



Servicio Andaluz de Salud
CONSEJERÍA DE SALUD

*Oficina Técnica para la Gestión y Supervisión de
Servicios TIC
Subdirección de Tecnologías de la Información*

BEST PRACTICES DE SISTEMAS EN ENTORNOS ORACLE DATA GUARD

*Referencia documento: InfV5_JASAS_DG_BestPractices_V920.doc
Fecha: 16 de noviembre de 2018
Versión: 9.2.0*

Registro de Cambios

Fecha	Autor	Versión	Notas
13 de enero de 2011	Oracle ACS	2.1	Versión inicial
12 de January de 2012	Oracle ACS	2.2	Versión revisada abril 2011
14 de Julio de 2011	Oracle ACS	2.3	Version revisada Julio 2011
13 de octubre de 2011	Oracle ACS	2.4	Version revisada octubre 2011
12 de enero de 2012	Oracle ACS	3.1	Versión de enero de 2012
14 de marzo de 2013	Paola Juárez	4.1	Revisión de marzo de 2013, contrato 2012-2014
17 de octubre de 2013	Paola Juárez	4.3	Revisión de octubre de 2013, contrato 2012-2014
16 de Julio del 2015	Paola Juárez	6.1	Revisión de Julio de 2015, contrato 2014-2016
16 de diciembre del 2015	Paola Juárez	6.2	Revisión de diciembre de 2015, contrato 2014-2016
16 de junio del 2016	Paola Juárez	7.1	Revisión de junio de 2016, contrato 2014-2016
16 de junio del 2017	Paola Juárez	8.1	Revisión de junio de 2017, contrato 2016-2018
16 de noviembre del 2017	Paola Juárez	8.2	Revisión de noviembre de 2017, actualización a versión 12cR2, contrato 2016-2018.
16 de junio del 2018	Paola Juárez	9.1	Revisión de junio de 2018, contrato 2016-2018.
16 de noviembre del 2018	Paola Juárez	9.2	Revisión de noviembre de 2018, contrato 2016-2018.

Revisiones

Nombre	Role
Gregorio Adame	Oracle Advanced Services Engineer
Jonathan Ortiz	Oracle Advanced Services Engineer
José María Gómez	Oracle Technical Account Manager

Distribución

Copia	Nombre	Empresa
1	Subdirección de Tecnologías de la Información	Servicio Andaluz de Salud, Junta de Andalucía
2	Servicio de Coordinación de Informática de la Consejería de Hacienda y Administración Pública	Consejería de Hacienda y Administración Pública, Junta de Andalucía

Índice de Contenidos

CONTROL DE CAMBIOS	4
INTRODUCCIÓN	5
OBJETIVOS DE ESTE DOCUMENTO	6
RECOMENDACIONES DE ADMINISTRACIÓN Y CONFIGURACIÓN	7
<i>Recomendaciones genéricas de la configuración</i>	7
<i>Herramientas de Administración</i>	8
<i>Arranque y paradas de instancias</i>	10
<i>Consideraciones del fichero de parámetros</i>	11
RECOMENDACIONES DE ALMACENAMIENTO	13
<i>Recomendaciones generales</i>	13
<i>Oracle Flexible Architecture</i>	13
<i>Ficheros de base de datos</i>	14
<i>Arquitectura de directorios</i>	15
RECOMENDACIONES EN LOS SERVICIOS DE TRANSPORTE	16
<i>Recomendaciones generales de configuración de red</i>	16
<i>Recomendaciones generales de configuración de métodos de transporte</i>	16
<i>Recomendaciones de configuración para LGWR SYNC Redo Transport</i>	17
<i>Recomendaciones de configuración para Standby</i>	17
<i>Eventos de espera relacionados con los servicios de transporte</i>	18
RECOMENDACIONES EN LOS SERVICIOS DE REDO APPLY	20
<i>Recomendaciones generales de configuración</i>	20
RECOMENDACIONES EN LOS SERVICIOS DE SQL APPLY	22
<i>Recomendaciones generales de configuración</i>	22
RECOMENDACIONES DURANTE CAMBIOS DE ROL	23
<i>Recomendaciones generales de configuración para Switchover</i>	23
<i>Recomendaciones generales de configuración para Failover</i>	26
<i>Recomendaciones generales de configuración de los clientes</i>	29
RECOMENDACIONES DE BACKUP & RECOVERY	30
<i>Arquitectura de backup</i>	30
<i>Estrategia de backup</i>	31
<i>Configuración de base de datos</i>	31
<i>Configuración recomendada para RMAN</i>	32
<i>Mantenimiento de Archive Logs</i>	34
<i>Restauraciones en entorno Data Guard</i>	35
RECOMENDACIONES DE UPGRADE Y APLICACIÓN DE PATCHES	36
<i>Nuevas instalaciones</i>	36
<i>Consideraciones de Upgrade e Instalación de Parches</i>	36
<i>Rolling Upgrade</i>	38
<i>Standby First Apply</i>	39

Control de cambios

Cambio	Descripción	Página
	No se realizan cambios en esta versión del documento.	N/A

Introducción

Este documento recoge una serie de recomendaciones de Oracle Soporte planteadas como buenas prácticas de sistemas para administradores que hagan uso de *Oracle RDBMS 12cR2* y *Oracle RDBMS 12cR2 Data Guard (DG)*.

Estas recomendaciones están encaminadas a minimizar los posibles problemas de configuración y rendimiento en sistemas de cualquier tamaño y en la gran mayoría de los casos se basan en la experiencia de casos reales gestionados por Oracle Soporte.

Objetivos de este documento

A lo largo de los puntos de este documento se irá definiendo una guía de buenas prácticas para la administración de bases de datos en Activo – Pasivo a través de *Oracle RDBMS Data Guard*. Esta guía contendrá tanto prácticas recomendadas como prácticas a evitar y se apoyará en ejemplos y en información que permita analizar las recomendaciones en cada uno de los entornos de desarrollo y preproducción.

Este documento está definido para la versión *Oracle RDBMS Data Guard 12cR2*.

Esta guía de buenas prácticas tiene varios objetivos:

- Aprovechamiento de las características del producto Oracle RDBMS Data Guard.
 - Alta disponibilidad
 - Aprovechamiento de recursos de sistemas en standby
- Facilitar la gestión y administración de las bases de datos en producción con sistemas basados en Oracle RDBMS Data Guard.

RECOMENDACIONES DE ADMINISTRACIÓN Y CONFIGURACIÓN

La aplicación de estas recomendaciones generales puede tener un mayor impacto en un entorno Data Guard, o responder a las cuestiones o problemas que ocurren con más frecuencia en Data Guard. En este caso, las recomendaciones genéricas hacen referencia a las cuestiones más frecuentes propias de las implementaciones de Data Guard en cualquier plataforma.

Recomendaciones genéricas de la configuración

Oracle Soporte propone las siguientes recomendaciones genéricas de configuración:

- Como primer paso para la implementación de un entorno en Data Guard se recomienda tener conocimientos previos de los distintos elementos que componen estos sistemas, así como una elección adecuada del tipo de configuración idónea para el entorno en cuestión. Por ello se recomienda consultar la documentación general del producto disponible OTN.
- Hacer uso de Automatic Storage Management (ASM) para el almacenamiento de archivo de datos. En la siguiente URL se hace referencia al enlace de ASM y técnicas de best practices
<https://docs.oracle.com/database/122/OSTMG/title.htm>
- Una vez acabada la implantación del entorno es necesario realizar un conjunto de pruebas que ayuden a planificar el modo de actuación ante pérdidas de servicio en la base de datos primaria. En este punto se engloban principalmente los cambios de rol entre ambas instancias.
- Es necesario desarrollar una estrategia proactiva de parches, para mantenerse a la vanguardia de los últimos problemas conocidos. Manténgase actualizado con las últimas actualizaciones siguiendo la nota *Release Update y Release Update Revisions for Database Proactive Patch Program* (2285040.1) y esté al tanto de los parches más recientes recomendados (como se documenta en la nota 756671.1). Este punto se detallará en el apartado de recomendaciones de aplicación de Parches en Data Guard.

Herramientas de Administración

Como norma no se especifica ninguna herramienta de administración obligatoria, pero si hace referencia a las herramientas proporcionadas por Oracle para la administración.

La siguiente sección introduce a la administración de Oracle Data Guard haciendo uso de las siguientes herramientas:

1. **Data Guard Broker 12c:** Es una herramienta administración que automatiza la creación, mantenimiento y monitorización de configuraciones en Data Guard. Se puede usar directamente a modo comando (DGMGRL) o bien mediante la interfaz de gráfica de Enterprise Manager (GUI).

Se pueden llevar a cabo las siguientes tareas:

- Habilitar configuraciones, incluida la configuración de los servicios de transporte y aplicación de redo.
- Mantenimiento de la configuración desde cualquier sistema integrante de la misma.
- Administración y monitorización de configuraciones que contengan Oracle RAC como base de datos primaria o standby.
- Simplificación de las operaciones de switchover y failover.
- Habilitar fast-start failover para realizar el failover a una instancia en standby cuando la primaria no se encuentra disponible.

Además, desde la interfaz gráfica se automatizan y simplifican las siguientes operaciones:

- Creación de una standby física o lógica partiendo de un backup de la base de datos primaria.
- Añadir nuevas o existentes bases de datos en standby a una configuración ya existente.
- Monitorización de la aplicación de redo, captura de información de diagnóstico y detección centralizada de problemas.
- Validación de la configuración de los entornos con el comando `VALIDATE DATABASE` y validación de la integridad de los datafiles y detección de corrupciones Lost-Write con el comando `VALIDATE DATABASE DATAFILE`

Documentación oficial:

Data Guard Broker

https://docs.oracle.com/cd/E82638_01/DGBKR/title.htm

Changes in Oracle Database 12c Release 1

https://docs.oracle.com/database/121/DGBKR/release_changes.htm#DGBKR3847

Changes in Oracle Database 12c Release 2

https://docs.oracle.com/database/122/DGBKR/release_changes.htm#DGBKR3847

- 1.1. **Oracle Enterprise Manager Grid Control (también referenciado como Enterprise Manager):** Proporciona una interfaz gráfica para la consulta, monitorización y administración de las instancias primaria y standbys pertenecientes a una configuración en Data Guard. Funciona en combinación con Data Guard Broker. Desde la consola de Grid Control se pueden realizar las operaciones de mantenimiento de forma local o remota. Se tiene acceso a las consolas de administración de las instancias pudiendo iniciar y parar instancias, monitorizar su rendimiento, ver eventos, programar trabajos y hacer operaciones de backup y recovery.
- 1.2. **The Data Guard command-line interface (DGMGRL):** Permite controlar y monitorizar una configuración en Data Guard desde la interfaz de comando o usando scripts. Con esta interfaz se pueden llevar a cabo la mayor parte de las actividades requeridas para la administración y monitorización de las bases de datos de la configuración.
2. **SQL*Plus:** Es la interfaz de comando para operar con las bases de datos Oracle. Es una herramienta muy potente y conocida por los administradores, por lo que no vamos a entrar en detalles de su uso. Por defecto SQL*Plus no identifica la instancia actual sobre la que estamos trabajando. Por lo que, si hacemos uso de ella, y para evitar confusiones, se recomienda la modificación del prompt a través del siguiente comando

```
SET SQLPROMPT '_CONNECT_IDENTIFIER>'
```

Con este comando conseguimos identificar sobre qué instancia estamos trabajando. Por último, hay que tener en cuenta que desde SQL*Plus se permiten ciertos comandos que afectan a la instancia en la que estamos conectado o a la configuración completa.

Arranque y paradas de instancias

El procedimiento de arranque de instancias en Oracle Data Guard tiene las siguientes puntualizaciones:

- La instancia primaria se inicia de forma habitual como cualquier instancia.
- Las instancias en standby física deben de ser montadas. Solamente serán abiertas en caso de que hagan uso de Active Dataguard (funcionalidad disponible a partir de 11gR2 que requiere licenciamiento) o si se utilizan en modo sólo lectura, periodo en el cual no estará activo la aplicación de los cambios provenientes de la primaria.
- Tras el arranque, en las instancias en standby física hay que iniciar los procesos de Redo Apply. (si se dispone de bróker el reinicio será automático)
- Las instancias en standby lógica se iniciarán de forma habitual como cualquier instancia.
- Tras el arranque, en las instancias en standby lógica hay que iniciar los procesos de SQL Apply. (si se dispone de bróker el reinicio será automático)

El procedimiento de parar instancias en Oracle Data Guard es idéntico al procedimiento tradicional.

Para parar una configuración de base de datos Oracle Data Guard completamente es necesario realizar el shutdown de todas las instancias.

En caso de parar alguna de las instancias en standby se recomienda poner en diferido el envío de información de redo desde la primaria para evitar la aparición de errores de conexión y los consiguientes reintentos para el envío de información.

Para un mayor detalle de los procesos de arranque y parada de las bases de datos integrantes de una configuración en Data Guard se recomienda atender a la documentación oficial del producto.

La parada y arranque de las instancias es un procedimiento conocido por los administradores de bases de datos y se puede realizar desde cualquier interfaz descrita en el apartado anterior.

Consideraciones del fichero de parámetros

Al crear la base de datos, Oracle crea un SPFILE en la ubicación del archivo que se especifique. Esta ubicación puede ser en:

- Un grupo de discos ASM
- Un file system
- Un raw devices

La recomendación es almacenar el SPFILE en ASM, si no se está usando ASM la recomendación es usar filesystem.

Si se crea manualmente la base de datos, Oracle recomienda que se cree un SPFILE a partir de un archivo de parámetros de inicialización (PFILE).

Cada instancia de base de datos que forme parte del Data Guard debe poseer su propio SPFILE.

En Oracle Data Guard se recomienda que se utilice SPFILE para simplificar la administración y mantener la coherencia de ajuste de parámetros.

Además, permite configurar RMAN para realizar copias de seguridad del SPFILE.

Para la modificación del fichero de parámetros SPFILE, se recoge como norma general el uso del comando:

```
SQL> alter system set
```

Uso de parámetros en Data Guard

Por defecto, la mayoría de los parámetros son configurados a sus valores por defecto y tendrán el mismo valor a lo largo de todas las instancias. Sin embargo, hay ciertos parámetros que deben ser configurados de forma distinta entre la base de datos primaria y standby. A continuación, se muestran unas tablas que recogen los parámetros a modificar en un entorno en Data Guard:

Parámetros específicos de base de datos en Data Guard
DB_NAME
DB_UNIQUE_NAME
COMPATIBLE
LOG_ARCHIVE_CONFIG
LOG_ARCHIVE_DEST_N
LOG_ARCHIVE_DEST_STATE_N
LOG_ARCHIVE_FORMAT
REMOTE_LOGIN_PASSWORDFILE

Parámetros específicos de base de datos en Data Guard
LOG_ARCHIVE_MAX_PROCESSES
FAL_SERVER
FAL_CLIENT * (No es necesario definir este parámetro en 12cR2)
STANDBY_FILE_MANAGEMENT
DB_FILE_NAME_CONVERT
LOG_FILE_NAME_CONVERT
Parámetros que DEBEN ser idénticos para todas las instancias
DB_NAME
LOG_ARCHIVE_CONFIG
COMPATIBLE
Parámetros para la configuración del BROKER
DATAGUARD_BROKER
DG_BROKER_START
DG_BROKER_CONFIG_FILE1
DG_BROKER_CONFIG_FILE2

Con respecto a estos parámetros se harán las siguientes recomendaciones:

- Como buena práctica el formato de los archivos en destino debe ser distinto de los generados en la primaria ya que pueden producirse errores de sobre escritura de los ficheros. Una opción sería poner el nombre de cada base de datos delante del formato, por ejemplo, sigloexa%t_%s_%r.dbf.
- A partir de 12C, si se usa Oracle Clusterware o Oracle Restart ya no es necesario incluir un registro estático (DGMGRL) para el bróker en el listener. Si usamos Single instance sin Oracle Restart se debería seguir realizando como en 11GR2. Para la configuración de Data Guard Broker en 11.2 es necesario añadir la cláusula `db_unique_name_DGMGRL.db_domain` en la configuración del listener de la instancia del siguiente modo:

```

LISTENER = (DESCRIPTION =
  (ADDRESS_LIST=(ADDRESS=(PROTOCOL=tcp) (HOST=host_name)
    (PORT=port_num))) ) SID_LIST_LISTENER=(SID_LIST=(SID_DESC=(SID_NAME
=sid_name) (GLOBAL_DBNAME=db_unique_name_DGMGRL.db_domain)
    (ORACLE_HOME=oracle_home)))

```
- Oracle recomienda que se configuren todos los parámetros tanto en las bases de datos primarias como en standby (Cross Configuration) para evitar futuros problemas tras cambios de rol.

RECOMENDACIONES DE ALMACENAMIENTO

Este apartado describe las recomendaciones respecto al almacenamiento en Oracle Data Guard.

Recomendaciones generales

A partir de la versión 10gR2 Oracle recomienda que todos los archivos de datos o datafiles (incluyendo el tablespace de UNDO) y ficheros de redolog residan en un diskgroup de ASM. En caso de no disponer de ASM se recomienda el uso de file system para almacenar estos ficheros.

Si se hace uso de ASM, se recomienda seguir la guía de buenas prácticas de ASM referenciada en la doc Automatic Storage Management Administrator's Guide <https://docs.oracle.com/database/122/OSTMG/title.htm>

A menos que se indique lo contrario, la base de datos Oracle seguirá las recomendaciones de almacenamiento siguiendo las best practices de Oracle Management Files (OMF), la gestión automática de espacio en los segmentos, y así sucesivamente.

Oracle Flexible Architecture

Optimal Flexible Architecture (OFA), como se conoce a la guía de buenas prácticas de nomenclatura y configuración de base de datos Oracle, asegura instalaciones fiables y mejora la administración de las bases de datos. Estas recomendaciones están guiadas para optimizar la forma en que las instalaciones de software de Oracle se organizan, simplifica la gestión de instalaciones y mejora la capacidad de una buena administración ofreciendo las opciones de OFA por defecto, haciendo bases de datos Oracle que se instalen más en concordancia con las especificaciones de la OFA.

Durante la instalación, se le pide que especifique una ubicación para la ruta de (ORACLE_BASE), que tiene que ser propietaria del usuario que realiza la instalación. Puede elegir un ORACLE_BASE existente, o elegir otra ubicación dentro de un directorio que no tiene la estructura de un directorio ORACLE_BASE.

Utilizando la ruta del Oracle Base ayuda para facilitar la organización de las instalaciones de Oracle, y ayuda a garantizar que las instalaciones de varias bases de datos mantienen una configuración en concordancia con la OFA.

Durante la instalación, ORACLE_BASE es el único valor requerido como entrada, ya que el ORACLE_HOME es una ubicación secundaria dentro de la elegida sobre la para la ORACLE_BASE. Además, Oracle recomienda que se establezca la variable de entorno ORACLE_BASE además de la variable ORACLE_HOME, para ser cargadas en los perfiles de los usuarios que se dispongan a arrancar las bases de datos Oracle. Tenga en cuenta que ORACLE_BASE puede convertirse en una variable de entorno necesaria para el inicio de base de datos en una futura versión.

Ficheros de base de datos

Cada base de datos que forma parte de una configuración en Data Guard posee su propio conjunto de ficheros independientes de los de las otras bases de datos. Entre estos ficheros tendremos:

- **Fichero de parámetros (SPFILE o PFILE):** Se recomienda la utilización de SPFILE ya que permiten un mejor mantenimiento. Los ficheros de parámetros de las instancias en standby provendrán de una copia del existente en la base de datos primaria, realizando las modificaciones correspondientes.
- **Controlfiles:** Cada base de datos debe poseer al menos tres copias consistentes del controlfile situadas en distintas localizaciones. Estos controlfiles no son compartidos entre las distintas bases de datos.
- **Datafiles:** Cada base de datos debe poseer su propio conjunto de data files. Además, Oracle recomienda que se sitúen en la misma ruta siempre y cuando la instancia primaria y la standby no se encuentren en el mismo host. Estos ficheros deberán poseer el mismo nombre en todas las bases de datos en caso de no hacer uso de OMF.
- **Redologs:** Los redo logs son independientes entre cada base de datos que forme parte de la configuración. En Oracle Data Guard existen dos tipos de redo log:
 - **Online redo log:** Utilizado por la base de datos primaria. Se recomienda al menos la existencia de 3 grupos de redos con dos miembros cada uno situado en distintas localizaciones.
 - **Standby redo log:** Utilizado por las bases de datos en standby. Su tamaño debe ser igual al de los online redo log de la primaria. Debe existir un standby redo log en las standby más que online redo logs en la primaria.

Archived logs: Todas las bases de datos que formen parte de una configuración en Data Guard deben estar en modo archivado y por lo tanto cada una generará sus propios archives.

Arquitectura de directorios

Existen diferentes opciones a la hora de establecer la arquitectura de directorios en los que se va a construir una base de datos en standby en caso de no hacer uso de ASM. Las opciones son las siguientes:

- Crear la instancia en standby en un host diferente que la primaria, pero con la misma estructura de directorios.
- Crear la instancia en standby en un host diferente que la primaria, pero en una estructura de directorios distinta.
- Crear la instancia en standby en el mismo host que la primaria, pero en una estructura de directorios distinta.

Oracle recomienda que las bases de datos en standby se encuentren en un host distinto a la primaria y que además usen la misma estructura de directorio.

En el caso de tener diferentes estructuras de directorios es necesario establecer los siguientes parámetros para evitar fallos en el manejo de datafiles y redo logs: DB_FILE_NAME_CONVERT y LOG_FILE_NAME_CONVERT.

Para la creación y manejo de ciertos ficheros como data files en bases de datos en standby es necesario establecer el parámetro STANDBY_FILE_MANAGEMENT a AUTO.

RECOMENDACIONES EN LOS SERVICIOS DE TRANSPORTE

En este apartado se detallan las configuraciones recomendadas para los distintos métodos de transporte de información entre la base de datos primaria y las standby en un entorno de Data Guard.

Recomendaciones generales de configuración de red

Esta sección describe las recomendaciones con respecto a la configuración de red aplicables a todos los métodos de transporte para mejorar el rendimiento del envío de redo en un entorno de Data Guard. Los aspectos a tener en cuenta son los siguientes:

- Asegurar que el ancho de banda para transmitir a las bases de datos standby los redo generados por la primaria es suficiente.
- Establecer los parámetros de Oracle Net RECV_BUF_SIZE y SEND_BUF_SIZE iguales a 3 veces el Bandwidth Delay Product (BDP). El tamaño del buffer puede ser establecido a nivel de sistema operativo o a nivel de Oracle Net. Se recomienda establecerlos a nivel de Oracle Net para que otras sesiones TCP no usen más memoria de la necesaria. Estos parámetros se pueden establecer en el listener.ora a nivel de DESCRIPTION o ADDRESS.
- Usar un tamaño de 65535 para Oracle Net Session Data Unit (SDU). Subir este parámetro requerirá más consumo de memoria. Para configurarlo debemos añadir el parámetro DEFAULT_SDU_SIZE en el fichero sqlnet.ora.
- Incrementar los tamaños de las colas de envío y recepción asociadas con los dispositivos de red. Para futuros cambios de rol se recomienda cambiar estos valores tanto en la base de datos primaria como standby.

Documentación oficial:

Best Practices for Synchronous Redo Transport

<http://www.oracle.com/technetwork/database/availability/sync-2437177.pdf>

Database Net Services Administrator's Guide 12c

<https://docs.oracle.com/database/122/NETAG/optimizing-performance.htm#NETAG014>

Recomendaciones generales de configuración de métodos de transporte

Independientemente del método de transporte usado, se recomienda:

- Hacer tuning de los standby redo logs para un eficiente I/O. Con esto, se evita que el proceso RFS escriba en la standby frenando los procesos de envío (LNS

and ARCH) en la base de datos de producción. RFS es el proceso de Data Guard en la base de datos standby que recibe los redo y los escribe en el standby redo log. Las áreas típicas en las que hacer tuning en el subsistema de I/O de la standby pueden incluir:

- Asegurar que los redo logs de la standby redo logs están bien colocados en un disk group rápido.
- No multiplexar standby redo logs. Eliminar los standby redo log members multiplexados para prevenir escrituras adicionales.

Recomendaciones de configuración para LGWR SYNC Redo Transport

Si se hace uso de envío de información a través de LGWR SYNC se recomienda:

- Decrementar el valor del atributo NET_TIMEOUT para reducir el impacto de interrupciones en la red sobre el rendimiento de bases de datos de producción. Este atributo especifica el número de segundos que LGWR espera en la base de datos de producción a que Oracle Net Services responda a una de sus peticiones. En Oracle Database 12 Release 2 el valor por defecto de NET_TIMEOUT es de 30 segundos. Aunque se permite un valor de 1 segundo, Oracle recomienda 10 segundos como mínimo para evitar una desconexión innecesaria de la base de datos standby.

Nota: Los usuarios tienen a menudo la tentación de poner este valor a menos de 10 segundos. Es importante conocer muy bien el entorno para determinar el valor óptimo en lugar de ponerlo tan bajo. Por ejemplo, si se pone a 2 segundos, y en la red se pueden producir caídas en la red de hasta 3 segundos, se podrán producir tiempos de espera y un gran impacto a los niveles de protección de datos.

- Al usar LGWR SYNC los commits no son finalizados hasta que la información de redo no se escribe tanto localmente en la primaria como en remoto en la standby. Opcionalmente, se puede usar el parámetro COMMIT NOWAIT para que los commits se devuelvan a la aplicación sin tener que esperar a que los redo se escriban a disco. Por lo tanto, las aplicaciones o transacciones que pueden utilizar COMMIT NOWAIT tendrán una importante mejora en tiempo de respuesta y el rendimiento de la base de datos sobre las aplicaciones o transacciones que utilizan el comportamiento por defecto de COMMIT WAIT.

Recomendaciones de configuración para Standby

Si no está configurado el Real Time Apply el redo en la standby se escribe a disco. En algunas configuraciones, la escritura en disco debe ser anterior al envío de la confirmación a la primaria de que el redo se ha recibido. Por lo tanto, es importante optimizar el I/O en la standby. Para mejorar el rendimiento del I/O en la standby, hay que considerar las siguientes buenas prácticas:

1. Asegurar que Oracle puede utilizar ASYNC I/O. Por defecto la base de datos de Oracle está configurada para asynchronous I/O. Sin embargo, también debe configurar adecuadamente el sistema operativo, Host Bus Adapter (HBA) driver, y storage array. Revisar el valor del parámetro `filesystemio_options`. El valor recomendado sería `SETALL`.
2. Maximizar la entrada I/O a través de todas las capas: sistema operativo (incluyendo `async write size`), drivers de dispositivos, storage network transfer size, disk array.
3. Poner SRLs en el diskgroup de ASM que tiene al menos, el mismo número de discos que el diskgroup de ASM donde residen los online redo logs de la primaria.
4. No multiplexar los redo logs de la standby.
5. Normalmente los controladores RAID configurados en RAID5 lleva a cabo escrituras más lentas que cuando se configuran con mirroring. Si el proceso de escritura a SRL pasa por un cuello de botella habrá que considerar el cambio de configuración de RAID.

Eventos de espera relacionados con los servicios de transporte

El tiempo empleado en enviar redo desde la base de datos de producción a una standby puede ser dividido en dos secciones; el tiempo en atravesar la red y el de escritura en disco en el host de standby. Los eventos de espera que capturan el total del tiempo se obtienen en la base de datos de producción, mientras que el tiempo empleado para el I/O se puede ver en la standby.

A partir de 12c desaparece el proceso LNS (Log Network Server) que en 11g era el responsable de mandar el redo a la standby. En 12c tendremos:

- El proceso NSS, que envía el redo desde LGWR a la standby remota cuando estamos en modo SYNC.
- El proceso NSA, que envía el redo desde los online redo logs a la standby remota cuando estamos en modo ASYNC.

En la siguiente tabla se muestran los principales eventos de espera en 12c:

EVENT NAME	DESCRIPTION
ARCH REMOTE WRITE	The time (in centi-seconds) that ARCn background processes spend blocked waiting for network write operations to complete.
ASYNC REMOTE WRITE	The time (in centi-seconds) for asynchronous streaming RFSWRITE operations. This includes stall reaps and streaming network submission time. This

	time is accumulated by TTnn (Redo Transport Slave) background processes.
REDO TRANSPORT ATTACH	The time spent (in centi-seconds) doing Connect, Logon, and RFSATTACH for any network process.
REDO TRANSPORT CLOSE	The time spent (in centi-seconds) by ARCn, NSSn, and TTnn processes doing RFSCLOSE and RFSRGSTR operations.
REDO TRANSPORT DETACH	The time spent (in centi-seconds) doing RFSDETACH and Disconnect for any network process.
REDO TRANSPORT OPEN	The time spent (in centi-seconds) by ARCn, NSSn, and TTnn background processes doing RFSCREAT and RFSANNCE operations.
REDO TRANSPORT PING	The time spent (in centi-seconds) by ARCn background processes doing RFSPING operations. Redo Transport Slave Shutdown The time spent (in centi-seconds) by LGWR doing NSSn and TTnn process shutdown and termination.
REDO TRANSPORT SLAVE STARTUP	The time spent (in centi-seconds) by LGWR doing NSSn and TTnn process startup and initialization
REDO WRITER REMOTE SYNC COMPLETE	The time spent (in centi-seconds) by LGWR reaping completed network writes to remote destinations.
REDO WRITER REMOTE SYNC NOTIFY	The time spent (in centi-seconds) by LGWR issuing network writes to remote destinations.
REMOTE SYNC PING	The time spent (in centi-seconds) by the LGWR and NSSn background processes doing synchronous PING operations.
SYNC REMOTE WRITE	The time spent by LGWR doing SYNC RFSWRITE operations.

Si la standby es física, podemos usar la siguiente consulta para sacar información de los eventos de espera:

```
SQL> SELECT EVENT, TOTAL_WAITS,
ROUND(TIME_WAITED/100) "TIME(S)",
AVERAGE_WAIT*10 "AVG(MS)",
TO_CHAR(SYSDATE, 'DD-MON-YYYY HH:MI:SS') TIME
FROM V$SYSTEM_EVENT;
```

En caso de existir problemas de rendimiento en la fase de transporte se recomienda revisar el White paper **Best Practices for Synchronous Redo Transport** <http://www.oracle.com/technetwork/database/availability/sync-2437177.pdf> y la nota **Troubleshooting Data Guard Log Transport Services (Doc ID 1604963.1)**

RECOMENDACIONES EN LOS SERVICIOS DE REDO APPLY

En este apartado se detallan las configuraciones recomendadas para la aplicación de cambios en una standby física en un entorno de Data Guard. La aplicación de cambios se lleva a cabo a través de Redo Apply.

Recomendaciones generales de configuración

La recuperación se lleva a cabo cuando uno o más datafiles o controlfiles son restaurados desde un backup previo o cuando se usa Data Guard Redo Apply (base de datos standby física). El objetivo del proceso es llevar a la base de datos a un estado consistente en el tiempo o aplicar todas las transacciones realizadas en la base de datos primaria en las bases de datos standby físicas.

A partir de 12c, el proceso MRP se activa por defecto con la opción Real time apply. Esto permite que los cambios se apliquen en la standby a la misma vez que son escritos en los redologs de la primaria, no es necesario que estos cambios queden pendientes hasta la generación de un Archive. Si quisiéramos desactivar Real-Time usaríamos la cláusula USING ARCHIVED LOGFILE.

Para aumentar el rendimiento durante el proceso de recover, Oracle recomienda:

- Configurar el parámetro `PARALLEL_EXECUTION_MESSAGE_SIZE` a 65535. Este parámetro es usado por las parallel query y extrae memoria de la shared pool. Cuando se incrementa su valor hay que tener en cuenta la cantidad de shared pool disponible.
- Establecer el parámetro `DB_BLOCK_CHECKING` a FALSE en la standby durante la recuperación incrementa notablemente el rendimiento durante el proceso. Oracle recomienda habilitar la comprobación a nivel de bloque en las bases de datos de producción.
- Tunear el subsistema de I/O:
 - o Asegurar que Oracle puedes usar ASYNC I/O. La base de datos funciona en este modo por defecto, pero es necesario configurar el sistema operativo y el hardware para que pueda ser posible.
 - o Maximizar el tamaño de escritura de I/O a través de todas las capas de la pila de I/O. Entre estas capas se encuentran, por ejemplo, el sistema operativo y el tamaño de transferencia a través de la red.
 - o Establecer el parámetro `DISK_ASYNC_IO` a TRUE (por defecto).
 - o Establecer el parámetro `DB_WRITER_PROCESSES` a un valor superior a 1 cuando I/O asíncrono está disponible y los eventos de espera free buffer waits o checkpoint completed se encuentran entre los más encontrados.

- Si siguen apareciendo “free buffer wait” como un evento de espera significativo se recomienda incrementar el buffer cache.
 - Incrementar el tamaño de los online redo logs de la primaria y los standby redo logs en la base de datos en standby para disminuir el número de checkpoints realizados.
 - Situar los online y standby redo logs en los discos con mayor rendimiento.
- La vista V\$RECOVERY_PROGRESS permite monitorizar el rendimiento del recovery en tiempo real.
 - La vista V\$SYSTEM_EVENT permite monitorizar los eventos de espera ocurridos durante el recover y ayudar a realizar optimizaciones en el sistema.

Es necesario destacar que cuando se tiene una base de datos standby en RAC el recover se realice en una única instancia llamada apply instance.

Documentación oficial:

Applying Redo Data to Physical Standby Databases

https://docs.oracle.com/database/121/SBYDB/log_apply.htm#SBYDB00500

RECOMENDACIONES EN LOS SERVICIOS DE SQL APPLY

En este apartado se detallan las configuraciones recomendadas para la aplicación de cambios en una standby lógica en un entorno de Data Guard. La aplicación de cambios se lleva a cabo a través de SQL Apply.

Recomendaciones generales de configuración

Para aumentar el rendimiento durante el proceso de SQL apply, Oracle recomienda:

- Confirmar el soporte de los tipos de datos. Cualquier tabla que contenga tipos de datos no soportados no será actualizada.
- El parámetro COMPATIBLE restringe el número de tipo de datos soportados por la base de datos standby lógica. Se recomienda establecer el parámetro al valor más alto posible.
- Usar Standby Redo Logs (obligatorio en 12c). Con su uso SQL Apply no debe esperar a que el archive log sea recibido y registrado en la base de datos en standby para comenzar a extraer la información.
- Usar Real-Time Apply (configuración por defecto en 12c). Permite aplicar cambios a medida que se van recibiendo sin tener que esperar a que el actual standby redo log sea archivado.
- Debido al diferente uso que se hace de la base de datos en standby lógica puede ser necesario una diferente configuración de las distintas estructuras de memoria de la instancia. Por eso es necesario realizar un estudio de su rendimiento y aplicar las acciones necesarias.
- Puede ser necesaria la creación de índices adicionales para aumentar el rendimiento, así como la modificación de las sentencias lanzadas directamente contra la instancia en standby atendiendo a las estadísticas obtenidas del sistema y los planes de ejecución de las mismas. Se recomienda revisar la nota 312434.1.
- Ajustar el número de procesos APPLIER y PREPARER
- Ajustar la memoria usada por la cache LCR
- Ajustar el número de transacciones aplicadas en la standby lógica

Documentación oficial:

Managing a Logical Standby Database

https://docs.oracle.com/database/121/SBYDB/manage_ls.htm#SBYDB4804

Applying Redo Data to Logical Standby Databases

https://docs.oracle.com/database/121/SBYDB/log_apply.htm#SBYDB4766

RECOMENDACIONES DURANTE CAMBIOS DE ROL

En este apartado se detallan las configuraciones recomendadas y buenas prácticas para la realización efectiva de un cambio de rol en un entorno Data Guard 12cR2.

Recomendaciones generales de configuración para Switchover

Un switchover garantiza que no se perderán datos y es la típica solución ante una parada de mantenimiento planificada en un entorno productivo. Durante un switchover los roles se intercambian. Tras el cambio, pasaremos a dar servicio desde la antigua standby.

En este documento se detallan las buenas prácticas para entornos DG con standby físicas, si se desea realizar un switchover a una standby de tipo lógico o snapshot se recomienda leer con detalle la documentación oficial.

Documentación oficial:

Performing a Switchover to a Physical Standby Database

<https://docs.oracle.com/database/122/SBYDB/managing-oracle-data-guard-role-transitions.htm#GUID-AAD70601-D248-4309-B8DD-F461EE31A5FF>

Before You Perform a Switchover Operation

<https://docs.oracle.com/database/122/DGBKR/using-data-guard-broker-to-manage-switchovers-failovers.htm#DGBKR340>

Existen tres formas de realizar un switchover, de forma manual usando sqlplus, mediante la interfaz del bróker (dgmgrl) o través de la consola de Cloud Control. Para la última opción se recomienda ir a la documentación oficial.

Buenas prácticas switchover con SQLPLUS

A continuación, se enumeran algunas recomendaciones a tener en cuenta durante la realización de un switchover mediante el bróker.

Las recomendaciones de esta sección pertenecen a la documentación oficial y a la nota **12c Data guard Switchover Best Practices using SQLPLUS (Doc ID 1578787.1)**.

- Asegurarse que el destino está listo para realizar el switchover.

```
SQL>alter database switchover to <target standby db_unique_name>  
verify;
```

El comando previo verifica la sincronización del entorno, las versiones y la configuración de los Standby redo logs.

- Revisar los ficheros temporales en ambos entornos, pueden existir tempfiles que no se hayan propagado a los entornos standby.

```
SQL> col name for a45
```

```
SQL> select ts#, name,ts#,status from v$tempfile;
```

- Activar el trazo por si fuera necesario para un diagnostico posterior.

```
SQL>alter system set log_archive_trace=8191 sid='*';
```

- Durante el switchover se debe hacer un tail a los ficheros de alert para poder ver la aparición de posibles errores.

```
tail -f <alert log of primary>
```

```
tail -f <alert log of standby>
```

- Realizar el switchover

```
SQL>alter database switchover to standby-db-unique-name
```

- Abrir la nueva primaria

```
SQL>alter database open;
```

- Reiniciar la standby y activar el MRP

```
SQL>shut immediate;
```

```
SQL>startup
```

```
SQL>alter database recover managed standby database disconnect;
```

- Chequear la sincronización.

Buenas prácticas switchover con DGMGRL

A continuación, se enumeran algunas recomendaciones a tener en cuenta durante la realización de un switchover mediante el bróker.

Las recomendaciones de esta sección pertenecen a la documentación oficial y a la nota *12c Dataguard Switchover Best Practices using DGMGRL (Doc ID 1582837.1)*

Después de que se complete el switchover, el broker preservara el modo de protección que estuviera configurado de forma previa al switchover e igualmente realizará el inicio automático de los procesos de redo apply (MRP) en las standby del entorno.

- Asegurarse que los standby redo logs existen en ambos entornos. El bróker realizará dicho chequeo como paso previo al switchover, pero se recomienda validarlo manualmente.
- Chequear que la parametrización en el Broker es la correcta. Los chequeos deben mostrar que los estados de los entornos son satisfactorios (success).

```
DGMGRL>show configuration;
```

```
DGMGRL>show database verbose <primary>;
```

```
DGMGRL>show database verbose <standby>;
```

Revisar que los valores de los parámetros LogXptMode, NetTimeout, StandbyArchiveLocation, AlternateLocation y RedoRoutes son los adecuados.

- También se recomienda revisar que no existen incongruencias en la configuración del bróker para ninguna de las bases de datos pertenecientes al entorno DG.

```
DGMRL> show database <primary-db-unique-name> logxptstatus;
```

```
DGMGRL> show database <standby-db-unique-name>  
inconsistentlogxptprops;
```

- A partir de la versión 12, aparece la funcionalidad VALIDATE. Esta opción realiza un conjunto bastante completo de chequeos. (Revisión de redologs, flashback, ficheros temporales, estado standby redo logs, aplicación de redo, propiedades transporte, etc...)

Se recomienda realizar lo siguiente:

```
DGMGRL> validate database verbose <primary db-unique-name>
```

```
DGMGRL> validate database verbose <standby db-unique-name>
```

- Si se hubiera configurado un delay entre la primaria y la standby, se debería eliminar antes de realizar el switchover.

```
DGMGRL> edit database <STANDBY db-unique-name> set property  
'DelayMins' = '0';
```

- Si recomienda activar el traceo como paso previo al switchover.

```
DGMGRL> edit configuration set property tracelevel=support;
```

```
DGMGRL> edit database primary-db-unique-name set property  
LogArchiveTrace=8191;
```

```
DGMGRL> edit database standby-db-unique-name set property  
LogArchiveTrace=8191;
```

- Durante el switchover se debe hacer un tail a los ficheros de alert y bróker para poder ver la aparición de posibles errores.

```
tail -f <alert log of primary>

tail -f <alert log of standby>

tail -f <drc<SID> log of primary>

tail -f <drc<SID> log of standby>
```

- Conectarse con el usuario sysdg para realizar el switchover:

```
DGMGRL> connect sysdg

Password:

Connected as SYSDBG.

DGMGRL> switchover to standby-db-unique-name
```

- Chequear la configuration and sincronización.

Recomendaciones generales de configuración para Failover

En un failover se realiza una conversión de la standby a primaria, este cambio se debe realizar causado por un fallo irrecuperable en la primaria.

Para llevar a cabo un failover de forma satisfactoria es necesario seguir los pasos indicados en los manuales oficiales del producto.

Documentación oficial:

Performing a Failover to a Physical Standby Database

<https://docs.oracle.com/database/122/SBYDB/managing-oracle-data-guard-role-transitions.htm#SBYDB5171>

Complete and Immediate Manual Failovers

<https://docs.oracle.com/database/122/DGBKR/using-data-guard-broker-to-manage-switchovers-failovers.htm#DGBKR3405>

Existen tres formas de realizar un failover, de forma manual usando sqlplus, mediante la interfaz del bróker (dgmgrl) o través de la consola de Cloud Control. Para la última opción se recomienda ir a la documentación oficial.

Debemos diferenciar entre dos tipos de Failover, Completo o Inmediato.

- **Failover Completo.** Este failover es el recomendado. Durante el procedimiento recuperamos la standby hasta el último cambio generado por la primaria. Con este procedimiento existe la seguridad de que no se están dejando cambios sin aplicar. Si existieran más standbys en el entorno estas podrían mantenerse como standbys de la nueva primaria.

- **Failover Inmediato.** Este tipo de failover es el más rápido. Pero por el contrario no fuerza que se apliquen en la standby todos los cambios generados. Si existieran más entornos standby estos deberían de ser reinstanciados o recreados para resincronizarlos con la nueva primaria.

Failover Completo con SQLPLUS

- Chequeamos el estado de la standby. Como la primaria probablemente se encuentre caída, nos mostrará el estado NOT ALLOWED.

```
SQL> SELECT SWITCHOVER_STATUS FROM V$DATABASE;  
  
SWITCHOVER_STATUS  
-----  
  
NOT ALLOWED
```

- Chequemos si existen GAPS.

```
SQL> SELECT THREAD#, LOW_SEQUENCE#, HIGH_SEQUENCE# FROM  
V$ARCHIVE_GAP;  
  
no rows selected
```

- Si dichos archivos se pudieran mandar a la standby, los moveríamos y los registraríamos.

```
SQL> ALTER DATABASE REGISTER PHYSICAL LOGFILE 'file1';
```

- Si pudiéramos montar la primaria, realizaríamos un FLUSH del redo.

```
SQL> ALTER SYSTEM FLUSH REDO TO STANDBY_DB_UNIQUE_NAME;
```

- En la standby cancelamos el MRP y lo activamos con la opción finish.

```
SQL> ALTER DATABASE RECOVER MANAGED STANDBY DATABASE CANCEL;  
  
Database altered.
```

```
SQL> ALTER DATABASE RECOVER MANAGED STANDBY DATABASE FINISH;  
  
Database altered.
```

Si el finish no finalizará tendríamos que realizar un Failover Inmediato.

- Si el FINISH acaba correctamente podríamos ver que el switchover_status ya nos permitiría cambiar la standby a primaria.

```
SQL> SELECT SWITCHOVER_STATUS FROM V$DATABASE;  
  
SWITCHOVER_STATUS  
-----  
  
TO PRIMARY
```

- Cambiamos el rol de la standby a nueva primaria

```
SQL> ALTER DATABASE COMMIT TO SWITCHOVER TO PRIMARY WITH SESSION  
SHUTDOWN;  
  
Database altered.
```

- Abrimos la nueva primaria

```
SQL> ALTER DATABASE OPEN;  
  
Database altered.
```

Failover Inmediato con SQLPLUS

Si el error no se pudiera resolver, la opción que tendríamos es activar la standby como primaria, también llamado failover inmediato. Este procedimiento puede activar la nueva primaria sin que está tenga aplicados todos los cambios que se han generado en la primaria, provocando una pérdida de datos.

- Activamos la nueva primaria lanzando el siguiente comando en la standby

```
SQL> ALTER DATABASE ACTIVATE PHYSICAL STANDBY DATABASE;
```

- Tras activarla, la abrimos.

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

La antigua primaria tendremos que reinstanciarla o recrearla.

Failover Completo con DGMGRL

```
DGMGRL> FAILOVER TO database-name
```

Si nos aparecieran algunos de los siguientes errores deberíamos realizar un Failover Inmediato con DGMGRL

- ORA-752 en la standby
- ORA-600 [3020] ocurrido por una corrupción Lost_write de la primaria
- Cualquier tipo de error que nos imposibilite realizar un failover completo

Failover Inmediato con DGMGRL

Este procedimiento puede activar la nueva primaria sin que ésta tenga aplicados todos los cambios que se han generado en la primaria, provocando una pérdida de datos.

```
DGMGRL> FAILOVER IMMEDIATE TO database-name
```

Recomendaciones generales de configuración de los clientes

Una arquitectura en alta disponibilidad no solo tiene que conseguir failover a nivel de base de datos, sino conseguir también el failover de los clientes conectados a la misma de forma transparente.

A partir de la versión 10gR2 de Oracle Data Guard se añade la funcionalidad de redireccionar de forma automática a los clientes y aplicaciones a la nueva base de datos primaria. Esto disminuye también el tiempo empleado en realizar un cambio de rol ya que se suprime la redirección manual de los usuarios finales.

Además, Oracle Database 12c aporta aún más capacidades en el área de Failover de cliente y reduce en gran medida los cambios en la aplicación para habilitar la notificación rápida de aplicaciones (FAN). Configurar la arquitectura de máxima disponibilidad en un entorno 12c nos va a permitir que, tras una caída o un mantenimiento planificado, los usuarios pueden continuar procesando sus transacciones sin interrupciones.

El siguiente artículo describe las mejores prácticas de MAA para transferir automáticamente las conexiones de aplicación de una base de datos primaria fallida a una nueva base de datos primaria después de que se haya producido una transición de rol de Oracle Data Guard.

[Client Failover Best Practices for Highly Available Oracle Databases for Oracle Database 12c](#)

- Notas de My Oracle Support:
 - o Application Client Failover Considerations in an Oracle Data Guard Environment (Doc ID 2123709.1)

RECOMENDACIONES DE BACKUP & RECOVERY

Esta sección explica cómo realizar un backup y restore de bases Oracle en Data Guard haciendo uso de Recovery Manager (RMAN), así como un conjunto de buenas prácticas y pasos a tener en cuenta en este tipo de arquitecturas.

Como norma, se hará uso de la herramienta RMAN como software de backup de base de datos Oracle. RMAN permite la realización de backup, restores, recuperación de datafiles, ficheros de control, SPFILES y archivelogs. RMAN está incluido con el software de Oracle RDBMS.

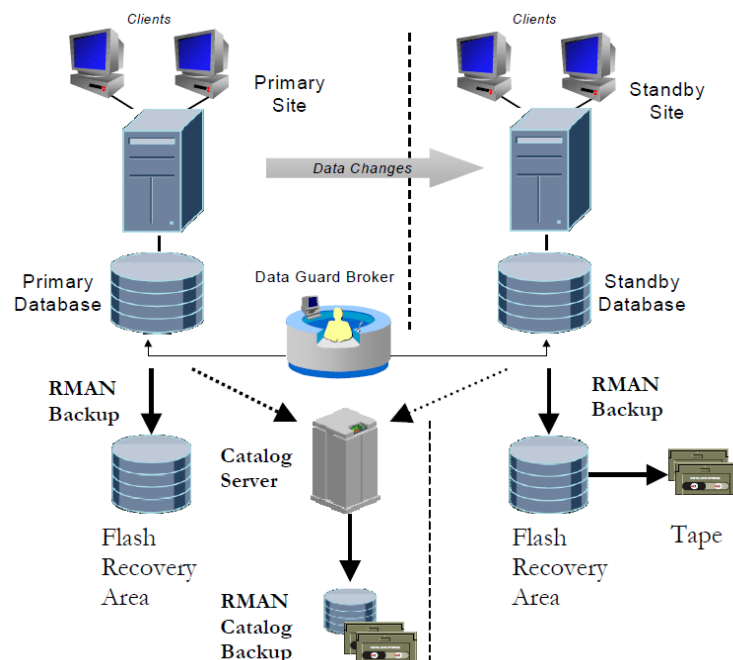
El procedimiento para usar RMAN en entornos Data Guard no difiere substancialmente del uso realizado para entornos single-instance. En los siguientes apartados se comentarán algunas particularidades del mismo.

Documentación:

<https://docs.oracle.com/database/122/SBYDB/using-RMAN-in-oracle-data-guard-configurations.htm#SBYDB04700>

Arquitectura de backup

En la siguiente imagen se muestra una posible arquitectura de servidores necesaria para la realización de backups en un entorno de Data Guard:



Documentación:

<https://docs.oracle.com/database/122/SBYDB/using-RMAN-in-oracle-data-guard-configurations.htm#SBYDB04700>

https://docs.oracle.com/cd/E18283_01/server.112/e17022/rman.htm#BAJEDHFB

Estrategia de backup

Utilizar la base de datos de standby física para la realización de backups puede descargar de trabajo a la instancia primaria e incluso permite la realización de backups en frío de la instancia sin necesidad de haber cortes en el sistema en producción.

A la hora de realizar backups en las bases de datos en standby hay que tener en cuenta los siguientes aspectos:

- En caso de ser una base de datos standby lógica es necesario realizar el backup en dicha instancia y en la primaria para tener backups válidos de todos los entornos. Los backups en estos entornos no son intercambiables entre ambas bases de datos.
- Es necesario realizar el backup del controlfile en todos los entornos ya que no son intercambiables.
- Únicamente los backups realizados en standby físicas pueden ser utilizados para restaurar instancias primarias.
- Se recomienda usar el catálogo de RMAN. Si no se hiciera uso del catálogo se tendrían que registrar en la primaria los backups tomados en la standby, el controlfile de la primaria no conocería por defecto los backups realizados.
- Es recomendable que el RMAN Recovery Catalog se encuentre en un servidor independiente a la primaria y a la standby. Configuración recomendada para Oracle Database.

Configuración de base de datos

Independiente del destino seleccionado para realizar el backup, se recomienda realizar la siguiente configuración en ambos entornos:

- Configurar Flash Recovery Area. Los nuevos backups y archive redo logs serán almacenados en la Flash Recovery Area y los obsoletos serán automáticamente eliminados.
- Usar SPFILE, lo que permite que será restaurado desde un backup tomado desde otra instancia.
- Identificar con un nombre único los archived log y los directorios de backup para cada base de datos. Esto permite el uso de ciertos comandos RMAN como BACKUP ARCHIVELOG, CROSSCHECK y DELETE, en conjunción con la cláusula LIKE para seleccionar los ficheros correspondientes a una determinada instancia.
- Etiquetar de forma unívoca los backups si son realizados tanto en la base de datos primaria como en la standby. Esto permite diferenciar el entorno en el que se ha realizado el backup.
- Habilitar Flashback Database. Permite revertir la base de datos a un punto en el tiempo sin necesidad de realizar un restore.
- Se recomienda usar catálogo para registrar los backups. Únicamente será necesario registrar la primaria.
- Se deben configurar ambos entornos en el catálogo, usando el DB_UNIQUE_NAME como identificador único.

```
RMAN> CONFIGURE DB_UNIQUE_NAME orcl12 CONNECT IDENTIFIER 'orcl12';
```

```
RMAN> CONFIGURE DB_UNIQUE_NAME orcl12dg CONNECT IDENTIFIER  
'orcl12dg';
```

Configuración recomendada para RMAN

Si el backup se realiza en la primaria

- La siguiente configuración se llevará a cabo tras conectarse a la base de datos **primaria** donde se van a realizar los backups y al catálogo de RMAN:
 - CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF <n> DAYS. La base de datos de standby hará uso de este parámetro al conectarse al catálogo. Todos los backups realizados en la base de datos de standby serán conservados al menos <n> días. La Flash Recovery Area eliminará los ficheros obsoletos de forma automática si es necesario.
 - CONFIGURE ARCHIVELOG DELETION POLICY TO APPLIED ON ALL STANDBY BACKED UP 'n' TIMES TO DISK. Habilita el borrado automático de los archived logs en la base de datos primaria que han sido aplicados en, al menos, una de las standby. Además, imposibilita que se pueda borrar un archive si no existe al menos un backup de este.

- CONFIGURE CONTROLFILE AUTOBACKUP ON para realizar backups automáticos del control file y el SPFILE.
- CONFIGURE BACKUP OPTIMIZATION ON para no realizar backup de aquellos ficheros de base de datos para los que exista un backup válido.
- CONFIGURE CHANNEL DEVICE TYPE SBT PARMS '<channel parameters>' para configurar los parámetros de los canales requeridos por el software de copia a cinta.
- La siguiente configuración se llevará a cabo tras conectarse al resto de bases de datos **standby** y al catálogo de RMAN:
 - CONFIGURE ARCHIVELOG DELETION POLICY TO APPLIED ON ALL STANDBY. Permite el borrado automático de los archived logs de la standby donde no se están realizando los backups que han sido aplicados en el resto de destinos remotos si se requiere espacio para nuevos archives.

Si el backup se realiza en la standby

- La siguiente configuración se llevará a cabo tras conectarse a la base de datos **primaria** y al catálogo de RMAN:
 - CONFIGURE ARCHIVELOG DELETION POLICY TO APPLIED ON ALL STANDBY. Permite el borrado automático de los archived logs de la standby donde no se están realizando los backups que han sido aplicados en el resto de destinos remotos si se requiere espacio para nuevos archives.
- La siguiente configuración se llevará a cabo tras conectarse a la base de datos **standby** donde se van a realizar los backups y al catálogo de RMAN:
 - CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF <n> DAYS. La base de datos de standby hará uso de este parámetro al conectarse al catálogo. Todos los backups realizados en la base de datos de standby serán conservados al menos <n> días. La Flash Recovery Area eliminará los ficheros obsoletos de forma automática si es necesario.
 - CONFIGURE ARCHIVELOG DELETION POLICY BACKED UP 1 TIMES TO DISK. Imposibilita que se pueda borrar un archive si no existe al menos un backup de este.
 - CONFIGURE CONTROLFILE AUTOBACKUP ON para realizar backups automáticos del control file y el SPFILE.
 - CONFIGURE BACKUP OPTIMIZATION ON para no realizar backup de aquellos ficheros de base de datos para los que exista un backup válido.

- `CONFIGURE CHANNEL DEVICE TYPE SBT PARMS '<channel parameters>'` para configurar los parámetros de los canales requeridos por el software de copia a cinta.

NOTA:

En caso de switchover o failover, tras el cambio de rol, es necesario realizar la configuración adecuada en la nueva primaria y standby.

La versión 11GR2 está afectada del siguiente BUG 13829787: DELETE BACKED UP X TIMES DELETES TO QUICK DUE TO COPIES.

Mantenimiento de Archive Logs

Para el mantenimiento de los archive logs en las distintas bases de datos en Data Guard tendremos en cuenta los siguientes aspectos:

- Los archivers pueden ser borrados manualmente usando el comando `DELETE` si no se establece el borrado automático.
- En caso de ser necesario espacio en la Flash Recovery Area los archivers serán borrados de forma automática si no cumplen el periodo de retención o si se ya ha realizado backup a cinta de los mismos.
- Cualquier cambio estructural sucedido en la base de datos primaria requiere que se realice la resincronización del catálogo para que la base de datos standby tenga en cuenta estos cambios para futuras operaciones de restauración.
- Los archived log recibidos en la base de datos standby deberán ser catalogados manualmente en el caso de que el control file en la primaria o standby sea recreado.
- Si realizamos el backup en el entorno primario, podemos seguir usando la opción `delete input`, nuestra política se asegurará de no borrar ningún archive si no está aplicado o si no tiene backup, para la standby se recomienda dejar en local los archivos de varios días, para ello podemos usar la opción `delete archivelog until time 'SYSDATE-3';`
- Si realizamos el backup en el entorno standby, se recomienda dejar en la primaria los archivos de varios días, la política configurada nos asegurará que no borremos ningún archive no enviado o aplicado en la standby. Usaríamos `delete archivelog until time 'SYSDATE-3'`. En la standby que es donde se realizarían los backups podríamos usar la opción `delete Input`.

Restauraciones en entorno Data Guard

Tal y como se ha comentado anteriormente, únicamente los backups tomados en standbys físicas son útiles para realizar backup y restores en la base de datos primarias. Con los backups tomados en standby físicas se pueden realizar las siguientes recuperaciones:

- Recuperación ante pérdida de data file en la base de datos primaria o standby
- Recuperación ante pérdida de control file en la base de datos en standby. Si la pérdida se produce en la primaria es necesario haber realizado el backup en dicha base de datos. El control file difiere entre base de datos primaria y standby.
- Block media recovery en la base de datos primaria
- Recuperación incompleta de la base de datos primaria

Un backup incremental puede ser usado para sincronizar una base de datos standby física.

Para llevar a cabo estas operaciones en Data Guards lógicos es necesario realizar backups tanto en la instancia primaria como en las standbys.

RECOMENDACIONES DE UPGRADE Y APLICACIÓN DE PATCHES

Esta sección está dirigida tanto a usuarios que deseen realizar una nueva instalación de Oracle Data Guard, como para aquellos que ya la poseen y están pensando en implantar una estrategia proactiva de actualización de la instalación existente.

Nuevas instalaciones

La misma release de base de datos debe ser instalada en el nodo primario y en todas las bases de datos en standby que formen parte de un Data Guard. De forma excepcional pueden existir de forma concurrente diferentes versiones durante procesos de rolling upgrade haciendo uso de standbys lógicas.

Se recomienda encarecidamente que se aplique el último patchset disponible para la versión y plataforma elegida tanto para el entorno primario como el standby, ya sea físico o lógico.

Los parches recomendados para Dataguard deben siempre pasar la revisión de conflicto con restantes parches, responsables de cubrir diferentes features de Oracle, y aplicados sobre kernel o software Oracle.

También es recomendable consultar las siguientes notas de My Oracle Support:

- Patch Set Updates for Oracle Products [ID 854428.1]
- Release Schedule of Current Database Releases [ID 742060.1]
- Quick Reference to Patchset Patch Numbers [ID 753736.1]

Consideraciones de Upgrade e Instalación de Parches

En las siguientes notas, disponibles en MyOracleSupport, se puede consultar el proceso de aplicación de parches en una base de datos que posee una standby:

- Standby Física:
 - Applying Patch Sets / Interim Patches with Physical Standby Database in Place [ID 187242.1]
 - How do you apply a Patchset, PSU or CPU in a Data Guard Physical Standby configuration [ID 278641.1]
- Standby Lógica:

- Upgrading Oracle Database with a Logical Standby Database In Place [ID 437276.1]

Como buenas prácticas desde Oracle soporte se recomienda tener en cuenta los siguientes puntos:

- Antes de parchear la base de datos usando opatch chequear la disponibilidad de espacio libre y usar la documentación referenciada en la Nota How To Avoid Disk Full Issues Because OPatch Backups Take Big Amount Of Disk Space. [ID 550522.1] disponible en MyOracleSupport (<https://support.oracle.com>)
- Poner en marcha una estrategia proactiva, para fijar los últimos problemas conocidos a través de mantener actualizado el software con la aplicación de los Patch Set Updates (PSU) que son liberados de forma cuatrimestral por Oracle.
- Para reducir el downtime del entorno es posible paralelizar la aplicación del parche sobre los binarios de base de datos en todos los entornos que formen parte del Data Guard.
- En caso de ser una standby física nunca se ha de realizar operaciones de postinstalación que conlleven la ejecución de scripts sobre la instancia en standby.
- Para evitar que los errores afecten tanto a la base de datos primaria como a las standby es posible poner en diferido la aplicación de cambios en la standby hasta que se aplique completamente el parche en la primaria.
- En caso de hacer uso de Data Guard Broker para la administración del Data Guard es necesario acometer alguna de las siguientes acciones durante la aplicación de parches:
 - a. Parar el Data Guard Broker
 - b. Deshabilitar la configuración
 - c. Realizar todos los cambios de la configuración haciendo uso del Data Guard Broker

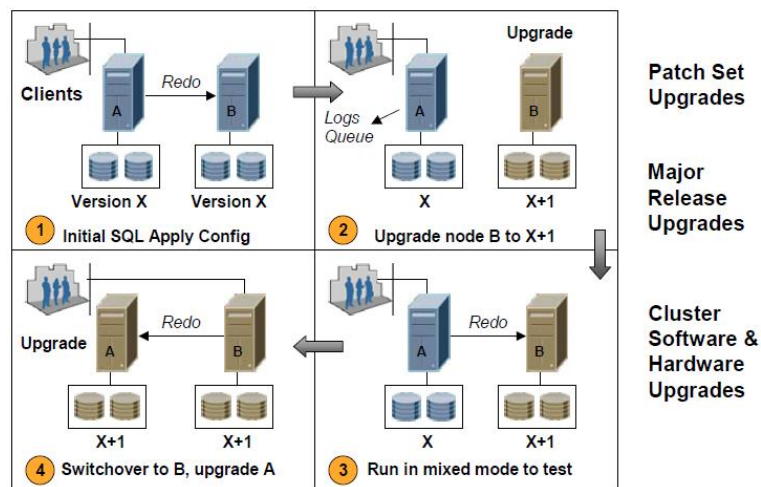
Oracle Soporte recomienda realizar la opción a o b. Esto evitará futuras inconsistencias en los ficheros de configuración de Data Guard Broker. En caso de que estas inconsistencias se lleguen a producir será necesario recrear la configuración del Data Guard Broker.

El Broker podrá ser activado una vez que ambas instancias estén sincronizadas de nuevo.

Rolling Upgrade

El concepto de Rolling Upgrade, que se podría traducir como una actualización de forma gradual del software.

A partir de Oracle Database 10g release 1 (10.1.0.3), es posible usar una base de datos standby lógica para llevar a cabo el rolling upgrade del software de una base de datos. Durante este proceso dos bases de datos de diferente versión pueden convivir en un entorno de Data Guard Lógico mientras estas se actualizan, reduciendo el tiempo de parada del entorno. Un esquema básico del proceso es el siguiente:



Para llevar a cabo este procedimiento es necesario seguir las instrucciones marcadas en los manuales de administración de Data Guard de la versión correspondiente en conjunción a los del propio parche a aplicar.

En un rolling upgrade, nos referimos a la actualización del software (Oracle Database, Oracle Clusterware, ASM o el propio sistema operativo), mientras que la instancia primaria está activa se actualiza la instancia en standby. Se restablece el envío de información, trabajando en modo mixto, y se realiza la actualización de la instancia primaria. La principal ventaja será el mínimo downtime.

Esta actualización es posible sólo para algunos parches individuales que están marcados como compatibles con rolling upgrade. Es el caso de la mayoría de bundle patch y Actualizaciones de Parches Críticos, también conocido como CPU.

Para actualizar el software haciendo uso de rolling upgrade es necesario el uso de una base de datos auxiliar de tipo Logical Standby, bien podemos usar una standby creada para tal propósito o la standby física que ya tengamos. Para realizar Rolling upgrade la standby usada en el procedimiento será temporalmente de tipo lógico y existen prerequisites que deben cumplir (Prerequisite Conditions for Creating a

Logical Standby Database,

https://docs.oracle.com/database/121/SBYDB/create_ls.htm#SBYDB4730)

Este método de actualización sólo es compatible con configuraciones en Máximo Performance o Máximo Availability.

A partir de la versión 12.1 aparece una nueva funcionalidad llamada Rolling Upgrade Using Oracle Active Data Guard, esta funcionalidad simplifica el procedimiento, pero no está disponible para los organismos de la Jda ya que Active Dataguard no se encuentra dentro del contrato corporativo.

En la versión 11GR2 si se quiere realizar un Rolling upgrade se debe desactivar el bróker. En cambio, en 12c, si se tiene configurado el bróker se debe revisar la documentación oficial, ya hay funcionalidades de Rolling upgrade que ya están integradas con el bróker. **Enhancements to Oracle Data Guard Broker 12c and Rolling Upgrades** <https://docs.oracle.com/database/122/UPGRD/enhancements-oracle-data-guard-broker-rolling-upgrades.htm#UPGRD-GUID-79BAB049-7A0D-42CA-B514-E1BB159486F6>

Se recomienda revisar las buenas prácticas de Rolling upgrade publicadas en el documento **Upgrading and Migrating to Oracle Database 12c Release 2 (12.2.0.1)** <http://www.oracle.com/technetwork/database/upgrade/overview/upgrading-oracle-database-wp-122-3403093.pdf>

Standby First Apply

Si bien Data guard nos permite usar distintas plataformas, versiones de sistemas operativos, hardware o estructura entre el entorno Primario y el Standby, hasta la aparición de la funcionalidad Standby First Apply se restringía la posibilidad de tener un distinto versionado entre ambos entornos si el Data guard era físico.

Esta funcionalidad aparece a partir de la versión 11.2 y nos va a permitir validar la aplicación de un parche en el entorno Standby minimizando así el impacto en nuestra primaria. Para realizar esta validación aplicaremos el parche en la standby y la convertiremos en snapshot standby, una vez validado procederemos a aplicarlo en la primaria.

Esta funcionalidad, también llamada “Standby-First Installable” actualmente no está disponible para todos los parches liberados, únicamente para:

- Database home interim patches
- Exadata bundle patches
- PSU

Se recomienda leer con detalle el readme del parche a aplicar para validar si es Standby-First.

Para más información se recomienda consultar la nota **Oracle Patch Assurance - Data Guard Standby-First Patch Apply (Doc ID 1265700.1)** o la documentación oficial:

<https://docs.oracle.com/database/122/SBYDB/upgrading-patching-downgrading-oracle-data-guard-configuration.htm#SBYDB-GUID-A5226768-DB6B-4714-BB9A-0A3EF17A01C8>