Total Questions: 107
Latest Version: 6.1

Question: 1

Which two are true about database roles in an Oracle Data Guard configuration?

A. A Physical Standby Database can be converted into a Logical Standby Database.
B. A Snapshot Standby Database can be a fast-start failover target.
C. A Logical Standby Database can be converted to a Snapshot Standby Database.
D. A Logical Standby Database can cascade redo to a terminal destination.
E. A configuration consisting only of a primary and one or more physical standby databases can support a rolling release upgrade.

Answer: A, E

Explanation:
A Physical Standby Database can indeed be converted into a Logical Standby Database, providing flexibility in a Data Guard configuration. This allows for the database to switch roles and supports SQL apply operations, enabling more granular control over the data and transactions being replicated and applied. Additionally, having a configuration with a primary database and one or more physical standby databases allows for rolling upgrades to be performed. This means that each database in the Data Guard configuration can be upgraded in a phased manner, minimizing downtime and ensuring high availability during the upgrade process
.

Question: 2

You must design an Oracle Data Guard configuration for a DSS database that meets these permanent
requirements:
1. Creating and maintaining bitmap indexes should not impact the performance of the primary database.
2. Creating and maintaining materialized views should not impact the performance of the primary database.
Additionally, there are these requirements, only one of which is ever done at any one time:
1. It should be possible to apply designated patches with a minimum amount of downtime.
2. Upgrading to a new database release should be performed with the least possible amount of downtime.

3. New application software releases should be tested against an exact and up-to-date replica of the primary database.
Which configuration meets these requirements with the fewest of databases?

A. a primary database with one logical standby database
B. a primary database with two logical standby databases
C. a primary database with one physical standby database
D. a primary database with two physical standby databases
E. A primary database with one logical and one physical standby database

Answer: A

Explanation:
Logical standby databases allow the execution of DDL and DML operations, which makes them suitable for maintaining bitmap indexes and materialized views without affecting the performance of the primary database .
Logical standby databases can be used for performing rolling upgrades and patching with minimum downtime, meeting another requirement .
They also enable the testing of new application software releases against an up-to-date replica of the primary database, fulfilling the last requirement.
Other configurations involving physical standby databases or combinations of logical and physical standby databases might not meet all the specified requirements as efficiently or with the same level of performance isolation for the primary database.

Question: 3

You created two remote physical standby databases using SQL and RMAN.
The primary database is a four-instance RAC database and each physical standby database has two instances.
Roles-based services are used for client connectivity and have been defined in the Grid Infrastructure.
Consider these operational requirements:
- The ability to manage multiple standby databases with a single tool
- The simplification of switchovers, failovers, reinstatements, and conversions to and from snapshot standby databases
- The automation of failovers to a specified target standby database

Which TWO tools can be used to fulfill these requirements7

A. RMAN
B. SQL*Plus
C. CRSCTL
D. Enterprise Manager Cloud Control
E. DGMGRL
F. SRVCTL
G. GDCCTL

Answer: D, E

Explanation:
Enterprise Manager Cloud Control provides a graphical interface to manage multiple standby databases, simplify switchovers and failovers, and automate failover processes to a specified target standby database. It offers a comprehensive view and control over the Data Guard configuration, making complex operations more manageable.
DGMGRL is a command-line tool specifically designed for managing Data Guard configurations. It allows the administration of multiple standby databases, simplifies the execution of switchovers and failovers, reinstatements, and conversions to and from snapshot standby databases, and supports the automation of failover processes to a specified standby database.
Other options like RMAN, SQL*Plus, CRSCTL, SRVCTL, and GDCCTL do not provide the same level of integrated management functionality for Data Guard environments as Enterprise Manager Cloud Control and DGMGRL.

Question: 4

The Oracle database 19c Observer is currently running on host1 and you wish to have it running on host2.
Examine this list of possible steps:
1) Stop the observer on host1
2) Disable Fast-Start Failover
3) Update the broker configuration with the new observer hostname
4) Enable Fast-Start Failover
5) Start the Observer on host2
Which contains the minimum required steps to move the observer to host2?

A. Execute tasks 1 and 5
B. Execute only task 5
C. Execute tasks 1, 3, and 5
D. Execute tasks 1, 2, 3, 4, and 5

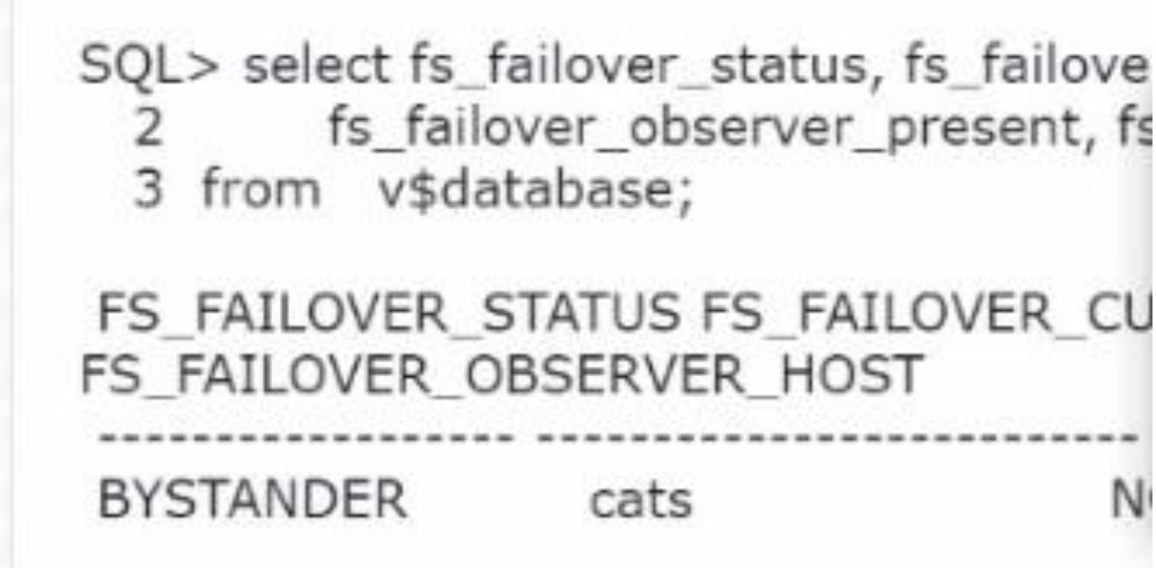
Answer: C

Explanation:
Stop the Observer on host1 to ensure that there are no conflicts between the instances of the Observer running on different hosts.
Update the Data Guard Broker configuration with the new hostname for the Observer. This step is crucial to redirect the Data Guard Broker to communicate with the Observer on the new host.
Start the Observer on host2 to resume its operations in the new environment.
Disabling and re-enabling Fast-Start Failover (steps 2 and 4) are not strictly necessary for moving the Observer to a new host. These steps would be more relevant if changes to the configuration

of Fast-Start Failover itself were required, which is not the case when simply relocating the Observer.

Question: 5

Examine this query and its output:



```
SQL> select fs_failover_status, fs_failove
  2        fs_failover_observer_present, fs
  3  from   v$database;

 FS_FAILOVER_STATUS FS_FAILOVER_CU
FS_FAILOVER_OBSERVER_HOST
 ---------------- ----------------------
 BYSTANDER          cats                N
```

Which two statements are true?

A. The master observer is connected to the database on which the query was executed.
B. The master observer is currently running on ol7.example.com.
C. The master observer is not running, but should run on ol7.example.com.
D. Cats is a bystander database.
E. The master observer is not connected to the database on which the query was executed.

Answer: D, E

Explanation:
D . The database role indicated by FS_FAILOVER_STATUS as BYSTANDER implies that the database is a standby database in the Data Guard configuration. This means the database is neither a primary database nor an active failover target.
E . Since the FS_FAILOVER_OBSERVER_HOST column shows cats, it suggests that this is the host on which the observer would run. However, because the FS_FAILOVER_OBSERVER_PRESENT column is not shown, we cannot definitively state if the observer is currently connected or not. If FS_FAILOVER_OBSERVER_PRESENT is 'YES', the observer is connected, if 'NO', then it's not. In the absence of this column's output, the best assumption based on the available data is that the observer is not connected.
The output shows that the FS_FAILOVER_STATUS is BYSTANDER, which indicates that the database in question is not actively involved in a fast-start failover configuration as a primary or standby. It is in a bystander role, meaning that while it is part of a Data Guard configuration, it is

neither a target for failover nor actively participating in failover operations. Additionally, FS_FAILOVER_OBSERVER_HOST shows 'cats', which indicates the host where the observer process is expected to run. However, since there is no information about the observer being present, we can infer that although 'cats' is designated for the observer to run, the observer is not currently connected to this database.

Reference

Oracle documentation on Data Guard configurations and the V$DATABASE view which provides information about the fast-start failover status and observer host.

Question: 6

Which three statements are true……. With no Oracle Streams or Goldengate configured?

A. It is recommended to have them on the...
B. Only standby databases can write redo....
C. The LGWR process writes to them on ....
D. They are required on a logical standby for real-time apply
E. They are required on a physical standby for real-time apply.
F. They are required only for synchronous redo transport

Answer: C, D, E

Explanation:

C . The LGWR (Log Writer) process is responsible for writing redo entries from the redo log buffer to the online redo log files on the primary database. This is a fundamental process in the Oracle Database architecture, ensuring that all changes made to the database are captured for purposes such as recovery, replication, and high availability.

D . Real-time apply on a logical standby database requires standby redo log files. The standby redo log files are used to store redo data received from the primary database before it is applied to the logical standby database. This enables the logical standby to apply changes as they are received, without waiting for the current redo log file to be archived.

E . Similarly, on a physical standby database, standby redo log files are used for real-time apply. They store redo data from the primary database, allowing the physical standby to apply redo data concurrently as it is received, rather than waiting for redo log files to be archived. This capability is crucial for maintaining a physical standby database that is closely synchronized with the primary database with minimal lag.

These functionalities are integral to Oracle Data Guard configurations and are not dependent on Oracle Streams or Oracle GoldenGate, which are separate technologies for data replication and integration.

Question: 7

Which THREE statements are true........ open in real time query mode, which becomes a new.

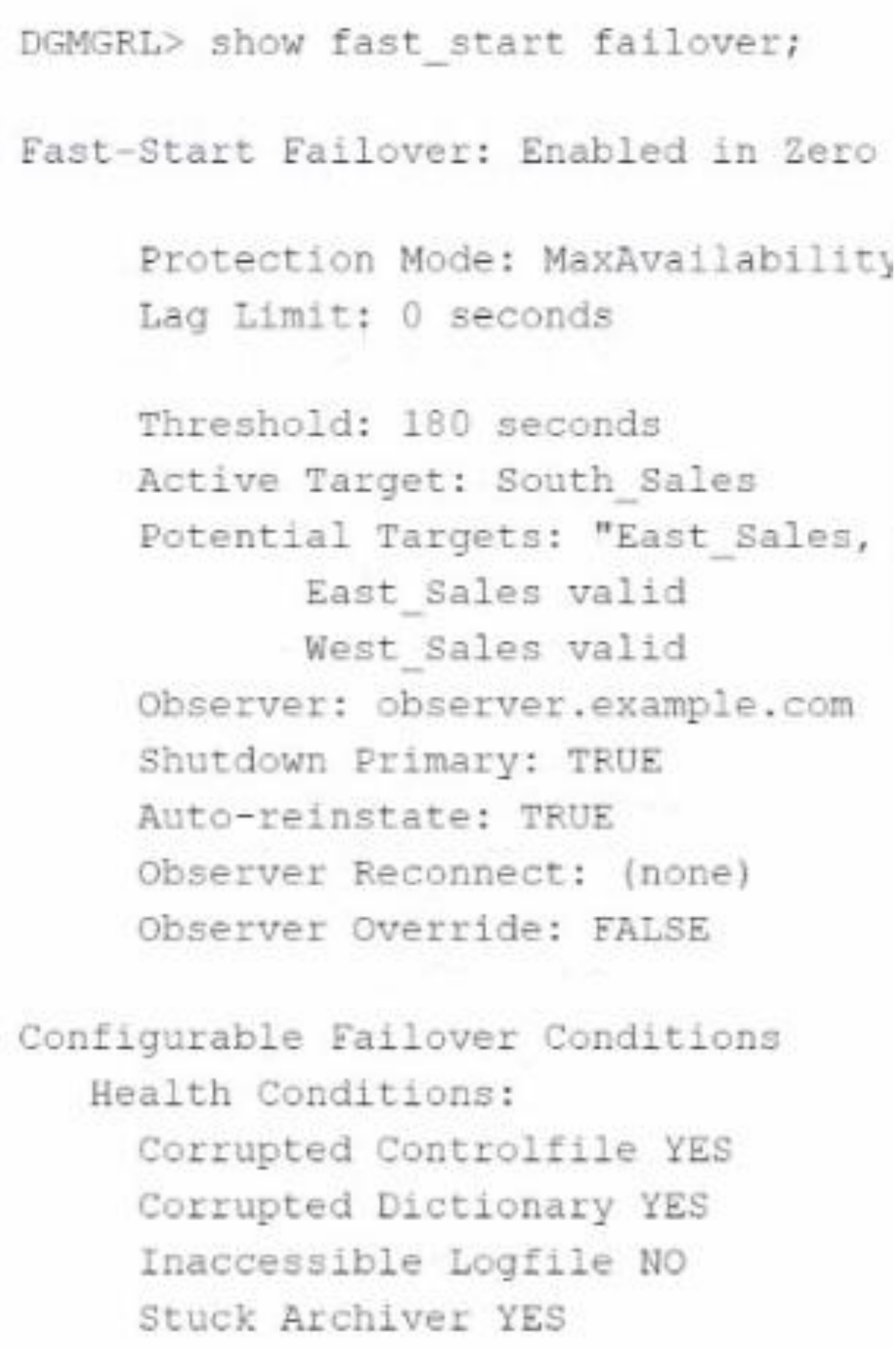
A. All sessions are disconnected and all
B. Sessions that are using database links
C. All current buffers can be retained.
D. Sessions that have long running queries can be retained.
E. User sessions and Current Buffers are maintained by default.
F. User sessions can be retained.

Answer: A, C, F

Explanation:
When a physical standby database is opened in real-time query mode, which may be referred to as real-time apply when using Active Data Guard, certain operations can disrupt ongoing sessions. However, with features like Application Continuity and the proper configuration of initialization parameters such as STANDBY_DB_PRESERVE_STATES, user sessions and current buffers may be preserved during role transitions such as a switchover or failover. Specifically, the STANDBY_DB_PRESERVE_STATES parameter can be set to preserve none, all, or only user sessions during such transitions. This ensures that in-flight transactions are not lost and that users do not experience disruptions during the role transitions of a physical standby database.
Reference
Oracle Data Guard Concepts and Administration
Oracle Database Licensing Information User Manual
Oracle Data Guard Broker User Manual

Question: 8

Examine the fast-start failover configuration:



```
DGMGRL> show fast_start failover;

Fast-Start Failover: Enabled in Zero

     Protection Mode: MaxAvailabilit
     Lag Limit: 0 seconds

     Threshold: 180 seconds
     Active Target: South_Sales
     Potential Targets: "East_Sales,
            East_Sales valid
            West_Sales valid
     Observer: observer.example.com
     Shutdown Primary: TRUE
     Auto-reinstate: TRUE
     Observer Reconnect: (none)
     Observer Override: FALSE

Configurable Failover Conditions
   Health Conditions:
     Corrupted Controlfile YES
     Corrupted Dictionary YES
     Inaccessible Logfile NO
     Stuck Archiver YES
```

A. A failover may occur if the observer has lost connectivity to the primary database, even if the Fast-Start Failover target standby database has a good connection to the primary database
B. If South_Sales develops a problem and cannot be the target of a failover, the broker automatically changes the fast-start failover target to one of the other candidate targets.
C. The observer will initiate a failover when the primary database is unable to produce local archived redo log files.
D. You must disable fast-start failover first to change the fast-start failover target to East sales.
E. The observer is running.

Answer: A, C, E

Explanation:

Question: 9

You must configure on Oracle Data ....
1. A primary database
2. Three Physical Standby Databases
Examine these requirements:
A designated physical standby database should become the primary database automatically whenever the primary database fails.
2. The chosen protection mode should provide the highest level of protection possible without violating the other requirement.
Which redo transport mode and protection mode would you configure to meet these requirements?

A. FASTSYNC and Maximum Protection
B. ASYNC and Maximum Performance
C. FASTSYNC and Maximum Availability
D. SYNC and Maximum Protection

Answer: C

Explanation:
To meet the requirements of automatic failover and the highest level of protection without data loss, the combination of FASTSYNC redo transport mode and Maximum Availability protection mode is appropriate. FASTSYNC ensures that the performance impact on the primary database is minimized while still providing synchronous transport. Maximum Availability protection mode offers the highest level of data protection without compromising the availability of the primary database. In case of a network failure or a standby failure, the primary will not halt, avoiding disruption to the primary database operations.
Reference

Oracle Data Guard Concepts and Administration guide, which details the different protection modes and their respective levels of data protection and impact on database operations.

Question: 10

You must configure an Oracle Data……….
1. A primary database
2. A physical standby database
Examine these requirements: 1. Data loss is not permitted.
1. Data loss is not permitted.
2. It should be possible to convert the physical standby database to a snapshot standby database.
3. Under normal operations, transactions should commit when redo is written to disk on the primary database and as soon as it has been received by the standby database instance.
4. The availability of the primary database should not be compromised by the availability of the standby database.
5. It should be possible to convert the physical standby database to a logical standby database
6. It should be possible to deploy Real Application Clusters on the primary database.
7. It should be possible to deploy Real Application Clusters on the physical standby database.
You configure SYNC redo transport mode in combination with Maximum Protection mode.

A. 1, 2, 3, 6, and 7
B. 1, 2, 3, 4, 5, 6, and 7
C. 1, 2, 6, and 7
D. 1, 6, and 7
E. 1, 2, and 5

Answer: B

Explanation:
When SYNC redo transport mode is combined with Maximum Protection mode, it ensures that no data loss will occur (requirement 1). The physical standby can be converted to a snapshot standby (requirement 2) and later to a logical standby database (requirement 5), satisfying both transformation requirements. Transactions commit as soon as redo data is received by the standby database (requirement 3). The availability of the primary is not dependent on the standby database in Maximum Protection mode, as the primary database will halt if the standby cannot acknowledge the redo (requirement 4), thus indirectly ensuring its availability. It is also possible to deploy Real Application Clusters on both the primary (requirement 6) and the physical standby database (requirement 7), providing high availability and scalability.
Reference

Oracle Data Guard documentation detailing the requirements for different database roles, protection modes, and redo transport modes, as well as the capabilities and limitations of each configuration.

Question: 11

Which three types of backups offload …….. with the primary database in a data Guard

A. Control files
B. Broker configuration files
C. Password files
D. Data files
E. Online logs
F. Archive logs

Answer: A, D, F

Explanation:
In a Data Guard environment, you can offload the backups of certain database components to a physical standby database. Incremental backups of a standby database are interchangeable with the primary database, meaning you can apply a backup taken on a standby database to a primary database and vice versa. This includes control files, data files, and archive logs. Backups of control files and nonstandby control files are interchangeable. You can restore a standby control file on a primary database and a primary control file on a physical standby database, demonstrating their interchangeability and the ability to offload control file backups to one database in a Data Guard environment.

Question: 12

In Oracle Database 19c, you can set the value of database initialization parameters in a database using
the EDIT DATABASE... SET PARAMETER Command:
DGMGRL> EDIT DATABASE 'boston' SET PARAMETER log_archive_trace - 1;
Which THREE statements are TRUE about the command?

A. The EDIT DATABASE PARAMETER command can be used to set the value of a static parameter in a database.
B. The edit database parameter command can only be used to modify the value of a dynamic parameter in a database.
C. The database must be available when the above command is run.
D. The value set using this command is directly stored in the broker configuration file.
E. The value set using this command is directly applied to the boston database.

Answer: B, C, E

Explanation:
The EDIT DATABASE...SET PARAMETER command in Data Guard Management (DGMGRL) is used to modify the value of initialization parameters for a database within a Data Guard configuration. This command can be used to modify both static and dynamic parameters, but if a static parameter is changed, the new value will take effect only after the database is restarted. The database must be up and running for the command to execute, and the values set using the command are directly applied to the specified database (in this case, 'boston') .

Question: 13

Your Data Guard environment consists of these components and settings:
1. A primary database
2. Two remote physical standby databases
3. The redo transport mode is set to sync
4. Real-time query is enabled for both standby databases
5. The DB_BLOCK_CHECKING parameter is set to TRUE on both standby databases
You notice an increase in redo apply lag time on both standby databases.
Which two would you recommend to reduce the redo apply lag on the standby databases?

A. Increase the size of standby redo log files on the standby databases.
B. Decrease the redo log file size on the primary database.
C. Increase the number of standby redo log files on the standby databases.
D. Lower DB_BLOCK_CHECKING to MEDIUM or low on the standby databases.
E. Increase the size of the buffer cache on the physical standby database instances.

Answer: A, D

Explanation:
To reduce the redo apply lag on standby databases, one could increase the size of the standby redo log files. Larger redo log files can accommodate more redo data, which may reduce the frequency of log switches and allow for more continuous application of redo data. Additionally, lowering the DB_BLOCK_CHECKING parameter to MEDIUM or LOW on the standby databases can help improve redo apply performance. High block checking can impose additional CPU overhead during the application of redo data, potentially increasing apply lag times. By reducing the level of block checking, you can lessen this overhead and help reduce the apply lag .

Question: 14

Your Data Guard environment consists of these components and settings:
1. A primary database
2. A remote physical standby database
3. Real-time query is enabled.
4. The redo transport mode is set to SYNC.

5. The protection mode is set to Maximum Availability.
You notice that queries executed on the physical standby database receive errors: ORA-03172: STANDBY_MAX_DATA_DELAY of 15 seconds exceeded. Which two would you recommend to avoid this error?

A. Increase the size of the buffer cache on the standby database instance.
B. Reduce I/O latency for the storage used by the primary database.
C. Increase the number of standby redo log files on the primary database.
D. Change the protection mode to Maximum Performance.
E. Increase the network bandwidth between the primary and standby databases.
F. Change the protection mode to Maximum Protection.

Answer: B, E

Explanation:
The ORA-03172: STANDBY_MAX_DATA_DELAY error indicates that the real-time query on the physical standby database is experiencing delays beyond the specified maximum data delay threshold. Increasing the network bandwidth (Option E) can enhance the speed at which redo data is transferred from the primary to the standby database, thereby reducing the likelihood of exceeding the STANDBY_MAX_DATA_DELAY threshold. Reducing I/O latency on the primary database's storage (Option B) ensures that redo data is generated and shipped more efficiently, further mitigating the risk of delay. These actions, focused on optimizing data transfer and processing speed, address the root causes of the ORA-03172 error in a synchronous Data Guard configuration operating in Maximum Availability mode.

Question: 15

Active Data Guard (ADG) databases are widely used to offload reporting or ad hoc query-only jobs from the primary database. Reporting workload profile is different from the primary database and often requires tuning.
Which tool is used to tune SQL workloads running on an ADG database?

A. Standby Statspack
B. In-Memory Active Session History (ASH)
C. Automatic Diagnostic Database Monitor (ADDM)
D. Automatic Workload Repository (AWR)
E. SQL Tuning Advisor

Answer: D

Explanation:
AWR collects, processes, and maintains performance statistics for problem detection and self-tuning purposes. In an Active Data Guard environment, where the physical standby database can be used for read-only workloads, AWR can be instrumental in identifying performance

bottlenecks and areas for optimization. It provides detailed reports that include wait events, time model statistics, and active session history, making it an invaluable tool for tuning SQL queries and overall database performance in an ADG setup.

Question: 16

Your Data Guard environment contains a primary database and three standby databases with these attributes:

1. prod : Primary database
2. prod_prq : Physical standby database with real-time query enabled used by reporting applications
3. prod_lsby: Logical standby database used by DSS
4. PROD_SSBY: Snapshot standby database used for Real Application Testing

Which TWO can be used to prevent clients from connecting to the wrong database instance?

A. Create role based services with the si vet] utility when using clusterware for Oracle RAC databases or Oracle Restart for single instance Oracle databases.
B. Establish Oracle Net connectivity to the primary database instance from all the standby database instances.
C. Create a static service for each of the databases, register it with the local listener of each database instance, and add connection descriptors on clients to connect to those services.
D. Create database services on each of the standby databases, start the services, and add connection descriptors on the clients to connect to those services.
E. Create database services for each database and use event triggers to make sure that services are activated only when the database is in the correct role.

Answer: D, E

Explanation:
Creating dedicated database services for each database instance (Option D) and utilizing event triggers to manage these services based on the role of the database (Option E) ensure that clients connect to the appropriate database instance based on its current role and state. This approach leverages the flexibility and control provided by Oracle Net services and database event management to direct client connections to the suitable primary or standby instance, enhancing the overall robustness and reliability of the Data Guard environment. Based on Oracle Database 19c best practices for managing connectivity and services in a Data Guard setup, including the use of role-based services and event-driven service management.

Question: 17

Your Data Guard environment has a remote physical standby database with real-time query enabled, which is used for reporting, and a logical standby database used for DSS reporting. Switchovers or failovers are possible due to testing or in case of a disaster.

Clients use local TNSNAMES.ORA files to define connection strings to the database instances. Which three will prevent clients from connecting to the wrong database instances?

A. Oracle Net connectivity to the primary database instance must be established on all the standby database instances.
B. The standby database services must be defined statically with the Listeners running on the standby database hosts.
C. The LOCAL_LISTENER parameter on the primary database instance must always be set.
D. The client applications must use the correct TNS entries when requesting connections to the database instances.
E. Client TNS entries for the databases use the correct service names for the intended service.
F. The DB_NAME and DB_UNIQUE_NAME parameters must be set to the same value for all the databases in the Data Guard environment.
G. A service name is registered with the local listener of each database instance.

Answer: B, D, E

Explanation:
Based on Oracle Database 19c: Data Guard Administration documents, the three measures that can prevent clients from connecting to the wrong database instances during switchovers, failovers, or regular operations in a Data Guard environment are:
B . The standby database services must be defined statically with the Listeners running on the standby database hosts.
D . The client applications must use the correct TNS entries when requesting connections to the database instances.
E . Client TNS entries for the databases use the correct service names for the intended service.
In an Oracle Data Guard configuration, correctly configuring Oracle Net Services (including TNS entries and listeners) is crucial for ensuring that clients connect to the appropriate database instance, whether it's the primary or standby. Defining services on the standby database and associating them with listeners ensures that client applications can connect to the standby when needed, especially useful in a role transition or when the standby is open for read-only access or real-time query. It's essential that TNS entries used by client applications specify the correct service names that correspond to the intended database roles, such as primary or standby. This setup facilitates seamless connectivity to the appropriate instance based on the role, especially critical during switchovers and failovers when the roles of the databases change.
Reference:

Oracle's Data Guard concepts and administration guide provides extensive information on configuring network services for Data Guard environments, ensuring that applications connect to the correct database instance based on the current role of the databases in the Data Guard configuration.

Question: 18

Examine the Data Guard configuration: DGMGRL> show configuration;

Configuration - Animals
Protection Mode: MaxPerformance
Databases:
dogs- Primary database
sheep - Physical standby database
cats- Snapshot standby database
Fast-Start Failover: DISABLED
Configuration Status: SUCCESS
You receive an error while attempting to raise the protection mode to Maximum Protection:
DGMGRL> edit configuration set protection mode as maxprotection;
Error: ORA-16627: operation disallowed since no standby databases would remain to support protection
mode
Failed.
What can you conclude based on this error?

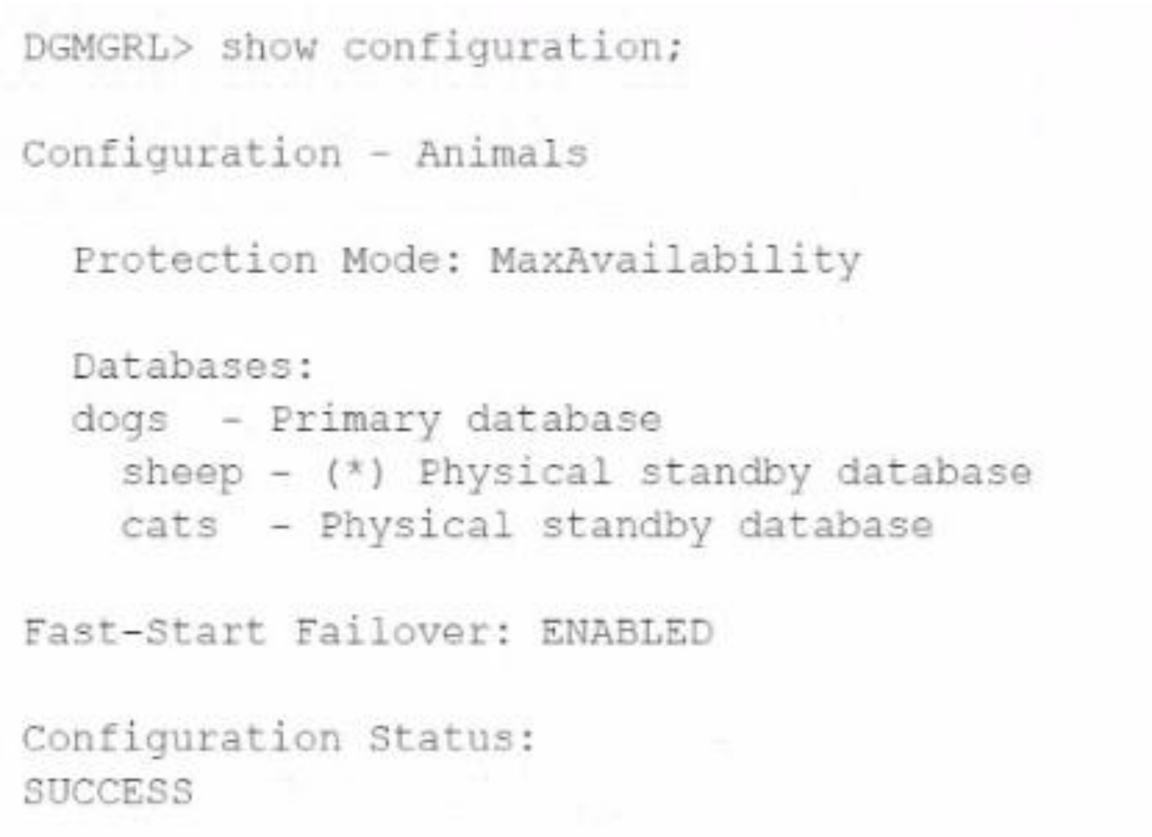
A. The redo transport mode is set to async for the standby database Sheep.
B. The redo transport mode is set to asyn: for the standby database Cats.
C. The redo transport mode is set to async for both standby databases.
D. Cats is a snapshot standby database.
D. Cats is a snapshot standby database.

Answer: D

Explanation:
The error indicates that switching the protection mode to Maximum Protection is not possible due to the presence of a snapshot standby database in the Data Guard configuration, which cannot participate in synchronous redo transport required by the Maximum Protection mode. Therefore, the correct answer is:

Question: 19

Examine the Data Guard configuration:



```
DGMGRL> show configuration;

Configuration - Animals

  Protection Mode: MaxAvailability

  Databases:
  dogs  - Primary database
    sheep - (*) Physical standby database
    cats  - Physical standby database

Fast-Start Failover: ENABLED

Configuration Status:
SUCCESS
```

What happens if you issue "switchover to sheep;" at the DGMGRL prompt?

A. The switchover succeeds and Cats becomes the new failover target.
B. It results in an error indicating that a switchover is not allowed.
C. The switchover succeeds but Dogs needs to be reinstated.
D. The switchover succeeds and Fast-Start Failover is suspended.
E. The switchover succeeds and Dogs becomes the new failover target.

Answer: E

Explanation:
When issuing a "switchover to sheep;" command in a Data Guard configuration, the primary database (Dogs) transitions to a standby role, and the target standby database (Sheep) becomes the new primary database. Fast-Start Failover (FSFO) remains enabled, but its target changes according to the new roles of the databases. Since Cats is also a physical standby database, it does not become the failover target by default unless it is specified in the broker configuration. After the switchover, the original primary (Dogs) becomes the new standby database and thus the new failover target for FSFO.

Reference:

Oracle Data Guard Broker documentation provides detailed procedures and explanations of switchover operations, including how FSFO targets are affected post-switchover. This behavior is consistent across different Oracle Database versions that support Data Guard and FSFO.

Question: 20

Which four statements are true regarding SQL Apply filters for a logical standby database?

A. They can be used to skip execution of DML triggers on a table while allowing the DML to execute.
B. They can be used to skip CREATE TABLE commands.
C. They can be used to skip ALTE1 STEM and ALTER DATABASE commands.
D. They can only be used to skip DML statements on a table.
E. They can be used to skip all SQL statements executed on a specific pluggable database (PDB) within a standby multitenant container database (CDB).
F. They can be used to stop SQL apply if it encounters an error.
G. They can be used to skip ALTER TABLE commands on specific tables.

Answer: A, B, C, G

Explanation:
Based on the Oracle Database 19c documentation, the correct answers about SQL Apply filters for a logical standby database are:

A. They can be used to skip execution of DML triggers on a table while allowing the DML to execute.

B. They can be used to skip CREATE TABLE commands.

C. They can be used to skip ALTER SYSTEM and ALTER DATABASE commands.

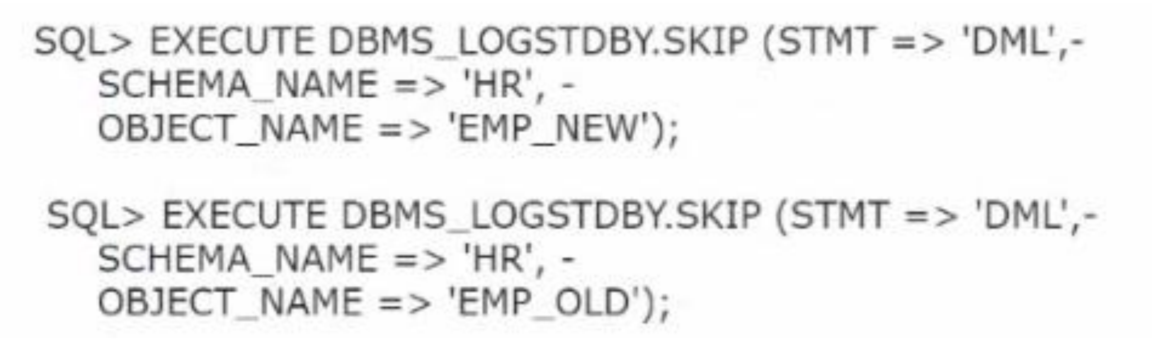
G. They can be used to skip ALTER TABLE commands on specific tables.
Comprehensive Detailed Explanation:

SQL Apply filters in a logical standby database can be set to control which SQL operations are applied to the standby. These filters allow for certain commands to be skipped, ensuring that they do not impact the standby database. For example, filters can be used to skip the execution of DML triggers to prevent them from firing during SQL Apply, while still allowing the underlying DML to be executed on the logical standby database. This is particularly useful when certain triggers are not desired to run in a standby environment. CREATE TABLE, ALTER SYSTEM, ALTER DATABASE, and specific ALTER TABLE commands can also be skipped using SQL Apply filters to prevent unwanted structural changes or administrative operations from affecting the logical standby database. These capabilities provide a level of control to ensure that the logical standby database reflects only the desired state of the primary database.
Reference:

Oracle Database SQL Language Reference and Oracle Data Guard Concepts and Administration guide offer comprehensive details on the use of SQL Apply filters, including the range of SQL statements that can be influenced by these filters in a logical standby database environment.

Question: 21

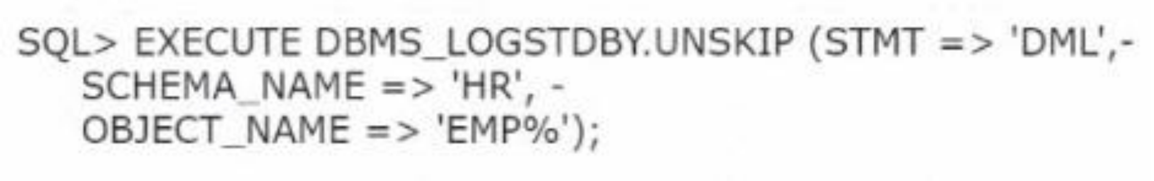
On your logical standby database, you specified these rules:



```
SQL> EXECUTE DBMS_LOGSTDBY.SKIP (STMT => 'DML',-
    SCHEMA_NAME => 'HR', -
    OBJECT_NAME => 'EMP_NEW');

 SQL> EXECUTE DBMS_LOGSTDBY.SKIP (STMT => 'DML',-
    SCHEMA_NAME => 'HR', -
    OBJECT_NAME => 'EMP_OLD');
```

After completion of the weekend batch cycle you attempt to delete the SQL Apply filters:



```
SQL> EXECUTE DBMS_LOGSTDBY.UNSKIP (STMT => 'DML',-
    SCHEMA_NAME => 'HR', -
    OBJECT_NAME => 'EMP%');
```

Which is TRUE regarding the execution of the UNSKIP procedure?

A. It succeeds only if all DML statements executed on the primary have been applied on the logical standby deleting the SQL Apply filter.
B. It deletes both the SQL Apply filters.
C. It succeeds but the SQL Apply filters are not deleted.
D. It succeeds only if SQL apply is stopped before deleting the SQL Apply filter.
E. It returns an error because the syntax to delete a SQL Apply filter must specify the same object names as specified when the filter was added.

Answer: B

Explanation:
The execution of the UNSKIP procedure is designed to remove SQL Apply filters that have been previously set up on a logical standby database. Based on the provided statements, the UNSKIP procedure is directed to delete any SQL Apply filters for DML statements associated with objects in the 'HR' schema that start with 'EMP'. Since both SKIP procedures had the same schema name ('HR') and statement type ('DML'), and the UNSKIP procedure uses a wildcard (%) for the object name, it will successfully remove both of the SQL Apply filters for 'EMP_NEW' and 'EMP_OLD', as both object names match the pattern provided in the UNSKIP procedure.
Reference:

Oracle's Data Guard documentation and SQL Language Reference provide insights into managing SQL Apply filters on a logical standby database using the DBMS_LOGSTDBY package. This includes adding and removing filters through SKIP and UNSKIP procedures.

Question: 22

Which TWO observations are true about the Far Sync instance?

A. Receives redo synchronously from the primary database
B. Can be created using the RMAN DUPLICATE command
C. Includes a standby control file, password file, data files, standby redo logs, and archive logs
D. Can only be created using a series of SQL commands
E. Applies redo received

Answer: A, E

Explanation:
A Far Sync instance is a special kind of Oracle Data Guard configuration that allows synchronous redo transport from a primary database to a remote standby database with minimum impact on the primary database's performance. The Far Sync instance receives redo data synchronously from the primary database (A), then ships it asynchronously to the remote standby database, thus extending zero data loss protection over longer distances and higher network latency environments than would be practical with a synchronous standby alone. The Far Sync instance does not apply the redo data; it just receives and ships it (E). A Far Sync instance does not have data files, and it cannot apply redo to stay synchronized with the primary database.
Reference:

Oracle Database High Availability Overview and Oracle Data Guard Concepts and Administration documentation detail the role and configuration of Far Sync instances, including how they contribute to achieving zero data loss disaster recovery over long distances.

Question: 23

Which three Data Guard monitoring activities may be performed using Enterprise Manager Cloud Control?

A. You can monitor the redo apply rate on a logical standby database.
B. You can set a critical threshold on the redo generation rate metric for a primary database.
C. You can set a warning threshold on the redo generation rate metric for a physical standby database.
D. You can check if redo apply needs to be tuned.
E. You can check the potential data loss in the event of a disaster.
F. You can monitor the redo apply rate on a snapshot standby database.

Answer: A, B, E

Explanation:
Enterprise Manager Cloud Control offers comprehensive monitoring capabilities for Oracle Data Guard environments. It enables monitoring the rate at which redo is being applied on a logical standby database (A), which is crucial for ensuring that the standby database is keeping up with the changes from the primary. It also allows setting thresholds on performance metrics, such as the redo generation rate on the primary database (B), to alert administrators when values exceed critical or warning thresholds. Additionally, it provides the capability to estimate the potential data loss in the event of a disaster (E), helping in disaster recovery planning and ensuring business continuity.
Reference:

Oracle Enterprise Manager Cloud Control documentation provides extensive information on its monitoring features for Oracle Data Guard, including setting thresholds, estimating potential data loss, and tracking redo apply rates.

Question: 24

Which two statements are true regarding asynchronous redo transport in a Data Guard

A. This transport mode satisfies the minimum requirements for Maximum Availability data protection mode.
B. A transaction can commit without waiting for redo to be sent to any standby database in the data guard configuration.
C. This transport mode satisfies the minimum requirements for Maximum Performance data protection mode.
D. Real-time query performance on a physical standby database improves for current read requests when using this transport mode.
E. The performance of SQL apply on a logical standby database always improves when using this transport mode.

Answer: B, C

Explanation:
Asynchronous redo transport is a method where the primary database does not wait for an acknowledgment from the standby database before committing transactions, which helps in minimizing the impact on the primary database's performance (B). This transport mode is associated with the Maximum Performance data protection mode, which prioritizes performance over synchronicity of data between the primary and standby databases (C). While it provides a level of data protection, there could be some data loss in the event of a primary database failure because redo data may not have been transmitted to the standby database at the time of the failure.

Reference:

Oracle Data Guard Concepts and Administration documentation provides detailed explanations of different redo transport modes and their implications on data protection and performance. Asynchronous transport mode's behavior and association with Maximum Performance mode are outlined explicitly.

Question: 25

Your Data Guard configuration consists of these components and settings:
1. A primary database
2. A remote physical standby database
3. Real-time query is enabled
4. Redo transport mode is synchronous
5. Protection mode is maximum availability
6. The Data Guard broker is used

You notice that the standby destination fails to acknowledge reception of redo within net_timeout period of time.
Which is true in this scenario?

A. Real-time query will be disabled on the physical standby.
B. The protection mode will automatically change to Maximum Performance.
C. Synchronous redo transport mode connections to the standby database are terminated.
D. The physical standby database instance is shut down by the Data Guard broker.

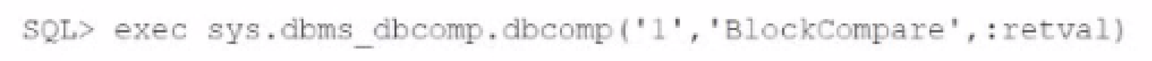
Answer: C

Explanation:
In a Data Guard configuration where the protection mode is set to Maximum Availability and synchronous redo transport is enabled, if the standby destination fails to acknowledge the reception of redo within the net_timeout period, the primary database will terminate the synchronous redo transport mode connections to the standby database to protect the primary database from hanging (C). The primary database then operates in a Maximum Performance mode until the issue is resolved. This behavior ensures that the primary database can continue to process transactions even when the standby database is temporarily unavailable.
Reference:

The Oracle Data Guard Broker documentation and Oracle Data Guard Concepts and Administration guide detail the behavior of different protection modes and the response to network timeouts, including the fallback to asynchronous redo transport to maintain primary database availability.

Question: 26

You are planning to perform block comparison using the dbms comp package:



```
SQL> exec sys.dbms_dbcomp.dbcomp('1','BlockCompare',:retval)
```

Which TWO statements are true?

A. The databases should be at least mounted before block comparison.
B. Logical standby databases can be the target database for the dbms_dbcomp.dbcomp procedure.
C. It requires that the DB_LOST_WKITE_protect initialization parameter be enabled.
D. You can monitor the progress of an ongoing block comparison operation by querying VS SES SION_LONGOPS.
E. It can be used to detect lost writes and inconsistencies between the primary database and the cascaded standbys.

Answer: A, D

Explanation:
The DBMS_COMPARISON package, used for comparing and converging data objects within a single database or between databases, requires that the databases involved in the block comparison be at least mounted (A). This allows the procedure to access the data blocks for comparison. Additionally, the progress of long-running operations such as block comparison can be monitored using the dynamic performance view V$SESSION_LONGOPS (D), which provides information on the operation's progress and estimated completion time.
Reference:

Oracle Database PL/SQL Packages and Types Reference provides comprehensive details on the DBMS_COMPARISON package, including its procedures and how to monitor their progress. Additionally, Oracle Database Reference explains the V$SESSION_LONGOPS view, which is commonly used for monitoring long operations in the database.

Question: 27

Which THREE are among the various tasks performed by the Data Guard Monitor (DMON) process?

A. performing role transitions when switchover requests are made
B. maintaining information about all members of the broker configuration in binary configuration files.
C. activating role-based services appropriately in the various database instances of the configuration, based on the database role
D. communicating with the DMON process of the observer to monitor a primary database in case a fast start failover is required
E. communicating with dkon processes in other database instances that are part of the broker configuration

Answer: A, B, C

Explanation:
The Data Guard Monitor (DMON) process is a key component of Oracle Data Guard. It plays a crucial role in managing and monitoring the state of both the primary and standby databases in a Data Guard configuration.
Performing role transitions when switchover requests are made (A): DMON is responsible for coordinating the switchover process between the primary and standby databases. This involves safely transitioning the roles of the databases to ensure data protection and availability.
Maintaining information about all members of the broker configuration in binary configuration files (B): DMON maintains detailed information about the databases in the Data Guard configuration, including their roles, states, and network addresses. This information is stored in binary configuration files, which are used by the Data Guard Broker to manage the Data Guard environment.
Activating role-based services appropriately in the various database instances of the configuration, based on the database role (C): DMON activates services that are appropriate for the role of each database in the Data Guard configuration. For example, it may activate different services on a primary database than on a standby database, based on the specific requirements of each role.

Reference:
Oracle Data Guard Concepts and Administration
Oracle Data Guard Broker documentation

Question: 28

Which three are prerequisites for using Data Guard Broker?

A. The primary and standby databases must run the same version of the Oracle Database server.
B. Network connectivity to the primary database instance must be defined on the servers hosting the standby database instances.
C. DG_BROKEB_START must be set to TRUE for a database instance before adding the database to the broker configuration.
D. If any database in the configuration is a RAC database, then the broker configuration files must reside in shared storage accessible by all database instances for all databases in the broker configuration.
E. The broker configuration files for a RAC database must reside in shared storage accessible by all the RAC database instances.
F. A statically defined listener end-point must be registered with the local listener on the servers hosting the standby database instances.

Answer: A, B, D

Explanation:
Data Guard Broker is a management tool that simplifies the configuration, management, and monitoring of Data Guard environments. The prerequisites for using Data Guard Broker include:
The primary and standby databases must run the same version of the Oracle Database server (A): This ensures compatibility between the primary and standby databases and enables seamless role transitions and data synchronization.
Network connectivity to the primary database instance must be defined on the servers hosting the standby database instances (B): Proper network connectivity is essential for communication between the primary and standby databases, allowing for the replication of data and the synchronization of changes.
If any database in the configuration is a RAC database, then the broker configuration files must reside in shared storage accessible by all database instances for all databases in the broker configuration (D): In Real Application Clusters (RAC) environments, shared storage ensures that all instances of the RAC database can access the broker configuration files, facilitating the management of the Data Guard environment across all instances.

Reference:
Oracle Data Guard Broker documentation
Oracle Real Application Clusters Administration and Deployment Guide

Question: 29

Which four requirements can be met by deploying a logical standby database?

A. Support for workloads requiring additional materialized views.
B. It must have the same physical structure as the primary database.
C. It can be used to create additional tables.
D. It must provide a disaster-recovery solution that protects all data with capability of performing switchovers and failovers.
E. It can be used for Real Application Testing without affecting the disaster recovery capabilities.
F. Support for workloads requiring additional indexes.
G. It can be used to create additional schemas.

Answer: A, C, E, F

Explanation:
A logical standby database is part of Oracle Data Guard and allows the standby database to be open for read-write operations, providing additional flexibility. The requirements met by a logical standby database include:
Support for workloads requiring additional materialized views (A): Logical standby databases can support materialized views, allowing for complex data summarization and reporting workloads.
It can be used to create additional tables (C): Unlike physical standby databases, logical standby databases allow for the creation of additional tables that do not exist in the primary database, enabling custom workloads and reporting.

It can be used for Real Application Testing without affecting the disaster recovery capabilities (E): Logical standby databases can be used to test application changes, patches, and upgrades while still maintaining their role as part of the disaster recovery strategy.
Support for workloads requiring additional indexes (F): Logical standby databases allow for the creation of additional indexes to optimize query performance for reporting and analytical workloads.

Reference:
Oracle Data Guard Concepts and Administration
Oracle Database High Availability Overview

Question: 30

Which THREE are always benefits of using a logical standby database?

A. It provides a disaster-recovery solution with switchover and failover options that can recover any data updated on the primary database.
B. It can be used for reporting workloads requiring additional indexes or materialized views or both.
C. It can be used for testing patchsets without affecting the primary database.
D. It can be used for database rolling release upgrades.
E. It can be used to replicate a single pluggable database (PDB) in a multitenant container database.
F. It can be used as an updatable database for Real Application Testing and then converted back to a standby database without affecting the updates.

Answer: A, B, D

Explanation:
Logical standby databases are a key feature of Oracle Data Guard and offer several distinct advantages, especially in terms of flexibility for reporting, upgrades, and disaster recovery:
Disaster-recovery solution with switchover and failover options (A): Logical standby databases provide a robust disaster-recovery solution, ensuring that any data updated on the primary database can be recovered. They support both switchover and failover operations, allowing for smooth role transitions between the primary and standby databases.
Used for reporting workloads requiring additional indexes or materialized views (B): Logical standby databases can be opened for read-write operations and can have additional indexes or materialized views that are not present in the primary database. This makes them ideal for offloading reporting and querying workloads from the primary database.
Database rolling release upgrades (D): Logical standby databases can be used to perform rolling upgrades of the Oracle Database software. This allows the database to be upgraded with minimal downtime, as the standby database is upgraded first, followed by a switchover to make it the new primary.

Reference:

Oracle Data Guard Concepts and Administration Guide
Oracle Database High Availability Overview

Question: 31

Which two statements are true regarding Data Guard environments in an Oracle Muti-tenant architecture?

A. Different redo transport methods can be configured for different pluggable databases within one Data Guard environment.
B. The Data Guard broker may be used for multi-tenant databases.
C. PDB_FILE_NAME CONVERT must be set to enable creation of standby databases if they are
D. Standby redo log files are required for each pluggable database that is protected with Data Guard.
E. A Data Guard environment with a multi-tenant primary database can operate in any Protection mode.

Answer: B, E

Explanation:
Oracle Multi-tenant architecture and Data Guard have several interactions, but specific aspects hold true in such environments:
The Data Guard broker may be used for multi-tenant databases (B): Data Guard Broker simplifies the management and monitoring of Data Guard configurations and is fully compatible with the Oracle Multi-tenant architecture, allowing for easy management of Data Guard configurations that include multi-tenant container databases (CDBs) and their pluggable databases (PDBs).
A Data Guard environment with a multi-tenant primary database can operate in any Protection mode (E): Data Guard can be configured to operate in Maximum Performance, Maximum Availability, or Maximum Protection mode, regardless of whether the primary database is a multi-tenant database. This flexibility ensures that Data Guard can meet various data protection and availability requirements in multi-tenant environments.

Reference:
Oracle Data Guard Broker documentation
Oracle Multitenant Administrator's Guide

Question: 32

You are licensed to use Oracle Active Data Guard.
Which TWO statements are true after enabling block change tracking on a physical standby database?

A. It starts the RVWR process on the physical standby database instance.
B. It starts the CTWR process on the primary database instance.
C. It allows fast incremental backups to be offloaded to a snapshot standby database, when the physical standby database is converted.
D. It starts the CTWR process on the physical standby database instance.
E. It allows fast incremental backups to be offloaded to the physical standby database.
F. It allows fast incremental backups to be taken on the primary database.

Answer: A, E

Explanation:
Block change tracking is a feature that enhances the efficiency of incremental backups by recording changed blocks in a tracking file. When used with Oracle Active Data Guard:
It starts the RVWR process on the physical standby database instance (A): When block change tracking is enabled on a physical standby database, the Recovery Writer (RVWR) process is initiated. This process is responsible for recording the changes to blocks in the block change tracking file, which is then used to optimize incremental backups.
It allows fast incremental backups to be offloaded to the physical standby database (E): With block change tracking enabled on the physical standby database, fast incremental backups can be offloaded from the primary database. This reduces the workload on the primary database and utilizes the standby database for backup operations, improving overall system performance and efficiency.

Reference:
Oracle Database Backup and Recovery User's Guide
Oracle Active Data Guard documentation

Question: 33

Which THREE steps are prerequisites for the creation of a physical standby database on a separate server using the RMAN active database duplication method?

A. Configure Oracle Net connectivity on the primary host to the standby database instance.
B. Establish user equivalence for the database software owner between the primary host and standby host.
C. startup nomount the standby database instance.
D. Set the DB_UNIQUE_NAME parameter on the primary database to a different value than that of the DB_NAME name parameter.
E. Put the primary database into archivelog mode.

Answer: A, B, C

Explanation:

Creating a physical standby database using RMAN active database duplication requires certain prerequisites to ensure a successful and seamless operation:
Configure Oracle Net connectivity on the primary host to the standby database instance (A): Proper Oracle Net connectivity between the primary and standby servers is essential for communication and data transfer during the duplication process. Oracle Net services provide the network foundation for Oracle Database, Oracle Net Listener, and Oracle applications.
Establish user equivalence for the database software owner between the primary host and standby host (B): User equivalence ensures that the user who owns the Oracle Database software on the primary server has the same privileges on the standby server. This is crucial for RMAN to perform operations on both servers without encountering permission issues.
Startup nomount the standby database instance (C): The standby database instance needs to be started in the NOMOUNT stage before the duplication can begin. This prepares the environment for creating the control file and restoring the database without mounting it, which is a necessary step in the RMAN duplication process.

Reference:
Oracle Database Backup and Recovery User's Guide
Oracle Data Guard Concepts and Administration

Question: 34

Which THREE are true about using flashback database in a Data Guard environment?

A. When a flashback database operation is performed on a primary database, a physical standby database is also flashed back automatically.
B. You can use it when real-time apply is enabled in case the phylt may not be used to flash back a primary database after a failover to a logical standby.
C. It may be used to flash back a physical standby that receives redo from a far sync instance.
D. You can use it when real-time apply is enabled in case the physical standby suffers from logical corruption.
E. It may not be used to flash back a primary database after a failover to a physical standby.
F. When a flashback database operation is performed on a primary database, a logical standby database is also flashed back automatically.

Answer: C, D, E

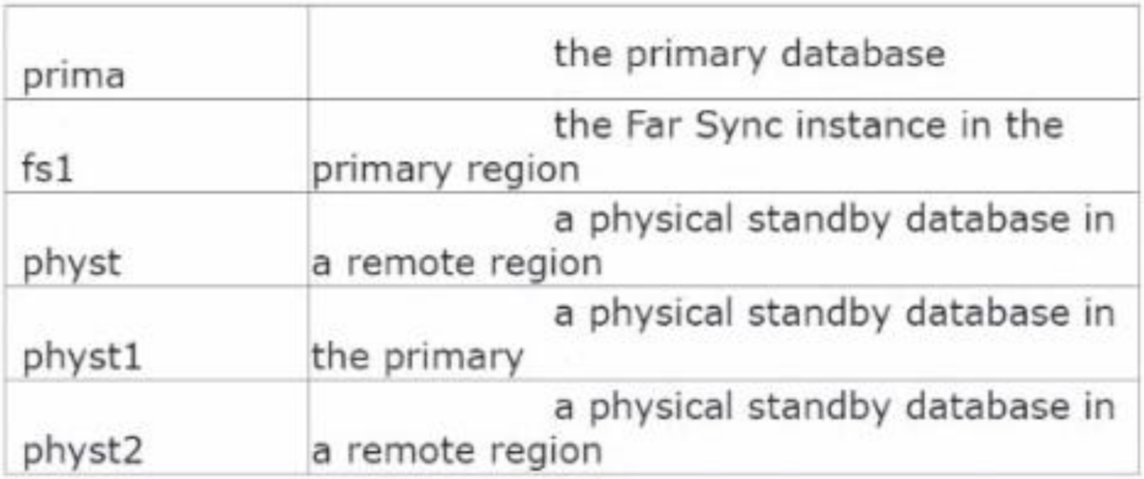
Explanation:
Flashback Database is a feature that allows reverting a database to a previous point in time, which is extremely useful in various Data Guard configurations:
It may be used to flash back a physical standby that receives redo from a far sync instance (C): Flashback Database can be used on a physical standby database to revert it to a past point in time, even when it is receiving redo data from a far sync instance. This can be particularly useful to recover from logical corruptions or unwanted changes.
You can use it when real-time apply is enabled in case the physical standby suffers from logical corruption (D): Even when real-time apply is enabled, which allows redo data to be applied to

the standby database as soon as it is received, Flashback Database can be used to revert the physical standby database to a point in time before the logical corruption occurred.
It may not be used to flash back a primary database after a failover to a physical standby (E): After a failover has occurred from a primary to a physical standby database, making the standby the new primary, Flashback Database cannot be used to revert the old primary database to a state before the failover because the failover operation makes irreversible changes to the database role and configuration.

Reference:
Oracle Database Backup and Recovery User's Guide
Oracle Data Guard Concepts and Administration

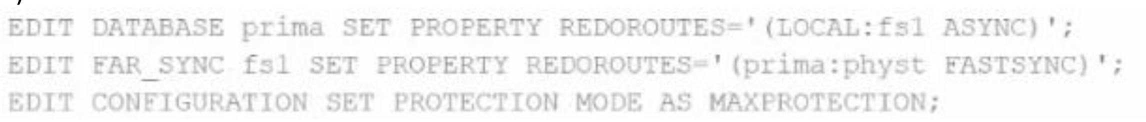
Question: 35

A customer has these requirements for their proposed Data Guard implementation:
1. Zero data loss must still be guaranteed through the loss of any one configuration component.
2. The primary database must be protected against a regional disaster.
3. Performance overheads on the primary should be minimized as much as possible given these requirements.
4. Downtime on the primary database for any reason must be kept to a minimum.
Components referred to in the broker commands are:



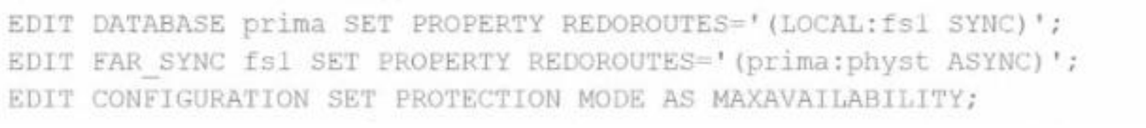
prima	the primary database
fs1	the Far Sync instance in the primary region
physt	a physical standby database in a remote region
physt1	a physical standby database in the primary
physt2	a physical standby database in a remote region

A)



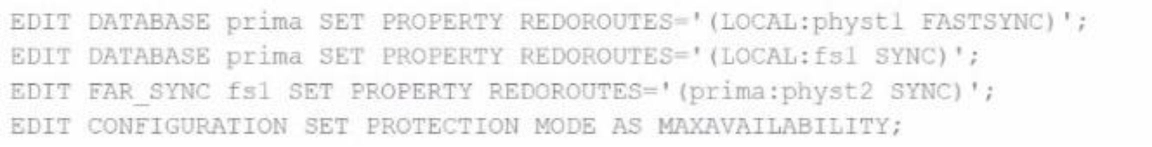
```
EDIT DATABASE prima SET PROPERTY REDOROUTES='(LOCAL:fs1 ASYNC)';
EDIT FAR_SYNC fs1 SET PROPERTY REDOROUTES='(prima:physt FASTSYNC)';
EDIT CONFIGURATION SET PROTECTION MODE AS MAXPROTECTION;
```

B)



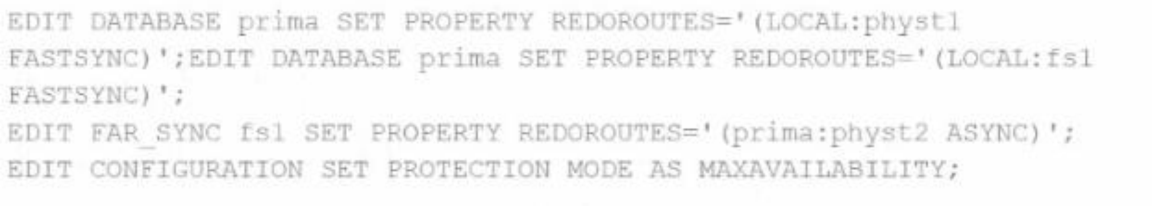
```
EDIT DATABASE prima SET PROPERTY REDOROUTES='(LOCAL:fs1 SYNC)';
EDIT FAR_SYNC fs1 SET PROPERTY REDOROUTES='(prima:physt ASYNC)';
EDIT CONFIGURATION SET PROTECTION MODE AS MAXAVAILABILITY;
```

C)



```
EDIT DATABASE prima SET PROPERTY REDOROUTES='(LOCAL:physt1 FASTSYNC)';
EDIT DATABASE prima SET PROPERTY REDOROUTES='(LOCAL:fs1 SYNC)';
EDIT FAR_SYNC fs1 SET PROPERTY REDOROUTES='(prima:physt2 SYNC)';
EDIT CONFIGURATION SET PROTECTION MODE AS MAXAVAILABILITY;
```

D)



```
EDIT DATABASE prima SET PROPERTY REDOROUTES='(LOCAL:physt1
FASTSYNC)';EDIT DATABASE prima SET PROPERTY REDOROUTES='(LOCAL:fs1
FASTSYNC)';
EDIT FAR_SYNC fs1 SET PROPERTY REDOROUTES='(prima:physt2 ASYNC)';
EDIT CONFIGURATION SET PROTECTION MODE AS MAXAVAILABILITY;
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation:
According to the requirements stated:
Zero data loss must be guaranteed despite the loss of any one component: This necessitates synchronous redo transport to at least one standby database (for no data loss).
The primary database must be protected against a regional disaster: This implies that there must be a standby database in a different region.
Performance overhead on the primary should be minimized: This suggests that asynchronous transport should be used where possible to reduce the performance impact on the primary.
Downtime on the primary for any reason must be kept to a minimum: This is indicative of a requirement for a fast failover mechanism, possibly with a fast-start failover (FSFO) and high availability.
Given these requirements, the appropriate option that fulfills all these is:
Option C, where 'prima' is the primary database, 'fs1' is the Far Sync instance in the primary region, and 'physt' and 'physt2' are physical standby databases in the primary and remote regions, respectively. In this configuration:
'prima' is set to send redo to 'fs1' using SYNC to guarantee zero data loss.
'fs1' is set to send redo to 'physt' (local standby) using FASTSYNC, which is a low-latency synchronous transport that is optimized for performance.
The Data Guard configuration's protection mode is set to MAXAVAILABILITY to provide the highest level of data protection that is possible without compromising the availability of the primary database.
This configuration ensures that there is zero data loss even if the primary region is completely lost, maintains performance by limiting the synchronous transport to the local region with a Far Sync instance, and has a remote standby database in a separate region for disaster recovery purposes.
Oracle Data Guard Concepts and Administration
Oracle Data Guard Broker documentation

Question: 36

Which THREE statements are true about snapshot standby databases?

A. A snapshot standby database may be opened read-only.
B. FLASHBACK DATABASE is enabled automatically on a snapshot standby database after converting it from a physical standby database if not already enabled.
C. FLASHBACK DATABASE is enabled automatically on a physical standby database as part of the conversion into a snapshot standby database, if not already enabled.
D. A snapshot standby database can have Real-Time apply enabled.
E. A snapshot standby database may be opened read-write.
F. FLASHBACK DATABASE must be manually enabled on a physical standby database before converting it into a snapshot standby database.

Answer: B, C, E

Explanation:
Snapshot standby databases are a feature of Oracle Data Guard that allows a physical standby database to be temporarily converted into a read-write database for testing or other purposes.
The true statements about snapshot standby databases are:
FLASHBACK DATABASE is enabled automatically on a snapshot standby database after converting it from a physical standby database if not already enabled (B): When a physical standby is converted to a snapshot standby, FLASHBACK DATABASE is automatically enabled to allow the database to be easily reverted back to its original state.
FLASHBACK DATABASE is enabled automatically on a physical standby database as part of the conversion into a snapshot standby database, if not already enabled (C): As part of the conversion process, FLASHBACK DATABASE is turned on to ensure that changes made while the database is in snapshot standby mode can be undone.
A snapshot standby database may be opened read-write (E): Once a physical standby is converted to a snapshot standby, it can be opened for read-write operations, allowing for testing and other tasks that require a writable database.
Oracle Data Guard Concepts and Administration
Oracle Database Backup and Recovery User's Guide

Question: 37

Examine the following parameter settings of the physical standby database:
• STANDBY_FILE_MANAGEMENT=AUTO
• ENABLED_PDBS_ON_STANDBY=<null>
During which TWO tasks are files automatically created in the physical standby database after structure changes on the primary database?

A. Performing transportable tablespaces
B. Adding or dropping a redo file group
C. Adding a data file or creating a tablespace
D. Creating a PDB from the existing PDB within the same CDB
E. Renaming a data file in the primary database

Answer: C, D

Explanation:
When STANDBY_FILE_MANAGEMENT is set to AUTO, the Oracle Data Guard automatically creates, deletes, and renames files on the standby database to match the changes made on the primary database. The tasks that lead to the automatic creation of files on the standby include:
Adding a data file or creating a tablespace (C): When a new tablespace is created or a new data file is added on the primary database, the standby database automatically replicates this action, maintaining structural consistency with the primary database.
Creating a PDB from the existing PDB within the same CDB (D): Creating a new Pluggable Database (PDB) within a Multitenant Container Database (CDB) on the primary database triggers an automatic creation of the corresponding PDB within the standby CDB.

Reference:
Oracle Data Guard Concepts and Administration Guide

Question: 38

Suppose that you manage the following databases in your environment:

- boston: Primary database with a single PDB called DEVI
- london: Physical standby database protecting the PDB called DEVI
- orcl: Stand-alone database with a single PDB called PDB1 as a remote clone source

You are planning to run the following command to create a remote clone in the primary database (boston) using pdbi in orcl:
Which are the THREE prerequisites for automating instantiation of the PDB in the standby database (london)?

A. Open PDBI (remote clone source) in Read Only.
B. Open PDBI (remote clone source) in Read Write.
C. Set STANDBY_PDB_SOURCE_FILE_DIRECTORY to <location of the PDB> in the london database.
D. Set standby_pdb_source_file_dblink to clone_link in the london database.
E. Enable Active Data Guard in the _ondon database.
F. Set STANDBY_FILE_MANAGEMENT to auto in the london database.

Answer: A, C, F

Explanation:

To automate the instantiation of a PDB in the standby database after creating a remote clone in the primary database, certain conditions must be met:
Open PDBI (remote clone source) in Read Only (A): The source PDB from which the clone is created must be open in read-only mode to ensure a consistent state during cloning.
Set STANDBY_PDB_SOURCE_FILE_DIRECTORY to <location of the PDB> in the london database (C): This parameter specifies the location on the standby database where the files from the source PDB should be placed.
Set STANDBY_FILE_MANAGEMENT to auto in the london database (F): This parameter automates the management of file changes on the standby database when structural changes occur on the primary database, ensuring that the clone operation is reflected automatically on the standby.

Reference:
Oracle Multitenant Administrator's Guide
Oracle Data Guard Broker documentation

Question: 39

You are using Data Guard in conjunction with Global Database Services.
You have a Data Guard Broker configuration called Sales and a GDS pool called Prod.
Which three are true concerning the management of the broker configuration when using GDS?

A. DGMGRL may be used to add the Sales configuration to the Prod pool in gds.
B. Performing a role change with DGMGRL automatically notifies GDS which in turn activates the appropriate services.
C. DGMGRL may be used to add a single database to the Sales configuration even if Sales is a member of the Prod pool.
D. Adding a database to the Sales configuration with DGMGRL automatically adds the database to the Prod Pool.
E. Adding a database to the Sales configuration with DGMGRL requires that the Sales configuration be disabled first. It must then be enabled after the new database is added to the configuration.

Answer: A, B, C

Explanation:
In the context of Oracle Data Guard and Global Database Services (GDS):
DGMGRL may be used to add the Sales configuration to the Prod pool in gds (A): Data Guard Broker's command-line interface DGMGRL can be utilized to manage configurations with GDS, allowing the addition of Data Guard Broker configurations to GDS pools.
Performing a role change with DGMGRL automatically notifies GDS which in turn activates the appropriate services (B): When a role change is executed using DGMGRL, GDS is automatically notified, and it then activates the services that are appropriate for the new database roles.
DGMGRL may be used to add a single database to the Sales configuration even if Sales is a member of the Prod pool (C): DGMGRL provides the capability to manage individual databases

within a broker configuration, including adding databases to a configuration that is already part of a GDS pool.

Reference:
Oracle Data Guard Broker documentation
Oracle Global Data Services documentation

Question: 40

Which two are true about managing and monitoring Oracle container databases in a Data Guard environment using the broker?

A. If the primary database is not a container database, then a standby may be a container database.
B. If the primary database is a container database, then a physical standby may be a non-container database.
C. If the primary database is a container database, then a logical standby may be a non-container database.
D. All broker actions execute at the root container for container databases.
E. After a role change, the broker opens all Pluggable databases (pdbb) on the new primary.

Answer: D, E

Explanation:
In the context of Oracle Data Guard and container databases (CDBs) managed by Data Guard Broker:
All broker actions execute at the root container for container databases (D): When using Data Guard Broker to manage a CDB, the actions performed by the broker are executed at the level of the root container. This is because the root container maintains the control and configuration information that applies to the entire CDB, including all of its pluggable databases (PDBs).
After a role change, the broker opens all Pluggable databases (PDBs) on the new primary (E): Following a role transition such as a switchover or a failover, Data Guard Broker ensures that all PDBs within the CDB of the new primary database are opened, which is essential to resume operations of the PDBs without manual intervention.

Reference:
Oracle Data Guard Broker documentation
Oracle Multitenant Administrator's Guide

Question: 41

Which TWO are benefits of using Transaction Guard in a Data Guard environment?

A. It protects against user errors being replicated to standby databases.
B. It provides application continuity by rolling back uncommitted transactions interrupted by a failover or switchover.
C. It protects against logical corruptions being replicated to standby databases.
D. It protects against recoverable errors during a planned or an unplanned outage of a primary database.
E. It provides application continuity by replaying transactions interrupted by a failover or a switchover

Answer: B, D

Explanation:
Transaction Guard provides benefits in terms of transaction consistency and recovery in a Data Guard environment:
It provides application continuity by rolling back uncommitted transactions interrupted by a failover or switchover (B): Transaction Guard ensures that any uncommitted transactions at the time of an outage are rolled back consistently, thus preserving the integrity of the application's data and state.
It protects against recoverable errors during a planned or an unplanned outage of a primary database (D): Transaction Guard offers protection against errors that can occur during outages, allowing applications to resume operations more quickly and reliably after recovery.

Reference:
Oracle Database High Availability Overview
Oracle Real Application Clusters Administration and Deployment Guide

Question: 42

Which THREE statements are true about Far Sync instances?

A. The Data Guard Broker must be used to deploy and manage Far Sync instances.
B. They work with any protection level.
C. They enable standby databases to be configured at remote distances from the primary without impacting performance on the primary.
D. They use an spfMe, a standby controlfile, and standby redo logs.
E. A primary database can ship redo directly to multiple Far Sync instances.

Answer: A, C, E

Explanation:
Far Sync instances are a feature of Oracle Data Guard designed to support zero data loss protection over long distances:

The Data Guard Broker must be used to deploy and manage Far Sync instances (A): Data Guard Broker simplifies the deployment and management of Far Sync instances, which are an integral part of zero data loss protection configurations.

They enable standby databases to be configured at remote distances from the primary without impacting performance on the primary (C): Far Sync instances are designed to receive redo from the primary database and then forward it to a remote standby database, thereby avoiding any performance impact on the primary database itself.

A primary database can ship redo directly to multiple Far Sync instances (E): A primary database can be configured to send redo logs to more than one Far Sync instance, which can then forward the redo to their respective remote standby databases.

Reference:
Oracle Data Guard Concepts and Administration Guide
Oracle Database High Availability Overview

Question: 43

Which TWO statements are true about Real-Time Query?

A. Setting standby_max_data_delay=0 requires synchronous redo transport.
B. Real-Time Query has no limitations regarding the protection level of the Data Guard environment.
C. Disabling Real-Time Query prevents the automatic start of redo apply when a physical standby databases opened read only.
D. Real-Time Query sessions can be connected to a Far Sync instance.
E. A standby database enabled for Real-Time Query cannot be the Fast-Start Failover target of the Data Guard configuration.

Answer: A, C

Explanation:
Real-Time Query is a feature that allows queries to be run on a physical standby database while it is applying redo data. The relevant truths about it are:

Setting standby_max_data_delay=0 requires synchronous redo transport (A): For the real-time apply feature to function with no data delay (zero delay), synchronous redo transport must be used. This setting ensures that the data on the standby database is as current as possible before queries are executed against it.

Disabling Real-Time Query prevents the automatic start of redo apply when a physical standby database is opened read-only (C): If Real-Time Query is disabled, opening the standby database in read-only mode will not start the redo apply process automatically. Redo apply needs to be manually started to synchronize the standby database with the primary.

Reference:
Oracle Data Guard Concepts and Administration Guide

Question: 44

Which TWO statements correctly describe the behavior of Automatic Block Media Recovery in a Data Guard environment, for a corrupt block in the example tablespace encountered by a session logged in as the SH user?

A. A corrupt block on the primary database can be automatically recovered, using a block from a standby database with Real-Time Query enabled.
B. A corrupt block on the primary database is automatically recovered, using a block from a flashback log from a standby database with Real-Time Query enabled.
C. A corrupt block on a standby database with Real-Time Query enabled, is automatically recovered, using flashback logs from the standby database.
D. A corrupt block on a standby database with Real-Time Query enabled, can be automatically recovered, using a block from the primary database.
E. A corrupt block on the primary database is automatically recovered, using a block from a flashback log from the primary database.

Answer: A, E

Explanation:
Automatic Block Media Recovery can be a significant feature for maintaining data integrity within a Data Guard configuration.
A corrupt block on the primary database can be automatically recovered, using a block from a standby database with Real-Time Query enabled (A): When a corrupted block is encountered on the primary database, Oracle can automatically replace it with a good block from the standby database where Real-Time Query is enabled, leveraging the standby as a source of good data.
A corrupt block on the primary database is automatically recovered, using a block from a flashback log from the primary database (E): If a good block version is available in the flashback logs of the primary database, Automatic Block Media Recovery can use it to recover the corrupted block on the primary.

Reference:
Oracle Database Backup and Recovery User's Guide

Question: 45

Your Data Guard environment has two remote physical standby databases.
Client applications use the local naming method to connect to the primary database instance.
You want applications to automatically connect to the new primary database instance in case of a switchover or a failover.
Which set of actions will fulfill this requirement?

A. Set the LOCAL_LISTENER parameter for all the database instance to register services with the default listener on the primary database host.
B. Create a database service on the primary database that is started automatically by a trigger, when the database role is PRIMARY; modify the connection descriptors used by client applications to include all the standby hosts and connect to the database instance using that service name.
C. Set DB_NAME and DB_UNIQUE_NAME identically on all databases; modify the connection descriptors on client applications to include all the standby hosts and connect to the database instance using that service name.
D. Set the INSTANCE NAME parameter identically on all databases; modify the connection descriptor on client applications to include all the standby hosts and connect to the database instance using that service name.

Answer: B

Explanation:
For seamless client redirection in a Data Guard environment, the following steps should be taken:
Create a database service on the primary database that is started automatically by a trigger when the database role is PRIMARY (B): This ensures that the service is only available on the primary database and is automatically started after a role transition due to switchover or failover.
Modify the connection descriptors used by client applications to include all the standby hosts and connect to the database instance using that service name (B): Client applications use the connection descriptors that include all potential primary hosts (i.e., the current primary and all standbys). This enables clients to connect to whichever database is currently acting as the primary using the service name.

Reference:
Oracle Data Guard Concepts and Administration Guide
Oracle Real Application Clusters Administration and Deployment Guide

Question: 46

Your Data Guard environment contains a four-instance RAC primary database whose SID is PROD and a RAC physical standby database whose std is PROD_SBY.
Examine the command executed on a node of the primary database cluster to create a service OLTPWORKLOAD that the applications will use to connect to the database when it is in the FRlMARYTclatabase role:
srvctl add service -db PROD -service oltpworkload -role PRIMARY -failovertype SESSION -failovermethod BASIC -failoverdelay 10 -failoverretry 150
The service is then started
Consider this list of tasks:
1. On a node of the standby database cluster execute:

srvctl add service -db PROD_SBY -service oltpworkload -role PRIMARY -failovertype SESSION -failovermethod BASIC -failoverdelay 10 -failoverretry 150
2. On the primary database, create the oltpworkload database service using the dbms_service.create_service procedure.
3. Configure tap for clients in the tnsnames.ora files.
4. Make sure clients use the OLTPWORKLOAD service to connect to the database instances.
5. On the standby database, create the oltpworkload database service using the dbms_service.create_servi;l procedure.
Identify the required steps to configure and use Transparent Application Failover (taf).

A. 4
B. 2,3,4
C. 5
D. 1.4
E. 3,4
F. 1,3,4

Answer: D

Explanation:
To set up Transparent Application Failover (TAF) in a Data Guard environment with RAC, you would need to:
On a node of the standby database cluster, execute the srvctl command to add the oltpworkload service for the PRIMARY role (1): This prepares the standby cluster to provide the oltpworkload service in case a failover occurs, and the standby becomes the primary database.
Make sure clients use the OLTPWORKLOAD service to connect to the database instances (4): This ensures that client connections are directed to the correct service, which is managed by TAF and can fail over in case of a primary database outage.

Reference:
Oracle Real Application Clusters Administration and Deployment Guide
Oracle Data Guard Concepts and Administration Guide

Question: 47

Examine the Data Guard configuration:
DGMGRL> show configuration;
Configuration - Animals
Protection Mode: Max Availability
Databases:
dogs - Primary database sheep
- Physical standby database cats
- Physical standby database
Fast-Start Failover: DISABLED
Configuration Status: SUCCESS

An attempt to enable fast-start failover raises an error:

```
DGMGRL> enable fast_start failover;
Error: ORA-16693: requirements not met for enabling fast-start failover
Failed.
```

Identify three possible reasons for this error.

A. The fastStartFailoverTarget property is not set on Dogs.
B. The LogxptModr property is set to async on Sheep while Sheep is the target standby database.
C. The LogXptMode property is set to FASTSYNC on Cats while Sheep is the target standby database.
D. The LogXptMode property is set to async on Dogs.
E. The LogXptMode property is set to fastsync on Dogs.

Answer: A, B, D

Explanation:
When enabling fast-start failover, certain conditions must be met:
The fastStartFailoverTarget property is not set on Dogs (A): The primary database (Dogs) needs to have a fast-start failover target configured for the operation to succeed.
The LogXptMode property is set to ASYNC on Sheep while Sheep is the target standby database (B): Fast-start failover requires synchronous redo transport (SYNC or FASTSYNC) to ensure zero data loss, which is a prerequisite for enabling the feature.
The LogXptMode property is set to ASYNC on Dogs (D): Similar to the previous point, the primary database must be configured to use synchronous redo transport for the fast-start failover to be possible.

Reference:
Oracle Data Guard Broker documentation
Oracle Database Error Messages Guide

Question: 48

Which three are prerequisites for enabling Fast-Start Failover?

A. The Data Guard environment must be managed by the Data Guard Broker.
B. Flashback Database must be enabled only on the Fast-Start Failover target standby database.
C. You can specify only one standby database as the fast-start failover target.
D. The configuration must be operating in either Maximum Performance or Maximum Protection mode.
E. The maximum protection mode can be used, but with two or more standby databases.
F. Flashback Database must be enabled on both the primary database and the Fast-Start Failover target standby database.

Answer: A, C, F

Explanation:
To enable Fast-Start Failover in a Data Guard environment, the following conditions must be in place:
The Data Guard environment must be managed by the Data Guard Broker (A): The Broker simplifies management tasks and is required to enable fast-start failover, which is an automatic failover mechanism provided by Data Guard.
You can specify only one standby database as the fast-start failover target (C): Fast-start failover is designed to fail over to a single, predetermined standby database, known as the target standby.
Flashback Database must be enabled on both the primary database and the Fast-Start Failover target standby database (F): Flashback Database provides a quick way to revert a database to a point in time before a logical or physical corruption or error occurred. It must be enabled on both the primary and target standby databases to allow for the possibility of reinstating the old primary as a standby after a failover.

Reference:
Oracle Data Guard Concepts and Administration Guide
Oracle Database High Availability Overview

Question: 49

Examine this list of possible steps:
1. Raise the compatibility level on both databases.
2. Restart SQL Apply on the upgraded logical standby database.
3. Start SQL Apply on the old primary database.
4. Perform a Switchover to the logical standby database.
5. Upgrade the logical standby database.
6. Upgrade the old primary database.

Which is the minimum number of steps in the correct order, to perform a rolling release upgrade of a data guard environment using an existing logical standby database and to enable the new functionality?

A. 1,5,2,4,6,3
B. 5,2,4,6,3,1
C. 4,6,5,2,3,1
D. 5,2,4,1
E. 5,2,4,3,6,1

Answer: A

Explanation:

The process of performing a rolling release upgrade in a Data Guard environment using a logical standby database generally involves these steps:
Raise the compatibility level on both databases (1): Ensuring both the primary and logical standby databases are operating with the same and correct compatibility level is essential before starting the upgrade process.
Upgrade the logical standby database (5): Apply the database upgrade to the logical standby first, which allows the primary database to continue serving the workload without interruption.
Restart SQL Apply on the upgraded logical standby database (2): Once the logical standby has been upgraded, SQL Apply must be restarted to apply the redo data from the primary database, which is still running the earlier version.
Perform a switchover to the logical standby database (4): After confirming that the logical standby database is successfully applying redo data, perform a switchover to make it the new primary database.
Upgrade the old primary database (6): With the new primary database now in place, upgrade the old primary database (which is now the new standby) to the new Oracle Database release.
Start SQL Apply on the old primary database (3): Finally, start SQL Apply on what is now the standby database to synchronize it with the new primary database.

Reference:
Oracle Data Guard Concepts and Administration Guide
Oracle Database Upgrade Guide

Question: 50

Which three actions are performed by the START PLAN procedure of the DBMS ROLLING package?

A. converting the designated physical standby database into a logical standby database
B. creating a guaranteed restore point on the standby databases
C. building a LogMiner dictionary on the primary database instance
D. creating a guaranteed restore point on the primary database
E. starting media recovery on all the Leading Group Standby databases
F. switching the primary database to the logical standby role

Answer: B, C, D

Explanation:
The DBMS_ROLLING package facilitates a rolling upgrade process across a Data Guard configuration. The START PLAN procedure in particular handles several critical actions, including:
Creating a guaranteed restore point on the standby databases (B): This ensures that the standby databases can be reverted to their state before the rolling upgrade process in case of any issues.
Building a LogMiner dictionary on the primary database instance (C): This is necessary for logical standby databases to interpret redo data during the SQL Apply process.
Creating a guaranteed restore point on the primary database (D): Similar to the standby databases, this ensures that the primary database can be reverted to a known good state if

necessary.

Reference:
Oracle Database PL/SQL Packages and Types Reference
Oracle Data Guard Concepts and Administration Guide

Question: 51

You detected an unrecoverable archive gap in your data guard environment. So, you need to roll standby.
forward in time without applying a large number of archive log files using this command:
RMAN> RECOVER STANDBY DATABASE FROM SERVICE-<primary database name>;
When running this command, which of the following steps can be performed automatically?

1. Remember all data file names on the standby.
2. Restart standby in nomount.
3. Restore controlfile from primary.
4. Mount standby database.
5. Rename data files from stored standby names.
6. Restore new data files to new names.
7. Recover standby.

A. 2,3,5,6,7
B. 2,3,6,7
C. 1,3,5,6,7
D. 1,2,3,4,5,6,7
E. 1, 2,3,4,6,7

Answer: E

Explanation:
The RECOVER STANDBY DATABASE FROM SERVICE command in RMAN is designed to automate various steps required to recover the standby database, especially when dealing with an archive gap. When this command is executed, the following actions can occur automatically:
Remember all data file names on the standby (1): RMAN has the capability to recall the names and paths of all data files associated with the standby database.
Restart standby in nomount (2): The standby database can be automatically restarted in the NOMOUNT state, allowing recovery operations to proceed without the database being open.
Restore controlfile from primary (3): RMAN can restore the control file from the primary database to the standby system, ensuring that the standby has the most up-to-date control file.
Mount standby database (4): After restoring the control file, the standby database is mounted to prepare for data file recovery.
Rename data files from stored standby names (5): Not typically done automatically by this command.
Restore new data files to new names (6): New data files added to the primary since the last synchronization can be restored to the standby with their correct names.

Recover standby (7): Finally, RMAN will apply any necessary redo logs to bring the standby database up to date with the primary.

While some steps, such as renaming data files (5), typically require manual intervention or scripting, most of the recovery process can be handled by RMAN automatically, streamlining the recovery of the standby database.

Oracle Database Backup and Recovery User's Guide

Oracle Data Guard Concepts and Administration Guide

Question: 52

Examine this validate command:

DGMGRL> VALIDATE DATABASE VERBOSE "<database name>";

Which THREE statements are TRUE?

A. The command performs a comprehensive set of database checks prior to a role change.

B. The command performs a comparison of SPFILE entries between the primary database and a specified standby database.

C. The command performs network connectivity checks between members of a broker configuration.

D. The command can be used for a logical standby database.

E. The command uses information available in various Oracle Data Guard views as well as the Automatic Diagnostic Repository.

Answer: A, C, D

Explanation:

The command performs a comprehensive set of database checks prior to a role change (A): The VALIDATE DATABASE command in Data Guard Manager (DGMGRL) is designed to perform an exhaustive check of a specified database's readiness for a role change, such as a switchover or failover.

The command performs network connectivity checks between members of a broker configuration (C): One of the checks includes verifying that the necessary network connectivity exists between the databases in a Data Guard Broker configuration.

The command can be used for a logical standby database (D): The VALIDATE DATABASE command is versatile and can be used for both physical and logical standby databases to ensure their readiness for role changes.

Oracle Data Guard Broker documentation

Oracle Data Guard Concepts and Administration Guide

Question: 53

Which two statements are true when using non-rolling release upgrades in a Data Guard environment?

A. The compatible parameter on a standby database that is applying redo, must be equal to or greater than the compatible parameter on the primary that is shipping redo to that standby.
B. Modifications to the data dictionary on the primary database caused by the upgrade, are applied on a logical standby database.
C. Modifications to the data dictionary on the primary database caused by the upgrade, are applied on a physical standby database.
D. During the upgrade of a logical standby database, standby redo log files must reside on O/S file systems.
E. User equivalence must be established for the owner of the Oracle software on the affected hosts prior to the upgrade.

Answer: A, C

Explanation:
The compatible parameter on a standby database that is applying redo, must be equal to or greater than the compatible parameter on the primary that is shipping redo to that standby (A): This ensures that the standby database can apply redo from the primary, even after the primary has been upgraded. The COMPATIBLE parameter setting on the standby database should not preclude it from understanding the redo it receives.
Modifications to the data dictionary on the primary database caused by the upgrade, are applied on a physical standby database (C): When the primary database undergoes a non-rolling upgrade, any resulting data dictionary changes are transmitted through redo data and applied to the physical standby database.
Oracle Database Upgrade Guide
Oracle Data Guard Concepts and Administration Guide

Question: 54

Which FOUR database parameters might be affected by or influence the creation of standby databases?

A. DB_NAME
B. ARCHIVE_LAG_TARGET
C. db_file_name_convert
D. COMPATIBLE
E. FALSERVER
F. STANDBY_ARCHIVE_DEST

Answer: A, C, D, F

Explanation:
DB_NAME (A): The name of the database, which should remain consistent across the primary and standby databases.

db_file_name_convert (C): This parameter helps define the mapping of data file names from the primary to the standby database, which is crucial during the creation and operation of a standby database.
COMPATIBLE (D): The compatibility level can influence the features that can be used on the standby database and must be consistent with or higher than that of the primary database, especially after upgrades.
STANDBY_ARCHIVE_DEST (F): This parameter specifies the destination of archived redo log files on the standby database, which is important for log transport and apply services.
Oracle Data Guard Concepts and Administration Guide
Oracle Database Reference

Question: 55

Which TWO statements are true about configuring Oracle Net Service in a Data Guard environment?

A. A static service must be registered with the local listener to enable DGMGRL to restart instances during the course of broker operations.
B. Install the oracle-database-preinstall-19c package to set the kernel parameters for Oracle Net based on the Data Guard best practice guidelines.
C. Installing the oracle-database-preinstall-19c package is NOT sufficient to set up operating system kernel parameters for Oracle Net.
D. Enterprise Manager does not require static service registration to restart instances during the course of broker operations.
E. It is necessary to use the failover clause for an address_list with multiple address lists in the tnsnames.ora file.

Answer: A, C

Explanation:
A static service must be registered with the local listener to enable DGMGRL to restart instances during the course of broker operations (A): For DGMGRL (Data Guard Manager Command-Line Interface) to perform instance management operations, such as restarting instances, a static service registration in the listener is required. This allows the broker to connect to the database instance even when the instance is not fully up and the dynamic service registration is not available.
Installing the oracle-database-preinstall-19c package is NOT sufficient to set up operating system kernel parameters for Oracle Net (C): While the oracle-database-preinstall-19c package automates the setting of several kernel parameters to meet the preinstallation requirements for Oracle Database, it does not specifically tailor all settings for Oracle Net in a Data Guard configuration. Additional manual configuration may be required to optimize Oracle Net services for Data Guard operations.
Oracle Data Guard Broker documentation
Oracle Net Services Administrator's Guide

Question: 56

A customer asks for your recommendation regarding this requirement:
1. We plan to have a Data Guard Configuration with one primary database and one physical standby database.
2. We want zero data loss in case of a disaster involving the loss of one component.
3. We want to do Real Application Testing occasionally on the Standby Database.
Which solution, if any, satisfies these requirements?

A. These requirements cannot be met.
B. A physical standby database with synchronous redo transport that can be converted regularly into a snapshot standby to do real application testing
C. A snapshot standby database with real time query that can be converted regularly into a physical standby database open read write, to do real application testing
D. A far sync instance plus a snapshot standby database and real time apply that can be converted regularly into logical standby database to do real application testing

Answer: B

Explanation:
Synchronous redo transport for zero data loss (B): To guarantee zero data loss in the case of a disaster, synchronous redo transport must be configured between the primary and standby databases.
Conversion to snapshot standby for testing (B): A physical standby database can be temporarily converted into a snapshot standby database to perform real application testing. After testing is completed, the snapshot standby can be converted back to a physical standby to resume its disaster recovery role.
Oracle Data Guard Concepts and Administration Guide
Oracle Database Testing Guide

Question: 57

Which two are prerequisites for configuring flashback database for Oracle 19c databases, in a Data Guard environment?

A. A far sync instance must be configured to flash back a standby when the primary has been flashed back.
B. A fast recovery area must be configured.
C. The database must be in ARCHTVELOG mode.
D. The Data Guard real-time apply feature must be enabled.
E. The data guard broker must be used.

Answer: B, C

Explanation:
A fast recovery area must be configured (B): Flashback Database requires a fast recovery area to be set up because flashback logs are stored there. The fast recovery area is a unified storage location for all recovery-related files and activities.
The database must be in ARCHIVELOG mode (C): Flashback Database operation relies on the ability to archive redo logs. Therefore, the database must be running in ARCHIVELOG mode for Flashback Database to be enabled.
Oracle Database Backup and Recovery User's Guide
Oracle Data Guard Concepts and Administration Guide

Question: 58

You must configure flashback database for your Oracle 19c databases that will be part of a Data Guard Broker configuration.
The databases are all in ARCHIVELOG mode.
You will execute the SQL statement:
ALTER DATABASE FLASHBACK ON;
Which three are true concerning this command?

A. It will execute successfully while an Oracle 19c primary database is open.
B. It will execute successfully while an Oracle 19c primary database is mounted.
C. It will execute successfully on an Oracle 19c physical standby database while Real Time Query is active.
D. If executed successfully on an Oracle 19c primary database, flashback will also be enabled on all logical standby databases that are part of the configuration.
E. It will execute successfully on an Oracle 19c logical standby database while SQL apply is active.
F. If executed successfully on an Oracle 19c primary database, flashback will also be enabled on all physical standby databases that are part of the configuration.

Answer: A, B, E

Explanation:
The command ALTER DATABASE FLASHBACK ON; enables the Flashback Database feature, which provides a way to quickly revert an entire Oracle database back to a previous point in time. This command can be executed while an Oracle 19c primary database is either open (option A) or mounted (option B). It is also applicable to an Oracle 19c logical standby database while SQL Apply is active (option E). However, it's important to note that enabling Flashback Database on the primary does not automatically enable it on all associated standby databases, whether they are physical or logical. Each database in a Data Guard configuration must have Flashback Database explicitly enabled if desired. Real Time Query being active on a physical standby does not directly relate to the ability to execute this command on the standby. The explanation is based on Oracle's concepts for Flashback Technology and Data Guard configurations as detailed

in the Oracle Database Backup and Recovery User's Guide and the Oracle Data Guard Concepts and Administration guide.

Question: 59

Which three are true concerning database states after a successful switchover?

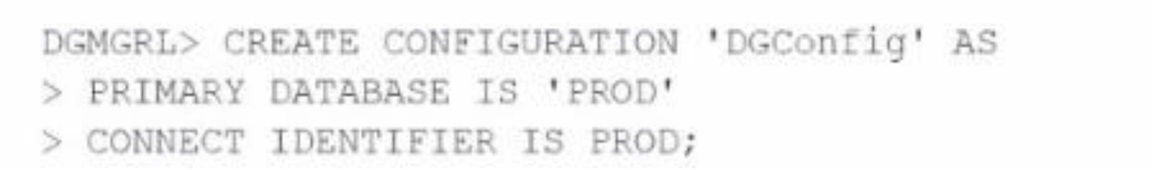
A. The new primary database will be open read-write.
B. If the former primary database became a logical standby database it will be in mount state.
C. If the former primary database became a logical standby database it will be open read-write.
D. If the former primary database became a physical standby database it will be in the same state as the former physical standby database.
E. If the former primary database became a physical standby database it will always be open readonly.
F. The former primary database will always be open.

Answer: A, C, D

Explanation:
After a successful switchover operation in a Data Guard environment, the new primary database (the former standby) will be open read-write (option A). If the former primary database transitions to a logical standby database, it will also be open read-write (option C), allowing it to apply redo data while servicing read-only queries. The former primary, if converted to a physical standby, will adopt the state that the former physical standby database was in prior to the switchover, which can vary based on the configuration prior to the switchover (option D). The state of a physical standby database can range from mounted to open read-only, depending on whether Real-Time Query was enabled. Thus, the exact state will depend on the pre-switchover setup. It's also essential to highlight that options B and E suggest specific states for a former primary turned logical standby, and a former primary turned physical standby, respectively, but these states are not fixed and depend on the configurations set up by the database administrators. The answers are corroborated by Oracle's documentation on Data Guard switchovers, specifically in the Oracle Data Guard Concepts and Administration guide, which explains the roles and states of databases in a Data Guard configuration before and after switchovers.

Question: 60

You created the PRODSBY1 physical standby database for the PROD primary database using gql and RMAN. You are planning to create a Data Guard Broker configuration. You execute the command:



```
DGMGRL> CREATE CONFIGURATION 'DGConfig' AS
> PRIMARY DATABASE IS 'PROD'
> CONNECT IDENTIFIER IS PROD;
```

Which three statements are true regarding the execution of the command?

A. The command will execute successfully only if the DG_BROKER_START initialization parameter is set to TRUE for the PROD database instance.
B. The PRODSBY1 standby database is automatically added to the configuration if DG_BROKER_START is TRUE for PRODSBYl.
C. The PRODSBYI standby database is automatically added to the configuration if Oracle Net connectivity to the PRODSBYl database instance is defined on the primary host.
D. The command will execute successfully only if Oracle Net connectivity to the PROD database instance is defined on the primary host.
E. The Data Guard Broker configuration files is automatically created in the destinations specified by the DG_BROKER_CONFIG_FILEn initialization parameters on the primary database.
F. The command will execute successfully only if Oracle Net connectivity to the PROD and PRODSBYl database instances are defined on the primary host.

Answer: A, D, E

Explanation:
The command executed (CREATE CONFIGURATION 'DGConfig' AS PRIMARY DATABASE IS 'PROD' CONNECT IDENTIFIER IS PROD;) is used to create a Data Guard Broker configuration named 'DGConfig'. The successful execution of this command depends on several conditions:
A: The DG_BROKER_START parameter must be set to TRUE on the primary database to start the Data Guard Broker processes. Without the broker processes running, the configuration cannot be created.
D: Oracle Net connectivity to the PROD database instance must be established on the primary host. This is because the Data Guard Broker requires network accessibility to communicate with the primary database and manage the configuration.
E: When the configuration is created, the Data Guard Broker configuration files are indeed automatically created in the locations specified by the DG_BROKER_CONFIG_FILEn parameters on the primary database.
It's important to note that the command will not automatically add the PRODSBY1 standby database to the configuration (thus B and C are not correct), and there is no requirement for the standby database to have Oracle Net connectivity defined on the primary host for the execution of this command (making F incorrect as well).

Question: 61

You created a physical standby database prodsbyi from the primary database prod using SQL and RMAN. Which THREE are prerequisites for creating a Data Guard Broker configuration to manage these databases?

A. A local net service name to enable connectivity to the PRODSBYI database instance must be defined on the primary database host.
B. The primary database must have supplemental logging enabled.
C. The LOG_ARCHIVE_DEST_n parameters with the service attribute set must be cleared.
D. The standby database must have supplemental logging enabled.
E. The primary database must have FORCE LOGGING enabled.
F. The DG_BROKER_START parameter must be set to TRUE for both database instances.

Answer: A, B, F

Explanation:
When setting up a Data Guard Broker configuration for a primary database and its physical standby, the following prerequisites must be met:
A: Oracle Net connectivity must be defined on both the primary and standby hosts to enable the respective database instances to communicate with each other.
B: Supplemental logging is required on the primary database because it provides additional logging necessary for the standby database to be able to apply changes from the primary database accurately.
F: The DG_BROKER_START parameter must be set to TRUE for both the primary and standby database instances. This parameter is used to start the Data Guard Broker process which manages the configuration.
Options C and D are not prerequisites for creating a Data Guard Broker configuration. Additionally, while FORCE LOGGING mode (option E) is recommended as a best practice to prevent possible data inconsistencies during media recovery, it is not a strict prerequisite for creating a Data Guard Broker configuration.

Question: 62

Which TWO are TRUE about offloading backups to a physical standby database in a Data Guard environment?

A. The standby database must be registered in an RMAN catalog after the primary database has been registered.
B. The standby database can not be registered in an RMAN catalog if the primary database has not been registered.
C. Backups of the standby control file taken while connected to the catalog where the database is registered, may be used to restore the control file on the primary database.
D. The standby database must be registered in an RMAN catalog before the primary database has been registered.

Answer: A, C

Explanation:

In a Data Guard environment, offloading backups to a physical standby database has certain requirements:
A: Once the primary database is registered in an RMAN catalog, the standby database can also be registered. This allows RMAN to manage backups coherently across both databases and leverage the standby database for backup purposes without interfering with the primary database's workload.
C: Backups of the standby control file taken while connected to the catalog where the database is registered can be used to restore the control file on the primary database. This ensures that backup metadata is consistent across the Data Guard configuration.
Options B and D are incorrect because there is no strict requirement for the order in which the primary and standby databases must be registered in an RMAN catalog. However, it is a common practice to register the primary database first.

Question: 63

Which three statements are true about snapshot standby databases?

A. The FATLOVER TO   command results in a transition of a snapshot standby database to the primary role.
B. Tablespaces can be dropped.
C. Tablespaces can be created.
D. The switchover TO   command allows a switchover operation to a snapshot standby database.
E. Tables can be dropped.
F. A logical standby database can be converted into a snapshot standby database.

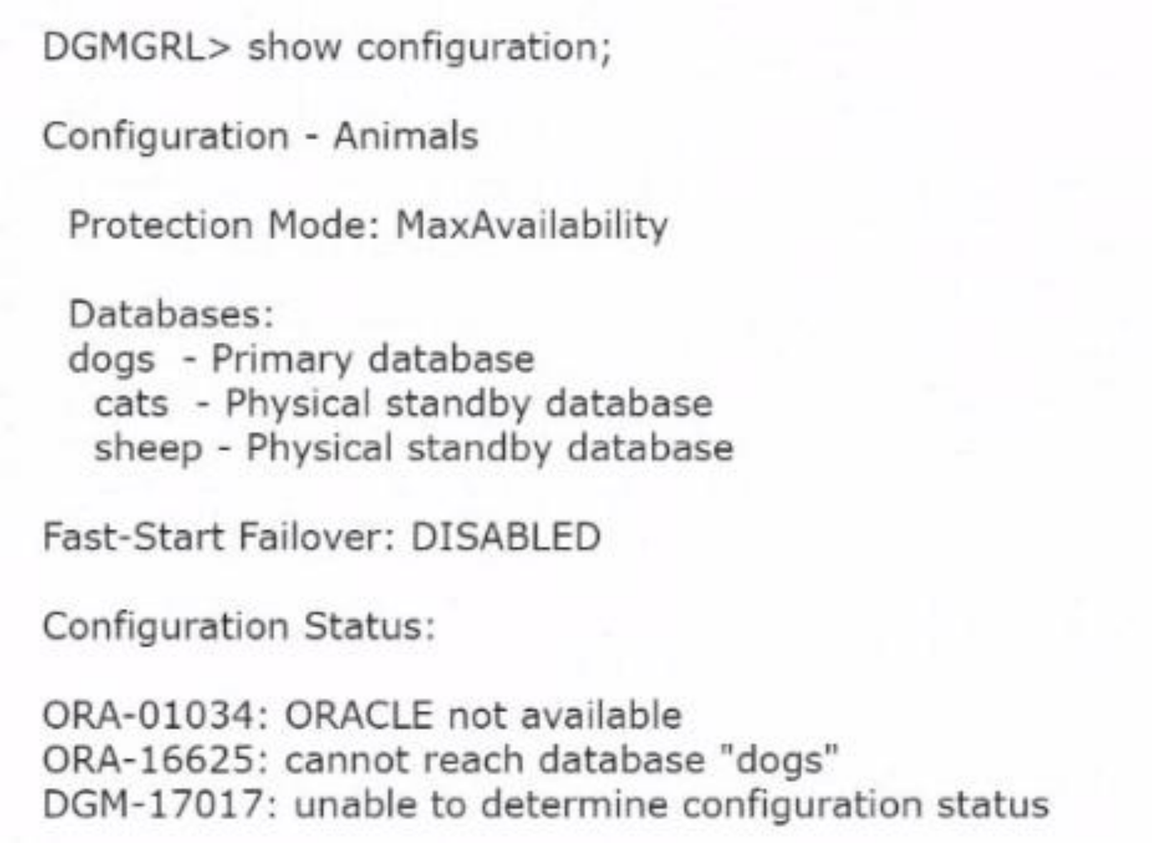
Answer: B, C, E

Explanation:
A snapshot standby database is a fully updateable standby database that is created by converting a physical standby database into a snapshot standby database. The main characteristics of a snapshot standby database include:
B: Tablespaces can indeed be dropped in a snapshot standby database because it is updateable and allows all types of DML and DDL operations that do not conflict with the standby role.
C: Tablespaces can be created in a snapshot standby database for the same reasons that they can be dropped; it supports all operations that do not interfere with its standby nature.
E: Tables can be dropped in a snapshot standby database, as it is a fully updateable standby.
Options A and D are incorrect because 'FAILOVER TO' and 'SWITCHOVER TO' commands are not used with snapshot standby databases in these contexts. A failover converts a standby database into the primary role after the original primary has become unavailable, and is not a reversible role transition. Switchover is a planned role reversal between the primary database and one of its standby databases and is not applicable to snapshot standby databases in the context provided.
Option F is incorrect because a logical standby database cannot be converted into a snapshot standby database directly. A logical standby is used for different purposes such as reporting and

querying with real-time data, and its structure is different from a physical standby which can be converted into a snapshot standby.

Question: 64

Examine the Data Guard configuration:



```
DGMGRL> show configuration;

Configuration - Animals

  Protection Mode: MaxAvailability

  Databases:
  dogs  - Primary database
    cats  - Physical standby database
    sheep - Physical standby database

Fast-Start Failover: DISABLED

Configuration Status:

ORA-01034: ORACLE not available
ORA-16625: cannot reach database "dogs"
DGM-17017: unable to determine configuration status
```

Which three will be true after a successful failover to Cats?

A. The configuration will be in Maximum Performance mode.
B. Sheep will be in the enabled state.
C. Sheep will be in the disabled state.
D. Dogs will be in the disabled state and has to be manually reinstated.
E. The configuration will be in Maximum Availability mode.

Answer: B, D, E

Explanation:
After a successful failover to the 'cats' database in a Data Guard configuration:
B: Sheep, being another standby database, would typically remain in the enabled state unless specifically disabled or if there was a configuration issue.

D: Dogs, which was the primary database prior to failover, will be in a disabled state as part of the failover process. Manual intervention is required to re-establish 'dogs' as a standby database or to return it to the primary role through another role transition.
E: If the configuration was in Maximum Availability mode before failover, it would remain in this mode after failover, provided all settings were properly configured and no changes were made to the protection mode.
Option A is incorrect because failover does not automatically change the protection mode to Maximum Performance. The protection mode remains as it was prior to the failover unless manually altered.

Question: 65

Which THREE statements are TRUE about the supported workload in Active Data Guard standby databases?

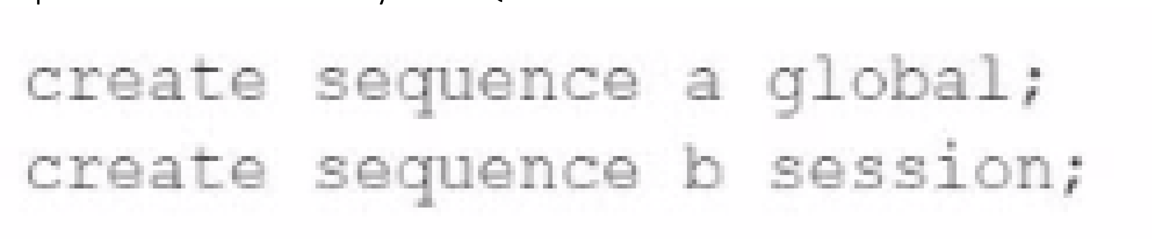
A. PL/SQL blocks that you run on Active Data Guard standby databases can be always redirected to and run on the primary database.
B. Read-mostly reporting applications that use global temporary tables for storing temporary data can be offloaded.
C. You might have to use sequences with global temporary tables to support read-mostly applications by using Active Data Guard.
D. The DDL operations on private temporary tables are transparently redirected to the primary database.
E. The DML operations on a standby can be transparently redirected to and run on the primary database

Answer: B, C, E

Explanation:
In an Oracle Active Data Guard environment:
B: Read-mostly reporting applications that utilize global temporary tables to store session-specific data can be effectively offloaded to an Active Data Guard standby database, reducing the load on the primary database.
C: Sequences can be used with global temporary tables on an Active Data Guard standby database to support certain types of read-mostly applications, though some restrictions on sequence use may apply.
E: In Oracle Database 19c and later, DML redirection allows DML operations performed on an Active Data Guard standby database to be transparently redirected to the primary database. This is part of the DML Redirection feature.
Option A is incorrect because not all PL/SQL blocks run on an Active Data Guard standby database can be redirected to the primary database. Some PL/SQL executions, specifically those that would attempt to make changes to the database, are not supported on the standby.
Option D is incorrect because DDL operations on private temporary tables are not redirected; instead, private temporary tables are session-specific and are not persisted on disk, so they do not generate redo and are not applicable to an Active Data Guard standby.

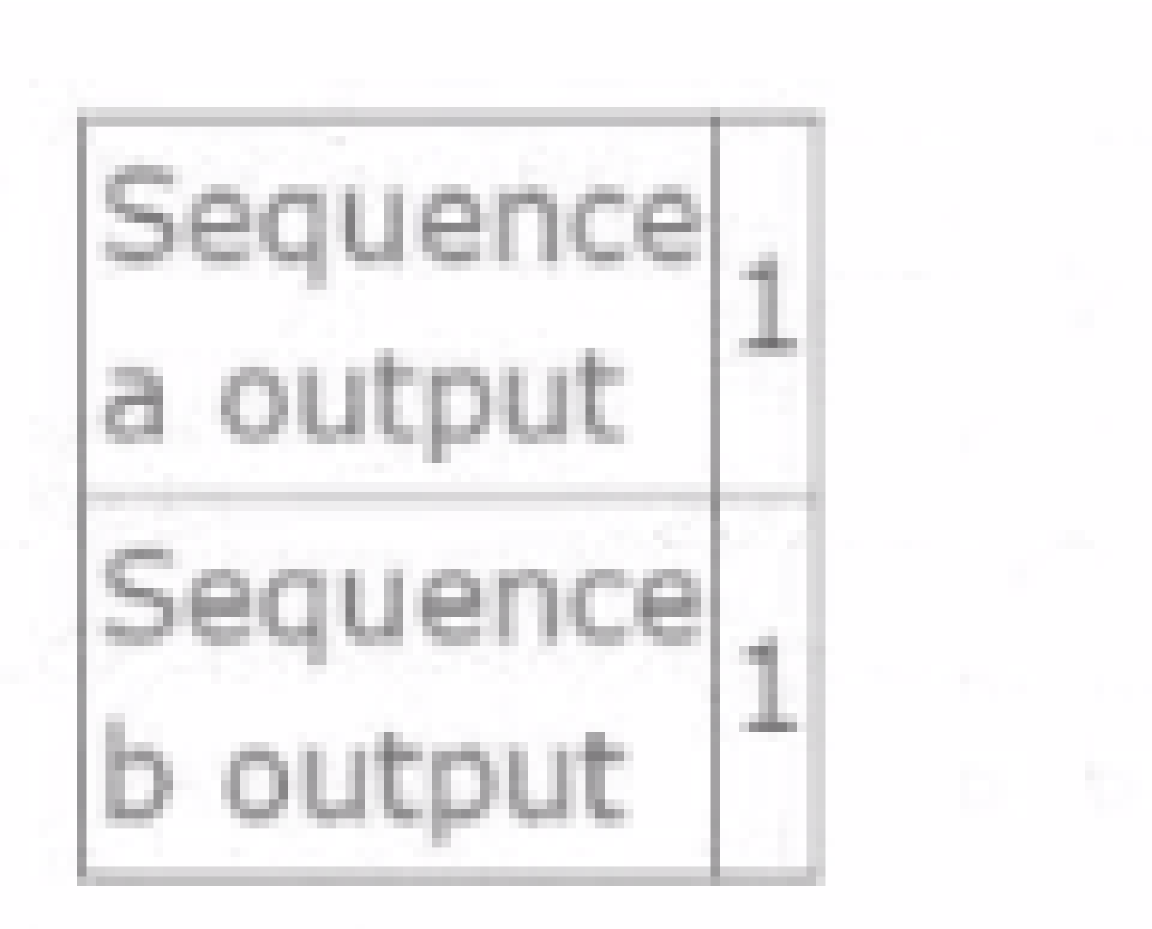
Question: 66

Your Data Guard environment has one physical standby database using Real-Time Query. Two sequences have been created by these SQL statements:



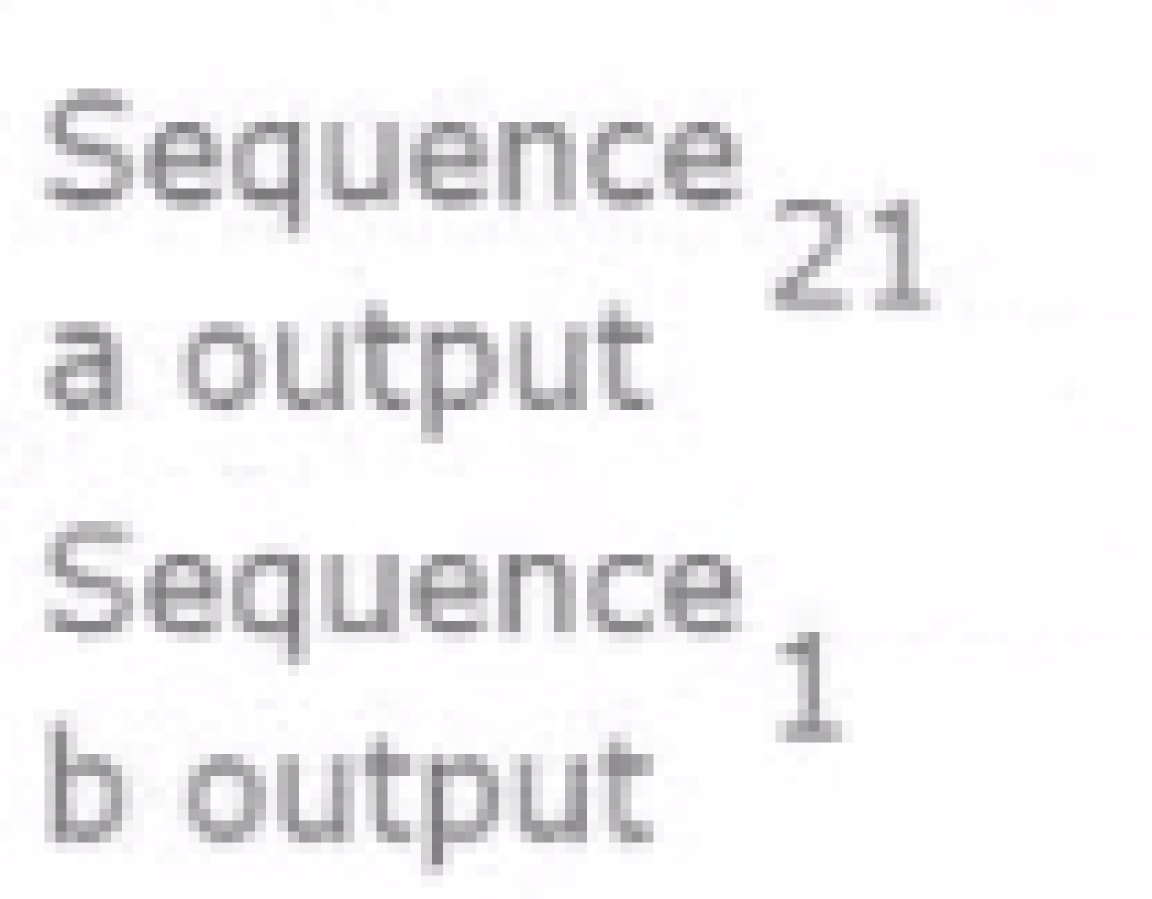
```
create sequence a global;
create sequence b session;
```

Neither sequence has been used since being created.
Session 1 connects to the primary database instance and issues these two SQL statements:
SELECT a.nextval FROM DUAL; SELECT b.nextval FROM DUAL;
Then session 2 connects to the physical standby database instance and issues the same SQL statements. Which output will be seen for session 2?
Then session 2 connects to the physical standby database instance and issues the same SQL statements. Which output will be seen for session 2?
A)



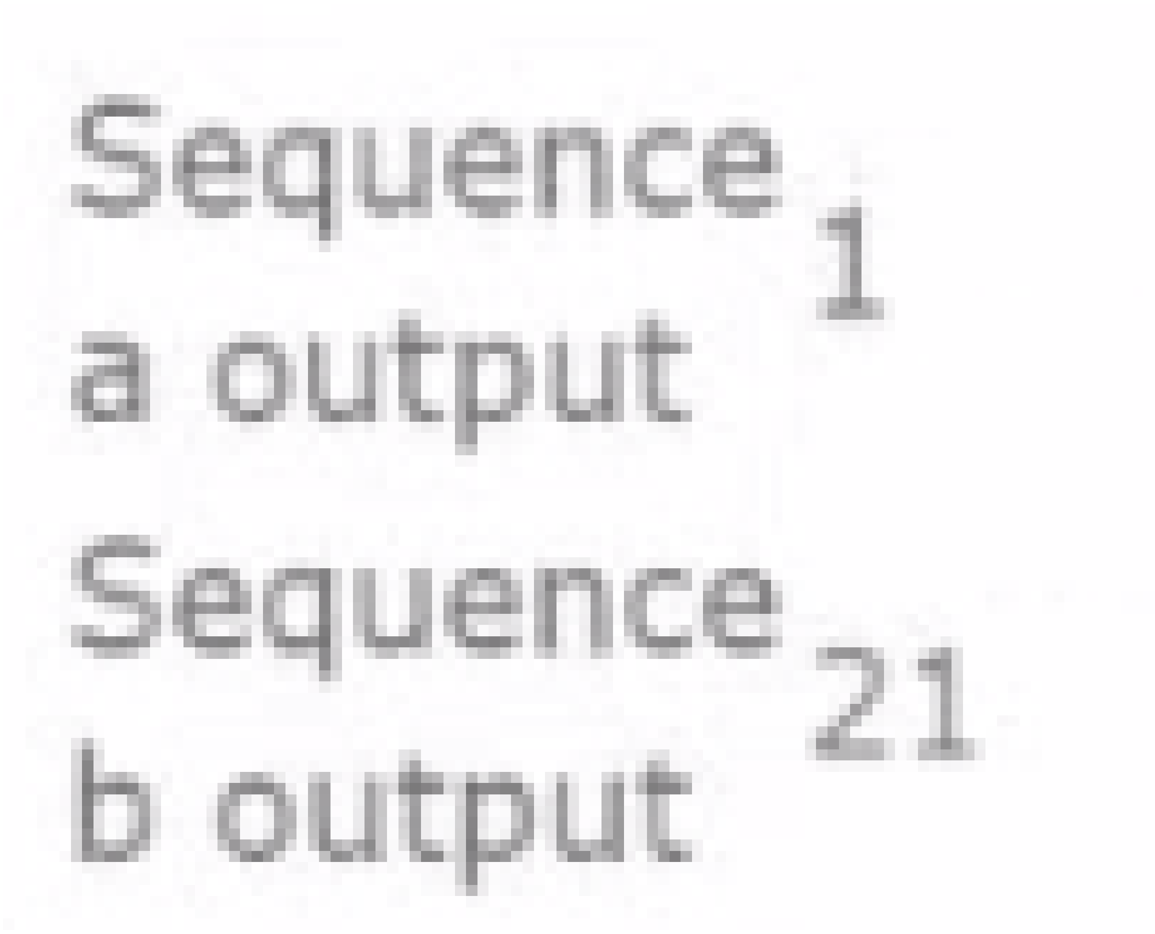
Sequence a output	1
Sequence b output	1

B)

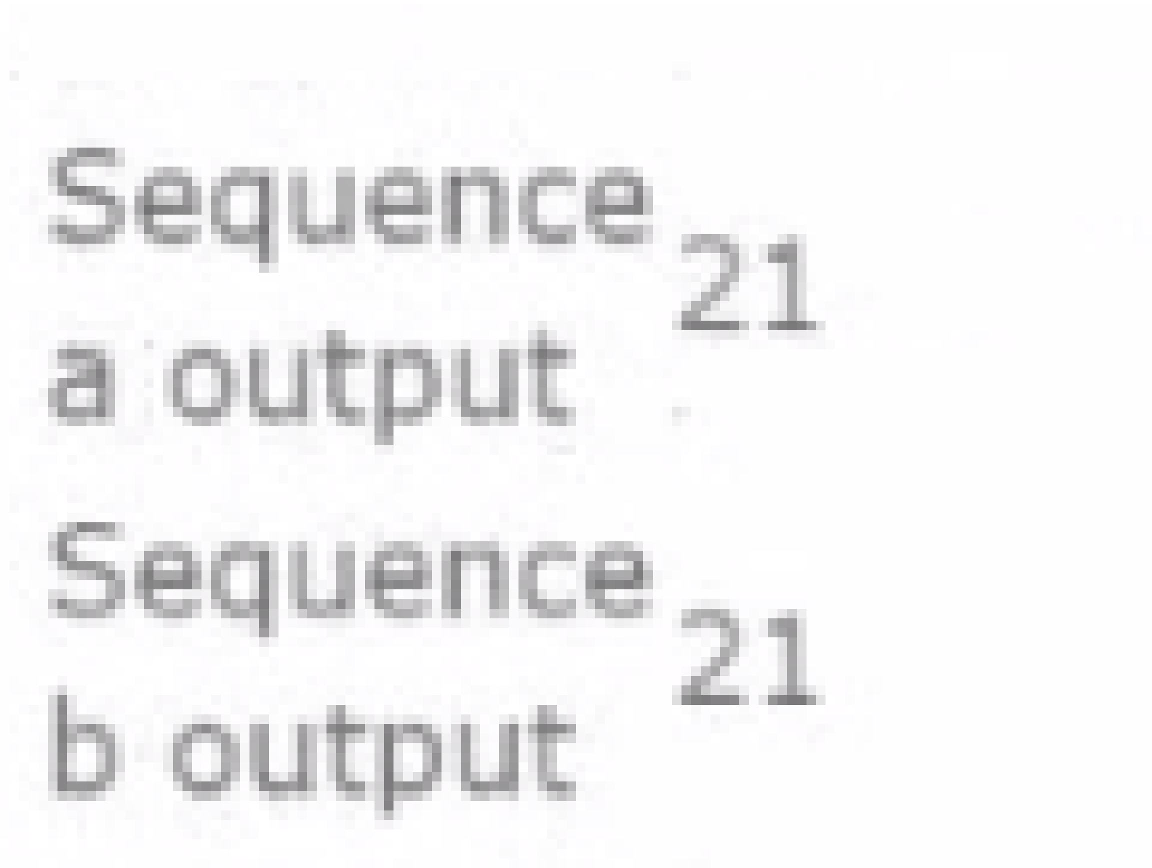


```
Sequence a output   21
Sequence b output   1
```

C)



```
Sequence
a output  1
Sequence
b output  21
```



Sequence a output 21

Sequence b output 21

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation:
In Oracle, a sequence created with the GLOBAL keyword is available and can produce values across all sessions and instances. However, a sequence created with the SESSION keyword is only specific to the session it was created in. When the NEXTVAL is called for a sequence, it will increment according to the sequence's properties set during its creation.
Given the sequence creation statements and the actions performed:
The a sequence is global, which means it is available across the entire database, including the standby database with Real-Time Query enabled. So, when session 2 calls a.nextval, it will get the next value in the sequence, which is 21 since session 1 already retrieved 1.
The b sequence is session-specific, so when session 2 calls b.nextval, it will get the value 1 because for this new session on the standby, this is the first time the sequence is being accessed.
Therefore, the output for session 2 will be a output as 21 and b output as 1, which corresponds to Option C.

Question: 67

Which THREE statements are TRUE about Global Sequences when connected to a physical standby database with Real-Time Query enabled?

A. Their usage will always have a performance impact on the primary database.
B. Their creation requires that a LOG archive_dest_n parameter be defined in the standby that points back to the primary.
C. If the CACHE option is set then the size of the cache must be at least 100.
D. Their usage may have a performance impact on the physical standby database if the CACHE size is too small.
E. They must have the NOORDEK and CACHE options set.

Answer: A, D, E

Explanation:
Global Sequences are Oracle sequences that generate unique values across multiple instances in an Oracle RAC or a Data Guard configuration. Regarding their behavior and performance when connected to a physical standby database with Real-Time Query enabled:
A: The usage of Global Sequences can indeed have a performance impact on the primary database due to the need to generate unique values that are consistent across both primary and standby databases.
D: The performance impact on the physical standby database may occur if the CACHE size is too small. This is because the standby database will frequently have to access the primary database to replenish the cache, which can increase the load and potentially lead to performance degradation.
E: Global Sequences should have the NOORDER and CACHE options set. The NOORDER option ensures that sequence numbers are provided without guaranteeing sequence order, thus improving scalability and performance. The CACHE option is used to specify how many sequence values will be held in memory for faster access.
Option B is incorrect as the LOG_ARCHIVE_DEST_n parameter's definition for standbys pointing back to the primary does not directly pertain to the creation of sequences.
Option C is incorrect because there is no requirement that the size of the cache for a sequence must be at least 100. The CACHE size can be set to a different number based on specific use cases or performance considerations.

Question: 68

You notice that the SQL apply lag on your logical standby database has increased but the redo transport lag has not.
Which four could be reasons for the increase in SQL apply lag?

A. An undersized undo tablespace on the logical standby
B. Many SQL apply operations do full table scans
C. An increased number of bulk updates on the primary
D. An increased number of bulk inserts on the primary
E. The standby redo log files are undersized on the primary database
F. An undersized shared pool

Answer: A, B, C, F

Explanation:
The SQL apply lag on a logical standby database can be caused by several factors:
A: An undersized undo tablespace can lead to delays in SQL apply operations as it may not be able to handle the volume of undo records generated by the SQL apply process.
B: SQL apply operations that do full table scans can consume significant system resources, potentially leading to higher apply lag.
C: An increased number of bulk updates on the primary database may generate a large volume of redo data, which can cause apply lag if the logical standby cannot apply the changes quickly enough.
F: An undersized shared pool may affect the parsing and execution of SQL statements by SQL apply, which can contribute to the apply lag.
Option D is less likely to be a direct cause of SQL apply lag compared to bulk updates, as inserts generate new data rather than modifying existing data, which SQL apply can typically handle more efficiently.
Option E is incorrect because the size of the standby redo log files on the primary database impacts redo transport lag, not SQL apply lag.

Question: 69

There are currently 6 applief. and 6 pfepafef processes running and no idle applier processes on y logical standby database.
The max_SERVERS SQL apply parameter and number of archiver processes are both set to 12.
Identify two changes, each of which would allow you to increase the number of applier processes.

A. Decrease the number of archiver processes on the standby database.
B. Increase the processes initialization parameter. D Decrease the number of FREPARER processes.
C. Increase the value for the MAX_SERVERS SQL apply parameter.
D. Increase the parallel_max_server initialization parameter.
E. Increase the RECOVERY_PARALLEL initialization parameter.

Answer: C, D

Explanation:

To increase the number of applier processes on a logical standby database, the following changes can be made:
C: Increasing the value for the MAX_SERVERS SQL apply parameter would allow for more applier processes to be initiated, assuming that system resources permit.
D: Increasing the PARALLEL_MAX_SERVERS initialization parameter would allow for more parallel execution processes, which can be used by SQL apply to increase the number of applier processes.
Option A is incorrect as decreasing the number of archiver processes will not necessarily increase the number of applier processes; these are unrelated components.
Option B is incorrect because the 'FREPARER' processes do not exist, it seems to be a typographical error, and the 'REPARER' is not a valid Oracle process or parameter.
Option E is incorrect because the RECOVERY_PARALLELISM parameter controls the number of processes used for instance recovery and media recovery, not for SQL apply.

Question: 70

Which four factors can influence the rate of SQL apply on a logical standby database?

A. the number of PREPAER processes
B. the number of coordinator processes on the standby database instance
C. the number of full table scans performed by SQL apply
D. the size of the undo tablespace on the logical standby database
E. the number of applier processes
F. the size of the shared pool

Answer: A, B, C, E

Explanation:
The rate of SQL apply on a logical standby database can be influenced by:
A: The number of PREPARER processes (which seems to be a typographical error and should read as PREPARER or similar) which prepare the redo data for the applier processes.
B: The number of coordinator processes on the standby database instance which coordinate the SQL apply activities.
C: The number of full table scans performed by SQL apply since full table scans can be resource-intensive and slow down the apply rate.
E: The number of applier processes which apply the redo data to the logical standby database.
Option D is incorrect as the size of the undo tablespace on the logical standby database is more likely to affect the SQL apply lag rather than the rate of SQL apply.
Option F is incorrect because the size of the shared pool would typically not influence the rate of SQL apply. The shared pool is more related to the caching of shared SQL and PL/SQL code and control structures.

Question: 71

Which three are true about using Flashback database through role transitions in a Data Guard environment?

A. Physical standby databases retain their current role when you flash back to a point in time before a reinstate occurred which caused this database to become a physical standby.
B. Logical standby databases retain their current role when you flash back through to a point in time before the switchover occurred which caused this database to become a logical standby.
C. Logical standby database roles are reverted to their original role when you flash back to a point in time before the switchover occurred which caused this database to become a logical standby.
D. Physical standby databases retain their current role when you flash back to a point in time before the switchover occurred which caused this database to become a physical standby.
E. Flashback database may not be used to undo a physical standby database activation.

Answer: A, D, E

Explanation:

Question: 72

Which two Data Guard features require the use of flashback database by the broker?

A. Far Sync Instances
B. Snapshot Standby databases
C. Read-Mostly physical standby implementations
D. Fast-Start Failover
E. Real Time Query

Answer: B, D

Explanation:

Question: 73

Which two are prerequisites for configuring Transaction Guard in a Data Guard environment?

A. Grant execute permission on the DBMS_APP_CONT package to relevant database schema owners.
B. Ensure that connection descriptors for database clients use the failover clause with the COMMIT_OUTCOME parameter set to TRUE.

C. Set INSTANCE_NAME identically on all the Data Guard Configuration databases and modify the local service name on the client to include a CONNECTION_LIST containing all the standby hosts.
D. Create a database service with COMMIT_OUTCOME set to TRUE, and ensure clients use that service to connect to the database instance.
E. Create a database service with COMMIT_OUTCOME set to TRUE and ensure that the service is statically registered with the default listener on the primary host.

Answer: A, D

Explanation:

Question: 74

Examine the Data Guard configuration:
DGMGRL> show configuration;
Configuration - Animals
Protection Mode: MaxAvailability
Databases:
dogs - Primary database
sheep - Snapshot standby database
cats - Physical standby database
Fast-Start Failover: DISABLED
Configuration Status:
SUCCESS
You receive an error while attempting to raise the protection mode to Maximum Protection:
DGMGRL> edit configuration set protection mode as maxprotection;
Error: ORA-16627: operation disallowed since no standby databases would remain to support protection mode
Failed.
Which is the minimum statement, or sequence of statements you must execute to enable successful raising of the protection mode to Maximum Protection?

A. DGMGRL> edit database dogs set property LogxptMode=sync;
B. DGMGRL> edit database dogs set property LogXptMode=sync;
C. DGMGRL> edit database cats set property LogXptMode=sync;
D. DGMGRL> edit database dogs set property LogxptMode=sync;
E. DGMGRL> edit database dogs set property LogXptMode=sync;
F. DGMGRL> edit database sheep set property LogXptMode=sync;

Answer: B

Explanation:

Question: 75

Which three can be done using Data Guard Broker?

A. Create a new physical standby database.
B. Configuring the standby control file, server parameter file, and data files for a standby database.
C. Define logical standby database skip rules.
D. Converting physical standby databases to snapshot standby databases.
E. Monitoring and managing redo transport services, and log apply services.
F. Automating failover to a specified target standby database.

Answer: A, D, F

Explanation:

Question: 76

Attempting to start the observer raises an error:
DGMGRL> start observer;
DGM-16954: Unable to open and lock the Observer configuration file
Failed.
Identify two possible ways to start the observer successfully.

A. Enable Fast-Start Failover before starting the observer.
B. Start the observer in a different working directory.
C. Create a broker configuration and enable Fast-Start Failover before starting the observer.
D. Start the observer using a different observer configuration file.
E. Set the ObserverOverride property to TRUE before starting the observer.

Answer: B, D

Explanation:

Question: 77

Which two are true concerning the configuring of Flashback database in a Data Guard environment?

A. It permits a physical standby database to be converted to a snapshot standby database.
B. It is required in order for a snapshot standby database to be converted to a physical standby database.
C. It enables the use of far sync instances.
D. It permits a primary database that was disabled after failover to be reinstated as a standby.
E. It is a prerequisite for the use of Fast Start Failover.

Answer: A, D

Explanation:

Question: 78

Which TWO statements are true about database parameters for databases in a Data Guard environment?

A. If DB_RECOVERY_FILE_DEST is specified, then LOG_ARCHIVE_DEST_n is not required for local archive logs.
B. The databases that are part of a Data Guard configuration must have different DB_UNIQUE_NAME initialization parameters.
C. COMPATIBLE must have identical values for primary and standby databases.
D. LOG_FILE_NAME_CONVERT applies to online redo logs and archived logs.
E. DB_FILE_NAME_CONVERT is only required if the standby database is on the same host as the primary database.

Answer: B, C

Explanation:

Question: 79

Your current Data Guard environment consists of:
A primary database containing no abstract data types used for user tables.
Two separate remote physical standby databases used for reporting.
Examine these requirements for adding a new standby database to this Data Guard environment:
The new standby database must provide a disaster recovery solution.
There must be minimal additional performance overheads on the primary database.
The new standby database may require additional indexes and materialized views not present in the primary.
New tables or schemas may be required in the standby database that are not present in the primary.

What would you recommend to fulfill these requirements?

A. A physical standby database with synchronous redo transport and Real-Time Query enabled.
B. A physical standby database with asynchronous redo transport and Real-Time Query enabled.
C. A logical standby database with synchronous redo transport and redo apply on.
D. A logical standby database with synchronous redo transport and SQL apply on.
E. A logical standby database with asynchronous redo transport and SQL apply on.

Answer: E

Explanation:

Question: 80

Which TWO statements are true regarding Data Guard Broker?

A. It can be used to create and manage standby databases.
B. It can be used to perform failovers and switchovers.
C. It automatically starts the DMON process for the database instances that are part of a Data Guard configuration.
D. It can be used to monitor redo transport and log apply services.
E. It automatically adds the primary database to an existing broker configuration when Enterprise Manager Cloud Control is used to create a standby.

Answer: A, B

Explanation:

Question: 81

Which three are true regarding prerequisites for a logical standby database as a disaster recovery solution?

A. Ensure that supplemental logging is enabled on the primary database.
B. Ensure that no ROWID data types are contained in the primary database.
C. Ensure that no BFILE LOB data types are contained in the primary database.
D. Do not perform any nologging operations on the primary.
E. Ensure that flashback is enabled on the primary database.

Answer: A, C, D

Explanation:

Question: 82

Which two factors can cause an increase in redo transport lag?

A. The size of the online redo log files on the standby database.
B. The size of the standby redo log files on the primary database.
C. Increase in network latency between the primary database and a redo transport destination.
D. The size of the online redo log files on the primary database.
E. Increase in redo generation rate on the primary database.

Answer: C, E

Explanation:

Question: 83

Which two are true about the use of RMAN recovery catalogs when offloading backups to a physical standby database?

A. The physical standby database may be used to register the database in the recovery catalog, if the primary is not registered.
B. It backups that are offloaded to a physical standby database are taken when not connected to a recovery catalog, then they may still be used for restoration on the primary database.
C. The primary and physical standby databases must be registered separately in the recovery catalog, if a far sync instance is used to route redo to the physical standby database.
D. Primary and physical standby databases may use different virtual recovery catalogs in the same physical recovery catalog.
E. It is not necessary to use a recovery catalog unless a far sync instance is used to route redo to the physical standby database.

Answer: B, D

Explanation:

Question: 84

A Data Guard environment has this configuration and these attributes:
The primary database prima is in the local region.
A physical standby database physt1 is in the local region.

A physical standby database physt2 is in a remote region.
The primary ships redo to physt1.
physt1 ships redo to physt2.
physt1 and physt2 have Real-Time Query enabled.
A sequence has been created with this SQL statement in the primary database:
CREATE SEQUENCE a NOCACHE SESSION;
Which TWO statements are TRUE?

A. The sequence is usable on physt1 and physt2.
B. The sequence is usable on physt2 if physt1 becomes unavailable, but only if an alternate redo destination has been configured on the primary database.
C. physt2 will no longer receive redo if physt1 becomes unavailable, unless LOG_ARCHIVE_DEST_n has the ALTERNATE attribute specified on the primary database.
D. physt2 will no longer receive redo if physt1 becomes unavailable, unless LOG_ARCHIVE_DEST_n has the ALTERNATE attribute specified on physt1.
E. The sequence is usable on physt1 but not usable on physt2.

Answer: A, C

Explanation:

Question: 85

Which feature is available when monitoring a Data Guard configuration using Enterprise Manager Cloud Control, but is not available using DGMGRL or by using SQL?

A. Analyzing the dmon process trace file
B. Creating a broker configuration before creating the databases
C. Viewing a logical standby database apply lag
D. Automatic creation of standby redo logs
E. Performing a verify operation

Answer: C

Explanation:

Question: 86

You have a Data Guard broker configuration consisting of:
A primary database
One local physical standby database
One far sync instance

A remote physical standby database
The broker configuration was created with the DGMGRL utility after creating all the databases and the far sync instance with command-line tools.
What is the correct way to add this configuration to Enterprise Manager Cloud Control assuming all the nodes have been discovered already as Enterprise Manager targets?

A. Discover the primary as a target by refreshing the node on which it runs, and the other databases and instances in the Data Guard broker configuration will be discovered as targets automatically and be ready to be monitored.
B. Delete the Data Guard Broker configuration using DGMGRL and then re-create it using Enterprise Manager Cloud Control to enable all the databases in the configuration to be discovered as targets and to be ready to be monitored.
C. Discover the primary database as a target in Enterprise Manager Cloud Control. Then discover the existing Data Guard Broker configuration for the primary and all the other databases in the configuration will be discovered as targets and be ready to be monitored.
D. Use the DGMGRL utility to register the configuration with the Enterprise Manager Cloud Control agent on the primary database node. This will enable the discovery of all the other databases in the configuration as targets which will be ready to be monitored.
E. Discover either of the physical standby databases as a target by refreshing the node on which they run, and the other databases and instances in the Data Guard Broker configuration will be discovered as targets automatically and be ready to be monitored.

Answer: C

Explanation:

Question: 87

Which TWO statements are true about Far Sync instances?

A. They do not work with Logical Standby databases.
B. They work in Maximum Availability mode.
C. They do not work with Snapshot Standby databases.
D. They work in Maximum Performance mode.
E. They work in Maximum Protection mode.

Answer: A, D

Explanation:

Question: 88

You are monitoring your Data Guard broker configuration and issue this set of DGMGRL commands:

```
DGMGRL> SHOW CONFIGURATION;
Configuration - DRSolution
Protection Mode: MaxPerformance
Databases:
Close_by - Primary database
FS_inst - Far Sync
Far_away - Physical standby database
Fast-Start Failover: DISABLED
Configuration Status:
SUCCESS
```

What is true concerning this configuration?

A. The Close_by primary database instance forwards redo to the FS_inst Far Sync instance, which forwards the redo in turn to the Far_away physical standby database instance.
B. The FS_inst Far Sync instance forwards redo to the Far_away physical standby only if the Close_by primary database is not able to do so.
C. The Far Sync instance will not forward redo to the Far_away physical standby because Fast-Start Failover is disabled.
D. The Close_by primary database forwards redo to the Far_away physical standby directly and also sends redo to the FS_inst Far Sync instance.
E. The Far Sync instance will not forward redo to the Far_away physical standby because the Protection mode is not MaxProtection.

Answer: A

Explanation:

Question: 89

You have a Data Guard Broker configuration called 'Somewhere' as shown:

```
DGMGRL> SHOW CONFIGURATION;
Configuration - Somewhere
Protection Mode: MaxPerformance
Databases:
Nearby - Primary database
FS - Far Sync
Farout - Physical standby database
Fast-Start Failover: DISABLED
Configuration Status:
SUCCESS
```

You then run this command:

```
DGMGRL> SHOW DATABASE 'Nearby' 'InconsistentProperties';
```

Which two are true about the output of this DGMGRL command?

A. A far sync instance cannot have inconsistent properties because it has no database.
B. It shows all properties whose broker configuration values for database Nearby are inconsistent with the broker configuration values for database Farout.
C. Any inconsistency reported is on an instance-specific basis.
D. It shows all properties whose broker configuration values for database Nearby are inconsistent with the values in the corresponding server parameter file or the runtime values for database instance Nearby.

Answer: A, D

Explanation:

Question: 90

A Data Guard environment has this configuration and these attributes:
A primary database
A physical standby database named sbdb
The configuration is in maximum availability protection mode.
Then sbdb is converted to a snapshot standby database.
Which two statements are true?

A. The recovery time objective increases.
B. sbdb can still receive redo.
C. The protection mode is lowered to maximum performance.
D. sbdb can still apply redo.
E. The recovery point objective increases.

Answer: B, E

Explanation:

Question: 91

Examine the Data Guard configuration:
DGMGRL> show configuration;
Configuration - Animals
Protection Mode: MaxAvailability
Databases:
dogs - Primary database
cats - Snapshot standby database
sheep - Snapshot standby database

```
Fast-Start Failover: DISABLED
Configuration Status:
ORA-01034: ORACLE not available
ORA-16625: cannot reach database "dogs"
DGM-17017: unable to determine configuration status
```

ou wish to perform a failover to sheep. Which command, or sequence of commands, should you issue to the broker before executing failover to sheep; using the broker?

A. DGMGRL> convert database sheep to physical standby;
B. DGMGRL> convert database cats to physical standby;
C. DGMGRL> convert database sheep to physical standby;
D. DGMGRL> convert database cats to physical standby;
E. None, because you can directly failover to a Snapshot Standby Database.

Answer: A

Explanation:

Question: 92

You must propose an Oracle Data Guard configuration for a database supporting an OLTP workload that meets these permanent requirements:
Data loss is not permitted.
Read-only applications should not connect to the primary database instance.
Additionally, there are these requirements, only one of which is ever done at any one time:
It should be possible to apply and test designated patches with a minimum amount of downtime.
Upgrading to a new database release should be performed with the least possible amount of downtime.
New application software releases should be tested against an exact up-to-date replica of the production database.
You propose a primary database with one physical standby database configured in Maximum Protection mode.
Which requirements do you meet?

A. 1 and 2
B. 1, 2, 3, 4, and 5
C. Only requirement 5
D. Only requirement 1
E. 2, 3, 4, and 5

Answer: D

Explanation:

Question: 93

Which TWO statements are true for Data Guard environments with multi-tenant databases?

A. A multi-tenant standby database can have fewer pluggable databases than the primary container database.
B. Different pluggable databases within a logical standby database may have different guard statuses.
C. The Data Guard broker automatically opens all pluggable databases of a primary database after a role change operation.
D. The Data Guard broker automatically always opens the pluggable databases of a standby database after a role change operation.
E. The CDBDBA privilege must be used instead of the SYSDBA privilege for connections as SYS to the root container of a multi-tenant standby database.

Answer: A, B

Explanation:

Question: 94

Which three statements are true about snapshot standby databases?

A. A resize command to reduce the size of an empty datafile in the snapshot standby database, which was created in the primary database, will succeed.
B. A resize command to reduce the size of an empty datafile in the snapshot standby database, which was created in the snapshot standby database, will succeed.
C. A resize command to extend the size of a datafile in the snapshot standby database, which was created in the snapshot standby database, will succeed.
D. A resize command to reduce the size of an empty datafile in the snapshot standby database, which was created in the physical standby database, will succeed.
E. A resize command to extend the size of a datafile in the snapshot standby database, which was created in the primary database, will succeed.

Answer: B, C, E

Explanation:

Question: 95

Which THREE statements are true about snapshot standby databases?

A. A snapshot standby database must be opened at least once in read-write mode before it can be converted into a physical standby database.
B. A snapshot standby database can be the only standby database in a Maximum Protection Oracle Data Guard configuration.
C. Snapshot standby databases may be used for rolling database upgrades.
D. If datafiles grow while a database is a snapshot standby database, then they shrink when converted back to a physical standby database.
E. A guaranteed restore point is created automatically when a physical standby database is converted into a snapshot standby database.

Answer: A, C, E

Explanation:

Question: 96

Which three are prerequisites for enabling Fast-Start Failover?

A. A static service name must be configured only for the Fast-Start Failover target standby database.
B. The Fast-Start Failover target standby database may receive REDO either synchronously or asynchronously when the configuration operates in Maximum Performance mode.
C. Flashback Database must be enabled on the primary database.
D. The Fast-Start Failover target standby database must receive REDO synchronously when the configuration operates in Maximum Availability mode.
E. Flashback Database must be enabled on the Fast-Start Failover target standby database.

Answer: C, D, E

Explanation:

Question: 97

Which three statements are true about Data Guard database modes and states?

A. Force Logging Mode is not required for a primary database but is recommended.
B. The Primary Database can operate in noarchivelog mode.
C. A Logical Standby Database can be in MOUNT state while applying changes.
D. Databases in a Data Guard Configuration need not operate in Flashback Logging mode.

E. A primary database may ship redo directly to more than nine standby databases.

Answer: A, C, D

Explanation:

Question: 98

Which three statements are true about redo transport?

A. With synchronous redo transport, LGWR ships redo directly to RFS processes on the standby database instances and waits for an acknowledgment.
B. An RFS process on a standby database instance may receive redo from an archiver process on the primary database instance to perform archive gap resolution.
C. With asynchronous redo transport, TTnn processes may read redo from the log buffer or from standby redo logs on the primary database.
D. Multiple RFS processes may receive redo on one standby database instance.
E. Multiple RFS processes may receive redo on one far sync instance.

Answer: A, B, D

Explanation:

Question: 99

Which three are true about using RMAN in a Data Guard environment?

A. Backups of archived redo logs taken on a physical standby are interchangeable with a primary.
B. Backups of control files taken on a physical standby are not interchangeable with a primary.
C. A recovery catalog is required when RMAN is used to take backups from a physical standby database if you plan to recover the primary using those backups.
D. Backups of data files taken on a physical standby are interchangeable with a primary.
E. A recovery catalog is required when RMAN is used to take backups from a logical standby database in a Data Guard configuration if you plan to recover the primary using those backups.

Answer: A, B, D

Explanation:

Question: 100

A customer asks you to propose the most appropriate solution for this set of requirements:
We need a disaster recovery solution that enables us to fail over from our production database with zero data loss.
We want to generate reports from the proposed standby database at the same time that it is used for data protection.
Developers may need to test occasionally on a copy of the live database
Which TWO solutions would you recommend?

A. A snapshot standby database with synchronous redo transport
B. A physical standby database with real-time query enabled
C. A logical standby database with real-time query enabled
D. A physical standby database with real-time apply enabled
E. A logical standby database with real-time apply enabled

Answer: B, C

Explanation:

Question: 101

Your Data Guard environment has two remote physical standby databases.
Client applications use the local naming method to define connectivity to the primary database instance.
Which will automatically redirect clients to the new primary database in case of a switchover or failover?

A. Configure a PRIMARY role service on the Primary and Standby and modify the Client connect descriptor to include both the Primary and the Standby.
B. Set the LOCAL_LISTENER parameter for all the database instances, to register services with the default listener on the primary database host.
C. Set the DB_NAME parameter identically on all databases; modify the connection descriptor on the clients to use DB_NAME to connect to the primary database instance.
D. Create a database service on the standby databases; automate the start of the service after a role change, and modify the connection descriptor on the clients to use that service.

Answer: D

Explanation:

Question: 102

Which two steps must be performed before running DUPLICATE TARGET DATABASE FOR STANDBY using RMAN?

A. Transfer a copy of the password file from the primary host to the standby host.
B. Run the nid utility to modify the DBID of the primary database.
C. Create an SPFILE for the standby database.
D. Create a standby control file.
E. Configure Oracle Net connectivity between the primary host and the standby host.

Answer: A, E

Explanation:

Question: 103

Examine the Data Guard configuration after an accidental switchover to Sheep:

```
DGMGRL> show configuration;
Configuration - Animals
Protection Mode: MaxAvailability
Databases:
sheep - Primary database
dogs - Logical standby database
cats - Physical standby database (disabled)
ORA-16795: the standby database needs to be re-created
Fast-Start Failover: DISABLED
Configuration Status:
SUCCESS
```

Which three statements will be true after a switchover to Dogs?

A. Sheep will be a disabled logical standby database.
B. Cats will be a disabled physical standby database that can be manually enabled.
C. Sheep will be an enabled logical standby database.
D. Dogs will be the primary database.
E. Cats will be an enabled physical standby database.

Answer: B, C, D

Explanation:

Question: 104

Your expertise is requested for these customer requirements:
The Data Guard environment must be in maximum protection mode.
Reports must be offloaded to a physical standby database.
There must be no lag between the primary and standby databases that affect the reports produced.
The primary database must be resilient in case of a single network failure.
Which solution is correct for these requirements?

A. Two standby databases, at least one of them a physical standby with Real-Time Query enabled and the STANDBY_MAX_DATA_DELAY parameter set to zero, receiving redo from the primary with synchronous transport
B. Two standby databases, at least one of them a physical standby with Real-Time Query enabled and the STANDBY_MAX_DATA_DELAY parameter set to zero, receiving redo from the primary with asynchronous transport
C. One physical standby database with Real-Time Query enabled, receiving redo from two Far Sync instances that are connected to the primary
D. One physical standby database with Real-Time Query enabled and STANDBY_MAX_DATA_DELAY parameter set to zero, receiving redo from the primary with synchronous transport
E. Two physical standby databases with Real-Time Query enabled, receiving redo from the primary with the LOG_ARCHIVE_DEST_n attributes SYNC NOAFFIRM to minimize the performance impact on the primary

Answer: A

Explanation:

Question: 105

Which statement is true regarding Oracle Net connectivity for a Data Guard Broker configuration?

A. To enable Real-Time Query on a physical standby database, a TNS entry enabling connectivity to the standby database instance must be defined on the primary database host.
B. To start SQL Apply on a logical standby database, a TNS entry enabling connectivity to the primary database instance must be defined on the logical standby database host.
C. A TNS entry enabling connectivity to the primary database instance must be defined on each of the standby database hosts.
D. A TNS entry or entries enabling connectivity to standby database instance(s) must be defined on the primary database host.
E. The LOCAL_LISTENER initialization parameter must be set to the listener used to register the primary database instance.

Answer: D

Question: 106

Your Data Guard environment consists of these components and settings:
A primary database supporting an OLTP workload
A remote physical standby database
Real-time query is enabled
The redo transport mode is set to SYNC
The protection mode is set to Maximum Availability
Which two statements are true regarding the DelayMins database property for the standby database?

A. It can only be enabled for a configuration in Maximum Availability mode.
B. It allows user errors on the primary to be recovered by using the physical standby database.
C. It can only be enabled for a configuration in Maximum Performance mode.
D. It specifies a delay before the primary ships redo to the standby destination having DelayMins set.
E. It allows logical corruptions on the primary to be recovered by using the physical standby database.
F. It enables you to bypass the default network timeout interval specified for the standby redo transport destination.

Answer: B, E

Question: 107

Examine the procedure that you plan to execute on your logical standby:
SQL> EXECUTE DBMS_LOGSTDBY.SKIP(stmt => 'DML', schema_name => 'HR', object_name => 'EMPLOYEE');
What is a prerequisite for execution of this procedure?

A. Change the redo transport mode if necessary to ASYNC.
B. Stop SQL Apply on the logical standby database.
C. Execute the DBMS_LOGSTDBY.APPLY_SET procedure to record errors that might cause SQL Apply to stop.
D. Stop redo transport to the logical standby database.

Answer: B