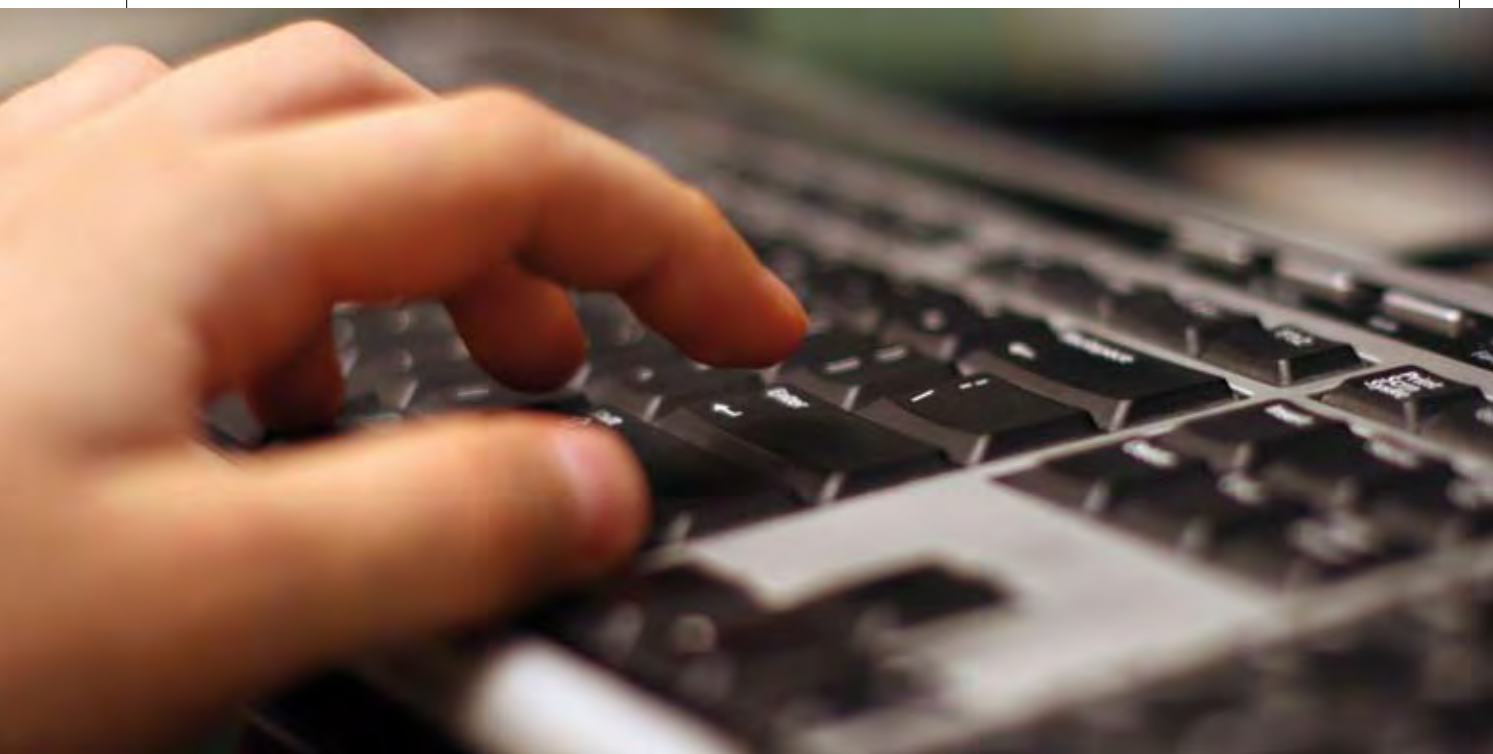


Administración electrónica 24x7 para los aplicativos orientados al ciudadano

POR LYDIA LÓPEZ SÁNCHEZ Y ANTONIO PIQUERO

Prestar el mejor servicio al ciudadano es el motivo de las reformas que, tras la aprobación de la Constitución, se han ido realizando en España para configurar una Administración moderna, que haga del principio de eficacia y eficiencia su eje vertebrador, siempre con la mira puesta en los ciudadanos." La Exposición de motivos de la Ley 11/2007, de Acceso electrónico de los ciudadanos a los servicios públicos, marca el horizonte de trabajo que los profesionales TIC de la Administración debemos fijarnos como meta.



El reciente desarrollo normativo en materia de trámites administrativos se encamina hacia una Administración más sencilla y cercana al ciudadano, en donde los procedimientos sean eficaces, puedan realizarse por diversidad de canales, eviten trámites innecesarios y, punto fundamental en lo que respecta a este proyecto, estén disponibles a cualquier hora. En otras palabras, debe ser la Administración la que tienda a adaptarse al ciudadano, frente al enfoque tradicional en el que se le obligaba al ciudadano a ajustarse a la rigidez burocrática.

Así pues, las diversas Administraciones están realizando un notable esfuerzo a la hora de proveer servicios que cumplan con los principios de eficacia, eficiencia y simplificación en todo momento y en todo lugar. En este contexto, los Sistemas de Verificación de Datos de Residencia y Datos de Identidad (SVDR/I, en adelante) aparecen como elemento clave en la simplificación de trámites administrativos.

Nos corresponde a los departamentos de Sistemas complementar y respaldar con la infraestructura adecuada este tipo de proyectos. En esta línea se enmarca el proyecto presente, que proporciona alta disponibilidad a sistemas definidos como 24x7 mediante una infraestructura repartida en dos CPD con configuración activo-activo en todas sus capas. Para lograr esta alta disponibilidad, la capa de datos suponía un auténtico desafío, que finalmente fue resuelto mediante la implantación de un cluster extendido geográficamente basado en las tecnologías de Oracle RAC.

El proyecto de Centro de Respaldo

El proyecto de puesta en marcha del

centro de respaldo de S.A.R.A. se inició en 2007 con el objetivo de asegurar el funcionamiento de las aplicaciones de gestión de los Recursos Humanos, servicios comunes de Administración Electrónica y servicios básicos del Centro de Servicios Comunes (CSC) de la Red SARA, responsabilidad de la Dirección General de Modernización Administrativa del Ministerio de Administraciones Públicas (actual Dirección General para el Impulso de la Administración Electrónica del Ministerio de la Presidencia).

Inicialmente se concibió con una configuración activo-pasivo, con réplica síncrona de los datos mediante las utilidades de replicación de las cabinas de almacenamiento y conmutación entre centros en base a modificación de los registros de DNS.

Una vez alcanzado este objetivo, se decidió ir más allá: alcanzar una arquitectura que garantizara una disponibilidad 24x7 para aquellos aplicativos orientados al servicio al ciudadano (SVDR/I inicialmente). Ello, sin perder de vista otros objetivos no menos importantes tales como asegurar la escalabilidad del sistema y su continua evolución (IaaS), al tiempo que racionalizar recursos a partir de tres principios: ahorro energético, facilidad de administración y minimización del número de recursos ociosos.

En esta línea, en proyecto conjunto con el Departamento de Comunicaciones (responsable de la Red SARA), se realiza extensión de VLANs entre ambos centros con el objetivo de que los recursos pertenecientes a una misma capa puedan comunicarse entre sí con independencia de su ubicación geográfica. Además, se diseña una arquitectura en tres capas (acceso, aplicación y

datos) para garantizar la seguridad de cada entorno. El acceso a los servicios se realiza a través de SARA de forma balanceada e indistinta entre uno y otro CPD.

En la capa de servidores de aplicaciones, encontramos un diseño basado en arquitecturas web, con aplicativos desplegados sobre Apache Tomcat que, básicamente, proveen y consumen servicios web. Este diseño facilita enormemente la distribución de los elementos en sitios dispersos geográficamente, permite plenamente la configuración activa-activa y el balanceo y simplifica la escalabilidad.

Aprovechando estas circunstancias, para proveer la infraestructura se plantea una arquitectura virtualizada que, además de permitir la consolidación de servidores en busca de la eficiencia energética y el ahorro de recursos, proporcione una plena flexibilidad en el despliegue de nueva infraestructura. Originariamente, el sistema SVDR/I que se implantó en el CPD principal corría sobre servidores virtualizados con la tecnología de *zoning* de Solaris 10. Por esta razón, el despliegue del resto de servidores en el segundo CPD se realizó con la misma tecnología. No obstante, se está trabajando en una nueva infraestructura de virtualización basada en tecnologías VMWare. Desde el punto de vista del aplicativo, ambas infraestructuras son equivalentes y la migración de una a otra es sencilla y transparente.

Finalmente, el auténtico *tour de force* a la hora de proveer una configuración puramente activo-activo, que permitiera garantizar un servicio 24x7, lo encontramos en la capa de datos.



Oracle Rac y el Activo-Activo

Si para la capa de servidores de aplicaciones los problemas de *failover* y balanceo de carga están ampliamente resueltos gracias a las arquitecturas web y las granjas de servidores, el panorama cambia sensiblemente cuando hablamos de la capa de datos, donde la eliminación de todos los puntos únicos de fallo aparecía, hasta hace poco, como una barrera insalvable.

La evolución en este campo ha tendido siempre a tratar de evitar ese punto único de fallo, buscando

la redundancia de cada uno de los elementos implicados en el servicio (agrupamiento de interfaces de red, uso de almacenamiento externo con configuraciones RAID, tecnología *multipath* en el acceso al mismo, etc.). En esta línea, el paso de bases de datos *standalone* a configuraciones en cluster venía a eliminar el servidor como punto único de fallo de la base de datos.

Pero para lograr una alta disponibilidad con garantías quedaba aún un punto único de fallo: el CPD completo y, más concretamente, la cabi-

na de discos donde residen los datos. En efecto, un problema grave en la cabina o una interrupción eléctrica en el CPD donde residían los datos conllevaba irremediablemente una caída del servicio, haciendo que toda la infraestructura del CPD no afectado resultara inservible al perder el acceso a los datos.

Las soluciones que se nos plantearon a la hora de respaldar la capa de datos comprendían tres alternativas:

* *Réplica síncrona basada en cabina (disk array mirroring)*. Bajo esta solución, se instala una base de datos de respaldo inactiva donde los datos son replicados síncronamente por las cabinas. La gran ventaja es la facilidad de implementación. Sin embargo, supone asumir un tiempo medio-alto de caída en caso de pérdida de la cabina, obliga a una infrautilización de recursos y, en caso de contingencia brusca, se produce una pérdida de datos no consolidados en disco. Esta es la solución por la que se optó en el primer proyecto de respaldo.

* *Oracle Datagard*. Este producto de Oracle requiere tener una infraestructura de base de datos paralela a la de producción, si bien puede ser inferior en recursos. En este caso, cada transacción de la base de datos se va replicando automáticamente mediante el software de Oracle en la base de datos de Datagard. En caso de contingencia, esta segunda base de datos podría actuar como base de datos principal, si bien requiere una serie de procedimientos manuales para su puesta en producción. La ventaja frente al anterior es que, al ser el mismo software de Oracle el que gestiona la réplica, la pérdida de datos no consolidados en caso de contingencia se ve muy disminuida. No obstante, seguimos teniendo que asumir un cierto tiempo de caída y

una infrautilización de recursos, si bien es cierto que las últimas versiones de Datagard permiten tener la base de datos de respaldo levantada en modo de sólo lectura.

* *Cluster extendido con Oracle RAC.* Con el desarrollo del ASM (Automatic Storage Management), Oracle comienza a ofrecer la posibilidad de implementar clusters de base de datos extendidos geográficamente. Se trata de distribuir en dos Centros de Proceso de Datos los servidores para configurar, con todos ellos, una única base de datos que permanecería plenamente operativa incluso en el caso de caída total de uno de los dos CPDs. No hay pérdida de servicio por contingencia ni, por tanto, pérdida de datos. El inconveniente, evidentemente, es que al tratarse de una tecnología bastante novedosa, la complejidad de implantación es grande y requiere un proceso minucioso de ajuste de toda la configuración para alcanzar toda su funcionalidad en cualquier circunstancia. Además, existe un límite máximo de distancia entre CPDs y es necesario un enlace de fibra oscura entre ambos.

En nuestro caso, el Centro de Proceso de Datos secundario (concepto que deja de tener sentido en esta configuración) está ubicado relativamente cerca del principal, a unos dos kilómetros aproximadamente, y el enlace de fibra ya estaba contemplado en el proyecto inicial de centro de respaldo. Además, esta tercera solución nos permitía cumplir con el exigente RTO de 15 minutos que se había marcado inicialmente.

Se abordó, por tanto, la instalación de un cluster extendido Oracle RAC entre ambos CPDs para resolver el problema de alta disponibilidad en la capa de datos. El cluster se compone de cuatro servidores cuyo almacena-

miento reside en dos cabinas de discos. En cada CPD se ubican una de las cabinas y dos de los servidores. Como características generales de este tipo de clusters, podemos destacar:

* Cada uno de los nodos tiene visibilidad de todos los dispositivos de almacenamiento que le presentan las dos cabinas. Para evitar el punto de fallo, los nodos tienen tarjetas de fibra redundadas y ven ambas cabinas por dos caminos diferentes.

* Existe una capa de software, Oracle ASM (Automatic Storage Management), que gestiona el almacenamiento de forma que todos los nodos ven los discos que les presentan las cabinas como un único pool de almacenamiento.

* Los nodos se comunican entre sí mediante una red privada (red de interconnect) con un ancho de banda inicial de 1 Gbit. A través de esta red intercambian información de lo que está haciendo cada nodo y realizan una fusión de cachés (todos los nodos comparten la caché), que es lo que permite que la caída de uno de ellos sea transparente para la sesión del usuario.

* Todas las interfaces de red, tanto las del *interconnect* como las de la red de servicio, deben estar redundadas (mediante bonding en Linux, IPMP en Solaris, etc.) para evitar que constituyan un punto único de fallo.

* Otra capa de software por debajo de ASM, Oracle Clusterware, gestiona todos los recursos del cluster, mantiene al nodo dentro del grupo y proporciona a ASM los recursos necesarios para su funcionamiento.

* Toda la información de estado del cluster se ubica en un dispositivo denominado *voting disk*. Para evitar que éste constituya un punto de fallo, Oracle recomienda mantener tres *voting disk*, uno en cada cabina y un

tercero en un servidor ubicado en un tercer CPD al que, en este caso, accederán los nodos mediante NFS.

Esta arquitectura supone un aprovechamiento total de los recursos, está completamente redundada y carece de punto único de fallo. Además, es completamente escalable puesto que la adición de nuevos servidores de aplicaciones o de nuevos nodos al cluster de base de datos es sencilla y puede realizarse sin pérdida alguna de servicio.

La instalación se llevó a cabo por un equipo de trabajo constituido tanto por personal externo como interno, puesto que la complejidad de este tipo de infraestructura requiere la existencia de personal altamente formado en esta tecnología dentro de la organización.

Tras diversos procesos de ajustes de configuración y parcheados, las últimas pruebas realizadas han mostrado que, al apagar completamente uno de los dos CPDs, el servicio continúa prestándose con normalidad. Por tanto, la infraestructura provista conjuntamente por los departamentos de Sistemas y Comunicaciones de la División de Proyectos de Administración Electrónica ofrece una plataforma escalable, preparada para proporcionar altísima disponibilidad, de forma rápida y sin excesivos costes de migración a cualquier aplicativo de servicio al ciudadano que responda a un diseño de arquitectura web. 🍷

Lydia López
Jefa de Servicio de Sistemas
Antonio Piquero
Jefe de Área de Sistemas
D. G. para el Impulso de
la Administración
Electrónica
Ministerio de la Presidencia