

Administración 24x7. Centros de Proceso de Datos para contingencia y continuidad de negocio.

Introducción

Con el auge de las nuevas tecnologías las ventanillas con horarios rígidos empiezan a desaparecer. Los desplazamientos físicos para realizar gestiones son innecesarios y nos hacen perder tiempo. Los entornos en los que tradicionalmente existían las esperas y las colas se han agilizado de tal manera que no tengamos que esperar y podamos realizar la mayor parte de gestiones desde casa.

La administración tiene que seguir estos pasos y estar abierta al ciudadano en todo momento. Para que todos estos servicios se puedan ofrecer es necesario unas infraestructuras de Tecnologías de la Información que permitan un funcionamiento ininterrumpido veinticuatro horas al día los trescientos sesenta y cinco días del año.

Con esta comunicación pretendemos dar una visión global de cómo se ha abordado este problema desde la Subdirección General de Informática y Comunicaciones del MAPA configurando un modelo de CPD's de producción y respaldo controlados remotamente en la medida de lo posible y preparados para dar diversos niveles de disponibilidad y recuperación ante desastres desde el tradicional backup a cinta a sistemas con cero paradas.

Configuración del CPD

La infraestructura de sistemas y comunicaciones del Ministerio de Agricultura, Pesca y Alimentación está formada por dos centros de

procesos de datos entre los que se reparten los aplicativos. Uno de estos centros alberga la mayor parte de la producción y el otro actúa como respaldo. No obstante, la configuración actual permite utilizar los dos en modo activo - activo, consiguiendo un mayor aprovechamiento de las inversiones realizadas en equipamiento al permitir el reparto de la producción entre los dos centros.

En el CPD principal está ubicada la mayor parte del equipamiento informático del MAPA. Es la sede de todos los equipos que no cuentan con respaldo en el otro centro y es donde residen las conexiones troncales de la red.

Este centro está dotado de un grupo electrógeno para mantener los equipos en funcionamiento en caso de fallo del suministro eléctrico, a su vez todos los equipos informáticos están alimentados por dos cuadros eléctricos independientes.

El disponer de dos cuadros eléctricos permite conectar los equipos con fuentes de alimentación redundantes a cada cuadro, permitiendo la desconexión de uno de los cuadros para tareas puntuales de mantenimiento manteniendo los equipos en funcionamiento.

Así mismo el acceso al CPD está controlado por tarjeta magnética que permite el registro de los accesos realizados al mismo.

También es muy importante la refrigeración en las salas de servidores del CPD. Los equipos informáticos deben mantenerse a una temperatura entre 20 y 25 grados. El CPD dispone de tres equipos de aire acondicionado que rotan semanalmente manteniendo dos en funcionamiento y un tercer equipo de reserva por si alguno de los activos fallara.

La rotación de equipos se realiza automáticamente para que todos tengan periodos de actividad.

Uno de los problemas que tarde o temprano aparece en los CPD's es la falta de espacio y el aumento de consumo eléctrico según van creciendo el número de equipos necesarios. Para solucionar este problema desde el MAPA se ha optado por dos estrategias: La primera consiste en el uso de servidores tipo blade. Estos servidores mucho más pequeños que los tradicionales permiten aumentar el aprovechamiento de los armarios hasta en una relación de 1:1,5. La otra estrategia seguida para la reducción del espacio físico es la virtualización de servidores. La virtualización nos permite configurar varios servidores virtuales dentro de un mismo servidor físico manteniendo estos servidores virtuales independientes unos de otros. Con esto conseguimos un mayor aprovechamiento de los servidores físicos ya que aumentamos el porcentaje de utilización medio de un servidor desde un 20 o 30 por ciento hasta un 80 por ciento. Con lo que aprovechamos mucho mejor nuestra infraestructura. La configuración de servidores virtuales nos da además otra serie de ventajas para la alta disponibilidad que no tendríamos en el caso de utilizar servidores físicos.

Todos los equipos eléctricos, de refrigeración y control de accesos están controlados por una aplicación de gestión de alarmas que notifica a los operadores del CDP de forma visual, sonora y mensajería SMS de las incidencias operativas y alarmas que se produzcan en el CPD.

El CPD de respaldo de MAPA aunque de un tamaño más reducido tiene una configuración parecida al CPD principal. También dispone de grupo electrógeno y dobles cuadros eléctricos para aprovechar las fuentes de alimentación redundantes de los equipos. Los equipos de refrigeración tienen un esquema de rotación similar al del CPD principal y el sistema de alarmas está conectado con el personal de seguridad del edificio y con el sistema de alarmas ubicado en el CPD principal permitiendo su control remoto.

Los servidores de ambos CPD's tienen disponible una consola remota que permite su administración desde fuera de los CPD's. La funcionalidad de esta consola es similar a estar sentado delante del servidor con un teclado y una pantalla conectados a él. Permite también conectar unidades de cdrom remotas para instalar software. Gracias a esta funcionalidad y a que el programa de gestión de alarmas físicas es accesible a través de web, el CPD puede ser administrado y monitorizado desde cualquier puesto informático del ministerio teniendo los privilegios y la conectividad de red necesarias.

Conectividad entre CPD's

Ambos CPD's están conectados mediante varias mangueras de fibra óptica. Estas fibras soportan las conexiones tanto de redes SAN como LAN entre los dos CPD's.

Los dos CPD's están conectados a través de una conexión Ethernet a 10Gbps con los equipos troncales situados en el CPD principal. En cuanto a la red SAN se encuentran configuradas dos fabric extendidas por ISL además de disponer de una conexión dedicada para la replicación de las dos cabinas de almacenamiento Symmetrix.

Configuraciones normalizadas de los CPD's

Con el tiempo y debido a las distintas ampliaciones de equipos, el cableado y la distribución de equipos en el CPD se ha vuelto demasiado compleja. Los diferentes armarios tenían muchos cables que iban desde los servidores al falso suelo (corriente, red de datos, fibra, consolas) Esto impedía mover con facilidad armarios y que el número de cables que discurrían por el falso suelo fuera considerable. Para mejorar este aspecto se decidió estandarizar la configuración de los armarios de servidores de los CPS's con el objetivo de minimizar los cables que salen del armario hasta el falso suelo.

Para ello se ha configurado como enchufe normalizado del CPD las tomas cetac de 32 A distribuyéndose por el falso suelo cuatro tomas por cada armario conectados dos a cada cuadro eléctrico. A las tomas del suelo estarán conectadas las PDU a las que se conectarán los servidores y los equipos de comunicaciones. De esta forma conseguimos conectar todos los servidores de un armario tendiendo solamente cuatro cables al falso suelo.

Cada armario dispondrá de dos switch de 24 bocas de Ethernet a 1Gbps que proporcionan las conexiones de red necesarias a los servidores y un switch de 100Mbps en el que se conectan los cables de las consolas de cada servidor para crear la red de consola. Estos equipos de red se conectan por fibra o cobre a unos equipos que conectan a 10Gbps con la troncal de la LAN. Con esta configuración tenemos que con tres cables más se da servicio a 48 puertos de red y 24 consolas. Los únicos cables que quedan por tender son los cables de conexión a la red SAN. No se han implementado paneles de parcheado puesto que los equipos conectados a la red SAN son limitados y no había conectores rápidos para enchufar y desenchufar las mangueras de fibra.

El suelo del CPD ya está preparado con las tomas de corriente y las bandejas necesarias para el tendido de los cables separando en bandejas diferentes el tendido de los cables de datos de los cables de corriente.

Contingencias y alta disponibilidad

La configuración de los dos CPD's nos permite ofrecer diferentes niveles de contingencia según la criticidad de los servicios. El disponer de un CPD de respaldo permite tener una salvaguarda de todos los datos contenidos en el backup del CPD principal y ofrecer para determinados

servicios un tiempo de parada en caso de contingencia de pocos segundos.

El primer objetivo de disponer de un centro de respaldo fue el tener una copia de la mayor cantidad de datos del CPD principal posible. Para ello se replican las cabinas de almacenamiento situadas en un centro en el otro a través de la red SAN utilizando tecnologías propias de cada fabricante como pueden ser SRDF, Mirrorview de EMC y Metrocluster de NetAPP. Para el resto de datos que requieren algún tipo de respaldo, los almacenados en el backup diario a cinta, se ha incorporado una librería virtual de cintas que almacena en discos los datos de la última semana de backup. Estos datos una vez almacenados en la librería virtual se copian a las cintas físicas en el CPD de respaldo. El uso de una librería virtual evita la necesidad de que un operador tenga que encargarse in situ del mantenimiento de las cintas del backup en el centro de respaldo. Este último paso junto a las consolas remotas de los servidores, y la propagación de las alarmas al centro principal hacen que el centro remoto no necesite personal ya que todas sus funciones habituales pueden ser controladas remotamente. Sólo es necesario desplazarse al CPD de respaldo para el montaje en el armario de los servidores y otros equipos y para las tareas de mantenimiento de los elementos de calidad ambiental. Aun así se establecen una serie de visitas de inspección visual del estado del CPD a lo largo de la semana.

El siguiente paso una vez respaldados los datos es ofrecer alta disponibilidad en los servicios buscando que el tiempo de parada sea el mínimo posible dependiendo de la criticidad del servicio.

La infraestructura de los CPD's ofrece diferentes configuraciones de disponibilidad en contingencia:

Clúster Activo – Activo

En este tipo de clúster estamos ejecutando simultáneamente la misma aplicación en diferentes servidores encargándose el aplicativo o el balanceador hardware del reparto de carga y de gestionar el fallo. En una configuración típica usando balanceadores hardware los clientes se conectan a una IP virtual del balanceador. Este comprueba que los nodos definidos para esa IP virtual se encuentren activos enviando las peticiones a cada uno de ellos. En caso de caída de algún nodo balanceado. El balanceador dejaría de enviarle las peticiones hasta que vuelva a estar disponible. Esta configuración se está utilizando para el soporte de aplicaciones J2EE utilizando Oracle OAS. En otros casos es el aplicativo servidor el que se ejecuta en varios nodos teniendo conocimiento los clientes de los diferentes servidores que prestan el servicio y conectándose a ellos según estén o no disponibles como sería el caso del correo Lotus

Clúster Activo – Pasivo

En el modelo de clúster activo – pasivo se realiza un montaje de clúster geográfico aprovechando que los datos están replicados en las cabinas de discos situadas en cada CPD. De este modo tenemos el servidor ubicado en el CPD principal que accede a sus datos locales situados en una cabina de almacenamiento local. En caso de fallo del servidor, de la cabina de datos o del CPD al completo, se arrancaría el servicio en un servidor en el centro de respaldo utilizando los datos replicados en la cabina situada en el centro remoto. Este entorno está disponible en el entorno HP-UX a través de la herramienta Serviceguard – MetroCluster y en entorno Microsoft utilizando GeoSpan.

Para no desperdiciar el equipo de respaldo que estaría en reposo en un funcionamiento normal se ponen servicios en este equipo de respaldo configurados de tal manera que en caso de fallo en el CPD de respaldo se utilizaría el CPD principal como respaldo de estas aplicaciones de manera análoga al funcionamiento en contingencia del CPD principal.

Es decir, en este caso se invierten los papeles entre el centro de respaldo y el principal.

La configuración activo – pasivo con cambio de cabina de discos en caso de contingencia requiere un tiempo del orden de minutos en caso de fallo en alguno de los CPD's. Para aplicaciones con requerimientos muy estrictos se está realizando una configuración en la que se monta un clúster tradicional con dos equipos compartiendo datos del mismo almacenamiento. Este clúster provee de disponibilidad en caso de parada de un nodo en un tiempo de pocos segundos y sólo se traslada la ejecución al otro CPD en el caso de una caída completa del CPD principal.

El uso de servidores virtuales en entorno Vmware también nos permite proporcionar alta disponibilidad a los servidores. En el caso de intervenciones programadas que requieran la parada de algún servidor físico que aloje máquinas virtuales, estas se pueden migrar de forma transparente a otro servidor físico. En caso de caída repentina de un servidor físico las máquinas virtuales que se encontraran ejecutando en él, se relanzarían en otro servidor físico de forma automática.