Oracle Data guard (high availability feature)

Oracle Data Guard is a high availability (HA) feature of Oracle that ensures data protection and disaster recovery by maintaining standby databases as exact copies of the primary database. If the primary database becomes unavailable, Data Guard can quickly switch operations to a standby database, minimizing downtime.

Part-1

Data Guard consists of a primary database and one or more standby databases. It uses redo log shipping to synchronize the standby databases with the primary. The main components are:

- **Primary Database**: The production database that handles transactions.
- **Standby Database(s)**: A duplicate database that receives redo data from the primary.
- **Redo Transport Services**: Handles the transfer of redo logs from the primary to standby databases.
- **Apply Services**: Applies redo logs to the standby database to keep it synchronized with the primary.

Types of Standby Databases

- **Physical Standby**: An exact copy of the primary, synchronized through redo logs.
- **Logical Standby**: Similar to the primary but can have different physical structures (e.g., different indexes or tables), using SQL apply instead of redo apply.
- **Snapshot Standby**: A read/write version of a physical standby used for testing or reporting, which can be converted back to a standby state.

Data Guard operates in three different protection modes to manage availability, performance, and data protection based on business requirements:

1. **Maximum Protection Mode**
    - Guarantees zero data loss.
    - Requires at least one standby database to acknowledge redo receipt before committing on the primary.
    - If the standby is unavailable, the primary will shut down.
2. **Maximum Availability Mode**
    - Balances zero data loss with primary database availability.
    - Primary waits for standby acknowledgment unless a network delay occurs, allowing it to continue if standby fails temporarily.
    - Provides high availability with minimal data loss risk.

3. **Maximum Performance Mode (default)**
    - Aims to maximize primary database performance.
    - Primary database does not wait for standby acknowledgment, leading to possible data loss if the primary fails before redo transmission.
    - This is the most common setup for less critical systems.

Configuring Oracle Data Guard

Prerequisites:

- Oracle software installed on both primary and standby servers.
- Both primary and standby databases in ARCHIVELOG mode.
- Enable FORCE LOGGING on primary to ensure all changes are logged.

Configuration Steps:

1. **Set Initialization Parameters**:
    - Configure primary and standby servers with db_unique_name, log_archive_config, log_archive_dest_n, and remote_login_passwordfile parameters.
    - Enable FORCE LOGGING and ARCHIVELOG mode on the primary database.

Create a Standby Database:

- Use RMAN to duplicate the primary database to create a physical standby:

RMAN> DUPLICATE TARGET DATABASE FOR STANDBY FROM ACTIVE DATABASE DORECOVER;

Alternatively, use a backup-based method with RMAN.

Configure Redo Transport Services:

- Set up log_archive_dest_n parameter on the primary to define redo transport.

ALTER SYSTEM SET log_archive_dest_2='SERVICE=standby_db LGWR SYNC AFFIRM';

Start Redo Apply:

- On the standby, start applying redo logs using:

ALTER DATABASE RECOVER MANAGED STANDBY DATABASE DISCONNECT FROM SESSION;

Switch to Real-Time Apply (optional):

- This allows standby to apply redo data as soon as it is received.

ALTER DATABASE RECOVER MANAGED STANDBY DATABASE USING CURRENT LOGFILE;

1. **Verify Data Guard Configuration**:

- Use SHOW CONFIGURATION in Data Guard Broker or SQL queries to verify the sync between primary and standby databases.

Mode Configuration:

- **Set Protection Mode**:

ALTER DATABASE SET STANDBY DATABASE TO MAXIMUM AVAILABILITY;

Monitoring and Managing Data Guard

- **Data Guard Broker**: Oracle provides Data Guard Broker, a management tool to simplify and automate Data Guard tasks.
- **Switchovers and Failovers**: Use ALTER DATABASE SWITCHOVER and ALTER DATABASE FAILOVER commands to transition roles between primary and standby.

Role Transition (Switchover and Failover)

- **Switchover**: Planned role reversal with no data loss, useful for maintenance.
- **Failover**: Emergency transition when the primary is unavailable.

Key Considerations:

- **Network Bandwidth**: Redo transport can consume bandwidth, especially in SYNC mode.
- **Latency**: Higher latency networks may benefit from Maximum Performance mode to reduce delays.
- **Testing**: Test failover and switchover regularly to ensure availability in case of primary failure.

Oracle Data Guard is highly flexible, allowing customization of HA settings to align with specific business needs.

Part-2

Fast-Start Failover (FSFO) is an Oracle Data Guard feature that automates the failover process, ensuring near-instantaneous switchover to a standby database if the primary database becomes unavailable. Here are the primary benefits of using FSFO:

Automatic and Fast Failover

- FSFO allows for automatic, quick failover to a standby database without manual intervention, minimizing downtime and eliminating the need for DBA presence during an unexpected failure.
- This automated failover process is monitored and executed by the Data Guard Broker, which assesses database health and triggers failover within seconds if needed.

Minimized Data Loss

- When configured with **Maximum Availability** or **Maximum Protection** modes, FSFO provides nearly zero data loss in a failover scenario by ensuring that redo logs are sent and applied to the standby database.
- For applications requiring high data protection, FSFO can prevent data loss by waiting for acknowledgment from the standby database before committing changes on the primary.

Enhanced Disaster Recovery

- FSFO improves disaster recovery capabilities by reducing Recovery Time Objective (RTO), which is the time required to restore normal operations after a disaster.
- It simplifies the failover process during unforeseen issues, allowing critical applications to resume quickly.

Automatic Reinstatement of Failed Primary (optional)

- After a failover, FSFO can optionally reinstate the original primary as a standby automatically, helping maintain Data Guard configuration without additional manual steps.
- This feature reduces the need for manual intervention in re-establishing the failed primary as part of the Data Guard configuration, enhancing overall system resilience.

Reduced DBA Intervention and Simplified Management

- With FSFO, DBAs are not required to manually initiate failover, which can be crucial in scenarios with strict uptime requirements.
- FSFO works with the **Data Guard Broker**, which provides an intuitive interface for configuring, managing, and monitoring the Data Guard setup, further simplifying administrative tasks.

Improved High Availability for Mission-Critical Applications

- FSFO is beneficial for mission-critical applications where downtime is costly. By significantly reducing failover times, it keeps business operations running smoothly with minimal interruptions.
- Combined with Oracle Data Guard's high-availability features, FSFO enhances the reliability of applications that need continuous access to data, such as financial services, e-commerce, or healthcare applications.

Configurable Conditions for Failover

- FSFO allows DBAs to set conditions under which failover will occur, giving fine-grained control over failover criteria (e.g., network issues, storage failures).
- This allows organizations to tailor FSFO behaviour based on business priorities and the specific requirements of their database environment.

In a typical FSFO setup, if the Data Guard Broker detects a failure on the primary database (e.g., due to hardware issues or network partition), it will initiate failover to the designated standby database automatically. This automated response ensures the standby becomes the primary without significant delay, allowing applications to continue with minimal impact.

Key Requirements for FSFO

1. **Observer Process**: An observer process runs on a separate, reliable server and continuously monitors both the primary and standby databases. It initiates failover if it detects a primary failure and the primary database cannot communicate with the standby.
2. **Synchronous Redo Transport**: To prevent data loss, FSFO usually requires synchronous redo transport in Maximum Availability or Maximum Protection mode.
3. **Data Guard Broker Configuration**: FSFO requires the Data Guard Broker, which acts as the central management and monitoring component.

In Summary

FSFO is an essential feature for enterprises that need automated failover with minimal downtime and data loss. It allows systems to maintain high availability with automatic responses to primary failures, ensuring applications continue to operate even in the face of critical failures.

Part-3

To deploy the **Observer process** for Fast-Start Failover (FSFO) in a location separate from both the primary and standby servers, you need to ensure that the observer setup meets certain requirements to function effectively. Here's what you'll need to consider:

1. Network Connectivity

- The Observer must have reliable, continuous network connectivity to both the primary and standby databases.
- This connectivity is essential because the Observer constantly monitors both databases to ensure that it can detect a primary failure and initiate a failover if needed.

2. Oracle Database Client Installation

- The server hosting the Observer process must have the **Oracle Database Client** installed. This client installation should be at the same or a compatible version as the primary and standby databases.
- The client provides the necessary tools and libraries for the Observer to communicate with the databases and manage the Data Guard configuration.

3. Data Guard Broker Configuration

- FSFO requires that Data Guard Broker be configured for both the primary and standby databases. The Observer uses the Broker to monitor and control failover processes.
- Make sure that the Data Guard Broker is enabled (dg_broker_start = TRUE) on both the primary and standby databases.

4. Observer TNS Configuration

- The Observer machine must have a **TNSNAMES.ORA** file configured with entries for both the primary and standby databases. These entries allow the Observer to connect to both databases using their respective service names.
- Example tnsnames.ora entries:

```
PRIMARY_DB =
 (DESCRIPTION =
  (ADDRESS = (PROTOCOL = TCP)(HOST = primary_host)(PORT = 1521))
  (CONNECT_DATA =
   (SERVER = DEDICATED)
   (SERVICE_NAME = primary_service)
  )
 )

STANDBY_DB =
 (DESCRIPTION =
  (ADDRESS = (PROTOCOL = TCP)(HOST = standby_host)(PORT = 1521))
  (CONNECT_DATA =
   (SERVER = DEDICATED)
   (SERVICE_NAME = standby_service)
  )
 )
```

5. Observer Process Setup and Management

- To start the Observer, you can use the dgmgrl utility from the Oracle Database Client. For example:

```
dgmgrl sys/password@PRIMARY_DB
```

DGMGRL> START OBSERVER;

- You may also configure the Observer to start automatically upon system startup using a script, especially in environments where high availability is critical.

6. Separate Server or Data Center

- Ideally, the Observer should be located in a separate physical location or data center from both the primary and standby databases. This ensures that if there's a site failure affecting both primary and standby, the Observer remains unaffected and can initiate failover.
- Ensure the server running the Observer is on a stable network with high availability.

7. Monitoring and Security

- It's important to regularly monitor the Observer's status. Use SHOW OBSERVER in dgmgrl to verify that the Observer is active.
- Ensure that secure network connections (SSL/TLS) are configured if the Observer needs to connect over public or less secure networks, especially when it resides outside the primary/standby network.

8. Observer Configuration Parameters

- In some cases, additional Data Guard Broker parameters may be tuned to optimize FSFO and Observer behavior, such as setting FastStartFailoverThreshold to control the delay before failover is triggered.

Following these requirements ensures the Observer operates reliably in an independent location, enhancing the resilience of your FSFO configuration by adding a robust, remote monitoring component.

Prepared By:

Zaheer Abbas Mitaigiri **(OCA, OCP, OCE, OCS).**

Oracle Database Specialist.