if you execute the SQL*Plus DESCRIBE command to view the structure of the MASTER table. When you use the SET UNUSED option with the ALTER TABLE statement, the column specified as unused is marked as unused in the table but not dropped immediately. The column can be dropped at a later point using the ALTER TABLE...DROP COLUMN or ALTER TABLE...DROP UNUSED COLUMNS statement. After a column has been set as unused, it will not be displayed by SELECT statements or by the SQL*Plus DESCRIBE command.

Values cannot be inserted into the column because after a column is set as unused it is no longer accessible. You would not be able to successfully issue an INSERT statement inserting values into the CODE column.

The CODE column is not permanently dropped from the table. The SET UNUSED clause only sets the column as unused and does not immediately drop the column from the table.

The data contained in the CODE column of the MASTER table is not cleared. Using the SET UNUSED clause does not affect the column's data. The data still remains in the CODE column, and will remain there until the column is dropped using an ALTER TABLE...DROP statement.

Item: 2 (Ref:1Z0-042.3.3.3)

Two users JULIA and SAMUEL are simultaneously working on the table EMP_DET, which has thousands of rows. User SAMUEL issues the following statement:

```
SQL> UPDATE EMP_DET SET EMP_SAL=25000 WHERE EMP_NAME='JACK';
```

Immediately afterwards, the user JULIA issues the following statement:

```
SQL> SELECT * FROM EMP_DET WHERE EMP_NAME='JACK';
```

What will happen when the user JULIA issues her SELECT statement?

- The user JULIA will receive an error because she cannot view the data because SAMUEL is modifying the data.
- The user JULIA will be able to view the data including the changes made by SAMUEL.
- The user JULIA will be able to view the data as it existed before the UPDATE statement was issued by SAMUEL.
- The user JULIA's session will hang because she is trying to access the same row that is currently being modified by SAMUEL's session.

Answer:

The user JULIA will be able to view the data as it existed before the UPDATE statement was issued by SAMUEL.

Explanation:

The user JULIA can access the data being modified by SAMUEL's session, but she will be able to view the data as it existed before SAMUEL's modification. This is because changes made to the data are visible only to the user SAMUEL. SAMUEL has not committed the changes. Therefore, other users view the data as it existed before being modified by SAMUEL. This concept is called read consistency and is implemented by the rollback segments in the database.

The option that states that the user JULIA will receive an error is incorrect because she can view the data.

The option that states that the user JULIA will be able to view the data including the changes made by SAMUEL is incorrect. This is because SAMUEL has not committed the changes. Therefore, JULIA cannot view the changes made by SAMUEL.

The option that states that JULIA's session will hang is incorrect because JULIA's session will not hang. She will be able view the data selected by her query.

Item: 3 (Ref:1Z0-042.3.1.3)

You are using Enterprise Manager Database Control to administer your database. The database has lost some of the configuration files due to media failure. This failure has not affected the availability of the database. Among the lost files is the `portlist.ini` file.

Which information is contained in this `portlist.ini` file?

- the initialization parameters configured for the database
- the list of listener configuration parameters used by the remote listeners
- the port number of the HTTP listener being used by Enterprise Manager Database Control
- the port number used by the listener configured to listen for the incoming database connections

Answer:

the port number of the HTTP listener being used by Enterprise Manager Database Control

---

Explanation:

The `portlist.ini` file contains information regarding the port number of the HTTP listener being used by Enterprise Manager Database Control. This file can be used to determine the port number if no information is available regarding the port number of the HTTP listener being used by Enterprise Manager Database Control. The `portlist.ini` file also contains the port number used by *i*SQL*Plus, and the file is stored in the location pointed to by the `ORACLE_HOME` environment variable.

The file does not contain the initialization parameters configured for the database. The `init`*`sid`*`.ora` file contains the initialization parameters configured for the database.

The file does not contain the list of listener configuration parameters used by the remote listeners. This information is present in the `listener.ora` file.

The file does not contain the port number used by the listener configured to listen for the incoming database connections. This information is present in the `listener.ora` file.

Item: 4 (Ref:1Z0-042.3.5.1)

Click the Exhibit(s) button to analyze a set of statements issued in a session.

If the salary of the employee in the MASTER table with the CODE value of J4569 was 20000 at the beginning of the session, what will be the salary value of this employee in the MASTER2 table displayed when the last query is run?

- NULL
- 10000
- 20000
- 25000

Answer:

25000

```
SQL> SELECT ENAME, CODE, SALARY FROM MASTER;

SQL> UPDATE MASTER SET SALARY=25000 WHERE CODE='J4569';

SQL> SAVEPOINT AFTER_UPDATE;

SQL> UPDATE MASTER SET SALARY=10000 WHERE CODE='J4569';

SQL> ROLLBACK TO AFTER_UPDATE;

SQL> CREATE TABLE MASTER2 AS SELECT * FROM MASTER;

SQL> SELECT * FROM MASTER2;
```

Explanation:

After the last query is run, the salary of the employee with the CODE value of J4569 will be 25000. In the given set of statements, you first issue a SELECT statement, which does not affect the salary column contents. Next, you issue an UPDATE statement that updates the SALARY column of the MASTER table for the employee with a CODE value of J4569. This UPDATE statement sets the SALARY column value to 25000. However, the change has not yet been committed. Next, you issue a SAVEPOINT command. The SAVEPOINT command marks a point to which you can later roll back if necessary, but does not perform a commit. Next, you issue another UPDATE statement that updates the SALARY column to 10000. However, this change is not committed either. After the second UPDATE statement is issued, you issue a ROLLBACK statement including the TO AFTER_UPDATE clause. This rolls back the changes to the savepoint you created named AFTER_UPDATE. After this statement is executed, the SALARY column will contain the value that it contained at the point the SAVEPOINT was issued, namely 25000. However, the pending changes from the first update still have not been committed. Next, you issue a CREATE TABLE statement to create the MASTER2 table. When you have a transaction in progress and issue a DDL statement, such as this CREATE TABLE statement, the current transaction is ended and any pending DML statements in the transaction are committed. Then, the DDL statement is executed. When this CREATE TABLE statement is executed, the pending changes to the SALARY column of the MASTER table are committed before the CREATE TABLE statement is executed. Therefore, the SALARY column value in both the MASTER and MASTER2 tables for this employee will contain a value of 25000.

All of the other options are incorrect because they do not reflect the correct SALARY value of the employee with the CODE value of J4569 that will be displayed by the last query executed.

Item: 5 (Ref:1Z0-042.3.3.4)

Click the Exhibit(s) button to view the details of the ITEMS and ORDERS tables.

Which statement will return all the records where PROD_ID values are common to the two tables and any PROD_ID values that are not common to the two tables?

- SELECT i.PROD_ID, i.PRODUCT_NAME, o.ORDER_ID, o.CUSTOMER_NAME
  FROM ITEMS i
  NATURAL JOIN ORDERS o;
- SELECT i.PROD_ID, i.PRODUCT_NAME, o.ORDER_ID, o.CUSTOMER_NAME
  FROM ITEMS i
  FULL OUTER JOIN ORDERS o
  ON i.PROD_ID=o.PROD_ID;
- SELECT i.PROD_ID, i.PRODUCT_NAME, o.ORDER_ID, o.CUSTOMER_NAME
  FROM ITEMS i
  LEFT OUTER JOIN ORDERS o
  ON i.PROD_ID=o.PROD_ID;
- SELECT i.PROD_ID, i.PRODUCT_NAME, o.ORDER_ID, o.CUSTOMER_NAME
  FROM ITEMS i
  RIGHT OUTER JOIN ORDERS o
  ON i.PROD_ID=o.PROD_ID;
- SELECT i.PROD_ID, i.PRODUCT_NAME, o.ORDER_ID, o.CUSTOMER_NAME
  FROM ITEMS i
  INNER JOIN ORDERS o
  ON i.PROD_ID=o.PROD_ID;

Answer:

```
SELECT i.PROD_ID, i.PRODUCT_NAME, o.ORDER_ID, o.CUSTOMER_NAME

FROM ITEMS i
FULL OUTER JOIN ORDERS o
ON i.PROD_ID=o.PROD_ID;
```

ITEMS

PROD_ID	PRODUCT_NAME	PRICE	MANUFACTURER
1	MODEM	2000	TELSTAR
2	CPU	25000	TRITECH
3	CABLE	500	UNITED SALES
4	MONITOR	15000	VERIGON
5	KEYBOARD	1000	GEOTREK
6	PINS	2000	METROIL
7	SOUNDCARD	3000	GEOTREK
8	LANCARD	1500	TELSTAR

ORDERS

ORDER_ID	PROD_ID	AMOUNT	CUST_NAME
200	2	50000	ANTHONY
215	3	4000	SAMUEL
256	5	5000	AMY
265	5	1000	JOHN
276	4	45000	ERIC
212	1	6000	KATE
245	6	10000	TIMOTHY
249	5	2000	SCOTT

Explanation:

The SELECT statement that uses a FULL OUTER JOIN will return all the records where PROD_ID values are common to the two tables and any PROD_ID values that are not common to the two tables. A full outer join will return all the rows from the joined tables including the rows that are common in the joined tables and retain the rows that are not common in the tables and the extended null values. The join query will return rows from the ITEMS and the ORDERS table where the PROD_ID is common to both the tables. It will also return the records where the PROD_ID is not present in the ORDERS table but present in the ITEMS table, namely the rows in ITEMS with PROD_ID 7 and 8.

The statement that uses a NATURAL JOIN will not return the rows that are not common to both the tables. A natural join will only return the rows that are common to the two tables. A natural join is based on all the columns in the two tables that have the same name. You are not required to specify on which columns the join operation will be performed. The natural join query will only return rows from the ITEMS and the ORDERS table where the PROD_ID is common to both the tables. No other records will be returned by this query.

The statement that uses a LEFT OUTER JOIN will only return all the rows that are common to the two tables and the rows from the table specified on the left side of the join that do not satisfy the join condition. This join will not include the rows from the table on the right side of the join that do not satisfy the join condition. The left outer join query will return rows from the ITEMS and the ORDERS table where the PROD_ID is common to both the tables. It will also return the records from the table specified on the left of the join, ITEMS, which do not satisfy the join condition.

The statement that uses a RIGHT OUTER JOIN will only return all the rows that are common to the two tables and the rows from the table specified on the right side of the join that do not satisfy the join condition. This join will not include the rows from the table specified on the left side of the join that do not satisfy the join condition. The right outer join query will return rows from the ITEMS and the ORDERS table where the PROD_ID is common to both the tables. It will also return the records from the table specified on the right side of the join, ORDERS, which do not satisfy the join condition. In this scenario, there are no rows that are unique to the ORDERS table and therefore, no other rows will be returned.

The statement that uses an INNER JOIN will only return the rows that satisfy the join condition. An inner join performs a join on the two tables and returns the rows from the two tables that satisfy the join condition. An inner join will not return the rows from the two tables that do not satisfy the join condition. The inner join query will only return rows from the ITEMS and the ORDERS table where the PROD_ID is common to both the tables.

Item: 6 (Ref:1Z0-042.3.1.1)

You are assigned the task of creating a SQL*Plus report for the number of products sold for a specific manufacturer. You also want to calculate the average sales of products for the given manufacturer for the current year. You want SQL*Plus to prompt you for the name of the manufacturer when the report is run. However, SQL*Plus should not prompt you for the name when the report runs subsequently in the current session.

Which option should you use to achieve the objective?

- a bind variable
- the `DEFINE` command
- a substitution variable with a & prefix
- a substitution variable with a && prefix

Answer:

a substitution variable with a && prefix

Explanation:

You should use a substitution variable with a && prefix. Using a double ampersand (&&) prefix with a substitution variable will ensure that SQL*Plus does not prompt for the same value again within the current session. SQL*Plus automatically defines any substitution variable preceded by two ampersands. After you define a variable, SQL*Plus will not prompt for its value a second time in the current session. Therefore, SQL*Plus will prompt for the name of the manufacturer during the first execution, but will not prompt again for the same variable during subsequent executions in the current session.

A bind variable would not achieve the objective because a bind variable cannot be used to define the value for a variable. A bind variable improves performance by enabling use of a common cursor that is opened for a bind variable for different variables.

If you use the `DEFINE` command, SQL*Plus will not prompt for the variable's value. When a `DEFINE` command is used to specify a value for a particular variable, the command will specify the value when you issue the command, and SQL*Plus will not prompt for the value when a report or program construct using the variable is run.

SQL*Plus does not implicitly define the substitution variable preceded by only one ampersand. Using this would prompt for the manufacturer every time you run the report. A substitution variable with an ampersand (&) prefix is used when you must run the report with a different value of the variable every time.

Item: 7 (Ref:1Z0-042.3.3.2)

You created a table EMP using the following statement:

```
SQL> CREATE TABLE EMP
(NAME CHAR(10),
ADDRESS VARCHAR2(10),
CITY VARCHAR2(20),
EMPCODE NUMBER(10),
DEPT_ID NUMBER(8));
```

This table contains 1000 records. The largest values in the NAME, ADDRESS, CITY, EMPCODE, and DEPT_ID columns are six characters, 10 characters, 20 characters, four digits, and six digits, respectively. You want to reduce the size of the columns. There are no constraints defined on the table.

Which modifications to column(s) of the EMP table CANNOT be made using the ALTER TABLE...MODIFY statement? (Choose all that apply.)

- ☐ The NAME column's width can be reduced to seven characters.
- ☐ The ADDRESS column's width can be reduced to nine characters.
- ☐ The CITY column's width can be reduced to 15 characters.
- ☐ The EMPCODE column's width can be reduced to six digits.
- ☐ The DEPT_ID column's width can be reduced to six digits.

Answer:

The ADDRESS column's width can be reduced to nine characters.

The CITY column's width can be reduced to 15 characters.

Explanation:

In the given scenario, the ADDRESS column's width cannot be reduced to nine characters, and the CITY column's width cannot be reduced to 15 characters. You can reduce the width of any of the columns in the EMP table. However, an error will be generated if the width of the data currently present in the column is greater than the new width specified for the column. In this scenario, the ADDRESS column currently contains at least one value that is 10 characters long. Therefore, its width cannot be reduced to nine characters. Also, the CITY column currently contains at least one value that is 20 characters long. Therefore, its width cannot be reduced to 15 characters.

The NAME column's width can be reduced to seven characters using the ALTER TABLE...MODIFY statement because the NAME column does not currently contain data that exceeds seven characters.

The EMPCODE column's width can be reduced to six digits using the ALTER TABLE...MODIFY statement because the EMPCODE column does not currently contain data that exceeds six digits.

The DEPT_ID column's width can be reduced to six digits using the ALTER TABLE...MODIFY statement because the DEPT_ID column does not currently contain data that exceeds six digits.

Item: 8 (Ref:1Z0-042.3.1.2)

You are trying to connect to the Oracle database server by using *i*SQL*Plus.

Which component must be running to enable you to successfully connect to the database?

- *i*SQL*Plus server
- *i*SQL*Plus on clients
- Oracle Enterprise Manager
- Oracle Management Agent

Answer:

***i*SQL*Plus server**

Explanation:

To successfully connect to the database server, the *i* SQL*Plus server must be running and the database must be open. Also, the server-side listener process of *i* SQL*Plus must be running before you can connect using a browser. If the *i* SQL*Plus server is not running, a **`Could not connect to the server`** error is generated. After receiving the error, you must start the *i* SQL*Plus server to overcome the error and contact the administrator for assistance. *i* SQL*Plus is a browser-based interface used to connect to an Oracle database. To start the *i* SQL*Plus server, you must issue the following command:

```
isqlplusctl start
```

It is not necessary that *i* SQL*Plus be running on the clients. After the *i* SQL*Plus server is started, the clients can connect to *i* SQL*Plus by using the following syntax:

http://hostname:port/isqlplus.

It is not necessary that Oracle Enterprise Manager be running to connect to the database server by using *i* SQL*Plus. Oracle Enterprise Manager is a graphical tool used to monitor and manage your database environment.

It is not necessary that the Oracle Management Agent be running to connect to the database server by using *i* SQL*Plus. The Oracle Management Agent is a process responsible for managing and maintaining the host and its target databases.

Item: 9 (Ref:1Z0-042.3.4.1)

Which two interfaces can be used as command-line interfaces for accessing an Oracle database? (Choose two.)

- SQL*Plus
- *i*SQL*Plus
- Oracle Forms
- Oracle Reports
- Oracle Enterprise Manager

Answer:

SQL*Plus
***i*SQL*Plus**

Explanation:
SQL*Plus and *i*SQL*Plus can be used as command-line interfaces for accessing an Oracle database. SQL*Plus and *i*SQL*Plus are the two commonly used command-line interfaces available with Oracle that can be used to access the database using SQL. SQL*Plus can be used interactively or in batch mode to write SQL*Plus, SQL, and PL/SQL commands to perform various tasks in the database, such as running PL/SQL blocks, executing SQL statements, listing column definitions for tables in the database, and performing database administration activities. *i*SQL*Plus is a browser based command-line interface to access the Oracle database. *i*SQL*Plus can be used to perform tasks such as describing data, querying and manipulating data from different tables in the database, and creating objects in the database.

Oracle Forms is not a command-line interface. Oracle Forms is a graphical tool that can be used to create application forms that hide the underlying SQL and PL/SQL from database users.

Oracle Reports is not a command-line interface. Oracle Reports is a graphical tool that can be used to create reports. Complex database queries and logic can be incorporated into these reports and allow users to execute reports without having to write complex queries or know how to use programming constructs.

Oracle Enterprise Manager is not a command-line interface. Oracle Enterprise Manager is a graphical tool that can be used to query and manipulate objects in the database. Enterprise Manager provides the ability to perform data management tasks such as querying the data and creating objects, such as tables and indexes, without the need to know the syntaxes required for creation of these objects.

Controlling the Database

Item: 1 (Ref:1Z0-042.4.6.5)

Evaluate this statement:

```
ALTER SYSTEM SET UNDO_TABLESPACE='UNDOTEMP' SCOPE=SPFILE;
```

What will be the result of executing this statement?

- The change will only be made in the instance currently running.
- The change will be persistent across instance shutdown and startup.
- The change will be made in both the currently running instance and the SPFILE.
- The statement will fail because the only valid SCOPE values are MEMORY and BOTH.

Answer:

The change will be persistent across instance shutdown and startup.

Explanation:

With the given statement, the change will be persistent across instance shutdown and startup. You can use the ALTER SYSTEM SET statement to change the value of the instance parameters. The SCOPE clause determines the scope of the change. The valid SCOPE values are:

- MEMORY - Changes the parameter value only in the currently running instance.
- SPFILE - Changes the parameter value in the SPFILE only.
- BOTH - Changes the parameter value in the currently running instance and the SPFILE.

In the given statement, SCOPE is specified as SPFILE. Therefore, the change to the UNDO_TABLESPACE parameter will be made in the SPFILE only. Changes made to the SPFILE are persistent across instance shutdown and startup.

The option stating that the changes will only be made in the instance currently running is incorrect because the changes will not be made to the currently running instance. The changes will be made only to the SPFILE. The changes will take effect when the database is started up the next time.

The option stating that the changes will be made in the currently running instance and the SPFILE is incorrect because the changes will not be made in the currently running instance.

The statement will not fail because you can use SPFILE as a valid value in the SCOPE clause of the ALTER SYSTEM SET statement.

Item: 2 (Ref:1Z0-042.4.7.4)

Eric is working on his production database, PROD. Eric detects a deadlock involving transactions between two users in his database. He wants to view the details of the deadlock to prevent it from occurring the next time.

Which initialization parameter will determine the location of the file containing the details of the deadlock?

- CORE_DUMP_DEST
- USER_DUMP_DEST
- LOG_ARCHIVE_DEST
- BACKGROUND_DUMP_DEST

Answer:

BACKGROUND_DUMP_DEST

Explanation:

The BACKGROUND_DUMP_DEST initialization parameter will determine the location of the alert log. This alert log file contains the details of the deadlock.

The CORE_DUMP_DEST parameter is used to specify the location at which Oracle dumps core files.

The USER_DUMP_DEST parameter does not specify the directory that points to the location of the background process trace files. The user trace files are located in the directory specified by the USER_DUMP_DEST initialization parameter.

The LOG_ARCHIVE_DEST parameter specifies the directory in which the archive log files are stored. It does not specify the directory in which the background process trace files are stored.

Item: 3 (Ref:1Z0-042.4.6.1)

You are using SQL*Plus. Which two commands can you use to display the value assigned to the DB_BLOCK_SIZE parameter? (Choose two.)

- SHOW ALL
- SHOW DB_BLOCK_SIZE
- DESCRIBE DB_BLOCK_SIZE
- SHOW PARAMETER DB_BLOCK_SIZE
- SHOW PARAMETERS DB_BLOCK_SIZE

Answer:

SHOW PARAMETER DB_BLOCK_SIZE
SHOW PARAMETERS DB_BLOCK_SIZE

Explanation:

You can view the value assigned to the DB_BLOCK_SIZE parameter by executing either of the following commands in the SQL*Plus interface:

```
SHOW PARAMETER DB_BLOCK_SIZE
```

Or

```
SHOW PARAMETERS DB_BLOCK_SIZE
```

The SQL*Plus SHOW command is used to display different types of information, including values of SQL*Plus variables, initialization parameters, errors, and objects in the recycle bin. The SHOW command syntax to display the value of initialization parameters is:

```
SHOW PARAMETER[S] [parametername]
```

The *parametername* specifies the name of the initialization parameter for which you want to display the current value. If you specify the SHOW PARAMETER command without specifying a *parametername*, then the values of all the initialization parameters are displayed.

The SQL*Plus SHOW ALL command will display the settings of the SQL*Plus interface. The SHOW ALL command does not display the values assigned to initialization parameters.

The SHOW DB_BLOCK_SIZE command will generate an error because you must include the PARAMETER clause along with the SHOW command.

The DESCRIBE DB_BLOCK_SIZE command cannot be used to view the details because the DESCRIBE command cannot be used to view the settings of initialization parameters. The DESCRIBE command is used to display the structure of a database table, including the column names and their corresponding data types.

Item: 4 (Ref:1Z0-042.4.5.3)

Your database instance fails to start when you issue the following command:

```
SQL> STARTUP NOMOUNT;
```

Which of the following could be the reason for the failure?

- Oracle database cannot read the datafiles.
- Oracle database cannot read the control file.
- Oracle database cannot read the redo log files.
- Oracle database cannot read the initialization parameter file.

Answer:

Oracle database cannot read the initialization parameter file.

Explanation:

The Oracle database instance will fail to start if the Oracle database is unable to read the initialization parameter file. During the `NOMOUNT` stage of database startup, the initialization parameter file is read. The initialization parameter file contains the Oracle database instance parameters and the values defined for these parameters.

The datafiles are read after the Oracle database instance is started. The datafiles and redo log files are read at the `OPEN` stage during database startup.

The control file is read-only after the Oracle database instance is started. The control file is read at the `MOUNT` stage of database startup.

The redo log files are read after the Oracle database instance is started. The datafiles and the redo log files are read at the `OPEN` stage during database startup.

Item: 5 (Ref:1Z0-042.4.2.3)

Your database exists on a remote location. You want to connect to the database using a Web browser and manage it with Enterprise Manager.

Which syntax is correct for you to connect to your database remotely?

- http://*host:portnumber*/em
- http://*host.portnumber*/em
- http://*host:portnumber*.em
- http://www.*host.portnumber*.em
- http://www.*host:portnumber*/em

Answer:

http://*host:portnumber*/em

Explanation:

The correct syntax for connecting to a remote database using a Web browser to manage the database using Enterprise Manager is http://*host:portnumber*/em, where *host* is the host name or host IP address and *portnumber* is the Enterprise Manager Console HTTP port number. This will start Enterprise Manager. If the database is not started, the **Startup/Shutdown and Perform Recovery** page is displayed, and you can use this page to start the database. Otherwise, the **Database Control Login** page is displayed, from which you can log in and manage your database remotely using Database Control.

All the other options are incorrect because they do not provide the correct syntax to connect to your database.

Item: 6 (Ref:1Z0-042.4.2.2)

You are configuring your Database Control with the Enterprise Manager console. You also need automatic storage management for the database files of the PRODUCT database.

Which steps must you perform to successfully configure Database Control for using automatic storage management? (Choose all that apply.)

- Use the command `emca -s`.
- Use the command `emca -a`.
- Use the command `emca -m`.
- Use the command `emca -x product`.
- Change the directory to `ORACLE_HOME/bin` directory.
- Set the `ORACLE_HOME` and `ORACLE_SID` environment variables for the PRODUCT database.
- Set the `ORACLE_HOME` and `LD_LIBRARY_PATH` environment variables for the PRODUCT database.

Answer:

Use the command `emca -a`.
Change the directory to `ORACLE_HOME/bin` directory.
Set the `ORACLE_HOME` and `ORACLE_SID` environment variables for the PRODUCT database.

Explanation:

To configure Database Control for the PRODUCT database to use automatic storage management, you must first set the `ORACLE_SID` and `ORACLE_HOME` environment variables that correspond to the PRODUCT database. Next, you must change the directory to `ORACLE_HOME/bin`. From this prompt, you must issue the command `emca -a` to configure automatic storage management for the database. The `ORACLE_HOME` and `ORACLE_SID` environment variables are used to set the Oracle home and SID for the database to be managed using Database Control. Then, the `-a` command-line argument is used in the command to configure the database for automatic storage management.

The command `emca -s` is incorrect because this option cannot be used to configure automatic storage management. This option is used to configure the Enterprise Manager console to run in silent mode.

The command `emca -m` is incorrect because this option cannot be used to configure automatic storage management. This option is used to configure the database so that it can be managed centrally by the Oracle Enterprise Manager 10*g* Grid Control Console.

The option that states that you must set the `LD_LIBRARY_PATH` environment variable is incorrect. You only need to set the `ORACLE_HOME` and `ORACLE_SID` environment variables. The `LD_LIBRARY_PATH` environment variable specifies the directory that contains OVS files.

Item: 7 (Ref:1Z0-042.4.6.4)

Which view will you query to display the PFILE information currently in effect for a database that was started by using the initialization parameter file?

- V$DATABASE
- V$PARAMETER
- V$SPPARAMETER
- V$CONTROLFILE

Answer:

V$PARAMETER

Explanation:

The V$PARAMETER view displays the current initialization parameters in the database.

The V$SPPARAMETER view displays the parameters defined in the server parameter file (SPFILE), if the server parameter file was used to start the instance.

The V$DATABASE view displays database information such as database name, creation timestamp, and ARCHIVELOG mode.

The V$CONTROLFILE view displays information about the names and locations of the control files of the database.

Item: 8 (Ref:1Z0-042.4.3.1)

You have two listeners named `LISTENER` and `listener2` configured for your database and listening on different port numbers. You executed this command at the command-line:

```
lsnrctl stop
```

What is the result of executing this command?

- An error will be generated.
- Both the listeners will be stopped.
- The default listener will be stopped.
- The listener that was started first will be stopped.

Answer:

The default listener will be stopped.

Explanation:

If two listeners are configured and you execute the `lsnrctl stop` command, the default listener named `LISTENER` will be stopped. The syntax of the `lsnrctl stop` command is:

```
lsnrctl stop [listenername]
```

If specified, the *listenername* must be a valid listener defined in the `listener.ora` file. If a *listenername* is specified, then the specified listener is stopped. However, if no *listenername* is specified, the default listener is stopped. If you stop all of the listeners configured for the database, users will not be able to connect to the database remotely.

The option stating that an error will be generated is incorrect because the command will execute successfully and stop the default listener.

The option stating that both the listeners will be stopped is incorrect because only the default listener named `LISTENER` will be stopped.

The option stating that the listener that was started first will be stopped is incorrect because the default listener named `LISTENER` will be stopped. To stop the listener named `listener2`, you should execute the command `lsnrctl stop listener2`.

Item: 9 (Ref:1Z0-042.4.6.2)

You have altered the size of the database buffer cache by using the following statement:

```
SQL> ALTER SYSTEM SET DB_CACHE_SIZE=335566624 SCOPE=BOTH;
```

Which two statements characterize the result of this statement? (Choose two.)

- The value of the DB_CACHE_SIZE parameter is modified. This information is modified only in memory if the PFILE was used to start the instance.
- The value of the DB_CACHE_SIZE parameter is modified. This information is modified only in the PFILE, if the PFILE was used to start the instance.
- The value of the DB_CACHE_SIZE parameter is modified. This information is modified in both the SPFILE and PFILE, if the PFILE was used to start the instance.
- The value of the DB_CACHE_SIZE parameter is modified. This information is modified in both memory and the SPFILE, if the SPFILE was used to start the instance.
- The value of the DB_CACHE_SIZE parameter is modified only for the current instance. This will be changed back to the previous value after the instance is shut down and restarted.

Answer:

The value of the DB_CACHE_SIZE parameter is modified. This information is modified only in memory if the PFILE was used to start the instance.

The value of the DB_CACHE_SIZE parameter is modified. This information is modified in both memory and the SPFILE, if the SPFILE was used to start the instance.

Explanation:

While using the ALTER SYSTEM statement containing the SCOPE=BOTH option to modify parameters, the information is modified both in memory and the SPFILE, depending on which parameter file was used to start the instance. If the PFILE was used to start the instance, the information is modified only in memory. If the SPFILE was used to start the instance, the information is modified in both memory and the SPFILE. The changes made are persistent across database startups.

The option stating that the value of the DB_CACHE_SIZE parameter is modified only in the PFILE, if the PFILE was used to start the instance is incorrect because the PFILE is not modified by issuing any ALTER SYSTEM statement. The PFILE must be modified manually after the database instance is shut down.

The option stating that the value of the DB_CACHE_SIZE parameter is modified in both the SPFILE and the PFILE, if the PFILE was used to start the instance is incorrect. The reason for this is the PFILE is not modified by issuing any ALTER SYSTEM statement. The PFILE must be modified manually.

The option stating that the value of the DB_CACHE_SIZE parameter is modified only for the current instance and will be changed to the previous value after the instance is shut down and restarted, is incorrect. If the MEMORY value is used for the SCOPE clause instead of the BOTH value, the modified values will change to the previous values after the instance is restarted. The other valid value for the SCOPE clause is SPFILE.

Item: 10 (Ref:1Z0-042.4.4.1)

After changing some parameters in your initialization parameter file, you start the database in the NOMOUNT state using the following command:

```
SQL> STARTUP NOMOUNT;
```

After this, you want to enable redo archiving and therefore, you issue the following statement to mount the database:

```
SQL> ALTER DATABASE MOUNT;
```

At this stage, the database fails to mount.

Which condition could be the reason for the failure?

- A datafile in the database cannot be accessed.
- The control file in the database cannot be accessed.
- The redo log files in the database cannot be accessed.
- The parameter file in the database cannot be accessed.

Answer:

The control file in the database cannot be accessed.

Explanation:

The database will fail to mount if it cannot access the control file. The control file is accessed when the database is mounted. If the control file is missing, an error is generated and the database fails to mount. The database is opened in the MOUNT state to enable or disable redo log archiving.

Datafiles are accessed when the database is opened. In the MOUNT state, only the control files are accessed.

Redo log files are accessed when the database is opened. In the MOUNT state, only the control files are accessed.

The initialization parameter file is accessed when the database instance is started and is in the NOMOUNT state. In the MOUNT state, only the control files are accessed.

Item: 11 (Ref:1Z0-042.4.6.3)

In your production database, you use a parameter file and a server parameter file alternately. You have modified some parameters in your parameter file. After this, you want to incorporate the same changes into your server parameter file.

Which action will you use to incorporate PFILE changes into the SPFILE?

- Create a new SPFILE from the modified PFILE.
- Use RMAN to update the SPFILE to reflect the changes made in the PFILE.
- Manually edit the SPFILE to incorporate the changes made in the PFILE.
- Do not make any changes. The Oracle server will automatically incorporate the changes in the SPFILE.

Answer:

Create a new SPFILE from the modified PFILE.

Explanation:

To incorporate the PFILE changes into the SPFILE, you must create a new SPFILE from the modified PFILE by using the statement:

```
CREATE SPFILE ['spfile name'] FROM PFILE ['pfile name'];
```

The option to use RMAN to update the SPFILE to reflect the changes made in the PFILE is incorrect because RMAN cannot be used to update the SPFILE. RMAN can only be used to back up the SPFILE.

The option to manually edit the SPFILE to incorporate the changes made in the PFILE is incorrect because the SPFILE is a server-side binary file that cannot be edited manually.

The option to not make any changes because the Oracle server will incorporate the changes in the SPFILE automatically is incorrect. The Oracle server will not update the SPFILE to incorporate the changes made to the PFILE. The Oracle server only maintains the SPFILE.

Item: 12 (Ref:1Z0-042.4.2.1)

You are required to stop the Database Control process. Which command will achieve your objective?

- `emctl stop dbconsole`
- `emctl dbconsole stop`
- `emctl stop dbconsole process`
- `emctl dbconsole process stop`

Answer:

`emctl stop dbconsole`

Explanation:

To stop the Database Control process, you can issue the following command at the command prompt of the Oracle server:

```
emctl stop dbconsole
```

All the other options are incorrect because the commands have invalid syntax.

Item: 13 (Ref:1Z0-042.4.3.3)

When trying to connect to a database, you receive an error in Enterprise Manager stating that the network adapter could not establish the connection.

What is the reason for receiving this error?

- No listener is configured for the database.
- The database is not configured for the listener.
- The database you are trying to connect to is not open.
- The listener configured for the database is not running.
- The service name provided in the `tnsnames.ora` file is incorrect.

Answer:

The listener configured for the database is not running.

Explanation:

You receive the error stating that the network adapter could not establish the connection when the listener configured for the database is not running. If you receive this error, you can start the listener using the START command of the listener control utility. To connect to the database, at least one listener must be running.

The option that states no listener is configured for the database is incorrect because in that situation you receive the following error message: **`ORA-12521: TNS:listener could not resolve INSTANCE_NAME given in connect descriptor`**. It is important to configure a listener for the database if you want users from remote computers to connect to your database.

The option that states the database is not configured for the listener is incorrect because in that situation you receive the following error message: **`ORA-12521: TNS:listener could not resolve INSTANCE_NAME given in connect descriptor`**.

The option that states the database you are trying to connect to is not open is incorrect because in that situation you receive the following error message: **`ORA-03113: TNS:end-of-file on communication channel`**. It is important that the database is open or you will not be able to access the database.

The option that states the service name provided in the `tnsnames.ora` file is incorrect is not the correct answer because in that situation you receive the following error message: **`ORA-12154: TNS:could not resolve service name`**.

Item: 14 (Ref:1Z0-042.4.5.1)

While starting your database, you receive an error stating that the database cannot identify one of the redo log files in it.

At which stage will you receive this error?

- when the database changes from the MOUNT to the OPEN state
- when the database changes from the NOMOUNT to the MOUNT state
- when the database changes from the SHUTDOWN to the MOUNT state
- when the first transaction ends and the changes to the database must be written to the redo log files

Answer:

when the database changes from the MOUNT to the OPEN state

Explanation:

The error will be generated in the database when the database tries to access the redo log files in it. The redo log files are accessed when the database changes from the MOUNT state to the OPEN state.

The option that states that you will receive this error when the database changes from the NOMOUNT to the MOUNT state is incorrect. The redo log files are not accessed at this stage. Only the control files are accessed when the database changes from the NOMOUNT to the MOUNT state.

The option that states that you will receive this error when the database changes from the SHUTDOWN to the MOUNT state is incorrect. The redo log files are not accessed at this stage. The parameter file and the control files are accessed when the database is started and the state changes from SHUTDOWN to MOUNT.

The option that states that you will receive this error at the end of the first transaction is incorrect. The redo data generated is written to the log files when the first transaction ends. However, the redo log files are accessed by the database before this when the database changes from the MOUNT to the OPEN state.

Item: 15 (Ref:1Z0-042.4.3.2)

While trying to connect to the database you receive the following error:

ORA-12514: TNS:listener does not currently know of service requested in connectdescriptor

Which two conditions could this indicate? (Choose two.)

- ☐ The database is not open.
- ☐ The database service is not dynamically registered with the listener.
- ☐ The database service name is not configured in the `listener.ora` file.
- ☐ The user trying to connect to the database does not have the SYSDBA privilege.
- ☐ The listener is not running on the database specified in the connect descriptor.

Answer:

The database service is not dynamically registered with the listener.
The database service name is not configured in the `listener.ora` file.

Explanation:

This error could occur because the database service is not dynamically registered with the listener or because the database service name is not configured in the `listener.ora` file. This error occurs because the listener is not yet registered for the service name mentioned in the connect descriptor. This registration can be done dynamically by using PMON, or it can be configured manually by modifying the listener configuration file, `listener.ora`, for the specific listener.

The error does not occur because the database is not open. In that situation, the user will encounter the following error message:

ORA-03113: TNS:end-of-file on communication channel

The error does not occur because the user trying to connect to the database does not have the SYSDBA privilege. The SYSDBA privilege is not necessary to connect to a database through a listener.

The option that states that the listener is not running on the database specified in the connect descriptor is incorrect because in that situation it will display the following error message:

ORA-12541: TNS:no listener

Item: 16 (Ref:1Z0-042.4.5.2)

Your database went down abnormally because of power failure. You could not perform a clean shutdown on the database. After this, you start the database by running the STARTUP command.

Which statements are true regarding this scenario? (Choose all that apply.)

- [ ] The recovery is coordinated by the process monitor.
- [ ] The uncommitted changes are rolled back from the database.
- [ ] The committed changes in the database are written to the datafiles.
- [ ] The information required for recovery is derived from the alert log file.
- [ ] The lost changes in the database are recovered by performing a media recovery.

Answer:

The uncommitted changes are rolled back from the database.
The committed changes in the database are written to the datafiles.

Explanation:

When the database is started after an abnormal termination or by issuing the SHUTDOWN ABORT command, the SMON process coordinates the recovery of the database. This is known as instance recovery. In this process, the uncommitted changes in the database are rolled back from the database by using the information stored in the rollback segments. In addition, the committed changes that were not written to the datafiles are written to the datafiles on disk. This committed information is derived from the online redo log file.

During an instance crash, the database will not be closed or dismounted, and the uncommitted changes in the database will be rolled back. Also, the committed changes contained in database buffers of the database buffer cache and the redo buffers in the redo log buffer will not be written to the disk. The instance recovery procedure performs all these functions and synchronizes the datafiles and the control file.

The option that states that the recovery is coordinated by the process monitor is incorrect because the recovery is coordinated by SMON.

The option that states that the information required for recovery is derived from the alert log file is incorrect because the information is derived from the control file.

The option that states that the lost changes in the database are recovered by performing a media recovery is incorrect because the database is recovered automatically by Oracle. You are not required to perform a media recovery on the database.

Item: 17 (Ref:1Z0-042.4.1.2)

You must query the EMP table owned by the user SCOTT. You do not have the Oracle client software installed on your computer. You want to invoke *i*SQL*Plus and query the EMP table. The host name of the database server is UNS. The IP address of the database server is 172.17.24.77. You are using the default port number to access *i*SQL*Plus.

Which two URLs will invoke *i*SQL*Plus from the Web browser of your computer? (Choose two.)

- `http://uns:5560/isqlplus`
- `http://uns:5550/isqlplus`
- `http://uns/isqlplus:5560`
- `http://172.17.24.77:5560/isqlplus`
- `http://172.17.24.77/isqlplus:5550`

Answer:

`http://uns:5560/isqlplus`
`http://172.17.24.77:5560/isqlplus`

Explanation:

The `http://uns:5560/isqlplus` and `http://172.17.24.77:5560/isqlplus` URLs will invoke *i*SQL*Plus from the Web browser of your computer. The default port number in which *i*SQL*Plus executes is 5560. The correct syntax for accessing *i*SQL*Plus from the Web browser is `http://`*`hostname`*`:`*`portnumber`*`/isqlplus`.

The URL `http://uns:5550/isqlplus` will not invoke *i*SQL*Plus from the Web browser of your computer because the port number defined is incorrect. In this scenario, you are using the default port number 5560.

The URL `http://uns/isqlplus:5560` will not invoke *i*SQL*Plus from the Web browser of your computer because the syntax of the URL is incorrect. The correct syntax for accessing *i*SQL*Plus from the Web browser is `http://`*`hostname`*`:`*`portnumber`*`/isqlplus`.

The URL `http://172.17.24.77/isqlplus:5550` will not invoke *i*SQL*Plus from the Web browser of your computer because the port number defined is incorrect. In this scenario, you are using the default port number 5560.

Item: 18 (Ref:1Z0-042.4.4.2)

Your database aborted while you were performing database backups by placing the tablespaces in the online backup mode. The tablespaces continued to be in the online backup mode when your database aborted. You issued the following command to start up the database after the instance crash.

```
SQL> STARTUP;
```

Which statement is true in the given scenario?

- Instance recovery should be performed to recover the database.
- The undo segments recover the tablespaces that were in the backup mode.
- The archive redo log files in the database cannot be used to perform recoveries after the instance recovery.
- Nothing must be done because the database will open successfully on its own.

Answer:

Nothing must be done because the database will open successfully on its own.

Explanation:

After an instance crash, nothing must be done because the database will open successfully on its own. The instance requires a recovery that will be performed by the SMON background process. The SMON background process does not require the intervention of the DBA. The SMON process will coordinate the recovery that involves the roll forward of committed transactions and the rollback of uncommitted transactions.

The option stating that instance recovery should be performed to recover the database is incorrect because you need not perform an instance recovery to recover the database. The SMON process will automatically perform an instance recovery.

The option stating that the undo segments recover the tablespaces that were in the backup mode is incorrect because the undo segments do not recover the tablespaces that were in the backup mode. The SMON process performs the recovery.

The option stating that the archive redo log files in the database cannot be used to perform recoveries after the instance recovery is incorrect because there is no change in the archive redo log files after an instance crash. These files can be used at any time to perform recoveries.

Item: 19 (Ref:1Z0-042.4.7.2)

Your Oracle server has a set of four databases. You want to monitor the startup and shutdown times of the ORCL Oracle database.

Assuming you have not modified the default file name, which file will you view to obtain information regarding the startup and shutdown of the ORCL database?

- ORA00122.TRC
- ALERT_ORCL.LOG
- ORCL_ALERT.TRC
- TRACE_ALERT.LOG

Answer:

ALERT_ORCL.LOG

Explanation:

To view the startup and shutdown times of the database, you can use the alert log file for the specific database. The default name of the alert log file is ALERT_<*ORACLE_SID*>.LOG. In this scenario, the default alert log file is ALERT_ORCL.LOG because the name of the database is ORCL. The alert log file is a special trace file that stores information regarding the database and error messages related to the different processes running in the background of the Oracle database. The alert log file is recorded in chronological order, starting from the oldest activity. Oracle-tuning methodology focuses on certain aspects of information available in the ALERT_<*ORACLE_SID*>.LOG file to gather statistical information required for tuning.

The ORA00122.TRC file is incorrect because ORA00122.TRC is a trace file. Startup- and shutdown-related information is not stored in trace files. These files store tracing information for the Oracle background processes.

The ORCL_ALERT.TRC file is incorrect because this is a trace file and startup- and shutdown-related information is not stored in the trace files.

The TRACE_ALERT.LOG file is incorrect because the name of the alert log file is not valid.

Item: 20 (Ref:1Z0-042.4.7.3)

You view the alert log file regularly to keep track of important messages that may be generated.

Which problems can be identified by using the alert log file? (Choose all that apply.)

- deadlocks occurring in the database
- the SYSTEM tablespace becoming full
- a control file missing from the database
- a redo log file missing from the database
- users consuming a high amount of CPU
- dropping of an important user from the database
- using the SYSTEM tablespace as the temporary tablespace

Answer:

deadlocks occurring in the database
a control file missing from the database
a redo log file missing from the database
using the SYSTEM tablespace as the temporary tablespace

Explanation:

The alert log file can be used to identify the following problems in a database:

- A control file missing in the database
- A datafile missing in the database
- A redo log file or redo log member file missing in the database
- The SYSTEM tablespace being used as the temporary tablespace
- All internal, block corruption, and deadlock errors occurring in the database

The alert log file can also be used to determine information about the administrative operations occurring for a database, such as creating, altering, or dropping tablespaces or other database startup and shutdown activities.

The option stating you can identify the SYSTEM tablespace becoming full is incorrect because the alert log file cannot be used to identify this problem in the database. To check for space utilization in the SYSTEM tablespace, you can set a warning threshold that generates a warning alert when the SYSTEM tablespace is becoming full.

The option stating you can identify users consuming a high amount of CPU is incorrect because the alert log file cannot be used to identify the users who are using a high amount of CPU. To identify the users using a high amount of CPU time, you can use Automatic Database Diagnostic Monitor (ADDM).

The option stating you can identify dropping of an important user from the database is incorrect because the alert log file cannot be used to identify whether a user has been dropped from the database. The alert log file can identify when a tablespace, datafile, or redo log file has been dropped from the database, but it cannot identify when a user has been dropped from the database. You must use the data dictionary tables and views to determine whether users have been dropped from the database.

Item: 21 (Ref:1Z0-042.4.7.1)

Your production database has crashed due to media failure. After analysis, you discover that the instance crashed because some database files were located on failed media.

Which file contains detailed information about the background processes, the files that caused the instance to crash, and the time of the crash?

- datafile
- control file
- alert log file
- redo log file

Answer:

alert log file

Explanation:

The alert log file stores information about the background processes and the time of the instance crash. The alert log file is located in the directory specified by the `BACKGROUND_DUMP_DEST` initialization parameter.

The datafiles do not store information about the background processes and the time of the instance crash. The datafiles contain the user data.

The control file does not store information about the background processes and the time of the instance crash. The control file stores the structural information of the database.

The redo log files do not store information about the background processes and the time of the instance crash. The redo logs are used to record every change in the database.

Storage Structures

Item: 1 (Ref:1Z0-042.5.3.3)

You are required to rename the EXAMPLE.DBF datafile of your Oracle database. First, you relocate the file using OS utilities.

After relocating the file by using OS utilities, which statement will accomplish the task of updating the control file with the new name of the datafile?

- ALTER DATAFILE...RENAME FILE
- ALTER DATABASE...RENAME DATAFILE
- ALTER DATABASE...RENAME DATA FILE
- ALTER TABLESPACE...RENAME DATAFILE

Answer:

ALTER TABLESPACE...RENAME DATAFILE

Explanation:

The ALTER TABLESPACE...RENAME DATAFILE statement is used to rename the datafiles of your Oracle database. The syntax for renaming a datafile is as follows:

ALTER TABLESPACE *tablespacename* RENAME DATAFILE <*oldfilename*> TO <*newfilename*>;

The ALTER DATAFILE...RENAME FILE statement is syntactically incorrect. ALTER DATAFILE is not a valid statement.

The ALTER DATABASE...RENAME DATAFILE statement is syntactically incorrect. The RENAME DATAFILE clause is not valid with the ALTER DATABASE statement. You can use the RENAME FILE clause of the ALTER DATABASE statement to rename datafiles or redo log file members.

The ALTER DATABASE...RENAME DATA FILE statement is syntactically incorrect. The RENAME DATA FILE clause is not a valid clause of the ALTER DATABASE statement. You can use the RENAME FILE clause of the ALTER DATABASE statement to rename datafiles or redo log file members.

Item: 2 (Ref:1Z0-042.5.3.5)

You have issued the following statement in your Oracle database:

```
SQL> ALTER TABLESPACE SYSAUX OFFLINE;
```

Which statement correctly describes the outcome of this statement?

- You can write data to the SYSAUX tablespace but cannot read data from it.
- This statement fails because you cannot take the SYSAUX tablespace offline.
- You can read data from the SYSAUX tablespace after the SYSAUX tablespace has been taken offline.
- You cannot read data from or write data to the SYSAUX tablespace after the SYSAUX tablespace has been taken offline.

Answer:

You cannot read data from or write data to the SYSAUX tablespace after the SYSAUX tablespace has been taken offline.

Explanation:

In the given scenario, you cannot read data from or write data to the SYSAUX tablespace after the SYSAUX tablespace has been taken offline. The datafiles of the SYSAUX tablespace become inaccessible after the SYSAUX tablespace has been taken offline.

The option stating that you can write data to the SYSAUX tablespace but cannot read data from it is incorrect. You cannot read from or write to the SYSAUX tablespace after the tablespace is taken offline.

The option stating that this statement fails because you cannot take the SYSAUX tablespace offline is incorrect because you can take the SYSAUX tablespace offline.

The option stating that you can read data from the SYSAUX tablespace after the SYSAUX tablespace has been taken offline is incorrect because you cannot read data from the SYSAUX tablespace after it has been taken offline.

Item: 3 (Ref:1Z0-042.5.1.1)

You are administering an Oracle 10*g* database in a Windows environment. You must create a smallfile locally-managed tablespace. The default tablespace type for the database was set to SMALLFILE at the time of database creation.

Which two statements will accomplish the task of creating a smallfile locally-managed tablespace in this database? (Choose two.)

- ☐
```
CREATE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 150M;
```
- ☐
```
CREATE SMALLFILE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 150M;
```
- ☐
```
CREATE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 50G

SMALLFILE;
```
- ☐
```
CREATE SMALLFILE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 150M

EXTENT MANAGEMENT DICTIONARY;
```
- ☐
```
CREATE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 150M

EXTENT MANAGEMENT DICTIONARY
DEFAULT STORAGE (
INITIAL 50K
NEXT 50K
MINEXTENTS 2
MAXEXTENTS 50
PCTINCREASE 0);
```

Answer:

```
CREATE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 150M;
CREATE SMALLFILE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 150M;
```

Explanation:

The option

```
CREATE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 150M;
```

will create a smallfile locally-managed tablespace. A smallfile tablespace can contain up to 1022 files. If you do not use the EXTENT MANAGEMENT LOCAL clause with the CREATE TABLESPACE statement, Oracle creates a locally-managed tablespace by default. Locally-managed tablespaces manage space more efficiently, provide better methods for reducing fragmentation, and increase reliability. Because the default tablespace type has been set to SMALLFILE, the mydata tablespace created will be a smallfile locally-managed tablespace. The option

```
CREATE SMALLFILE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 150M;
```

will also create a smallfile locally-managed tablespace. A smallfile tablespace can also be created if you explicitly specify the SMALLFILE keyword in the CREATE TABLESPACE statement.

The option

```
CREATE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 50G SMALLFILE;
```

is syntactically incorrect.

The option

```
CREATE SMALLFILE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 150M
EXTENT MANAGEMENT DICTIONARY;
```

is incorrect because this statement will create a dictionary-managed tablespace. A dictionary-managed tablespace is created by explicitly specifying the `EXTENT MANGEMENT DICTIONARY` clause in the `CREATE TABLESPACE` statement.

The option

```
CREATE TABLESPACE mydata DATAFILE
'f:\oracle\product\10.1.0\oradata\orcl\mydata.dbf' SIZE 150M
EXTENT MANAGEMENT DICTIONARY
DEFAULT STORAGE (
INITIAL 50K
NEXT 50K
MINEXTENTS 2
MAXEXTENTS 50
PCTINCREASE 0);
```

is incorrect because this statement will create a dictionary-managed tablespace. A dictionary-managed tablespace is created by explicitly specifying the `EXTENT MANGEMENT DICTIONARY` clause in the `CREATE TABLESPACE` statement.

Item: 4 (Ref:1Z0-042.5.2.4)

In your production database, you set the COMPATIBLE initialization parameter to 10.0.0. Then, you create seven tablespaces in the database. The details of the tablespaces in the database are summarized as follows:

SYSTEM - Locally-managed system tablespace
SYSAUX - Locally-managed tablespace auxiliary to the SYSTEM tablespace
UNDO - Locally-managed default undo tablespace
TEMP - Default temporary tablespace
TEMP1 - Temporary tablespace
USERS - Locally-managed tablespace to store user data
IND1 - Locally-managed tablespace to store index data

To manage the data more effectively, you plan to add a few more tablespaces to the database.

Which two statements are true in this scenario? (Choose two.)

- [ ] A bigfile tablespace can be created in the database.
- [ ] All tablespaces in the database will be locally-managed.
- [ ] You cannot create another undo tablespace in the database.
- [ ] All tablespaces will use automatic segment space management.
- [ ] A dictionary-managed tablespace can be created in the database.
- [ ] All newly created tablespaces in the database will be bigfile tablespaces.

Answer:

A bigfile tablespace can be created in the database.
All tablespaces in the database will be locally-managed.

Explanation:

In this scenario, a bigfile tablespace can be created in the database, and all the tablespaces in the database will be locally-managed. You can create a bigfile tablespace in the database because the COMPATIBLE initialization parameter is set to 10.0.0. When this parameter is set in the database, a bigfile tablespace can be created in the database. A bigfile tablespace is a new feature to Oracle 10*g.* Therefore, you must set the COMPATIBLE parameter to 10.0.0 to create a bigfile tablespace in your database. A bigfile tablespace contains a large, single datafile, up to 4G blocks in size, and can be created by using the CREATE BIGFILE TABLESPACE statement. All the tablespaces in the database will be locally-managed because the SYSTEM tablespace of the database is locally-managed. When you create a locally-managed SYSTEM tablespace in a database, all the other tablespaces in the database will be locally-managed.

The option stating that you cannot create another undo tablespace in the database is incorrect. This is because you can create another undo tablespace in the database even if a default undo tablespace exists. This tablespace cannot be used to store the undo data because only one undo tablespace, which is the default undo tablespace for the database, can be active at a given time.

The option stating that all the tablespaces will use automatic segment space management is incorrect. This is because the tablespaces can use automatic or manual segment space management. Setting the COMPATIBLE parameter imposes no restriction on the type of segment space management that will be used by tablespaces in a database.

The option stating that a dictionary-managed tablespace can be created in the database is incorrect because you cannot create a dictionary-managed tablespace in a database that has a locally-managed SYSTEM tablespace. If the SYSTEM tablespace in a database is locally-managed, all the other tablespaces in the database will be locally-managed.

The option stating that all newly created tablespaces in the database will be bigfile tablespaces is incorrect. After setting the COMPATIBLE parameter to 10.0.0, you can create a bigfile tablespace in the database. However, all the tablespaces created in the database do not have to be bigfile tablespaces.

Item: 5 (Ref:1Z0-042.5.2.1)

You have created the USERS tablespace in your PROD database by issuing the following statement:

```
SQL> CREATE TABLESPACE USERS DATAFILE 'D:\USERS1.DBF'
SIZE 2M AUTOEXTEND ON
EXTENT MANAGEMENT LOCAL UNIFORM SIZE 500K
SEGMENT SPACE MANAGEMENT AUTO;
```

Which statements regarding the USERS tablespace are true? (Choose all that apply.)

- ☐ The USERS tablespace is a bigfile tablespace.
- ☐ The USERS tablespace can hold only one datafile.
- ☐ The free space in the USERS tablespace is recorded using bitmaps.
- ☐ The size of all the extents in the USERS tablespace will be the same.
- ☐ Within the USERS tablespace, the maximum size up to which the datafile can grow is 2 MB.
- ☐ Within the USERS tablespace, the datafile automatically increases in size when it becomes full.

Answer:

The free space in the USERS tablespace is recorded using bitmaps.

The size of all the extents in the USERS tablespace will be the same.

Within the USERS tablespace, the datafile automatically increases in size when it becomes full.

Explanation:

The free space in the USERS tablespace is recorded in bitmaps because you have used the EXTENT MANAGEMENT LOCAL clause that enables local extent management. The free space in the tablespace is recorded in bitmaps. Using the given CREATE TABLESPACE statement, all the extents in the tablespace will be of the same size because you have used the UNIFORM SIZE 500K clause. The size of all the extents will be 500K. The datafile of the tablespace will automatically increase when the tablespace becomes full because you have used the AUTOEXTEND ON clause while creating the tablespace. This clause enables automatic extension of datafiles when they become full.

The option stating that the USERS tablespace is a bigfile tablespace is incorrect because the given statement creates a locally-managed tablespace that is a type of smallfile tablespace. The reason for this is the BIGFILE clause is not specified while creating this tablespace. If this clause is not specified, the tablespace defaults to a smallfile tablespace.

The option stating that the USERS tablespace can hold only one datafile is incorrect because the tablespace can hold more than one datafile. While creating a tablespace, the default tablespace is a smallfile tablespace that can hold more than one datafile.

The option stating that within the USERS tablespace the maximum size up to which the datafile can grow is 2 MB is incorrect because the maximum size up to which the datafile can grow is not specified in the statement. This maximum size can be specified by using the MAXSIZE clause within the AUTOEXTEND clause.

Item: 6 (Ref:1Z0-042.5.2.3)

You have created a tablespace by using the following statement:

```
SQL> CREATE TABLESPACE TBS1 DATAFILE '\NEWDB\DATA\DA1.DBF' SIZE 100M
EXTENT MANAGEMENT LOCAL
SEGMENT SPACE MANAGEMENT AUTO
NOLOGGING;
```

Which two statements are true about the tablespace created using this statement? (Choose two.)

- The TBS1 tablespace can be changed to the LOGGING mode.
- Transactions on the TBS1 tablespace will save space in the redo log files.
- The statement will generate an error because the NOLOGGING clause cannot be specified for the TBS1 tablespace.
- All the tables, indexes, and views created in the TBS1 tablespace will be in the NOLOGGING mode.
- A table created in the TBS1 tablespace will consume less space because of the use of the NOLOGGING clause.

Answer:

The TBS1 tablespace can be changed to the LOGGING mode.

Transactions on the TBS1 tablespace will save space in the redo log files.

Explanation:

With the given CREATE TABLESPACE statement, the tablespace created can be changed to the LOGGING mode, and using the NOLOGGING clause in the statement will save space in the redo log files. The tablespace created using the NOLOGGING clause can be changed to the LOGGING mode by using the ALTER TABLESPACE statement with the LOGGING clause. When a tablespace is created by using the NOLOGGING clause, the operations in the tablespace will not generate any redo data. As a result, space will be saved in the redo log files. The objects created using the NOLOGGING clause cannot be recovered because no redo is generated for these objects. Therefore, the NOLOGGING clause should be used with objects that can be easily re-created without the redo data.

The option stating that the statement will generate an error because the NOLOGGING clause cannot be specified for the tablespace is incorrect. The clause is valid for the TBS1 tablespace. The LOGGING clause is not valid for a temporary or undo tablespace.

All the tables, indexes, and views created in the TBS1 tablespace will not be in the NOLOGGING mode because this can be overridden by specifying the LOGGING clause with the CREATE TABLE statement.

The option stating that a table created in the tablespace will consume less space because the tablespace is created with the NOLOGGING option is incorrect because tables created in this table will consume the same amount of space. Transactions on the table created using the NOLOGGING attribute will take less time compared to the time taken when the LOGGING attribute is used. This is because no redo data is generated when you use the NOLOGGING option.

Item: 7 (Ref:1Z0-042.5.3.1)

You have executed the following statement:

```
SQL> ALTER TABLESPACE SYSAUX RENAME TO SYSAUXTAB;
```

Which statement is true about executing this statement?

- The statement will fail because you cannot rename the SYSAUX tablespace.
- The statement will fail because you cannot rename tablespaces in Oracle 10*g*.
- The statement will change the name of the SYSAUX tablespace to SYSAUXTAB.
- The statement will drop the existing SYSAUX tablespace and re-create a new SYSAUX tablespace.

Answer:

The statement will fail because you cannot rename the SYSAUX tablespace.

Explanation:

The statement will fail because you cannot rename the SYSAUX tablespace. The `ALTER TABLESPACE...RENAME TO` statement allows you to rename only the following tablespaces:

- undo tablespaces
- read-only tablespaces
- temporary tablespaces
- default permanent tablespaces

The statement will not fail because you cannot rename tablespaces in Oracle 10*g*. You can rename tablespaces in Oracle 10*g* by using the `RENAME TO` clause of the `ALTER TABLESPACE` statement.

The statement will not change the name of the SYSAUX tablespace to SYSAUXTAB. You cannot rename the SYSAUX and SYSTEM tablespaces.

The statement will not drop the existing SYSAUX tablespace and then re-create a new SYSAUX tablespace. The `RENAME TO` clause of the `ALTER TABLESPACE` statement simply renames the tablespace name, and the Oracle database updates all the references of the tablespace in the data dictionary and the control file. However, you cannot rename the SYSAUX tablespace.

Item: 8 (Ref:1Z0-042.5.2.2)

On your Oracle database server, you have installed Oracle Database 10*g* software and set the COMPATIBLE initialization parameter to 10.0.0. After doing this, you create a database using the CREATE DATABASE statement. Click the Exhibit(s) button to view the statement used to create the database.

After the database creation, you create a tablespace using the following statement:

```
CREATE TABLESPACE DATA1 DATAFILE '/ORACLE/ORADATA/TS1.DBF' SIZE 50M;
```

Which statement is true regarding the tablespace created using this statement?

- The tablespace is a bigfile tablespace.
- The tablespace will be a locally-managed tablespace.
- The tablespace will be a dictionary-managed tablespace.
- The tablespace will have automatic segment space management.

Answer:

The tablespace will be a locally-managed tablespace.

```
CREATE DATABASE PROD1
     USER SYS IDENTIFIED BY SYSPASS
     USER SYSTEM IDENTIFIED BY SYSTEMPASS
     SET DEFAULT SMALLFILE TABLESPACE
     UNDO TABLESPACE UNDOTBS1
     DEFAULT TEMPORARY TABLESPACE TEMPTAB1;
```

Explanation:

The tablespace will be a locally-managed tablespace. In the given CREATE TABLESPACE statement, you do not provide an EXTENT MANAGEMENT clause. In Oracle 10*g*, all tablespaces created in the database have extent management as local by default. You should note that even though this is the default, the EXTENT MANAGEMENT LOCAL clause would be required if you wanted to specify the UNIFORM option to indicate that uniform-sized extents would be used.

The tablespace will not be a bigfile tablespace because the CREATE DATABASE statement used to create the database specifies that the default tablespace type is smallfile using the SET DEFAULT SMALLFILE TABLESPACE clause. When a tablespace is created without specifying the tablespace type, smallfile or bigfile, a smallfile tablespace will be created by default.

The tablespace will not be a dictionary-managed tablespace because in Oracle 10*g* all tablespaces created in the database have extent management as local by default. Because no EXTENT MANAGEMENT clause was included in the CREATE TABLESPACE statement, the extent management will be local.

The tablespace will not have automatic segment space management. It will have manual segment space management if no segment space management is specified while creating the tablespace.

Item: 9 (Ref:1Z0-042.5.5.1)

Eric is a newly hired database administrator for TelStar. He has been assigned the task of deleting the tablespaces that are not being used by any users. Eric issues the following statement to delete the PROD tablespace:

```
SQL> DROP TABLESPACE PROD INCLUDING CONTENTS;
```

Which statement regarding the result of executing this statement is true?

- The PROD tablespace and the data contained in it are deleted from the database.
- The PROD tablespace and the data contained in it are deleted from the database and the associated OS files are removed.
- The statement will return an error stating that the PROD tablespace cannot be dropped because it contains database objects.
- Only the PROD tablespace is removed from the database, and the data contained in PROD is transferred to the respective owner's default tablespace.

Answer:

The PROD tablespace and the data contained in it are deleted from the database.

Explanation:

With the DROP TABLESPACE...INCLUDING CONTENTS statement given in this scenario, the PROD tablespace and the data contained in it are deleted from the database. The DROP TABLESPACE...INCLUDING CONTENTS statement will delete the tablespace as well as the segments contained in it. Dropping a tablespace using this statement will not be possible if the tablespace is the default temporary tablespace or a part of the default temporary tablespace group.

The OS files associated with the tablespace are not deleted implicitly. They must be deleted using separate OS commands or by using the AND DATAFILES clause with the DROP TABLESPACE statement.

The statement will not return an error because the tablespace can be dropped from the database even if it contains database objects. However, you would receive an error if the segments in the tablespace are active and taking part in an ongoing transaction.

The data contained in the tablespace is deleted, but is not transferred to the owner's default tablespace. The DROP TABLESPACE statement does not transfer data to any other tablespace.

Item: 10 (Ref:1Z0-042.5.3.8)

Your junior DBA has placed a tablespace in your database offline by using the following statement:

```
SQL> ALTER TABLESPACE TS2 OFFLINE TEMPORARY;
```

Which two statements reflect results of altering the status of the tablespace by using this statement? (Choose two.)

- ☐ The statement will force a checkpoint to be performed in the database.
- ☐ The tablespace cannot be brought online without performing recovery on it.
- ☐ The statement will generate an error if some files in the tablespace are read-only.
- ☐ The tablespace can be brought online the next time without performing a recovery on it.
- ☐ All the datafiles in the tablespace need a recovery before the tablespace can be brought online.

Answer:

The statement will force a checkpoint to be performed in the database.
The tablespace can be brought online the next time without performing a recovery on it.

Explanation:

If the tablespace is placed offline using the `OFFLINE TEMPORARY` option of the `ALTER TABLESPACE` statement, the statement will force a checkpoint on all the online datafiles in the tablespace. Also, the tablespace can be brought online the next time without performing a recovery on it. When a tablespace is placed offline using the `OFFLINE TEMPORARY` option of the `ALTER TABLESPACE` statement, the tablespace is taken offline even if there are error conditions for one or more datafiles in the tablespace. If no datafiles in the tablespace are offline, the tablespace can be brought online without performing a recovery on it. If there are certain offline datafiles when the tablespace is taken offline using the `TEMPORARY` clause, you must perform a recovery on the datafiles before the tablespace can be brought online.

The option that states that the tablespace cannot be brought online without a recovery is incorrect because the tablespace can be brought online without a recovery on it. If the tablespace is taken offline by using the `OFFLINE IMMEDIATE` option, it cannot be brought online without performing a recovery on it. When the tablespace is taken offline using the `OFFLINE IMMEDIATE` option, the statement does not force a checkpoint on the datafiles of the tablespace. Therefore, whenever the tablespace is brought online after taking it offline using the `OFFLINE IMMEDIATE` option, you must perform a media recovery on the datafiles of the tablespace to bring the tablespace online.

The option that states that the statement will generate an error if some files in the tablespace are read-only is incorrect because the statement will not generate an error and will execute successfully even if some files in the tablespace are read-only.

The option that states that all the datafiles in the tablespace need a recovery before the tablespace can be brought online is incorrect because only the offline datafiles in the tablespace may need a recovery. All the other datafiles can be opened without a recovery performed on them.

Item: 11 (Ref:1Z0-042.5.1.2)

You are using locally-managed tablespaces in your database. Which three situations will NOT arise in your database? (Choose three.)

- contention on the SYSTEM tablespace
- free extents being managed by the data dictionary
- allocation and de-allocation of extents using bitmaps
- contention on a default temporary tablespace in the database
- the need to specify the default storage parameters when creating segments in these tablespaces

Answer:

contention on the SYSTEM tablespace

free extents being managed by the data dictionary

the need to specify the default storage parameters when creating segments in these tablespaces

---

Explanation:

When using locally-managed tablespaces in your database, the following conditions will not arise in your database:

- Contention on the SYSTEM tablespace - In a locally-managed tablespace, the recursive operations on the data dictionary table will be minimized. This will reduce the contention on the SYSTEM tablespace.
- Free extents being managed by the data dictionary - In a locally-managed tablespace, free extents will be managed using bitmaps, not the data dictionary.
- The need to specify default storage parameters when creating segments in these tablespaces - In a locally-managed tablespace, you are not required to specify storage parameters when creating objects because the space for the segments is managed using bitmaps.

The option stating that allocation and de-allocation of extents using bitmaps will not arise is incorrect because in locally-managed tablespaces, allocation and de-allocation of extents is done using bitmaps.

The option stating that contention on the temporary tablespace will not arise is incorrect. This is because using a locally-managed tablespace does not reduce contention on the temporary tablespace. Contention on a default temporary tablespace arises when there is lack of space in the tablespace and user transactions are waiting for the space to be freed for use. To eliminate contention on a temporary tablespace, you must allocate more space to the tablespace or modify the application so that it generates less temporary data to be stored in the tablespace. To allocate more space to the tablespace, you can add a datafile to the tablespace, increase the size of one or more datafiles of the tablespace, or set the AUTOEXTEND option to ON for the existing datafiles in the tablespace.

Item: 12 (Ref:1Z0-042.5.2.5)

You are working on your production database. The USERS tablespace of your database is running out of space. The USERS tablespace contains the D:\DATA\USERS01.DBF datafile of size 10 MB.

Which two statements will add more space to the datafile of the USERS tablespace? (Choose two.)

- ALTER DATABASE DATAFILE 'D:\DATA\USERS01.DBF' RESIZE 20M;
- ALTER DATABASE DATAFILE 'D:\DATA\USERS01.DBF' AUTOEXTEND ON;
- ALTER TABLESPACE USERS DATAFILE 'D:\DATA\USERS01.DBF' RESIZE 20M;
- ALTER TABLESPACE USERS ADD DATAFILE 'D:\DATA\USERS.DBF' SIZE 10M;
- ALTER TABLESPACE USERS DATAFILE 'D:\DATA\USERS01.DBF' AUTOEXTEND ON;

Answer:

ALTER DATABASE DATAFILE 'D:\DATA\USERS01.DBF' RESIZE 20M;
ALTER DATABASE DATAFILE 'D:\DATA\USERS01.DBF' AUTOEXTEND ON;

Explanation:

To add more space to the datafiles of a tablespace, you can either resize the datafile by using the ALTER DATABASE DATAFILE 'D:\DATA\USERS01.DBF' RESIZE 20M; statement or enable the autoextensible feature by using the ALTER DATABASE DATAFILE 'D:\DATA\USERS01.DBF' AUTOEXTEND ON; statement. The datafile can be resized to increase or decrease the size of the datafile. In the given scenario, the statement with the RESIZE option will increase the size of the datafile. The autoextensible feature of the datafile automatically enables the file size to increase after the file reaches the size it was assigned.

The options that use the ALTER TABLESPACE statement with the RESIZE option or the AUTOEXTEND option are incorrect because you cannot use the ALTER TABLESPACE statement to modify the size of the datafiles of the tablespace. You must use the ALTER DATABASE statement.

The option that adds a datafile to the tablespace by using the ALTER TABLESPACE USERS ADD DATAFILE 'D:\DATA\USERS.DBF' SIZE 10M; statement is incorrect because this statement adds a datafile to the tablespace and not more space to the existing datafile, USERS01.DBF, as required in this scenario.

Item: 13 (Ref:1Z0-042.5.3.6)

The undo tablespace of your database must be renamed. Which two conditions must be met to update the tablespace name in the server parameter file? (Choose two.)

- [ ] The database must be started by using the server parameter file.
- [ ] The database must be started by using the static initialization parameter file.
- [ ] A new undo tablespace must be created and made the default undo tablespace for your database.
- [ ] The UNDO_MANAGEMENT=MANUAL parameter must be specified for the database instance.
- [ ] The UNDO_TABLESPACE parameter must be specified to indicate the name of the undo tablespace of the database instance.

Answer:

The database must be started by using the server parameter file.
The UNDO_TABLESPACE parameter must be specified to indicate the name of the undo tablespace of the database instance.

Explanation:

The new undo tablespace name can be updated in the server parameter file if the following conditions are met:

- The database is started by using the server parameter file (SPFILE).
- The UNDO_TABLESPACE parameter is specified to indicate the name of the undo tablespace for the database instance.

When you rename the undo tablespace, the UNDO_TABLESPACE parameter in the server parameter file is updated with the new name of the undo tablespace.

The option stating that the database must be started by using the static initialization parameter file is incorrect. When you start the database with a traditional initialization parameter file (PFILE) and rename the undo tablespace, a message is generated in the alert log file. You must manually edit the initialization parameter file to change the value of the UNDO_TABLESPACE parameter with the new name of the undo tablespace. After the traditional initialization file is edited, the new server parameter file must be re-created.

The option stating that a new undo tablespace must be created and made the default undo tablespace for your database is incorrect. You can rename the undo tablespace even if the undo tablespace is being used as the default undo tablespace for the database.

The option stating that the UNDO_MANAGEMENT=MANUAL parameter must be specified for the database instance is incorrect because you can rename the tablespace even if the UNDO_MANAGEMENT=MANUAL parameter is not specified for the database.

Item: 14 (Ref:1Z0-042.5.3.2)

You are working on the PROD database that is running in the ARCHIVELOG mode. You want to drop the datafile that exists in the TS1 tablespace of the database.

Which sequence of steps will enable you to achieve this objective?

- Take the TS1 tablespace offline and then drop the datafile by using the ALTER TABLESPACE...DROP DATAFILE statement.
- Shut down the database, open it in the MOUNT state, and drop the datafile by using the ALTER DATABASE...DROP DATAFILE statement.
- Shut down the database, open it in the MOUNT state, and drop the datafile by using the ALTER TABLESPACE...DROP DATAFILE statement.
- Take the datafile offline by using the ALTER DATABASE...DATAFILE...OFFLINE statement, and drop the datafile by using the ALTER DATABASE...DROP DATAFILE statement.

Answer:

Take the datafile offline by using the ALTER DATABASE...DATAFILE...OFFLINE statement, and drop the datafile by using the ALTER DATABASE...DROP DATAFILE statement.

Explanation:

To drop a datafile from the database, you should take the datafile offline by using the ALTER DATABASE...DATAFILE...OFFLINE statement and then drop the datafile by using the ALTER DATABASE...DROP DATAFILE statement.

The datafile cannot be dropped by using the ALTER TABLESPACE...DROP DATAFILE statement. The DROP DATAFILE clause is not valid with the ALTER TABLESPACE statement.

The datafile belongs to a nonsystem tablespace. Therefore, you are not required to shut down the database and open it in the MOUNT state to drop a datafile.

The datafile cannot be dropped by using the ALTER TABLESPACE...DROP DATAFILE statement. The DROP DATAFILE clause is not valid for the ALTER TABLESPACE statement.

Item: 15 (Ref:1Z0-042.5.3.7)

You are working on your PROD database that contains the following configuration of tablespaces:

- PROD - tablespace used to store the nonsystem user data and is assigned to all nonsystem users as the default permanent tablespace
- IND1 - tablespace used to store the indexes created on nonsystem tables
- SYSTEM - tablespace used to store the system data
- SYSAUX - tablespace used as an auxiliary to the SYSTEM tablespace
- TEMP - tablespace used as the default temporary tablespace for the database
- UNDOTS - tablespace used as the default undo tablespace for the database

Which of the following statements is NOT true for the TEMP tablespace?

- You can drop the TEMP tablespace.
- You can assign the TEMP tablespace to database users.
- You cannot change the status of the TEMP tablespace from online to offline.
- You cannot convert the TEMP tablespace to a permanent tablespace.

Answer:

You can drop the TEMP tablespace.

Explanation:

The option that states that you can drop the TEMP tablespace is not true. You cannot drop the TEMP tablespace of the Oracle database if it is the default temporary tablespace. However, you can drop the TEMP tablespace if you have already created another default temporary tablespace and made it available to Oracle database users. In that situation, the other temporary tablespace becomes the default temporary tablespace for the database.

You can assign the TEMP tablespace to database users even if the tablespace is made the default temporary tablespace for the database.

You cannot change the status of the default temporary tablespace from online to offline. An error will be generated if you attempt to make the status of the temporary tablespace offline.

You cannot convert the default temporary tablespace to a permanent tablespace. According to the Oracle guidelines, a temporary tablespace cannot be converted to a permanent tablespace. You must create a new tablespace by using the CREATE TABLESPACE statement and specify the PERMANENT clause in the statement.

Item: 16 (Ref:1Z0-042.5.6.3)

Examine the details of the PROD database:

SYSTEM - Locally-managed system tablespace
SYSAUX - Locally-managed tablespace auxiliary to the SYSTEM tablespace
UNDO - Locally-managed default undo tablespace
TEMP1 - Temporary tablespace
DATA1 - Default permanent tablespace
USERS - Locally-managed tablespace to store user data
IND1 - Locally-managed tablespace to store index data

You create a user ADAM using the following statement:

```
SQL> CREATE USER ADAM IDENTIFIED BY PASSWORD;
```

Which two statements are true in the given scenario? (Choose two.)

- ☐ Tables created by ADAM will be stored in the DATA1 tablespace.
- ☐ Tables created by ADAM will be stored in the USERS tablespace.
- ☐ Tables created by ADAM will be stored in the SYSTEM tablespace.
- ☐ Sort data generated by ADAM's transactions will be stored in the IND1 tablespace.
- ☐ Sort data generated by ADAM's transactions will be stored in the TEMP1 tablespace.
- ☐ Sort data generated by ADAM's transactions will be stored in the SYSTEM tablespace.

Answer:

Tables created by ADAM will be stored in the DATA1 tablespace.
Sort data generated by ADAM's transactions will be stored in the SYSTEM tablespace.

Explanation:

In this scenario, tables created by ADAM will be stored in the DATA1 tablespace, and sort data generated by ADAM's transactions will be stored in the SYSTEM tablespace. The PROD database contains a default permanent tablespace DATA1, but does not contain a default temporary tablespace. When you create a user without assigning him a permanent and temporary tablespace, the tables created by the user will be stored in the default permanent tablespace for the database, and the sort data generated by the user's transactions will be stored in the default temporary tablespace of the database. If no default permanent tablespace is specified for the database, then the user's objects are stored in the SYSTEM tablespace, and if no default temporary tablespace is specified for the database, the user's sort data is stored in the SYSTEM tablespace. In this scenario, there is no default temporary tablespace in the database, so the sort data generated by ADAM's transactions will be stored in the SYSTEM tablespace. To avoid this, you can create a default temporary tablespace in the database or explicitly assign ADAM a temporary tablespace in the CREATE USER statement. In this scenario, a default permanent tablespace has been defined for the database, DATA1, so objects that ADAM creates will be stored in the DATA1 tablespace.

Tables created by ADAM will not be stored in the USERS tablespace because ADAM has not been granted any privileges on the tablespace and the USERS tablespace was not specified in the CREATE USER statement. The objects created by ADAM will be stored in the USERS tablespace when ADAM specifies the tablespace name during object creation and he has been granted the required privileges on the USERS tablespace.

Tables created by ADAM will not be stored in the SYSTEM tablespace because a default permanent tablespace, DATA1, exists for the database. A table created by ADAM will be stored in the SYSTEM tablespace when no default permanent tablespace exists for the database and ADAM does not explicitly specify any other tablespace name when creating the table.

Sort data generated by ADAM's transactions will not be stored in the IND1 tablespace. This sort data will be stored in the SYSTEM tablespace because no default temporary tablespace exists in the database. The IND1 tablespace is created to store the index data.

Sort data generated by ADAM's transactions will not be stored in the TEMP1 tablespace because the TEMP1 tablespace has not been assigned to ADAM as his temporary tablespace and the TEMP1 tablespace is not the default temporary tablespace for the database. Therefore, the sort data generated by ADAM's transactions will be stored in the SYSTEM tablespace.

Administering Users

Item: 1 (Ref:1Z0-042.6.4.2)

A system administrator issues the following statement to alter the profile of a user JOHN:

```
ALTER PROFILE PROF2 LIMIT
CPU_PER_SESSION 3600
IDLE_TIME 30;
```

As a result, how much CPU time and time of inactivity is allowed to the user JOHN in the next session?

- 6 hours of CPU time and 30 minutes of inactivity
- 60 minutes of CPU time and 30 minutes of inactivity
- 60 seconds of CPU time and 30 minutes of inactivity
- 36 seconds of CPU time and 30 seconds of inactivity

Answer:

60 seconds of CPU time and 30 minutes of inactivity

Explanation:

In the next session, JOHN is allowed 60 seconds of CPU time and 30 minutes of inactivity. CPU_PER_SESSION specifies the maximum CPU time measured in hundredths of seconds. Therefore, a CPU_PER_SESSION value of 3600 allows 60 seconds of CPU time to the next session for users assigned the PROF2 profile. IDLE_TIME specifies the allowed period of user inactivity and is expressed in minutes. Therefore, an IDLE_TIME of 30 allows the user JOHN 30 minutes of inactivity. The user JOHN's session is killed automatically if JOHN stays inactive for more than 30 minutes.

The option of 6 hours of CPU time and 30 minutes of inactivity is incorrect because the user will have only 60 seconds of CPU time. The CPU_PER_SESSION is specified in hundredths of seconds.

The option of 60 minutes of CPU time and 30 minutes of inactivity is incorrect because the user will have only 60 seconds of CPU time. The CPU_PER_SESSION is specified in hundredths of seconds.

The option of 36 seconds of CPU time and 30 seconds of inactivity is incorrect because the user will be allowed 30 minutes of inactivity. The IDLE_TIME is specified in minutes.

Item: 2 (Ref:1Z0-042.6.4.5)

ERIC is a database user on your database. When at work, ERIC's session times out frequently. This disrupts his progress.

What can be done to prevent this situation?

- Drop and re-create the user.
- Assign the CONNECT role to the user.
- Assign the RESOURCE role to the user.
- Modify the profile assigned to the user.
- Assign the required system privileges to the user.

Answer:

Modify the profile assigned to the user.

Explanation:

The maximum time for which the user is allowed to connect to the database is controlled by the profile assigned to the user and therefore, the user's profile should be modified. The CONNECT_TIME resource parameter specifies the maximum number of minutes for which a user can stay connected to the Oracle database. After the user remains connected to the database for the specified time, the user is automatically disconnected from the database. By modifying the profile, you can modify different resources assigned to the users. These resources include the CPU time, number of sessions created by a user, amount of SGA, logical reads, and the time for which the user can remain connected to the database.

The option to drop and re-create the user is incorrect because doing this does not modify the maximum time for which the user can remain connected to the database.

The option to assign the CONNECT role to the user is incorrect because assigning the CONNECT role gives several privileges to the user including the CREATE SESSION, CREATE TABLE, CREATE CLUSTER, CREATE DATABASE LINK, and CREATE SEQUENCE privileges. It does not modify the maximum time for which the user can remain connected to the database.

The option to assign the RESOURCE role to the user is incorrect because assigning the RESOURCE role does not make changes to the maximum time for which the user can remain connected to the database. The RESOURCE role includes the CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, and CREATE TYPE privileges.

The option to assign the required system privileges to the user is incorrect because by using the system privileges, you cannot modify the maximum time for which the user can remain connected to the database. System privileges are privileges required to perform a particular database operation or a set of database operations. Common system privileges include the CREATE TABLE, CREATE SESSION, ALTER TABLE, and DROP TABLE privileges.

Item: 3 (Ref:1Z0-042.6.2.2)

You are using Oracle Enterprise Manager 10*g* Database Control. You have created a user JOHN, and are assigning him the HR_MGR role. You have selected the DEFAULT check box.

Which statement best describes the result of selecting this check box?

- The user JOHN is granted the HR_MGR role.
- The user JOHN is granted the ownership of the HR_MGR role.
- The user JOHN is granted the HR_MGR role as his default role.
- The user JOHN is granted the HR_MGR role with the ADMIN option.

Answer:

The user JOHN is granted the HR_MGR role as his default role.

Explanation:

Using Oracle Enterprise Manager 10*g* Database Control, you can assign roles to users. A role can be made a default role for the user by selecting the DEFAULT check box. The default roles are automatically enabled for the user at logon, and the user does not need to enable the role explicitly by using the SET ROLE statement.

Selecting the DEFAULT check box does grant the HR_MGR role to the user JOHN. However, this role is assigned as the default role to the user JOHN, and he does not need to explicitly enable this role at logon.

Selecting the DEFAULT check box does not grant the user JOHN ownership of the HR_MGR role. A role in a database is neither owned by a user, nor does it belong to a particular schema in the database. A role needs to be assigned to a user so that the user can use the privileges granted to the role.

Selecting the DEFAULT check box does not grant the user the role with the ADMIN option. To assign the role with the ADMIN option, you can use the WITH ADMIN OPTION clause in the GRANT statement.

Item: 4 (Ref:1Z0-042.6.1.3)

As a database administrator, you are creating a user. You run the following statement to create the user:

```
SQL> CREATE USER ADAM IDENTIFIED BY PASSWORD
DEFAULT TABLESPACE SYSTEM
QUOTA 1M ON TS1
QUOTA 10M ON USERS
PROFILE USER_PROF;
```

What will be the result of running this statement?

- The user will not be able to change his password.
- The user will be assigned the database's default temporary tablespace, if one exists.
- The statement will fail because the temporary tablespace for the user has not been specified.
- The statement will fail because you cannot assign the SYSTEM tablespace as the user's default tablespace.

Answer:

The user will be assigned the database's default temporary tablespace, if one exists.

Explanation:

When you issue this statement, a user ADAM will be created. The SYSTEM tablespace will be the default tablespace and the default temporary tablespace of the database will be the default temporary tablespace of the user ADAM. The DEFAULT TABLESPACE clause of the CREATE USER statement is used to specify a default tablespace for the user. In this scenario, you specify DEFAULT TABLESPACE SYSTEM, which specifies that the SYSTEM tablespace will be used as ADAM's default tablespace. In this statement you do not explicitly specify a temporary tablespace for the user using the DEFAULT TEMPORARY TABLESPACE clause of the CREATE USER statement. Therefore, the database's default temporary tablespace will be used if one exists. If one does not exist, Oracle will use the SYSTEM tablespace.

The option that states that the user will not be able to change his password is incorrect because the statement does not specify any limitation on the password of the user.

The option that states that the statement will fail because the temporary tablespace for the user has not been specified is incorrect. It is not mandatory to specify the temporary tablespace when creating a user. If this is not specified, the user is assigned the database's default temporary tablespace, if one exists. If no default temporary tablespace exists for the database, then the SYSTEM tablespace is used to store the user's temporary data. This is also true for a permanent tablespace. If a user is not explicitly assigned a default permanent tablespace when the user is created, the user will be assigned the default permanent tablespace of the database, if one exists. If no default permanent tablespace exists for the database, then the SYSTEM tablespace stores the objects created by the user.

The option that states that the statement will fail because you cannot assign the SYSTEM tablespace as the user's default tablespace is incorrect. The SYSTEM tablespace can be assigned to a user as the user's default tablespace. However, this is not recommended.

Item: 5 (Ref:1Z0-042.6.3.2)

A user ERIC in your PROD database is the owner of the DETAIL, MASTER, and PRODUCT_DET tables. The tables are located on the TS1, USERS, and PRODUCTS tablespaces, respectively. New rows are constantly being added to the tables. The quotas for users on these tablespaces are rapidly exceeded, and no further insertions can be done before increasing the quotas for the users on these tablespaces.

Which is the best method for you to use to avoid this overhead of repeatedly modifying the quotas of the users?

- Grant the RESOURCE role to the users.
- Grant the UNLIMITED TABLESPACE role to the users.
- Grant the UNLIMITED TABLESPACE privilege to the users.
- Alter the users to ensure that they are granted unlimited quota on the three tables.
- Alter the users to ensure that they are granted unlimited quota on the three tablespaces.

Answer:

Grant the UNLIMITED TABLESPACE privilege to the users.

Explanation:

To avoid the overhead of repeatedly modifying quotas for the users, you can grant the users the UNLIMITED TABLESPACE privilege. This privilege will provide the users with unlimited space on all the tablespaces, and eliminate the requirement of increasing the quotas of the users.

Granting the RESOURCE role to the users is incorrect because the RESOURCE role does not ensure unlimited space on the tablespaces. The RESOURCE role grants you privileges such as CREATE PROCEDURE and CREATE TRIGGER.

UNLIMITED TABLESPACE is a privilege and not a role. Therefore, the option to grant the UNLIMITED TABLESPACE role to the users is incorrect.

Altering the users to ensure that they are granted unlimited quota on the three tables is incorrect because you cannot alter the quotas on the tables. You can only alter the quotas on tablespaces.

Altering the users to ensure that they are granted unlimited quota on the three tablespaces will require you to execute three different statements for the three different tablespaces. Therefore, this option is not the easiest way to accomplish this task.

Item: 6 (Ref:1Z0-042.6.4.4)

You are working in your production environment in which you are administering a large number of users. These users are posing a threat to your system by not being prompt in modifying their passwords. You want the users' passwords to expire in 30 days and to issue them a warning five days before the password expiration.

Which actions should you take to achieve this objective? (Choose all that apply.)

- Set the PASSWORD_LOCK_TIME parameter in the users' profile to 30 days.
- Set the PASSWORD_LIFE_TIME parameter in the users' profile to 30 days.
- Set the PASSWORD_LOCK_TIME parameter in the users' profile to five days.
- Set the PASSWORD_LIFE_TIME parameter in the users' profile to five days.
- Set the PASSWORD_GRACE_TIME parameter in the users' profile to 25 days.
- Set the PASSWORD_GRACE_TIME parameter in the users' profile to five days.

Answer:

Set the PASSWORD_LIFE_TIME parameter in the users' profile to 30 days.
Set the PASSWORD_GRACE_TIME parameter in the users' profile to five days.

Explanation:

To ensure that the users' passwords expire in 30 days, you must set the PASSWORD_LIFE_TIME parameter in the users' profile to 30 days. The PASSWORD_LIFE_TIME parameter indicates the number of days that a user can use the same password. To ensure that the users are issued a warning five days before the password expiration, you must also set the PASSWORD_GRACE_TIME parameter in the users' profile to five days. The PASSWORD_GRACE_TIME parameter indicates the number of days a user will receive a warning about a pending password expiration.

Setting the PASSWORD_LOCK_TIME parameter in the users' profile is incorrect. The PASSWORD_LOCK_TIME parameter is set to lock a user's account for a specified number of days after the user fails to log in after the specified number of failed login attempts, identified by FAILED_LOGIN_ATTEMPTS.

Setting the PASSWORD_LOCK_TIME parameter in the users' profile to five days is incorrect. The PASSWORD_LOCK_TIME parameter is set to lock a user's account for a specified number of days after the user fails to log in after the specified number of failed login attempts.

Setting the PASSWORD_LIFE_TIME parameter in the users' profile to a value of five days is incorrect because you want the passwords to expire in 30 days.

Setting the PASSWORD_GRACE_TIME parameter in the users' profile to 25 days is incorrect because you must set this value to five days. Setting it to 25 days would issue a warning to the users 25 days before the expiration of the password.

Item: 7 (Ref:1Z0-042.6.1.1)

John is a database administrator at GlobeComm Corporation. John has been assigned the task of creating users. He issues the following statements to create a user BARRY and grant privileges to the user:

```
SQL> CREATE USER BARRY IDENTIFIED BY PASSWORD
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP
QUOTA 2M ON PROD
PASSWORD EXPIRE
ACCOUNT LOCK;
SQL> GRANT CREATE SESSION, CREATE TABLE TO BARRY;
```

Which statements correctly describe the user BARRY? (Choose all that apply.)

- ☐ The password assigned to BARRY will never expire.
- ☐ BARRY can create a table in the USERS tablespace.
- ☐ BARRY cannot create a table in the USERS tablespace.
- ☐ BARRY does not have privileges on the TEMP tablespace.
- ☐ BARRY cannot access his account without the intervention of the DBA.

Answer:

BARRY cannot create a table in the USERS tablespace.
BARRY does not have privileges on the TEMP tablespace.
BARRY cannot access his account without the intervention of the DBA.

Explanation:

In this scenario, BARRY cannot create a table in the USERS tablespace, BARRY does not have privileges on the TEMP tablespace, and BARRY cannot access his account without the intervention of the DBA. The CREATE USER statement creates a user BARRY and assigns him the password, PASSWORD. After the first successful login, the PASSWORD EXPIRE clause will expire the password, and BARRY will be prompted to change his password. The ACCOUNT LOCK clause locks the user account immediately upon creation, and BARRY cannot access his account unless the DBA unlocks his account. BARRY cannot create a table in the USERS tablespace because BARRY has not been given any quota on the USERS tablespace. BARRY does not have privileges on the TEMP tablespace because he has not been given any quota on the TEMP tablespace.

The option stating that the password assigned to BARRY will never expire is incorrect. The password assigned to BARRY will expire. In this scenario, the PASSWORD EXPIRE clause specifies that the password will expire. After an initial successful login, the password will expire, and BARRY will be prompted to change his password.

The option stating that BARRY can create a table in the USERS tablespace is incorrect because BARRY has not been assigned any quota on the USERS tablespace.

Item: 8 (Ref:1Z0-042.6.1.4)

You created a user SUSAN in your database and assigned her the MANAGER profile. Later, you assigned the SYSDBA privilege to the user to enable the user to perform some administration tasks on the database. After some time, you realize that you do not require the MANAGER profile and decide to drop the profile.

What is the result of dropping the profile from the database?

- The user will not have any profile.
- The user will have the default profile.
- The user will have the MANAGER profile.
- The user will have the profiles assigned to the SYS and SYSTEM users.
- An error will be received stating the profile is assigned to users in the database and cannot be dropped.

Answer:

The user will have the default profile.

Explanation:

In this scenario, the user will have the default profile because no other profile has been assigned to her. The SYSDBA privilege does not affect the profile assigned to the user. When a profile assigned to the user is dropped from the database and you do not assign any other profile to the user, the user will have the default profile.

The option stating that the user will have no profile is incorrect because the user always has the default profile if no profile has been assigned explicitly.

The option stating that the user will have the MANAGER profile is incorrect because the MANAGER profile has been dropped from the database.

The option stating that the user will have the profiles of the SYS and SYSTEM users is incorrect because having the SYSDBA privilege does not give a user the profiles assigned to the SYSTEM user. Also, a user cannot have two profiles at any given time.

The option stating that an error will be received stating the profile is assigned to users in the database and cannot be dropped is incorrect. A profile can be dropped from the database even if it is assigned to users. Any users in the database assigned this profile will be assigned the default profile.

Item: 9 (Ref:1Z0-042.6.2.1)

During a single session, you run the following set of statements in your database:

```
SQL> CREATE USER SCOTT IDENTIFIED BY SCOTT;
SQL> CREATE ROLE HR_ADMIN;
SQL> GRANT SELECT ANY TABLE TO HR_ADMIN;
SQL> GRANT CREATE ANY VIEW TO HR_ADMIN;
SQL> GRANT HR_ADMIN TO SCOTT;
```

The database user SCOTT tries to execute a SELECT statement against a table in the HR user's schema, but the following error is generated:

```
SQL> SELECT * FROM HR.TRAINING;

ORA-01031: insufficient privileges
```

Which two could be the possible reasons for this error? (Choose two.)

- ☐ The HR_ADMIN role is a secured application role.
- ☐ The HR_ADMIN role has not been set as the default role for the user SCOTT.
- ☐ A password must be provided to access the privileges granted by the HR_ADMIN role.
- ☐ The user HR has not granted select access on the TRAINING table to the user SCOTT.
- ☐ The user SCOTT has not enabled the HR_ADMIN role by using the SET ROLE statement.

Answer:

The HR_ADMIN role has not been set as the default role for the user SCOTT.

The user SCOTT has not enabled the HR_ADMIN role by using the SET ROLE statement.

Explanation:

The two possible reasons for this error are that the HR_ADMIN role has not been set as the default role for the user SCOTT or that the user SCOTT has not enabled the HR_ADMIN role by using the SET ROLE statement. When a role is assigned to a user, the role must be enabled using the SET ROLE statement or the role must be set as the default role for the user so that the user can access the privileges granted to them through the role. The default role is enabled for the user at log on. A non-default role must be enabled using the SET ROLE statement. If the role is not enabled for the user, the user cannot access the privileges. The HR_ADMIN role created in this scenario is granted the SELECT ANY TABLE privilege and the CREATE ANY VIEW privilege. The SELECT ANY TABLE privilege enables you to issue SELECT statements against any tables in any user's schema. The CREATE ANY VIEW privilege enables you to create views based on any table in any user's schema. Apart from having the CREATE ANY VIEW privilege, the user must also have SELECT privileges on the tables on which he is trying to create the view. If the user does not have SELECT privileges on the table on which he is trying to create the view, the user SCOTT will receive an error stating he does not have the required privileges.

The HR_ADMIN role created in this scenario is not a secure application role. A secure application role is created using the USING package clause in the CREATE ROLE statement. An application role is a role that can be enabled only by applications by using an authorized PL/SQL package.

A user does not need to provide a password to access the privileges of the HR_ADMIN role because the role is not password protected. A password protected role can be created using the IDENTIFIED BY clause in the CREATE ROLE statement. When enabling a password protected role, you must provide the password to enable the role.

The user SCOTT does not need specific privileges on the HR.TRAINING table because the HR_ADMIN role provides the SELECT ANY TABLE privilege. The SELECT ANY TABLE privilege will allow users granted the privilege to query tables in any database schema. The user SCOTT will receive this privilege through the HR_ADMIN role.

Item: 10 (Ref:1Z0-042.6.1.5)

The default temporary tablespace, TEMP, for your database has become corrupt because of bad disks. To ensure that the database functions properly, the users of the TEMP tablespace and any new users created in the database must use the newly created NEW_TEMP tablespace instead.

What would be the best action to take to enable this?

- While creating any new user, assign the NEW_TEMP tablespace as the temporary tablespace.
- Alter all the users in the database and assign the NEW_TEMP tablespace as their temporary tablespace.
- Drop the TEMP tablespace and ask the users to use the NEW_TEMP tablespace for storing the temporary data.
- Alter the database and make the NEW_TEMP tablespace the default temporary tablespace for the database.

Answer:

Alter the database and make the NEW_TEMP tablespace the default temporary tablespace for the database.

Explanation:

You should alter the database and make the NEW_TEMP tablespace the default temporary tablespace for the database. You should change the default temporary tablespace for the database to ensure that the users in the database use the new default temporary tablespace, NEW_TEMP, instead of the old default temporary tablespace. All users created that do not explicitly have a different temporary tablespace specified use the default temporary tablespace.

The option stating that while creating any new user, you should assign the NEW_TEMP tablespace as the temporary tablespace is incorrect because doing this will only change the temporary tablespace for the new user. The present users in the database will continue to use the TEMP tablespace.

The option stating that you should alter all the users in the database and assign the NEW_TEMP tablespace as their temporary tablespace is incorrect because this will not take care of new users created in the database. In addition, you would then have to explicitly specify the new temporary tablespace as the temporary tablespace for all new users. Any new users created without being assigned a temporary tablespace will continue to use the TEMP tablespace.

The option stating you should drop the TEMP tablespace and ask the users to use the NEW_TEMP tablespace to store the temporary data is incorrect because you cannot drop the default temporary tablespace from the database.

Item: 11 (Ref:1Z0-042.6.4.3)

You must limit the amount of CPU time that a user session can utilize.

Which resource parameter in the user's profile will you modify to achieve this objective?

- CONNECT_TIME
- CPU_PER_CALL
- CPU_PER_SESSION
- LOGICAL_READS_PER_SESSION

Answer:

CPU_PER_SESSION

Explanation:

The CPU_PER_SESSION resource parameter limits the amount of CPU time that a user session can utilize. By default, this parameter is assigned a value of UNLIMITED. This value provides unlimited CPU time to user sessions. Therefore, to limit the CPU time per user session, you assign a specific value to this parameter. The value of this parameter is specified in hundredths of a second. For example, to limit the amount of CPU time for one user session to five seconds, you assign a value of 500 to the CPU_PER_SESSION resource parameter. When a user session exceeds the limit specified by this parameter, the following error will be generated and the user will be logged off from the database:

```
ORA-02392: exceeded session limit on CPU usage, you are being logged off
```

The CONNECT_TIME resource parameter limits the time for which a user can remain connected to the database. This parameter does not limit the amount of CPU time that a user session can utilize.

The CPU_PER_CALL resource parameter limits the amount of CPU time used by a database call. This parameter value is specified in hundredths of a second. For example, to limit the amount of CPU time available to a database call to five seconds, you assign a value of 500 to the CPU_PER_CALL resource parameter.

The LOGICAL_READS_PER_SESSION resource parameter limits the number of data blocks read in a user's session. This parameter helps to control user session activities by limiting a user's read access to the data blocks from the disk and memory.

Item: 12 (Ref:1Z0-042.6.2.3)

You have created a role, WORK_USER, with a set of system and object privileges. You grant this role to a group of users. These users need to perform additional tasks in the database and therefore, there is a need to assign a few more privileges to this group of users. You modify the WORK_USER role and grant the required privileges to this role.

Which two statements are true? (Choose two.)

- ☐ The roles that are granted this role will get the new set of privileges.
- ☐ The users who are assigned the role will get the new set of privileges immediately.
- ☐ The users that are granted this role in the future will get only the new set of privileges.
- ☐ The users who are assigned the role will get the new set of privileges in their next session.
- ☐ The users will need to disable the role and re-enable it to get the new set of privileges.

Answer:

The roles that are granted this role will get the new set of privileges.
The users who are assigned the role will get the new set of privileges immediately.

Explanation:

When you grant a new set of privileges to a role that is already assigned to users, then the users who are assigned the role will acquire the modified or new set of privileges automatically and immediately. The roles that are granted this particular role also acquire the new privileges immediately.

The users who are granted this role in the future will get all the privileges granted to this role and not just the new privileges granted to this role.

The users who are assigned this role will get the new set of privileges immediately, not in their next session.

The users do not need to re-enable the role to acquire the new set of privileges.

Item: 13 (Ref:1Z0-042.6.4.6)

Mark is a team manager of your company's Oracle development team. He is required to work on a new project that involves more resource use. As a DBA, you do not know how much resources he requires to complete this project because the client requirement is still expanding. You have decided to allow him full resource use rights.

Which action should you take to enable this?

- Specify the user as a member of the `DEFAULT_CONSUMER_GROUP`.
- Create a profile with `RESOURCE_LIMIT=null` and assign it to the user.
- Create a profile and specify the `NO LIMIT` value for all resource parameters. Then, assign the profile to the user.
- Create a profile and specify the `UNLIMITED` value for all resource parameters. Then, assign the profile to the user.

Answer:

Create a profile and specify the `UNLIMITED` value for all resource parameters. Then, assign the profile to the user.

Explanation:

To enable unlimited access to the resources, you should create a profile and specify the `UNLIMITED` value for all resource parameters. Then, assign this profile to the user. After this profile is assigned to the user, the user will have unlimited access to all the resources.

The option that states you should specify the user as a member of the `DEFAULT_CONSUMER_GROUP` is incorrect because specifying the user as a member of the `DEFAULT_CONSUMER_GROUP` does not allow full resource use rights to the user. The `DEFAULT_CONSUMER_GROUP` is the initial consumer resource group that is always present in the data dictionary and cannot be altered or dropped. This group is granted to all the users in the database who have not been granted any resource group explicitly. The `DEFAULT_CONSUMER_GROUP` grants the switch privilege to `PUBLIC`. The switch privilege allows the users to switch between their current resource consumer groups to a specified resource consumer group.

The option that states you should create a profile with `RESOURCE_LIMIT=null` and assign it to a user is incorrect because the `RESOURCE_LIMIT` parameter is an initialization parameter and cannot be specified in profiles. The `RESOURCE_LIMIT` parameter is set to enforce resource limits on profiles.

The option that states you should create a profile and specify the `NO LIMIT` value for all resource parameters and then assign the profile to the user is incorrect because the `NO LIMIT` value is not a valid value for resource parameters.

Item: 14 (Ref:1Z0-042.6.1.2)

You have created a user GLENN in your Oracle database. You have two permanent tablespaces, PROD and DATA, to store the users' data. You must ensure that the user GLENN does not create any objects in the DATA tablespace and uses only the PROD tablespace to create database objects.

Which statements will you execute to ensure this?

- ALTER USER GLENN QUOTA UNLIMITED ON PROD AND DATA;
- ALTER USER GLENN QUOTA 0M ON DATA;
  ALTER USER GLENN QUOTA UNLIMITED ON PROD;
- ALTER USER GLENN QUOTA NULL ON DATA;
  ALTER USER GLENN QUOTA UNLIMITED ON PROD;
- ALTER USER GLENN QUOTA UNLIMITED ON DATA;

  ALTER USER GLENN QUOTA 0M ON PROD;

Answer:

ALTER USER GLENN QUOTA 0M ON DATA;
ALTER USER GLENN QUOTA UNLIMITED ON PROD;

Explanation:

You will execute the ALTER USER GLENN QUOTA 0M ON DATA; and the ALTER USER GLENN QUOTA UNLIMITED ON PROD; statements. The ALTER USER GLENN QUOTA 0M ON DATA; statement allocates no quota on the DATA tablespace. The ALTER USER GLENN QUOTA UNLIMITED ON PROD; statement allocates unlimited quota on the PROD tablespace. Therefore, these statements ensure that the user GLENN cannot create any objects in the DATA tablespace, and can only use the PROD tablespace to create database objects.

The ALTER USER GLENN QUOTA UNLIMITED ON PROD AND DATA; statement is syntactically incorrect.

The ALTER USER GLENN QUOTA UNLIMITED ON PROD; statement allocates unlimited quota on the PROD tablespace to the user GLENN. However, the ALTER USER GLENN QUOTA NULL ON DATA; statement generates an error because the statement is syntactically incorrect.

The ALTER USER GLENN QUOTA UNLIMITED ON DATA; statement allocates unlimited quota on the DATA tablespace, and the ALTER USER GLENN QUOTA 0M ON PROD; statement allocates no quota on the PROD tablespace to the user GLENN. Therefore, the user GLENN cannot create any objects on the PROD tablespace, and can only use the DATA tablespace to create database objects. This is the opposite of what you wanted to ensure.

Item: 15 (Ref:1Z0-042.6.4.1)

In your database, the user JOHN is creating numerous sessions. You want to restrict the number of sessions JOHN can create. You assign a profile to JOHN and restrict the number of user sessions that he can create. However, you realize that the restrictions are not being enforced.

Which initialization parameter must you modify to enforce the limit?

- RESOURCE_LIMIT
- CPU_PER_SESSION
- LICENSE_MAX_USERS
- SESSIONS_PER_USER
- LICENSE_MAX_SESSIONS

Answer:

RESOURCE_LIMIT

Explanation:

You must modify the RESOURCE_LIMIT initialization parameter. After you assign profiles to users, the Oracle database enforces the limits only when the RESOURCE_LIMIT parameter is set to TRUE. Therefore, you modify the RESOURCE_LIMIT initialization parameter to enforce the resource limits defined within each user's profile.

The CPU_PER_SESSION option is incorrect because it is a resource parameter that limits the amount of CPU time a user session can utilize. This parameter does not enforce the resource limits defined within the user's profile.

The LICENSE_MAX_USERS option is incorrect because this initialization parameter is used to limit the number of users that can be created in a database. This parameter does not enforce the resource limits defined within the user's profile.

The SESSIONS_PER_USER option is incorrect because it is a resource parameter and not an initialization parameter. This parameter is used to restrict the maximum number of concurrent sessions that a database user can create.

The LICENSE_MAX_SESSIONS option is incorrect because this initialization parameter is used to limit the number of concurrent user sessions in the database. This parameter does not limit the number of sessions created by a particular database user.

Item: 16 (Ref:1Z0-042.6.3.1)

You have created a new user, BOB, by executing the following statement:

```
SQL> CREATE USER BOB IDENTIFIED BY PASSWORD;
```

You have not granted privileges to the user BOB.

Which three roles and privileges are mandatory for the user BOB to create a table in the default tablespace? (Choose three.)

- CREATE VIEW
- CREATE TABLE
- RESOURCE
- CREATE SESSION
- SELECT ANY TABLE
- RESTRICTED SESSION
- UNLIMITED TABLESPACE

Answer:

CREATE TABLE
CREATE SESSION
UNLIMITED TABLESPACE

Explanation:

To create a table in the default tablespace assigned to the user, the user requires the CREATE TABLE, CREATE SESSION, and UNLIMITED TABLESPACE privileges. The CREATE SESSION privilege will enable the user to establish a session with the Oracle database. The UNLIMITED TABLESPACE privilege will grant the user an unlimited quota on the assigned tablespace. The user can also be granted quota on the default tablespace for creating tables on the default tablespace. Finally, the CREATE TABLE privilege will enable the user to create a table in the tablespace.

The CREATE VIEW privilege enables a user to create a view. The privilege does not allow a user to create a table.

The RESOURCE role is not required in this scenario because the RESOURCE role provides you with privileges such as CREATE PROCEDURE and CREATE TRIGGER. The user BOB requires only the CREATE TABLE system privilege. Therefore, you need not grant the user BOB the RESOURCE role.

The SELECT ANY TABLE privilege is not required in this scenario because the user is not trying to access the data in the tables. The SELECT ANY TABLE privilege is required when a user tries to access the tables created by other users.

The RESTRICTED SESSION privilege is not required in this scenario because the user is not connecting to the database when the database is opened in the RESTRICTED mode. You require the RESTRICTED SESSION privilege only if you are trying to connect to a database that is opened in the RESTRICTED mode.

Item: 17 (Ref:1Z0-042.6.3.3)

You are a DBA in your organization. You want to identify the set of privileges granted to the user SCOTT on the EMPLOYEE table owned by the user JACK.

Which view will provide the required information?

- DBA_SYS_PRIVS
- DBA_TAB_PRIVS
- USER_SYS_PRIVS
- USER_TAB_PRIVS

Answer:

DBA_TAB_PRIVS

Explanation:

The DBA_TAB_PRIVS view provides information regarding the privileges granted to the user on the objects owned by other users.

The DBA_SYS_PRIVS view provides information regarding the system privileges granted to the users and roles.

The USER_SYS_PRIVS view provides information regarding the system privileges granted to the current user.

The USER_TAB_PRIVS view provides information regarding the object privileges for objects owned by the user, granted to the current user or granted by the current user.

Managing Schema Objects

Item: 1 (Ref:1Z0-042.7.3.1)

You have a table named EMPLOYEES. Given these attributes of the table:

1. the column attributes
2. the constraints created on the table
3. the storage attributes for the table
4. the segments associated with the table

Which attributes of the EMPLOYEES table can you view using Oracle Enterprise Manager?

- only 1
- only 1 and 2
- only 1 and 3
- only 1, 2, and 4
- 1, 2, 3, and 4

Answer:

1, 2, 3, and 4

Explanation:

Using Oracle Enterprise Manager, you can view various attributes of a table, such as the column attributes, the constraints created on the table, the storage attributes for the table, and the segments associated with the table.

All the other options are incorrect because you can use Oracle Enterprise Manager to view all of these attributes.

Item: 2 (Ref:1Z0-042.7.2.3)

You change the state of a PRIMARY KEY constraint of a table from ENABLE VALIDATE to DISABLE VALIDATE by using the following statement:

```
SQL> ALTER TABLE MASTER PRIMARY KEY DISABLE VALIDATE;
```

Which two statements are true in reference to the primary key in this scenario? (Choose two.)

- The constraint checking will be disabled.
- The index on the primary key will be disabled.
- The primary key cannot be dropped from the table.
- The table can contain data that violates the constraint.
- The modification of old constrained data that the table contains is allowed.
- Rows containing data that violates the PRIMARY KEY constraint cannot be inserted in the table.

Answer:

The constraint checking will be disabled.
The table can contain data that violates the constraint.

Explanation:

When the state of a constraint is changed from ENABLE VALIDATE to DISABLE VALIDATE, the constraint checking on the table is disabled, and the table can contain data violating the PRIMARY KEY constraint. The index on the primary key will also be dropped from the table. The DISABLE VALIDATE clause is used to disable an integrity constraint.

The option stating that the index on the primary key will be disabled is incorrect because this index will be dropped from the table. This index will be re-created when you modify the state of the primary key to ENABLE VALIDATE.

The option stating that the primary key cannot be dropped from the table is incorrect because the primary key can be dropped from the table even if the constraint is in the DISABLE VALIDATE state.

The option stating that the modification of old constrained data in the table is allowed is incorrect because the modification of old constrained data in the table is not allowed. When the constraint state is DISABLE VALIDATE, the old constrained data in the table cannot be changed. The data will always satisfy the constraint condition.

The option stating that rows containing data that violates the PRIMARY KEY constraint cannot be inserted in the table is incorrect because disabling the constraint allows you to insert data violating the constraint.

Item: 3 (Ref:1Z0-042.7.2.2)

Your database has two tables, MASTER and EMP_MASTER. You want to alter the EMP_MASTER table to create a foreign key on its CODE column, which refers to the CODE column of the MASTER table. You also want to ensure that when you delete a row from the MASTER table, the child records are deleted from the EMP_MASTER table automatically.

Which statement should you use for this purpose?

- `ALTER TABLE EMP_MASTER (`
  `FOREIGN KEY (CODE) REFERENCES MASTER);`
- `ALTER TABLE EMP_MASTER (`
  `FOREIGN KEY (CODE) REFERENCES MASTER ON DELETE CASCADE);`
- `ALTER TABLE EMP_MASTER (`
  `FOREIGN KEY (CODE) REFERENCES MASTER ON DELETE SET NULL);`
- `ALTER TABLE EMP_MASTER (`
  `FOREIGN KEY (CODE) REFERENCES MASTER CASCADE CONSTRAINTS);`

Answer:

`ALTER TABLE EMP_MASTER (`
`FOREIGN KEY (CODE) REFERENCES MASTER ON DELETE CASCADE);`

Explanation:

In the given scenario, you should use the `ALTER TABLE EMP_MASTER (FOREIGN KEY (CODE) REFERENCES MASTER ON DELETE CASCADE);` statement. If you need to create a foreign key in such a way that deleting a row in the parent table will delete the corresponding rows in the child table, you should use the `ON DELETE CASCADE` option when creating the `FOREIGN KEY` constraint.

You should not use the `ALTER TABLE EMP MASTER (FOREIGN KEY (CODE) REFERENCES MASTER);` statement. Not specifying any of the options when creating a foreign key will generate an error if you try to delete a row from the parent table that has corresponding rows in the child table.

You should not use the `ALTER TABLE EMP MASTER (FOREIGN KEY (CODE) REFERENCES MASTER ON DELETE SET NULL);` statement. If the `FOREIGN KEY` constraint is created with the `ON DELETE SET NULL` option and a row is deleted from the parent table, the referenced column in the child table will be set to `NULL`.

You should not use the `ALTER TABLE EMP MASTER (FOREIGN KEY (CODE) REFERENCES MASTER CASCADE CONSTRAINTS);` statement. The `CASCADE CONSTRAINTS` option cannot be used in the `ALTER TABLE` statement. The `CASCADE CONSTRAINTS` option is used when dropping tables that have referential integrity constraints defined on other objects.

Item: 4 (Ref:1Z0-042.7.1.2)

You must shrink the EMP table and its dependent segments to release the unused space below and above the High Water Mark (HWM) of the segments. The EMP table and its dependant segments are located in the USERS tablespace, which uses automatic segment space management.

Which statement should you use to release the space below the HWM?

- `ALTER TABLE EMP COALESCE;`
- `ALTER TABLE EMP SHRINK SPACE;`
- `ALTER TABLE EMP SHRINK SPACE CASCADE;`
- `ALTER TABLE EMP SHRINK SPACE INCLUDING CONTENTS;`
- You cannot release the space because the USERS tablespace uses automatic segment space management.

Answer:

`ALTER TABLE EMP SHRINK SPACE CASCADE;`

Explanation:

To shrink the EMP table and its dependent segments, you should use the `ALTER TABLE EMP SHRINK SPACE CASCADE;` statement. Shrinking of segments is a new concept introduced in Oracle 10*g*. Using the CASCADE clause with the SHRINK SPACE clause of the ALTER TABLE statement also shrinks all the dependant segments of the EMP table. For example, if an index is associated with the EMP table, the `ALTER TABLE EMP SHRINK SPACE CASCADE;` statement, in addition to shrinking the EMP table, shrinks the index and releases the unused space below and above the HWM of the segments. You should note that for shrinking the space in a table, the table should be located in a tablespace on which automatic segment space management is enabled. If the table is located in a tablespace on which manual segment space management is enabled, you cannot shrink the table.

The `ALTER TABLE EMP COALESCE;` statement is incorrect because it will generate an error. The COALESCE option cannot be used while altering a table. The COALESCE option is used with the ALTER INDEX statement to coalesce the leaf blocks in indexes.

The `ALTER TABLE EMP SHRINK SPACE;` statement releases only the unused space below and above the HWM of the EMP table and not in its dependent segments because it does not include the CASCADE clause.

The `ALTER TABLE EMP SHRINK SPACE INCLUDING CONTENTS;` statement is incorrect because the INCLUDING CONTENTS clause is not valid with the ALTER TABLE statement. The INCLUDING CONTENTS clause is used with the DROP TABLESPACE statement when dropping tablespaces.

You can release the space because the USERS tablespace uses automatic segment space management. You cannot use the SHRINK SPACE clause to shrink a table that resides in a tablespace that uses manual segment space management.

Item: 5 (Ref:1Z0-042.7.8.1)

You have just created a sequence, MASTER_SEQ, for generating unique values for the ID column of your MASTER table. Which statement issued on the newly created sequence will complete successfully?

- SELECT MASTER_SEQ FROM DUAL;
- SELECT MASTER_SEQ.NEXTVAL FROM DUAL;
- SELECT MASTER_SEQ.CURRVAL FROM DUAL;
- SELECT MASTER_SEQ.CURRVAL FROM MASTER;
- SELECT MASTER_SEQ.NEXTVAL FROM MASTER;

Answer:

SELECT MASTER_SEQ.NEXTVAL FROM DUAL;

Explanation:

Only the SELECT MASTER_SEQ.NEXTVAL FROM DUAL; statement will complete successfully. The statement will complete successfully because to use a sequence you must first reference the NEXTVAL pseudocolumn of the sequence. Only then can you refer to the CURRVAL pseudocolumn of the sequence. The first reference to the NEXTVAL returns the initial value of the sequence. After this, any reference to the CURRVAL will return the current value of the sequence. Any subsequent references to the NEXTVAL will return the next value in the sequence.

The SELECT MASTER_SEQ FROM DUAL; statement is incorrect because none of the pseudocolumns have been referred to in the given statement.

The SELECT MASTER_SEQ.CURRVAL FROM DUAL; statement is incorrect because the CURRVAL pseudocolumn cannot be referenced until the sequence is initialized by referencing the NEXTVAL pseudocolumn. Considering the fact that this is the first statement issued after sequence creation, the statement will give an error stating that the NEXTVAL pseudocolumn must be referenced first.

The SELECT MASTER_SEQ.CURRVAL FROM MASTER; statement is incorrect because the statement is syntactically incorrect. Although the sequence has been created to generate unique values for the MASTER table, the sequence cannot be referred to in this manner.

The SELECT MASTER_SEQ.NEXTVAL FROM MASTER; statement is incorrect because the statement is syntactically incorrect. Although the sequence has been created to generate unique values for the MASTER table, the sequence cannot be referred to in this manner.

Item: 6 (Ref:1Z0-042.7.2.1)

You create a primary key on the CODE column in your MASTER table using the following statement:

```
SQL> ALTER TABLE MASTER ADD CONSTRAINT PRIMARY KEY (CODE);
```

Which statements are true if the constraint is created successfully? (Choose all that apply.)

- ☐ The primary key created will be in the deferred state.
- ☐ A NOT NULL constraint will be created on the CODE column.
- ☐ A unique index will be created on the CODE column of the table.
- ☐ A CHECK constraint will be created on the CODE column of the table.
- ☐ No index will be created because this is not specified by the statement.

Answer:

A NOT NULL constraint will be created on the CODE column.

A unique index will be created on the CODE column of the table.

Explanation:

Issuing the statement in the given scenario to create a primary key on the CODE column of the MASTER table will create a unique index on the CODE column and also create a NOT NULL constraint on the CODE column. Whenever a primary key is created on a column in a table, a unique index is created on the column to ensure the uniqueness of the primary key, and a NOT NULL constraint is created on the column to ensure that the primary key column does not contain null values.

The primary key created by issuing the statement in this scenario will not be in the deferred state because you have not specified the DEFERRABLE clause in the ALTER TABLE statement. By default, a primary key will be created in the immediate state.

A CHECK constraint will not be created on the CODE column because you are issuing a statement only to create a PRIMARY KEY constraint. A CHECK constraint can be created using the ADD CONSTRAINT CHECK(*condition*) clause in the CREATE TABLE or ALTER TABLE statement. A CHECK constraint is created to specify one or more conditions that each row of the table must satisfy.

The option stating that no index will be created is incorrect because a unique index will be created. When adding a PRIMARY KEY constraint, you must be granted the CREATE INDEX privilege because creating a PRIMARY KEY constraint creates a unique index on the column.

Item: 7 (Ref:1Z0-042.7.1.1)

The default permanent tablespace for your Oracle database is set to PROD. You have created a user JOHN in your database, and assigned the USERS tablespace to the user JOHN.

Which tablespace stores the tables that the user JOHN creates?

- PROD
- USERS
- SYSTEM
- UNDOTBS1

Answer:

USERS

Explanation:

The tables created by a user are stored in the tablespace that is assigned to the user at the time of creating the user. This assignment overrides the default permanent tablespace assigned to all the database users. In this scenario, JOHN is assigned the USERS tablespace. Therefore, the tables that the user JOHN creates are stored in the USERS tablespace and not in the PROD tablespace.

All the database users except SYS and SYSTEM are assigned the PROD tablespace as the default permanent tablespace. However, the tablespace assigned to a user at the time of creating the user overrides the default permanent tablespace. Therefore, the tables that the user JOHN creates are not stored in the PROD tablespace.

The SYSTEM tablespace is the default permanent tablespace for the SYS and the SYSTEM users. The objects created by the SYS and the SYSTEM users are stored in the SYSTEM tablespace.

The UNDOTBS1 tablespace stores undo records. These undo records are used to undo the changes made to the database by an uncommitted transaction.

Item: 8 (Ref:1Z0-042.7.7.1)

You are in the process of creating a table to hold records for the employees in your organization. Which data type would be best for the BIRTH_DATE column in your table?

- DATE
- NUMBER
- VARCHAR2
- TIMESTAMP WITH TIMEZONE
- TIMESTAMPWITH LOCAL TIMEZONE

Answer:

DATE

Explanation:

The best data type for the BIRTH_DATE column in your table would be the DATE data type because you only need to store the date in the BIRTH_DATE column. A DATE data type stores dates in fixed-length fields of seven bytes.

The NUMBER data type is used to store numeric values. This data type can also be used to store date values, but you cannot use the date functions on the values stored in a column with a NUMBER data type. Every time, you would need to use a TO_DATE function to convert the date stored in this column to a DATE data type.

The VARCHAR2 data type is used to store variable length character data. A column defined as VARCHAR2 can store numbers as well as dates, but the data stored will be interpreted as character data. You will not be able to use any numeric or date functions on the column values until you use a TO_NUMBER or TO_DATE function to convert them to a number or date value, respectively.

Using the TIMESTAMP WITH TIMEZONE data type will only increase the space used by the column because you do not need to store the time zone with the date. The TIMESTAMP WITH TIMEZONE data type stores a value fixed at 13 bytes. This value contains the date and time, and an associated time zone setting. This data type should be used when you want to store the time zone value in the column.

Using the TIMESTAMP WITH LOCAL TIMEZONE data type will only increase the space used by the column because you do not need to store the time zone with the date. The TIMESTAMP WITH LOCAL TIMEZONE data type stores values which vary from 7 to 11 bytes in size. The TIMESTAMP WITH LOCAL TIMEZONE data type is identical to the TIMESTAMP WITH TIMEZONE data type except that the data stored in the column with this data type is normalized to the database time zone.

Item: 9 (Ref:1Z0-042.7.6.2)

You run the following statement to create a table:

```
SQL> CREATE TABLE TAB$4-8 (NO NUMBER);
```

However, this statement fails to create the table.

What could be the reason for the failure of this statement to create the table?

- The column name is too short.
- You cannot use the - symbol in the table name.
- You cannot use the $ symbol in the table name.
- You can use only one numeric character in the table name.
- You cannot use the NUMBER data type without specifying a precision.
- You have not specified the name of the tablespace in which the table is to be stored.

Answer:

You cannot use the - symbol in the table name.

Explanation:

The given statement fails because you have used the - symbol in the table name. You cannot use this symbol in the table name. The valid characters that can be included in a table name are alphanumeric characters from your database character set, the underscore (_), the dollar sign ($), and the pound sign (#).

The option that states that the column name is too short is incorrect because you can name a column with a single letter.

The option that states that you cannot use the $ symbol in the table name is incorrect because you can use the $ symbol in a table name.

The option that states that you can use only one numeric character in the table name is incorrect because you can use more than one numeric character in the table name.

The option that states that you cannot use the NUMBER data type without specifying a precision is incorrect because you can create a column with a NUMBER data type without specifying the precision.

The option that states that you have not specified the name of the tablespace is incorrect because you can create a table without specifying the name of the tablespace in which the table is to be stored. In this scenario, the table will be stored in the user's permanent tablespace. If the user has not been assigned a default permanent tablespace, the object created by the user will be stored in the default permanent tablespace for the database. If no default permanent tablespace has been specified for the database, then the object will be stored in the SYSTEM tablespace.

Item: 10 (Ref:1Z0-042.7.5.1)

You have been assigned the task of tuning an application that is performing poorly. The application extensively uses a table named DETAIL from the PROD database. There are millions of rows in the DETAIL table, of which only a few rows are returned when the queries are run on the table. The WHERE clauses of the queries used in the application typically contain a condition on the ITEM_NO column that has sequential values.

Which action should you take to improve the performance of the application?

- Truncate and repopulate the table.
- Sort the output of the queries based on the ITEM_NO column.
- Reorganize the table by moving it to a different tablespace that contains more free extents.
- Create a B-tree index on the ITEM_NO column of the table, if a B-tree index does not already exist.
- Create a bitmap index on the ITEM_NO column of the table, if a bitmap index does not already exist.

Answer:

Create a B-tree index on the ITEM_NO column of the table, if a B-tree index does not already exist.

Explanation:

In this scenario, you should create a B-tree index on the ITEM_NO column. The ITEM_NO column is used in the WHERE clause of most queries, and the number of rows returned is less than the number of rows present in the table. Therefore, a B-tree index on the ITEM_NO column will improve the performance of the application. Also, the ITEM_NO column contains sequential values. Therefore, creating a B-tree index will be more useful. B-tree indexes can be created on columns that have high cardinality values and the columns are used frequently in the WHERE clause of a SELECT statement. B-tree indexes are useful when the query returns only a few rows from the table.

Repopulating the table after truncating it will not improve the performance of the queries that are performing badly due to missing indexes.

Sorting the output of the queries based on the ITEM_NO column will not improve performance. The only way to improve the performance of the query is to reduce the amount of time that the query takes to retrieve the desired rows.

Reorganizing the data in the table by moving the data to a different tablespace is incorrect because this step will not improve the performance of the queries that are performing badly due to missing indexes.

Creating a bitmap index will not help in this case because the ITEM_NO column contains varied values and the queries return a small portion of data. Bitmap indexes are created on columns that have a relatively low cardinality value. Bitmap indexes are also created on columns that are frequently used with conditional operators such as AND and OR. Bitmap indexes are useful when the query returns a higher number of rows from the table.

Item: 11 (Ref:1Z0-042.7.5.2)

In which scenario can you create a bitmap index to gain considerable improvement in the performance of reports accessing the tables?

- The EMP_MASTER table is 8 GB in size, and the table contains few rows.
- The TRANS_DETAIL table contains 8 million rows, and the key column TRANS_NO that is accessed by major queries has high cardinality.
- The SHIPPING table contains thousands of records, is accessed by an Online Transaction Processing (OLTP) system, and is updated frequently.
- The EMPLOYEES table contains 10 million rows, the key columns have low cardinality, and most of the SELECT queries are a combination of multiple WHERE conditions with the OR and AND operators.

Answer:

The EMPLOYEES table contains 10 million rows, the key columns have low cardinality, and most of the SELECT queries are a combination of multiple WHERE conditions with the OR and AND operators.

Explanation:

To gain considerable improvement in the performance of reports, you can create a bitmap index for the EMPLOYEES table that contains 10 million rows. The reason is that the key columns of the table have low cardinality. Also, most SELECT queries retrieve data from the columns by using multiple WHERE conditions with the OR and AND operators. Bitmap indexes are suitable for tables with millions of rows and low cardinality of data in the key columns. Bitmap indexes perform better than B-tree indexes when:

- Queries often use a combination of multiple WHERE conditions with the OR operator.
- The table is read-only.
- The key columns of the table are not frequently updated.

A bitmap index created on the EMP_MASTER table would not produce considerable performance improvement. This table is not an ideal candidate for bitmap index creation because the table contains few rows. A bitmap index can considerably improve performance if the table contains many rows. Therefore, in this scenario you would not create a bitmap index on the EMP_MASTER table.

A bitmap index would not produce considerable performance improvement on the TRANS_DETAIL table because the key column TRANS_NO in the table that is accessed by major queries has high cardinality values. Therefore, the TRANS_DETAIL table is not an ideal candidate for bitmap index creation. In the given scenario, you should create a B-tree index on the TRANS_NO column if one does not exist. The reason for this is that a B-tree index is more effective when the values in the column have high cardinality and major queries on the table access this column.

A bitmap index would not be best on the SHIPPING table because the table is frequently updated. Bitmap indexes should not be created on tables that have frequent updates because updates on indexed columns are expensive.

Item: 12 (Ref:1Z0-042.7.5.3)

You want to view the SQL statements used by all the users in the database to create views. Which dynamic view should you use to obtain this information?

- ALL_VIEWS
- DBA_VIEWS
- USER_VIEWS
- DBA_OBJECTS
- ALL_OBJECTS

Answer:

DBA_VIEWS

Explanation:

You should use the DBA_VIEWS view to display the SQL statements used by all the users in the database to create views. The DBA_VIEWS view will provide you with information, such as the owner of the view, the name of the view, the text of the view, the length of the text of the view, and other related information about the view. When a view is created, the SQL statement used to create the view is stored in the data dictionary. You can obtain all the information regarding a view from the data dictionary view by using the DBA_VIEWS view.

The ALL_VIEWS view cannot be used to display the SQL statements used by all the users in the database to create views. The ALL_VIEWS view will only provide information about the views that are accessible to the current user.

The USER_VIEWS view cannot be used to display the SQL statements used by all the users in the database to create views. The USER_VIEWS view will only provide information about the views that are owned by the current user.

The DBA_OBJECTS view cannot be used to display the SQL statements used by all the users in the database to create views. The DBA_OBJECTS view will provide information regarding all the objects in the database created by different users. The DBA_OBJECTS view will only provide the owner name, the object name, and the object ID of the objects. The DBA_OBJECTS view will not provide the SQL statement that was used to create the view.

The ALL_OBJECTS view cannot be used to display the SQL statements used by all the users in the database to create views. The ALL_OBJECTS view will provide information regarding all the objects accessible by the current user. The ALL_OBJECTS view has columns similar to the DBA_OBJECTS view.

Managing Data

Item: 1 (Ref:1Z0-042.8.1.2)

Click the Exhibit(s) button to view the structure of the EMP table.

The EMP table contains 50 rows. You execute the following set of statements in a session:

```
SQL> DELETE FROM EMP WHERE 1=2;

SQL> CREATE TABLE TEMP AS SELECT * FROM EMP WHERE 2=1;

SQL> COMMIT;
```

Which statements are true about the result of executing this set of statements? (Choose all that apply.)

- ☐ The newly created TEMP table will contain no rows.
- ☐ The newly created TEMP table will contain 50 rows.
- ☐ The newly created TEMP table will have a structure similar to the EMP table.
- ☐ The newly created TEMP table will contain double the rows as in the EMP table.
- ☐ The structure of the newly created TEMP table will contain only the first two columns from the EMP table.

Answer:

The newly created TEMP table will contain no rows.

The newly created TEMP table will have a structure similar to the EMP table.

```
@> DESC EMP
 Name                                                                                  Null?    Typ
 ------------------------------------------------------------------------------------ -------- ---
 EMPLOYEE_ID                                                                                    NUM
 FIRST_NAME                                                                                     VAR
 LAST_NAME                                                                             NOT NULL VAR
 EMAIL                                                                                 NOT NULL VAR
 PHONE_NUMBER                                                                                   VAR
 HIRE_DATE                                                                             NOT NULL DAT
 JOB_ID                                                                                NOT NULL VAR
 SALARY                                                                                         NUM
 COMMISSION_PCT                                                                                 NUM
 MANAGER_ID                                                                                     NUM
 DEPARTMENT_ID                                                                                  NUM

@>
```

Explanation:

In this scenario, the newly created TEMP table will contain no rows and will have a structure similar to the EMP table. First, you issue a DELETE statement. The condition specified in the WHERE clause of the DELETE statement always evaluates to FALSE, and no rows are deleted from the EMP table. Next, you execute the CREATE TABLE statement. The WHERE clause in this statement also always evaluates to FALSE. Therefore, only the structure of the EMP table is copied, and the TEMP table will contain no rows.

The option that states that the newly created TEMP table will contain 50 rows is incorrect because the TEMP table will contain no rows because the WHERE clause in the subquery of the CREATE TABLE statement always evaluates to FALSE.

The option that states that the newly created TEMP table will contain double the rows as in the EMP table is incorrect because the SELECT * FROM EMP 2=1 clause specified in the CREATE TABLE statement includes a WHERE clause that always evaluates to FALSE, and only the structure of the EMP table will be created. If the SELECT clause in the CREATE TABLE AS statement included a WHERE clause that always evaluated to TRUE, the newly created table would contain the same number of rows as in the EMP table.

The option that states that the structure of the TEMP table will only contain the first two columns from the EMP table is incorrect because the structure of the newly created TEMP table will be similar to the EMP table. While using the CREATE TABLE AS

statement, the table created will have the number of rows specified in the SELECT clause of the CREATE TABLE AS statement. In the given scenario, you are using the SELECT * FROM EMP statement, which means that all the columns from the EMP table will be contained in the newly created TEMP table.

Item: 2 (Ref:1Z0-042.8.5.2)

You issue the following statement to grant a privilege to the database user JOHN:

```
SQL> GRANT CREATE ANY DIRECTORY TO JOHN;
```

Which statement is true regarding the privilege granted to JOHN?

- JOHN can create files anywhere in the OS.
- JOHN can create directories anywhere in the OS.
- JOHN can read files located on all the directories in the OS.
- JOHN can grant this privilege to any other user in the database.
- JOHN can read and write to the files located on the OS only if JOHN has the read and write permissions on the OS directories in which the files are located.
- JOHN can read and write to the files located on the OS only if the Oracle database processes have read and write permissions on the OS directories in which the files are located.

Answer:

JOHN can read and write to the files located on the OS only if the Oracle database processes have read and write permissions on the OS directories in which the files are located.

Explanation:

With the given GRANT statement, JOHN can read and write to the files located on the OS only if the Oracle database processes have read and write permissions on the OS directories where the files are located. When any user is granted the CREATE ANY DIRECTORY privilege, the user can read the files located on the OS only if the database processes have read and write permissions on the OS directories referred to by the directory objects created by the user. If the Oracle database processes do not have the required privileges on the OS directories, the user will not be able to read from or write to the directories even after creating a directory object pointing to the OS directory.

The option stating that JOHN can create files anywhere in the OS is incorrect because JOHN cannot create files on the OS until the Oracle database processes have the read and write privileges on the OS directories. Any attempt by the user to create or read a file will fail if the Oracle database processes do not have the read and write privileges on the OS directory.

The option stating that JOHN can create directories anywhere in the OS is incorrect because JOHN cannot create directories on the OS if he has the CREATE ANY DIRECTORY privilege. To create a directory on the OS, he must have the privileges from the OS. The CREATE ANY DIRECTORY privilege only gives rights to create a directory object pointing to an OS directory location.

The option stating that JOHN can read files located on all the directories in the OS is incorrect because JOHN cannot read files located on the OS until the Oracle database processes have the read privileges on the OS directories.

The option stating that JOHN can grant this privilege to any other user in the database is incorrect because the privilege has not been granted to JOHN using the WITH ADMIN OPTION clause. JOHN can grant this privilege to other users in the database only if the privilege has been granted to him using the WITH ADMIN OPTION clause.

The option stating that JOHN can read and write to the files located on the OS only if he has the read and write permissions on the OS directories where the files are located is incorrect because JOHN cannot read or write to the OS even if he has the read and write permissions on the OS directories. For JOHN to be able to read or write to these directories, the Oracle database processes must have the read and write privileges on the OS directories.

Item: 3 (Ref:1Z0-042.8.1.3)

The user A attempts to insert data into the user JOHN's EMP table by issuing the following statement:

```
SQL> INSERT INTO JOHN.EMP VALUES (4563,'ADAM', 5000, 'ACCOUNTS', 125);
```

This statement returns the following error:

ORA-01653: unable to allocate extent table JOHN.EMP by 8 in tablespace EXAMPLE

What should you do to resolve this problem and ensure that user A can insert data into the EMP table?

- Add more space to user A's default tablespace.
- Grant the INSERT ANY TABLE privilege to the user.
- Add more space to the user JOHN's default tablespace.
- Allocate additional quota to user A on user A's default tablespace.
- Add more space to the tablespace in which the EMP table resides.
- Allocate quota to user A on the tablespace in which the EMP table resides.

Answer:

Add more space to the tablespace in which the EMP table resides.

Explanation:

You should add more space to the tablespace in which the EMP table resides. The error occurs because Oracle is unable to allocate an extent to the EMP table. The EXAMPLE tablespace, in which the EMP table resides, does not contain enough space. To solve the problem, you must allocate more space to the EXAMPLE tablespace to ensure that extents can be allocated and data inserted into the table. Additional space can be allocated to the tablespace by adding more datafiles, manually allocating extents, or by enabling the autoextensible feature for the datafiles that exist in the tablespace.

The option to add more space to user A's default tablespace is incorrect because the error is due to lack of enough space in the tablespace in which the EMP table resides. Allocating more space to the user's default tablespace will not solve the problem.

The option to grant the INSERT ANY TABLE privilege to the user is incorrect because the user already has the INSERT privilege on the EMP table owned by JOHN. If user A does not have the required privileges, a different error will be generated. The error generated in this scenario is due to space problems.

The option to add more space to the user JOHN's default tablespace is incorrect because it is not mentioned that the EMP table resides in the user JOHN's default tablespace. Therefore, allocating more space to the user JOHN's default tablespace might not solve the problem. It would solve the problem only if the EMP table resides in JOHN's default tablespace.

The option to allocate additional quota to user A on user A's default tablespace is incorrect because the error is due to the lack of enough space in the tablespace in which the EMP table resides. Allocating additional quota to user A on his default tablespace will not solve the problem.

The option to allocate quota to user A on the tablespace in which the EMP table resides is incorrect because the error is due to the lack of enough space in the tablespace in which the EMP table resides. Allocating more space to user A will not solve the problem. The problem can be solved by adding more space to the tablespace in which the EMP table resides, EXAMPLE.

Item: 4 (Ref:1Z0-042.8.1.1)

Click the Exhibit(s) button to view the details of the ITEMS and ORDERS tables where the ITEMS table is the parent table and ORDERS table is the child table. The PROD_ID column is the primary key column in the ITEMS table and a foreign key column in the ORDERS table.

User A is trying to update the ORDERS table to update the status of ORDER_ID 249 using the following SQL statement:

```
SQL> UPDATE ORDERS SET PROD_ID=8 WHERE ORDER_ID=249;
```

However, upon execution, the statement returns the following error:

ORA-02291: integrity constraint (ORDERS.FK_ID) violated - parent key not found

Which of these identifies the correct solution to avoid this error?

- Drop the primary key from the ITEMS table.
- Truncate the ITEMS table and then update the ORDERS table.
- Drop the ITEMS table using the CASCADE CONSTRAINTS clause.
- Insert the product details with PROD_ID number 8 into the ITEMS table, and then update the ORDERS table.

Answer:

Insert the product details with PROD_ID number 8 into the ITEMS table, and then update the ORDERS table.

ITEMS

PROD_ID	PRODUCT_NAME	PRICE	MANUFACTURER
1	MODEM	2000	TELSTAR
2	CPU	25000	TRITECH
3	CABLE	500	UNITED SALES
4	MONITOR	15000	VERIGON
5	KEYBOARD	1000	GEOTREK
6	PINS	2000	METROIL

ORDERS

ORDER_ID	PROD_ID	AMOUNT	CUST_NAME
200	2	50000	ANTHONY
215	3	4000	SAMUEL
256	5	5000	AMY
265	5	1000	JOHN
276	4	45000	ERIC
212	1	6000	KATE
245	6	10000	TIMOTHY
249	5	2000	SCOTT

Explanation:

To rectify the error generated when updating records in the ORDERS table, you need to take care that the integrity constraints are not violated. Here, the foreign key on the PROD_ID column is violated because the specific PROD_ID you are trying to update does not exist in the ITEMS table. To overcome this, you should first insert a row in the ITEMS table with the PROD_ID value of 8 and then run the UPDATE statement on the ORDERS table again. When updating data in the child table, care must be taken that the updated values are not violating any values in the parent table and also that the corresponding values are present in the parent table. Similarly, while deleting data from the parent table you must ensure that no dependent values are present in the child table. Otherwise, you will receive an error stating there are dependent records in the child table. To avoid the error, you must either delete the child records first and then delete the records from the parent table or specify the DELETE CASCADE option in the FOREIGN KEY constraint. The DELETE CASCADE option in the FOREIGN KEY constraint specifies that when a row from the parent table is deleted, all the dependent rows from the child table are also deleted.

Dropping the primary key from the ITEMS table would disable the integrity constraints that you have specified on the two tables.

This will not accomplish the objective of using integrity constraints on the two tables.

Truncating the `ITEMS` table will not accomplish the objective in this scenario because you only want to update one row in the `ORDERS` table. Truncating the `ITEMS` table will delete all the data from it.

Dropping the `ITEMS` table will not accomplish the objective in this scenario because you only want to update one row in the `ORDERS` table. Dropping the `ITEMS` table will delete all the data from it.

Item: 5 (Ref:1Z0-042.8.3.4)

Due to changes in the responsibilities of the users, you want to transfer the tables owned by one user to another user's schema.

Which tool should you use to effectively achieve this objective with the least administrative effort?

- direct path load to load the data from one schema to another schema
- transportable tablespaces to transfer the tablespace that contains the data
- the command-line mode of Data Pump Import to import the data into the other user's schema
- the Oracle Enterprise Manager 10*g* Database Control **Re-map Schemas** page to import the data into the other user's schema

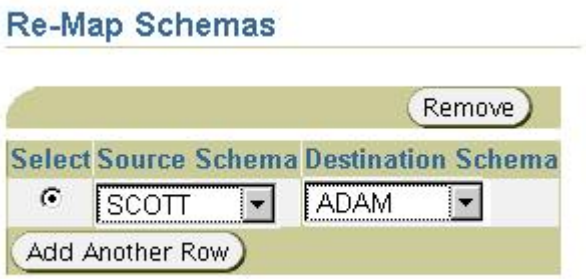
Answer:

the Oracle Enterprise Manager 10*g* Database Control Re-map Schemas page to import the data into the other user's schema

---

Explanation:

You should use the Oracle Enterprise Manager 10*g* Database Control **Re-map Schemas** page to import the data into the other user's schema because this method requires the least administrative effort. To import data by using Oracle Enterprise Manager 10*g* Database Control, you can select the source and destination schemas for transferring the data from the **Re-Map Schemas** page, as shown in this graphic:



The data objects from the source schemas will be imported to the destination schema.

You cannot use the direct path load to load the data from one schema to another schema in this scenario. Direct path load is used when you are employing SQL*Loader to import data from flat files. In this scenario, you have to transfer data from one schema to another; therefore, you cannot use the direct path load.

You cannot use transportable tablespaces to transfer the tablespace that contains the data in this scenario. The transportable tablespaces feature is not used to transfer data within the database. The transportable tablespace feature can be used to transfer data contained in a tablespace from one database to another database. The tablespace cannot be used to transfer data from one schema to another schema in the same database.

You should not use the command-line mode of the Data Pump Import to import the data into the other user's schema because this method will require more administrative effort than using Oracle Enterprise Manager 10*g* Database Control. Using the command-line mode of the Data Pump Import will require you to type the complete command to perform the import. Oracle Enterprise Manager 10*g* Database Control only requires you to select the source and destination schemas. Therefore, the command-line mode of the Data Pump Import is not the best option in this scenario.

Item: 6 (Ref:1Z0-042.8.2.1)

You are performing an export of certain objects in your database by using Oracle Data Pump. You are required to unload only the data in the export file and not the metadata information.

Which parameter of the Data Pump Export should you use in this scenario?

- TABLES
- CONTENT
- EXCLUDE
- ESTIMATE
- DIRECTORY

Answer:

CONTENT

Explanation:

You should use the CONTENT parameter of the Data Pump Export. The CONTENT parameter enables you to filter the data, the metadata, or both the data and metadata. The CONTENT parameter has three values, ALL, DATA_ONLY, and METADATA_ONLY. These values specify whether both data and metadata will be exported, only the data will be exported, or only the metadata will be exported.

The TABLES parameter of the Data Pump Export does not allow you to filter the data or metadata that you want to export. The TABLES parameter specifies that you perform a table mode export.

The EXCLUDE parameter of the Data Pump Export does not allow you to filter the data based on the data or metadata that will be exported. The EXCLUDE parameter enables you to exclude specific objects and object types from the metadata that will be exported.

The ESTIMATE parameter of the Data Pump Export determines the mode that export will use to estimate how much space each table in the export job will consume. The estimate done in this process is for the table row data only, not the metadata. This parameter of Data Pump Export is not used to filter the type of data to be exported.

The DIRECTORY parameter of the Data Pump Export specifies the location to which the export writes the dump file set and the log file.

Item: 7 (Ref:1Z0-042.8.3.2)

While performing an import by using the Data Pump Import utility, you use the following command in the import procedure:

```
> impdp HR/hr TABLES=employees DIRECTORY=data1 SCHEMAS=scott
NETWORK_LINK=telstar.uk.oracle.com FLASHBACK_SCN=235
```

Which three statements correctly characterize this command? (Choose three.)

- The EMPLOYEES table will be imported into the HR schema.
- The EMPLOYEES table will be imported into the SCOTT schema.
- The SCN number refers to the SCN number of the target database.
- The SCN number refers to the SCN number of the source database.
- The data is transferred to the target database referred to by the telstar.uk.oracle.com link.
- The data is transferred from the source database referred to by the telstar.uk.oracle.com link.

Answer:

The EMPLOYEES table will be imported into the HR schema.

The SCN number refers to the SCN number of the source database.

The data is transferred from the source database referred to by the telstar.uk.oracle.com link.

Explanation:

With the given command, the EMPLOYEES table will be imported into the HR schema, the SCN number refers to the SCN number of the source database, and the data is transferred from the source database referred to by the telstar.uk.oracle.com link. In this command, the NETWORK_LINK parameter points to the source database referred to by the telstar.uk.oracle.com link. The link specifies that the data must be transferred from the source database. While performing an import from a remote location, you must use the NETWORK_LINK parameter to specify the name of the remote server from which the data is retrieved. You should not use the DUMPFILE parameter when you specify the NETWORK_LINK parameter. The SCN number specified in the command refers to the SCN number of the source database. The table EMPLOYEES will be imported into the HR schema.

The EMPLOYEES table will not be imported to the SCOTT schema. Instead, the EMPLOYEES table will be imported to the HR schema. The SCHEMAS=scott parameter indicates that the SCOTT schema is to be imported.

The SCN number does not refer to the SCN number of the target database. Instead, the SCN number refers to the SCN number of the source database.

The data is not transferred to the target database referred to by the telstar.uk.oracle.com link. The telstar.uk.oracle.com link refers to the source database from which the data is retrieved.

Item: 8 (Ref:1Z0-042.8.3.3)

You are importing data into your database by using Data Pump Import. While importing data from the dump file, dump01.dmp, you want only the views in the ADAM schema to be imported into the database. You also want only those views whose names contain the SALES string to be imported.

Which import command will successfully achieve this objective?

- $ impdp john/john
  SCHEMAS=adam
  INCLUDE=view:"like '%SALES%'"
- $ impdp john/john
  DUMPFILE=dump01.dmp
  SCHEMAS=adam
  INCLUDE=view:"like '%SALES%'"
- $ impdp john/john
  DUMPFILE=dump01.dmp
  INCLUDE=view:"like '%SALES%'"

  CONTENT=VIEW_ONLY
- $ impdp john/john
  DUMPFILE=dump01.dmp
  SCHEMAS=adam
  EXCLUDE=view:"like '%SALES%'"
- $ impdp john/john
  DUMPFILE=dump01.dmp
  SCHEMAS=adam
  EXCLUDE=view:"like '%SALES%'"

  CONTENT=VIEW_ONLY

Answer:

$ impdp john/john
DUMPFILE=dump01.dmp
SCHEMAS=adam
INCLUDE=view:"like '%SALES%'"

Explanation:

The following import command is correct:

```
$ impdp john/john
DUMPFILE=dump01.dmp
SCHEMAS=adam
INCLUDE=view:"like '%SALES%'"
```

This import command will import only views containing the SALES string in the view name from the ADAM schema. The DUMPFILE parameter in the import command specifies the name of the dump file from which the data is to be imported into the database. The SCHEMAS parameter in the import command specifies that only the data in the ADAM schema is to be imported. The INCLUDE parameter in the import command specifies the objects or object types to be imported. In this command, the INCLUDE parameter specifies that only views containing the SALES string in their names are to be imported.

The command that does not specify the DUMPFILE parameter is incorrect. The DUMPFILE parameter must be specified in the import command. This parameter specifies which dump file will be used while performing the import. If no dump file is specified, the default value of expdat.dmp will be used. However, in this case you need the data in the dump01.dmp file to be imported.

The command that does not specify the SCHEMAS parameter and specifies a CONTENT parameter value of VIEW_ONLY is incorrect. The SCHEMAS parameter is needed to import data only from ADAM's schema. The CONTENT parameter used in this command will generate an error because the three valid values for the CONTENT parameter are ALL, DATA_ONLY, and METADATA_ONLY. The CONTENT parameter enables you to filter the data to be loaded by specifying the data, the metadata, or both to be loaded by the import process.

The command that uses the EXCLUDE parameter and does not specify a CONTENT parameter is incorrect. The EXCLUDE

parameter is the opposite of the INCLUDE parameter. This command will exclude the views that contain the SALES string in their names. Therefore, this command will not achieve the desired objective.

The command that uses the EXCLUDE parameter and specifies a CONTENT parameter value of VIEW_ONLY is incorrect. The EXCLUDE parameter is the opposite of the INCLUDE parameter. This command will exclude the views that contain the SALES string in their names. The CONTENT parameter enables you to filter the data to be loaded by specifying the data, the metadata, or both to be loaded by the import process. The CONTENT parameter used in this command will generate an error because the three valid values for the CONTENT parameter are ALL, DATA_ONLY and METADATA_ONLY.

Item: 9 (Ref:1Z0-042.8.1.4)

You have created a deferred `NOT NULL` constraint on a column in a table. You are updating the data in the table. Several rows being updated do not conform to the constraint.

What will happen when you commit the transaction?

- All the rows will be updated.
- No rows will be updated.
- Only the rows that conform to the constraint will be updated.
- All the rows will be updated and the constraint state will change to disabled.

Answer:

No rows will be updated.

Explanation:

The option stating that no rows will be updated is correct. When a constraint is violated by rows in the table, no rows are updated. In this scenario, the constraint is a deferred constraint. Therefore, the `NOT NULL` constraint will be checked at the end of the transaction. Because rows in the table violate the constraint, the transaction will be terminated with an error and no rows in the table will be updated. When the constraint is an immediate constraint, it is checked when you execute a SQL statement to modify the data. In such a scenario, an error indicating the constraint has been violated will be returned as soon as you execute the SQL statement and no rows will be updated.

The option stating that all the rows will be updated is incorrect because no rows will be updated.

The option stating that only the rows that conform to the constraint will be updated is incorrect because no rows will be updated. The only way to update these rows would be to disable the constraint and reissue the update.

The option stating that all the rows will be updated and the constraint state will change to disabled is incorrect because no rows will be updated. A constraint state does not change on its own but is changed when the user issues a statement to change the state of the constraint.

Item: 10 (Ref:1Z0-042.8.2.2)

A user in the database of your company has inadvertently modified some critical data in the MASTER table, and you do not know the exact time at which the data was modified. You must recover the table to undo the modifications made to the table.

Which action should you take to recover the table?

- Use the LogMiner utility to recover the table.
- Use the time-based recovery procedure to recover the table.
- Use the change-based recovery procedure to recover the table.
- Recover the table by importing the table from the previous export dump of the table.
- Use the FLASHBACK_SCN option of the Oracle Data Pump Export to perform a flashback export of the table followed by an import of the table.
- Use the FLASHBACK_TIME option of the Oracle Data Pump Export to perform a flashback export of the schema followed by an import of the schema.

Answer:

Use the FLASHBACK_SCN option of the Oracle Data Pump Export to perform a flashback export of the table followed by an import of the table.

Explanation:

You should use the FLASHBACK_SCN option of the Oracle Data Pump Export to perform a flashback export of the table followed by an import of the table. In the given scenario, you must recover the table to a prior point in time at which the data in the table was not modified. This can be done in several ways. However, the best option is to use the Data Pump Export with the FLASHBACK_SCN option, which will enable flashback export for the table. This process will export the table as it existed at the specified SCN. The table can then be imported from the export dump created by the export process. This is the best option because this does not involve shutting down the database and affecting the other users connected to the database. Flashback Table and Flashback Query can also be used in a similar scenario to recover the table to a prior point in time.

You should not use the LogMiner utility to recover the table because LogMiner cannot be used to recover the table. The LogMiner utility is used to query the redo log files to check for the activities performed on the database. The LogMiner utility gives you the SQL queries that were used to perform alterations in the database.

You should not use the time-based recovery procedure to recover the table. This is not the best option in this scenario because you should know the exact time at which the data in the table was modified. In the given scenario, you are not aware of the exact time at which the table was modified. Also, a time-based recovery will not be suitable in this scenario because you need to shut down the database to perform a time-based recovery and this will affect the user connections.

You should not use the change-based recovery procedure to recover the table because the change-based recovery procedure will involve shutting down the database and affecting the other user connections. The best option in the given scenario would be the one that does not affect the other user connections.

You should not recover the table by importing the table from the previous export dumps of the table. You may not have performed an export on the table before the table was modified.

You should not use the FLASHBACK_TIME option of the Oracle Data Pump Export to perform a flashback export of the schema followed by an import of the schema. To use the FLASHBACK_TIME option of Oracle Data Pump, you must know the exact time at which the table was modified. Also, you do not need to perform a schema level export. The reason for this is only the table is modified, and you can recover the table even by performing a table-level export followed by an import.

Item: 11 (Ref:1Z0-042.8.3.1)

Due to changes in the policies of your organization, you are required to restructure your database. You issue the following command from the Oracle Data Pump Import:

```
> impdp SYSTEM/password DIRECTORY=expdat_dmp DUMPFILE=expdat.dmp NOLOGFILE=Y
REMAP_SCHEMA=hr:scott
```

Which two statements are true about the result of issuing this command? (Choose two.)

- The HR schema will be renamed as the SCOTT schema.
- All objects in the SCOTT schema will be transferred to the HR schema.
- All objects in the HR schema will be transferred to the SCOTT schema.
- No errors and import progress messages will be generated during the import process.
- Errors and the import progress messages generated during the import will be stored in the log file.
- Errors and import progress messages will be written to the standard output device.
- The objects in the SCOTT schema will be transferred to the HR schema, and the SCOTT schema will be dropped.
- The objects in the HR schema will be transferred to the SCOTT schema, and the HR schema will be dropped.

Answer:

All objects in the HR schema will be transferred to the SCOTT schema.
Errors and import progress messages will be written to the standard output device.

Explanation:

With the given command, all objects in the HR schema will be transferred to the SCOTT schema, and the errors and import progress messages will be written to the standard output device. If you use the REMAP_SCHEMA parameter, the import procedure will transfer all the objects from the HR schema to the SCOTT schema. This feature is typically useful for transferring database objects owned by one user to another user in a different database. After the import procedure is completed, the two schemas will remain unchanged. Neither of the two schemas will be dropped. The use of the NOLOGFILE=Y parameter specifies that the error and import progress messages are not written to the log files. In this scenario, the errors and import progress messages will be written to standard output devices such as monitors and printers.

The HR schema will not be renamed as the SCOTT schema. Only the objects in the HR schema will be transferred to the SCOTT schema.

All the objects from the SCOTT schema will not be transferred to the HR schema. Instead, the objects will be transferred from the HR schema to the SCOTT schema.

Errors and import messages will be generated and will be written to the standard output device because the NOLOGFILE=Y parameter is included.

Errors and import progress messages generated during the import will not be stored in the log file because NOLOGFILE=Y indicates that no log file will be created.

The objects in the SCOTT schema will not be transferred to the HR schema and the SCOTT schema dropped because the objects from the SCOTT schema will not be transferred to the HR schema. Instead, the objects from the HR schema will be transferred to the SCOTT schema.

The objects from the HR schema will be transferred to the SCOTT schema, but the HR schema will not be dropped after the objects are transferred from the HR schema to SCOTT schema.

Item: 12 (Ref:1Z0-042.8.4.1)

You are a DBA in your company. Due to a revision in company policies, you must transfer all the data in the FIN_TBS tablespace of your database to the database located at your company head office.

Which tool or feature would be the best to use in the given scenario?

- Data Pump
- SQL*Loader
- conventional path load
- transportable tablespace

Answer:

transportable tablespace

Explanation:

It would be best to use a transportable tablespace. A transportable tablespace can be used in this scenario because an entire tablespace can be moved from one database to another by using this feature. Using this feature does not involve a lot of administrative effort and does not affect the performance of the database. The only task you must perform is to copy the metadata of the tablespace and then transfer this metadata and datafiles in the tablespace from one location to another.

Data Pump should not be used in this scenario because this feature is not faster in transferring tablespaces than using a transportable tablespace. Data Pump is used to enable speedy transfer of data in one database to another. Data Pump should be used when you want to transfer a table or a schema and the corresponding data from one database to another.

SQL*Loader cannot be used in this scenario because you cannot use SQL*Loader to transport a tablespace from one database to another. SQL*Loader is used to extract data from flat files and load the data into tables of an Oracle database.

Conventional path load cannot be used in this scenario because conventional path export cannot be used to transport a tablespace from one database to another. Conventional path load uses SQL SELECT statements to load data. In this scenario, you want to transfer a tablespace data from one database to another. Therefore, you cannot use a conventional path load.

PL/SQL

Item: 1 (Ref:1Z0-042.9.3.2)

In your database, you want compilation of your PL/SQL code to only generate messages for conditions that can cause performance problems or generate an unexpected behavior or incorrect results.

Which initialization parameter value setting can you use to achieve this objective?

- `PLSQL_WARNINGS='ENABLE:ALL'`
- `PLSQL_WARNINGS='ENABLE:SEVERE'`
- `PLSQL_WARNINGS='ENABLE:PERFORMANCE'`
- `PLSQL_WARNINGS='ENABLE:PERFORMANCE', 'ENABLE:SEVERE'`

Answer:

`PLSQL_WARNINGS='ENABLE:PERFORMANCE', 'ENABLE:SEVERE'`

Explanation:

PL/SQL warning messages are divided into three categories, `SEVERE`, `PERFORMANCE`, and `INFORMATIONAL`. Using the `SEVERE` option, you receive messages for conditions that might cause unexpected behavior or incorrect results. Using the `PERFORMANCE` option, you receive messages for errors that might be causing a performance problem. Using the `INFORMATIONAL` option, you only receive messages for conditions that do not affect performance or correctness, but only help make the code more maintainable.

The `ALL` option is incorrect because this category will show all the messages.

The `SEVERE` option is incorrect because this category will only show the messages for conditions that might cause unexpected behavior or incorrect results.

The `PERFORMANCE` option is incorrect because with this setting you will only receive messages for errors that might be causing a performance problem.

Item: 2 (Ref:1Z0-042.9.2.2)

You have created a database trigger using the following statement:

```
CREATE OR REPLACE TRIGGER resume_timeout
AFTER SUSPEND ON DATABASE BEGIN
DBMS_RESUMABLE.SET_TIMEOUT(10800);
END;
```

When will this database trigger fire?

- when a user abruptly disconnects from the session
- when a user's session disconnects due to space allocation problems
- when a user's session is suspended due to space allocation problems
- when a user's statement is suspended and resumable space allocation is not enabled in the user's session
- when a user's statement is suspended due to space allocation problems and resumable space allocation is enabled for the user's session

Answer:

when a user's statement is suspended due to space allocation problems and resumable space allocation is enabled for the user's session

---

Explanation:

The trigger in this scenario is fired when a user's statement is suspended due to space allocation problems when resumable space allocation is enabled in the user's session. The given trigger changes the default system timeout to 10800 seconds, or three hours, when the AFTER SUSPEND event occurs. When resumable space allocation is enabled in a session, certain operations or SQL statements that encounter space-related problems, such as the space quota being reached, a problem in extending the tablespace, or the maximum extents reached condition occurring, can be resumed after the problems have been corrected. These operations will only suspend and not terminate until the error has been corrected. A triggering event can be used in this scenario that specifies the action to be performed when the operation suspends and resumable space allocation is enabled. The AFTER SUSPEND event can be used in situations such as these so that the event is triggered whenever a resumable operation encounters a correctable error, namely space-related problems.

The trigger is not fired when a user abruptly disconnects from the session. If a user abruptly disconnects from the session the PMON background process will perform a cleanup of the user process and roll back any uncommitted changes. No trigger will be fired in this scenario.

The trigger is not fired when a user's session disconnects due to space allocation problems. The trigger will only be fired if a user's session is suspended due to space allocation problems. If a user gets disconnected due to space allocation problems, the trigger will not be fired.

The trigger is not fired when a user's session is suspended due to space allocation problems. The trigger will only be fired if resumable space allocation is enabled in the user's session. Resumable space allocation can be enabled in the user's session using the following statement:

```
ALTER SESSION ENABLE RESUMABLE;
```

The trigger is not fired when a user's statement is suspended and resumable space allocation is not enabled in the user's session. The trigger will be fired only when resumable space allocation is enabled in the user's session.

Item: 3 (Ref:1Z0-042.9.2.1)

A user JOHN is the owner of the MASTER table, which has a PRIMARY KEY constraint defined on the CODE column. The MASTER table is used to store the data related to the products manufactured by the company. JOHN wants the values in the CODE column of the MASTER table to range from 1 to 200 because the company does not manufacture more than 200 items.

Which action can JOHN take to accomplish this objective?

- Create a trigger.
- Create a package.
- Create a function.
- Create an anonymous PL/SQL block.
- Modify the PRIMARY KEY constraint of the CODE column.

Answer:

Create a trigger.

Explanation:

To accomplish this objective, JOHN can create a trigger. A trigger is a PL/SQL construct, similar to a stored procedure, which automatically executes in response to a specific event. Triggers are generally used to enforce business rules, implement integrity checks, or track changes that occur. In this scenario, JOHN can create a trigger to enforce the condition that the value of CODE column must range from 1 to 200.

A package cannot be used to accomplish this objective because a package cannot be used to enforce a condition, such as restricting the values in the CODE column. A package is a PL/SQL construct that is used to group related PL/SQL objects.

A function cannot be used to accomplish this objective because a function cannot be used to enforce a condition, such as restricting the values in the CODE column. A function is a PL/SQL subprogram that can accept parameters, perform a calculation, and return a single value.

An anonymous PL/SQL block cannot be used to accomplish this objective because an anonymous PL/SQL block cannot be stored in the database, and therefore cannot be invoked when required. An anonymous PL/SQL block can be run in an interactive tool such as SQL*Plus or can be embedded in an OCI program. At run time, these blocks are sent to the compiler to be compiled and executed.

Modifying the PRIMARY KEY constraint of the CODE column cannot be used to accomplish this objective because the primary key cannot be used to restrict the values in the CODE column. A primary key is used to enforce uniqueness for values in a column and ensure that no column values contain a NULL value. Whenever a primary key on a table is created, a unique index will be created along with a NOT NULL constraint on the column.

Item: 4 (Ref:1Z0-042.9.1.1)

You want to create a PL/SQL construct that will accept the monthly salary and employee number of an employee, calculate the tax the employee will need to pay for the current period, and return this value so that it can be stored in a database. You also want to be able to call this construct from within SQL statements.

Which PL/SQL construct would you use for this purpose?

- trigger
- function
- procedure
- anonymous PL/SQL block

Answer:

function

Explanation:

The PL/SQL construct that you will need in the given scenario is a function. A function is a PL/SQL subprogram that can accept an argument, compute a value, and then return a value to the calling program. A function can be stored in the database and can be used from within SQL statements. In this scenario, you must use a function that will accept the salary and employee number of an employee and return the computed tax for the employee so the tax value can be stored in the database.

You would not use a trigger in this scenario. A trigger is a PL/SQL construct, similar to a stored procedure, which executes automatically in response to a specific event. Triggers are generally used to enforce business rules, implement integrity checks, or track changes that occur. For example, you can create a trigger that will be invoked when you perform a specific action on a table, such as deleting a row from a table, inserting a row into a table, or updating a table.

You would not use a procedure in this scenario because procedures cannot be called from within SQL statements. A procedure is a PL/SQL construct, which is stored in the database and is called by applications. A procedure can be used to store a frequently used code and when the procedure is executed, the statements within the procedure are executed. A procedure can accept input parameters and can return values using out parameters.

You would not use an anonymous PL/SQL block in this scenario because an anonymous PL/SQL block cannot be stored in the database and it cannot be called from within SQL statements.

Item: 5 (Ref:1Z0-042.9.3.1)

Your senior database administrator has instructed you to change the PL/SQL configuration options for your database such that the compiled PL/SQL code in your database is stored as native machine code.

Which statement will achieve the desired objective?

- `ALTER SYSTEM SET PLSQL_CODE_TYPE='NATIVE';`
- `ALTER SYSTEM SET PLSQL_CODE_NATIVE='TRUE';`
- `ALTER SESSION SET PLSQL_CODE_NATIVE='ENABLE';`
- `ALTER SYSTEM SET PLSQL_CODE_TYPE='INTERPRETED';`

Answer:

`ALTER SYSTEM SET PLSQL_CODE_TYPE='NATIVE';`

Explanation:

To store the compiled PL/SQL code as native machine code, you need to set the `PLSQL_CODE_TYPE` initialization parameter to a value of `NATIVE`. You can use the following statement to do this:

```
ALTER SYSTEM SET PLSQL_CODE_TYPE='NATIVE';
```

The `PLSQL_CODE_TYPE` initialization parameter is used to specify the compilation mode for PL/SQL code. The parameter has two values, `NATIVE` and `INTERPRETED`. Setting the parameter to `NATIVE` specifies that the compiled PL/SQL code is to be stored as native machine code. Setting the parameter to `INTERPRETED` specifies that the compiled PL/SQL code is to be stored as interpreted bytecode. The value of the `PLSQL_CODE_TYPE` initialization parameter defaults to `INTERPRETED`.

The `ALTER SYSTEM SET PLSQL_CODE_NATIVE='TRUE';` statement is incorrect because the parameter `PLSQL_CODE_NATIVE` is invalid. The correct initialization parameter to be set is `PLSQL_CODE_TYPE`.

The `ALTER SYSTEM SET PLSQL_CODE_NATIVE='ENABLE';` statement is incorrect because the parameter `PLSQL_CODE_NATIVE` is invalid. The correct initialization parameter to be set is `PLSQL_CODE_TYPE`.

Setting the value of the `PLSQL_CODE_TYPE` parameter to `INTERPRETED` will store the compiled PL/SQL code as interpreted bytecode. This code is then executed by the PL/SQL interpreter engine.

Item: 6 (Ref:1Z0-042.9.3.3)

You were recently hired as a database administrator for your company. In your testing environment, you notice this parameter setting in your initialization parameter file:

```
PLSQL_DEBUG=TRUE
```

Which two statements are true about this parameter setting? (Choose two.)

- ☐ It will disable the extended PL/SQL debugging features in your database.
- ☐ It will enable the extended PL/SQL debugging features in your database.
- ☐ It will cause compiled PL/SQL code to be stored as interpreted bytecode regardless of the of PLSQL_CODE_TYPE setting.
- ☐ It will cause compiled PL/SQL code to be stored as native machine code regardless of the PLSQL_CODE_TYPE setting.
- ☐ It will optimize the PL/SQL compiler to enable better run-time performance but degrade the compiler performance slightly.

Answer:

It will enable the extended PL/SQL debugging features in your database.

It will cause compiled PL/SQL code to be stored as interpreted bytecode regardless of the of PLSQL_CODE_TYPE setting.

Explanation:

Setting the parameter PLSQL_DEBUG to TRUE enables the additional PL/SQL debugging features that are helpful in a development environment. When the PLSQL_DEBUG parameter is set to TRUE, the compiler will store the compiled code as interpreted bytecode, regardless of the PLSQL_CODE_TYPE parameter setting. This interpreted bytecode provides for the use of extended debugging features.

This parameter setting will not disable the extended PL/SQL debugging features. Setting this parameter to a value of FALSE will disable the extended debugging features.

The parameter setting will not cause compiled PL/SQL code to be stored as native machine code regardless of PLSQL_CODE_TYPE setting. When the PLSQL_DEBUG parameter is set to TRUE, the compiler will store compiled PL/SQL as interpreted bytecode rather than native machine code.

This parameter setting will not optimize the PL/SQL compiler to enable better run-time performance, but slightly degrade the compiler performance. The PLSQL_OPTIMIZE_LEVEL parameter is used to optimize the compiler performance. The default setting of PLSQL_OPTIMIZE_LEVEL=1 will provide optimum compiler performance. The PLSQL_OPTIMIZE_LEVEL=2 parameter setting provides better run-time performance but slightly degrades compiler performance.

Oracle Database Security

Item: 1 (Ref:1Z0-042.10.1.2)

Eric has been hired as a new DBA in his organization. His supervisor asks him to make changes in the database to disable OS authentication from remote clients.

Which action must Eric take to achieve this objective?

- Set the value of the REMOTE_OS_AUTHENT parameter to TRUE.
- Set the value of the REMOTE_OS_AUTHENT parameter to FALSE.
- Set the value of the OS_AUTHENT_PREFIX parameter to REMOTE.
- Set the value of the REMOTE_LOGIN_PASSWORDFILE parameter to NONE.
- Set the value of the REMOTE_LOGIN_PASSWORDFILE parameter to EXCLUSIVE.

Answer:

Set the value of the REMOTE_OS_AUTHENT parameter to FALSE.

Explanation:

To disable OS authentication from remote clients, Eric must set the value of the REMOTE_OS_AUTHENT parameter to FALSE. The REMOTE_OS_AUTHENT parameter is used to specify whether or not OS authentication from remote clients should be enabled. The default setting of REMOTE_OS_AUTHENT=FALSE specifies that OS authentication from remote clients is disabled. If remote OS authentication is enabled, the database user is authenticated externally from a remote system and users log on to the database without any further authentication. This poses a potential threat to the system.

Eric must not set the value of the REMOTE_OS_AUTHENT parameter to TRUE because setting the parameter to TRUE will enable OS authentication from remote clients.

Eric must not set the value of the OS_AUTHENT_PREFIX parameter to REMOTE because this parameter is not used for OS authentication from remote clients. This parameter is used to prefix a specified variable to all usernames when using OS authentication.

Eric must not set the value of the REMOTE_LOGIN_PASSWORDFILE parameter to NONE. This parameter is not used for OS authentication from remote clients. Setting it to NONE will not make any difference to the authentication from remote clients. This parameter is used when you use a password file for authenticating users on your database.

Eric need not set the value of the REMOTE_LOGIN_PASSWORDFILE parameter to EXCLUSIVE. This parameter is not used for OS authentication from remote clients. Setting it to EXCLUSIVE will not make any difference to the authentication from remote clients. This parameter is used when you use a password file for authenticating users on your database.

Item: 2 (Ref:1Z0-042.10.4.3)

You are administering 100 users in your database. You want to view the fine-grained audit records and the standard audit trail entries generated for the user AMY in your database.

Which SQL statement should you use to achieve this objective?

- SELECT * FROM DBA_AUDIT_TRAIL WHERE USERNAME='AMY';
- SELECT * FROM USER_AUDIT_TRAIL WHERE USERNAME='AMY';
- SELECT * FROM DBA_FGA_AUDIT_TRAIL WHERE DB_USER='AMY';
- SELECT * FROM DBA_FGA_AUDIT_TRAIL WHERE USERNAME='AMY';
- SELECT * FROM DBA_COMMON_AUDIT_TRAIL WHERE DB_USER='AMY';

Answer:

SELECT * FROM DBA_COMMON_AUDIT_TRAIL WHERE DB_USER='AMY';

Explanation:

To view the fine-grained audit records and the standard audit trail entries for database user AMY, you should use the following SQL statement:

```
SELECT * FROM DBA_COMMON_AUDIT_TRAIL WHERE DB_USER='AMY';
```

This statement will query the DBA_COMMON_AUDIT_TRAIL view, which contains the fine-grained audit records and the standard auditing records for all users in the database. To restrict the details to a particular database user, you must use the WHERE clause to specify the username contained in the DB_USER column of the DBA_COMMON_AUDIT_TRAIL view.

The statement that queries the DBA_AUDIT_TRAIL view is incorrect because the DBA_AUDIT_TRAIL view does not contain the fine-grained audit records. It only contains the standard audit records for database users. This view should be queried when you want to view only the standard audit records for database users.

The statement that queries the USER_AUDIT_TRAIL view is incorrect because the USER_AUDIT_TRAIL view does not contain the fine-grained audit records. The USER_AUDIT_TRAIL view only contains standard auditing records for a particular database user.

The statements that query the DBA_FGA_AUDIT_TRAIL view are incorrect because the DBA_FGA_AUDIT_TRAIL view will only display the fine-grained auditing records. This view will not display the standard auditing records. The DBA_FGA_AUDIT_TRAIL view can be used when you want to view fine-grained auditing records for database users.

Item: 3 (Ref:1Z0-042.10.4.1)

You decide to implement a Fine-Grained Auditing (FGA) policy in your database to audit the SQL statements for a particular user. Which statements can be audited using an FGA policy?

- SELECT and ALTER only
- DELETE and ALTER only
- SELECT, INSERT, and ALTER only
- SELECT, INSERT, and UPDATE only
- SELECT, INSERT, UPDATE, and DELETE

Answer:

SELECT, INSERT, UPDATE, and DELETE

Explanation:

An FGA policy can audit the SELECT, INSERT, UPDATE, and DELETE statements. An FGA policy is used to capture the SQL statements used and the SQL operations performed on objects in the database. FGA can be used in situations where database triggers or standard auditing options would not accomplish your objectives.

SELECT and ALTER only is incorrect because an FGA policy cannot audit ALTER statements.

DELETE and ALTER only is incorrect because an FGA policy cannot audit ALTER statements.

SELECT, INSERT and ALTER only is incorrect because you cannot audit ALTER statements using an FGA policy.

SELECT, INSERT and UPDATE only is incorrect because you can also audit DELETE statements using an FGA policy.

Item: 4 (Ref:1Z0-042.10.1.1)

You have included the following parameter in your initialization parameter file for PL/SQL users to create files on the host computer:

```
UTL_FILE_DIR=*
```

Which statement is true?

- The PL/SQL users cannot create any file on the host computer.
- The PL/SQL users can only read all the files on the host computer.
- The PL/SQL users can create files in any location on the host computer.
- The PL/SQL users can create files only in the root directory of the host computer.
- The PL/SQL users can create files only at the location specified by the ORACLE_HOME environment variable.

Answer:

The PL/SQL users can create files in any location on the host computer.

Explanation:

The PL/SQL users can create files in any location on the host computer if the initialization parameter UTL_FILE_DIR is assigned the value of asterisk (*). The value * indicates all destinations. The PL/SQL users can create files at the location specified by the UTL_FILE_DIR parameter by using the UTL_FILE package.

The option stating that PL/SQL users cannot create files is incorrect because with this setting the PL/SQL users can create files in any location on the host computer.

The option stating that PL/SQL users can only read all the files on the host computer is incorrect because with this setting the PL/SQL users can read, write, and create files on any location on the host computer.

The option stating that PL/SQL users can create files only in the root directory of the host computer is incorrect because with this setting the PL/SQL users can create files in any location on the host computer.

The option stating that the PL/SQL users can create files only at the location specified by the ORACLE_HOME environment variable is incorrect. The ORACLE_HOME environment variable specifies the location of the Oracle home directory where the Oracle software is installed.

Item: 5 (Ref:1Z0-042.10.3.1)

You have created a password verify function to validate the password of the users when new users are created or when existing users try to change their existing passwords.

Which characteristics of passwords can be verified using this function? (Choose all that apply.)

- ☐ the frequency that the password must be changed
- ☐ the minimum number of characters for the password
- ☐ whether or not the password can be similar to one of the last three passwords created
- ☐ the number of numeric, alphabetic and special characters that the password must contain
- ☐ whether or not password authentication of the user should be done by the operating system

Answer:

the minimum number of characters for the password
the number of numeric, alphabetic and special characters that the password must contain

---

Explanation:

When you create a password verify function for verifying the user password, this function can verify the following password characteristics:

- The minimum number of characters for the password
- The characters that the password must contain, such as when a password should contain a specific number of numeric, alphabetic or special characters
- Whether or not the password can be the same as the username
- Whether or not the new password can be similar to the previous password

The option that states that the password verify function can verify the frequency that the password must be changed is incorrect. The frequency that the password should be changed can be set in the user's profile. The `PASSWORD_LIFE_TIME` parameter determines the life of a password in number of days. After the specified number of days have elapsed, the password must be changed.

The option stating that the password verify function can verify whether or not the password can be similar to the last three passwords created is incorrect. The password verify function can be used to ensure that the new password is not similar to the previous password, but not the last three passwords.

The option stating that the password verify function can specify whether or not password authentication of the user should be done by the operating system is incorrect because the password verify function is enabled only when the password authentication of users is done by the database.

Item: 6 (Ref:1Z0-042.10.1.3)

You do not want the database users of your database to query the data in the data dictionary tables.

Which action will you perform to achieve your objective?

- Set the COMPATIBLE parameter to FALSE.
- Revoke the SELECT ANY TABLE privilege from the users.
- Set the REMOTE_LOGIN_PASSWORDFILE parameter to NONE.
- Set the O7_DICTIONARY_ACCESSIBILITY parameter to TRUE.
- Set the O7_DICTIONARY_ACCESSIBILITY parameter to FALSE.
- Set the REMOTE_LOGIN_PASSWORDFILE parameter to EXCLUSIVE.

Answer:

Set the O7_DICTIONARY_ACCESSIBILITY parameter to FALSE.

Explanation:

To prevent the users from querying data in the data dictionary tables, you must set the O7_DICTIONARY_ACCESSIBILITY parameter to FALSE. Setting this parameter to FALSE prevents users from accessing the tables in the data dictionary even if they have the SELECT ANY TABLE privilege.

The option stating that you must set the COMPATIBLE parameter to FALSE is incorrect because this parameter does not restrict access to the data dictionary tables. The COMPATIBLE parameter enables you to use new features in a new release of Oracle and guarantees backward compatibility with an earlier release. The value of FALSE is not valid for this parameter. To successfully use the features of Oracle 10*g,* you must set this parameter to 10.0.0 or higher.

The option stating that you must revoke the SELECT ANY TABLE privilege from the users is incorrect because this will prevent users from accessing all the tables in the database. To prevent users with the SELECT ANY TABLE privilege from accessing only the data dictionary tables, you must set the O7_DICTIONARY_ACCESSIBILITY parameter to FALSE.

The option stating that you must set the REMOTE_LOGIN_PASSWORDFILE parameter to NONE is incorrect because this parameter does not restrict access to the data dictionary. The REMOTE_LOGIN_PASSWORDFILE parameter specifies whether or not password file authentication is to be used for authenticating remote users to the database. It also specifies the number of databases that can use the password file and the number of database users who can be granted the SYSDBA or SYSOPER privilege. Setting the REMOTE_LOGIN_PASSWORDFILE parameter to NONE specifies that the password file will not be used.

The option stating that you must set the O7_DICTIONARY_ACCESSIBILITY parameter to TRUE is incorrect because setting this parameter to TRUE will allow the users with the SELECT ANY TABLE privilege to access tables in the data dictionary.

The option stating that you must set the REMOTE_LOGIN_PASSWORDFILE parameter to EXCLUSIVE is incorrect because this parameter does not restrict access to the data dictionary. The REMOTE_LOGIN_PASSWORDFILE parameter specifies whether or not password file authentication is to be used for authenticating remote users to the database. It also specifies how many databases can use the password file and the number of database users who can be granted the SYSDBA or SYSOPER privilege. Setting the REMOTE_LOGIN_PASSWORDFILE parameter to EXCLUSIVE specifies that the password file is to be used for user authentication and that only one database can use this password file.

Item: 7 (Ref:1Z0-042.10.4.2)

You are a database administrator handling auditing and security of the database in your company. You want to see how inserts and updates are being audited on the JIM.MASTER table.

Which statement can you use to view this information?

- SELECT OBJECT_NAME, OBJECT_TYPE, INS, UPD

  FROM DBA_OBJ_AUDIT_OPTS
  WHERE OBJECT_NAME='JIM.MASTER';
- SELECT OBJECT_NAME, OBJECT_TYPE, INS, UPD

  FROM DBA_AUDIT_OBJ_OPTS
  WHERE OBJECT_NAME='JIM.MASTER';
- SELECT OBJECT_NAME, OBJECT_TYPE, INSERT, UPDATE

  FROM DBA_OBJ_AUDIT_OPTS
  WHERE OBJECT_NAME='JIM.MASTER';
- SELECT OBJECT_NAME, OBJECT_TYPE, INSERT, UPDATE

  FROM DBA_AUDIT_OBJ_OPTS
  WHERE OBJECT_NAME='JIM.MASTER';

Answer:

```
SELECT OBJECT_NAME, OBJECT_TYPE, INS, UPD

FROM DBA_OBJ_AUDIT_OPTS
WHERE OBJECT_NAME='JIM.MASTER';
```

Explanation:

To find out the options provided for auditing inserts and updates on the JIM.MASTER table, you can use the following statement:

```
SELECT OBJECT_NAME, OBJECT_TYPE, INS, UPD
FROM DBA_OBJ_AUDIT_OPTS
WHERE OBJECT_NAME='JIM.MASTER';
```

The DBA_OBJ_AUDIT_OPTS view contains the auditing options for all database objects. The output of the given statement will display a value such as A/S, -/S, or A/- in the INS and UPD columns. Audit options are displayed as a successful value and a not successful value, separated with a slash (/). The following are the three possible values for each successful or unsuccessful status:

- Not Audited
S Collect audit records by session
A Collect audit records by access

You cannot use either of the statements that query the DBA_AUDIT_OBJ_OPTS view because this is not a valid view.

You cannot use the statement that queries the INSERT and UPDATE columns of the DBA_OBJ_AUDIT_OPTS view because INSERT and UPDATE are not valid column names in the DBA_OBJ_AUDIT_OPTS view.

Item: 8 (Ref:1Z0-042.10.3.2)

You create a database user JOHN and assign him the PROF1 profile. Click the Exhibit(s) button to view the statement used to create the PROF1 profile.

Which conditions in the database would lock the user JOHN's account? (Choose all that apply.)

- [ ] if the CONNECT role is revoked from JOHN
- [ ] if the DBA runs a command to expire JOHN's password
- [ ] if JOHN fails to change the password within the grace period
- [ ] if JOHN's account was created with the ACCOUNT LOCK clause
- [ ] if JOHN tries to connect to the database with an incorrect password five times
- [ ] if JOHN tries to connect to the database with an incorrect password five times consecutively

Answer:

if JOHN's account was created with the ACCOUNT LOCK clause

if JOHN tries to connect to the database with an incorrect password five times consecutively

```
SQL> CREATE PROFILE PROF1 LIMIT
     FAILED_LOGIN_ATTEMPTS 5
     PASSWORD_LIFE_TIME 60
     PASSWORD_REUSE_TIME 50
     PASSWORD_REUSE_MAX 4
     PASSWORD_LOCK_TIME UNLIMITED
     PASSWORD_GRACE_TIME 10;
```

Explanation:

JOHN's account will be locked if it has been created with the ACCOUNT LOCK clause in the CREATE USER statement. The ACCOUNT LOCK clause of the CREATE USER statement locks the user account. In addition, JOHN's account will be locked if he tries to connect to the database by using an incorrect password five times consecutively because the PROF1 profile assigned to JOHN has a FAILED_LOGIN_ATTEMPTS parameter value of 5. The FAILED_LOGIN_ATTEMPTS parameter indicates the number of consecutive times that a user can unsuccessfully attempt to log in before the account is locked. After the user account is locked, it can be unlocked by the DBA by running the ALTER USER...ACCOUNT UNLOCK statement.

JOHN's account will not be locked if the CONNECT role is revoked from it. The CONNECT role is an Oracle-supplied role that provides basic user privileges. If you revoke the CONNECT role, JOHN will receive an error stating that he does not have sufficient privileges.

JOHN's account will not be locked if the DBA runs a command to expire his password. In that situation, JOHN would receive a message stating that his password had expired and be prompted to create a new password.

JOHN's account will not be locked if he fails to change his password within the grace period. In that situation, only JOHN's password would expire.

JOHN's account will not be locked if he connects to the database with an incorrect password five times. It will be locked only if he connects to the database with an incorrect password five times consecutively.

Oracle Net Services

Item: 1 (Ref:1Z0-042.11.5.1)

You are connecting to the database using the Local naming method. While connecting from the client to the database, which two pieces of information must be provided in the connect string to successfully connect to the database? (Choose two.)

- [ ] host name
- [ ] service name
- [ ] database name
- [ ] naming method
- [ ] listener port number
- [ ] valid username and password

Answer:

service name
valid username and password

Explanation:

To connect to the database by using a connect string, you must provide a valid username and password and the service name. The service name contains the information of the database name and the host name. The following gives the syntax of the connect string when using Local naming:

`CONNECT` *`username/password@servicename`*

When you configure the Local naming method to connect to the database, the net service names are added to the `tnsnames.ora` file. These net service names map to a connect descriptor.

You are not required to provide the host name in the connection string while connecting to the database using the Local naming method. The host name is present in the address list of the connect descriptor.

You are not required to provide the database name in the connection string while connecting to the database using the Local naming method. The database name is determined from the `SERVICE_NAME` parameter in the connect descriptor.

You are not required to provide the naming method in the connection string while connecting to the database using the Local naming method. The naming method to be used is determined by using the `sqlnet.ora` file.

You are not required to provide the listener port number in the connection string while connecting to the database using the Local naming method. This port number is present in the `listener.ora` file specific to the database.

Item: 2 (Ref:1Z0-042.11.4.4)

You have set the value for the TRACE_LEVEL_L1 parameter to 16, where L1 is the name of the listener.

Which two statements are true about setting this parameter? (Choose two.)

- The value of 16 is invalid for this parameter.
- This parameter is set in the listener.ora file.
- This parameter is set in the initmaster.ora file.
- Setting this value enables tracing to identify installation-specific problems.
- Setting this value enables tracing to identify user-induced error conditions.
- Setting this value enables maximum tracing, which is required by Oracle Support services for troubleshooting.

Answer:

This parameter is set in the listener.ora file.

Setting this value enables maximum tracing, which is required by Oracle Support services for troubleshooting.

Explanation:

The parameter TRACE_LEVEL_L1 is set in the listener.ora file and setting this parameter to a value of 16 provides maximum trace information for troubleshooting information for Oracle Support services. The TRACE_LEVEL_*listener* parameter in the listener.ora file specifies the level of detail that will be captured in listener trace records. This parameter can be specified as a number between 0 and 16, where a zero value indicates no listener tracing and a value of 16 indicates maximum tracing for listeners. This parameter can also be specified using the values off, user, admin, and support, which indicate tracing level values of 0, 4, 6, and 16, respectively.

The value of 16, which is equivalent to a value of support, is not invalid for this parameter. A value of 16 indicates maximum tracing for the listener.

This parameter is not set in the initmaster.ora file. Instead, this parameter is set in the listener.ora file. The TRACE_LEVEL_*listener* parameter is a listener-specific parameter that can be specified for each listener.

Setting this value does not enable tracing to identify installation-specific problems. Setting the parameter to a value of admin or 6 enables tracing to identify installation-specific problems.

Setting this value does not enable tracing to identify user-induced error conditions. Setting the parameter to a value of user or 4 enables tracing to identify user-induced error conditions.

Item: 3 (Ref:1Z0-042.11.3.2)

You have enabled connect-time failover in your database. What does this connect-time failover feature achieve?

- It instructs Oracle Net to enable multiple listeners at a time.
- It instructs Oracle Net to fail over to a different listener if the first listener fails at connect time.
- It instructs Oracle Net to use the listener that has the minimum load when multiple listeners have been configured.
- It instructs Oracle Net to balance the load on the various listeners by progressing through a list of protocol addresses at random.

Answer:

It instructs Oracle Net to fail over to a different listener if the first listener fails at connect time.

Explanation:

Enabling connect-time failover instructs Oracle Net to fail over to a different listener if the first listener fails at connect time. The number of addresses present in the list determines the number of addresses that will be tried. To enable connect-time failover in a database, you can add the `FAILOVER=ON` parameter to the `ADDRESS_LIST` parameter of your `tnsnames.ora` file as shown in the following example:

```
sales.us.esoft.com=
(DESCRIPTION=(ADDRESS_LIST=
(FAILOVER=ON)
(ADDRESS=(PROTOCOL=tcp)(HOST=sales1-server)(PORT=1521))
(ADDRESS=(PROTOCOL=tcp)(HOST=sales2-server)(PORT=1521)))
(CONNECT_DATA=
(SERVICE_NAME=sales.us.esoft.com)))
```

Enabling connect-time failover does not instruct Oracle Net to enable multiple listeners at a time.

Enabling connect-time failover does not enable load balancing on different listeners. The load balancing feature is used to balance the load across the various listeners. This is enabled by setting the `LOAD_BALANCE=ON` parameter in the `ADDRESS_LIST` parameter of your `tnsnames.ora` file.

Enabling connect-time failover does not enable using the listener with the minimum load when multiple listeners have been configured for a database.

Item: 4 (Ref:1Z0-042.11.2.2)

You have configured shared server architecture in your database environment. This configuration consists of three listeners named `L1`, `L2` and `L3`. These listeners have been configured to listen for the two database instances `FIN1` and `FIN2` in your Oracle environment. The two instances have one dispatcher each. The automatic service registration for the listeners is enabled. As a result, the listeners receive the required information from the two instances.

There are multiple users on the two databases. Therefore, you must balance the load on both the listeners.

Using Oracle Enterprise Manager 10*g* Database Control, you have selected the following option from the **Address List Options** dialog box:

- **Try one address, selected at random**

Which other option should you choose to balance the load on the listeners?

- **Use only the first address**
- **Try each address, in order, until one succeeds**
- **Try each address, randomly, until one succeeds**
- **Use each address in order until destination reached**

Answer:

Try each address, randomly, until one succeeds

Explanation:

To balance the load across all the listeners in a shared server environment, you should choose the following two options:

- **Try one address, selected at random**
- **Try each address, randomly, until one succeeds**

Connection load balancing is performed to balance the load of the incoming connections on the listener, when two or more listeners have been configured for the database instance. At connect time, these two options instruct Oracle Net to fail over to a different listener if the first listener fails.

The **Use only the first address** option does not configure load balancing on the listener. Setting this option configures source routing.

The **Try each address, in order, until one succeeds** option does not configure load balancing on the listener. Setting this option configures connect-time failover.

The **Use each address in order until the destination** is reached option does not configure load balancing on the listener. Setting this option configures source routing.

Item: 5 (Ref:1Z0-042.11.5.3)

You configure the `sqlnet.ora` file on your database server. In which scenario would it be appropriate to examine the `sqlnet.ora` file?

- You want to know the number of listeners listening for the database.
- You want to know the number service names configured on the database server.
- You want to know the order of naming methods the client will use while resolving a service name.
- You want to determine whether your database server is configured as a shared server or as a dedicated server.

Answer:

You want to know the order of naming methods the client will use while resolving a service name.

Explanation:

The `sqlnet.ora` file on the database server would be examined when you want to know the order of naming methods the client will use while resolving the net service name. This file is a net configuration file that can be present on the server or the client. The `sqlnet.ora` file specifies the order of the naming methods used by the client to resolve the service name, the logging and tracing features to use, external naming features, and other details about the network. While connecting to the database, if the database server is not able to resolve the service name, you will receive the following error:

```
ORA-12154: TNS:could not resolve service name
```

To resolve this error, you must refer to the `sqlnet.ora` file and the `tnsnames.ora` file. These two files contain the information about the net service names used by clients while connecting to the database server.

You would not examine the `sqlnet.ora` file when you want to know the number of listeners listening for the database. The information regarding the number of listeners listening for the database exists in the `listener.ora` file.

You would not examine the `sqlnet.ora` file when you want to know the number service names configured on the database server. The information about the number of service names configured on the database server is provided in the `tnsnames.ora` file.

You would not examine the `sqlnet.ora` file if you want to determine whether your database server is configured as a shared server or as a dedicated server. The configuration of shared or dedicated servers is specified in the initialization parameter file of the database.

Item: 6 (Ref:1Z0-042.11.3.1)

Using Oracle Enterprise Manager on your database, you have chosen the following options in the **Address List Options** dialog box:

- **Try each address, in order, until one succeeds**
- **Try each address, randomly, until one succeeds**

Which two features are enabled in your database by setting these options? (Choose two.)

- ☐ load balancing
- ☐ source routing
- ☐ standby failover
- ☐ instance failover
- ☐ database failover
- ☐ connect-time failover

Answer:

load balancing
connect-time failover

Explanation:

With these options, load balancing and connect-time failover are enabled in your database. To enable connect-time failover and load balancing by using the Oracle Enterprise Manager, you should choose the following options on your database's **Address List Options** dialog box:

- **Try each address in order, until one succeeds**
- **Try each address randomly, until one succeeds**

Source routing is not enabled by using these parameters. Source routing instructs Oracle Net to use each address in the presented order until the destination is reached. Source routing is mainly required to reach a destination using a specific route. To enable source routing, you should choose the **Use each address in order until destination reached** option in the database's **Address List Options** dialog box.

Standby failover is an incorrect option because there are no options in Oracle Net services to configure standby failover.

Instance failover is not enabled by using these parameters. Applying instance failover is done in a database environment using Data Guard.

Database failover is not enabled by using these parameters. Database failover involves switching over to a standby database when the primary database goes down. Database switchover is done using specific SQL*Plus statements.

Item: 7 (Ref:1Z0-042.11.4.1)

You are a database administrator in your company. You have configured two listeners on your host computer to listen to your PROD database. These listeners are named LISTENER and L2. LISTENER uses the TCP/IP protocol and port 1521. L2 uses the TCP/IP protocol and port 1421.

In this scenario, which statement is true about the registration of the listeners?

- Both of the listeners will be registered dynamically by the PMON process.
- To enable dynamic registration of L2, you will need to set the LOCAL_LISTENER=L2 parameter in the parameter file.
- To enable dynamic registration of L2, you will need to set the REMOTE_LISTENER=L2 parameter in the parameter file.
- To enable dynamic registration of all the listeners, you will need to set the LOCAL_LISTENER=LISTENER, L2 parameter in the parameter file.
- To enable dynamic registration of both listeners, you will need to set the REMOTE_LISTENER=LISTENER, L2 parameter in the parameter file.

Answer:

To enable dynamic registration of L2, you will need to set the LOCAL_LISTENER=L2 parameter in the parameter file.

Explanation:

To enable dynamic registration for a nondefault listener L2, you must specify the parameter LOCAL_LISTENER=L2 in the parameter file. The listener that uses the standard protocol TCP/IP and port 1521 is the default listener. By default, the PMON process will register the information for this listener dynamically. In this scenario, you also have the nondefault listener L2. This listener will not be registered dynamically without specifying the LOCAL_LISTENER parameter in the parameter file.

The option that states that both listeners will be registered by PMON is incorrect because the listener L2 cannot be registered dynamically without specifying the LOCAL_LISTENER parameter in the parameter file.

The option that states that you will need to set the parameter REMOTE_LISTENER=L2 in the parameter file to enable dynamic registration of listener L2 is incorrect because the listener L2 is not a remote listener. L2 is a local listener. Therefore, you need to set the LOCAL_LISTENER parameter, rather than the REMOTE_LISTENER parameter, to specify the name of the listener.

The option that states that you will need to set the parameter LOCAL_LISTENER=LISTENER, L2 in the parameter file to enable dynamic registration of all the listeners is incorrect. LISTENER is the default listener and is registered dynamically without specifying its value in the parameter LOCAL_LISTENER.

The option that states that you will need to set the parameter REMOTE_LISTENER=LISTENER, L2 in the parameter file to enable dynamic registration of both the listeners is incorrect because both of these are local listeners. You use the LOCAL_LISTENER parameter, not the REMOTE_LISTENER parameter, for local listeners. Also, LISTENER is the default listener and is registered dynamically without specifying its value in the LOCAL_LISTENER parameter in the parameter file.

Item: 8 (Ref:1Z0-042.11.1.2)

You have created a listener by using Database Control. After configuring the listener for your database, you executed the following command:

```
C:\> SQLPLUS scott/tiger@10g
```

While executing the command, you received the following error message:

```
ORA-12154: TNS:could not resolve the connect identifier specified.
```

Why did the error occur?

- The syntax of the command is incorrect.
- The listener is running on the Oracle server.
- The port number used by the new listener is already in use.
- The connect identifier supplied does not exist in the `tnsnames.ora` file.
- A listener is not available to listen to the service name mentioned in the `tnsnames.ora` file.

Answer:

The connect identifier supplied does not exist in the `tnsnames.ora` file.

Explanation:

You will receive an `ORA-12154: TNS:could not resolve the connect identifier specified` error message because the connect identifier supplied does not exist in the `tnsnames.ora` file. The connect identifier identified by 10*g* must be configured in the `tnsnames.ora` file to connect to the destination Oracle database.

The stated syntax of the command is correct. Therefore, the error is not generated due to incorrect syntax.

If the listener is not running on the Oracle server, the `TNS-12541/ORA-12541: TNS:no listener` error is generated.

If the port number used by the new listener is already in use, the error in this scenario will not be generated. Instead, the error generated will be `TNS-12560: TNS:protocol adapter error`.

The unavailability of a listener to listen to the service name mentioned in the `tnsnames.ora` file is not a valid reason for the error to occur. This error signifies that a listener is configured in the Oracle database but not configured to listen to the service name being configured in the `tnsnames.ora` file of the client computer. If the listener is not available, the `TNS-12541/ORA-12541: TNS:no listener` error will be generated.

Item: 9 (Ref:1Z0-042.11.1.1)

You want to know the uptime duration of your default listener. Which command-line command can you use to determine the uptime duration of the default listener?

- `lsnrctl stop`
- `lsnrctl start`
- `lsnrctl status`
- `lsnrctl services`

Answer:

`lsnrctl status`

Explanation:

You can use the `lsnrctl status` command to display the uptime duration of the default listener. The `lsnrctl status` command displays information about a listener, including the listener's status, configuration settings, and whether or not the listener was dynamically registered. The syntax of the `lsnrctl status` command is:

`lsnrctl status [`*`listenername`*`]`

If a *`listenername`* is specified then the status of the specified listener is displayed. However, if no *`listenername`* is specified, the status and configuration of the default listener, `LISTENER`, is displayed.

The `lsnrctl stop` command is used to stop the default listener.

The `lsnrctl start` command is used to start the default listener.

The `lsnrctl services` command is used to view detailed information regarding the different databases, instances, and dispatchers to which the listener forwards client requests. It also provides information on whether or not the listener was dynamically registered.

Item: 10 (Ref:1Z0-042.11.2.1)

You are a database administrator in your company working on the ADMIN database. There are 25 users in the office that must access this database by using the TCP/IP protocol. You must configure the database so that these users can access the database from their local computers. You are using Database Control to configure the naming methods.

Configuring which naming method would involve the least administrative overhead in this scenario?

- Local naming method
- External naming method
- Directory naming method
- Easy Connect naming method

Answer:

Easy Connect naming method

Explanation:

In this scenario, the Easy Connect naming method would be the best option to ensure the least administrative overhead. The Easy Connect naming method is enabled by default and does not require any client-side configuration or naming service method and the directory system. It can be used in the situation where there are fewer users accessing the database. Also, the Easy Connect naming method is supported only by the TCP/IP protocol. It does not provide support for advanced options such as connect-time failover, source routing, and load balancing.

Local naming can also be used in this scenario, but Local naming involves more administrative overhead than the Easy Connect naming method. Local naming involves using the `tnsnames.ora` file, which contains the list of net service names. These net service names map to a connect descriptor that contains detailed information about the connection options and the database for which the net service name is configured. The Local naming method can be used in a similar situation that uses a protocol other than TCP/IP, where you cannot use the Easy Connect naming method.

External naming should not be used in this scenario because it involves more administrative overhead than the Easy Connect method. External naming involves resolving a net service name stored in a non-Oracle naming service.

Directory naming should not be used in this scenario because it involves more administrative overhead than the Easy Connect method. Directory naming involves a centralized LDAP-compliant directory server, which stores the information required by the client computers. This directory enables central administration of database services and net service names when changes are made in the configuration. Directory naming should be used in scenarios where you have a large number of users and want to store and administer the required connection information centrally. This naming method does not involve updating the user-specific files used for resolving connections to the database because all the required information is located centrally.

Item: 11 (Ref:1Z0-042.11.2.3)

You have set the following parameter for your database:

```
NAMES.DEFAULT_DOMAIN=as.telstar.com
```

Which statement is true about the setting of this parameter?

- This parameter is applicable for all the naming methods.
- This parameter is set in the `tnsnames.ora` configuration file.
- This parameter specifies which naming method is used while resolving the net service name.
- This value is appended to any unqualified net service name specified in the connect string.

Answer:

This value is appended to any unqualified net service name specified in the connect string.

Explanation:

With the given setting, this value is appended to any unqualified net service name specified in the connect string. The `NAMES.DEFAULT_DOMAIN` parameter is specified in the `sqlnet.ora` configuration file when the clients specifically request names from a particular domain. This parameter is specified in the `sqlnet.ora` file as the default domain to be used by the clients. The same domain name must be specified in the `tnsnames.ora` file, or you would receive the following error:

```
ORA-12154: TNS: could not resolve service name
```

For example, when a client tries to connect to the database using the connect string `CONNECT adam/password@sales`, where the domain name is not mentioned and the `tnsnames.ora` file contains the net service name as `sales.as.telstar.com`, the domain name `as.telstar.com` will be appended to `sales` and it will be searched as `sales.as.telstar.com` in the `tnsnames.ora` file.

The option that the parameter is applicable for all naming methods is incorrect because the `NAMES.DEFAULT_DOMAIN` parameter is only valid for the Local naming method.

The option that this parameter is set in the `tnsnames.ora` configuration file is incorrect because the `NAMES.DEFAULT_DOMAIN` parameter is specified in the `sqlnet.ora` file.

The option that this parameter specifies which naming method is used while resolving the net service name is incorrect because this parameter does not specify the naming method to be used. The `NAMES.DIRECTORY_PATH` parameter specifies which naming method is used while resolving the net service name.

Item: 12 (Ref:1Z0-042.11.4.3)

You have updated the `listener.ora` file in your database to contain the information about the newly created listener `L1`.

Which four pieces of information present in the `listener.ora` file specifically pertain to the `L1` listener? (Choose four.)

- [ ] the location of the datafiles in the instance
- [ ] an indicator of whether or not the listener was dynamically registered
- [ ] the services for which the listener is listening
- [ ] the password configured for securing the listener
- [ ] the location of the `ORACLE_HOME` of the instance
- [ ] the parameters in the parameter file that are specific to the listener
- [ ] the protocol address on which the listener is accepting connection requests

Answer:

the services for which the listener is listening
the password configured for securing the listener
the location of the `ORACLE_HOME` of the instance
the protocol address on which the listener is accepting connection requests

---

Explanation:

The `listener.ora` file in your database contains the following information about the configuration of the listener:

- the name of the listener
- the services for which the listener is listening
- the password configured for securing the listener
- the location of the `ORACLE_HOME` of the instance
- the protocol address on which the listener is accepting connection requests

The `listener.ora` file does not provide information about the location of the datafiles in the instance. The information on location of datafiles in the database instance can be obtained from the control file trace or the `DBA_DATA_FILES` view.

The `listener.ora` file does not provide information regarding whether or not the listener was dynamically registered. The default listener `LISTENER` is always registered dynamically. To enable dynamic registration for other local listeners, you can set the `LOCAL_LISTENER` parameter with the listener name in the initialization parameter file. To enable dynamic registration for remote listeners, you can set the `REMOTE_LISTENER` parameter in the initialization parameter file.

The `listener.ora` file does not provide information about the parameters in the parameter file that are specific to the listener. The information about the parameters specific to the listener can be gathered by viewing the initialization parameter file for the database.

Item: 13 (Ref:1Z0-042.11.1.5)

Which command of the listener control utility should you use to verify whether the dispatcher configured has registered with the listener after the database startup?

- `lsnrctl help`
- `lsnrctl spawn`
- `lsnrctl status`
- `lsnrctl services`

Answer:

`lsnrctl services`

Explanation:

The `lsnrctl services` command of the listener control utility should be used to verify whether the dispatcher has registered with the listener upon database startup. This command of the listener control utility can also be used to verify whether the listener has dynamically registered with the database.

The `lsnrctl help` command of the listener control utility provides a list of all the commands in the listener control utility and syntax help for all these commands.

The `lsnrctl spawn` command of the listener control utility is used to start a stored program on the computer on which the listener is running and is listed with an alias in the `listener.ora` file.

The `lsnrctl status` command of the listener control utility is used to display the status information of the listener, the configuration settings of the listener, and the services registered with the listener. This command can also be used to verify whether the listener has dynamically registered with the database.

Item: 14 (Ref:1Z0-042.11.1.4)

You have created a listener by using Database Control and configured a listener named LSR2. Later, you issued the following command:

```
C:\> SQLPLUS scott/tiger@10g
```

While executing this command, you received the following error message:

```
ORA-12541: TNS:no listener.
```

Why did the error occur?

- The syntax of the command is incorrect.
- A listener does not exist in the Oracle database.
- The service name supplied does not exist in the `tnsnames.ora` file.
- A listener is not available to listen to the service name mentioned in the `tnsnames.ora` file.

Answer:

A listener does not exist in the Oracle database.

Explanation:

You receive the `ORA-12541: TNS:no listener` error message because a listener does not exist in the Oracle database. The reason can be either because the listener service is not running or because the listener is not capable of listening to the service name on the port number specified in the `tnsnames.ora` file. For example, if the listener is configured to listen to a service name on port number 1521, and the port number for the same service is specified as 1522 in the `tnsnames.ora` file, you will receive the `ORA-12541: TNS:no listener` error while connecting to the Oracle database.

The syntax of the command is correct.

The option that the service name supplied does not exist in the `tnsnames.ora` file is not a valid cause of the error. You receive the `ORA-12154: TNS:could not resolve service name` error if the service name supplied does not exist in the `tnsnames.ora` file.

The option that a listener is not available to listen to the service name mentioned in the `tnsnames.ora` file is not a valid reason for the error to occur. You receive the `ORA-12514: TNS:listener does not currently know of service requested in connectdescriptor` error if the service name is mentioned in the `tnsnames.ora` file but the listener is not configured to listen to the service name.

Item: 15 (Ref:1Z0-042.11.6.1)

You are testing connectivity from clients to the database server by using the TNSPING utility. You enter the following command to test the connectivity:

```
TNSPING MASTER 6
```

Which three statements are true for this command? (Choose three.)

- [ ] If successful, the command returns a single value.
- [ ] The command tries to test connectivity for the database MASTER.
- [ ] The command tries to connect to the service name named MASTER.
- [ ] The command specifies that TNSPING should attempt the connection six times.
- [ ] The command specifies that TNSPING should attempt to connect using six bytes of data.
- [ ] If successful, the command displays an estimate of the time it takes to reach the Oracle Net service.
- [ ] If successful, the command displays an estimate of the round trip time it takes to reach the Oracle Net service.

Answer:

The command tries to connect to the service name named MASTER.

The command specifies that TNSPING should attempt the connection six times.

If successful, the command displays an estimate of the round trip time it takes to reach the Oracle Net service.

Explanation:

The command TNSPING MASTER 6 tries to connect to the service name named MASTER six times. If successful, it returns a set of six values that are an estimate of the round trip time it takes to reach the Oracle Net service. The following command syntax can be used to invoke the TNSPING utility:

```
TNSPING net_service_name count
```

The *net_service_name* is a service name that must exist in the tnsnames.ora file or the net service name should be in use. The *count* specifies the number of times the program attempts to reach the server.

The option stating that if successful, the command returns a single value is incorrect because the command will return a set of six values for the six attempts it made to connect to the service name.

The option stating that the command tries to test connectivity for the database MASTER is incorrect because the command tries to connect to the specified Oracle Net service.

The option stating that the command specifies that TNSPING should attempt to connect using six bytes of data is incorrect because the command tries to connect six times.

The option stating that if successful, the command displays an estimate of the time it takes to reach the Oracle Net service is incorrect. This command will display an estimate of the round trip time it takes to reach the specified Oracle Net service.

Item: 16 (Ref:1Z0-042.11.1.3)

You have configured a listener named LSNR1 using Database Control. The listener is listening for two of your databases, MASTERDB and EMPDB. You create a new database, SALESDB, and then modify the listener.ora file for LSNR1 to ensure that LSNR1 also listens for the SALESDB database. Finally, you issue the following command from the lsnrctl utility:

```
LSNRCTL> RELOAD LSNR1
```

What does this command do?

- The command resets the listener, LSNR1, to listen only for the SALESDB database.
- The command stops the listener, LSNR1, and starts it with the new settings defined in the listener.ora file.
- The command dynamically resets the listener, LSNR1, with the new settings and rules defined in the listener.ora file.
- The command starts the listener, LSNR1, with the new settings defined in the listener.ora file, and resets all the client connections.

Answer:

The command dynamically resets the listener, LSNR1, with the new settings and rules defined in the listener.ora file.

Explanation:

The RELOAD LSNR1 command dynamically resets the listener, LSNR1, with the new settings and rules defined in the listener.ora file. The RELOAD command is a listener control utility command used to dynamically reset the listener with the new settings defined in the listener.ora file. Issuing this command will direct the listener control utility to reread the listener.ora file and apply the modified settings dynamically without modifying the current sessions.

Issuing the RELOAD LSNR1 command does not direct the listener to listen only for the SALESDB database. The listener will listen for all those databases whose information is present in the listener.ora file.

Issuing the RELOAD LSNR1 command to reset the listener with the new settings does not stop the listener. The new settings are applied dynamically.

Issuing the RELOAD LSNR1 command does not reset all the client connections. The settings are applied dynamically without modifying the current sessions.

Item: 17 (Ref:1Z0-042.11.4.2)

To secure the listener against unauthorized access, you have enabled a password on your default listener, LISTENER. You start the listener control utility and attempt to stop the listener using this command:

```
lsnrctl> STOP LISTENER
```

You encounter the following error:

TNS-01169: The listener has not recognized the password

Which lsnrctl command should you issue next to successfully stop the listener?

- STOP
- SET PASSWORD
- CHANGE PASSWORD
- STOP CURRENT_LISTENER

Answer:

SET PASSWORD

Explanation:

To stop the listener, you should issue the SET PASSWORD command. In this scenario, your default listener, LISTENER, is password protected. Therefore, to issue privileged commands against the listener, you must enter the password. To provide the password to enter such commands, you first run the SET PASSWORD command. If a password is set for the listener, you will be prompted to enter the password. After entering the password, you will then be able to issue your original STOP LISTENER command to stop the LISTENER listener.

The STOP command is incorrect. This command will again attempt to stop the default listener because no listener name is specified. However, you will receive the same error because you must first issue the SET PASSWORD command to enter the password for a listener that is password protected.

The CHANGE PASSWORD command is incorrect. This command is used to set a password for a listener.

The STOP CURRENT_LISTENER command is incorrect. This command will attempt to stop the listener named CURRENT_LISTENER. In this scenario, you are attempting to stop the default listener, LISTENER.

Item: 18 (Ref:1Z0-042.11.7.2)

You have configured a shared server for your networking environment in Oracle 10*g*. After configuring the listeners, the Local naming service and other network files required in the Local naming method, you attempt to connect from a client to the server.

What will happen as a result of this?

- The client connection will generate an error stating that the dispatchers are not configured.
- The client will connect to the database server because a dispatcher will be started automatically.
- The client will connect to the database server because dispatchers are not required in this configuration.
- The connection will fail because no dispatchers are configured.

Answer:

The client will connect to the database server because a dispatcher will be started automatically.

Explanation:

In this scenario, the client will connect to the database server because a dispatcher will be started automatically. In Oracle 10*g*, it is not necessary to configure the `DISPATCHERS` parameter. If this parameter is not configured and the shared server is enabled, a dispatcher listening on TCP/IP port 1521 will be configured and started automatically. Dispatchers are necessary in the shared server configuration because dispatchers enable many incoming user processes to connect to the same shared server processes. In this manner, dispatchers reduce the need for a dedicated shared server process for every incoming user connection request.

The option that states that the client connection will generate an error is incorrect because the client connection will not generate an error. Instead, it will connect to the server without any errors.

The option that states that the client connection will connect to the database server because no dispatchers are required is incorrect. A dispatcher is required to connect to the database in the shared server configuration, and this dispatcher will be configured automatically in Oracle 10*g.*

The option that states that the connection will fail because no dispatchers are configured is incorrect. The connection will not fail.

Item: 19 (Ref:1Z0-042.11.8.2)

Your server computer is configured to use the Local naming method. The `tnsnames.ora` and `sqlnet.ora` files on your computer contain the following information:

TNSNAMES.ORA

```
MASTER=(DESCRIPTION=
(ADDRESS=
(PROTOCOL=tcp)
(HOST=TELSTAR)
(PORT=1521))
(CONNECT_DATA=
(SERVICE_NAME=LOC)))
```

SQLNET.ORA

```
NAMES.DEFAULT_DOMAIN=US.TELSTAR.COM
NAMES.DIRECTORY_PATH=(LDAP, TNSNAMES, HOSTNAME)
```

What will happen when you try to connect to your database server by using these configuration settings?

- You will connect to the database by using the Easy Connect naming method.
- You will connect to the database by using the Host naming method.
- You will connect to the database by using the Local naming method.
- You will connect to the database by using the Directory naming method.
- You will receive an error while trying to connect to the database.

Answer:

You will receive an error while trying to connect to the database.

Explanation:

In this scenario, you will receive an error because the database has been configured to use the Local naming method, and you have specified LDAP to be the first option in the `NAMES.DIRECTORY_PATH` parameter. To rectify this, you should modify the `NAMES.DIRECTORY_PATH` parameter to include `TNSNAMES` as the first option as follows:

```
NAMES.DIRECTORY_PATH=(TNSNAMES, HOSTNAME)
```

This will specify Local naming as the first option. The `tnsnames.ora` file given in this scenario is correct and specifies `MASTER` as the service name for the connect descriptor.

The option that states that you will connect to the database by using the Easy Connect method is incorrect because you will receive an error while connecting to the database. The Easy Connect naming method is enabled by default and does not require any client-side configuration or naming service method and the directory system. It can be used in the situation where there are fewer users accessing the database. Also, the Easy Connect naming method is supported only by the TCP/IP protocol. It does not provide support for advanced options such as connect-time failover, source routing, and load balancing.

The option that states that you will connect to the database by using the Host naming method is incorrect because you will receive an error while connecting to the database. To connect by using the Host naming method, you must specify `HOSTNAME` as the first option in the `NAMES.DIRECTORY_PATH` parameter.

The option that states that you will connect to the database by using the Local naming method is incorrect because you will receive an error while connecting to the database. To connect to the database using the Local naming method, you must configure the database for using the Local naming method. Configuring Local Naming involves using the `tnsnames.ora` file.

The option that states that you will connect to the database by using the Directory naming method is incorrect because you will receive an error while connecting to the database. The Directory naming method does not use a `tnsnames.ora` file. It uses a centrally located directory server that stores all the information required by the client computers.

Item: 20 (Ref:1Z0-042.11.3.3)

You want to enable connect-time failover in your database to instruct Oracle Net to fail over to a different listener if the first listener fails.

Which parameter setting, when added to the ADDRESS_LIST parameter of your tnsnames.ora file, will provide you with the desired results?

- FAILOVER=ON
- FAIL_OVER=ON
- LOAD_BALANCE=ON
- CONNECT_TIME=FAILOVER

Answer:

FAILOVER=ON

Explanation:

The FAILOVER=ON parameter setting will provide you with the desired results. Enabling connect-time failover in a database is done by adding the FAILOVER=ON parameter to the ADDRESS_LIST parameter of your tnsnames.ora file as shown in the following example:

```
sales.us.esoft.com=
(DESCRIPTION=
(ADDRESS_LIST=
(LOAD_BALANCE=OFF)
(FAILOVER=ON)
(ADDRESS=(PROTOCOL=tcp)(HOST=sales1-server)(PORT=1521))
(ADDRESS=(PROTOCOL=tcp)(HOST=sales2-server)(PORT=1521)))
(CONNECT_DATA=
(SERVICE_NAME=sales.us.esoft.com)))
```

Enabling connect-time failover instructs Oracle Net to fail over to a different listener if the first listener fails at connect time. The number of addresses present in the list determines the number of addresses that will be tried.

The FAIL_OVER=ON setting is incorrect because the FAIL_OVER parameter is an invalid parameter and does not exist in Oracle Net services.

The LOAD_BALANCE=ON setting is incorrect because a failover to a different listener cannot be achieved by using this option. The LOAD_BALANCE=ON parameter enables the load balancing feature. The load balancing feature is used to balance the load across the various listeners. Specifying LOAD_BALANCE=OFF will turn off load balancing. The LOAD_BALANCE=ON parameter is also specified in the tnsnames.ora file.

The CONNECT_TIME=FAILOVER setting is incorrect because the CONNECT_TIME parameter is an invalid parameter and does not exist in Oracle Net services.

Item: 21 (Ref:1Z0-042.11.8.1)

You are working on database `FINDB1` with approximately 250 users. You want to modify the naming method to centrally store the data that is required for connection requests, to make changes in the Oracle Net service configurations. You also want to ensure that doing this does not generate a lot of overhead, considering that you have a considerable number of users in your database.

Which naming method should you use in this scenario?

- Local naming method
- Host naming method
- Easy Connect naming method
- External naming method
- Directory naming method

Answer:

Directory naming method

Explanation:

You should use the Directory naming method. The Directory naming method stores all the required connection information in a centralized LDAP-compliant directory server. Whenever there are changes in the Oracle Net service configurations, the centralized directory is updated simultaneously. This ensures that the updated information is available to the users as well. Using this naming method does not generate the overhead of updating the user-specific files used for resolving connections to the database.

The Local naming method cannot be used in this scenario because this method does not allow for central storage of data. The Local naming method should be used when you have a smaller client-server environment with few users and you want to store the connection information locally on the client computers. The Local naming method uses the `tnsnames.ora` net configuration file that contains the information required to connect to the database and is located on each client on the network environment.

The Host naming method cannot be used in this scenario because this method does not allow central storage of data. The Host naming method is recommended for simple TCP/IP environments.

The Easy Connect naming method cannot be used in this scenario because this method does not allow central storage of data. The Easy Connect naming method is enabled by default and does not require any client-side configuration or naming service method and the directory system. It can be used in the situation where there are fewer users accessing the database and the TCP/IP protocol is used. It does not provide support for advanced options such as connect-time failover, source routing, and load balancing.

The External naming method cannot be used in this scenario because this method does not allow storage of data centrally. The External naming method should be used when you want to store the net service names in a non-Oracle naming service.

Item: 22 (Ref:1Z0-042.11.5.2)

You must connect to the Oracle database by using the Easy Connect method. The service name is ORCLDB and the host name is ORACLESERVER. SCOTT is the user whose password is tiger.

Which statement will enable you to connect to the user SCOTT's schema in the Oracle database?

- CONNECT scott/tiger@orcldb
- CONNECT scott/tiger@orcldb:1521
- CONNECT scott/tiger@oracleserver
- CONNECT scott@oracleserver:1521/orcldb

Answer:

CONNECT scott/tiger@oracleserver

Explanation:

The CONNECT scott/tiger@oracleserver statement enables you to connect to the user SCOTT's schema in the Oracle database. By using the Easy Connect method, you can connect to the database by providing minimal information. This information includes the username, password, and host name of the server. The port and service name are optional for connecting to the database by using this method. The following syntax is used to connect to the Oracle database by using the Easy Connect method:

CONNECT *username/password@[//]host*[:*port*][/*service_name*]

The CONNECT scott/tiger@orcldb option is incorrect because this syntax is used to connect to the database by using the Local Naming method. When you connect to the database by using the Local Naming method, you must provide the service name.

The CONNECT scott/tiger@orcldb:1521 option is incorrect because this is syntactically incorrect. You must provide the host name while connecting to the database by using the Easy Connect naming method.

The CONNECT scott@oracleserver:1521/orcldb option is incorrect because the connect string is syntactically incorrect.

Oracle Shared Servers

Item: 1 (Ref:1Z0-042.12.4.1)

Eric is working in a database server, which has been recently configured for a shared server environment. Upon analysis, he realizes that there has been an increase in memory demands for the SGA component because some memory structures are now accommodated in the SGA.

Which component of the SGA should be allocated more memory to ensure that the new memory demands are met?

- java pool
- large pool
- shared pool
- program global area
- database buffer cache

Answer:

large pool

Explanation:

To allot additional memory for shared server processes, you must allocate more memory to the large pool area component of the SGA. When shared server architecture is used, the session data for database users is stored in the large pool component of the SGA. Therefore, whenever you configure shared server architecture for your server you must allot additional memory to the large pool. No other memory component in the SGA is affected as a result of changing from the dedicated server to shared server.

Allocating additional memory to the java pool will not add more memory to the shared server processes. It will add more memory to the java pool, which will help in storage of the session-specific java code and data in the Java Virtual Machine (JVM).

Allocating additional memory to the shared pool will not add more memory to the shared server processes. Adding more memory to the shared pool will increase the size of the library cache and dictionary cache, which might help to address problems related to the shared pool, but this will not help address the problem in this scenario.

Allocating more memory to the program global area is incorrect because the program global area is not a part of the SGA in a shared sever environment.

Allocating additional memory to the database buffer cache will not add more memory to the shared server processes. Adding more memory to the database buffer cache will increase the time for which the data blocks are stored in the database buffer cache, which might help to address problems related to the database buffer cache.

Item: 2 (Ref:1Z0-042.12.4.2)

The following events take place when a user submits a request on a shared server and the request is processed by the server:

1. The dispatcher retrieves the response from its own response queue.
2. The user process forwards a request to a dispatcher on the shared server.
3. The dispatcher places the request in the common request queue in the SGA.
4. The response is returned to the user.
5. The shared server process picks up the request, processes it and places the response on the calling dispatcher's response queue.

Which is the correct sequence of events that take place when the request is submitted to the server and a response is returned to the user?

- 12354
- 14253
- 21354
- 21534
- 23514

Answer:

23514

Explanation:

The correct sequence of events is 23514. When a request is submitted to the server and a response returned to the user, the following events take place:

The user process forwards a request to a dispatcher on the shared server.
The dispatcher places the request in the common request queue in the SGA.
The shared server process picks up the request, processes it, and places the response on the calling dispatcher's response queue.
The dispatcher retrieves the response from its own response queue.
The response is returned to the user.

All of the other options are incorrect because they do not represent the correct sequence of events.

Item: 3 (Ref:1Z0-042.12.2.2)

You have set the parameter SHARED_SERVERS=20 in the initialization parameter file of your PRODUCTS database that is configured as a shared server.

Which two statements are true for this parameter? (Choose two.)

- This parameter value determines the initial number of servers to start at startup.
- This parameter value must be equal to the number of dispatchers in the database.
- The maximum number of shared servers in this scenario cannot be more than 20.
- This parameter value specified, 20, must be larger than the value specified for the PROCESSES parameter.
- This parameter value determines the minimum number of shared servers that will remain started at any given time.

Answer:

This parameter value determines the initial number of servers to start at startup.

This parameter value determines the minimum number of shared servers that will remain started at any given time.

Explanation:

The SHARED_SERVERS parameter is used to set the initial number of shared servers started at startup. This value also determines the minimum number of shared servers that will remain started any given time.

The option stating that this parameter value must be equal to the number of dispatchers in the database is incorrect. The parameter value is not related to the number of dispatchers in your database.

The option stating that the maximum number of shared servers cannot be more than 20 in this scenario is incorrect because 20 will be the minimum number of servers. This parameter does not define the maximum number of shared servers in your database. The MAX_SHARED_SERVERS parameter specifies the maximum number of shared servers that can be started. When you specify the SHARED_SERVERS parameter and the MAX_SHARED_SERVERS parameter, the number of shared servers started at any given time will range between these two parameter values.

The option stating that the value specified must be larger than the value specified for the PROCESSES parameter is incorrect because the value of this parameter should always be less than the PROCESSES parameter in your database. The PROCESSES parameter controls the number of server-side processes.

Item: 4 (Ref:1Z0-042.12.1.2)

In which two scenarios would you configure your database in the shared server mode? (Choose two.)

- Your database has a high number of users with minimal activity.
- Your database has few users performing major activities, such as bulk loading of data and reports.
- You must perform database administration tasks by using the shared server connection.
- Your database is a data warehouse that runs reports and frequently performs batch uploads of data.
- Your database runs many queries in which the amount of data retrieved is small and the time required to execute queries is less.

Answer:

Your database has a high number of users with minimal activity.

Your database runs many queries in which the amount of data retrieved is small and the time required to execute queries is less.

Explanation:

You should configure shared server on your database when your database has a high number of users with minimal activity and when your server runs many queries in which the amount of data retrieved is small and the time required to execute queries is less. In this scenario, the use of shared server is ideal because the user processes require less time and resources for execution of the query and a single server process can serve these user processes simultaneously.

You should use the dedicated server configuration if your database often performs batch processing of data. In this scenario, the use of a dedicated server is ideal because batch processing of data involves large volumes of data and a dedicated server process will serve the need better because dedicated server process serves only one user process at a time.

You should use the dedicated server configuration if you must perform database administration tasks. Database administration tasks are privileged tasks and should always be performed using a dedicated server connection. Oracle recommends that all DBA sessions use dedicated server sessions.

You should use the dedicated server configuration if your database is a data warehouse, which runs reports and frequently performs uploads of data. Reports in a data warehouse involve large volumes of data and shared server processes are effective where small volumes of data are being used. Therefore, in this scenario, you should use a dedicated server connection.

Item: 5 (Ref:1Z0-042.12.3.1)

You have configured your Oracle server as a shared server. You want to collect information to tune the server for optimal performance.

Which dynamic view should you use to obtain the most relevant information regarding the tuning of your server?

- V$SGA
- V$QUEUE
- V$SGASTAT
- V$SHARED_SERVER
- V$SHARED_POOL_ADVICE
- V$SHARED_SERVER_MONITOR

Answer:

V$SHARED_SERVER_MONITOR

Explanation:

You should use the V$SHARED_SERVER_MONITOR view. This view contains all the information regarding the tuning of shared servers.

The V$SGA can also be used to gain information regarding the tuning of shared servers. However, this is not the best option. This view primarily contains the size-related information of the various components of the SGA.

The V$QUEUE view cannot be used to tune the shared server. It is used to gather information on the shared server message queues.

The V$SGASTAT view cannot be used to tune the shared server. It is used to gather statistical information on tuning the SGA.

The V$SHARED_SERVER view cannot be used to tune the shared server. It is used to gather general information regarding shared servers, such as the number of shared servers running at a particular time.

The V$SHARED_POOL_ADVICE view cannot be used to tune the shared server. It is used to gather information on sizing the shared pool by displaying information on the estimated parse time in the shared pool for different sizes of shared pools.

Performance Monitoring

Item: 1 (Ref:1Z0-042.13.4.3)

The users on your SALESDB are complaining of slow response to their queries. Using the SQL Tuning Advisor, you determine that the SQL statements are using the best optimization plan. Querying the dynamic views, you see that the number of reloads for the SQL statements is high, which can cause performance degradation.

Which component of the SGA should you resize to reduce the number of reloads of the SQL statements?

- java pool
- redo log buffer
- large pool
- shared pool
- program global area
- database buffer cache

Answer:

shared pool

Explanation:

To reduce the number of reloads of the SQL statements, you should resize the shared pool because the library cache component of the shared pool stores the parsed SQL statements. Insufficient size of the library cache leads to reloads of the SQL statements because the SQL statements are aged out sooner. To address this problem, you must increase the size of the shared pool. This will increase the size of the library cache and enable the library cache to store the parsed SQL statements for a longer period of time.

The java pool does not store the parsed query information. Allocating more space to this component will not solve the problem of the SQL statements being reloaded. The java pool stores the session-specific java code and data in the Java Virtual Machine (JVM).

The redo log buffer does not store the parsed query information. Allocating more space to this component will not solve the problem of the SQL statements being reloaded. The redo log buffer stores the redo data generated when a transaction modifies objects in a database. This data stored in the redo log buffer is used in recovery operations.

The large pool does not store the parsed query information. Allocating more space to this component will not solve the problem of SQL statements being reloaded. The large pool stores the Recovery Manager (RMAN)-related information and some part of the program global area when a shared server environment is used.

The program global area does not store the parsed query information. The program global area stores session-related information such as cursor state.

The database buffer cache does not store the parsed query information. The database buffer cache stores the data that is retrieved from the datafiles and being accessed and changed by different user processes.

Item: 2 (Ref:1Z0-042.13.3.2)

Steven is a newly hired DBA in his company. Steven is assigned the task of tuning the database after continued complaints from users about slow database performance. Being new to the organization, Steven does not know much about the database's past performance.

Which source will provide Steven with the necessary information to determine the past performance of the database and tune the database effectively?

- the alert log file
- the fixed tables
- the operating system log file
- the dynamic performance views
- baseline metrics from the previous instances

Answer:

baseline metrics from the previous instances

Explanation:

To obtain information regarding the past performance of the database, Steven can view the baseline metrics from the previous instances. The previous instances are the snapshots or values contained in the dynamic performance views. These baseline metrics are gathered and saved when the database is performing well. The baseline metrics can then be compared to metrics collected while the database is facing performance problems. Copies of the dynamic performance views should be maintained because the dynamic views are reset at each startup, and all the previous data contained in the dynamic views are erased. The **Metrics Details** page will also provide details on tuning the database efficiently.

The dynamic performance views from the current instance cannot be viewed to check the performance of earlier instances because these views are reset at each startup.

The alert log file cannot be used to view the previous database metrics. The alert log file contains detailed information on errors occurring in the Oracle database, administrative operations such as startup and shutdown, and deadlocks.

The operating system log file cannot be used to view the previous database metrics. The operating system log file will contain all the applications, security, and system-related errors.

The fixed tables cannot be used to view the previous database metrics. Fixed tables are the tables that contain information regarding the database, such as names and details of datafiles and tablespaces. Fixed tables are used to collect information regarding the physical and logical structure of the database.

Item: 3 (Ref:1Z0-042.13.2.2)

Due to some batch processes uploading data into your database tables, the table statistics change very often, which affects the performance of the database.

Which is the best option you can use to ensure that the statistics are collected and updated frequently?

- Use OS utilities to schedule jobs at regular intervals.
- Use an RMAN script to collect statistics on a regular basis.
- Use Oracle Scheduler to collect statistics at regular intervals.
- Use the **Gather Statistics** wizard to create a job that collects statistics at regular intervals.

Answer:

Use the Gather Statistics wizard to create a job that collects statistics at regular intervals.

Explanation:

The Enterprise Manager's **Gather Statistics** wizard can be used for this purpose. This wizard can be used to collect or update the optimizer statistics manually. This wizard will prompt for the required information and then create a job to collect statistics based on this information.

The option that states that you should use the OS utilities to schedule jobs at regular intervals is incorrect because statistics cannot be collected by using OS utilities.

You can use RMAN scripts to collect optimizer statistics but this is not the best option in this scenario. Collecting statistics by using RMAN will require the creation of scripts. However, the **Gather Statistics** wizard does not involve creation of such scripts.

You can use the Oracle Scheduler to collect statistics, but Oracle recommends the usage of the **Gather Statistics** wizard to collect or update optimizer statistics.

Item: 4 (Ref:1Z0-042.13.4.4)

The users on your database are complaining that the queries are taking longer to complete. While performing monitoring activities on your database, you view the Database Control **Performance** page. You notice that at regular time intervals, the session waiting and working count is significantly high for CPU usage.

Which is the best action to take to reduce the waiting and working count for CPU usage in the most cost-effective manner without hampering user connections?

- Identify the CPU-intensive SQL statements and tune them.
- Add more CPUs to your database server to reduce the session waiting time.
- Identify the user sessions running the CPU-intensive SQL statements and kill the sessions of these users.
- Notify the users to commit their transactions more often so the CPU resources are released to be used by other sessions.

Answer:

Identify the CPU-intensive SQL statements and tune them.

Explanation:

To reduce the session waiting and working count for CPU usage, you should identify the CPU-intensive SQL statements and tune them. This will reduce the use of the CPU resources. On the Database Control **Performance** page, you can view the session waiting and working counts for CPU usage, user I/O, system I/O, and other database performance statistics. The CPU usage working count indicates that the CPU usage of the database server is high.

Adding more CPUs to your database server can only solve the problem temporarily and adding CPUs is not a cost-effective solution. In this scenario, the CPU-intensive SQL statements are a major cause of the problem. This is not the best option because increasing the number of CPUs will not solve the problem permanently.

Identifying the user sessions running the CPU-intensive SQL statements and killing the sessions is incorrect because this will disconnect the users. In the given scenario, user connections should not to be affected.

Notifying the users to commit their transactions more often so that the CPU resources are released for use by other sessions is incorrect because committing more often will not solve the problem in this scenario. Committing transactions will only ensure that the CPU resources held by users are released from time to time. It will not address the SQL statements that are consuming higher amounts of CPU resources.

Item: 5 (Ref:1Z0-042.13.2.3)

The statistics of the EMPLOYEES table in your database are updated by calling the procedure for updating the statistics in a timely manner. You want to ensure that the statistics have been collected successfully when the procedure was called earlier.

Which two views can you use to ensure this? (Choose two.)

- DBA_TABLES
- DBA_OBJECTS
- DBA_STATISTICS
- DBA_OBJECT_TABLES
- DBA_TAB_HISTOGRAMS

Answer:

DBA_TABLES
DBA_OBJECT_TABLES

Explanation:

To ensure that the statistics for a particular table have been collected, you can use the DBA_TABLES and DBA_OBJECT_TABLES views. The DBA_TABLES view contains information on all tables in the database. The DBA_OBJECT_TABLES view contains information about all object tables in the database. In both of these views, you can use the AVG_ROW_LEN column to check the average row length, the LAST_ANALYZED column to check the last analyzed data, and the BLOCKS column to verify the size of the table.

The DBA_OBJECTS view cannot be used to view the information regarding collection of statistics for a table. The DBA_OBJECTS view is used to obtain information about individual database objects, such as each object's storage characteristics and size.

The DBA_STATISTICS view is not a valid Oracle view.

The DBA_TAB_HISTOGRAMS view cannot be used to view the information regarding collection of statistics for a table. The DBA_TAB_HISTOGRAMS view describes histograms on columns of all tables in the database.

Item: 6 (Ref:1Z0-042.13.2.1)

You have a table named PRODUCT in your database, MASTER. The users in your database have been complaining that the reports run on the PRODUCT table are taking more time because new data has been inserted into the table. After analysis, you realize that the statistics of the table were not refreshed after the new records were inserted.

Which two methods can you use to update the statistics for the table? (Choose two.)

- Execute the DBMS_STATS.GATHER_TABLE_STATS procedure.
- Issue the ANLAYZE statement to collect statistics for the table.
- Execute the DBMS_STATS.GATHER_SCHEMA_STATS procedure.
- Set the STATISTICS_LEVEL parameter to a value of ALWAYS. This will update the statistics each time a table is modified.
- Set the OPTIMIZER_MODE parameter to the value CHOOSE. This will automatically update the statistics for the modified tables.

Answer:

Execute the DBMS_STATS.GATHER_TABLE_STATS procedure.
Issue the ANLAYZE statement to collect statistics for the table.

Explanation:

To update the statistics for the PRODUCT table, you can execute the DBMS_STATS.GATHER_TABLE_STATS procedure or issue the ANALYZE statement with the COMPUTE STATISTICS option. The DBMS_STATS.GATHER_TABLE_STATS procedure gathers statistics for a table and the columns and indexes of the table. The following statement can be used to collect statistics for the MASTER table that belongs to the user ROGER:

```
EXEC DBMS_STATS.GATHER_TABLE_STATS('ROGER','MASTER');
```

The GATHER AUTO option in the DBMS_STATS.GATHER_TABLE_STATS can be used to instruct Oracle to automatically gather the necessary statistics. Oracle then determines the objects that do not have new statistics and how these statistics must be collected. The ANALYZE statement can also be used to collect statistics for a table. The COMPUTE STATISTICS clause in the statement specifies the exact statistics computed for a particular table. The following statement can be used to compute statistics for a table, MASTER:

```
ANALYZE TABLE MASTER COMPUTE STATISTICS;
```

You cannot use the DBMS_STATS.GATHER_SCHEMA_STATS procedure to update the statistics for a particular table. You can use this procedure to collect the statistics for a particular schema.

Setting the STATISTICS_LEVEL parameter to a value of ALWAYS will not update the statistics of the PRODUCT table. The STATISTICS_LEVEL parameter is used to specify the level of collection for database and operating system statistics.

Setting the OPTIMIZER_MODE parameter to a value of CHOOSE will not automatically collect the statistics for the table. It will only set the mode of optimizer to cost-based.

Item: 7 (Ref:1Z0-042.13.1.1)

While performing maintenance operations last week, you relocated some tables to another tablespace using ALTER TABLE...MOVE statements. The users on your database are complaining that some reports are taking longer to run since the relocation.

In this scenario, what is the possible reason for the performance degradation of the reports?

- The statistics collected for the tables being used by the reports have become invalid.
- The relocation of the tables being used by the reports has led to loss of data from the tables.
- The relocation of tables being used by the reports has dropped the indexes built on the tables.
- There is not enough space in the tablespace in which the tables being used by the reports exist.
- The tables being used by the reports have become fragmented.

Answer:

The statistics collected for the tables being used by the reports have become invalid.

Explanation:

In this scenario, the statistics collected for the table have become invalid. Relocation of a table using the ALTER TABLE...MOVE statement causes the current statistics for the table to become invalid. This leads to slow performance of the queries that are using these tables. New statistics should be collected for the tables in this scenario.

The option stating that the relocation of tables has led to loss of data from the tables is incorrect because the relocation of tables does not cause loss of data. If you lose data, the reports using the data will not run or will give erroneous output upon execution.

The option stating that the indexes have been dropped as a result of table relocation is incorrect because relocation of tables does not lead to indexes on the table being dropped.

The option stating that there is not enough space on the tablespace is incorrect because running reports on a particular table is not affected by the space in the tablespace that contains the table. If there is not enough space in the tablespace, the users inserting data or updating data in the table would receive an error stating that the tablespace does not have enough space.

The option stating that the tables have become fragmented is incorrect because relocation of tables decreases the table fragmentation.

Item: 8 (Ref:1Z0-042.13.4.5)

You have been experiencing I/O problems in your database recently that have degraded database performance.

Which component or feature can you use in the database to address such problems related to I/O?

- a standby database
- the SQL Tuning and Access Advisors
- a file system without RAID disk striping
- Automatic Storage Management (ASM)

Answer:

Automatic Storage Management (ASM)

Explanation:

To address I/O related problems in your database, you can use Automatic Storage Management (ASM) in your database. ASM can address I/O problems in the database by managing the datafiles. ASM automatically distributes datafiles across disks according to the I/O on the datafiles. When using ASM, you do not need to specify and manage file names in your databases because these files are automatically managed by ASM. ASM also provides features, such as disk mirroring, which is helpful in maintaining datafiles and reducing potential loss due to single point of failure.

A standby database cannot be used to address problems related to I/O. A standby database increases the availability of the database and can be activated when the primary database stops functioning.

The SQL Tuning and Access Advisors cannot be used to address problems related to I/O. The SQL Tuning Advisor analyzes each SQL statement and provides suggestions to improve its performance. The SQL Access Advisor also analyzes all SQL statements issued within a given period and recommends the creation of additional indexes to improve performance of the SQL statements.

A file system without Redundant Array of Inexpensive Disks (RAID) disk striping cannot be used to address problems related to I/O. You should instead use file a system with RAID disk striping to address problems related to database I/O. RAID provides fault tolerance and increased performance. RAID can improve performance by disk striping by distributing bytes or groups of bytes across multiple drives, so more than one disk is reading and writing simultaneously.

Item: 9 (Ref:1Z0-042.13.4.2)

On your SALESDB database, users are complaining of a slow response when accessing the database. Upon investigation, you find that the wait time for datafiles is significantly high.

Which is the best available option to reduce the contention on datafiles and improve the performance of the database?

- Place the heavily accessed datafiles on different disks.
- Consider reparsing the SQL statements that are a major cause of contention on the datafiles.
- Increase the number of DBW*n* processes so that it can write to the datafiles more effectively.
- Consider partitioning of heavily accessed tables and place them on different datafiles.
- Increase the size of the database buffer cache to enable it to accommodate more data blocks retrieved from the datafiles.

Answer:

Place the heavily accessed datafiles on different disks.

Explanation:

In this scenario, the best option to reduce contention on the datafiles is to place the heavily accessed datafiles on different disks. This will distribute the load across the disks and improve performance of the database.

Reparsing SQL statements that are a major cause of contention will improve the database performance to some extent, provided the statements can be parsed to generate better optimization plans. Reparsing will not improve the database performance if the SQL statements already follow the best optimization plan.

Increasing the number of DBW*n* processes will ensure that the database buffer cache is freed of the dirty buffers more often. However, increasing the number of DBW*n* processes will increase the contention on the datafiles because the data is written to the datafiles more often. Therefore, increasing the number of DBW*n* processes is not the correct option.

Partitioning heavily accessed tables will improve the performance of the queries that are using these tables. Partitioning will not reduce contention on the datafiles and therefore, not improve the performance of the database significantly.

Increasing the size of the database buffer cache will not reduce the contention on the datafiles. This will only accommodate more data blocks retrieved from the datafiles. As a result, increasing the size of the database buffer cache allows the blocks to remain in the database buffer cache for a longer time.

Item: 10 (Ref:1Z0-042.13.4.1)

The users in your database are complaining of slow response from the database. After analyzing the problem, you notice that the LGWR process has to wait for a redo log group frequently because a checkpoint has not been completed.

What should you do to overcome this problem?

- Add a new redo log group.
- Add new redo log members.
- Clear the current redo log group.
- Reduce the number of log members.
- Increase the size of the redo log buffer.

Answer:

Add a new redo log group.

Explanation:

You should add a new redo log group. The redo log files record all the changes made to data. In the event of a system or media failure, the redo log files provide a recovery mechanism. The recorded information includes transactions that have not yet been committed, undo segment information, and schema and object management statements. A redo log group is a set of identical copies of online redo log files. Each online redo log file in a group is a member. The Oracle server sequentially records database changes in the redo log buffer. The LGWR background process writes entries from the redo log buffer to the current online redo log group. The LGWR process writes the contents from the redo log buffer in the following circumstances:

- When a transaction commits
- When the redo log buffer becomes one-third full
- When there is more than one megabyte of changed records in the redo log buffer
- Before the DBW*n* process writes modified blocks in the database buffer cache to the datafiles

When a redo log group is full, a log switch occurs. During a log switch, the LGWR process moves to the next log group. At each log switch, a checkpoint occurs. At a checkpoint, the DBW*n* process writes the dirty database buffers covered by the log being checkpointed to the datafiles. When determining the best configuration for the redo logs, monitor the LGWR trace file and the alert log file. If they indicate that the LGWR process has to frequently wait for a redo log group because a checkpoint has not completed or the group has not been archived, you should add redo log groups.

Adding more redo log members to the database will not solve the problem. Adding more redo log members means maintaining multiple copies of the existing redo log members. This does not allow additional time to complete the checkpoint in the database.

Clearing the redo log groups will not solve the problem of waits on the redo log buffer because the redo generated should still be written to the redo log files.

Reducing the number of redo log members in the database will not solve the problem because the number of redo log members does not affect the time needed to complete the checkpoint or reduce the waits on the redo log buffer.

Increasing the size of the redo log buffer will not solve the problem because the larger size of redo log buffer will not affect the time required to complete a checkpoint. The size of the redo log buffer must be increased when majority of wait time is on the redo log buffer. Also, you must consider placing the redo log groups on different disks when there is high I/O on the redo log files which is degrading the performance of your database.

Item: 11 (Ref:1Z0-042.13.3.1)

Your database users are complaining of slow response to queries. You are trying to identify the component of Oracle that could be the reason for the problem.

Which view can you use to determine that the instance is not facing memory-related problems?

- V$SGA
- V$SESSION
- V$SYSSTAT
- V$ROLLSTAT
- V$FILESTAT
- DBA_SEGMENTS

Answer:

V$SYSSTAT

Explanation:

To locate information regarding memory-related problems in the database, you can use the V$SYSSTAT dynamic view. This view contains instance-wide information regarding rollback segments, datafile I/O, parse data, and so on.

The V$SGA view only contains information regarding the distribution of SGA memory into different SGA components.

The V$SESSION view displays session-specific information.

The V$ROLLSTAT view contains information specific to the rollback segments.

The V$FILESTAT view contains detailed I/O information specific to each datafile, including the number of I/Os on each file.

The DBA_SEGMENTS view is an incorrect option because it cannot be used to view performance-related problems in the database.

Proactive Maintenance

Item: 1 (Ref:1Z0-042.14.5.2)

In your production environment, you use the Automatic Workload Repository (AWR). The statistics are collected in your database every 15 minutes and are retained for a period of eight days. After optimizing the database performance, you notice that the database performance is being adversely affected by frequent collection of statistics. These statistics are consuming a lot of disk space.

You want to continue capturing the statistics you are currently capturing, but you want to ensure that statistics are retained for only three days and collected every hour.

Which two actions should you take to achieve this objective? (Choose two.)

- ☐ Set the collection level to `ALL`.
- ☐ Set the collection level to `TYPICAL`.
- ☐ Set the retention level to three days.
- ☐ Set the retention period to three days.
- ☐ Set the retention interval to three days.
- ☐ Set the collection period to 60 minutes.
- ☐ Set the collection interval to 15 minutes.
- ☐ Set the collection interval to 60 minutes.

Answer:

Set the retention period to three days.
Set the collection interval to 60 minutes.

Explanation:

In the given scenario, you should set the retention period to three days and the collection interval to 60 minutes. This will ensure that the statistics are collected every 60 minutes and retained for a period of three days. Retaining the statistics for three days will decrease the space required on disk for the statistics. Collecting the statistics every hour, instead of every 15 minutes, will improve the database performance. Retention period is specified in the AWR to determine the number of days for which the statistics need to be retained in the AWR. The collection interval specifies the time interval between the collection of statistics.

You should not set the collection level to `ALL`. You set the collection level in AWR to determine which statistics are to be collected. Setting the collection statistics to `ALL` will collect all statistics generated from the database.

You should not set the collection level to `TYPICAL`. You set the collection level in AWR to determine which statistics are to be collected. Setting the collection statistics to `TYPICAL` will collect a few important statistics generated from the database. These statistics are useful in doing certain monitoring activities.

You should not set the retention level to three days because retention level is not the correct parameter to set the number of days the statistics are to be maintained in the database. The retention level parameter is an invalid parameter and does not exist in the AWR.

You should not set the retention interval to three days because retention interval is not the correct parameter to be set for the number of days the statistics are to be maintained in the database. The retention interval parameter is an invalid parameter and does not exist in the AWR.

You should not set the collection period to 60 minutes because collection period is not the correct parameter to be set. The collection period parameter is an invalid parameter and does not exist in the AWR.

You should not set the collection interval to 15 minutes because the collection interval must be set to 60 minutes. Setting the collection interval to 15 minutes will collect the statistics every 15 minutes. The collection interval is already set to 15 minutes in this scenario.

Item: 2 (Ref:1Z0-042.14.5.3)

You have set the retention period for statistics in Automatic Workload Repository (AWR) to seven days. However, the statistics are occupying a lot of disk space, and you want to delete some statistics manually.

Which tool can you use to do this?

- Enterprise Manager
- the DBMS_METADATA package
- the ALTER DATABASE statement
- the DBMS_WORKLOAD_REPOSITORY package

Answer:

the DBMS_WORKLOAD_REPOSITORY package

Explanation:

The DBMS_WORKLOAD_REPOSITORY package can be used to manually delete the statistical data from the AWR. The DROP_SNAPSHOT_RANGE procedure in the package allows you to drop statistics contained in a snapshot range. You can also use the DROP_BASELINE procedure to drop the baselines in the AWR. The DBMS_WORKLOAD_REPOSITORY package can also be used to view the AWR statistics.

Enterprise Manager cannot be used to delete the AWR statistics manually. Enterprise Manager can be used to view the AWR statistics.

The DBMS_METADATA package cannot be used to delete the AWR statistics manually. This package is used to retrieve metadata from data dictionaries, such as DDL for certain objects created in the database.

The ALTER DATABASE statement cannot be used to delete the AWR statistics manually. This statement does not contain options to modify the AWR statistics. This statement is issued to add or drop a tablespace, change status of datafiles and makes other structural changes in the database.

Item: 3 (Ref:1Z0-042.14.4.1)

The users on your database are complaining of slow response to their queries. You are using the Automatic Database Diagnostic Monitor (ADDM) to monitor the database. The ADDM discovers that the log files in your database are small.

Which other problems can the ADDM detect? (Choose all that apply.)

- ☐ lock contention
- ☐ missing offline datafiles
- ☐ tablespace fragmentation
- ☐ high checkpoint load cause
- ☐ high PL/SQL and Java execution time
- ☐ contention on the undo tablespace

Answer:

lock contention
high checkpoint load cause
high PL/SQL and Java execution time

Explanation:

The ADDM can detect the following common problems that arise in the database:

- lock contention
- high checkpoint load cause
- high PL/SQL and Java execution time
- CPU bottlenecks
- improper Oracle Net connection management
- I/O capacity
- space allocation problems in Oracle memory structures
- high load SQL statements

The ADDM runs automatically after each Automatic Workload Repository (AWR) snapshot, and the results of each ADDM analysis are stored in the AWR.

ADDM cannot be used to detect missing offline datafiles. This problem is detected by Oracle when you try to change the status of the datafiles from offline to online.

ADDM cannot be used to detect tablespace fragmentation. This problem is detected by the Segment Advisor.

ADDM cannot be used to detect contention on the undo tablespace. This problem is detected by the Undo Advisor.

Item: 4 (Ref:1Z0-042.14.2.2)

You have created a baseline metric for Monday's CPU utilization on your database. You want to use this baseline metric to compare today's performance with that of Monday's performance.

What should you do to achieve this objective?

- Create a function to compare today's performance with the baseline created for Monday's performance.
- Use Monday's baseline metrics for CPU utilization to define a threshold value for CPU utilization in the **Manage Metrics** page.
- Create a baseline for today's performance and compare it with the baseline that was created for Monday's performance, by using the **Manage Metrics** page.
- Create and save today's baseline in the **Manage Metrics** page. The Oracle server will compare the two values and generate an alert when today's performance deviates from Monday's performance.

Answer:

Use Monday's baseline metrics for CPU utilization to define a threshold value for CPU utilization in the Manage Metrics page.

Explanation:

To compare today's performance with Monday's performance, you should use Monday's baseline metrics for CPU utilization to define a threshold value for CPU utilization in the **Manage Metrics** page. An alert will be generated whenever the CPU utilization exceeds this value.

The option to create a function to compare today's performance with the baseline created for Monday's performance is incorrect because you cannot use a function to compare the values of the two days.

The option to create a baseline for today's performance and compare it with the baseline that was created for Monday's performance using the **Manage Metrics** page is incorrect because you cannot use the **Manage Metrics** page to compare the baseline metrics of the two days.

The option stating that the Oracle server will compare the two values and generate an alert when today's performance deviates from Monday's performance is incorrect because Oracle cannot compare the two values until you have set a threshold value. After specifying a threshold value, Oracle will compare this baseline value with the current performance.

Item: 5 (Ref:1Z0-042.14.3.3)

In which scenario will the Memory Advisor prove to be helpful?

- Lock contention issues arise frequently in your database.
- The undo tablespace needs to be sized for large transactions.
- The SQL statements must be tuned and the related initialization parameters changed for optimal performance.
- The SQL statements are running slowly, and you suspect lack of space in library cache to be the cause.

Answer:

The SQL statements are running slowly, and you suspect lack of space in library cache to be the cause.

Explanation:

The Memory Advisor might prove helpful if SQL statements are running slowly and you suspect lack of space in library cache to be the cause. The Memory Advisor is used to size the memory-related components in Oracle architecture. It can be used to size the database buffer cache, shared pool, program global area, and other memory components. In the given scenario, it is suspected that the library cache located in the shared pool must be resized. You can get advice on tuning the shared pool using the Memory Advisor.

The Memory Advisor cannot be used to address problems relating to lock contention. Lock contention is handled by using a less restrictive locking mechanism. Automatic Database Diagnostic Monitor (ADDM) can be used to gather information on the lock contention arising in a database.

The Memory Advisor cannot be used to gather information to size the undo tablespace for large transactions. The Undo Advisor must be used to gather information if the undo tablespace needs to be sized for the large transactions.

The Memory Advisor cannot be used to gather information to modify parameters related to poorly performing SQL statements. The SQL Tuning Advisor and SQL Access Advisor should be used if the SQL statements need to be tuned. The related initialization parameters must also be changed to ensure optimal performance.

Item: 6 (Ref:1Z0-042.14.4.2)

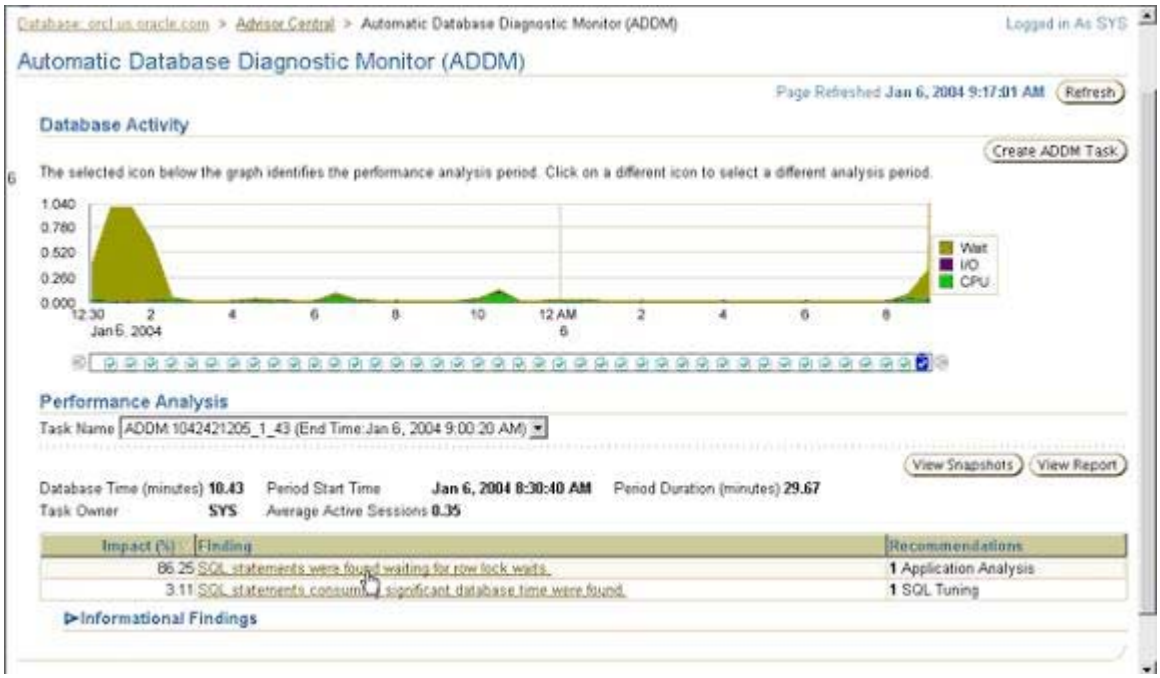
Click the Exhibit(s) button to examine the exhibit and analyze the Automatic Database Diagnostic Monitor (ADDM) findings.

Considering the ADDM findings, which statement is true?

- The rows have been locked because of an improper locking mechanism.
- There were no significant operations in the database to be analyzed by the ADDM.
- The major wait time on the database is due to a SQL statement consuming significant database time.
- The overall database performance has been affected because of poorly performing SQL statements.
- The database performance can be significantly improved by tuning the SQL statements that are causing the problem.

Answer:

The rows have been locked because of an improper locking mechanism.



Explanation:

Analysis of the ADDM findings reflects that the rows have been locked. The **Impact(%)** and **Finding** columns in the exhibit show the major wait time of 86.25 percent applies to SQL statements waiting for row lock waits. This degrades the database performance because more time is spent on waits due to locked rows. The database performance can be improved by performing application analysis, which involves checking for an improper locking mechanism. An improper locking mechanism indicates that unnecessary high levels of locking have been used, and the problem can be addressed by using a less restrictive locking mechanism.

The option that states that there were no significant operations in the database to be analyzed by the ADDM is incorrect because if there are no database operations to be analyzed by the ADDM, the following message will be displayed in the **Informational Findings** section:

```
There was no significant database activity to run the ADDM.
```

The major wait time is not due to a SQL statement consuming significant database time. The major wait time is due to row locks as shown by the **Impact(%)** and **Finding** columns in the exhibit.

The overall database performance has not been affected because of the poorly performing SQL statements. It can be deduced from the ADDM findings that the database performance has been affected by the poorly performing SQL statements only between 12:30 and 2:30.

The database performance cannot be significantly improved by tuning the SQL statements causing the problem. Considering the ADDM findings, SQL tuning will not boost performance. In this scenario, the major wait time in the database is due to row locks, and the performance will only be improved if you analyze the application for row locks.

Item: 7 (Ref:1Z0-042.14.1.1)

As a DBA, you have been using the table-monitoring features to track the transactions in a table. You now want to disable the table-monitoring feature.

What should you do?

- Do nothing. You cannot disable table-monitoring.
- Specify ALL as the value in the STATISTICS_LEVEL parameter.
- Specify BASIC as the value in the STATISTICS_LEVEL parameter.
- Specify TYPICAL as the value in the STATISTICS_LEVEL parameter.

Answer:

Specify BASIC as the value in the STATISTICS_LEVEL parameter.

Explanation:

You disable the table-monitoring feature by assigning the value BASIC to the STATISTICS_LEVEL parameter. The table-monitoring feature tracks the approximate number of inserts, updates, and deletes for a particular table, since the last time table statistics were gathered. When the STATISTICS_LEVEL parameter is set to BASIC, the collection of most of the important statistics required by Oracle Database features and utilities such as ADDM, AWR snapshots, Buffer Cache Advisory, MTTR Advisor, and server-generated alerts are disabled. Therefore, these features cannot be used if the STATISTICS_LEVEL parameter is set to BASIC.

The option to do nothing is incorrect because you can disable the table monitoring feature.

The table-monitoring feature is enabled when you set the STATISTICS_LEVEL parameter to ALL. When the STATISTICS_LEVEL parameter is set to ALL, all statistics provided by the TYPICAL setting of the STATISTICS_LEVEL parameter will be collected. Additionally, timed OS statistics and execution plan statistics are collected.

The table-monitoring feature is enabled when you set the STATISTICS_LEVEL parameter to TYPICAL. When the STATISTICS_LEVEL parameter is set to TYPICAL, all major statistics required for database self-management functions are collected. The TYPICAL setting provides best overall performance of the database.

Item: 8 (Ref:1Z0-042.14.2.3)

While optimizing your database server performance, you determine that there are a high number of baselines created for different times in the past. You decide to delete the baselines that are not required.

What should you do to achieve the objective?

- Delete the baselines using the Enterprise Manager.
- Use the DBMS_WORKLOAD_REPOSITORY.DROP_BASELINE procedure to delete the baselines.
- Set the maximum retention time for the baselines, after which they will be automatically deleted.
- To automatically delete the baselines, disable the baselines using the Database Control Home page.

Answer:

Use the DBMS_WORKLOAD_REPOSITORY.DROP_BASELINE procedure to delete the baselines.

Explanation:

To manually delete the baselines, you should use the DBMS_WORKLOAD_REPOSITORY.DROP_BASELINE procedure. The DROP_BASELINE procedure in the DBMS_WORKLOAD_RESPOSITORY package is used to drop baselines created in the database. The following is an example of deleting a baseline named my_baseline using the DROP_BASELINE procedure:

```
SQL> EXECUTE DBMS_WORKLOAD_REPOSITORY.DROP_BASELINE (
baseline_name => 'my_baseline');
```

You cannot delete the baselines using Enterprise Manager. Enterprise Manager is a graphical tool provided by Oracle to monitor and manage your database environment.

You cannot automatically delete baselines by setting the maximum retention time for the baselines. A retention time can be set for statistics collected by the Automatic Workload Repository (AWR), but they cannot be set for the baselines created.

You cannot delete the baselines by disabling them using the Database Control Home page. When a baseline is disabled, it is not currently being used by the database. However, the baseline will still be retained in the AWR until you delete it explicitly using the DBMS_WORKLOAD_REPOSITORY.DROP_BASELINE procedure.

Item: 9 (Ref:1Z0-042.14.1.2)

You specify 30 percent as the warning threshold for a user's tablespace usage metric. As a result, several alerts are raised on the Database Control Home page. After observing this, you decide to increase the warning threshold and clear all old alerts related to tablespace usage metrics.

Which view would you query to display the threshold settings defined for the instance?

- V$METRIC
- DBA_THRESHOLDS
- DBA_ALERT_HISTORY
- DBA_OUTSTANDING_ALERTS

Answer:

DBA_THRESHOLDS

Explanation:

The DBA_THRESHOLDS dictionary view displays the threshold settings defined for an instance. This view consists of columns that denote the warning and critical thresholds, WARNING_VALUE and CRITICAL_VALUE, set for the different database metrics and the objects on which the thresholds have been set. The OBJECT_TYPE column specifies the objects, such as SYSTEM, SERVICE, TABLESPACE, and FILE, on which the thresholds have been set. Additionally, the METRICS_NAME column specifies the name of the metrics for which the thresholds have been set.

The V$METRIC dictionary view displays the system-level metric values in memory.

The DBA_ALERT_HISTORY dictionary view displays the history of the cleared alerts.

The DBA_OUTSTANDING_ALERTS dictionary view displays the outstanding alerts in the database.

Item: 10 (Ref:1Z0-042.14.5.1)

You are working in your test environment on a new application designed by the application developers in your company. You must perform SQL tuning on this application before placing it in the production environment. You are using Automatic Workload Repository (AWR) to gather recommendations to assist in SQL tuning.

In the given scenario, which setting should you modify in the AWR?

- Set the collection level to `ALL`.
- Set the collection level to `DML`.
- Set the collection level to `BASIC`.
- Set the collection level to `TYPICAL`.

Answer:

Set the collection level to `ALL`.

Explanation:

In the given scenario, you should set the collection level for AWR to `ALL`. This will generate SQL execution plans and other statistics, which will make additional recommendations for tuning the SQL statements. Generating more recommendations on tuning SQL statements will help improve the tuning of the application's SQL statements.

The option to set the collection level to `DML` is incorrect because `DML` is not a valid value for the collection level.

The option to set the collection level to `BASIC` is incorrect because setting the collection level to `BASIC` will disable most of the Automatic Database Diagnostic Monitor (ADDM) functionality and will not provide any information or recommendations on SQL tuning.

The option to set the collection level to `TYPICAL` is incorrect because setting the collection level to `TYPICAL` will not generate additional recommendations for tuning the SQL statements in your application. This level is recommended when you have already tuned your application and do not need additional recommendations to tune the SQL statements in your application.

Item: 11 (Ref:1Z0-042.14.3.1)

Todd is the database administrator for Telstar. He discovers that the database is running out of space and therefore, starts maintenance activities. Todd needs to identify the tables in the database that have unused space in them.

Which component or feature would help Todd identify these tables?

- Memory Advisor
- Segment Advisor
- Undo Advisor
- Automatic Workload Repository
- SQL Tuning and Access Advisors

Answer:

Segment Advisor

Explanation:

The Segment Advisor can be used to identify space and space fragmentation issues in objects such as tables, indexes, segments, and tablespaces. The Segment Advisor can be used to analyze whether or not an object can be shrunk to reduce space consumption. The Segment Advisor can be invoked at the segment, tablespace, and object levels.

The Memory Advisor is used to determine the best settings for SGA components, such as the shared pool, java pool, and database buffer cache.

The Undo Advisor is used to provide information for proper sizing of the undo tablespace.

The SQL Tuning and Access Advisors are used to provide information on tuning of poorly performing queries.

The Automatic Workload Repository is used to collect and store snapshots of statistical information about various components of the database. The Segment Advisor uses information stored in the Automatic Workload Repository.

Item: 12 (Ref:1Z0-042.14.3.2)

In which scenario would you NOT use the SQL Tuning and SQL Access Advisors?

- The SQL statements have some common errors.
- The SQL statements are performing poorly due to lack of indexes.
- The SQL-related initialization parameters in the parameter file must be modified for optimal performance.
- The indexes used in the database have become fragmented, and the queries using these indexes are performing poorly.

Answer:

The indexes used in the database have become fragmented, and the queries using these indexes are performing poorly.

Explanation:

You would NOT use the SQL Tuning and SQL Access Advisors when the indexes have become fragmented and the queries using these indexes are performing poorly. Neither the SQL Tuning Advisor nor the SQL Access Advisor can advise on space fragmentation-related issues. To gather advice regarding space fragmentation, you must use the Segment Advisor. The SQL Tuning Advisor analyzes each SQL statement and gives suggestions to improve its performance. The SQL Access Advisor analyzes all SQL statements issued within a given period and recommends the creation of additional indexes to improve performance of the SQL statements.

You would use the SQL Tuning and SQL Access Advisors when the SQL statements have some common errors. You can detect common errors in SQL statement constructions by using the SQL Tuning Advisor and SQL Access Advisor.

You would use the SQL Tuning and SQL Access Advisors when the SQL statements are performing poorly due to lack of indexes. You can detect lack of indexes by using the SQL Tuning Advisor and SQL Access Advisor.

You would use the SQL Tuning and SQL Access Advisors when the SQL-related initialization parameters in the parameter file must be modified for optimal performance. The SQL Tuning Advisor and SQL Access Advisor can be used to provide suggestions regarding SQL-related initialization parameters that can be modified to achieve optimal performance.

Item: 13 (Ref:1Z0-042.14.2.1)

TelStar Corporation has hired Tom as a new database administrator. Tom is not familiar with this database's performance issues. Users on the database are complaining about the degraded performance of the database.

In this scenario, which information could Tom use to identify the problem areas in the database?

- a copy of dynamic views, starting from the time the database performance was considered acceptable
- database baseline metrics, starting from the time the database performance was considered acceptable
- the hit ratios of all the SGA components in the database, starting from the time the database performance was considered acceptable
- the statistics of the database, such as disk I/O, file I/O, free space, and used space in the tablespaces, and number of users, starting from the time the database performance was considered acceptable

Answer:

database baseline metrics, starting from the time the database performance was considered acceptable

---

Explanation:

Tom could use database baseline metrics, starting from the time the database performance was considered acceptable, to identify the problem areas in the database. Tom can use these database metrics to gather information about the database performance in the past. These metrics can also be compared to the present database metrics to identify problem areas.

The copy of dynamic views from the past will not help to identify the problem areas in the database. The dynamic performance views can be used to view information about the current status of the database because these views are reset at database startup.

The hit ratios of all the SGA components from the past will not help to identify the problem areas in the database. Hit ratios are only a measure of the performance of the database. Therefore, hit ratios from the past cannot be used to diagnose problems in the database.

The disk I/O statistics and other related information from the past cannot be used to identify the problem areas because there is no easy means to compare these statistics to the new statistics without using baselines.

Undo Management

Item: 1 (Ref:1Z0-042.15.6.1)

Your PROD database is using Automatic Undo Management. The following information is available to determine the appropriate size for the undo tablespace in your database:

Undo retention (UR) in seconds
Undo per second (UPS)
Database block size (DB_BLOCK_SIZE)

Which formula should you use to calculate the appropriate size of the undo tablespace in your database?

- (UR* UPS * DB_BLOCK_SIZE) MB
- (UR* UPS * DB_BLOCK_SIZE) KB
- (UR* UPS * 60 * DB_BLOCK_SIZE) MB
- (UR* UPS * 3600)/ DB_BLOCK_SIZE KB
- (UR* UPS * DB_BLOCK_SIZE *1024) MB

Answer:

(UR* UPS * DB_BLOCK_SIZE) KB

Explanation:

To calculate the appropriate size of the undo tablespace, you must use the following formula:

```
Number of undo blocks = (UR* UPS * DB_BLOCK_SIZE) KB
```

Consider an example where you have set the undo retention for your database to 1 hour. The undo per second is 100 blocks, and the database block size is 4 KB. The undo tablespace size would be calculated using the given formula as:

```
Number of undo blocks = (1*3600*100*4 KB) = 1440000 KB
```

In this example, the undo retention is one hour, but must be converted into seconds. Therefore, the undo retention is multiplied by 3600 to perform the conversion.

All of the other options are incorrect because they do not correctly calculate the appropriate size of the undo tablespace.

Item: 2 (Ref:1Z0-042.15.4.1)

You are working on your PROD database. You must configure this database to use the Oracle Flashback Query and Flashback Table features.

Which advisor or component should you use to gather recommendations for configuring these two features successfully for your database?

- Undo Advisor
- MTTR Advisor
- Memory Advisor
- Automatic Workload Repository
- Automatic Database Diagnostic Monitor

Answer:

Undo Advisor

Explanation:

To configure your database to use the Oracle Flashback Query and Flashback Table features, you should use the Undo Advisor to gather recommendations for the configuration. The Undo Advisor will provide recommendations for sizing the undo tablespace and undo retention period. This will help you configure the Oracle Flashback Query and Flashback features. The Oracle Flashback Query and Oracle Flashback Table features require the undo data stored in the undo tablespace to produce an image of an object at a prior point-in-time. Oracle Flashback will work only if undo data from the prior point-in-time is still present in the undo tablespace. If the undo data has been overwritten, Flashback will not be able to generate a prior image of the object or the query that was used to make changes to the object. For example, to flash back a table as it existed five hours ago, you must have the undo data for the last five hours.

The MTTR Advisor cannot be used to gather recommendations for configuring the Oracle Flashback Query and Flashback Table features in your database. The MTTR Advisor helps you set the time required for a database to recover from an instance crash. This time is referred to as Mean-Time-To-Recover (MTTR).

The Memory Advisor cannot be used to gather recommendations for configuring the Oracle Flashback Query and Flashback Table features in your database. The Memory Advisor helps you size the memory structures, such as the shared pool, the program global area, and the database buffer cache, in your database.

The Automatic Workload Repository (AWR) cannot be used to gather recommendations for configuring the Oracle Flashback Query and Flashback Table features in your database. This repository is used to gather and store performance information about the database. It collects all the information but does not generate any recommendations on the functioning of the database.

The Automatic Database Diagnostic Monitor (ADDM) cannot be used to gather recommendations for configuring the Oracle Flashback Query and Flashback Table features in your database. This tool is used to gather recommendations on common problems faced while managing a database. The problems detected by the ADDM include lock contention, CPU bottlenecks, high load SQL statements, I/O capacity, and other performance-related issues.

Item: 3 (Ref:1Z0-042.15.2.3)

You are using Automatic Undo Management in your database. The name of the undo tablespace in your database is UNDOTS. You want to ensure that no committed undo data is overwritten for 15 minutes.

Which two actions must you take to achieve this? (Choose two.)

- Set the UNDO_RETENTION parameter to 0.
- Set the UNDO_RETENTION parameter to 15.
- Set the UNDO_RETENTION parameter to 900.
- Run the ALTER TABLESPACE UNDOTS RETENTION GUARANTEE; statement.
- Run the ALTER TABLESPACE UNDOTS RETENTION NOGUARANTEE; statement.
- Run the ALTER TABLESPACE UNDOTS RETENTION GUARANTEE=TRUE; statement.
- Run the ALTER TABLESPACE UNDOTS RETENTION NOGUARANTEE=TRUE; statement.

Answer:

Set the UNDO_RETENTION parameter to 900.

Run the ALTER TABLESPACE UNDOTS RETENTION GUARANTEE; statement.

Explanation:

In this scenario, you must set the UNDO_RETENTION parameter to 900 and run the ALTER TABLESPACE UNDOTS RETENTION GUARANTEE; statement. This will retain the committed undo data for 15 minutes and guarantee undo. The UNDO_RETENTION parameter sets the time, in seconds, for which the undo data is to be retained. Running the ALTER TABLESPACE statement with the GUARANTEE clause ensures that undo is guaranteed. When undo is guaranteed for an undo tablespace in a database, the committed undo data from transactions will not be overwritten for the time specified in the UNDO_RETENTION parameter. This is true even if there are other transactions in the database that need space in the undo tablespace to store undo data.

Setting the UNDO_RETENTION parameter to 0 is incorrect because to retain the committed undo data for 15 minutes you must set the UNDO_RETENTION parameter to 900. This parameter value is specified in seconds. Setting the UNDO_RETENTION parameter to 0 indicates automatic undo retention mode.

Setting the UNDO_RETENTION parameter to 15 is incorrect because to retain the committed undo data for 15 minutes, you must convert the minutes to seconds because the parameter accepts a value in seconds. Therefore, to retain the undo data for 15 minutes you must set the UNDO_RETENTION parameter to 900.

Running the ALTER TABLESPACE UNDOTS RETENTION NOGUARANTEE; statement is incorrect because this will not guarantee that the committed undo data is retained for 15 minutes. When undo is not guaranteed, the committed undo data will be overwritten if any ongoing transactions require space in the undo tablespace.

Running the ALTER TABLESPACE UNDOTS RETENTION GUARANTEE=TRUE; statement is incorrect because the syntax of the statement is incorrect. When the statement is run, it will generate an error.

Running the ALTER TABLESPACE UNDOTS RETENTION NOGUARANTEE=TRUE; statement is incorrect because the syntax of the statement is incorrect. When the statement is issued, it will generate an error.

Item: 4 (Ref:1Z0-042.15.1.1)

You are using the CREATE DATABASE statement to create a database for your production environment. You include the following parameters in your initialization parameter file:

```
UNDO_RETENTION=120
UNDO_MANAGEMENT=AUTO
```

What will be the impact of using these parameters?

- Oracle will automatically create an undo tablespace because you have enabled Automatic Undo Management.
- The undo data will be stored in the SYSTEM tablespace because no undo tablespace is specified in the parameter file.
- You will have to create an undo tablespace in the database because no undo tablespace is specified in the parameter file.
- The CREATE DATABASE statement will generate an error stating that you must specify the undo tablespace if Automatic Undo Management is enabled.

Answer:

Oracle will automatically create an undo tablespace because you have enabled Automatic Undo Management.

Explanation:

In this scenario, Oracle will automatically create an undo tablespace because you have enabled Automatic Undo Management. The UNDO_MANAGEMENT parameter in the database specifies how undo will be managed in the database. Setting this parameter to AUTO specifies that undo data will be automatically managed by Oracle. Setting this to MANUAL specifies that undo data will be managed by the DBA. When using Automatic Undo Management, the UNDO_TABLESPACE parameter specifies the undo tablespace for the database. If you set the UNDO_MANAGEMENT=AUTO parameter in your initialization parameter file and do not set the UNDO_TABLESPACE parameter, Oracle will automatically create an undo tablespace and assign it a system-generated name, SYS_UNDOTS. If you set the UNDO_TABLESPACE parameter to the name of an undo tablespace, it will create an undo tablespace with the name specified in this parameter.

Undo data will not be stored in the SYSTEM tablespace because Oracle will automatically create an undo tablespace if the UNDO_MANAGEMENT parameter is set to AUTO, even if the UNDO_TABLESPACE parameter is not specified.

You will not have to create an undo tablespace in the database because a default undo tablespace will be automatically created by Oracle if Automatic Undo Management is enabled.

The CREATE DATABASE statement will not generate an error. The undo tablespace will be created by Oracle because Automatic Undo Management is enabled. The reason for this is if you have enabled Automatic Undo Management and do not specify the undo tablespace for the database at database creation time, Oracle will create an undo tablespace with a system-generated name.

Item: 5 (Ref:1Z0-042.15.2.2)

User A in your database has a long-running transaction that has resulted in read consistency problems. You must address this problem without affecting the other user connections. The UNDO_RETENTION parameter in your database is set to the value 600.

Which action can you use to achieve this objective?

- Run the ALTER SYSTEM SET UNDO_RETENTION=1000; statement.
- Run the ALTER DATABASE SET UNDO_RETENTION=1000; statement.
- Run the ALTER SESSION SET UNDO_RETENTION=1000; statement in user A's session.
- Shut down the database and change the UNDO_RETENTION parameter to a higher value in the initialization parameter file. Then, restart the database.

Answer:

Run the ALTER SYSTEM SET UNDO_RETENTION=1000; statement.

Explanation:

To avoid read consistency issues in user A's session, you can run the ALTER SYSTEM SET UNDO_RETENTION=1000; statement. This will increase the value of the UNDO_RETENTION parameter and reduce the read consistency problems in user A's session. Increasing the value of UNDO_RETENTION will retain the committed undo data in the undo tablespace, which will address the read consistency problems in this scenario. Read consistency problems occur when the undo data is overwritten due to lack of enough space in the undo tablespace. Increasing the UNDO_RETENTION will increase the time for which the undo data is retained in the undo tablespace.

The option that states to run the ALTER DATABASE SET UNDO_RETENTION=1000; statement is incorrect because you cannot use the ALTER DATABASE statement to increase the value of the UNDO_RETENTION parameter.

The option that states to run the ALTER SESSION SET UNDO_RETENTION=1000; statement in the user's session is incorrect because you cannot use the ALTER SESSION statement to increase the value of the UNDO_RETENTION parameter.

The option that states to shut down the database and change the UNDO_RETENTION parameter to a higher value in the parameter file is incorrect because in this scenario you must ensure that the connected users are not affected. Therefore, you cannot use this option because it requires shutting down the database.

Item: 6 (Ref:1Z0-042.15.1.2)

The following error is often generated in your development database:

ORA-1555: Snapshot too old

You investigate and notice that there are some long-running transactions in the database when the error is generated and that the UNDO_RETENTION initialization parameter has been set to 0.

Which two actions could you take to overcome this problem? (Choose two.)

- Increase the size of the SYSTEM tablespace.
- Increase the value of the UNDO_RETENTION initialization parameter.
- Increase the size of the undo tablespace in your database.
- Configure manual undo management mode for the undo tablespace.
- Create a new undo tablespace and assign it to the database users who have long-running transactions.

Answer:

Increase the value of the UNDO_RETENTION initialization parameter.

Increase the size of the undo tablespace in your database.

Explanation:

In this scenario, you could increase the value of the UNDO_RETENTION initialization parameter or increase the size of the undo tablespace in your database. The ORA-1555 error is generated in long-running transactions when the before image of the object it is modifying is not available in the undo tablespace. The UNDO_RETENTION parameter specifies the time, in seconds, after which the undo data is considered to be expired and can be overwritten. Setting the UNDO_RETENTION parameter to 0 indicates automatic undo retention mode. To avoid the ORA-1555 error in long-running transactions, you should increase the value of the UNDO_RETENTION parameter so that the undo data generated from the committed transactions is retained longer Transactions that take a long time to complete do not generate the ORA-1555 error. If you increase the size of the undo tablespace in your database, you ensure that more space is available for transactions.

Increasing the size of the SYSTEM tablespace is incorrect. Increasing the size of the SYSTEM tablespace does not reduce the occurrence of the ORA-1555 error because the undo data is not stored in the SYSTEM tablespace.

Configuring manual undo management mode for the undo tablespace is incorrect. The manual undo management mode is configured to manage the undo data manually. If you configure manual undo management, you must manage the undo data manually, which increases the administrative overhead. With manual undo management you need to create the undo tablespace and the undo segments on your own, and also manage the space allocation for these.

Creating a new undo tablespace and assigning it to the database users is incorrect because only one undo tablespace can remain active in the database at any particular time.

Item: 7 (Ref:1Z0-042.15.2.1)

You must retain the committed undo data in the undo tablespace for 10 minutes without hampering the uncommitted transactions in the database.

Which action can you take to achieve this objective?

- Set the `UNDO_RETENTION` parameter to `10` and guarantee the undo retention.
- Set the `UNDO_RETENTION` parameter to `600` and guarantee the undo retention.
- Set the `UNDO_RETENTION` parameter to `10` and do not guarantee the undo retention.
- Set the `UNDO_RETENTION` parameter to `600` and do not guarantee the undo retention.

Answer:

Set the `UNDO_RETENTION` parameter to `600` and do not guarantee the undo retention.

Explanation:

To set undo retention for 10 minutes, you must set the `UNDO_RETENTION` parameter to `600`. The `UNDO_RETENTION` parameter specifies the time, in seconds, after which the undo data is considered to be expired and can be overwritten. If you do not want to hamper the uncommitted transactions in the database, you should not guarantee undo retention on your database. If undo retention is guaranteed, the committed undo data will be retained in the database only if the current uncommitted transactions are not hampered. If undo retention is not guaranteed, the committed undo data will be overwritten if other uncommitted transactions need space in the undo tablespace to write the undo data. You can use the `ALTER TABLESPACE...RETENTION NOGUARANTEE` statement to ensure that undo retention is not guaranteed in your database.

Setting the `UNDO_RETENTION` parameter to `10` and guaranteeing the undo retention is incorrect because this will set the undo retention value to 10 seconds. In this scenario, you want to set this value to 10 minutes. You should not guarantee undo retention because this can cause the uncommitted transactions to fail due to lack of enough space in the undo tablespace.

Setting the `UNDO_RETENTION` parameter to `600` and guaranteeing the undo retention is incorrect because you should not guarantee undo retention. If undo retention is guaranteed, the committed data will remain in the undo tablespace, and the uncommitted transactions can fail due to lack of space.

Setting the `UNDO_RETENTION` parameter to `10` and not guaranteeing the undo retention is incorrect because this will set the undo retention value to 10 seconds instead of the desired 10 minutes.

Item: 8 (Ref:1Z0-042.15.5.1)

Click the Exhibit(s) button to view the records in the EMPLOYEES table.

You are running your database in the ARCHIVELOG mode.

Which three statements, when issued against the EMPLOYEES table, will NOT generate any undo data? (Choose three.)

- [ ] TRUNCATE TABLE EMPLOYEES;
- [ ] DELETE FROM EMPLOYEES;
- [ ] INSERT INTO EMPLOYEES(7531, 'WILLIAM',2500,20);
- [ ] ALTER TABLE EMPLOYEES ADD(LAST_NAME VARCHAR2(8));
- [ ] UPDATE EMPLOYEES SET SALARY=10000 WHERE EMPLOYEE_ID=7796;
- [ ] SELECT EMPLOYEE_ID, SALARY FROM EMPLOYEES WHERE DEPARTMENT_ID=20;

Answer:

TRUNCATE TABLE EMPLOYEES;
ALTER TABLE EMPLOYEES ADD(LAST_NAME VARCHAR2(8));
SELECT EMPLOYEE_ID, SALARY FROM EMPLOYEES WHERE DEPARTMENT_ID=20;

EMPLOYEES

EMPLOYEE_ID	FIRST_NAME	SALARY	DEPARTMENT_ID
7184	Adam	4200	50
7185	Eve	4100	50
7186	John	3400	50
7187	Eric	3000	50
7188	Mark	3800	50
7189	Joel	3600	50
7290	Timothy	2900	50
7191	Ronald	2500	50
7782	Scott	4000	50
7193	Brian	3900	50
7194	Samuel	3200	50
7195	Victor	2800	50
7796	Alan	3100	50
7197	Kevin	3000	50
7198	Donald	2600	50
7199	Dustin	2600	50
7200	Jason	4400	10
7201	Michael	13000	20
7202	Paul	6000	20
7203	Shawn	6500	40
7204	Henry	10000	70
7205	Seth	12000	110

Explanation:

The TRUNCATE TABLE, ALTER TABLE, and SELECT statements will not generate any undo data. The TRUNCATE TABLE and ALTER TABLE statements are DDL statements. DDL statements are statements that cannot be rolled back. Therefore, no undo data is generated when they are executed. The SELECT statement is only used to view the data in the table and does not modify any data. Therefore, the SELECT statement does not generate any undo data.

The DELETE statement will generate undo data. The DELETE statement is a DML statement and can be rolled back in a transaction. To support this rollback operation, the undo data is generated and stored in the undo tablespace. Of the given statements, the DELETE statement will produce more undo than any other statement because when you issue a DELETE statement to delete all the existing rows in the table, the undo data generated will contain the complete data in the table. Any other DML statement issued to change the existing data in the table will not generate as much undo data.

The INSERT statement will generate undo data. The INSERT statement is a DML statement and can be rolled back in a transaction. To support this rollback operation, the undo data is generated and stored in the undo tablespace.

The UPDATE statement will generate undo data. The UPDATE statement is a DML statement that can be rolled back in a transaction. To support this rollback operation, the undo data is generated and stored in the undo tablespace.

Item: 9 (Ref:1Z0-042.15.5.2)

Your database is configured for using Automatic Undo Management. Which two actions will enable read consistency for long-running transactions in your database? (Choose two.)

- ☐ increasing the undo retention period
- ☐ decreasing the undo retention period
- ☐ increasing the size of the undo tablespace
- ☐ increasing the size of the SYSTEM tablespace
- ☐ increasing the size of the database buffer cache
- ☐ increasing the number of redo log files in your database
- ☐ increasing the size and number of undo segments in your database

Answer:

increasing the undo retention period
increasing the size of the undo tablespace

Explanation:

The read consistency for long-running transactions will be enabled by increasing the undo retention period and by increasing the size of the undo tablespace. Increasing the undo retention period for your database will enable the before image of the table to be stored in the undo tablespace for a longer period of time. This will enable read consistency for the transactions involving this data. Increasing the size of the undo tablespace will have the same impact on the transactions because more space will be available to hold undo data.

Decreasing the undo retention period will not enable read consistency for long-running transactions. Decreasing the undo retention period will instead hamper the read consistency of long-running transactions because the before images of tables involved in transactions will be retained in the undo tablespace for a shorter period of time.

Increasing the size of the SYSTEM tablespace will not in any way impact the read consistency of long-running transactions. The reason for this is that SYSTEM tablespace does not store any undo data in this scenario because Automatic Undo Management is being used. When Automatic Undo Management is used, Oracle will create an undo tablespace if one does not exist and therefore the SYSTEM tablespace will not store any undo data. The SYSTEM tablespace stores the undo data when no undo tablespace exists in the database.

Increasing the size of the database buffer cache will not impact the read consistency of long-running transactions. Read consistency for long-running transactions is enabled by increasing the time for which the undo data for these transactions is stored in the undo tablespace. The database buffer cache is a component of SGA that stores the data blocks that are currently being accessed by the user transactions. Whenever a SQL query requests data from a datafile, the data is retrieved from the datafile and stored in the database buffer cache where users make changes to the data blocks. The database buffer cache does not store any undo-related information.

Increasing the number of redo log files in your database will not enable read consistency for long-running transactions because the undo data for transactions is not stored in the redo log files. It is stored in the undo tablespace when Automatic Undo Management is used.

Increasing the size and number of undo segments in your database in this scenario is incorrect because the number of undo segments in the database is managed by the Oracle server when the database is configured for Automatic Undo Management.

Item: 10 (Ref:1Z0-042.15.3.1)

You are using Automatic Undo Management in your database. You have enabled the guarantee option of undo retention by running the following statement:

```
SQL> ALTER TABLESPACE UNDOTS RETENTION GUARANTEE;
```

Which two statements are true about the guarantee option of undo retention? (Choose two.)

- Using the guarantee option of undo retention guarantees undo retention for all the tablespaces in the database.
- Using the guarantee option of undo retention can lead to failure of some transactions.
- You use Enterprise Manager to determine if retention guarantee is enabled for a tablespace.
- Using the guarantee option of undo retention causes the committed undo data to be overwritten by undo data from uncommitted transactions if space is needed in the undo tablespace.
- Using the guarantee option of undo retention causes the committed undo data to be retained for the time specified by the `UNDO_RETENTION` parameter, even if other transactions require space in the undo tablespace.

Answer:

Using the guarantee option of undo retention can lead to failure of some transactions.

Using the guarantee option of undo retention causes the committed undo data to be retained for the time specified by the `UNDO_RETENTION` parameter, even if other transactions require space in the undo tablespace.

Explanation:

Using the guarantee option of undo retention can lead to failure of some transactions in the database. Enabling the guarantee option of undo retention in the database retains the undo data from committed transactions in the undo tablespace even if there are other transactions that require space in the undo tablespace. This may cause other transactions to fail for lack of space in the undo tablespace. In addition, the committed undo data is retained for the time specified by the `UNDO_RETENTION` parameter. If you guarantee undo retention in the undo tablespace, the undo data will be retained in the tablespace for the time specified by the `UNDO_RETENTION` parameter.

Using the guarantee option of undo retention does not guarantee undo retention for all the tablespaces in the database. You can specify undo retention for only the undo tablespace in the database.

You do not use Enterprise Manager to determine if retention guarantee is enabled for a tablespace. This information can be determined by using the `DBA_TABLESPACES` view. The `RETENTION` column indicates whether or not undo retention is guaranteed for the tablespace. The possible values contained in this column are `GUARANTEE`, `NOGUARANTEE`, and `NOT APPLY`.

Using the guarantee option of undo retention does not cause the committed undo data to be overwritten by undo data from uncommitted transactions. Using the guarantee option of undo retention prevents the committed undo data from being overwritten by the uncommitted undo data.

Item: 11 (Ref:1Z0-042.15.6.2)

John is a database administrator in his company. John is administering the MASTER_DETAILS database. This database is configured for Automatic Undo Management. The EMP table in the MASTER_DETAILS database was modified at 1:00 P.M. to disable the PRIMARY KEY constraint on the table. The table was modified again at 2:00 P.M. the same day to delete some rows of the table.

John notices the deletion of these rows at 6:00 P.M., and he must recover the deleted rows.

In this scenario, which condition will enable John to successfully recover the deleted rows using the Flashback Table feature?

- The UNDO_RETENTION parameter is set to 0.
- The UNDO_RETENTION parameter is set to 4.
- The UNDO_RETENTION parameter is set to 5.
- The UNDO_RETENTION parameter is set to 14400.

Answer:

The UNDO_RETENTION parameter is set to 14400.

Explanation:

To recover the table by using the Flashback Table feature, the UNDO_RETENTION parameter in the database should be set to 14400. In this scenario, you need to flash back the table that was modified four hours ago. The Flashback Table feature can recover the table only if the committed undo data up to the point the table was modified is available in the undo tablespace. The time in hours must be converted to seconds because the UNDO_RETENTION parameter is specified in seconds. Therefore, the UNDO_RETENTION parameter must be set to a value of 14400, which is equal to four hours.

Setting the UNDO_RETENTION parameter to 0 will not retain any committed data, and you will not be able to recover the table using the Flashback Table feature.

Setting the UNDO_RETENTION parameter to 4 is incorrect because the value must be specified in seconds. You must convert 4 hours to 14400 seconds.

Setting the UNDO_RETENTION parameter to 5 is incorrect because the value of the UNDO_RETENTION parameter is specified in seconds. This would retain committed data for only five seconds, and you would not be able to recover the table using the Flashback Table feature.

Item: 12 (Ref:1Z0-042.15.5.3)

Click the Exhibit(s) button to view a set of statements run by two users in the same session starting at SCN number 78.

Which component of the Oracle architecture guarantees that the transactions of user A do not interfere with the transactions of user B?

- redo data stored in the redo log buffer
- undo data stored in the undo segments
- redo data stored in the online redo log files
- flashback data stored in the flashback tables
- temporary data stored in the temporary tablespace of the database

Answer:

undo data stored in the undo segments

```
USER A:                          USER B:

SQL> SELECT * FROM EMP;          SQL> SELECT * FROM EMP;
SQL> DELETE FROM EMP;            SQL> UPDATE EMP SET SALARY=25000 WHERE
SQL> COMMIT;                          MANAGER_ID=7189;
                                 SQL> SELECT SALARY FROM EMP WHERE
                                      MANAGER_ID=7169;
```

Explanation:

The undo data stored in the undo segments guarantees that the transactions of users do not interfere with each other. The undo data of each user issuing a DML statement is maintained in the undo segments. This undo data contains the before image of the data blocks that the user is trying to modify. The before image of the data supports read consistency for each user. In the given scenario, when user A issues the `DELETE FROM EMP;` statement, undo data is generated that contains the image of the table as it existed before issuing the `DELETE` statement. Any other user who is trying to view or modify the table uses this image of the table. Similarly, when user B issues the `UPDATE` statement, undo data is generated that contains the image of the table as it existed before issuing the `UPDATE` statement. The users will be able to see the changes made by other user transaction only after the transaction is committed or rolled back. The undo segments are held in the undo tablespace when Automatic Undo Management is enabled or in the `SYSTEM` tablespace if no undo tablespace is present in the database.

The redo data stored in the redo log buffer does not guarantee read consistency of transactions. The redo data is required for both instance and media recovery purposes.

The redo data stored in the online redo log files does not guarantee read consistency of transactions. This redo data is required for both instance and media recovery purposes.

The data stored in the flashback tables does not guarantee read consistency of transactions. This data is required to recover a table up to a particular point in time.

The data stored in the temporary tablespace does not guarantee read consistency of transactions. This data is required when a user is running a statement that must sort data.

Monitoring and Resolving Lock Conflicts

Item: 1 (Ref:1Z0-042.16.1.2)

You issue the following statement to modify the EMPLOYEE_ID column in the EMPLOYEES table of your database:

```
SQL> SELECT * FROM EMPLOYEES WHERE EMPLOYEE_ID > 2536 FOR UPDATE;
```

The user ADAM is accessing the EMPLOYEES table. He issues the following statement to update a column of the EMPLOYEES table:

```
SQL> UPDATE EMPLOYEES SET SALARY=5300 WHERE EMPLOYEE_ID=2600;
```

What is the result of the statement issued by the user ADAM?

- The statement causes ADAM's user session to terminate.
- The statement causes ADAM's session to stop responding.
- The statement causes ADAM's transaction to roll back.
- The statement returns an error stating that the resource is busy.
- The statement updates the SALARY column for EMPLOYEE_ID 2600 to 5300.

Answer:

The statement causes ADAM's session to stop responding.

Explanation:

The UPDATE EMPLOYEES SET SALARY=5300 WHERE EMPLOYEE_ID=2600; statement issued by the user ADAM causes ADAM's session to stop responding. The reason for this is that the row that ADAM is trying to update is locked by the SELECT FOR UPDATE statement that you issued. The SELECT FOR UPDATE statement places an EXCLUSIVE lock on the affected rows, which does not allow read or write operations on the selected rows until the lock is released. Any session trying to access the locked data for write operations will not respond until the lock is released. The session will stop responding while waiting for the locks to be released.

The statement does not cause ADAM's session to terminate. The session terminates if the DBA issues an ALTER USER KILL SESSION statement.

The statement does not cause ADAM's transaction to roll back. A user's transaction is rolled back only when a deadlock arises between the transactions of different users, the user issues a ROLLBACK to roll back the transaction, or the user disconnects abruptly.

The statement does not return an error stating that the resource is busy. Such an error is generated when the NOWAIT option is specified in a LOCK TABLE statement. The NOWAIT clause of the LOCK TABLE statement specifies that the statement should not wait for existing locks to be released before locking the table. If the statement is issued and locks are currently held on the table, then the error received would be:

ORA-00054: resource busy and acquire with NOWAIT specified

The statement does not update the SALARY column for EMPLOYEE_ID 2600 to 5300. Your SELECT FOR UPDATE statement locks the row corresponding to the EMPLOYEE_ID 2600. As a result, ADAM cannot modify the table until your locks are released.

Item: 2 (Ref:1Z0-042.16.3.1)

You are a DBA in a company. A user of your company's database, KATE, issues the following statements in her session:

```
SQL> UPDATE EMP SET SALARY=5000 WHERE EMPLOYEE_ID=5647;

SQL> DELETE FROM EMP WHERE EMPLOYEE_ID=6785;
```

Which two transactions are permitted for the user AMY on the EMP table, provided the user KATE has not committed her transactions? (Choose two.)

- AMY can execute a full table scan on the EMP table.
- AMY can delete the row corresponding to EMPLOYEE_ID 5647.
- AMY can drop the EMP table if she has the DROP ANY TABLE privilege.
- AMY can create a B-tree index on the DEPARTMENT_ID column of the EMP table.
- AMY can only query the information in the rows of the EMP table until KATE commits her transactions.
- AMY can modify the row corresponding to EMPLOYEE_ID 6785 for all the columns except the SALARY column.
- AMY can modify information in all the rows except the rows corresponding to EMPLOYEE_IDs 5647 and 6785.

Answer:

AMY can execute a full table scan on the EMP table.

AMY can modify information in all the rows except the rows corresponding to EMPLOYEE_IDs 5647 and 6785.

Explanation:

AMY can execute a full table scan on the EMP table, and AMY can modify the information in all the rows except the rows corresponding to EMPLOYEE_IDs 5647 and 6785. In this scenario, the user KATE issues statements to update and delete rows corresponding to EMPLOYEE_IDs 5647 and 6785, respectively. This results in a ROW EXCLUSIVE lock on the two rows. This lock allows the other users to query the data in the table. However, this lock prohibits the modification of the locked rows until the locks are released. As a result, AMY can execute a full table scan on the EMP table and can modify all the rows except the rows locked by KATE's transactions.

AMY cannot delete the row corresponding to EMPLOYEE_ID 5647 because the row is exclusively locked by KATE. Therefore, no other transactions can modify this row until the lock held by KATE is released.

AMY cannot drop the EMP table even if she has the DROP ANY TABLE privilege because the UPDATE statement is a DML statement. Each DML statement acquires a share table level lock for the table being modified. The share table level lock prevents the table from being dropped until the lock is released.

AMY cannot create a B-tree index on the DEPARTMENT_ID column of the EMP table. The UPDATE statement issued by KATE is a DML statement. Each DML statement acquires a ROW EXCLUSIVE lock for the rows being updated. This lock prohibits the creation of an index on the table containing the locked rows.

The option that states that AMY can only query the information in the rows of the EMP table until KATE commits her transactions is incorrect because AMY can perform other functions in addition to querying. AMY can modify or delete information in all the rows except the rows that KATE currently has locked, namely the rows corresponding to EMPLOYEE_IDs 5647 and 6785.

AMY cannot modify the row corresponding to EMPLOYEE_ID 6785 for all the columns except the SALARY column. In this scenario, the entire row is locked by KATE, and no updates to the any of the columns can be performed until the locks held by KATE are released.

Item: 3 (Ref:1Z0-042.16.1.4)

The user AMY is required to modify the EMP table. Therefore, she places a share mode lock on the table by using the following statement:

```
SQL> LOCK TABLE EMP IN SHARE MODE NOWAIT;
```

What is the result of running this statement?

- The user session stops responding if the EMP table is already locked by another user session.
- The user session places the lock on the EMP table immediately even if other locks are held on the table.
- The user session waits for 300 seconds before placing the lock if any other lock is held on the EMP table.
- The user session receives an error and the control returns to the user session if the EMP table is already locked by another session.

Answer:

The user session receives an error and the control returns to the user session if the EMP table is already locked by another session.

Explanation:

With the given statement, the user session receives an error and the control returns to the user session if the EMP table is already locked by another session. The NOWAIT option, available with the statements that lock a table, instructs the user session not to wait to place a lock if the specified table is already locked by another session. If a lock is already held, the following error message is returned and control immediately returns to the user session:

ORA-00054: resource busy and acquire with NOWAIT specified

The user session does not stop responding if the EMP table is already locked by another user session. The session will stop responding if the NOWAIT clause is not specified in the SQL statement. In this scenario, the session will wait to acquire the lock.

The user session does not immediately place the lock on the EMP table even if other locks are held on the table. The user session cannot place the lock on the table until the other locks on the table are released.

The user session does not wait for 300 seconds before placing the lock if any other lock is held on the EMP table. The session will wait for 300 seconds if the WAIT 300 clause, instead of the NOWAIT clause, is specified in the SQL statement.

Item: 4 (Ref:1Z0-042.16.1.1)

The users of the database in your company are complaining that they are not able to access the data in the MASTER table of the database. Upon investigation, you discover that the table has been locked by the user JOHN.

What should you do to make the data available to the other users?

- Use the ALTER USER statement to time out JOHN's session.
- Use the ALTER SESSION KILL statement to kill JOHN's session.
- Use the ALTER SESSION statement to release the locks held by JOHN.
- Use the ALTER SYSTEM KILL SESSION statement to kill JOHN's session.

Answer:

Use the ALTER SYSTEM KILL SESSION statement to kill JOHN's session.

Explanation:

To release the locks held by the user JOHN, you should kill the session by using the ALTER SYSTEM KILL SESSION statement. Killing the session rolls back the user's transactions and releases all the locks held by the user. This will make the data available to the other users.

The option to use the ALTER USER statement to time out JOHN's session is incorrect because the session cannot be timed out using the ALTER USER statement. A user's session is timed out when the user exceeds the time for which he can remain connected to the database. The time for which a user can remain connected to the database is specified by the CONNECT_TIME parameter specified in the user's profile.

The option to use the ALTER SESSION KILL statement to kill JOHN's session is incorrect because the KILL clause is not valid with the ALTER SESSION statement. The ALTER SESSION KILL statement will generate an error. The ALTER SESSION statement changes the configuration settings for a particular user session.

The option to use the ALTER SESSION statement to release the locks held by JOHN is incorrect. The locks held by the user are released only when the user issues a ROLLBACK or COMMIT, the user's session is ended, or you kill the user session using the ALTER SYSTEM KILL SESSION statement.

Item: 5 (Ref:1Z0-042.16.1.3)

The user KAREN issues the following statement in her session:

```
SQL> SELECT * FROM MASTER WHERE MAST_ID=896 FOR UPDATE;
```

After running this statement, which two locks are placed on the MAST_ID table? (Choose two.)

- an EXCLUSIVE lock on the table
- a ROW SHARE table lock on the table
- a ROW EXCLUSIVE lock on the row being updated
- a ROW EXCLUSIVE lock on all the rows in the table
- a ROW EXCLUSIVE table lock on the table being updated

Answer:

a ROW SHARE table lock on the table

a ROW EXCLUSIVE lock on the row being updated

Explanation:

The SELECT...FOR UPDATE statement places a ROW SHARE (RS) table lock on the table being updated and a ROW EXCLUSIVE (RX) lock on the rows being updated. A ROW SHARE (RS) lock indicates that a transaction has locked rows in a table and intends to update them. This lock is placed on a table when a user issues the SELECT FOR UPDATE statement or the LOCK TABLE...IN ROW SHARE MODE statement.

An EXCLUSIVE lock is not placed on the table. This lock is held only when the table is locked in the EXCLUSIVE mode.

A ROW EXCLUSIVE lock is not placed on all the rows in the table. This lock is held only when all the rows in the table have been locked for modification.

A ROW EXCLUSIVE table lock is not placed on the table being updated. This lock is held on the table being updated by using the INSERT, UPDATE, and DELETE statements.

Item: 6 (Ref:1Z0-042.16.4.1)

You issue the following statement in your Oracle 10*g* database to lock the MASTER table of the database in the ROW SHARE mode:

```
SQL> LOCK TABLE MASTER IN SHARE ROW EXCLUSIVE MODE;
```

What is the impact of this statement on the other users who might be trying to access the MASTER table? (Choose two.)

- The other users are not allowed to lock the table in the SHARE mode.
- The other users are allowed to lock the table only in the ROW SHARE mode.
- The other users are allowed to lock the table only in the ROW EXCLUSIVE mode.
- The other users are allowed to access the table only to query the data contained in the table.
- The other users are allowed to access the table to query and update the rows contained in the table.

Answer:

The other users are not allowed to lock the table in the SHARE mode.

The other users are allowed to access the table only to query the data contained in the table.

Explanation:

With the given statement, the other users are not allowed to lock the table in the SHARE mode, and the other users are allowed to access the table only to query the data contained in the table. The SHARE ROW EXCLUSIVE lock allows other users to query the rows in the table and does not allow the rows in the table to be modified by any other user.

The other users are not allowed to lock the table only in the ROW SHARE mode because the SHARE ROW EXCLUSIVE lock mode does not allow any other locks to be placed on the table.

The other users are not allowed to lock the table in the ROW EXCLUSIVE mode because the SHARE ROW EXCLUSIVE lock mode does not allow any other locks to be placed on the table.

The other users are not allowed to access the table to query and update the rows contained in the table because locking a table in the ROW EXCLUSIVE mode locks all the data in the table. Therefore, no other transactions can modify this data. You can only access the table to view the locked data.

Item: 7 (Ref:1Z0-042.16.2.1)

Click the Exhibit(s) button to view the statements simultaneously issued by two users:

Which of these statements is true of these two transactions?

- The transactions of users A and B roll back because a deadlock occurs in the two transactions.
- The Oracle server automatically resolves the deadlock and rolls back the statement that detects the deadlock.
- The Oracle server automatically resolves the deadlock and rolls back the transaction that detects the deadlock.
- The DBA must kill one of the user sessions to release the locks held by that user and allow the other user session to proceed.

Answer:

The Oracle server automatically resolves the deadlock and rolls back the statement that detects the deadlock.

```
USER A:                              USER B:

SQL> UPDATE PROD SET PROD_NAME=      SQL> UPDATE PROD SET PROD_RATE=67980
     'RT001' WHERE PROD_ID=1001;          WHERE PROD_ID=2009;
SQL> UPDATE PROD SET PROD_NAME=      SQL> UPDATE PROD SET PROD_RATE=67980
     'RT001' WHERE PROD_ID=2009;          WHERE PROD_ID=1001;
```

Explanation:

In this scenario, the Oracle server automatically resolves the deadlock and rolls back the statement that detects the deadlock. The deadlock arises because the two user processes are waiting for the data that has been locked by each other. The Oracle server automatically resolves such deadlocks. The Oracle server enables the user processes to proceed further by rolling back the statement that detects the deadlock.

The transactions of users A and B do not roll back because a deadlock occurs in the two transactions. Oracle rolls back only the statement that detects the deadlock.

The Oracle server automatically resolves the deadlock but does not roll back the transaction that detects the deadlock. Only the statement that detects the deadlock is rolled back. The entire transaction is not rolled back.

The option stating that the DBA must kill one of the user sessions to release the locks held by the user so that the other user session can proceed is incorrect. The Oracle server resolves a deadlock automatically. No action is required on the DBA's part to resolve it.

Backup and Recovery Concepts

Item: 1 (Ref:1Z0-042.17.5.3)

The database is running in the NOARCHIVELOG mode. You shut down the database, open the database in the MOUNT state, and alter the database to the ARCHIVELOG mode by issuing the following statement:

```
SQL> ALTER DATABASE ARCHIVELOG;
```

After opening the database, which dynamic view will you use to determine if the archive mode of the database has been altered successfully?

- V$LOG
- V$VERSION
- V$INSTANCE
- V$DATABASE
- V$PARAMETER

Answer:

V$DATABASE

Explanation:

To view the archiving mode enabled for the database, you can use the V$DATABASE view. The LOG_MODE column of the V$DATABASE view indicates whether the ARCHIVELOG or NOARCHIVELOG mode is enabled for the database. The ARCHIVE LOG LIST command from the SQL prompt also shows which archiving mode is enabled for the database.

The V$LOG view does not display the archiving mode for the database. The V$LOG view displays information regarding the redo log files in your database.

The V$VERSION view does not display the archiving mode for the database. The V$VERSION view displays information regarding the database version installed on an Oracle server.

The V$INSTANCE view does not display the archiving mode for the database. The V$INSTANCE view displays the state of the current instance.

The V$PARAMETER view does not display the archiving mode for the database. The V$PARAMETER view displays information about the initialization parameters that are in effect for the current instance.

Item: 2 (Ref:1Z0-042.17.1.2)

You are running your database in the ARCHIVELOG mode. Last time you could not shut down your database properly because of a power failure.

You issue the STARTUP command to start the database. The STARTUP command performs an instance recovery.

Which two statements correctly describe the tasks performed by the instance recovery process in this scenario? (Choose two.)

- The redo data from the online redo log is applied to roll forward the committed changes.
- The undo data from the undo segments is applied to roll forward the committed changes.
- The undo data from the undo segments is applied to roll back the uncommitted changes.
- The redo data from the online redo logs is applied to roll back the uncommitted changes.
- The redo data from the archived redo log files is applied to roll forward the committed changes.

Answer:

The redo data from the online redo log is applied to roll forward the committed changes.
The undo data from the undo segments is applied to roll back the uncommitted changes.

Explanation:

During instance recovery, the redo data from the online redo log is applied to roll forward the committed changes, and the undo data from the undo segments is applied to roll back the uncommitted changes. An instance recovery synchronizes the datafiles and control files in the database. To roll forward the committed and uncommitted changes and synchronize the datafiles and control files, the redo data from the online redo log files is applied to the affected data blocks. After this, the undo data from the undo segments is applied to the affected data blocks to roll back the uncommitted changes.

The option stating that the undo data from the undo segments is applied to roll forward the committed changes is incorrect because the undo data from the undo segments can only roll back the uncommitted changes.

The option stating that the redo data from the online redo logs is applied to roll back the uncommitted changes is incorrect because the redo data from the online redo logs can only roll forward the committed changes in the database.

The option stating that the redo data from the archived redo log files is applied to roll forward the committed changes is incorrect because the archived redo log files do not affect instance recovery.

Item: 3 (Ref:1Z0-042.17.1.1)

The database users in your company are not trained adequately and are likely to make mistakes. To manage this, you have configured the database in the ARCHIVELOG mode.

What are three other advantages of running the database in the ARCHIVELOG mode? (Choose three.)

- reduced MTTR for the database
- increased availability of the database
- minimum downtime of the database in case of media failure
- ability to back up the database when the database is in the OPEN state
- ability to recover the database up to a particular point in time before an error event

Answer:

increased availability of the database
ability to back up the database when the database is in the OPEN state
ability to recover the database up to a particular point in time before an error event

---

Explanation:

Other advantages of running the database in the ARCHIVELOG mode include increased availability of the database, ability to back up the database when the database is in the OPEN state, and ability to recover the database up to a particular point in time before an error event. The ARCHIVELOG mode facilitates the recovery of the database from user errors. The ARCHIVELOG mode archives the redo log files before they are overwritten. These archived files enable the recovery of the database up to a particular point in time before an error event. Configuring a database in the ARCHIVELOG mode also enables you to create a backup of the database when the database is open. When the database is in the ARCHIVELOG mode, you can place the tablespaces in the database in backup mode and back up the datafiles in the tablespace, followed by a backup of log file generated during the backup procedure. This can be accomplished only when the database is in the ARCHIVELOG mode and cannot be done when the database is running in the NOARCHIVELOG mode. Being able to back up an open database increases the availability of the database. The availability of the database can also be increased by configuring a standby database that is activated when the primary database is down.

Configuring the database in the ARCHIVELOG mode cannot reduce the MTTR for the database. The MTTR is reduced by tuning the checkpoint process.

Running a database in the ARCHIVELOG mode does not minimize downtime of the database in case of media failure. In case of media failure, the database downtime depends on the time required to replace the failed media or to perform a database recovery. To minimize the database downtime, you can configure a standby database that is activated when the primary database is down.

Item: 4 (Ref:1Z0-042.17.2.1)

User A has locked some tables in the database. As a result, other users in the database are not able to access the data in the locked tables. To solve the problem, you kill user A's session.

Which two statements are true in this scenario? (Choose two.)

- The RECO process will perform a recovery of user A's transaction.
- The PMON process will perform a recovery of user A's transaction.
- The SMON process will perform a recovery of user A's transaction.
- The PMON process will release the locks held by user A's transaction.
- The database buffer cache will contain the data blocks that were requested by the killed user process.

Answer:

The PMON process will perform a recovery of user A's transaction.

The PMON process will release the locks held by user A's transaction.

Explanation:

When a user process is killed by the DBA, the PMON process recovers the user's transaction. The PMON process will release all the locks and resources held by the user's session. It will also clean up the database buffer cache removing the data blocks that were requested by the killed user process.

The option stating that the RECO process will perform a recovery of user A's transaction is incorrect because this task is performed by the PMON process. The RECO process is used in the distributed database configuration and will automatically resolve failures related to distributed transactions.

The option stating that the SMON process will perform a recovery of user A's transaction is incorrect because this task is performed by the PMON process. The SMON process performs instance recovery of the database after an instance crash.

The option stating that the database buffer cache will contain the data blocks that were requested by the killed user process is incorrect. The PMON process will clean up all the data blocks from the database buffer cache that were requested by the failed user process.

Item: 5 (Ref:1Z0-042.17.5.5)

You have changed your database to run in the ARCHIVELOG mode. After changing the archive mode, you want to specify the destination at which the archive log files must be stored.

Which initialization parameter is used to specify the location at which the archive log files of the database will be stored?

- LOG_ARCHIVE_DEST_*n*
- ARCHIVE_LOG_DEST_*n*
- LOG_ARCHIVE_FORMAT
- DB_CREATE_FILE_DEST
- DB_RECOVERY_FILE_DEST
- DB_CREATE_ONLINE_LOG_DEST

Answer:

LOG_ARCHIVE_DEST_*n*

Explanation:

The LOG_ARCHIVE_DEST_*n* parameter is used to specify the location at which the archive log files of the database will be stored. You can specify up to ten different destinations for the archive logs by using this parameter. The value of *n* can range between 1 and 10. When these parameters are used to specify archive log destinations for a standby database, they can be local or remote.

The location for the archive log files is not specified by using the ARCHIVE_LOG_DEST_*n* parameter. The ARCHIVE_LOG_DEST_*n* parameter is an invalid parameter that does not exist in Oracle.

The location for the archive log files is not specified by using the LOG_ARCHIVE_FORMAT parameter. The LOG_ARCHIVE_FORMAT parameter specifies the default file name format for the archive log files in the database.

The location for the archive log files is not specified by using the DB_CREATE_FILE_DEST parameter. The DB_CREATE_FILE_DEST parameter specifies the default location for datafiles in the database when using Oracle-Managed Files. This parameter also specifies the location for the control files and online redo log files of the database, if the DB_CREATE_ONLINE_LOG_DEST parameter is not set.

The location for the archive log files is not specified by using the DB_RECOVERY_FILE_DEST parameter. The DB_RECOVERY_FILE_DEST parameter specifies the default location for the flash recovery area.

The location for the archive log files is not specified by using the DB_CREATE_ONLINE_LOG_DEST parameter. The DB_CREATE_ONLINE_LOG_DEST parameter specifies the default locations for the control files and the online redo log files in a database, when you use Oracle-Managed Files.

The location for the archive log files is not specified by using the DB_ARCHIVE_MIN_SUCCEED_DEST parameter. The DB_ARCHIVE_MIN_SUCCEED_DEST parameter specifies the minimum number of archive log destinations on which archiving should be successful before the online redo log file is available for reuse.

Item: 6 (Ref:1Z0-042.17.6.1)

In your production database environment, you want the database to be configured for easy and effective recoverability from database failures.

What should be done to achieve this requirement? (Choose two.)

- [ ] Make regular backups of the database.
- [ ] Maintain a backup of the online redo log files.
- [ ] Configure the database to run in the ARCHIVELOG mode.
- [ ] Configure the database to run in the NOARCHIVELOG mode.
- [ ] Use large redo log files to keep track of all database changes.

Answer:

Make regular backups of the database.
Configure the database to run in the ARCHIVELOG mode.

Explanation:

To configure a database for easy and effective recoverability, you should make regular backups of the database and configure the database to run in the ARCHIVELOG mode. Making regular backups of a database ensures that the database can be recovered from failures. When you configure a database to run in the ARCHIVELOG mode, the changes made to the database that are stored in the redo log files are archived before these log files are overwritten. These archives are maintained in the form of archive log files. Whenever there is a database failure, these archive redo log files can be applied to the most recent backup to bring the database back to the point of the last commit. If the database is not configured for ARCHIVELOG mode, the database can only be recovered up to the last complete backup.

Maintaining a backup of the online redo log files does configure the database for easy and effective recoverability. However, Oracle suggests that you not back up the online redo log files.

If you configure your database to run in the NOARCHIVLEOG mode, recovery will not be easy and effective because with every recovery you can recover your database only up to the last full backup. When you run the database in the NOARCHIVLEOG mode, the online redo log files are not archived before being overwritten. Due to this, the database can be recovered only up to the point of last complete backup. The NOARCHIVELOG mode makes the recovery procedure easy because you only need to restore the backup of the database, but the recovery is not effective because any changes made to the database after the last complete backup cannot be recovered and must be reapplied.

Using large redo log files does not ease recoverability of a database. Using large redo log files will only increase the time between two log switches.

Item: 7 (Ref:1Z0-042.17.4.2)

A database is running in the ARCHIVELOG mode. A database user dropped the MASTER table that was created at log sequence 30. The dropped MASTER table must be recovered. The user had dropped the table at log sequence 52, and the current log sequence is 54.

You discover that the dropped MASTER table was present in the USERS tablespace that consists of the DA2.DBF datafile. You also discover that the archived log file corresponding to the log sequence 50 is missing.

Which method should you employ to recover the MASTER table?

- Shut down the database and perform a complete recovery up to log sequence 53.
- Shut down the database and perform a time-based recovery up to log sequence 49.
- Shut down the database and perform a cancel-based recovery up to log sequence 49.
- Shut down the database and perform a cancel-based recovery up to log sequence 51.
- Take the USERS tablespace offline and recover only the DA2.DBF datafile after restoring it from the latest backup.
- The dropped MASTER table cannot be recovered.

Answer:

Shut down the database and perform a cancel-based recovery up to log sequence 49.

Explanation:

To recover the table in this scenario, you should perform a cancel-based recovery up to log sequence 49. This will recover the table to the state at which it existed at log sequence 49. Although the table was dropped at log sequence 52, the table cannot be recovered up to that point because the archived log file with log sequence 50 is not available. If all the archived log files existed up to log sequence 52, recovering the table would have been possible. In a cancel-based recovery, you recover the database up to a prior SCN. This creates a new incarnation of the database at that particular point in time.

The option to shut down the database and perform a complete recovery up to log sequence 53 is incorrect because performing a complete recovery will not recover the table. A complete recovery is performed when you restore datafiles or control files from a backup and then apply the archived redo logs to ensure that the restored files are consistent with the other datafiles.

The option to shut down the database and perform a time-based recovery up to log sequence 49 is incorrect because you cannot perform a time-based recovery without knowing the exact time at which the table was dropped from the database.

The option to shut down the database and perform a cancel-based recovery up to log sequence 51 is incorrect. The database cannot be recovered up to log sequence 51 because log sequence 50 is missing.

The option to take the USERS tablespace offline and recover only the DA2.DBF datafile after restoring it from the latest backup is incorrect. This process will not recover the dropped table. A datafile is restored from the latest backup and recovered only if that particular datafile has been affected by a media failure.

The option stating that the dropped MASTER table cannot be recovered is incorrect because the table can be recovered by performing a cancel-based recovery on the database.

Item: 8 (Ref:1Z0-042.17.2.4)

Your database is running in the ARCHIVELOG mode. Which file, when lost, will cause the database to halt?

- alert log file
- password file
- parameter file
- offline datafile
- archive redo log file
- multiplexed control file

Answer:

multiplexed control file

Explanation:

The database will halt if you lose a multiplexed control file in the database. To enable a database to function, it is necessary to ensure that all the multiplexed copies of the control files are accessible to the database. If a single multiplexed control file is unavailable, the database will halt.

The database will not halt if the alert log file is lost. The alert log file will be re-created automatically. The alert log file in an Oracle database contains database-wide information regarding errors and other important events in the database. The alert log file contains the startup and shutdown times of the database, the default parameters used to start the database, and other important information regarding the database.

The database will not halt if the password file is lost. If the password file is lost, the database will be operational, but the users will face problems while logging on to the database by using the SYSDBA and SYSOPER privileges. The password file can be re-created if the file is lost. The password file contains information regarding the number of users that can be granted the SYSDBA or the SYSOPER privilege.

The database will not halt if the parameter file is lost. The parameter file is used by the database only when the database is started and is not read until the next startup. Therefore, the loss of the parameter file will not affect a running database. The parameter file specifies the Oracle database instance parameters and the values defined for these parameters. The parameter file can be re-created from a previous backup if it is lost.

The database will not halt if an offline datafile is lost because the datafile is offline and is not currently accessed by the database. An offline datafile can be restored from a backup.

The database will not halt if an archive redo log file is lost because archive redo log files are not necessary for the database to function. Archive redo log files, which are archived copies of redo log files, store transaction information.

Item: 9 (Ref:1Z0-042.17.2.5)

When an Oracle user process is terminated abnormally, the Oracle background process PMON cleans up the terminated process. Which tasks are accomplished by PMON when it attempts to clean up this abnormally terminated process? (Choose all that apply.)

- [ ] releasing the resources held by the failed process
- [ ] rolling back the transaction that caused the process to fail
- [ ] releasing the table and row level locks held by the failed process
- [ ] deallocating the temporary segments held by the failed user process
- [ ] coalescing of free space that exists within the space held by the failed process

Answer:

releasing the resources held by the failed process
rolling back the transaction that caused the process to fail
releasing the table and row level locks held by the failed process

---

Explanation:

The PMON process is responsible for cleaning up a failed user process. In this process, PMON releases the resources held by the failed user process, rolls back the transaction that caused the process to fail, and releases the row and table level locks held by the failed user process. Additionally, it also restarts the dead dispatchers. As PMON rolls back the transaction that caused the process to fail, the data up to the last commit before the abnormal termination is retained in the database.

The option that states that PMON deallocates the temporary segments held by failed user process is incorrect because deallocation of database-wide temporary segments is done by the SMON process.

The option that states that PMON coalesces free space is incorrect because the SMON process coalesces free space.

Item: 10 (Ref:1Z0-042.17.6.4)

Which actions should you perform in your database to minimize the potential for loss at a single point of failure? (Choose all that apply.)

- [ ] Multiplex the datafiles.
- [ ] Use a standby database.
- [ ] Multiplex the control files.
- [ ] Multiplex the online redo logs.
- [ ] Create more than two online redo log groups.
- [ ] Create a locally-managed SYSTEM tablespace.

Answer:

Multiplex the control files.
Multiplex the online redo logs.
Create more than two online redo log groups.

Explanation:

To minimize the potential for loss at a single point of failure, you should multiplex the control files and the online redo log files and create more than two online redo log groups in the database. Oracle recommends that you have three control files and suggests that you have at least two control files. These two control files should be stored on separate physical disks. This will minimize the potential loss at a single point of failure. Oracle also recommends that you multiplex your redo log files. This will prevent a potential loss at a single point of failure. When you multiplex the redo log files, Oracle maintains identical copies of redo logs at different multiplexed destinations. The loss potential due to a single point of failure damaging a redo log member is minimized because you have an identical copy of the redo log at the multiplexed destination. You can also create more than two online redo log groups in the database to minimize the loss potential at a single point of failure. The reason for this is when any redo log group becomes unavailable, the database operation does not halt if at least two online redo log groups are available. To enable a database to function, at least two online redo log groups must be available. You can create more than two online redo log groups to prevent against potential loss at a single point of failure.

You cannot multiplex the datafiles. To minimize the loss potential due to loss of datafiles you must perform regular backups of the database.

Using a standby database does not minimize the loss potential at a single point of failure. A standby database, which is an identical copy of the production database, is used to minimize the downtime of a database. When a production database stops functioning, the standby database can be used as the production database.

Using a locally-managed SYSTEM tablespace does not minimize the loss potential at a single point of failure. A locally-managed SYSTEM tablespace ensures better performance and easier management than a dictionary-managed tablespace, but does not in any way minimize the loss potential at a single point of failure.

Item: 11 (Ref:1Z0-042.17.2.3)

You are a database administrator working on the PROD database in your organization. The database is running in the ARCHIVELOG mode. A user modifies the data in the EMP table and commits the transaction at 10:30 P.M. While the database is running, another user drops the EMP table at 11:00 P.M.

Which method should you use to recover the dropped EMP table?

- Shut down the database and perform a complete recovery.
- Shut down the database and perform a time-based recovery.
- Shut down the database and perform a cancel-based recovery.
- Shut down the database and perform a tablespace point-in-time recovery.

Answer:

Shut down the database and perform a time-based recovery.

Explanation:

In this scenario, you should shut down the database and perform a time-based recovery to recover the dropped EMP table because you are aware of the time at which the transaction on the table was committed. Also, you are aware of the time at which the table was dropped. The incomplete recovery should be performed up to the time before the table was dropped.

The option to shut down the database and perform a complete recovery is incorrect because complete recovery will not recover the table. Only an incomplete recovery can recover the table because you must recover the database to its state at a prior point in time. On the other hand, a complete recovery is used when you restore a datafile or a control file from a backup and use the archive redo logs to apply the changes to these restored datafiles. You can perform a complete recovery to avoid any loss of data.

The option to shut down the database and perform a cancel-based recovery is incorrect because you were not aware of the SCN numbers when the changes to the table were committed and when the table was dropped. You can perform a cancel-based recovery when you need to recover the database up to a particular point in time in the past based on the SCN numbers.

The option to shut down the database and perform a tablespace point-in-time recovery is incorrect because you are not required to recover the tablespace in this scenario. An individual table cannot be recovered by using the tablespace point-in-time recovery. A tablespace point-in-time recovery is performed to recover a dropped tablespace.

Item: 12 (Ref:1Z0-042.17.2.2)

While users were inserting and updating data in a database, the instance crashed because one of the essential DBW*n* background processes failed.

Which two statements are true regarding the recovery of changes made to the database before the instance crashed? (Choose two.)

- The uncommitted changes in the database before the instance crashed cannot be recovered.
- The committed changes in the database before the instance crashed will remain intact in the database.
- The uncommitted changes in the database before the instance crashed will be recovered automatically when the database is restarted.
- The uncommitted changes in the database before the instance crashed can be recovered by applying the changes stored in the online redo log file.
- The uncommitted changes in the database before the instance crashed can be recovered by reapplying the undo data that is contained in the undo segments.

Answer:

The uncommitted changes in the database before the instance crashed cannot be recovered.

The committed changes in the database before the instance crashed will remain intact in the database.

Explanation:

In this scenario, the uncommitted changes in the database before the instance crashed cannot be recovered, and the committed changes in the database before the instance crashed will remain intact. After the instance crashes, SMON will perform an instance recovery. This recovery will retain only the committed data in the database. The redo log recovery begins at the checkpoint position and ends at the end of the redo log. The committed data that has not been written to the datafiles will be extracted from the online redo log file. Any uncommitted data in the database will be rolled back by using the undo information that is contained in the undo segments. After the instance recovery, the database files will be synchronized to ensure that the database contains only the committed data.

The option stating that the uncommitted changes in the database before the instance crashed will be recovered automatically when the database is restarted is incorrect because the next startup will only recover the committed changes. It will not recover the uncommitted changes.

The option stating that the uncommitted changes in the database before the instance crashed can be recovered by applying the changes in the online redo log file is incorrect because the uncommitted data cannot be recovered.

The option stating that the uncommitted changes in the database before the instance crashed can be recovered by reapplying the undo data that is contained in the undo segments is incorrect because the uncommitted changes before the instance crashed cannot be recovered. The uncommitted changes will be rolled back by performing an instance recovery on the database at startup.

Item: 13 (Ref:1Z0-042.17.1.3)

The database in your company runs in the NOARCHIVELOG mode. You take a weekly backup of the database every Saturday morning.

The user SHELLY created a table on Monday morning and inserted some important data into it. On Thursday, this table was erroneously dropped by another user who had been granted the DROP ANY TABLE privilege.

How will you recover the dropped table?

- The dropped table cannot be recovered.
- Perform a complete recovery to recover the dropped table from the database.
- Perform a time-based recovery to recover the database up to the time at which the table was dropped.
- Perform a point-in-time recovery to recover the database to the point in time before the table was dropped.

Answer:

The dropped table cannot be recovered.

Explanation:

The table cannot be recovered because the database is running in the NOARCHIVELOG mode. In this mode, the database can be recovered only up to the point of the last complete backup. Because the last complete backup was performed before the table was created, the backup does not contain the table.

The option to perform a complete recovery to recover the dropped table from the database is incorrect. When running in the NOARCHIVELOG mode, a complete recovery is only possible up to the point of the last complete backup. Because the last complete backup was performed before the table was created, the backup does not contain the table, and a complete recovery cannot restore the table.

The option to perform a time-based recovery on the database to recover the database up to the time at which the table was dropped is incorrect because you cannot perform a time-based recovery on a database running in the NOARCHIVELOG mode. A time-based recovery can be performed on databases running only in the ARCHIVELOG mode. A time-based recovery is a recovery based on time, where you perform recovery up to a specified non-current time.

The option to perform a point-in-time recovery to recover the database to the point in time before the table was dropped is incorrect because you cannot perform a point-in-time recovery on a database running in the NOARCHIVELOG mode. A point-in-time recovery can be performed on the databases running only in the ARCHIVELOG mode. A point-in-time recovery is a database recovery where you perform recovery up to a specified non-current SCN, time, or log sequence number.

Item: 14 (Ref:1Z0-042.17.4.3)

In your production database, you notice that due to the frequency of checkpoints, the uncommitted data is occasionally written to the datafiles. You want to tune the frequency of the checkpoints to address this problem.

Which advisor will enable you to address this problem?

- MTTR Advisor
- Segment Advisor
- Undo Advisor
- Automatic Database Diagnostic Monitor

Answer:

MTTR Advisor

Explanation:

To tune the checkpoint frequency in a database, you can use the MTTR Advisor. The MTTR Advisor is used to determine the most effective value for the FAST_START_MTTR_TARGET initialization parameter depending on the workload on the database. The FAST_START_MTTR_TARGET initialization parameter specifies the time required, in seconds, to perform an instance recovery after an instance crash. After the FAST_START_MTTR_TARGET initialization parameter is set, the other parameters in the database will be automatically tuned to meet this target.

The Segment Advisor cannot be used to tune the frequency of checkpoints. The Segment Advisor can be used to identify space and space fragmentation issues in objects, such as tables, indexes, segments, and tablespaces. The Segment Advisor can also be used to analyze whether an object can be shrunk to reduce space consumption or not. The Segment Advisor can be invoked at the segment, tablespace, and object levels.

The Undo Advisor cannot be used to tune the frequency of the checkpoints. The Undo Advisor is used to provide information for proper sizing of the undo tablespace.

The Automatic Database Diagnostic Monitor (ADDM) cannot be used to tune the frequency of the checkpoints. The ADDM is used to gather recommendations on common problems encountered while managing a database. The problems detected by the ADDM include CPU bottlenecks, high-load SQL statements, I/O capacity, and other performance-related issues.

Item: 15 (Ref:1Z0-042.17.5.2)

Due to certain changes in the database availability, you must ensure that the database is available to the users while performing a backup. Therefore, you must configure your database to run in the ARCHIVELOG mode.

Which steps are essential to convert the database from the NOARCHIVELOG mode to the ARCHIVELOG mode? (Choose all that apply.)

- Set the LOG_ARCHIVE_START parameter to TRUE.
- Increase the number of redo log files in the database.
- Issue the ALTER DATABASE ARCHIVELOG; statement.
- Shut down the database and open it in the MOUNT state.
- Shut down the database and open it in the NOMOUNT state.
- Perform a full database backup after configuring the database to the ARCHIVELOG mode.

Answer:

Issue the ALTER DATABASE ARCHIVELOG; statement.
Shut down the database and open it in the MOUNT state.

Explanation:

You must perform the following steps to change the database from the NOARCHIVELOG mode to the ARCHIVELOG mode:

1. Shut down the database.
2. Open the database in the MOUNT state.
3. Issue the ALTER DATABASE ARCHIVELOG; statement.

The archiving mode in the database can also be changed in the Database Control home page by checking the ARCHIVELOG mode check box.

The option that states that you must set the LOG_ARCHIVE_START parameter to TRUE is incorrect because setting this parameter is not essential for converting the database from the NOARCHIVELOG mode to the ARCHIVELOG mode. When the database is converted to the ARCHIVELOG mode from the NOARCHIVELOG mode, the archiving of the redo logs is automatically enabled. You are not required to set the LOG_ARCHIVE_START parameter.

The option that states that you must increase the number of redo log files in the database is incorrect because this step is not required to convert the database from the NOARCHIVELOG mode to the ARCHIVELOG mode. The minimum number of redo log files required in both the cases is two. Therefore, while converting a database to the ARCHIVELOG mode, you are not required to increase the number of redo log files in the database.

The option that states you must shut down the database and open it in the NOMOUNT state is incorrect because the database must be opened in the MOUNT state to change it to the ARCHIVELOG mode.

The option that states you must perform a full database backup after changing the database to the ARCHIVELOG mode is incorrect. This is not an essential step for converting the database from the NOARCHIVELOG mode to the ARCHIVELOG mode. However, as a safety measure, and to enable recovery of a database in the event of a failure, it is recommended that you take a backup of the database after converting it from the NOARCHIVELOG mode to the ARCHIVELOG mode.

Item: 16 (Ref:1Z0-042.17.6.3)

The database in your company is running in the NOARCHIVELOG mode. The database has one control file that must be guarded against failure. To guard the control file, you want to multiplex it to a different location.

The following is a list of potential steps to multiplex the control file:

1. Restart the database.
2. Shut down the instance.
3. Abort the running instance.
4. Start up the database in the MOUNT state.
5. Copy the control file to the desired location by using OS commands.
6. Modify the CONTROL_FILES parameter in the initialization parameter file contained in your database.

What is the correct sequence of steps you should follow to achieve the objective of multiplexing the control file?

- 1, 5, 6
- 1, 5, 2, 6
- 2, 5, 6, 1
- 3, 5, 1, 6
- 5, 2, 6, 1

Answer:

2, 5, 6, 1

Explanation:

The correct sequence of steps is 2, 5, 6, 1. To multiplex the database control files, you should follow the steps in this order:

1. Shut down the instance.
2. Copy the control file to the desired location by using OS commands.
3. Modify the CONTROL_FILES parameter in the initialization parameter file of your database.
4. Restart the database.

Oracle recommends that the database contain at least three copies of control files.

All of the other options are incorrect because they do not represent the correct sequence of steps you should follow to multiplex the control file.

Item: 17 (Ref:1Z0-042.17.5.4)

In the production database, you have set the following parameter in the parameter file:

```
LOG_ARCHIVE_FORMAT='arch_%t_%s_%r.arc'
```

With this parameter setting, which statement is true?

- The database is running in the ARCHIVELOG mode.
- The new archive redo log files in the database will start from 0 after a RESETLOGS operation.
- The old archive redo log files in the database will not be overwritten following a RESETLOGS operation.
- The archive redo log files in the database will include the log sequence number and the tablespace name in the file names.
- The archive redo log files in the database will include the database name and log sequence number in the file names.

Answer:

The old archive redo log files in the database will not be overwritten following a RESETLOGS operation.

Explanation:

Specifying the `arch_%t_%s_%r.arc` value for the LOG_ARCHIVE_FORMAT parameter in the initialization file will ensure that the old archive redo log files in the database are not overwritten following a RESETLOGS operation. The LOG_ARCHIVE_FORMAT parameter specifies a string that represents the default file name format for the archived redo log files. This string can consist of text and several variables. These variables are %s, %S, %t, %T, %a, %d, and %r. A RESETLOGS operation is performed after an incomplete recovery. After the RESETLOGS operation, all the old archive redo log files in the database are overwritten. The %r variable in the archive format indicates that the old archive redo log files should not be overwritten after the RESETLOGS operation. The %t variable indicates that the archive redo log file name must include the thread number in the file name. The %s variable indicates that the archive redo log file name must include the log sequence number in the file name.

Setting the LOG_ARCHIVE_FORMAT parameter does not indicate that the database is running in the ARCHIVELOG mode. If the database is running in NOARCHIVELOG mode, this parameter is ignored. The V$DATABASE view can be queried to determine whether the database is running in the ARCHIVELOG mode.

This parameter setting does not indicate that the new archive redo log files in the database should start from 0 after a RESETLOGS operation. This parameter is set to prevent the archive redo log files from being overwritten. Not setting this parameter will lead to a situation in which the new archive redo log files in the database will start from 0 after a RESETLOGS operation.

With this parameter setting, the archive redo log files in the database will include the log sequence number, but not the tablespace name in the file names. The %s variable includes the log sequence number in the file name, but no variable exists that allows you to include the tablespace name in the file name.

With this parameter setting, the archive redo log files in the database will include the log sequence number, but not the database name in the file names. The %s variable includes the log sequence number in the file name, but no variable exists that allows you to include the database name in the file name. You can use the %d variable to include the database ID in the file name.

Item: 18 (Ref:1Z0-042.17.4.1)

You are working on the PROD database. In the initialization parameter file of the database, you set the following parameter:

```
FAST_START_MTTR_TARGET=180
```

What does this parameter represent?

- the time required for instance recovery
- the time lag between two consecutive checkpoints
- the number of I/Os required during instance recovery
- the number of redo buffers required during instance recovery
- the number of database blocks required during instance recovery

Answer:

the time required for instance recovery

Explanation:

The FAST_START_MTTR_TARGET parameter represents the time required for instance recovery. The FAST_START_MTTR_TARGET parameter specifies the mean-time-to-recover for a database after an instance crash. In this scenario, the parameter setting specifies that the instance should be recovered from a crash within 180 seconds. Setting the FAST_START_MTTR_TARGET parameter will set all the other required parameter values to ensure that instance recovery takes no longer than the time specified by this parameter.

The FAST_START_MTTR_TARGET parameter does not represent the time lag between two consecutive checkpoints. The time lag between two consecutive checkpoints is set by using the LOG_CHECKPOINT_INTERVAL parameter.

The FAST_START_MTTR_TARGET parameter does not represent the number of I/Os required during instance recovery. The FAST_START_IO_TARGET parameter is used to specify the number of I/Os required for a checkpoint process to occur. This parameter directly affects the instance recovery phase because during the instance recovery phase, the instance must be recovered up to the last checkpoint position.

The FAST_START_MTTR_TARGET parameter does not represent the number of redo buffers required during instance recovery. The redo buffers that are required depend on the time difference between the checkpoint and the instance crash.

The FAST_START_MTTR_TARGET parameter does not specify the number of database blocks required during instance recovery. Database blocks are not required during instance recovery. Only redo buffers and undo blocks are required during instance recovery. Database blocks are the blocks of data retrieved by the users from datafiles.

Item: 19 (Ref:1Z0-042.17.5.1)

You have created your database by using the DBCA. After creating the database, you changed the state of the database from the NOARCHIVELOG mode to the ARCHIVELOG mode.

After placing the database in the ARCHIVELOG mode, what should you do to enable archiving?

- Set the LOG_ARCHIVE_TRACE parameter to TRUE.
- Set the LOG_ARCHIVE_START parameter to TRUE.
- Set the LOG_ARCHIVE_FORMAT parameter to TRUE.
- Set at least one destination for archiving the redo log files by using the LOG_ARCHIVE_DEST parameter.
- Do nothing. Oracle will automatically enable archiving.

Answer:

Do nothing. Oracle will automatically enable archiving.

Explanation:

You should do nothing because Oracle will automatically enable archiving. After changing the database state to the ARCHIVELOG mode, Oracle will automatically enable archiving. You are not required to set any parameters to enable archiving on the database. You should enable the ARCHIVELOG mode when you want to ensure that any erroneous modification performed by the users can be undone. Only the ARCHIVELOG mode enables you to perform an incomplete recovery to recover the database up to a prior point in time.

The option stating that you must set the value of the LOG_ARCHIVE_TRACE parameter to TRUE is incorrect because this parameter is used to control the output generated by the ARCHIVELOG process.

The option stating that you must set the value of the LOG_ARCHIVE_START parameter to TRUE is incorrect because this parameter has been deprecated in Oracle 10*g*. In earlier releases, this parameter was used to enable automatic archiving for a database.

The option stating that you must set the value of the LOG_ARCHIVE_FORMAT parameter to TRUE is incorrect because this parameter is used to set the default file name format. In addition, this parameter is not specified as a Boolean value, but rather a string that represents the file name.

The option stating that you must set at least one destination for archiving the redo log files is incorrect because setting this destination for redo log files does not enable proper functioning of a database in the ARCHIVELOG mode. The destination is set to specify the location at which the archive redo logs will be saved.

Item: 20 (Ref:1Z0-042.17.6.2)

You have two redo log members in each redo log group in your database. You are required to add a redo log member to an existing group in your database to increase the probability of recovering the redo logs in case of any failure.

What will happen if you attempt to add a member to an existing group without using the SIZE option?

- The statement will fail.
- The statement will prompt for the size of the redo log file.
- The Oracle server will use the default redo log member size.
- The Oracle server will use a multiple of the DB_BLOCK_SIZE parameter.
- The Oracle server will use the size of the existing members in the group.

Answer:

The Oracle server will use the size of the existing members in the group.

Explanation:

If you attempt to add a member to an existing group without using the SIZE option, the Oracle server will create the new member with a size similar to that of the existing members in the group. The status of the newly added redo log member will be INVALID. If the file already exists, the new file must have a size similar to the size of the existing files in the redo log group. In such a scenario, you must use the REUSE option.

The statement will not fail because the Oracle server will create a member that has a size similar to the size of the existing redo log members. However, the statement will fail if you use the SIZE option in the statement. You cannot use the SIZE option while adding a redo log member to an existing group by using the ALTER DATABASE ADD LOGFILE MEMBER statement.

The statement will not prompt for the size of the redo log file because the Oracle server will create the new member with a size similar to that of the existing members in the group.

The Oracle server will not use the default redo log member size because no default size is specified for the redo log member in the Oracle database.

The Oracle server will not use the DB_BLOCK_SIZE parameter to size the redo log member. The DB_BLOCK_SIZE parameter specifies the default block size for the database at the time of database creation. All tablespaces created in the database will have the same standard block size by default.

Database Backups

Item: 1 (Ref:1Z0-042.18.8.1)

You run the following statement in your database to add a datafile:

```
SQL> ALTER TABLESPACE TS1 ADD DATAFILE '\ORADATA\ORA90\MYNEWDB\DA2.DBF' SIZE 10M;
```

What should you do after running this statement in your database?

- Restart the instance.
- Rename the datafile.
- Back up the control file.
- Update the parameter file.

Answer:

Back up the control file.

Explanation:

You should back up the control file. The control file records the names and locations of the datafiles and redo log files. The control file is updated when a datafile or redo log file is added, renamed, or dropped. In this scenario, we are adding a datafile to the database, which causes a change in the structure of the database. The control file should be backed up after structural changes in the database. You can create a backup of the control file by running the `ALTER DATABASE BACKUP CONTROLFILE TO <filename>` statement. You can also create a file with the SQL statements required to re-create your control file by issuing the `ALTER DATABASE BACKUP CONTROLFILE TO TRACE` statement. In addition, structural changes are induced in the database when you create a tablespace, add a redo log file to the tablespace or drop a tablespace or redo log file from the database.

The option that states that you must restart the instance after running this statement is incorrect because you are not required to restart the instance after adding a datafile to a database.

The option that states that you must rename the datafile after running the statement is incorrect because you are not required to rename the datafile after adding it.

The option that states that you should update the parameter file is incorrect because it is not necessary to update the parameter file after adding a new datafile to an existing database. The parameter file does not store any information about the datafiles.

Item: 2 (Ref:1Z0-042.18.9.1)

The database of your company has gone down because of a media failure. Upon analysis, you discover that the DA1.DBF datafile has been corrupted and has caused the database instance to crash. On further investigation, you realize that the backup of this datafile taken using RMAN is also corrupted, and you have only a copy of this file taken using the OS commands.

How can you proceed in this scenario if you want to recover the database by using RMAN?

- Use the REPORT RMAN command.
- Use the CATALOG RMAN command.
- Use the RECOVER RMAN command.
- Use the CROSSCHECK RMAN command.
- The database cannot be recovered using RMAN. You must recover it using user-managed recovery.

Answer:

Use the CATALOG RMAN command.

Explanation:

You can use the RMAN CATALOG command to catalog the backup in the RMAN repository. In this scenario, the copy of the DA1.DBF datafile that was taken using the OS commands can be registered with RMAN by using the CATALOG command. The CATALOG command is used to add metadata regarding the user-managed datafile copies and control file copies to the RMAN repository. In this scenario, you can add the information regarding the datafile copy to the RMAN repository, using the CATALOG command. The RECOVER command can then be used by RMAN to perform a recovery.

The option to use the RMAN REPORT command is incorrect because this command cannot be used to add the information regarding the datafile copy to the RMAN repository. This command is used to collect information about the existing backups in the database.

The option to use the RMAN RECOVER command is incorrect because this command cannot be used to add the information regarding the datafile copy to the RMAN repository. This command is used to perform a recovery of the datafiles, tablespaces, and databases.

The option to use the RMAN CROSSCHECK command is incorrect because this command cannot be used to add the information regarding the datafile copy to the RMAN repository. This command is used to verify the status of the database backups created by using RMAN. This command will check the status of the backups and update the RMAN repository accordingly.

The option that states that the database cannot be recovered by using RMAN and must be recovered using user-managed recovery is incorrect. The database can be recovered using RMAN by first cataloging the datafile copy on the disk in the RMAN repository.

Item: 3 (Ref:1Z0-042.18.7.2)

The database of your company is running in the NOARCHIVELOG mode. The data in the database does not change frequently, but you must guard the database against failures. To do this, you must design a backup strategy.

Which option will ensure the best results in this scenario?

- Take an open database backup every week.
- Take a cold backup of the database every night.
- Take a cold backup of the database every three days.
- Take a hot backup of the database by sequentially placing the tablespaces in the online backup mode.

Answer:

Take a cold backup of the database every three days.

Explanation:

The option to take a cold backup of the database every three days is correct. In this scenario, you can only take a cold backup of your database because your database is running in the NOARCHIVELOG mode. You cannot perform any other type of backup when your database is running in the NOARCHIVELOG mode. Also, the database does not change frequently. Therefore, you should take a full backup of your database every three days instead of taking a full backup every night.

The option to take an open database backup every week is incorrect because you cannot perform an open database backup when your database is running in the NOARCHIVELOG mode.

The option to take a cold backup of the database every night is incorrect because in this scenario, the data in the database does not change frequently. Therefore, taking a cold backup every night is not necessary. You can take a cold backup every three days and minimize downtime.

The option to take a hot backup of the database by sequentially placing the tablespaces in the online backup mode is incorrect because you cannot place the tablespaces in the online backup mode when the database is running in the NOARCHIVELOG mode. You can place the tablespaces in the online backup mode when your database is running in the ARCHIVELOG mode.

Item: 4 (Ref:1Z0-042.18.2.3)

You are a database administrator working on the PROD database. Your database is running in the NOARCHIVELOG mode. Two datafiles in your database, DA1.DBF and IND1.DBF, are offline and the EX2.DBF datafile is read-only. You want to back up your database to guard against failure.

Which two methods can you employ to back up your database? (Choose two.)

- [ ] Take a full backup of the database when the database is open.
- [ ] Shut down the database and take a full backup of all the datafiles and the control file.
- [ ] Open the database in the MOUNT state and then back up all the datafiles and the control file of the database.
- [ ] Bring the offline datafiles online and take a backup of all the online datafiles, the read-only datafile, and the control file.
- [ ] Back up the offline and read-only datafiles. Take a backup of all the online datafiles one by one by placing them in the online backup mode. Then, back up the control file.

Answer:

Shut down the database and take a full backup of all the datafiles and the control file.
Open the database in the MOUNT state and then back up all the datafiles and the control file of the database.

Explanation:

In this scenario, your database is in the NOARCHIVELOG mode. Therefore, you can only perform a consistent backup. This can be done by shutting down the database and backing up the datafiles and the control file. A consistent backup can also be performed by starting the database in the MOUNT state and backing up the datafiles and the control file. The backup taken in both the scenarios will be a consistent backup.

You cannot take a full backup of the database when the database is open because you cannot perform an open database backup of a database running in the NOARCHIVELOG mode. If the database is running in the NOARCHIVELOG mode, you can only perform a backup after the database is shut down.

You cannot bring the offline datafiles online and take a backup of all the online datafiles, the read-only datafile, and the control file. You cannot take an open database backup of a database running in the NOARCHIVELOG mode. An open database backup in the NOARCHIVELOG mode is invalid.

You cannot back up the offline and read-only datafiles and take a backup of all the online datafiles one by one by placing them in the online backup mode because the datafiles cannot be placed in the backup mode if the database is running in the NOARCHIVELOG mode.

Item: 5 (Ref:1Z0-042.18.7.1)

You are working on the PROD database on which downtime is not allowed. This database is running in the ARCHIVELOG mode. The data in the database changes rapidly. You are required to design a suitable backup strategy that should not increase the workload on the database. A cold backup of your database takes three hours.

Which backup strategy will be appropriate in this scenario?

- Take a cold backup of the database every night.
- Take a full image copy of all the datafiles in the database every night.
- Take a cold backup of the database once a week and export the updated tables every night.
- Take a full image copy of all the datafiles in the database once a week and enable the block change tracking feature.
- Take a level 0 backup of the database every week, an incremental level 1 backup every night, and enable the block change tracking feature.
- Take an incremental level 1 backup of the database every week, a level 0 backup every night, and enable the block change tracking feature.
- Take a level 0 backup of the database every night, an incremental level 1 backup every one hour, and disable the block change tracking feature.

Answer:

Take a level 0 backup of the database every week, an incremental level 1 backup every night, and enable the block change tracking feature.

Explanation:

The option to take a level 0 backup of the database every week, an incremental level 1 backup every night, and enable the block change tracking feature is correct. The database cannot tolerate any downtime, and the data changes rapidly. Therefore, you should take a level 0 backup of the database every week and an incremental level 1 backup every night. A level 0 backup is a complete database backup that includes all the used blocks in the database and is taken as a base for all further incremental backups. A level 1 backup is an incremental backup of the database. A level 1 backup will back up only those data blocks that have changed since the last level 0 backup. You should also enable the block change tracking feature. The block change tracking feature can be enabled for RMAN incremental backups. When the block change tracking feature is enabled, the information about changed blocks in every datafile is maintained in a change tracking file. This change tracking file is read by RMAN while performing incremental backups. This avoids scanning complete datafiles for determining changed blocks and improves performance of the incremental backups. The block change tracking feature can be enabled using the following statement:

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

This backup strategy ensures that daily changes in the database are backed up and time spent on backups is reduced. This will guard against failure because the data from the day's work is backed up every night by using the incremental level 1 backup.

The option to take a cold backup of the database every night is incorrect because taking a cold backup will require you to shut down the database. In this scenario, you cannot do this because downtime is not allowed.

The option to take a full image copy of all the datafiles in the database every night is incorrect. The entire database must be backed up using this technique. This option will increase the workload on the database.

The option to take a cold backup of the database once a week and export the updated tables every night is incorrect because taking a cold backup requires the database to be shut down. In this scenario, you cannot do this because downtime is not allowed.

The option to take a full image copy of all the datafiles in the database once a week and enable the block change tracking feature is incorrect because this will not ensure backup of the daily changes that occur in the database. Taking a full image copy of all the datafiles in the database once a week will back up the database on a weekly basis and not allow daily changes in the database to be backed up. The block change tracking feature is valid only for incremental backups in RMAN, it is not valid for image copies taken using RMAN.

The option to take an incremental level 1 backup of the database every week, a level 0 backup every night, and enable the block change tracking feature is incorrect because taking a level 0 backup of the database every night will increase the workload on the database. A level 0 backup is a complete database backup that includes all the used blocks in the database and is taken as a base for all further incremental backups. A level 1 backup is an incremental backup of the database. A level 1 backup will back up only those data blocks that have changed since the last level 0 backup. While designing a backup strategy,

you must ensure that a level 0 backup is taken less frequently and a level 1 backup is taken more frequently. This will reduce the time required to perform backups.

The option to take a level 0 backup of the database every night, an incremental level 1 backup every one hour, and disable the block change tracking feature is incorrect because taking a full backup of the database every night will increase the workload on the database.

Item: 6 (Ref:1Z0-042.18.2.1)

In which scenario can you NOT create a backup without shutting down the database?

- The database has only one control file.
- The database has only two redo log file groups.
- The database is running in the ARCHIVELOG mode.
- The database is running in the NOARCHIVELOG mode.
- You want to back up the SYSTEM tablespace in the database.
- You want to back up a read-only tablespace in the database.
- You want to back up a dictionary-managed tablespace in the database.

Answer:

The database is running in the NOARCHIVELOG mode.

Explanation:

You cannot create a backup of a database without shutting down the database when the database is running in the NOARCHIVELOG mode. A database running in the NOARCHIVELOG mode should always be backed up after a clean shutdown. If the database is backed up when the database is open, the backup created will not be valid for a recovery because no redo log files will be available to bring the database back to a consistent state.

A database with only one control file can be backed up without the database being shut down provided it is running in the ARCHIVELOG mode. An image copy backup of the database and a backup of a database when the datafiles and control files are not synchronized can also be performed without shutting down the database.

A database with only two redo log file groups can be backed up without the database being shut down provided it is running in the ARCHIVELOG mode.

A database that is running in the ARCHIVELOG mode can be backed up without the database being shut down.

You can back up the SYSTEM tablespace in your database when the database is open. The SYSTEM tablespace can be backed up when the database is online by placing the SYSTEM tablespace in the online backup mode and then copying the datafiles belonging to the SYSTEM tablespace.

You can backup a read-only tablespace even when the database is open. You do not need to place the tablespace in the online backup mode because the tablespace is read-only and therefore, no changes are being made to the tablespace. To backup a read-only tablespace you must copy the datafiles belonging to the tablespace.

You can back up a dictionary-managed tablespace even when the database is open. A dictionary-managed tablespace can be backed up by placing the tablespace in the online backup mode and copying the corresponding datafiles.

Item: 7 (Ref:1Z0-042.18.4.1)

Using the backup scheduler, you schedule a backup job to create a complete backup of your database every Saturday night.

Which tool will the backup scheduler use to create a backup?

- the PL/SQL engine
- Recovery Manager
- Enterprise Manager
- the DBMS_JOB package
- operating system utilities

Answer:

Recovery Manager

Explanation:

The backup scheduler uses the Recovery Manager (RMAN) tool to create a complete backup of the database. The backup scheduler is located in Enterprise Manager and can be used to schedule periodic backups of your database. Scheduling a backup will generate an RMAN script that will execute at the scheduled time.

The PL/SQL engine is not used to back up the database. The PL/SQL engine is used to compile PL/SQL programs and subprograms.

Enterprise Manager is not used to back up the database. Enterprise Manager is used as an interface to schedule the backups that will be created by using RMAN.

The DBMS_JOB package is not used as a tool by the backup scheduler to create backups. The DBMS_JOB package is used to schedule jobs, which can include database backups.

Operating system utilities are not used to back up the database when the backups are scheduled by using Enterprise Manager. Operating system utilities can be used to create a backup by employing user-managed backup techniques.

Item: 8 (Ref:1Z0-042.18.9.3)

You are using RMAN to perform backup and recovery on your database. The backup of one of the files was lost because it was located on a failed media.

Which option correctly describes the information about the backup present in the RMAN repository?

- The status of the backup will be AVAILABLE in the RMAN repository.
- All the information of the backup will be removed from the RMAN repository.
- The status of the backup will be updated to EXPIRED in the RMAN repository.
- The status of the backup will be updated to DELETED in the RMAN repository.
- The status of the backup will be updated to OBSOLETE in the RMAN repository.

Answer:

The status of the backup will be AVAILABLE in the RMAN repository.

Explanation:

In this scenario, the status of the backup will be AVAILABLE in the RMAN repository. If a backup is removed without using RMAN commands, RMAN is not aware of the deleted status of the backup. Therefore, the status of the backup will be AVAILABLE until you use the CROSSCHECK command to verify the status of the backup. When you run the CROSSCHECK command, the status of the backup will be set to EXPIRED in the recovery catalog.

The option stating that all the information of the backup will be removed from the RMAN repository is incorrect because the backup will still be marked as AVAILABLE in the RMAN repository. The information will be removed from the RMAN repository when you delete the backup by using the DELETE command at the RMAN prompt. When you issue the DELETE command, the backup will also be deleted from the OS.

The option stating that the status of the backup will be updated to EXPIRED in the RMAN repository is incorrect because the backup will still be marked as AVAILABLE in the RMAN repository. The status will be updated to EXPIRED if you use the CROSSCHECK command to verify the existence of the backup.

The option stating that the status of the backup will be updated to DELETED in the RMAN repository is incorrect because the status will still be marked as AVAILABLE in the RMAN repository. This is because RMAN is unaware of the deleted status of the backup.

The option stating that the status of the backup will be updated to OBSOLETE in the RMAN repository is incorrect because the status will still be marked as AVAILABLE in the RMAN repository. The status will be changed to OBSOLETE when the backup becomes older than the retention policy specified for the database.

Item: 9 (Ref:1Z0-042.18.5.1)

The database in your company is running in the ARCHIVELOG mode on a Windows platform. You have set the location for flash recovery area in the database to E:\DB2\FLASH.

Which three statements correctly describe configuration of the flash recovery area? (Choose three.)

- The E:\DB2\FLASH location will only store the archive redo log files.
- The database will pause if the E:\DB2\FLASH location becomes full.
- The E:\DB2\FLASH location will store only the archive redo logs and database backups.
- The space available in the flash recovery area will be affected by the retention policy configured.
- The size of the flash recovery area is specified by using the DB_RECOVERY_FILE_DEST parameter.
- If the E:\DB2\FLASH location becomes full, a message will be written to the alert log file of the database.
- The E:\DB2\FLASH location will store the archive redo logs, multiplexed copies of control files, and database backups.
- The space available in the flash recovery area will be affected by the number of destinations set for the archive redo log files.

Answer:

The database will pause if the E:\DB2\FLASH location becomes full.

The space available in the flash recovery area will be affected by the retention policy configured.

The E:\DB2\FLASH location will store the archive redo logs, multiplexed copies of control files, and database backups.

Explanation:

The database will pause if the location E:\DB2\FLASH becomes full because this location stores the archive redo log files of the database. If the location becomes full and no space is available for storing the newly generated archive redo logs, the database will pause until more space is created in this location. Also, the size of the flash recovery area is directly affected by the retention policy configured because this retention policy determines the time for which the files are to be stored in the flash recovery area. The higher the value set for retention policy, the greater the space required to store the files. This flash recovery area will store the archive redo log files, multiplexed copies of control files and online redo log files, and database backups.

The option stating that the E:\DB2\FLASH location will only store the archive redo log files is incorrect because this location will store not only the archive redo log files but also the multiplexed copies of control files, online redo log files, and database backups.

The option stating that the E:\DB2\FLASH location will store only the archive redo logs and database backups is incorrect because this location will store not only the archive redo log files and database backups, but also the multiplexed copies of control files and online redo log files.

The option stating that the size of the flash recovery area is set using the DB_RECOVERY_FILE_DEST parameter is incorrect because the size of the flash recovery area is set by using the USE_DB_RECOVERY_AREA parameter.

The option stating that if the E:\DB2\FLASH location becomes full, a message will be written to the alert log file of the database is incorrect because the database will pause if this location becomes full.

The option stating that the space in the flash recovery area will be affected by the number of destinations set for the archive redo log files is incorrect because the space in the flash recovery area will not be affected by this. On the contrary, archive log destinations cannot be configured when using the flash recovery area.

Item: 10 (Ref:1Z0-042.18.3.2)

You perform an incremental level 0 backup of your database. Which database files does the incremental level 0 backup contain?

- all the datafiles
- only all the online datafiles
- the control file of the database
- the password file of the database
- the parameter file of the database
- the archived log files of the database
- the online redo log files of the database
- all data files except the read-only datafiles

Answer:

all the datafiles

Explanation:

The incremental level 0 backup will contain all the datafiles. When you perform an incremental level 0 backup using RMAN, the backup contains all the datafiles in the database. This backup acts as the base level backup for all the incremental level backups. When you perform a base level or level 0 backup, it will back up all the used data blocks in the datafiles. Consequently, when you perform an incremental level 1 backup, only the blocks changed since the level 0 backup are backed up. An incremental level backup can be performed on datafiles, tablespaces, and the complete database.

The incremental level 0 backup will not contain only all the online datafiles because all the online as well as offline datafiles are backed up when you perform an incremental level 0 backup.

The incremental level 0 backup will not contain the control file of the database because control files are not backed up when you perform an incremental level 0 backup.

The incremental level 0 backup will not contain the password file of the database because the password file is not backed up when you perform an incremental level 0 backup.

The incremental level 0 backup will not contain the parameter file of the database because the parameter file is not backed up when you perform an incremental level 0 backup.

The incremental level 0 backup will not contain the archived log files of the database because the archived log files are not backed up when you perform an incremental level 0 backup.

The incremental level 0 backup will not contain the online redo log files of the database because the online redo log files are not backed up when you perform an incremental level 0 backup.

The incremental level 0 backup will not contain all the datafiles except the read-only datafiles because even the read-only datafiles are backed up when you perform an incremental level 0 backup.

Item: 11 (Ref:1Z0-042.18.4.2)

You are using the backup scheduler in Enterprise Manager to automate the backups of the database.

Which **Object Type** options can you specify to perform a backup on the **Schedule Backup: Strategy** page? (Choose all that apply.)

- ☐ **Tables**
- ☐ **Datafiles**
- ☐ **Archivelogs**
- ☐ **Control files**
- ☐ **Tablespaces**
- ☐ **Password files**
- ☐ **Parameter files**
- ☐ **Whole Database**

Answer:

Datafiles
Archivelogs
Tablespaces
Whole Database

Explanation:

You can specify the **Datafiles**, **Archivelogs**, **Tablespaces**, or **Whole Database** option when using the backup scheduler in Enterprise Manager. These options appear in the **Object Type** option group on the **Schedule Backup: Strategy** page. The **Whole Database** backup option will include the server parameter file and all the datafiles, archive redo logs, and control files in the database.

Tables is not a valid option available on the **Schedule Backup: Strategy** page. You cannot schedule a backup for individual tables in a database. However, you can perform a table-mode export to maintain a copy of the table and guard against accidental deletion of the table.

Control files is not a valid option available on the **Schedule Backup: Strategy** page. The control file will be automatically backed up when the **Whole Database** option is used.

Password files is not a valid option available on the **Schedule Backup: Strategy** page. The password file is an OS file and should be backed up by using OS commands.

Parameter files is not a valid option available on the **Schedule Backup: Strategy** page. The server parameter file will be automatically backed up when the **Whole Database** option is used.

Item: 12 (Ref:1Z0-042.18.3.1)

The database of your company is running in the ARCHIVELOG mode. You use RMAN to implement backup and recovery in your database. On Tuesday, you take an incremental level 1 backup of the database.

Which data blocks will be backed up by this incremental level backup if the backup taken is NOT a cumulative incremental backup?

- all the data blocks in the database
- all the used data blocks in the database
- all the unused data blocks in the database
- only the data blocks that have been added since the last full backup
- the data blocks that are different from the incremental level 2 backup
- the data blocks that have been changed after the backup taken on Monday
- the data blocks that have been modified after the incremental level 0 backup

Answer:

the data blocks that have been modified after the incremental level 0 backup

---

Explanation:

In this scenario, the data blocks that have been modified after the incremental level 0 backup will be backed up. When you perform an incremental level 1 backup using RMAN, all the blocks modified after the incremental level 0 backup are backed up. The incremental level 0 backup is used as a base backup to ensure that incremental backups will back up only the data blocks that have been changed since the incremental level 0 backup.

All the data blocks in the database will not be backed up because the incremental level 1 backup does not back up all the data blocks in the database. All the data blocks in the database will be backed up if you use the user-managed backup strategy to back up all the datafiles in the database or take another level 0 backup.

All the used data blocks in the database will not be backed up because the incremental level 1 backup does not back up all the used blocks in the database. All the used blocks in the database are backed up if you perform a full backup or incremental level 0 backup using RMAN.

All the unused data blocks in the database will not be backed up because the incremental level 1 backup does not back up all the unused blocks in the database. RMAN cannot be used to back up the unused data blocks in the database.

The data blocks that have been added since the last full backup will not be the only data blocks backed up because the incremental level 1 backup backs up the data blocks that have been added since the last full backup and the data blocks that have been modified since the last full backup.

The data blocks that are different from the incremental level 2 backup will not be backed up because the incremental level 1 backup does not back up the blocks that are different from the incremental level 2 backup. The incremental level 2 backup will back up the database blocks that have been changed since the incremental level 1 backup.

The data blocks that have been changed after the backup taken on Monday might not be backed up. The incremental level 1 backup will back up the data blocks that have changed after the level 0 backup. However, this level 0 backup might not have been taken on Monday.

Item: 13 (Ref:1Z0-042.18.8.2)

You run the following statement in your database to create a trace file in the database:

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

Which two statements regarding the primary use of the trace file created using this statement are true? (Choose two.)

- [ ] The trace file is used to change the name of the database.
- [ ] The trace file can be used as a readable form of the control file.
- [ ] The trace file is used to locate the redo log files and datafiles in the database.
- [ ] The trace file is used to re-create a control file of the database in the event of a media failure.
- [ ] The trace file is used to store the information about the latest configuration of the database.

Answer:

The trace file is used to change the name of the database.

The trace file is used to re-create a control file of the database in the event of a media failure.

Explanation:

You run this statement in the database to create a text file that can be used to change the name of the database and re-create the control file. This trace file also contains a command which is used to re-create the control file. The file created by running this statement is stored in the location pointed to by the parameter USER_DUMP_DEST. This text file contains the structural information in the database. The primary use of this file is to change the name of the database and to re-create the control file. The control file is re-created if there is a failure in the database or there is a requirement to change the name of the database. This trace file can also be used to change the maximum allowed limit for the number of datafiles and log files in the database. The options that you can change are MAXDATAFILES, MAXLOGFILES, MAXLOGMEMBERS, and MAXLOGHISTORY for which you need to re-create the control file after making the required changes in the trace file. The control file records the name and location of the datafiles and redo log files. This information describes the physical structure of the database. Therefore, you should back up the control file immediately after making changes to the physical structure of the database, regardless of whether or not the control file is multiplexed.

The option that states that the trace file is created to be used as a readable form of the control file is incorrect. The trace file and the commands stored in it are used to re-create the control file.

The option that states that the trace file is used to locate the redo log files and datafiles in the database is incorrect. The trace file and the commands stored in it are used to re-create the control file. The location of the datafiles and redo log files can be viewed by using the V$DATAFILE and V$LOGFILE views, respectively.

The option that states that the trace file is used to store the latest configuration of the database is incorrect because that is not the trace file's primary use. The primary use of the trace file is to re-create the control file in the event of a media failure or to change the name of the database.

Item: 14 (Ref:1Z0-042.18.9.2)

You are using RMAN to implement a backup and recovery procedure on your database. After querying the status of the backups, you observe that the status of some of the backups is OBSOLETE.

What does this status indicate?

- The backups cannot be detected by RMAN.
- The backups have been deleted from the RMAN repository.
- The backups cannot be used by RMAN to perform a recovery.
- The backups are eligible for deletion according to the retention policy.

Answer:

The backups are eligible for deletion according to the retention policy.

Explanation:

The status of OBSOLETE indicates that the backups are eligible for deletion according to the retention policy. When the backups become older than the retention policy set for the database, the status of the backups is updated to OBSOLETE in the RMAN repository. These backups can later be deleted by issuing the DELETE OBSOLETE command.

The option stating that the backups cannot be detected by RMAN is incorrect because the OBSOLETE status of the backups does not describe the backups that cannot be found by RMAN. If the backups cannot be found by RMAN, the status of the backup will be EXPIRED.

The option stating that the backups have been deleted from the RMAN repository is incorrect because the OBSOLETE status of the backups does not describe the backups that have been deleted from the RMAN repository. If a backup is deleted from the RMAN repository, the status of such a backup is EXPIRED. These backups also include the backups that have been deleted using OS utilities, the status for which is updated using the RMAN CROSSCHECK command.

The option stating that the backups cannot be used by RMAN to perform a recovery is incorrect because the OBSOLETE status of the backups does not indicate backups that cannot be used by RMAN to perform a recovery. If the backups cannot be used by RMAN to perform a recovery, the status of the backup will be UNAVAILABLE.

Item: 15 (Ref:1Z0-042.18.2.2)

You are working on a 24X7 database. You want to design a backup strategy for your database.

Which option should be enabled to ensure back up for a 24X7 database?

- The database should be running in the ARCHIVELOG mode.
- The database should be running in the NOARCHIVELOG mode.
- All the tablespaces in the database should be locally-managed.
- All the tablespaces in the database should be dictionary-managed.
- The SYSTEM tablespace in the database should be locally-managed.
- All the tablespaces in the database should be in the read-only mode.

Answer:

The database should be running in the ARCHIVELOG mode.

Explanation:

To ensure backup for a 24X7 database, the database should be running in the ARCHIVELOG mode. On a database that is running in a 24X7 setup, you must back up the database without shutting it down. To enable this, the database must be running in the ARCHIVELOG mode. When the database is running in the ARCHIVELOG mode, it can be backed up by using RMAN or by using a user-managed backup procedure. You cannot perform an open database backup of the database if the database is running in the NOARCHIVELOG mode. In the given scenario, the database is running 24 hours a day, 7 days a week. This means that the database cannot be shut down to perform backups.

The option stating that the database should be running in the NOARCHIVELOG mode is incorrect because if your database is running 24 hours a day, 7 days a week, you must perform a backup of the database when the database is up. This is not possible if the database is running in the NOARCHIVELOG mode.

The option stating that all the tablespaces in the database should be locally-managed is incorrect because even if the tablespaces are locally-managed, the precondition to back up a 24X7 database is that the database should be running in the ARCHIVELOG mode.

The option stating that all the tablespaces in the database should be dictionary-managed is incorrect because even if all the tablespaces are dictionary-managed, the precondition to back up a 24X7 database is that the database should be in the ARCHIVELOG mode. However, a dictionary-managed tablespace can be backed up without shutting down the database if the database is running in the ARCHIVELOG mode.

The option stating that the SYSTEM tablespace in the database should be locally-managed is incorrect because a locally-managed SYSTEM tablespace does not enable you to back up a database online. The precondition to back up a 24X7 database is that the database should be running in the ARCHIVELOG mode.

The option stating that all the tablespaces in the database should be in the read-only mode is incorrect because all the tablespaces in the database cannot be placed in the read-only mode. The SYSTEM, SYSAUX, default undo tablespace, and default temporary tablespace in the database cannot be placed in the read-only mode.

Item: 16 (Ref:1Z0-042.18.7.3)

Your production database is running in the ARCHIVELOG mode. You are using RMAN to implement backup and recovery in your database.

Which three tasks can you perform using RMAN? (Choose three.)

- online redo log backups
- auto backups of control files
- recovery of corrupted blocks in datafiles
- backup of files on tapes and Named Pipes
- auto recovery of lost online redo log members
- recovery using backups taken by OS commands
- recovery of dropped tables without performing incomplete recovery

Answer:

auto backups of control files
recovery of corrupted blocks in datafiles
backup of files on tapes and Named Pipes

Explanation:

Using RMAN, you can perform auto backups of control files, recovery of corrupted blocks in datafiles, and backup of files on tapes and Named Pipes. RMAN can be used to perform several tasks on your database. RMAN can be used to take backups of the database while the database is in the MOUNT state, automatically back up the control files, back up the online read/write datafiles in the database, perform block level recovery, perform incremental backups, and create a backup of files on tapes, Named Pipes, and so on. RMAN can also be used to back up the database, the online datafiles, and the archived redo log files. When datafiles are backed up using RMAN, only the used data blocks in the datafile are backed up. The free or unused data blocks are not backed up.

RMAN cannot be used to perform online redo log backups. Oracle recommends that you do not perform backups of online redo log files. However, you can back up the online redo log files by using the OS commands.

RMAN cannot be used to perform auto recovery of lost online redo log members. To recover the lost online redo log members, you must perform a user-managed recovery on the database.

RMAN cannot recover a database by using the backup taken by running the OS commands. To recover a database using the backup taken by running the OS commands, you must perform a user-managed recovery.

RMAN cannot be used to recover dropped tables from the database without performing an incomplete recovery. Dropped tables in the database can be recovered by using the Data Pump or LogMiner utility.

Item: 17 (Ref:1Z0-042.18.1.1)

In which three scenarios is a backup considered to be inconsistent? (Choose three.)

- [ ] You perform a backup of a database after an instance crash.
- [ ] You perform a backup of a 24X7 database in which downtime is not acceptable.
- [ ] You perform a backup of a closed database that is running in the ARCHIVELOG mode.
- [ ] You perform a backup of a closed database that is running in the NOARCHIVELOG mode.
- [ ] You perform a backup of the datafiles in a tablespace after placing the tablespace in the begin backup mode.
- [ ] You perform a backup of a database that is running in the NOARCHIVELOG mode when the database is in the MOUNT state.

Answer:

You perform a backup of a database after an instance crash.

You perform a backup of a 24X7 database in which downtime is not acceptable.

You perform a backup of the datafiles in a tablespace after placing the tablespace in the begin backup mode.

Explanation:

An inconsistent backup is a backup that is taken when the database is in the open state. Inconsistent backups do not guarantee that the SCN in the datafile headers matches the SCN in the control file. A consistent backup is a backup that is taken when the database is not open. In a consistent backup, the SCN in the datafile headers matches the SCN in the control file. A backup is considered to be inconsistent in the following scenarios:

- You perform a backup of a database after an instance crash. In this scenario, the database files are not synchronized. Therefore, the database backup is considered inconsistent.
- You perform a backup of a 24X7 database in which downtime is not acceptable. In this scenario, the database can be backed up only when it is open. Therefore, the backup performed will be considered inconsistent.
- You perform a backup of datafiles in a tablespace after placing the tablespace in the begin backup mode. When a tablespace is placed in the begin backup mode, the datafiles in the tablespace are not consistent. Backup of these datafiles will be an inconsistent backup.

If you perform a backup of a closed database that is running in the ARCHIVELOG mode, this will be considered a consistent backup. A closed database backup is always a consistent backup. This is true for a database running in the ARCHIVELOG or NOARCHIVELOG mode.

If you perform a backup of a closed database running in the NOARCHIVELOG mode, this will be considered a consistent backup. A closed database backup is always consistent. This is true for a databases running in the ARCHIVELOG or NOARCHIVELOG mode.

If you perform a backup of a database that is running in the NOARCHIVELOG mode when the database is in the MOUNT state, this will be considered a consistent backup. A database backup when the database is in the MOUNT state will always lead to a consistent backup. The reason for this is that the datafiles are not open in the MOUNT state and are therefore consistent.

Database Recovery

Item: 1 (Ref:1Z0-042.19.4.3)

On your PROD database, you discover that the datafile from the IND1 tablespace is missing. Your database instance has crashed.

Which approach should you take to recover the tablespace?

- Drop and re-create the tablespace.
- Restore the file from the previous backup and recover it.
- Use the flashback feature of the database to recover the datafile.
- Perform a complete database recovery to recover the IND1 tablespace datafile.
- Shut down the database, restore the complete database from backup, and perform a tablespace point-in-time recovery to recover the IND1 tablespace datafile.

Answer:

Restore the file from the previous backup and recover it.

Explanation:

To recover the tablespace, you should restore the file from the previous backup and recover it. In this scenario, you have lost a nonsystem critical datafile. Therefore, you can perform an open database recovery. The datafile can be restored from a previous backup and can be recovered by applying the archive redo log files, provided all the archive redo log from the backup to the current point in time are available.

The option stating you should drop and re-create the tablespace is incorrect because dropping the tablespace will result in the loss of all the data in the tablespace. The tablespace can be dropped and re-created if it contains only temporary data such as the temporary tablespace of the database. If the temporary tablespace datafile is lost, you must drop and re-create a temporary tablespace.

The option stating you should use the flashback feature of the database to recover the datafile is incorrect because the flashback feature cannot be used to flashback physical changes in the database. It can be used to recover database objects that have been changed at a particular point in time, if you want to view these objects in their unmodified state.

The option stating you should perform a complete database recovery to recover the IND1 tablespace datafile is incorrect because you are not required to perform a complete database recovery to recover a missing nonsystem critical datafile. A complete recovery must be performed if you are restoring all the datafiles from a previous backup in a database.

The option stating you should shut down the database, restore the complete database from backup, and perform a tablespace point-in-time recovery to recover the IND1 tablespace datafile is incorrect because you do not need to perform a tablespace point-in-time recovery in this scenario. A tablespace point-in-time recovery is used a recover one or more tablespaces to a non-current point in time.

Item: 2 (Ref:1Z0-042.19.1.2)

You are working on your PROD database that is running in the ARCHIVELOG mode. You have three multiplexed copies of control files. When your database instance was down, you lost one of the control files due to media failure.

Which statement correctly describes the state of the database in this scenario?

- The database will open.
- The database will not open.
- The database will open in the normal state.
- The database will open in the RESTRICTED mode.
- The database can be opened after creating a new control file.
- The database will have to be started by using the STARTUP FORCE command.

Answer:

The database will not open.

Explanation:

If you lose one of the multiplexed copies of your control file, your database will not open. Using the existing copies, the control file must be restored to the location where it originally existed. After this, the database can be started without any recovery. You can also modify the CONTROL_FILES parameter in the initialization parameter file of the database to delete the name of the missing control file. After this, you can start the instance without any recovery. If a multiplexed copy of a control file is lost when the database is running, the instance will abort.

The option stating that the database will open is incorrect because the database will not open.

The option stating that the database will open in the normal state is incorrect because the database will not open.

The option stating that the database will open in the RESTRICTED mode is incorrect because the database will not open.

The option stating that the database can be opened after creating a new control file is incorrect because the database is opened by restoring the control file from the existing multiplexed copies. You are not required to create a new control file.

The option stating that the database will have to be started using the STARTUP FORCE command is incorrect because the database cannot be started until the missing control file is restored.

Item: 3 (Ref:1Z0-042.19.2.2)

Your junior DBA has reported some discrepancies in the redo log files. You query the V$LOGFILE view to check the status of the redo log files. The STATUS column in the V$LOGFILE displays the value INVALID for the redo log member LOG\REDO01.LOG.

What does the INVALID status of the redo log file indicate?

- The redo log file LOG\REDO01.LOG is not being used.
- The redo log file LOG\REDO01.LOG is not the current log.
- The redo log file LOG\REDO01.LOG has never been written to.
- The contents of redo log file LOG\REDO01.LOG are incomplete.
- The redo log file LOG\REDO01.LOG is no longer needed for recovery.
- The redo log file LOG\REDO01.LOG is not accessible to the database.

Answer:

The redo log file LOG\REDO01.LOG is not accessible to the database.

Explanation:

The value INVALID in the STATUS column of the V$LOGFILE indicates that the file is lost or not accessible by the database.

The option stating that the redo log file LOG\REDO01.LOG is not being used is incorrect because this status of the redo log is not reflected in the V$LOGFILE view.

The option stating that the redo log file LOG\REDO01.LOG is not the current log is incorrect because if this is true, the status of the file in the V$LOG view will be ACTIVE.

The option stating that the redo log file LOG\REDO01.LOG has never been written to is incorrect because if this is true, the status of the file in the V$LOG view will be UNUSED.

The option stating that the contents of the redo log file LOG\REDO01.LOG are incomplete is incorrect because if this is true, the status of the file in the V$LOGFILE view will be STALE.

The option stating that the redo log file LOG\REDO01.LOG is no longer needed for recovery is incorrect because if this is true, the status of the file in the V$LOG view will be INACTIVE.

Item: 4 (Ref:1Z0-042.19.2.4)

You query the V$LOGFILE view and find that a redo log member from group 3 has a STATUS value of INVALID.

Which statement correctly describes the status of the log file?

- The file is inaccessible.
- The file is no longer used.
- The file has never been written to.
- The file can currently be written to.
- The file does not need to be archived.
- The file is no longer needed for instance recovery.

Answer:

The file is inaccessible.

Explanation:

When you query V$LOGFILE view, the STATUS value for a redo log member can be any of the following:

- NULL - The file is in use.
- INVALID - The file is inaccessible.
- DELETED - The file is no longer used.
- STALE - The contents of the file are incomplete.

Group 3 has a STATUS column value of INVALID. Therefore, the file is inaccessible.

The option stating that the file is no longer used is incorrect because the file is not accessible. If the file is not being used its status will be DELETED.

The option stating that the file has never been written to is incorrect because the file has been used earlier but is inaccessible now. If the redo log file has never been written to, the status of the redo log file will be UNUSED in the V$LOG view.

The option stating that the file can be currently written to is incorrect because the file is not accessible. If the file is currently in use, the status of the file will be null.

The option stating that the file does not need to be archived is incorrect because the STATUS value does not indicate whether the file has been archived.

The option stating that the file is no longer required for instance recovery is incorrect because this status is not reflected in the V$LOGFILE view. If the file is no longer required for instance recovery, the status of the corresponding group in the V$LOG view will be INACTIVE.

When you query the V$LOG view, the STATUS of a redo log group can be any of the following:

- UNUSED - The redo log group has never been written to.
- CURRENT - The group is the current redo log group.
- ACTIVE - The group is online and needed for instance recovery but is not being written to.
- INACTIVE - The group is online but is not needed for instance recovery.
- CLEARING - The log is being re-created as an empty log.
- CLEARING_CURRENT - The current log file is being cleared of a closed thread.

Item: 5 (Ref:1Z0-042.19.4.1)

The database of your company is running in the NOARCHIVELOG mode. You perform a complete backup of the database every night. On Monday morning, you lose the USERS1.DBF file belonging to the USERS tablespace. Your database has four redo log groups, and there have been two log switches since Sunday night's backup.

Which statement about the status of the database in this scenario is true?

- The database cannot be recovered.
- The database can be recovered up to the last commit.
- The database can be recovered only up to the last complete backup.
- The database can be recovered by performing an incomplete recovery.
- The database can be recovered by restoring only the USERS1.DBF datafile from the most recent backup.

Answer:

The database can be recovered up to the last commit.

Explanation:

In this scenario, the database can be recovered up to the last commit. A nonsystem datafile is lost, and you must recover the database. Although the database is in the NOARCHIVELOG mode, the redo log groups have not been overwritten because there are four redo log groups and there have been only two log switches since the last complete backup. To recover the database, you must restore the complete backup of the database and recover it by applying the redo logs generated after the last backup. If the redo logs had been overwritten, you would only have had the option of restoring the database from the complete backup of the previous night and opening it.

The option stating that the database cannot be recovered is incorrect because the database can be recovered from the last complete backup up to the last commit.

The option stating that the database can be recovered only up to the last complete backup is incorrect because the database can be recovered up to the last commit. The redo logs in the database have not been overwritten since the last complete backup. If the redo logs are overwritten because more than four log switches have occurred, then the database could only have been recovered up to the last complete backup.

The option stating that the database can be recovered by performing an incomplete recovery is incorrect because an incomplete recovery is not required in this scenario. An incomplete recovery is required when either an archive redo log is missing or the database must be recovered up to a particular SCN number.

The option stating that the database can be recovered by restoring only the USERS1.DBF datafile from the most recent backup is incorrect because you must restore the complete backup of the database and then apply the redo logs generated after the last backup.

Item: 6 (Ref:1Z0-042.19.1.3)

While trying to open your database you receive the following error:

ORA-00205: error in identifying controlfile

Upon analyzing the database logs, you determine that you have lost all the control files in your database. However, you had created a control file script 20 days ago and two datafiles have been added to the database in the last 20 days.

What should you do to recover the database in this scenario?

- Perform a complete recovery up to the last complete backup.
- Do nothing. Opening the database will recover the control file through instance recovery.
- Restore the control file script to the location where the control file was originally located and start the database.
- Open the database in the NOMOUNT state and create a control file using the control file script. Then, open the database.
- Modify the control file script to reflect the newly-added datafiles, open the database in the NOMOUNT state, and re-create the control file from the modified script file.
- Restore the last full backup, create a control file from the control file script, and perform a complete recovery by applying all the archive logs up to the point of failure.

Answer:

Modify the control file script to reflect the newly-added datafiles, open the database in the NOMOUNT state, and re-create the control file from the modified script file.

Explanation:

You should modify the control file script to reflect the newly-added datafiles, open the database in the NOMOUNT state, and re-create the control file from the modified script file. In the given scenario, the control file has been lost, and you have a control file script from the time when the database structure was different from the current structure. Therefore, you must modify the control file script to reflect the newly-added datafiles, open the database in NOMOUNT state and re-create the control file from the modified script file. You can then open the database without performing any recovery on the database. The newly-created control file will contain all the information about structural changes in the database. If you have a similar scenario and you have a binary backup of the control file, you must restore the backup of the control file to the correct location and then open the database to the MOUNT state using this binary backup. After the database is open in the MOUNT state you can create a control file script, which can then be edited to reflect the structural changes in the database. This edited control file script can be used to re-create the control file that will contain all the structural changes made to the database. No recovery will be needed in this scenario either.

The option stating you should perform a complete recovery up to the last complete backup is incorrect because this will lead to loss of data modified after the last complete backup.

The option stating you should do nothing and opening the database will recover the control file through instance recovery is incorrect because the database will not recover the control file through instance recovery. Instance recovery is a process of recovering the database after an instance crash. This recovery involves rollback of uncommitted data and roll forward of the committed data that was not written to the datafiles because of the instance crash.

The option stating you should restore the control file script to the location where the control file was located and start the database is incorrect because the control file script cannot be used to start the database. The control file script can only be used to create a control file.

The option stating you should open the database in the NOMOUNT state and create a control file using the control file script and then open the database is incorrect. This is because creating a control file from the control file script without editing the script to reflect the new changes will create a control file that will not have the new changes incorporated in it. The new changes in this scenario refer to the addition of two datafiles that was done after creation of the control file script. The datafiles were added after the control file script was created. Therefore, the control file script does not have information about these datafiles. To incorporate these changes the control file script must be edited and the new information added to it.

The option stating you should restore the last full backup, create a control file from the control file script, and then perform a complete recovery by applying all the archive logs up to the point of failure is incorrect because you do not need to apply the archive redo logs in this scenario. You apply the archive redo logs to the datafiles to make them consistent with the database. Archive redo logs are not applied to the control files.

Item: 7 (Ref:1Z0-042.19.2.1)

Your database, PROD, is running in the ARCHIVELOG mode. You back up the datafiles and archive redo logs in the database every night. As a result of a media failure, one group member from the redo log group 2 has become corrupt. The database does not halt because the other members from the group are still available.

Which two methods can be used to recover the lost online redo log member? (Choose two.)

- Perform a recovery using RMAN.
- Perform a complete recovery after shutting down the database.
- Recover the lost redo log member from the most recent backup.
- Restore the missing log member by copying one of the remaining log files from the same group.
- Drop the redo log member and re-create it by using the ALTER DATABASE...ADD LOGFILE MEMBER statement.

Answer:

Restore the missing log member by copying one of the remaining log files from the same group.

Drop the redo log member and re-create it by using the ALTER DATABASE...ADD LOGFILE MEMBER statement.

Explanation:

If a redo log member is lost while the database is running, the database will not halt if the other members of the redo log group are available. The redo log can be recovered by using two methods. The redo log can be restored by copying one of the remaining log files from the same group. The redo log can also be dropped and then re-created by using the ALTER DATABASE...ADD LOGFILE MEMBER statement.

The option to perform a recovery using RMAN is incorrect because no recovery is required to recover a redo log file member if other members of the redo log group are available.

The option to perform a complete recovery after shutting down the database is incorrect because no recovery is required to recover a redo log file member if the other members of the redo log group are available.

The option to recover the lost redo log member from the most recent backup is incorrect because you do not have a backup of the redo log. Oracle recommends that you do not back up the online redo logs in a database.

Item: 8 (Ref:1Z0-042.19.3.2)

The database of your company is running in the ARCHIVELOG mode. The SYSTEM tablespace in the database has been corrupted, and you have a 30-day-old consistent backup of the database that was running in the NOARCHIVELOG mode. All the archive redo logs from the last 30 days are available to you.

Which statement is true in this scenario?

- The database cannot be recovered.
- The database can be recovered only by using RMAN.
- The database can be recovered up to the last 30 days.
- The database can be recovered to the point of the last complete backup.
- The database can be recovered up to the last commit by performing a complete recovery.

Answer:

The database cannot be recovered.

Explanation:

In this scenario, the database cannot be recovered. You have lost the datafile of the SYSTEM tablespace, and you do not have any backup of the datafile from the database that was in the ARCHIVELOG mode. Therefore, the database cannot be recovered. The database cannot be recovered using the 30-day-old backup because the backup was taken when the database was in the NOARCHIVELOG mode, and a backup of the NOARCHIVELOG mode cannot be used to recover a database running in the ARCHIVELOG mode. To recover a SYSTEM tablespace, the backup of your datafile must be in the mode in which the database is operating. All the archive redo logs since the backup should also be available to you.

The option stating that the database can be recovered only by using RMAN is incorrect because you cannot recover the database by using RMAN. RMAN can be used to recover the database if RMAN contains a complete backup of all the datafiles in the database. In this scenario, RMAN cannot use a backup that was taken when the database was running in the NOARCHIVELOG mode.

The option stating that the database can be recovered up to the last 30 days is incorrect because the database cannot be recovered.

The option stating that the database can be recovered to the point of the last complete backup is incorrect because the database cannot be recovered. The database can be recovered up to the point of the last complete backup if the backup is taken in the same mode in which the database is currently running.

The option stating that the database can be recovered up to the last commit by performing a complete recovery is incorrect because a complete recovery cannot be performed on the database unless a valid, complete backup of the database is available to you.

Item: 9 (Ref:1Z0-042.19.1.1)

Your database has been opened using the static initialization parameter file. In this database instance, suspecting bad sectors on the disk where the control file is located, you decide to relocate the control file to a different disk.

What should be the state of the database to allow you to relocate a control file?

- OPEN
- MOUNT
- CLOSED
- NOMOUNT

Answer:

CLOSED

Explanation:

The control file can be relocated when the database is in the CLOSED state. After the control file is relocated using operating system commands, the initialization parameter file must be updated with the new location of the control file before opening the database. Even if you are using multiple copies of control files on your database, the control file cannot be relocated without shutting down the database because the database has been started using the static initialization parameter file. Using the static initialization parameter file, the parameter CONTROL_FILES cannot be modified when the database is running. To update the parameter, you must shut down the database, relocate the control file using OS utilities and then update the CONTROL_FILES parameter in the initialization parameter file.

A control file cannot be relocated when the database is in the OPEN state because the control file is already being accessed when the database is open.

A control file cannot be relocated when the database is in the MOUNT state because the control file is already being accessed after the database is mounted. Oracle does not allow relocation of control files that are currently being accessed. To relocate control files, you must shut down the database.

A control file cannot be renamed when the database is in the NOMOUNT state because the initialization parameter file cannot be updated with the new name of the control file while the database is in this state.

Item: 10 (Ref:1Z0-042.19.4.2)

The database of your company is running in the ARCHIVELOG mode. Due to a media failure, the EXAMPLE.DBF datafile belonging to the EXAMPLE tablespace has been corrupted.

What will be the status of the EXAMPLE tablespace in this scenario?

- The tablespace will go offline.
- The tablespace will become read-only.
- The tablespace will be available for use.
- The tablespace must be recovered before it can be used.

Answer:

The tablespace will be available for use.

Explanation:

In this scenario, the EXAMPLE tablespace will be available for use. If a datafile from a tablespace is lost due to media failure, only the datafile will reach the offline stage. The tablespace will continue to be available to the users. However, the data contained in the lost datafile will not be accessible. The other datafiles in the tablespace will be online and can be accessed. The database will also remain open and operational if a nonsystem-critical datafile is lost.

The EXAMPLE tablespace will not go offline. Only the missing datafile will be offline.

The EXAMPLE tablespace will not become read-only because to make a tablespace read-only you must issue the ALTER TABLESPACE statement with the READ ONLY clause. In the given scenario, the tablespace will remain online, only the data stored in the lost datafile will not be accessible.

The EXAMPLE tablespace does not need to be recovered before it can be used. The tablespace will continue to be available. Only the missing datafile must be recovered so that it can be used.

Item: 11 (Ref:1Z0-042.19.2.3)

The disk on which your redo log file is located is corrupted. As a result, you decide to relocate the redo log file to a different disk.

After you shut down the database, which actions can you take to relocate the redo log file in your database?

- Use the OS commands to move the file, and then update the parameter file.
- Mount the database and issue the `ALTER DATABASE` statement to move the file, and then update the control file.
- Mount the database, use OS commands to move the file, and issue the `ALTER DATABASE...RENAME FILE` statement.
- Use the OS commands to move the file, mount the database, and issue the `ALTER DATABASE...RENAME FILE` statement.
- Copy the existing redo log file to the desired location by using OS commands. Then, restart the instance and use the `ALTER SYSTEM` statement to update the control file.

Answer:

Use the OS commands to move the file, mount the database, and issue the `ALTER DATABASE...RENAME FILE` statement.

Explanation:

You can relocate a redo log file in your database by adding a new log file and dropping the old log file or by using the `ALTER DATABASE...RENAME FILE` statement. To use the `ALTER DATABASE...RENAME FILE` statement, you should:

1. Shut down the instance.
2. Use the OS commands to move the file.
3. Mount the database.
4. Issue the `ALTER DATABASE...RENAME FILE` statement to update the control file. The new file must exist before you issue this statement or the statement will fail.
5. Open the database.

The option to use the OS commands to move the file, and then update the parameter file is incorrect because you do not need to edit the parameter file to relocate a redo log file in your database.

The option to mount the database and issue the `ALTER DATABASE` statement to move the file and update the control file is incorrect because you do not use the `ALTER DATABASE` statement to move the file. The files are moved by using the OS commands. In addition, the `ALTER DATABASE...RENAME FILE` statement is used to update the control file.

The option to mount the database, use the OS commands to move the file, and issue the `ALTER DATABASE...RENAME FILE` statement is incorrect because the files should be moved before mounting the database.

The option that states that you must use the `ALTER SYSTEM` statement to update the control file is incorrect because the `ALTER DATABASE...RENAME FILE` statement is used to update the control file.

Item: 12 (Ref:1Z0-042.19.3.3)

The database of your company is running in the ARCHIVELOG mode. The following configuration applies to the database:

TEMPTS - temporary tablespace
UNDOTBS - undo tablespace
SYSTEM - system tablespace
SYSAUX - tablespace auxiliary to SYSTEM tablespace
IND1 - index tablespace
USERS - default permanent tablespace

Datafiles belonging to which two tablespaces CANNOT be recovered without closing the database? (Choose two.)

- [ ] IND1
- [ ] USERS
- [ ] TEMPTS
- [ ] SYSTEM
- [ ] SYSAUX
- [ ] UNDOTBS

Answer:

SYSTEM
UNDOTBS

Explanation:

The SYSTEM and UNDOTBS tablespace datafiles cannot be recovered without closing the database. If any of the datafiles of these two tablespaces are damaged or lost, the datafiles can be recovered only after the database is shut down.

The IND1 tablespace datafiles can be recovered without closing the database because an index tablespace can be recovered without shutting down the database by performing an open database recovery.

The USERS tablespace datafiles can be recovered without closing the database because the datafiles belonging to the default permanent tablespace of the database can be recovered without shutting down the database by performing an open database recovery.

The TEMPTS tablespace datafiles can be recovered without closing the database because the datafiles of the temporary tablespace of the database can be recovered without shutting down the database by performing an open database recovery.

The SYSAUX tablespace datafiles can be recovered without closing the database because the SYSAUX tablespace datafiles in the database can be recovered without shutting down the database by performing an open database recovery.

Item: 13 (Ref:1Z0-042.19.2.5)

There are two redo log groups in your database, and you maintain two multiplexed copies of the redo log members. Both the members of the active online redo log group 2 are damaged as a result of block corruption, and the database activity has come to a halt. You issue the following statement to resolve the problem:

```
SQL> ALTER DATABASE CLEAR LOGFILE GROUP 2;
```

Which statement is true in this scenario?

- The redo log group should be archived.
- The redo data stored in this redo log group will be lost.
- The redo log group cannot be used after you issue this statement.
- The sequence of the redo logs will be reinitialized after you issue this statement.
- The backup of the database before issuing this statement cannot be used to perform a recovery.

Answer:

The redo log group should be archived.

Explanation:

When you issue this statement to clear the log group, the redo log group will be cleared and reinitialized. When this statement is issued to clear the log group, the log group should be archived to enable the database control to allow you to clear the log group. If the log group is not archived, you cannot use this statement to clear the log group. You can use the following statement to clear the log group 2 if it has not been archived:

```
SQL> ALTER DATABASE CLEAR UNARCHIVED LOGFILE GROUP 2;
```

This statement will clear the log group that has not been archived. After this statement is issued, the corrupted log group is cleared and reinitialized for use. Clearing an unarchived redo log group breaks the sequence of redo information in the database because the redo information contained in the unarchived redo log group is lost. Therefore, you must immediately take a backup of the database after clearing an unarchived log group.

The redo data stored in this redo log group will not be lost because the redo log group is already archived when you issue this statement. The redo data in the redo log file will be lost if you clear a log file that is not yet archived.

The redo log group can be used after you issue this statement because the redo log will be cleared and reinitialized for use.

The sequence of the redo log files will not be reinitialized after you issue this statement. The sequence of the redo logs will be reinitialized when you open a database after a recovery by using the `RESETLOGS` option.

The backup of the database before issuing this statement can be used to perform a recovery. The backup of the database will be rendered unusable when you clear an unarchived redo log group. Clearing an unarchived redo log group breaks the sequence of the redo information in the database because the redo information contained in the unarchived redo log group is lost. The backup before issuing the statement to clear an unarchived redo log group is rendered unusable, and you must immediately take a backup of the database after clearing an unarchived log group.

Item: 14 (Ref:1Z0-042.19.3.4)

The database of your company is running in the ARCHIVELOG mode. You lost one of the SYSTEM datafiles of the database due to hardware failure. You are required to recover the database after this failure.

Which sequence of actions should you take to recover the database?

- Perform a complete database import.
- Restore the datafile and recover the database by performing an open database recovery.
- Restore the datafile from the most recent backup. Mount the database and recover the tablespace.
- Mount the database, re-create the file by using the ALTER DATABASE CREATE DATAFILE statement, and recover the database.
- Restore the database from the most recent backup, mount the database, and recover the database by performing a complete database recovery.
- Restore the datafile from the most recent backup. Mount the database and recover the tablespace by performing a tablespace point-in-time recovery.

Answer:

Mount the database, re-create the file by using the ALTER DATABASE CREATE DATAFILE statement, and recover the database.

Explanation:

To recover the database, you should restore the datafile from the most recent backup, mount the database, and recover the tablespace. In this scenario, a datafile is lost from the SYSTEM tablespace. Therefore, you cannot perform an open database recovery. The database will crash if a system datafile is missing. Therefore, to recover the database, you must use the closed database recovery technique. Using the closed database recovery technique, you restore the SYSTEM datafile from a recent backup, mount the database, and then recover the tablespace. The changes made to the database after the backup will be applied to the backup of the datafile to make the datafile consistent with the current state of the database. After this, the database can be opened.

The option stating you should perform a complete database import is incorrect because performing a complete import will lead to the loss of the data that was inserted into the database after the export was performed.

The option stating you should restore the datafile and recover the database by performing an open database recovery is incorrect because you cannot perform an open database recovery on a database when the datafile belonging to the SYSTEM tablespace or the undo tablespace becomes unavailable.

The option stating you should mount the database, re-create the file by using the ALTER DATABASE CREATE DATAFILE statement, and recover the database is incorrect because the ALTER DATABASE CREATE DATAFILE statement cannot be used to create a datafile belonging to the SYSTEM tablespace.

The option stating you should restore the database from the most recent backup, mount the database, and recover the database by performing a complete database recovery is incorrect because you do not need to restore the complete backup of the database if only one datafile is missing. A complete database is restored when most of the datafiles are missing. In all other scenarios, you should perform an incomplete recovery.

The option stating you should restore the datafile from the most recent backup, mount the database, and recover the tablespace by performing a tablespace point-in-time recovery is incorrect because you do not need to perform a tablespace point-in-time recovery in this scenario. Tablespace point-in-time recovery involves recovery of one or more non-SYSTEM tablespaces to a non-current time.

Item: 15 (Ref:1Z0-042.19.3.1)

The database of your company is running in the NOARCHIVELOG mode. Due to a hard disk failure, a datafile of your SYSTEM tablespace is corrupted and your database instance has crashed.

Up to which point in the past can you recover the SYSTEM tablespace?

- up to the last commit
- up to the last log switch
- up to the last complete cold backup
- up to the point of the database crash
- The SYSTEM tablespace cannot be recovered.

Answer:

up to the last complete cold backup

Explanation:

You can recover the SYSTEM tablespace up to the last complete cold backup. When the SYSTEM tablespace datafile is lost and your database is running in the NOARCHIVELOG mode, the SYSTEM tablespace can be recovered only up to the last complete backup. In the NOARCHIVELOG mode, you can recover the database only up to the last complete cold backup.

You cannot recover the SYSTEM tablespace up to the last commit because to recover a database up to the last commit, you must perform an incomplete recovery. You cannot perform an incomplete recovery in a database that is running in the NOARCHIVELOG mode.

You cannot recover the SYSTEM tablespace up to the last log switch because to recover a database up to the last log switch, you must perform an incomplete recovery. You cannot perform an incomplete recovery in a database that is running in the NOARCHIVELOG mode.

You cannot recover the SYSTEM tablespace up to the point of the database crash because you cannot recover a database up to the point of the crash. When you perform a recovery on a database running in the NOARCHIVELOG mode the database can be recovered only up to the last complete backup because the redo log files generated after the complete backup will be overwritten in a database in running in the NOARCHIVELOG mode. Without these redo log files, you can perform a recovery only up to the last complete backup.

The option stating that the SYSTEM tablespace cannot be recovered is incorrect because the database can be recovered up to the last complete cold backup.