



Servicio Andaluz de Salud  
**CONSEJERÍA DE SALUD**

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

# *TESTING DE SISTEMAS PARA ENTORNOS ORACLE DATA GUARD*

*Referencia documento: InfV5\_JASAS\_DG\_SystemTest\_V920.doc  
Fecha: 16 de noviembre de 2018  
Versión: 9.2.0*



Certificado ISO-9002  
Nº: 20845/G

## Registro de Cambios

Fecha	Autor	Versión	Notas
1 de enero del 2010	Oracle ACS	4.1	Versión inicial
12 de enero de 2012	Oracle ACS	3.1	Revisión 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 de 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
PLANING PARA LOS TESTS DEL SISTEMA .....	7
<i>Test de Stress del sistema/Simulación de un entorno de producción.....</i>	<i>7</i>
<i>Test de fallos inducidos.....</i>	<i>8</i>
DESCRIPCIÓN DE LOS TESTS .....	9
<i>Testing del Sistema: Escenarios de paradas.....</i>	<i>10</i>
<i>Testing del Sistema: Fallos en los procesos del Data Guard .....</i>	<i>14</i>
<i>Test de componentes: Tools de diagnostico.....</i>	<i>15</i>
CONCLUSIONES Y RECOMENDACIONES .....	1

---

## Control de cambios

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

---

## Introducción

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

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.

Finalmente, este documento también recoge una serie de conceptos de componentes, módulos y tecnologías relacionadas con *Oracle RDBMS 12c* y *Data Guard (DG) 12c* que pueden ayudar en la realización de una configuración óptima para los entornos de Jda.

---

## Objetivos de este documento

Antes de que una nueva máquina/base de datos en standby entre en funcionamiento en producción, es importante que se pruebe el sistema en profundidad para verificar que el comportamiento será el esperado. También es recomendable el testeo cuando se introducen cambios en el sistema, ya sean grandes o pequeños.

El objetivo de este documento es doble. En primer lugar, proporcionar una guía de pruebas para testear las respuestas de un entorno activo-pasivo con Oracle Data Guard 12c antes de pasar a producción, entre lo que se destaca:

- Verificación de la red que soportara la comunicación entre bases de datos primarias y en standby.
- Verificar que el sistema ha sido correctamente instalado y configurado.
- Asegurar que el sistema sea capaz de alcanzar los objetivos esperados, particularmente de disponibilidad y rendimiento.

En segundo lugar, este documento puede servir como plantilla para realizar dichas pruebas y anotar los resultados obtenidos, verificando así la respuesta del sistema ante posibles fallos.

La configuración del sistema y procedimientos operacionales, deben también ser testeados para asegurar que los fallos de sus componentes y otros problemas pueden ser tratados de la manera más eficiente y con el menor impacto posible.

El propósito de este test es probar la robustez del sistema ante los distintos fallos.

Se recomienda que las pruebas sean ejecutadas bajo una carga de trabajo que simule al de un entorno de producción real, y en exclusividad de otras pruebas para poder medir eficientemente los resultados obtenidos.

---

## Planing para los tests del sistema

Las pruebas de testing del sistema requieren una planificación cuidadosa para que sean efectivas. Los objetivos de nivel de servicio para el sistema en sí mismo y para la prueba deben quedar claros y un plan detallado de las pruebas debe ser documentado. La base para todas las pruebas es que las best-practices actuales para la configuración del sistema en Oracle DG han sido llevadas a cabo antes de la prueba.

Las pruebas deben realizarse en un entorno que refleje el entorno de producción tanto como sea posible, lo ideal sería realizarlo en el mismo antes de la puesta en producción. La configuración de software debe ser idéntica, pero por razones de coste, podría ser necesario utilizar una configuración de hardware reducida en algunas ocasiones. Todas las pruebas serán realizadas durante la ejecución de una prueba de carga de trabajo lo más cercana a la producción como sea posible. Al planificar las pruebas del sistema es sumamente importante para entender cómo la aplicación ha sido diseñada para manejar los fallos descritos en este plan y asegurar que los resultados previstos se ajustan al nivel de alta disponibilidad que soporta la aplicación, así como al nivel de alta disponibilidad de la base de datos.

Generar una realista carga de trabajo de aplicación puede ser complejo y costoso, pero es el factor más importante para la eficacia de las pruebas. Para cada prueba individual del plan, se requiere:

- ¿Cuál es el objetivo de la prueba y cómo se relaciona este con los objetivos del sistema en general?
- Exactamente, ¿cómo se realiza la prueba y cuáles son los pasos de ejecución?
- ¿Cuáles son los criterios de éxito o fracaso, y cuáles son los resultados esperados?
- ¿Cómo se medirá el resultado de la prueba?
- ¿Qué herramientas se utilizarán?
- ¿Qué datos serán recogidos y cuáles son los ficheros de logs a revisar?
- ¿Qué procedimientos operativos son relevantes?

---

## Test de Stress del sistema/Simulación de un entorno de producción

La mejor manera de garantizar que el sistema funcionará bien sin ningún tipo de problemas es simular la carga de trabajo de producción y las condiciones de trabajo antes de publicarlo. Lo ideal sería que el sistema debe ser estresado en algo más de lo que se espera en la producción. Además de ejecutar la carga de trabajo de aplicación, todos los

procedimientos operativos normales también deben ser examinados al mismo tiempo, como procedimientos de ejecución periódica. El resultado de las pruebas se debe mantener y ser comparado con los datos reales cuando se realice la puesta en producción. Las operaciones normales de mantenimiento, como agregar usuarios, añadir espacio en disco, la reorganización de tablas e índices, copias de seguridad, el archivado de datos, etc. También se deben probar.

---

## Test de fallos inducidos

La configuración del sistema y los procedimientos operativos deben ser evaluados para asegurarse de que los fallos de componentes y otros problemas pueden ser tratados con la mayor eficacia posible y con el mínimo impacto sobre la disponibilidad del sistema. Esta sección proporciona algunos ejemplos de las pruebas que se pueden utilizar como parte de un plan de pruebas del sistema. La idea es poner a prueba la robustez del sistema frente a diferentes fallos.

Esta lista sólo incluye las pruebas para los componentes de DG. Se deberían realizar pruebas adicionales para dar por validado el sistema de forma completa, pero se salen del objetivo de este documento.

En algunos escenarios de fallo podría no ser posible recuperar el sistema dentro de un marco de tiempo aceptable y un plan de failover debe especificarse para cambiar a un sistema alternativo o a una ubicación alternativa. Esto también puede ser probado.

---

## Descripción de los Tests

En los siguientes apartados se describen las baterías de pruebas a realizar sobre el entorno. Se debe tener en cuenta que estas pruebas están orientadas tanto a entorno RAC como single instance en activo-pasivo, por lo que se debe aplicar lo que corresponda dependiendo del tipo de entorno que se esté probando.

Se incluye en las pruebas la opción de que el entorno tenga configurado el Fast Start Failover a través de un proceso Observer, aunque la configuración del Observer está desaconsejada para los entornos de la Junta de Andalucía.

Los test se han clasificado en diferentes apartados atendiendo, bien a la funcionalidad que comprueban, bien al componente que interviene. Los apartados en los que se han clasificado los test son los siguientes:

Grupo de Test	Descripción
Testing del Sistema: Escenarios de paradas	Este grupo de tests define una serie de escenarios de desastre que determinan un tipo de test a realizar. Se deben realizar los test que sean aplicables al entorno que se quiere validar, ya que no siempre los escenarios que se presentan son los que pueden ocurrir en el entorno, por las características del propio CPD, máquinas, etc.
Testing del Sistema: Fallos en los procesos del Data Guard	Este grupo de test se refiere a posibles fallos en los procesos del Data Guard.
Test de componentes: Tools de diagnostico	Pruebas de que los scripts de diagnóstico se ejecutan correctamente

## Testing del Sistema: Escenarios de paradas

Test ID	Descripción	Procedimiento	Resultados esperados	Medidas	Resultados obtenidos/ Notas
Test 1	Reinicio controlado de la instancia primaria sin Fast Start Failover (FSF) configurado y con/sin Client Failover (CF) configurado	<ul style="list-style-type: none"> <li>• Iniciar la carga de trabajo</li> <li>• Reiniciar la instancia primaria:               <ul style="list-style-type: none"> <li>○ SQL&gt; shutdown immediate</li> <li>○ SQL&gt; startup</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• La instancia primaria dejará de dar servicio.</li> <li>• La instancia en standby dejará de recibir cambios desde la primaria.</li> <li>• Los clientes conectados a la instancia primaria perderán la conexión a la misma.</li> <li>• Los clientes conectados a la instancia en standby o procesos lanzados en la misma no perderán la conexión, pero consultarán datos no actualizados si está en RO</li> <li>• Tras el reinicio de la instancia ésta seguirá siendo la primaria en la configuración.</li> <li>• Los clientes podrán conectarse normalmente a la instancia.</li> <li>• La instancia en standby volverá a recibir cambios de la primaria</li> </ul>	<ul style="list-style-type: none"> <li>• Tiempo para completar la recuperación de la instancia.</li> <li>• Tiempo para restaurar la actividad de los clientes al mismo nivel.</li> <li>• Tiempo empleado en la sincronización de ambas instancias.</li> </ul>	
Test 2	Reinicio controlado de la instancia primaria con FSF configurado y con /sin CF configurado	<ul style="list-style-type: none"> <li>• Iniciar la carga de trabajo</li> <li>• Reiniciar la instancia primaria:               <ul style="list-style-type: none"> <li>○ SQL&gt; shutdown immediate</li> <li>○ SQL&gt; startup</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Ocurrirá lo mismo que en el Test 1 ya que la parada controlada no será condición de inicio de Failover.</li> </ul>	<ul style="list-style-type: none"> <li>• Tiempo para completar la recuperación de la instancia.</li> <li>• Tiempo para restaurar la actividad de los clientes al mismo nivel</li> <li>• Tiempo empleado en la sincronización de ambas instancias.</li> </ul>	

Test 3	Reinicio no controlado de la instancia primaria con FSF configurado y sin CF configurado	<ul style="list-style-type: none"> <li>• Iniciar la carga de trabajo</li> <li>• Reiniciar el nodo en el que se encuentre la instancia primaria             <ul style="list-style-type: none"> <li>○ Para Solaris: 'reboot'</li> </ul> </li> <li>• O parar la instancia primaria de forma abrupta:             <ul style="list-style-type: none"> <li>○ SQL&gt; shutdown abort</li> <li>○ SQL&gt; startup</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• La instancia primaria dejará de dar servicio.</li> <li>• Si el timeout del Observer no es alcanzado el resultado esperado es el indicado en el Test 1.</li> <li>• Si el timeout del Observer es alcanzado se iniciará el failover a la instancia en standby designada.</li> <li>• Los clientes perderán la conexión a la instancia primaria.</li> <li>• Los clientes deberán ser reconfigurados para acceder a la nueva instancia primaria.</li> <li>• Cuando se reestablezca la primaria inicial se necesitará reconfiguración manual de clientes.</li> </ul>	<ul style="list-style-type: none"> <li>• Tiempo para la detección del fallo del nodo o de la instancia</li> <li>• Tiempo para completar la recuperación de la instancia.</li> <li>• Tiempo para restaurar la actividad de los clientes al mismo nivel</li> <li>• Tiempo empleado en la vuelta al estado original si es posible.</li> <li>• Tiempo en reconfiguración de clientes.</li> </ul>	
Test 4	Reinicio no controlado de la instancia primaria con FSF configurado y con CF configurado	<ul style="list-style-type: none"> <li>• Iniciar la carga de trabajo</li> <li>• Reiniciar el nodo en el que se encuentre la instancia primaria             <ul style="list-style-type: none"> <li>○ Para Solaris: 'reboot'</li> </ul> </li> <li>• O parar la instancia primaria de forma abrupta:             <ul style="list-style-type: none"> <li>○ SQL&gt; shutdown abort</li> <li>○ SQL&gt; startup</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• La instancia primaria dejará de dar servicio.</li> <li>• Si el timeout del Observer no es alcanzado el resultado esperado es el indicado en el Test 1.</li> <li>• Si el timeout del Observer es alcanzado se iniciará el failover a la instancia en standby designada.</li> <li>• Los clientes perderán la conexión a la instancia primaria.</li> <li>• Los clientes podrán conectarse a la instancia en standby a la que se ha hecho failover sin reconfiguración manual.</li> <li>• Cuando se reestablezca la primaria inicial no se necesitará reconfiguración de clientes.</li> </ul>	<ul style="list-style-type: none"> <li>• Tiempo para la detección del fallo del nodo o de la instancia</li> <li>• Tiempo para completar la recuperación de la instancia.</li> <li>• Tiempo para restaurar la actividad de los clientes al mismo nivel</li> <li>• Tiempo empleado en la vuelta al estado original si es posible.</li> </ul>	
Test 5	Reinicio no controlado de la instancia primaria sin FSF configurado y con/sin CF configurado	<ul style="list-style-type: none"> <li>• Iniciar la carga de trabajo</li> <li>• Reiniciar el nodo en el que se encuentre la instancia primaria             <ul style="list-style-type: none"> <li>○ Para Solaris: 'reboot'</li> </ul> </li> <li>• O parar la instancia primaria de forma abrupta:             <ul style="list-style-type: none"> <li>○ SQL&gt; shutdown abort</li> <li>○ SQL&gt; startup</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Ocurrirá lo mismo que en el Test 1.</li> </ul>	<ul style="list-style-type: none"> <li>• Tiempo para la detección del fallo del nodo o de la instancia</li> <li>• Tiempo para completar la recuperación de la instancia.</li> <li>• Tiempo para restaurar la actividad de los clientes al mismo nivel</li> </ul>	



Test 6	Reinicio controlado o no del nodo secundario con/sin FSF configurado y con/sin CF configurado	<ul style="list-style-type: none"> <li>• Iniciar la carga de trabajo en la primaria.</li> <li>• Reiniciar la base de datos en standby             <ul style="list-style-type: none"> <li>○ SQL&gt; shutdown immediate</li> <li>○ SQL&gt; startup</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• La instancia primaria seguirá dando servicio.</li> <li>• Los procesos y usuarios conectados a la instancia en standby perderán la conexión.</li> <li>• El nodo en standby dejará de estar sincronizado.</li> <li>• Errores de pérdida de conexión con la standby aparecerán en el alert.log de la instancia primaria.</li> </ul>	<ul style="list-style-type: none"> <li>• Tiempo para la detección del fallo del nodo o de la instancia</li> <li>• Tiempo para completar la recuperación de la instancia en standby.</li> <li>• Tiempo para restaurar la actividad de los clientes al mismo nivel</li> <li>• Tiempo empleado en la sincronización de ambas instancias.</li> </ul>	
Test 7	Fallo del Listener en la standby	<ul style="list-style-type: none"> <li>• Para Solaris:             <ul style="list-style-type: none"> <li>○ Obtener el PID para el listener proceso: # ps -ef   grep tnlsnr</li> <li>○ Kill del proceso del listener: # kill -9 &lt;listener pid&gt;</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Si la conexión con la primaria había sido establecida             <ul style="list-style-type: none"> <li>○ no impacta en la comunicación entre las instancias.</li> </ul> </li> <li>• Si la conexión con la primaria no había sido establecida             <ul style="list-style-type: none"> <li>○ no se recibirán cambios en la standby.</li> <li>○ El proceso NSS/NSA realizará tantos intentos de reenvío como tenga establecido en la configuración del destino.</li> <li>○ Los errores de conexión aparecerán en el alert.log de la instancia.</li> <li>○ En caso de estar configurada en el modo de protección Maximum Protection la base de datos primaria realizará una parada abrupta.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Tiempo para detectar el fallo del listener y reiniciarlo.</li> </ul>	



Test 8	Fallo de la Red entre ambas instancias	<ul style="list-style-type: none"> <li>• Desconectar todos los cables de red de la interfaz de la red publica.</li> </ul> <p><b>Nota:</b> No se recomienda usar ifconfig para parar la interfaz de red.</p>	<ul style="list-style-type: none"> <li>• No se recibirán cambios en la standby.</li> <li>• El proceso NSS/NSA realizará tantos intentos de reenvío como tenga establecido en la configuración del destino.</li> <li>• Los errores de conexión aparecerán en el alert.log de la instancia.</li> <li>• En caso de estar configurada en el modo de protección Máximum Protection la base de datos primaria realizará una parada abrupta.</li> </ul>	<ul style="list-style-type: none"> <li>• Tiempo para detectar el fallo de la red.</li> </ul>	
--------	--	---	--	--	--



## Testing del Sistema: Fallos en los procesos del Data Guard

Test ID	Descripción	Procedimiento	Resultados esperados	Medidas	Resultados obtenidos /Notas
Test 9	Fallo del proceso: NSS/NSA en la primaria	<ul style="list-style-type: none"> <li>Para Solaris:               <ul style="list-style-type: none"> <li>Obtener el PID del proceso: # ps -ef   grep</li> <li>Matar al proceso NSS/NSA: # kill -9 &lt;process pid&gt;</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Los cambios no serán enviados a la standby.</li> <li>El LGWR en la primaria dejará de funcionar en caso de estar configurado en modo síncrono.</li> <li>El proceso será reiniciado automáticamente por la instancia.</li> <li>Los errores se pueden consultar en el alert.log de la instancia</li> </ul>	<ul style="list-style-type: none"> <li>Tiempo para reiniciar el proceso NSS/NSA.</li> <li>En caso de ser comunicación síncrona, el tiempo de parada del LGWR.</li> </ul>	
Test 10	Fallo del proceso: RFS en la standby	<ul style="list-style-type: none"> <li>Para Solaris:               <ul style="list-style-type: none"> <li>Obtener el PID para el proceso RFS: # ps -ef   grep rfs</li> <li>Matar al proceso RFS: # kill -9 &lt;rfs pid&gt;</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Se dejarán de recibir cambios en la standby.</li> <li>El proceso será reiniciado automáticamente por la instancia.</li> <li>Los errores se pueden consultar en el alert.log de la instancia</li> </ul>	<ul style="list-style-type: none"> <li>Tiempo para reiniciar el proceso RFS.</li> </ul>	
Test 11	Parada del proceso: MRP en la standby física	<ul style="list-style-type: none"> <li>Parada manual usando el comando: SQL&gt; ALTER DATABASE RECOVER MANAGED STANDBY DATABASE CANCEL;</li> </ul>	<ul style="list-style-type: none"> <li>Se dejarán de aplicar los cambios provenientes de la primaria.</li> <li>La parada aparecerá recogida en el alert.log de la instancia en standby.</li> </ul>	<ul style="list-style-type: none"> <li>Tiempo para reiniciar el proceso MRP.</li> <li>Se ha de reiniciar la aplicación de cambios con el comando: SQL&gt; ALTER DATABASE RECOVER MANAGED STANDBY DATABASE DISCONNECT;</li> </ul>	

Test ID	Descripción	Procedimiento	Resultados esperados	Medidas	Resultados obtenidos /Notas
Test 12	Parada del proceso: LSP en la standby lógica	<ul style="list-style-type: none"> <li>Parada manual usando el comando:            SQL&gt; ALTER DATABASE START LOGICAL STANDBY APPLY;</li> </ul>	<ul style="list-style-type: none"> <li>Se dejarán de aplicar los cambios provenientes de la primaria.</li> <li>La parada aparecerá recogida en el alert.log de la instancia en standby.</li> </ul>	<ul style="list-style-type: none"> <li>Tiempo para iniciar el proceso LSP.</li> <li>Se ha de reiniciar la aplicación de cambios con el comando:            SQL&gt; ALTER DATABASE STOP LOGICAL STANDBY APPLY;</li> </ul>	

## Test de componentes: Tools de diagnóstico

Test ID	Descripción	Procedimiento	Resultados esperados	Medidas	Resultados obtenidos/Notas
Test 13	Procedimientos de diagnóstico	<ul style="list-style-type: none"> <li>Iniciar la carga de trabajo</li> <li>Ejecutar los procedimientos para recopilar la información de diagnóstico en primaria y standbys.</li> </ul>	<ul style="list-style-type: none"> <li>Los scripts de diagnóstico se han ejecutado correctamente.</li> <li>El tiempo de ejecución de estos scripts es aceptable.</li> </ul>		



---

## Conclusiones y Recomendaciones

La batería de test propuestos puede no aplicar a un sistema concreto, o haberse probado ya con anterioridad, por lo que se deben definir las pruebas de verificación de un sistema en conjunto entre los DBAs y Sistemas de forma que los escenarios que se prueben se correspondan con la realidad de los entornos.

