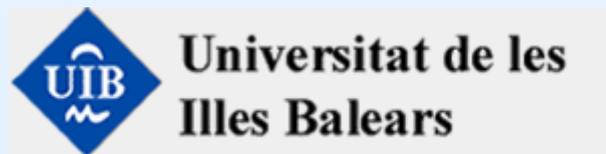


“Proyecto de implantación de un sistema de consolidación de servidores de alta disponibilidad”

Jornadas Técnicas RedIRIS 2005
Logroño, 26 de octubre de 2005



Maribel Barceló(maribel.barcelo@uib.es)
Llorenç Rigo(llorenc.rigo@uib.es)
Antonio Sola(toni.sola@uib.es)
Xavier Pons (xavier.pons@uib.es)

Índice

- Situación y problemática inicial
- Soluciones aplicables
- Virtualización
- Aplicación práctica: Proyecto UIB

Situación y Problemática Inicial

Existencia de multitud de servidores por:

- **Incompatibilidad** de unas aplicaciones con otras
- **Bajo coste** de los servidores clónicos INTEL/AMD en comparación con otras plataformas
- Necesidad de un entorno independiente de **desarrollo**
- Imposibilidad de detener/modificar un servicio en **producción** para añadir nuevas aplicaciones.

Problemática asociada:

- Uso ineficiente de los servidores
- Alto coste de mantenimiento y gestión
- Uso ineficiente del espacio
- Atención al usuario insatisfactoria



Mejoras y objetivos propuestos

Consolidación de servidores

Consolidación de servicios

Alta disponibilidad de servicios

Recuperación de desastres (2° CPD)

Soluciones analizadas

Consolidación hardware: blade, rack

Inconvenientes

- Uso ineficiente de los recursos de los servidores
- Uso ineficiente del espacio de almacenamiento
- Alto coste en inversión económica

Consolidación de servicios

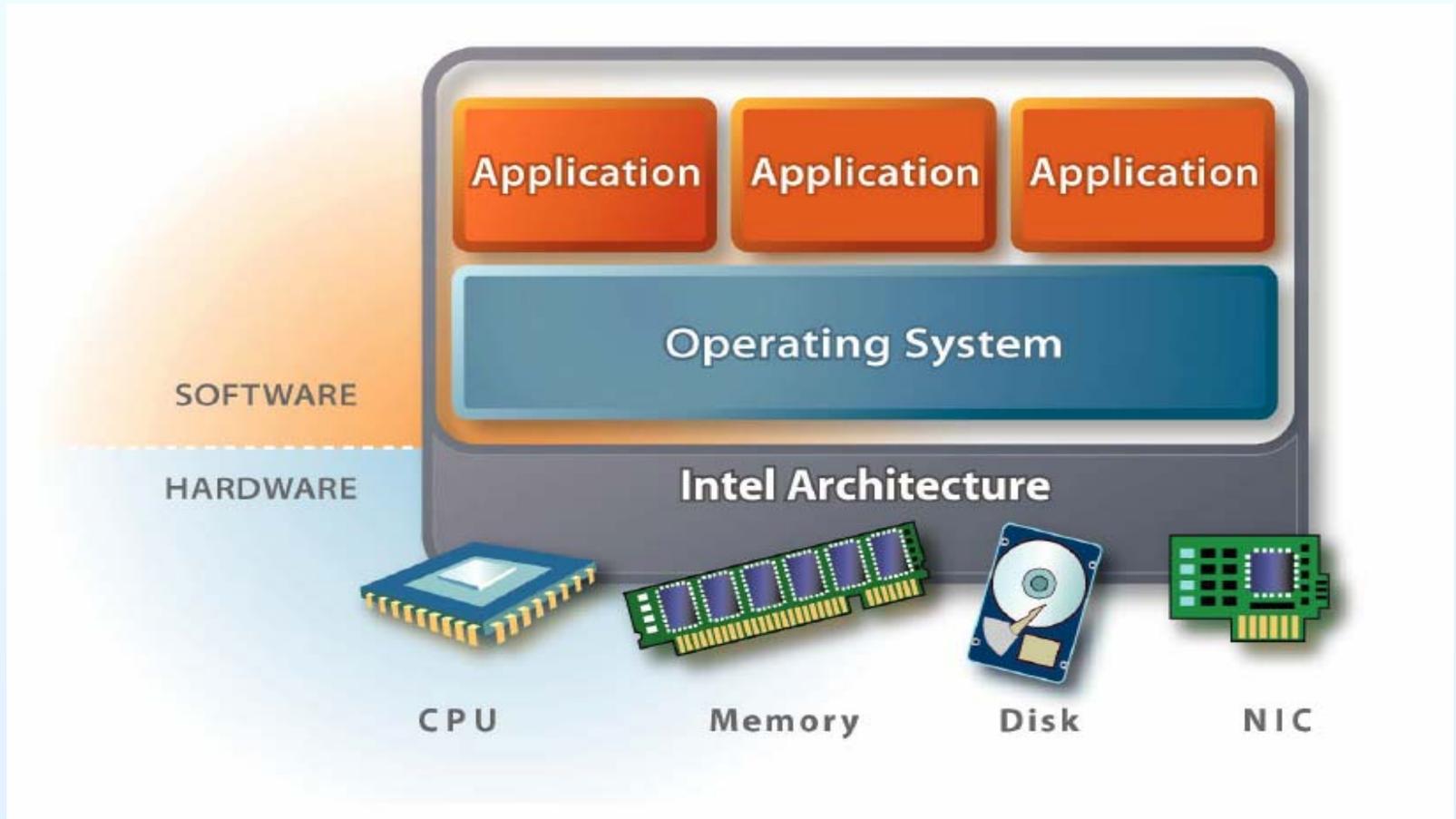
Inconvenientes

- Incompatibilidad Sistemas Operativos
- Incompatibilidad de versiones

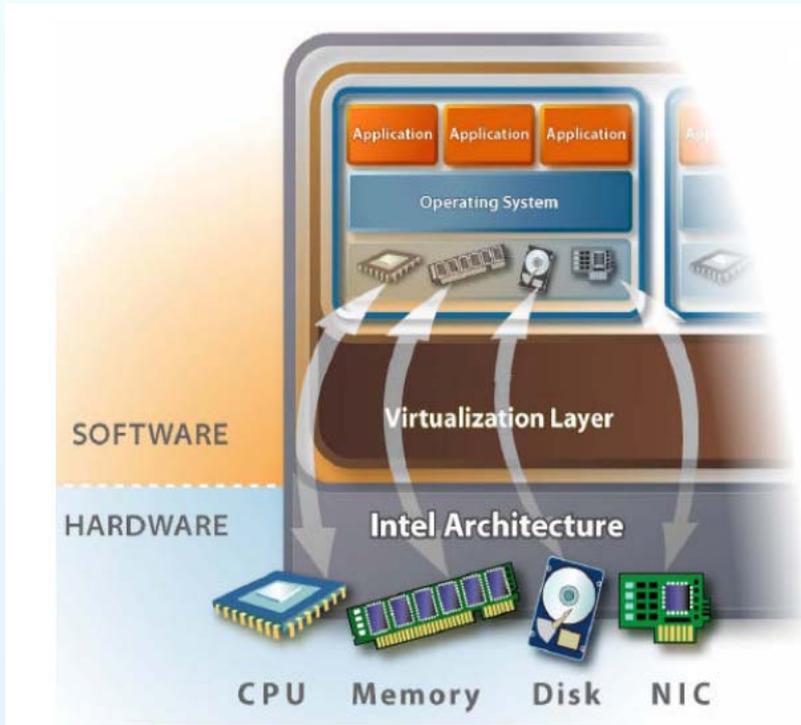
Solución mixta: basada en una **consolidación hardware** e implementación de una capa de **virtualización**

Virtualización(I)

Arquitectura Intel tradicional



Virtualización(II)



La capa de virtualización convierte la visibilidad del hardware físico en hardware virtual

Permite compartir un mismo hardware físico entre diferentes máquinas virtuales

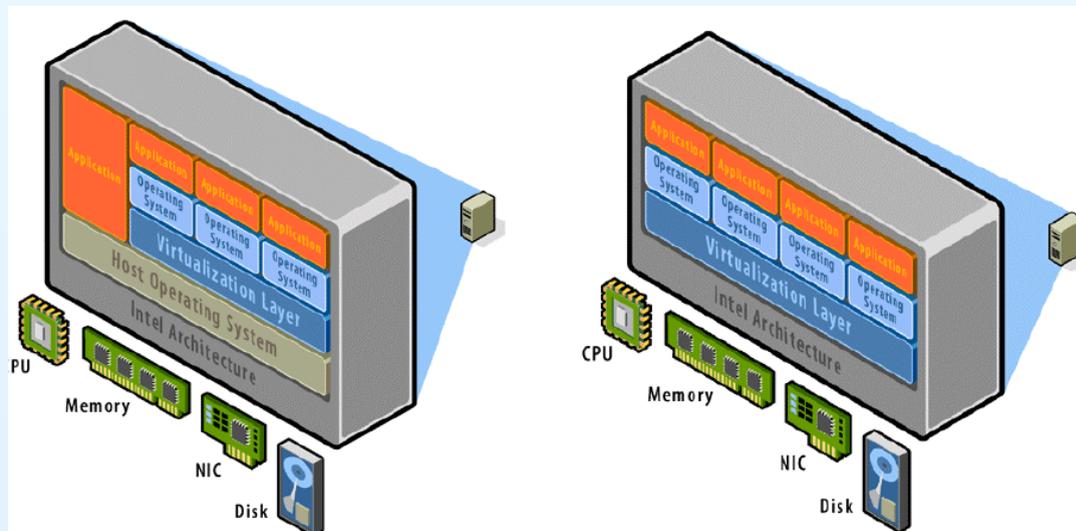
Arquitecturas de virtualización (I)

Opciones de mercado para virtualización consideradas
(Microsoft, Vmware, Open source)

- **Virtual Server (MS):** requiere estar instalado sobre sistema operativo windows. Consume muchos recursos para este SO host, los SO soportados en las MV es más reducido (entorno Windows), no ofrece SMP a los SO invitados.
- **Xen (Open Source):** Requiere un SO linux como host y nos limita a utilizar SO linux adaptados (paravirtualización) en las máquinas virtuales.

Arquitecturas de virtualización (II)

- **ESX (Vmware):** mini-SO específico para virtualización; ganando eficiencia, seguridad, y un consumo mínimo de recursos del hardware. Además ofrece un mayor listado de SO soportados en sus maquinas virtuales.

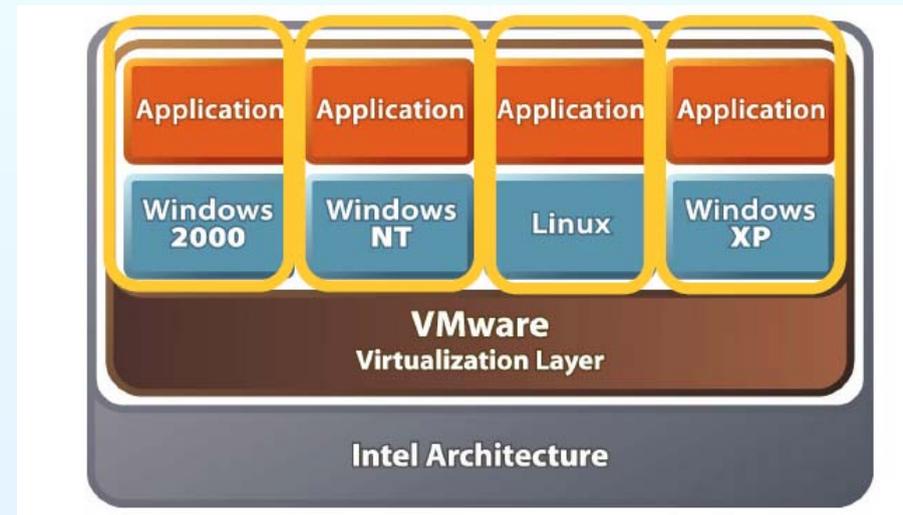


Capa de virtualización - Aislamiento

Las diferentes máquinas virtuales son totalmente **estancas e independientes** unas de otras

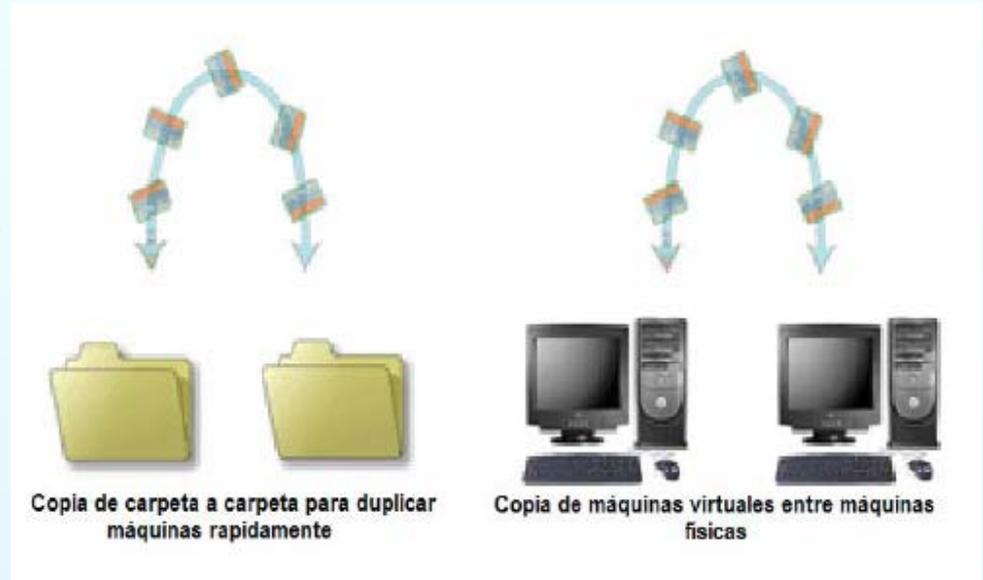
Los sistemas operativos, ficheros, aplicaciones y datos están totalmente **separados**

Si un SO sufre un **crash** no afecta de ningún modo a las demás máquinas virtuales

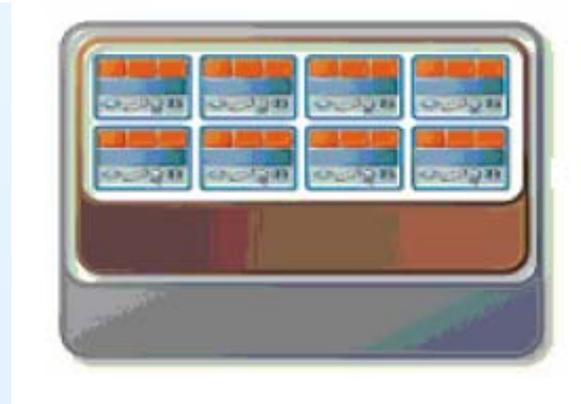


Aprovisionamiento

Se puede **duplicar** una máquina simplemente copiando los ficheros a otra carpeta



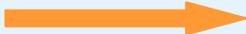
Tendremos una **biblioteca** de sistemas preconfigurados para generar uno nuevo cuando lo necesitemos



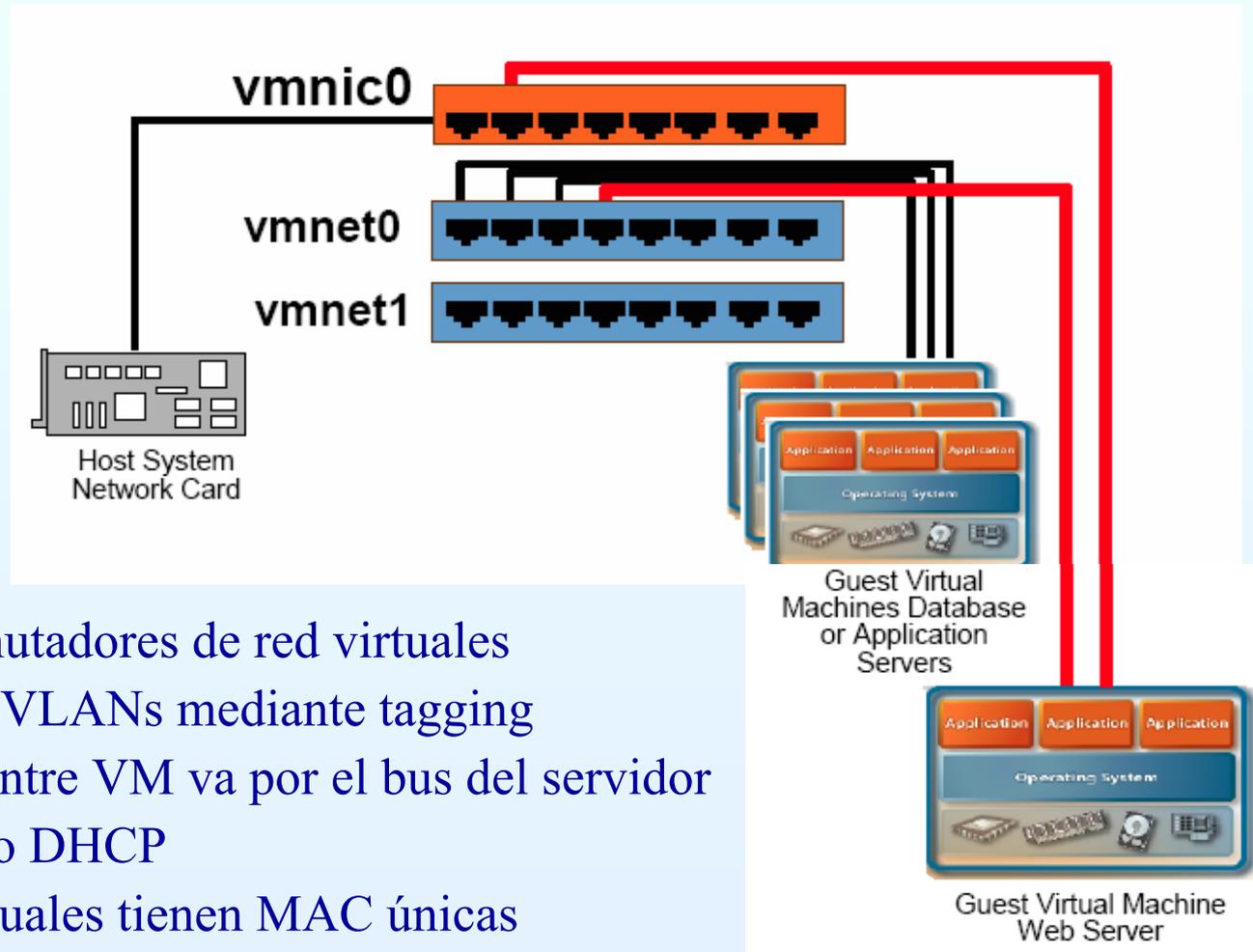
Snapshots y migración

- En cualquier momento podemos realizar una fotografía (**snapshot**) de todo el estado de una MV (disco, memoria, procesos) para en cualquier momento poder retornar a ese mismo punto.
- Facilita la realización del **backup** total de las MV (Disaster Recovery)
- Podemos **desplazar** una MV virtual de un nodo físico a otro si así lo requerimos, sea por motivos de sobrecarga del servidor físico, balanceo de carga tanto a nivel de datos como de red,etc.

Este desplazamiento puede ser:

- “**En frío**”, máquina parada  MIGRACIÓN
- “**En caliente**”, máquina en funcionamiento, podemos desplazarla sin provocar ninguna pérdida de servicio  VMOTION

Comunicaciones



- Creación de conmutadores de red virtuales
- Gestión eficaz de VLANs mediante tagging
- El tráfico de red entre VM va por el bus del servidor
- Direcciones fijas o DHCP
- Las máquinas virtuales tienen MAC únicas

Seguridad en el entorno virtual

- Separación total entre la máquina física y la virtual:
 - el **S.O.** del “host” y el de los invitados son totalmente independientes
 - A nivel de **datos**, se encuentran en entornos físicamente separados
 - A nivel de **comunicaciones**, utilizan dispositivos de red independientes para todas sus comunicaciones, así como segmentos ethernet distintos
- **Independencia** total entre máquinas virtuales

La seguridad a nivel de MV, se implementa de igual manera que en cualquier otra máquina física.
- Entorno de gestión y administración separado **físicamente** del entorno de servicio
- Diferentes **niveles de seguridad** de acceso y administración

Ventajas de la virtualización

- Utilización **eficaz** de los recursos hardware
- Administración **centralizada** de todas las máquinas
- Creación **inmediata** de nuevas máquinas virtuales
- **Portabilidad** de máquinas virtuales entre servidores físicos
- Facilita técnicas de “**Disaster Recovery**”
- Reducción drástica de los **costes** de inversión

Inconvenientes de la virtualización

Tenemos un **único punto de fallo** para todas las máquinas virtuales que corren sobre un único servidor físico

Soluciones a adoptar:

- Utilización de servidores físicos con un nivel importante de **redundancia** (disco, memoria, red, hba, fuente alimentación)
- **Replicar** los servidores físicos en una misma localización o en localizaciones distantes físicamente

Contingencia en entornos virtuales

- Una máquina virtual, en el mundo real esta contenida en un solo **fichero** de datos y en otro de configuración
- Con solo tener una copia de respaldo del fichero podemos tener una segunda máquina de **backup**
- Mediante la utilización de almacenamiento compartido (**SAN**) podemos **migrar** una maquina virtual de un servidor físico a otro sin perdida de visibilidad de la máquina por los usuarios
- Podemos implementar técnicas de “**clustering**” tanto a nivel de servidores físicos como a nivel de servidores virtuales si nuestras aplicaciones así nos lo requieren

El Proyecto

- Un segundo CPD para ofrecer alta disponibilidad y recuperación de desastres. Instalar una SAN extendida entre los 2 CPDs que nos ofrece redundancia total de datos y accesibilidad desde cualquier CPD a todos los datos.
- En cada CPD instalar una capa de virtualización que nos permita instalar las MV necesarias para ofrecer los servicios requeridos por nuestra comunidad universitaria.
- Crear sistemas “clusterizados” y sistemas balanceados entre MV, para ofrecer también alta disponibilidad a nivel de todas las aplicaciones de usuario.

Implementación del proyecto

En cada CPD se instaló el siguiente hardware:

- Instalación de una SAN EMC modelo CX500
- Instalación de rack de dell con 5 nodos PE2850
- 2 Conmutadores FC McData
- 2 Conmutadores Gbit-Ethernet

Y software:

- ESX Server 2.5 en cada nodo.
- VMware VirtualCenter , software de gestión de la infraestructura virtual que proporciona un punto único de control para los recursos virtuales de los 2 cpds.
- Sistema de monitorización y alerta de la SAN.

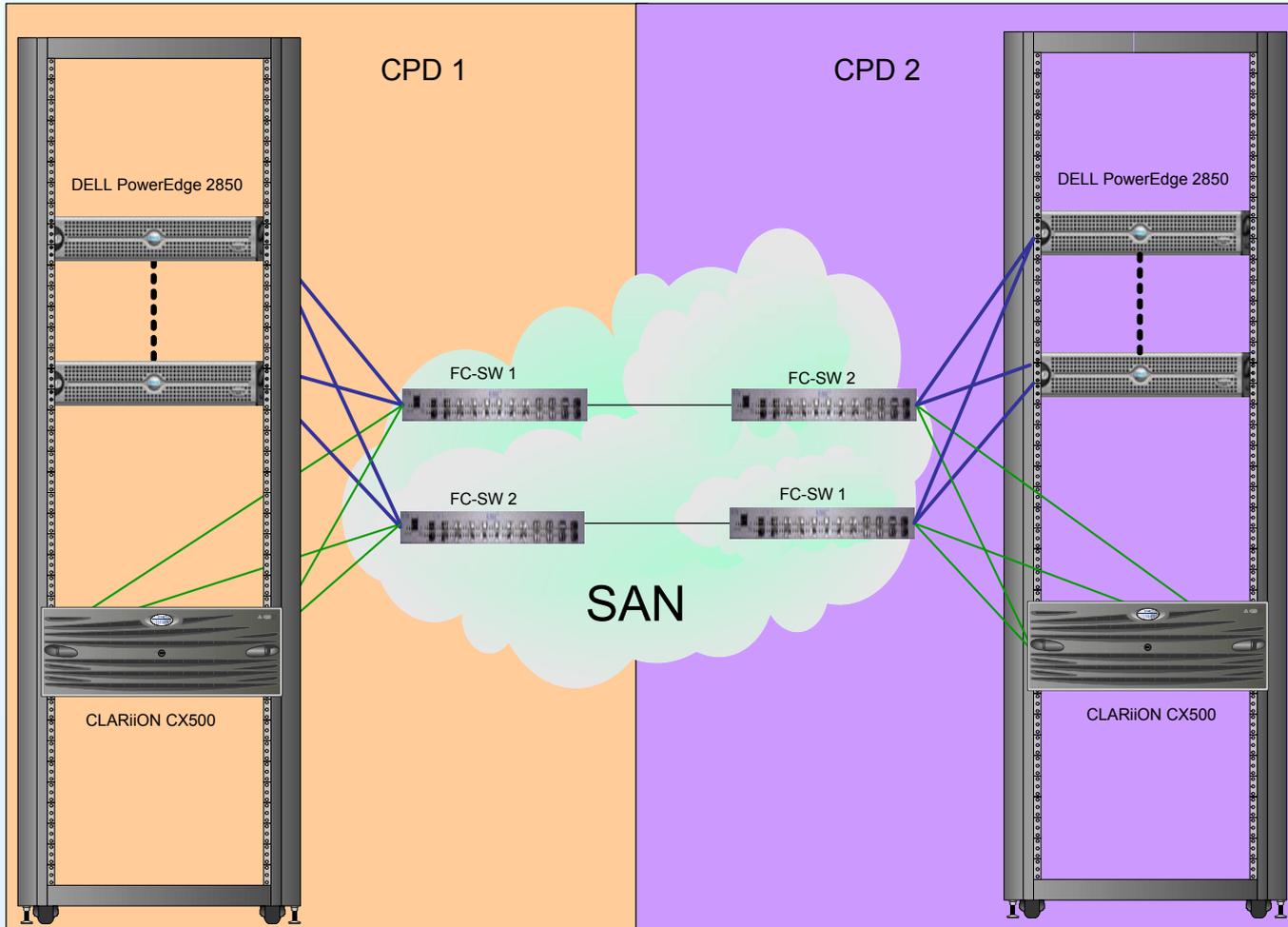
Configuración del almacenamiento

- El CX500 ofrece redundancia a nivel de **Storage Processor (2)** y cada SP tiene 2 puertos FC conectados a cada uno de los conmutadores ofreciendo una redundancia de 4 caminos para el acceso a los datos.
- A nivel de datos se crearon diversos “**raid groups**” con Raid 5, sobre los cuales se crearon las LUNS que se ofrecen a todos los ESX, que tienen visibilidad global y total sobre todas.
- Desde cualquier ESX de cualquiera de los CPDs tenemos la misma **visibilidad** de los datos.
- Mediante el software **Mirrorview** realizamos una replica automatizada síncrona, de todas las operaciones de I/O, entre los CX500 de cada CPD, consiguiendo así que si cae un CPD, desde el otro seguiremos teniendo acceso a todos los datos.

Configuración de los nodos ESX

- Cada nodo PE2850 está configurado con 2 Pentium IV Xeon 3.2Ghz, 8GB de memoria, 2 discos SCSI locales, 2 HBA y 4 puertos Gbit-Ethernet y fuentes redundantes.
- Cada nodo dispone de un total de 4 caminos para acceder a las LUNs.
- Cada ESX dispone del agente Vmotion para poder mover las MV en caliente (sin parada de máquina y sin pérdida de servicio) entre diferentes nodos físicos.
- El agente Virtual Center, que permite la gestión centralizada de todos los nodos físicos i máquinas virtuales.
- Licenciamiento para poder ofrecer hasta 2 procesadores para cada una de las MV, si así lo requerimos.

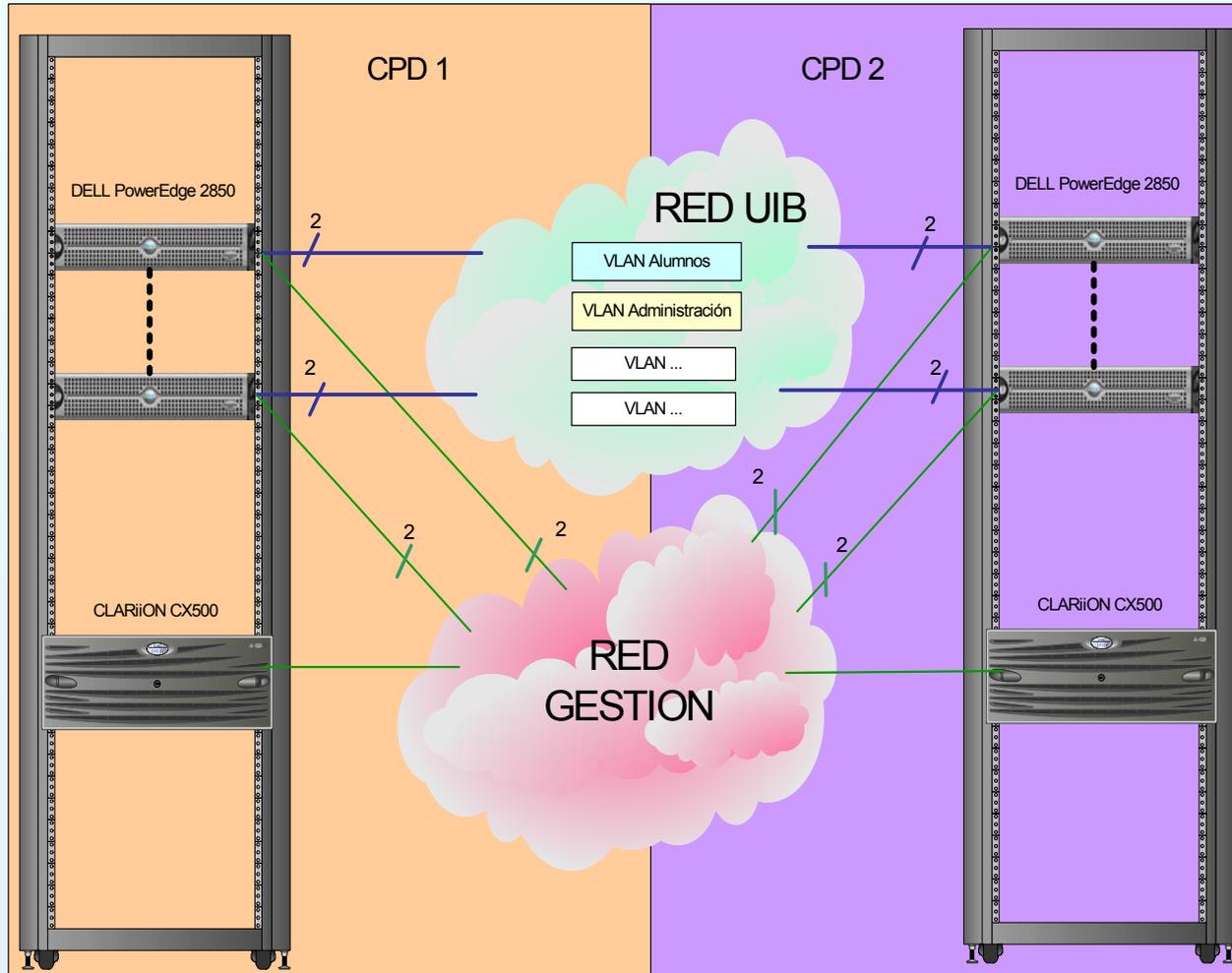
Configuración SAN UIB



Configuración del entorno de comunicaciones

- Cada CPD ofrece comunicación Gigabit conmutada
- Los dos CPD están interconectados mediante una fibra monomodo dedicada y un camino alternativo (backup).
- La red de gestión y la de servicio están físicamente separadas.
- Podemos conectar cualquier MV a cualquier VLAN de nuestra red.

Configuración red UIB

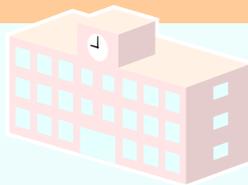


Configuración de las máquinas virtuales(I)

Entorno Windows

- Instalación de 3 Clusters Windows 2003:
 - Administración, Alumnos y General
 - Cada cluster esta formados por 3 nodos distribuidos entre los 2 sites
 - Finalidad: ofrecer **alta disponibilidad**, teniendo en cuenta también la carga global de cada CPD tanto a nivel de hardware como de comunicaciones
- Diversas MV para ofrecer diversos servicios independientes
- MV para nuestro entorno de desarrollo

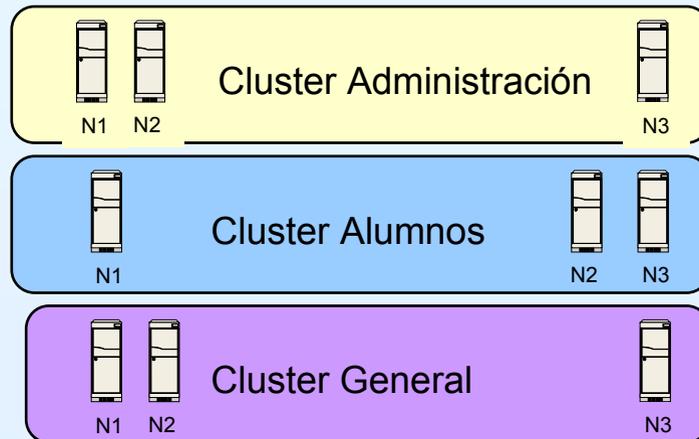
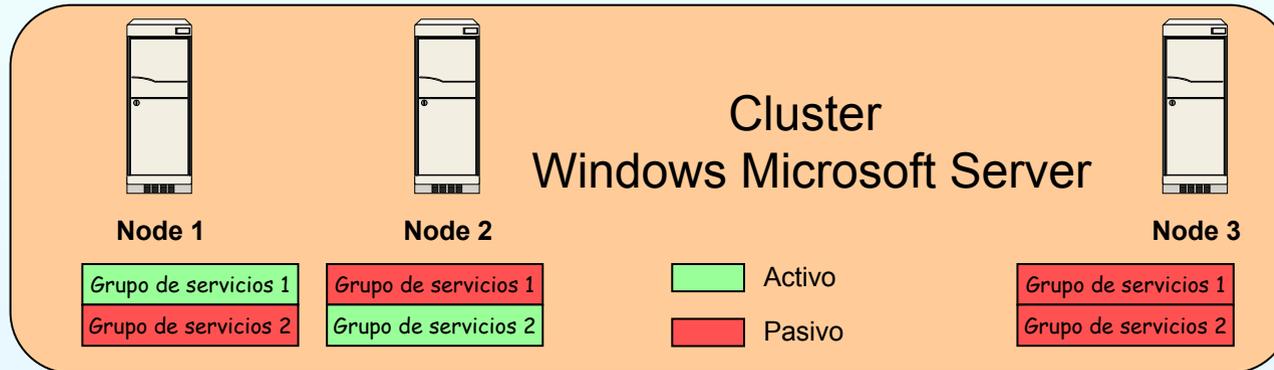
Configuración Clusters Windows



CPD 1



CPD 2



Configuración de las máquinas virtuales(II)

Entorno Linux

- La mayoría de servicios de red están implementados sobre el entorno linux (Web, DNS, DHCP, RADIUS, ...) así como los front-end de las aplicaciones Oracle (IAS).
- Cada uno de estos servicios esta instalado en una MV independiente permitiendo una mejora en la securización y en su administración.
- Todos estos servicios se ofrecen con redundancia mediante balanceo de carga (LVS).
- Cada servicio posee una réplica en cada uno de los CPDs asegurando una alta disponibilidad de todos estos servicios básicos.

Conclusiones del proyecto

- Evidente mejora en la **gestión** y organización de las salas de máquinas de los CPDs, así como del espacio ocupado.
- Mejora en la **utilización** y aprovechamiento de la inversión en hardware.
- **Alta disponibilidad** de los servicios de red y de los demás servicios ofrecidos a la comunidad universitaria.
- Mejora en la seguridad al “**microsegmentar**” servidores por servicio.
- Mejora en la **seguridad** y acceso a los datos almacenados.
- **Flexibilidad** en la creación y eliminación de servicios/servidores, según necesidades.
- Mejora en la **administración** general de los sistemas.

Futuro / Mejoras

- Adaptar el sistema de alarmas y eventos a nuestro entorno
- Integración con los procesos de backup
- Desarrollo de software para el desplazamiento automatizado de las MVs en función de la carga tanto del nodo físico como de la red.
- Implementación de diferentes niveles de acceso, gestión y control del entorno virtual.

Agradecimientos

www.dell.es



spain.emc.com



www.ermestel.com



www.vmware.com

