



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA



Escola Tècnica
Superior d'Enginyeria
Informàtica

Escuela Técnica Superior de Ingeniería Informática
Universitat Politècnica de València

Aplicación de soluciones libres a una empresa TIC

Proyecto Final de Carrera

Ingeniería Técnica en Informática de Gestión

Autor: Antonio Rodríguez Mompó

Director: José Ramón García Escrivá

23/07/2012

Resumen

El presente Proyecto Final de Carrera, expone los problemas y/o carencias a los que se enfrenta una empresa que proporciona toda la infraestructura y servicios TIC a una agrupación de empresas. Por otro lado muestra las posibles soluciones aplicables, valorando tanto alternativas comerciales como de código libre, y siempre justificando la opción elegida. En determinados casos, son problemas de infraestructura a resolver, mientras que en otros, se detectan determinadas carencias, las cuales hay que satisfacer. Con ello se obtendrá un mayor control y calidad de los servicios proporcionados por la organización a sus usuarios.

Se proporcionan servicios comunes a todos los usuarios, como por ejemplo el correo electrónico, intranet corporativa, antispam, pero dependiendo de cuál sea su rol en la organización, se encontrará disponible el acceso a determinados servicios. Por ejemplo, un equipo encargado del desarrollo de un proyecto deberá acceder a recursos diferentes a los que debería acceder un empleado del departamento de finanzas.

Palabras clave: almacenamiento, monitorización, planificación, incidencias, infraestructura TIC, servicios proporcionados.

Tabla de contenidos

Resumen	3
Tabla de contenidos	4
Introducción y objetivos.	5
1. Servicios proporcionados por la Empresa.....	7
1.1 Infraestructura	7
1.2 Comunicaciones.....	8
1.3 Proyectos para empresas del grupo	8
1.4 Herramientas de gestión corporativa	9
2. Descripción de la Infraestructura Corporativa	11
2.1 Hardware y servicios	11
2.2 Electrónica de red	13
2.3 Infraestructura VMWare	15
2.4 Almacenamiento.....	16
3. Software comercial y software de código libre	17
4. Debilidades y /o problemas a resolver	18
4.1 Mayor capacidad de almacenamiento.	18
4.2 Monitorización de servidores.	29
4.3 Planificación de proyectos.....	45
4.4 Gestión de Incidencias.	52
Conclusiones	60
Bibliografía.....	62

Introducción y objetivos.

En la actualidad, gracias a los actuales avances en el área de las Tecnologías de la Información e Informática, disponemos cada vez de sistemas más complejos, robustos y potentes que facilitan nuestro día a día tanto en el ámbito personal como en el empresarial.

Desde hace varias décadas no concebimos una empresa sin ordenadores, los cuales con el software apropiado, han automatizado, optimizado y flexibilizado ciertas tareas que anteriormente podrían resultar más lentas y tediosas, en las que los errores humanos eran más habituales y el proceso para obtener información crítica para la organización era mucho menos ágil.

Con el tiempo, en las organizaciones, los ordenadores han pasado de ser estaciones de trabajo independientes a formar parte de una red corporativa, donde se comparte información y recursos, en definitiva, se ha producido una evolución en la forma de trabajar en la que prima el buen aprovechamiento y centralización de los recursos, evitando así gastos innecesarios y duplicidades.

Esta evolución no se ha quedado sólo a nivel de las estaciones de trabajo, sino también ha afectado a los sistemas encargados de proporcionarnos los servicios necesarios para poder desarrollar nuestra actividad. Antiguamente, se disponía de una máquina física por cada servicio que queríamos proporcionar (servidor), y si el dimensionamiento no era el adecuado, estábamos desperdiciando los recursos y malgastando el presupuesto. Con las tecnologías de virtualización actuales, se intenta conseguir el máximo grado de aprovechamiento de los recursos ya sean hardware como software, con la consiguiente reducción de costes que supone el correcto dimensionamiento de los servicios proporcionados.

Para conseguir el mencionado grado de aprovechamiento es necesario el uso de hipervisores y agrupaciones de recursos donde el almacenamiento desempeña un papel fundamental.

La administración de los activos de almacenamiento es uno de los principales desafíos de TI en la actualidad. El continuo crecimiento en los requisitos de almacenamiento complica la administración de los datos, sobre todo a nivel corporativo. Por ello es necesaria una infraestructura ágil que permita adaptarse a los cambios.

Sin embargo disponer de toda ésta tecnología no nos sirve de mucho cuando se desconoce del estado y la calidad de los servicios que se están proporcionando.

Una caída de la web corporativa puede suponer pérdidas económicas importantes, ya que es un canal de comunicación con los clientes y proveedores, un medio muy rentable para darse a conocer y proporcionar la descripción de los servicios que se ofrecen. El fallo de otros servicios críticos como por ejemplo el correo electrónico puede paralizar el negocio. Por ello surge la necesidad de un sistema para la monitorización de los servicios corporativos, ya sean de uso interno como externo.

Para que una organización pueda alcanzar sus objetivos, es necesaria una correcta planificación. El objetivo de la planificación de proyectos es obtener una distribución de las actividades en el tiempo y una utilización de los recursos que minimice el coste del proyecto cumpliendo con los condicionantes exigidos de: plazo de ejecución, tecnología a utilizar, recursos disponibles y máximo nivel de ocupación de dichos recursos.

Las herramientas para la planificación de proyectos nos proporcionan un modo para obtener un calendario de las actividades a realizar y en cuánto tiempo deberemos completarlas, pudiéndose obtener una representación gráfica de las diferentes actividades e hitos.

En los departamentos de IT suele ser habitual, además de las herramientas para la planificación de proyectos, la utilización de herramientas con las que gestionar tareas más cotidianas, con un seguimiento del estado de la tarea, tiempo dedicado para su resolución, bases de conocimiento e informes. Dichas herramientas son las que constituyen los sistemas para la gestión de incidencias.

Los objetivos del presente proyecto son dar una visión de las posibles opciones para ampliación del almacenamiento utilizado por los servidores que emplean técnicas de virtualización, herramientas para la monitorización de sistemas, planificación de proyectos y gestión de incidencias en una empresa real, junto con una descripción de los servicios corporativos e infraestructura disponibles.

1. Servicios proporcionados por la Empresa

La Empresa proporciona todos los servicios TIC que cualquier Organización del Grupo pueda necesitar, de esta forma los mandos intermedios y alta dirección tienen su actividad totalmente enfocada a la generación de negocios y optimización del resultado, despreocupándose de todo aquello que no tiene que ver con la gestión directa del negocio.

1.1 Infraestructura

Gestión de Sistemas:

Se realizan todas las tareas relacionadas con la instalación y configuración de equipos, ya sea a nivel de sistema operativo como a nivel de aplicación. El sistema operativo utilizado en los equipos es Windows XP y Windows 7, ambos en su versión profesional, puesto que todos los sistemas se encuentran unidos al dominio corporativo.

También se gestionan los activos mediante un inventario de hardware, software (licencias) y ubicación física.

Gestión de impresión:

Se proporciona a las empresas del grupo los sistemas de impresión, junto con un contrato de mantenimiento que incluye el coste por copia, ya sea a color o en negro y los consumibles a emplear en dicho sistema.

Email:

Todos los empleados del grupo disponen de servicios de correo electrónico y gestión avanzada de spam. En la que cada usuario es capaz de admitir y bloquear aquellos correos que considere oportuno. También se mantiene una copia histórica del correo entrante y saliente, para que en caso de borrado accidental, poder recuperar dichos correos.

Para los usuarios de perfil técnico y directores de proyecto, se dispone del servicio Blackberry Enterprise Server, proporcionándoles la capacidad de gestionar su correo y calendario en dispositivos móviles.

Alojamiento web:

Se dispone de diversas plataformas como pueden ser LAMP, Sharepoint y Wordpress. Dependiendo de los requisitos y de la funcionalidad del servidor requerida, se recomendará la plataforma que más se ajusta a las necesidades del cliente.

Copias de Seguridad:

Existen mecanismos para la realización de copias de seguridad tanto para servidores, ya sean virtuales o físicos como para estaciones de trabajo. Así, en caso de catástrofe, minimizar al máximo la pérdida de información.

1.2 Comunicaciones

Voz Fija:

Disponemos de los acuerdos derivados de una gran cuenta en Telefónica. Esto se traduce en un soporte técnico dedicado, gestión prioritaria de averías e incidencias y reparto de los consumos por centros de coste.

Voz Móvil:

Los servicios de voz móvil son proporcionados por Vodafone, disponiendo también de las ventajas de poseer gran cuenta: gestión de altas / bajas de líneas, cambios de tarjetas SIM, cambio de terminales por avería, acceso a cobertura preferencial en lugares donde la cobertura es baja o nula, tarifas especiales y centralitas virtuales para su uso en las diversas sedes del grupo, proporcionando extensiones para llamadas internas.

Datos:

La comunicación entre las diversas sedes de las organizaciones se consigue mediante el uso de túneles VPN (Virtual Private Network) por software, pero actualmente estamos realizando un proceso de migración a la infraestructura Macrolan de Telefónica, que nos proporcionará la conectividad entre las diferentes sedes a nivel de ISP (Internet Service Provider), pudiendo así descartar la solución actual.

1.3 Proyectos para empresas del grupo

Proporcionamos todos los servicios e infraestructura necesaria para la gestión del ciclo completo de los proyectos que tienen relación con IT, como puede ser la definición de requisitos, oferta técnica, seguimiento del proyecto, apoyo a la puesta en marcha y mantenimiento.

También realizamos la selección de proveedores, evaluación de ofertas y la redacción de las propuestas de servicio (RFP o Request For Proposal).

Algunos ejemplos de los proyectos desarrollados son:

- Control de rondas: consiste en el despliegue de la infraestructura necesaria para poder justificar, que un empleado encargado de realizar determinada ronda de comprobación de instrumentación, la ha realizado y ha pasado por todos los puntos de control requeridos por el contratante del servicio.
- Desarrollo de aplicación para mantenimiento de dispositivos contra incendios: en el que se mantiene actualizada información relativa a fecha del último mantenimiento del dispositivo, comprobación de estado, certificación, marca y modelo. Todo ello accesible y gestionable desde una PDA.

- Control de presencia: despliegue y configuración de la infraestructura necesaria para desarrollar el proyecto mediante identificación biométrica.
- Extranet de clientes UTPR (Unidad Técnica de Protección Radiológica): aplicación web que permite a los clientes la capacidad de descargarse sus propias facturas e informes de los controles de calidad realizados a sus instalaciones radiológicas.

1.4 Herramientas de gestión corporativa

ERP:

Se dispone de Microsoft Dynamics Axapta como herramienta para la planificación de los recursos empresariales. Se ofrece soporte técnico, mantenimiento preventivo, correctivo, evolutivo y la gestión de la seguridad de acceso a dicha aplicación.

OLAP

Creación de cubos OLAP (OnLine Analytical Processing) para análisis multidimensional de información. También se confeccionan informes mediante la tecnología Microsoft Reporting Services.

Epsilon

Aplicación que integra la gestión de nóminas y RRHH. Se encuentra integrado con el ERP corporativo para la imputación de costes de personal a los proyectos y se proporciona los servicios de actualización del sistema y gestión de la seguridad de acceso.

Intranet

La intranet corporativa se encuentra desarrollada sobre la plataforma Sharepoint de Microsoft. Se proporciona la confección de formularios y flujos de trabajo mediante Infopath, además del mantenimiento preventivo, correctivo y evolutivo.

Web

Se proporcionan los servicios de gestión y actualización de los contenidos de las webs corporativas del grupo de empresas.

También se encuentra disponible una herramienta para la planificación y gestión de proyectos.

Help Desk:

El servicio de soporte informático se encuentra disponible al alcance de los usuarios, mediante el cual, ya sea de modo presencial o vía telefónica, se puede atender a las incidencias de los mismos.

Aplicación de soluciones libres a una empresa TIC

Para la resolución de dichas incidencias, se dispone de herramientas para el control remoto de las estaciones de trabajo, facilitando y optimizando así el tiempo requerido en resolver el problema y evitando la intervención del usuario. En aquellos casos en los que es imposible una solución por medio de control remoto existe la posibilidad del desplazamiento del técnico para resolver la avería in situ.

Para la gestión de las incidencias se dispone de una herramienta de tickets de IT. Ello permite un mayor control de las incidencias y permite conocer a cualquier miembro del departamento de IT el estado de cualquier solicitud de servicio.

2. Descripción de la Infraestructura Corporativa

2.1 Hardware y servicios

svrDC00:

Se dispone de un controlador de dominio principal, en máquina física, que dispone de un procesador de cuatro núcleos y 4GB de RAM. Tiene como sistema operativo Windows 2003 Server R2 SP2 STD.

Los servicios que proporciona dicho servidor son:

- Active Directory: es el único controlador de dominio físico, para que en caso de caída de la infraestructura virtual, el Virtual Center pueda autenticarse y arrancar, y los host ESX tengan un DNS al que consultar.
- DHCP: permite la configuración dinámica de la red de las estaciones de trabajo.
- Políticas de grupo: permite definir las políticas que cumplirán los equipos y usuarios miembros del dominio, como por ejemplo el montaje de unidades de red, impresoras y scripts de inicio de sesión.
- DNS: permite la traducción de nombres a direcciones IP y viceversa.

svrVC:

Este servidor dispone de un procesador de cuatro núcleos y 8GB de RAM. Utiliza como sistema operativo Windows 2003 Server R2 SP2 STD y es miembro del dominio.

El servicio proporcionado por dicho servidor es:

- VMWare Virtual Center: sistema de gestión centralizada de la infraestructura virtual. Desde dicho sistema se puede controlar cualquier máquina virtual en ejecución, modificar el hardware de la máquina, hacer instantáneas (snapshots) del estado de la máquina en un momento determinado, migración entre diversos hosts y muchas otras funcionalidades necesarias para la administración de servidores.

La infraestructura virtual está constituida por un servidor Virtual Center y por tres hosts ESX que serán los encargados de la ejecución de las máquinas virtuales.

ESX 1:

Se trata del primer host para la ejecución de máquinas virtuales, utiliza como sistema operativo VMware ESX4.0 y está gobernado por VMWare Virtual Center.

Dispone de dos procesadores de cuatro núcleos, 16GB de memoria RAM ECC, dos tarjetas de red gigabit y tarjetas fibre channel para acceder a la cabina de discos.

ESX 2:

Se trata del segundo host para la ejecución de máquinas virtuales, utiliza como sistema operativo VMware ESX4.0 y está gobernado por VMware Virtual Center.

Dispone de dos procesadores de cuatro núcleos, 16GB de memoria RAM ECC, dos tarjetas de red gigabit y tarjetas fibre channel para acceder a la cabina de discos.

ESX 3:

Se trata del tercer host para la ejecución de máquinas virtuales, utiliza como sistema operativo VMware ESX4.0 y está gobernado por VMware Virtual Center.

Dispone de dos procesadores de cuatro núcleos, 16GB de memoria RAM ECC, dos tarjetas de red gigabit y tarjetas fibre channel para acceder a la cabina de discos.

svrTS01:

Servidor que dispone de un procesador de cuatro núcleos y 2GB de memoria RAM. Utiliza como sistema operativo Windows 2003 Server R2 SP2 STD.

El servicio proporcionado por dicho servidor es:

- Terminal Server, permite el inicio de sesiones remotas y la utilización de las aplicaciones instaladas en dicho servidor mediante el protocolo RDP (escritorio remoto).

svrCCSS:

Servidor que dispone de un procesador de cuatro núcleos y 2GB de memoria RAM. Dispone de acceso a una unidad robótica para la realización de copias de seguridad y conectividad mediante fibra a la cabina de discos. Utiliza como sistema operativo Windows 2003 Server R2 SP2 STD.

Los servicios proporcionados por dicho servidor son:

- VMware VCB Proxy: componente de la infraestructura VMware que facilita el montaje de los volúmenes para su copia de seguridad.
- Symantec Backup Exec 12.5: Incluye agente sql, exchange y vmware. Con éste software se gestionan todas las copias de seguridad de los servidores, ya sean físicos o virtuales.

Se han instalado los Agentes Remotos de Backup Exec en todos los servidores para poder realizar copias de seguridad desde el propio servidor en remoto. Además también se ha instalado el componente "Advanced Open File Option" el cual permite hacer copia de los ficheros en caliente, es decir, aunque estos ficheros estén en uso se harán copia de seguridad de ellos sin que se corrompan los datos.

2.2 Electrónica de red

La red corporativa presenta un Backbone formado por un stack de switches de capa 3, que consta de nueve switches interconectados por módulos y cables de 24Gbs. Dichos switches presentan 24 puertos Gigabit y 4 bahías para módulos Ethernet de 10 Gigabits.

Sobre este stack de switches se ha establecido una estructura de red formada por 6 VLAN's (Servidores, VMotion, DMZ, Equipos, WIFI Invitados, WIFI empleados) destinadas a dar servicio a los diferentes segmentos de red (subredes) de la red corporativa.

Una VLAN (Virtual Local Area Network) es un método para crear redes lógicamente independientes dentro de una misma red física permitiendo separar los segmentos de red unos de otros.

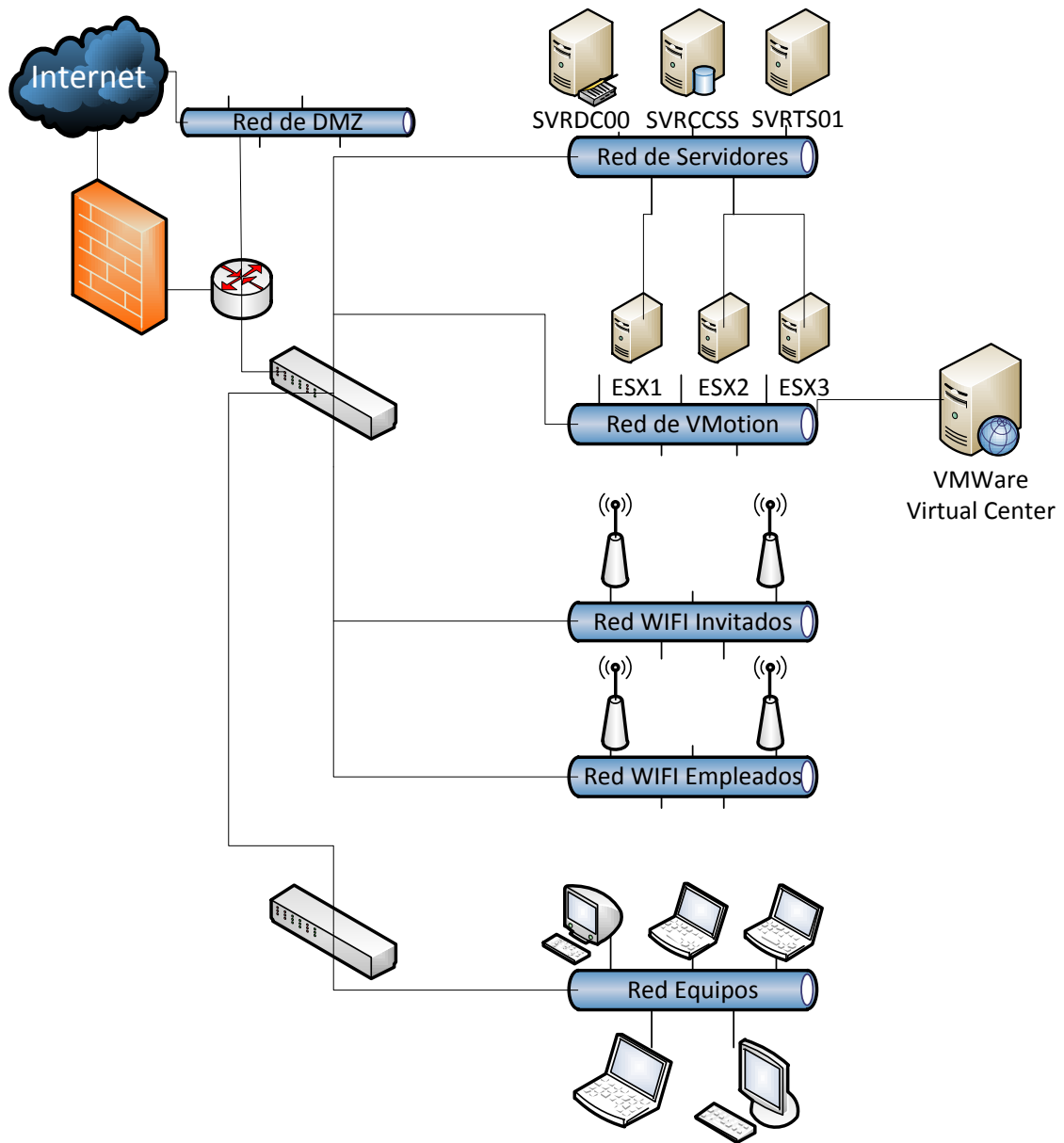
Existen instalados 5 puntos de acceso, los cuales tendrán la función de dar conexión WIFI a los usuarios que deseen conectarse por toda la oficina, donde distinguiremos dos tipos de usuarios: usuarios internos de la empresa y usuarios externos a la empresa (invitados). Estos últimos sólo dispondrán de acceso a internet, mientras que los primeros dispondrán de acceso a todos los recursos disponibles (servidores e impresoras).

Por último, se dispone un clúster formado por dos cortafuegos físicos, que son los responsables de proporcionar seguridad a la red corporativa, principalmente con la conexión a Internet así como conexiones VPN's con las sedes remotas, el acceso VPN de usuarios mediante software y la gestión de reglas de enrutamiento.

Ambos cortafuegos se encuentran configurados en alta disponibilidad, así en caso de avería del primero, el segundo entraría en funcionamiento de modo transparente a los usuarios.

Aplicación de soluciones libres a una empresa TIC

Diagrama de red.



2.3 Infraestructura VMWare

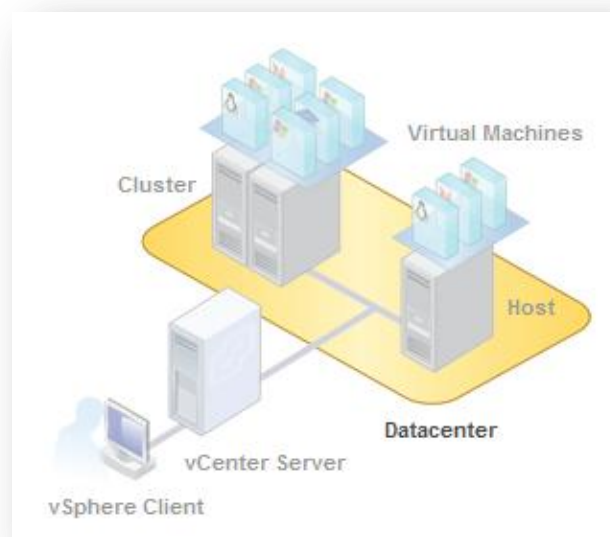
La Infraestructura VMWare que se ha implantado cuenta con los siguientes equipos:

- Tres servidores RX300 Fujitsu Siemens sobre los cuales se han instalado los servidores ESX que serán el motor de la Infraestructura VMWare.
- Una cabina de discos CX3-GD fibre-channel.
- Un Servidor RX200 donde está en ejecución el Virtual Center que controla los hosts ESX.
- Dentro de la Infraestructura VMWare, se ha creado un Datacenter.

Dentro del Datacenter se ha creado un clúster, el cual da lugar a que exista un sistema de alta disponibilidad con HA y DRS.

VMWare HA permitirá mover una máquina virtual de un host (servidor ESX) a otro migrándolo y sin parar la máquina virtual. Y también, por supuesto, por si cae un host que las máquinas virtuales que tenga en uso en ese momento se enciendan automáticamente en otro host. Se ha establecido en la configuración del HA que sólo permita el fallo de un servidor ESX del clúster.

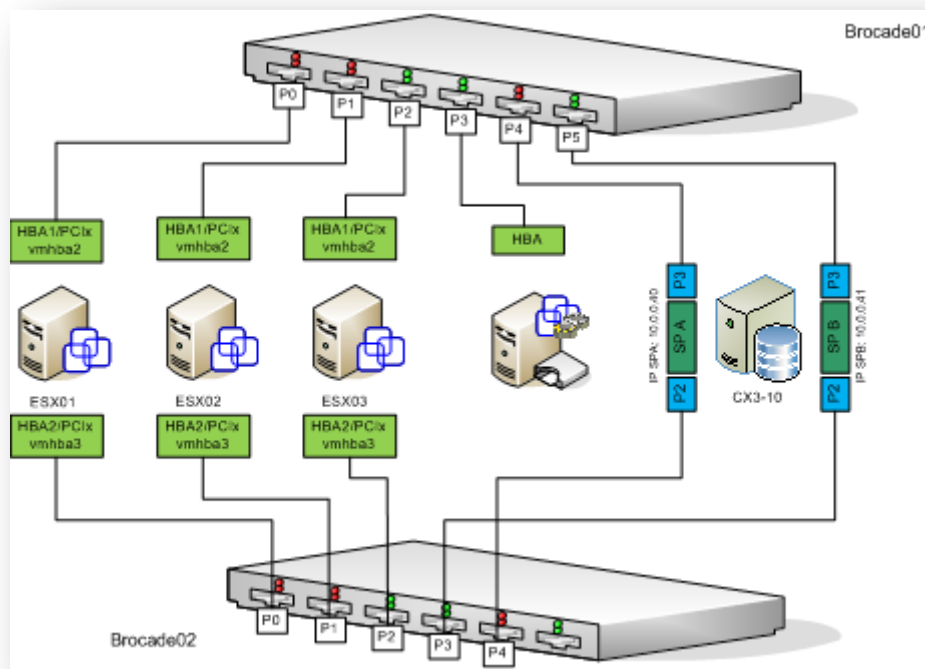
VMWare DRS, permite por un lado el poder crear los pool de recursos para gestionar el hardware que deseamos que tengan determinadas máquinas virtuales, y por otro una mejor gestión del uso que realizan las máquinas virtuales de los recursos que tienen los servidores ESX.



2.4 Almacenamiento

La cabina de discos consta de 15 discos duros, 140Gb FC, los cuales han sido configurados en RAID. Se han creado varios RAID's de acuerdo a las necesidades de rendimiento y/o fiabilidad requeridos para el almacenamiento de los servidores corporativos virtuales.

Un sistema RAID (Redundant Array of Independent Disks) hace referencia a un sistema de almacenamiento que usa múltiples discos duros en los que se distribuyen o replican los datos. Existen distintos niveles de RAID, dependiendo de cuál sea nuestra prioridad podemos optar por un volumen formado por la agrupación de varios discos (priorizamos capacidad de almacenamiento), podemos tener varios discos replicados entre sí (priorizamos seguridad frente a capacidad de almacenamiento) o podemos tener una situación de equilibrio entre las soluciones anteriores (equilibrio entre almacenamiento y seguridad). Dependiendo del uso al que vaya a ser destinado dicho almacenamiento nos podrá interesar una opción u otra.



3. Software comercial y software de código libre

Definición de software.

El software se corresponde con el conjunto de instrucciones necesarias para que el hardware disponible en un equipo realice una tarea determinada de modo eficiente y que cumpla con los resultados esperados.

Software comercial.

El software comercial es aquel que tiene limitadas las posibilidades de uso, modificación y redistribución, o que su código fuente se encuentra restringido y no está al alcance de la comunidad de usuarios. Habitualmente la empresa propietaria del producto software posee todos los derechos de autor sobre el producto, pudiendo así conceder o denegar derechos sobre el software.

Habitualmente los productos de software comercial tienen un coste, pudiendo distinguir varios modelos de licenciamiento, pero habitualmente será necesario a demás de comprar la licencia del software en sí, la compra de licencias de acceso a dicho producto, utilizadas por los usuarios de la aplicación. Por tanto el coste del producto sería la suma de la licencia del software más las licencias de acceso por parte de los usuarios.

Software libre.

El software libre es aquel que está bajo una licencia libre y que su uso, modificación y distribución no se encuentra restringida. Es por ello por lo que viene acompañado del código fuente, así todo aquel que desee, puede realizar las modificaciones que considere oportunas en el software para adaptarlo a sus necesidades sin tener que contar con el permiso del desarrollador.

Habitualmente no tienen coste de licenciamiento.

Conclusión.

Nosotros nos decantaremos, siempre que sea posible, por las herramientas de código libre, pues las licencias que incorporan habitualmente estas soluciones permiten beneficiarse de las contribuciones y mejoras realizadas por las comunidades activas de usuarios, por las posibilidades de realizar cambios internos en la aplicación (puesto que en una solución comercial estas acciones son imposibles ya que su licencia impide cualquier modificación, son como una “caja negra”) y por supuesto por el coste de una solución de código libre frente a una solución comercial.

4. Debilidades y /o problemas a resolver

4.1 Mayor capacidad de almacenamiento.

Detalles.

Después de 4 años de uso de la infraestructura anteriormente descrita, conforme va transcurriendo el tiempo las necesidades de almacenamiento de los servidores aumentan.

Gracias a la infraestructura virtual disponible, se dispone de una gestión dinámica de recursos, mediante la cual se puede ampliar / disminuir el hardware disponible para cada máquina virtual del clúster.

Por ejemplo añadir más memoria RAM a un servidor en concreto, reservar más núcleos, agregar una unidad nueva de almacenamiento o ampliar una ya existente o incluso llegar a al nivel de detalle de especificar cuántos MHz de CPU deseamos tener reservados para dicho servidor.

En el modelo tradicional de proporcionar un servicio por servidor, si no se encuentra correctamente dimensionado el hardware respecto a la carga del sistema, estaremos desperdiciando recursos, mientras que en un entorno virtualizado es mucho más fácil conseguir el correcto aprovechamiento de los recursos dedicados a un servidor.

Pero estamos llegando a un punto crítico en lo que a capacidad de almacenamiento se refiere. La cabina de fibra, que es la que proporciona todo el almacenamiento a la infraestructura virtual, está llegando a sus límites de almacenamiento.

Todos los días entran correos que el servidor debe almacenar, se genera documentación nueva para proyectos: ofertas, imágenes, presupuestos..., las bases de datos del ERP (Microsoft Dynamics Axapta) y el software de gestión de nóminas (Epsilon) crecen día a día. Por ello surge la necesidad de una mayor capacidad de almacenamiento.

Posibles soluciones.

Se han valorado las siguientes opciones para resolver el problema:

- a) Añadir una cabina de discos nueva con discos de mayor capacidad.
- b) Reemplazar los discos de la cabina actual por unos de mayor tamaño.
- c) NAS con certificación iSCSI para VMWare.

La solución ideal sería añadir una cabina de discos nueva con discos de mayor capacidad, puesto que nos ofrecería gran rendimiento pues funciona con la tecnología Fibre Channel.

Toma de decisiones.

El principal problema que nos enfrentamos si optamos por la solución a) o b) es el precio del hardware y el licenciamiento, una cabina de discos no es un hardware barato y los discos empleados SaS (Serial ATA SCSI) tampoco lo son. Debido a las limitaciones del presupuesto asignado, las dos primeras soluciones son descartadas y aceptamos la opción c) como candidata.

Tras consultar en la web del fabricante de la infraestructura virtual (VMWare) observamos que el rendimiento teórico para un NAS es bastante aceptable para el tipo de servidores que vamos a tener alojados.

Optamos por comprar un NAS (QNAP [TS-859U-RP Turbo NAS](#)) gobernado por una distribución Linux, dispone de 8 bahías para alojar discos duros SATA (Serial Advanced Technology Attachment), dos tarjetas de red soportando equilibrado de carga, tolerancia a fallos de conectividad, soporte para varios niveles de RAID, expansión dinámica de volúmenes, certificación VMWare y soporte para varios protocolos de acceso (FTP, SMB, NFS, iSCSI).

Estándares. Protocolos aplicables.

De acuerdo con las necesidades actuales de centralización de la información, protección de acceso, gestión de copias de seguridad y rendimiento, es habitual disponer en las organizaciones de un NAS (*Network Attached Storage*), que no es más que un servidor dedicado al almacenamiento que dispone de varios protocolos de acceso. Dichos dispositivos no tienen un coste prohibitivo y generalmente tienen funcionalidades de equilibrado de carga y tolerancia a fallos mediante RAID.

Algunos de los protocolos más utilizados para el acceso a los sistemas de almacenamiento son:

- SMB
- NFS

Un protocolo más avanzado y con mayores posibilidades que los mencionados anteriormente es iSCSI. Nos proporciona funcionalidades extra como la posibilidad de arrancar un servidor utilizando almacenamiento iSCSI a través de una red IP en lugar del almacenamiento local tradicional.

SMB

Es un protocolo de red que permite compartir archivos e impresoras en una red entre varios nodos. Fue desarrollado inicialmente por IBM, pero la más utilizada es la versión propuesta por Microsoft.

Microsoft renombró SMB a Common Internet File System (CIFS) en 1998 y añadió más características, que incluyen soporte para enlaces simbólicos, enlaces duros (hard links), y mayores tamaños de archivo.



Existe una implementación libre del protocolo SMB llamada SAMBA en los sistemas Unix, de tal modo que es posible que ordenadores con Linux o Mac OS X se vean como servidores o actúen como clientes en redes de Windows.

Para poder definir los permisos de acceso sobre los recursos de almacenamiento se puede optar por un servicio de autenticación local o uno centralizado.

NFS

El sistema de archivos de red (NFS) es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales. Originalmente fue desarrollado en 1984 por Sun Microsystems, con el objetivo de que sea independiente de la máquina, el sistema operativo y el protocolo de transporte.

En este sistema necesitamos un servidor (donde se encuentran los recursos) y clientes (son los que solicitan el acceso a los recursos del servidor).

Los datos se encuentran centralizados en un único lugar pero pueden ser accedidos y modificados por varios usuarios, de tal forma que no es necesario replicar la información, y facilitando las tareas de copia de seguridad.

NFS trabaja muy bien compartiendo sistemas de archivos con muchos hosts conocidos de un modo transparente. Sin embargo, esta facilidad de uso trae una variedad de problemas potenciales de seguridad.

Estos problemas radican en que NFS controla quien puede montar y exportar sistemas de archivos basados en la máquina que hace la petición, no el usuario que utiliza el sistema de archivos. Los hosts tienen que tener los derechos para montar los sistemas de archivos exportados explícitamente. El control de acceso no es posible para usuarios, aparte de los permisos de archivos y directorios. Por tanto, cualquier usuario que pueda acceder a una máquina que tenga permisos de lectura y/o escritura sobre el recurso NFS, podrá acceder a dicha información con el nivel de privilegios asignados a dicha máquina.

iSCSI

Este protocolo de implementación de código libre permite la negociación y el posterior intercambio de comandos SCSI utilizando redes IP. Al utilizar este estándar conseguimos un canal de almacenamiento local de alto rendimiento, siendo una alternativa de menor coste que la tecnología fibre channel.

La adopción del iSCSI en entornos de producción corporativos se ha acelerado en estos momentos gracias al aumento de la tecnología Gigabit Ethernet. La fabricación de almacenamientos basados en iSCSI es menos costosa y está resultando una alternativa a las soluciones SAN (storage area network) basadas en fibre channel.

El protocolo iSCSI utiliza TCP/IP para sus transferencias de datos, por tanto necesitamos una interfaz de red para poder funcionar. Este protocolo puede verse afectado por la sobrecarga que generan las transmisiones TCP/IP en una red, pero con la tecnología actual de Gigabit Ethernet, no debería haber una degradación excesiva en el rendimiento.

iSCSI utiliza iniciadores (initiator) para enviar comandos iSCSI a los dispositivos de almacenamiento. Estos iniciadores pueden ser basados en software o hardware. Los iniciadores software pueden ser suficientes pero una solución hardware ofrece un mejor rendimiento en E/S utilizando menos recursos del host. Hay que tener en cuenta que una solución software introduce una sobrecarga de CPU en el host que se conecta a la red de almacenamiento.

Respecto a la seguridad, iSCSI proporciona mecanismos de encriptación y autenticación.

Estándares y protocolos a utilizar.

Utilizaremos el protocolo iSCSI para la conexión entre los tres hosts ESX y el NAS, debido al rendimiento y a las funcionalidades de seguridad que proporciona dicho protocolo.

Puesta en marcha.

Los discos utilizados son 6 HDD's Seagate Barracuda de 2TB.

Se procederá a la creación de 2 RAID's:

- RAID5: 4 discos de 2TB, disponemos de 6TB para almacenamiento. Un disco está reservado por si falla alguno de los otros y no perder la información.
- RAID1: 2 discos de 2TB, disponemos de 2TB para almacenamiento. Es una copia en espejo del otro disco.

Una vez que ya se han creado los RAID's y están sincronizados, procederemos a crear un LUN iSCSI para poder hacer pruebas de rendimiento y estabilidad.

Un LUN (Logical Unit Number) representa un dispositivo iSCSI (Internet Small Computer System Interface) individualmente direccionable que es parte de un dispositivo iSCSI (target). En un entorno iSCSI, las LUNs son básicamente discos numerados. Un iniciador negocia con un target la conexión a un LUN. El resultado es una conexión iSCSI, emulando una conexión a un disco duro utilizando el protocolo SCSI.



Aplicación de soluciones libres a una empresa TIC

Ejecutamos el asistente de configuración.

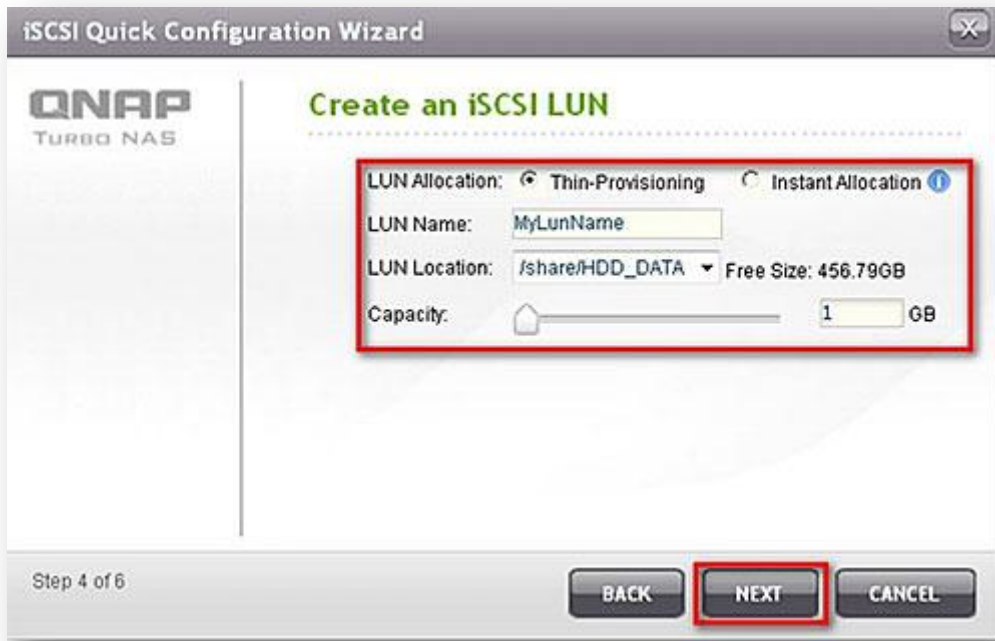


Queremos crear un iSCSI Target con un LUN mapeado (primera opción). Así dispondremos de una unidad lógica a la que posteriormente accederemos desde cada host ESX.



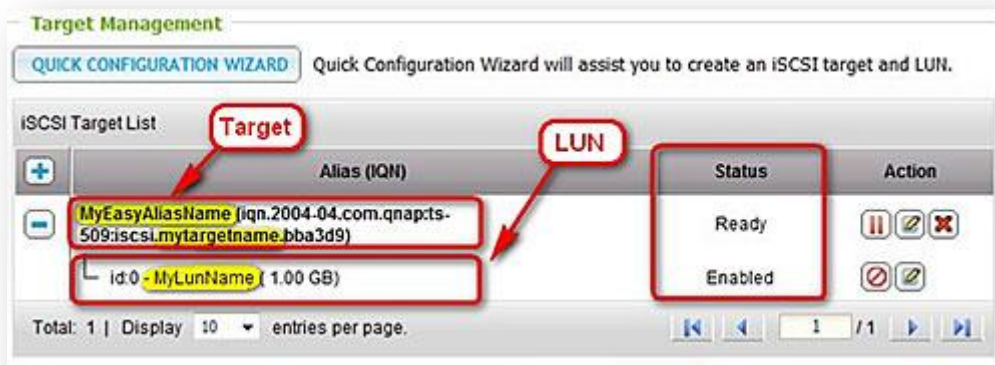
Asignamos el nombre, tamaño y tipo de LUN.

- *Thin provisioning*: el disco duro de la máquina virtual va creciendo dinámicamente conforme a las necesidades.
- *Instant allocation*: el disco duro de la máquina virtual se asigna en éste momento. Proporciona mayor rendimiento.



(imagen con datos ficticios)

Una vez que aceptemos los cambios solo tendremos que habilitar el LUN.

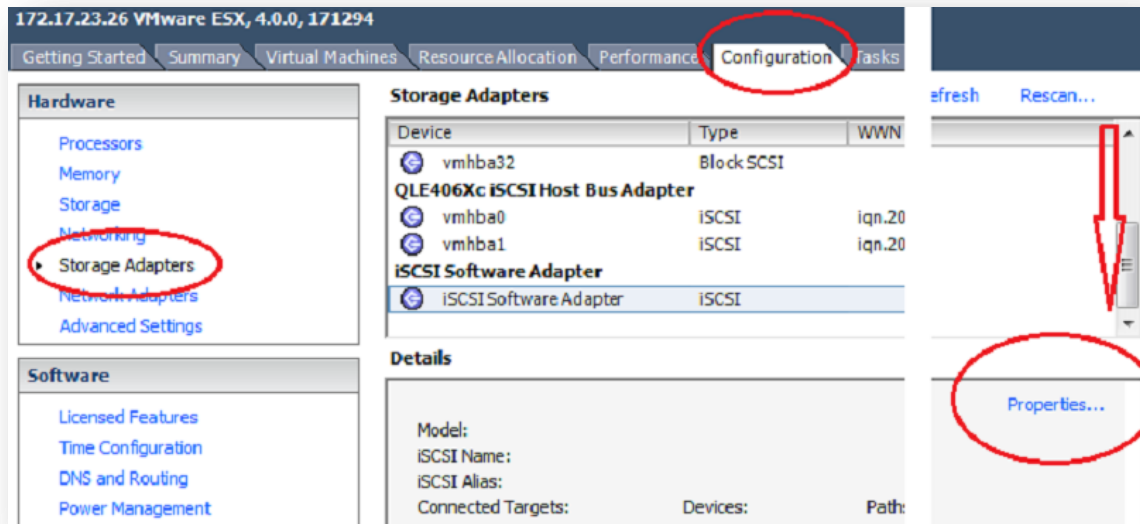


(imagen con datos ficticios)

Con estos pasos ya tendremos la parte de configuración del NAS realizada. Ahora realizaremos la configuración en cada uno de los hosts ESX de VMWare.

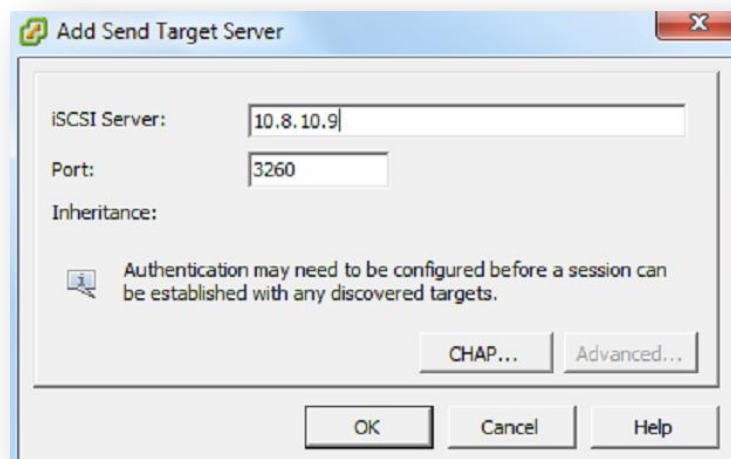
Aplicación de soluciones libres a una empresa TIC

Para ello iremos a configuration -> Storage Adapters y en el adaptador "iSCSI Software adapter" haremos clic en Properties y activaremos el soporte iSCSI.



(imagen con datos ficticios)

En la pestaña Dynamic Discovery añadiremos la IP de nuestro NAS.

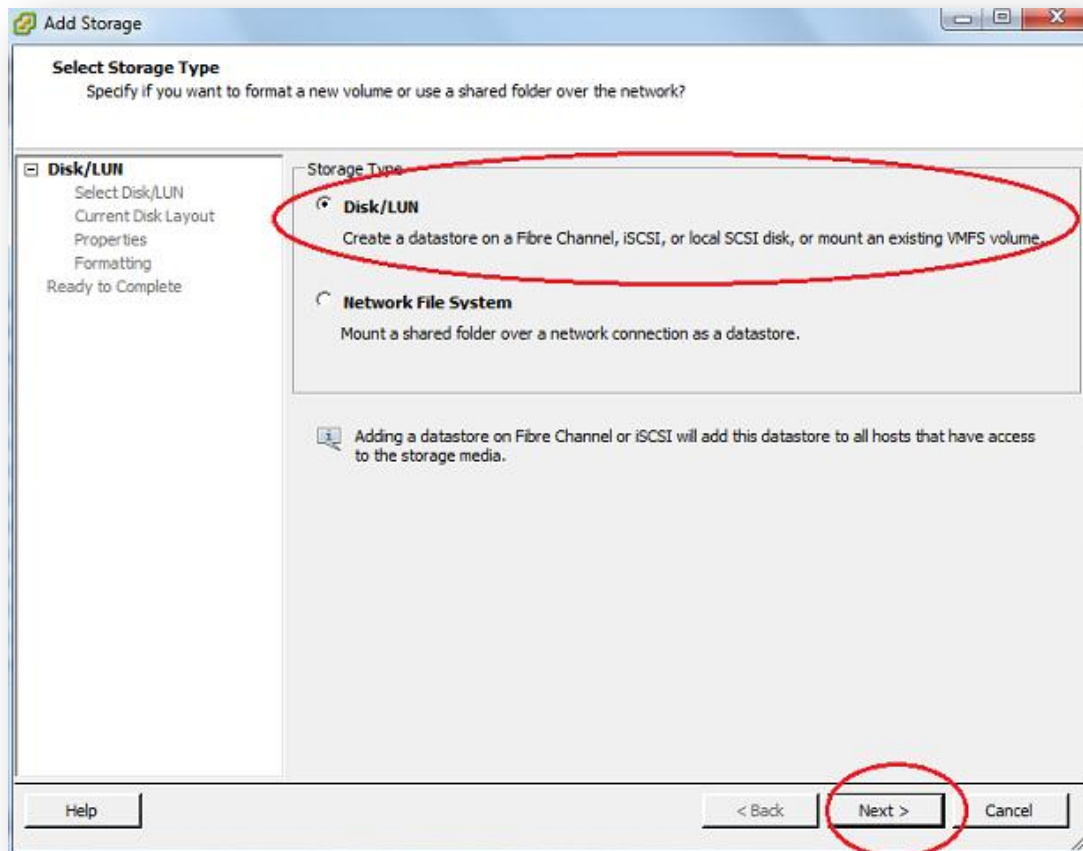


(imagen con datos ficticios)

Una vez que ya tenemos agregado el NAS, será necesario hacer un reescaneo del adaptador iSCSI. Tras finalizar dicha operación ya nos aparecerá disponible el adaptador y podremos ver el almacenamiento disponible.

Para habilitar el nuevo datastore iremos a configuration -> storage.

Seleccionaremos que el tipo de almacenamiento es un Disco/LUN



Al hacer clic en siguiente nos aparecerán las LUN's disponibles. Seleccionaremos la LUN que queramos, la formatearemos y le estableceremos un nombre.

Unos pocos segundos después nos aparecerá como un nuevo almacenamiento disponible.

View: **Datstores** Devices

Refresh Delete Add Storage...

Identification	Status	Device	Capacity	Free	Type	Last Update
VM_Working_Dir	✓ Normal	172.17.23.244:VM_Working_Dir	2.68 TB	2.62 TB	NFS	9/29/2009 18:28:58
ESXDataStore01	✓ Normal	10.8.10.9:/share/ESXDataStore01	457.23 GB	441.49 GB	NFS	9/29/2009 18:28:58
Storage1 (2)	✓ Normal	Local ATA Disk (t10.ATA W...	231.50 GB	223.52 GB	vmfs3	9/29/2009 18:28:58
ESXDataStore02	✓ Normal	IET ISCSI Disk (t10.9454450000...	499.75 GB	499.19 GB	vmfs3	9/29/2009 18:28:58

(imagen con datos ficticios)

Pruebas.

Una vez que ya disponemos de nuestro LUN iSCSI, procederemos a la migración de las máquinas virtuales. Debido a que contamos con la funcionalidad de HA (High Availability) podemos realizar esta migración en caliente, sin tener que detener el servicio y totalmente transparente para los usuarios.

Tras realizar la primera migración, todo ha ido correctamente, los usuarios no han notado una degradación del servicio y la migración se ha realizado con una tasa de transferencia de 48MB/s. Ahora procedemos a estresar el servidor. Vamos a realizar un escaneo completo del disco duro en busca de virus, esta operación nos asegura un uso intensivo del NAS, puesto que estaremos leyendo continuamente.

A la vez que se está realizando el escaneo procedemos a migrar otro servidor. Conseguimos picos de 48MB/s, pero la tasa de transferencia no es tan constante como en la anterior migración.

Transcurrido un par de días, el sistema continua totalmente estable, en línea y con un buen rendimiento, por lo que procedemos a migrar 3 servidores más.

Una vez completada la migración, tenemos 5 servidores en ejecución en el LUN con RAID5, todo funciona aparentemente bien.

Transcurridas unas horas, apreciamos una degradación en el rendimiento, quizá achacable a la carga del sistema producida por los usuarios. Conforme va transcurriendo el tiempo la degradación va en aumento, llegándose al punto de perder el control de la máquina virtual (no se puede acceder a la consola), pero el servicio sigue en funcionamiento, eso sí, más lento de lo habitual. Al final llegamos a una situación en la que las máquinas virtuales que se encuentran en ejecución con almacenamiento en el NAS aparecen como “desconectadas”, pero el servicio proporcionado sigue vivo. Por ejemplo una de las máquinas migradas es la intranet corporativa. A pesar de aparecer como desconectada, al escribir la URL en el navegador, puedes acceder a ella, pero funciona muy lentamente.

Para retomar el control de las máquinas virtuales se procede al reinicio de los servicios de gestión de los ESX. Transcurridos unos minutos, todo vuelve a funcionar con normalidad.

Al cabo de un día vuelve a ocurrir lo mismo: máquinas “desconectadas”, pérdida de HA (Alta Disponibilidad) y todos los servicios funcionan mucho peor. Se decide la migración de las máquinas virtuales del LUN iSCSI a su ubicación original.

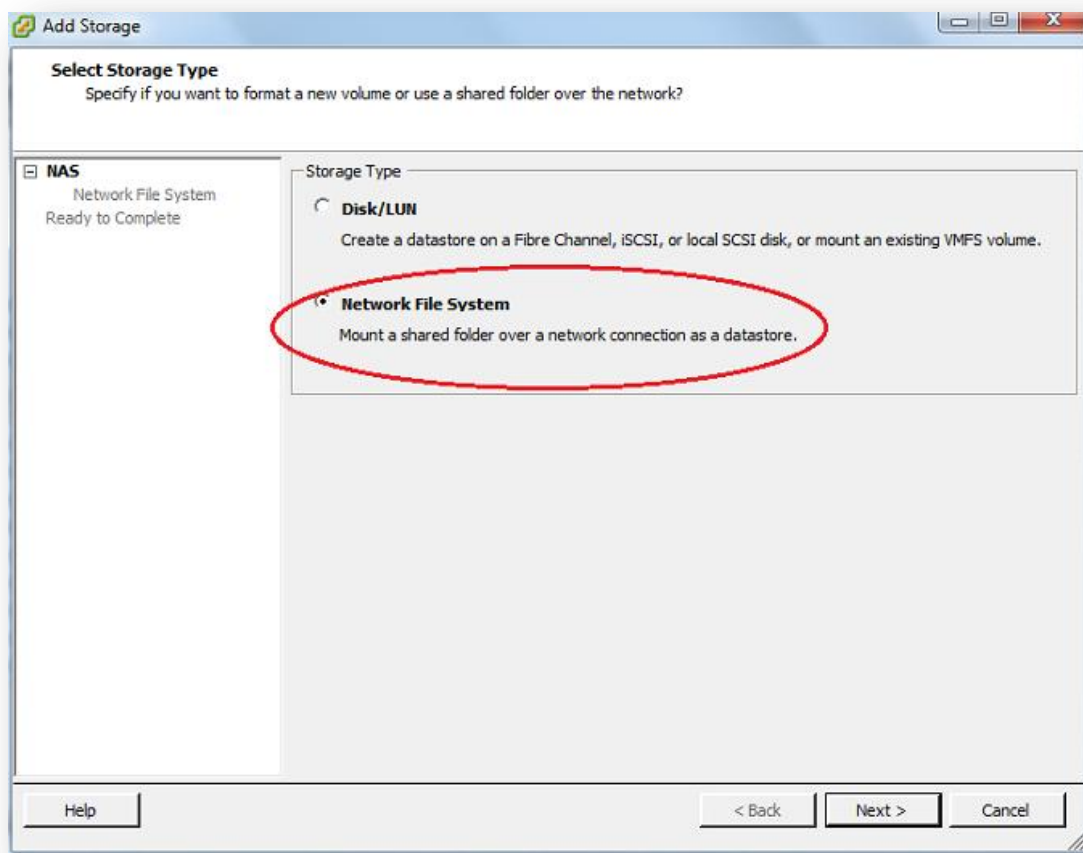
Tras varias semanas de investigación y con la ayuda de un entorno de pruebas (dos host ESXi compartiendo el NAS como dispositivo de almacenamiento) para intentar reconstruir en la medida de lo posible un entorno en producción, se descubre que el fallo que se está produciendo en el clúster se debe a una situación [APD](#) (All Paths Down).

Una situación APD surge cuando existe mapeado un LUN pero no es accesible. Por tanto perdemos la conectividad con el NAS, la Alta Disponibilidad (HA) y tenemos timeouts, produciendo una degradación de servicio considerable en todo el clúster.

Se ha efectuado una actualización del firmware del NAS que incorporaba mejoras a nivel de implementación del protocolo iSCSI, pero no han conseguido solucionar el problema.

Puesto que las pruebas realizadas con iSCSI han sido un fracaso, se ha optado por buscar un protocolo de red alternativo que nos pueda proporcionar una conexión estable, fiable y con un buen rendimiento entre el NAS y el clúster VMWare: el protocolo NFS. Antes de realizar cambios en el clúster en producción, haremos simulaciones en el entorno de pruebas.

Partiendo de que tenemos ya desactivado el protocolo iSCSI en el NAS y en el clúster, la configuración para NFS es muy similar, pero en éste caso añadiremos un datastore NFS.



Tras las pruebas realizadas utilizando el protocolo NFS, no se ha producido ninguna degradación en el rendimiento incluso cuando se estaba estresando el sistema con pruebas adicionales. La tasa de transferencia de las máquinas virtuales al NAS es cercana a los 80MB/s, bastante superior a la obtenida mediante iSCSI que era de 48MB/s en el mejor de los casos.

Tras los prometedores resultados obtenidos, se decide poner el sistema en producción. Se conecta cada host del clúster al NAS vía NFS.

Los resultados han sido los deseados: no se ha producido ninguna degradación en el servicio, ni pérdida de la Alta Disponibilidad. Actualmente hay 10 máquinas virtuales en ejecución.

Respecto a la seguridad sólo se permiten las conexiones de las direcciones IP de los hosts ESX y Virtual Center de VMWare, limitando así el posible acceso desde máquinas no autorizadas al NAS.

Conclusiones.

En un sistema en producción es muy delicado realizar cualquier modificación / reconfiguración del sistema. Sobre el papel todo es correcto y compatible, todo debería funcionar adecuadamente y alcanzar el rendimiento que se espera, pero tras la situación vivida anteriormente, se puede extraer la conclusión de la necesidad de un entorno de pruebas aunque los productos que vayamos a utilizar estén certificados por el fabricante.

Un problema como el descrito anteriormente, desemboca en situaciones de “crisis” en un Departamento de TI, viéndose seriamente afectados los usuarios por unas “mejoras” que ellos no entienden y que deberían ser transparentes para ellos.

Por ello la importancia de un entorno de pruebas, ya que al menos podremos simular con cierta garantía un entorno real, y si los resultados no son los esperados, se buscará una nueva solución, pero los servicios en producción no se verán afectados. Podremos detener, borrar, reconfigurar, realizar cualquier tipo de tarea que conlleve tiempos de parada, pero como se está trabajando en un entorno de pruebas, no hay prisa, se pueden meditar tranquilamente las decisiones y las acciones a tomar, para conseguir abordar la solución al problema del mejor modo posible. Por el contrario, el disponer de un entorno de pruebas que sea similar al entorno real, en cuanto a términos de hardware se refiere, tiene un impacto en el presupuesto. Pues deberemos comprar hardware similar al utilizado en las máquinas de producción para poder reproducir de un modo más fidedigno el entorno, asegurándonos así un mayor grado de éxito en nuestras pruebas a la hora de llevar los desarrollos al entorno real y no encontrarnos son “sorpresas de última hora”.

4.2 Monitorización de servidores.

Necesidad de la monitorización de sistemas.

Los objetivos de una infraestructura de monitorización de sistemas informáticos son principalmente la prevención de incidencias y conocer el aprovechamiento de los recursos TIC disponibles. Dado que estos objetivos son importantes en cualquier organización independientemente de su tamaño, resulta evidente que toda organización debería disponer de su propio sistema de monitorización.

Software para la monitorización de sistemas.

En el mercado existe una amplia variedad de productos para la monitorización de recursos TIC. Podemos distinguir fundamentalmente en dos grupos: aquellos cuya licencia es de código libre (open source) y las soluciones comerciales.

Las alternativas que se van a valorar son:

- En solución de código libre: Nagios y Zabbix.
- En solución comercial: OPManager y Solarwinds.

Estándares. Protocolos aplicables.

Los estándares a valorar son la autenticación de usuarios, servidores web y servicios de red.

Autenticación de usuarios.

La autenticación es el acto de establecimiento o confirmación de algo o alguien como genuino. La autenticación de un objeto puede significar la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad.

Disponemos de cuatro mecanismos principales para realizar la autenticación que detallaremos a continuación viendo sus posibles ventajas e inconvenientes a la hora de aplicarlos en un entorno corporativo:

- Autenticación local de sistema operativo.
- Autenticación local de aplicación.
- Active Directory.
- LDAP.

Autenticación local de sistema operativo.

La autenticación del sistema operativo (SO) o local es un método para identificar a un usuario individual con credenciales suministradas por el sistema operativo del equipo del usuario. Estas credenciales pueden ser la contraseña del SO o pueden incluir certificados digitales en el equipo del usuario.

En un entorno corporativo, donde se comparten recursos y disponemos de un elevado número de estaciones de trabajo, resulta una opción poco aconsejable, ya que, la administración de los usuarios locales de cada sistema se complica en exceso. Cada equipo tendría una lista con los usuarios permitidos, contraseñas y descripción del nivel de acceso (usuario limitado, invitado, administrador).

Dada la cantidad de los usuarios a gestionar, necesitamos algún sistema centralizado en el que la gestión de usuarios sea más ágil, flexible, segura y confiable.

Autenticación local de aplicación.

Hace referencia al sistema de autenticación intrínseco de la aplicación. Es la propia aplicación la encargada de verificar el usuario y contraseña consultando su propio almacén de identidades.

LDAP (Lightweight Directory Access Protocol).

El protocolo LDAP es una evolución del protocolo DAP (Directory Access Protocol) que se utilizaba para acceder a los servicios de directorio X.500 por OSI. Como este acceso era muy costoso se realizó una implementación que mejoraba la implementación original DAP, en este momento es cuando nace LDAP, una versión más ligera para el acceso a estructuras de directorio utilizando el protocolo TCP/IP.

Podemos encontrar implementaciones no propietarias de éste protocolo como por ejemplo OpenLDAP.

El Protocolo Ligero de Acceso a Directorios, hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos a la que pueden realizarse consultas. Permite disponer de manera centralizada todos los usuarios con sus contraseñas, facilitando así el trabajo de los administradores.

Active Directory.

Es una solución propietaria por parte de Microsoft, siendo una modificación del protocolo LDAP. Proporciona la capacidad de establecer un único inicio de sesión y un depósito central de información para toda la infraestructura, lo que simplifica ampliamente la administración de usuarios y equipos y proporciona una obtención de acceso superior a los recursos en red.

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Active Directory permite a los administradores establecer políticas a nivel de empresa a los equipos mediante políticas de grupo (fondo corporativo, página por defecto del navegador, scripts de inicio de sesión, despliegue de aplicaciones etc).

Active Directory podemos entenderlo como una base de datos centralizada y organizada en la que podemos almacenar entre otros objetos, los nombres de los usuarios, contraseñas, cargo en la empresa, dirección, teléfono...

El AD proporciona información sobre los objetos, los organiza, controla el acceso y establece la seguridad.

Los objetos se pueden clasificar en tres grandes categorías: recursos, servicios, y usuarios.

Por ejemplo para el acceso a recursos de almacenamiento compartidos podemos definir grupos en Active Directory, otorgándoles cierto nivel de privilegios (lectura y/o escritura) y como miembro de éste grupo podemos incluir otro grupo, en el cual tendremos a los usuarios. De éste modo dispondremos de un grupo para definir el nivel de acceso al recurso y por otro tendremos otro grupo en el que definiremos los usuarios que podrán acceder a dicho recurso.

Active directory realmente no es un estándar, sino que debido a su amplio uso en los entornos corporativos lo ha hecho que sea considerado como tal. Debido a que es un protocolo propietario, tiene costes de licenciamiento. Por cada usuario que utilice los servicios proporcionados por Active directory deberemos adquirir una licencia CAL (Client Access License). Pero también debido a las modificaciones internas introducidas por Microsoft, hace que se aleje del estándar LDAP, provocando así posibles incompatibilidades a la hora de acceder a los servicios de directorio desde diversas aplicaciones que utilizan el protocolo LDAP estándar.



Servidores Web.

Un servidor web es un ordenador remoto que proporciona los datos solicitados por parte de los navegadores de otros ordenadores. La información se almacena en páginas web y a través del protocolo HTTP, el servidor la entrega atendiendo a las peticiones formuladas por los navegadores de los clientes utilizando el protocolo HTML.

LAMP.

LAMP es el acrónimo de Linux, Apache, MySQL, PERL / Python / PHP. El término hace referencia al sistema creado por la conjunción de esas aplicaciones de código libre. Este grupo de aplicaciones habitualmente es usado para crear servidores web.

LAMP proporciona a los desarrolladores los elementos básicos para un servidor web: un sistema operativo (Linux), un sistema gestor de base de datos (MySQL), un software para servidor web (Apache) y un software de programación (PHP, Python, PERL).

LAMP se ha convertido un estándar para servidores web pues es de código libre y no se necesita pagar ningún tipo de licencia.

WAMP.

WAMP es el acrónimo de Windows, Apache, MySQL, PERL / Python / PHP. El término hace referencia al sistema creado por la conjunción de esas aplicaciones de código libre junto con un sistema operativo de Microsoft (Windows).

WAMP proporciona a los desarrolladores los elementos básicos para un servidor web: un sistema operativo (Windows), un sistema gestor de base de datos (MySQL), un software para servidor web (Apache) y un software de programación (PHP, Python, PERL).

El principal inconveniente de ésta solución es la utilización de un sistema operativo propietario, pues deberemos pagar el coste de la licencia para poder utilizarlo.

IIS.

IIS es el acrónimo de Internet Information Services, un software propietario de Microsoft para servidores web en plataformas Windows.

Servicios de Red

Los servicios de red son configurados en redes para asegurar la seguridad y el acceso a los recursos disponibles. Las redes locales corporativas usan servicios de red como DNS (Domain Name System) para realizar las traducciones de un nombre a una dirección IP, y DHCP para la configuración dinámica de dispositivos conectados a la red, esto facilita enormemente el proceso de configuración de red para los administradores.

DNS

Domain Name System o DNS es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en direcciones IP asociadas con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

DHCP

Dynamic Host Configuration Protocol o DHCP es un protocolo de red que permite a los equipos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Estándares y protocolos a utilizar.

Tras la exposición anterior, los protocolos y estándares seleccionados son: autenticación local a nivel de aplicación, servidor LAMP y el protocolo DNS.

Elegimos autenticación local a nivel de aplicación porque como se trata de un sistema de monitorización, éste debe ser independiente de cualquier mecanismo externo que sea susceptible de fallo para validar las credenciales. Si utilizáramos una autenticación basada en LDAP o Active Directory, en caso de que el servidor se encuentre no disponible, no podríamos verificar nuestras credenciales y por tanto no podríamos acceder a la aplicación.

La elección de un servidor LAMP se fundamenta principalmente por el buen funcionamiento de estos sistemas y por su coste, mucho menor que cualquier otro servidor web.

La herramienta hará uso del protocolo DNS para la resolución de nombres, ya sea para servidores o sitios web a monitorizar y para la búsqueda de actualizaciones del sistema operativo y de la propia aplicación.

Descartamos el uso de DHCP en el servidor ya que no nos interesa que la dirección IP varíe, ya que dificultaría la comunicación agente-servidor, por tanto utilizaremos una dirección IP estática.

Comparativa: Soluciones de código libre.

Zabbix	Nagios
A favor:	A favor:
<p>Soporta los principales protocolos (POP3, SMTP, SNMP, MySQL, HTTP, FTP, SSH, etc)</p> <p>Alertas vía email , sms y mensajería instantanea</p> <p>Varios niveles de criticidad en la alerta</p> <p>Interfaz web muy potente y dinámica</p> <p>Agentes disponibles para varias plataformas</p> <p>Cualquier elemento monitorizado puede ser visualizado y comparado</p> <p>Se puede monitorizar varios elementos en aplicaciones web simultáneamente (latencia, velocidad, ...)</p> <p>Existencia de plantillas predefinidas</p> <p>Monitorización de archivos de registro del servidor</p> <p>Panel principal personalizable</p> <p>Se pueden crear nuevas plantillas, servicios</p> <p>Informes de SLA (Service Level Agreement)</p>	<p>Soporta los principales protocolos (POP3, SMTP, SNMP, MySQL, HTTP, FTP, SSH, etc)</p> <p>Alertas vía email , sms</p> <p>Varios niveles de criticidad en la alerta</p> <p>Monitorización de contenidos web</p>
En contra	En contra
<p>Es complejo de configurar</p> <p>En algunos casos la documentación es algo escasa</p> <p>Utiliza una base de datos para almacenar los elementos monitorizados</p>	<p>Interfaz web poco potente</p> <p>Nativamente no muestra la información gráficamente, es necesario instalar plugins</p> <p>Configuración vía archivos de texto</p>

Comparativa: Soluciones comerciales.

Manage Engine: OPManger	Solarwinds: Server and Application Monitor
A favor:	A favor:
Interfaz gráfica intuitiva	Interfaz gráfica intuitiva
Herramienta de informes muy potente	Fácil de desplegar
Soporte para múltiples sistemas operativos	Soporte para múltiples sistemas operativos
No provoca una gran carga en el sistema	Plantillas predefinidas
Varias vistas seleccionables para el panel principal	Creación de scripts personalizados
En contra	En contra
Precio	Precio

Elección de la herramienta a utilizar.

Tras la exposición anterior en la que describíamos los aspectos a favor y los aspectos en contra de las soluciones a tener en cuenta, ya disponemos de criterios para poder ir seleccionando la herramienta que más se ajusta a nuestras necesidades de monitorización.

Debido principalmente al coste del licenciamiento de las soluciones comerciales, éstas quedarían descartadas por falta de presupuesto.

Ahora deberemos elegir entre las dos opciones de código libre: Zabbix o Nagios. Nos decantamos por la primera opción (Zabbix) por disponer una interfaz gráfica mucho más potente, la capacidad de generar gráficos sin la necesidad de instalar ningún paquete adicional de software, generación de informes, tendencias de los elementos monitorizados, por soportar la mayoría de plataformas disponibles en el mercado y por la capacidad de notificación de alertas. Pero el motivo de mayor peso para la elección de Zabbix como sistema de monitorización es por el buen soporte para la monitorización de sistemas Windows, puesto que la mayoría de nuestros servidores utilizan sistemas operativos de Microsoft y la posibilidad de realizar toda la configuración vía interfaz gráfica, cosa que no es posible con la solución de Nagios, pues para realizar la configuración es necesario editar archivos de texto.



Utilizando Zabbix.

Vamos a utilizar Zabbix para monitorizar los servidores corporativos (junto con sus servicios) y las webs corporativas, que no se encuentran alojadas en nuestras instalaciones, sino que se dispone de un servicio de hosting, así en caso de que alguno de los servicios no esté funcionando correctamente, se nos enviará una notificación por correo electrónico.

Para el caso de los servidores, utilizaremos lo que en Zabbix se llama ítems, que no son más que los elementos a monitorizar. Podemos utilizar los que ya se encuentran predefinidos en las plantillas que incorpora de serie la herramienta y también, en caso necesario, podemos agregar nuevos ítems para que sean monitorizados. Todos los ítems, ya sean nuevos o existentes en una plantilla, se pueden personalizar, permitiendo cambiar por ejemplo la periodicidad con la que se obtienen las lecturas de los elementos monitorizados y el tiempo que deseamos almacenarlos en la base de datos.

Para poder monitorizar los servidores y sus respectivos servicios, deberemos instalar el agente correspondiente a la plataforma a monitorizar. Por defecto utiliza el puerto 10050 TCP para las comunicaciones entre el agente y el servidor. Los elementos a monitorizar son uso de CPU, memoria RAM, espacio libre, tamaño de archivo de paginación, y el estado de los servicios que proporciona el servidor.

Para el caso de las webs corporativas, vamos a monitorizar el tiempo de respuesta, la velocidad de descarga por segundo y el código de respuesta HTTP obtenido al realizar la petición.

A continuación mostraremos algunas capturas sobre la creación de nuevos ítems a monitorizar, servidores monitorizados, gráfico de la información monitorizada para un servidor en concreto, y por último la monitorización web.

The screenshot displays the Zabbix web interface. At the top, there is a navigation menu with tabs for Monitoring, Inventory, Reports, Configuration, and Administration. Below this is a secondary menu with options like Dashboard, Overview, Web, Latest data, Triggers, Events, Graphs, Screens, Maps, Discovery, and IT services. The main content area is titled 'PERSONAL DASHBOARD' and is divided into several sections:

- Left sidebar:** Contains 'Favourite graphs' (with links to CPU utilisation, Disk usage, Network utilisation, Used disk space, and Zabbix performance) and 'Favourite screens' (listing various server groups like svrBES, svrCAS, svrCAU, svrCCSS, svrDC00, svrDCA, svrDCB, svrDosimetría, svrEclai, svrEpo, svrExch01, svrFileWebServer, svrFS01, and svrFTMG).
- Status of Zabbix:** A table showing overall system health.

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (monitored/not monitored/templates)	75	21 / 4 / 50
Number of items (monitored/disabled/not supported)	922	544 / 187 / 191
Number of triggers (enabled/disabled)[problem/unknown/ok]	291	224 / 67 [2 / 23 / 199]
Number of users (online)	2	2
Required server performance, new values per second	1.33	-
- System status:** A table showing the status of different host groups.

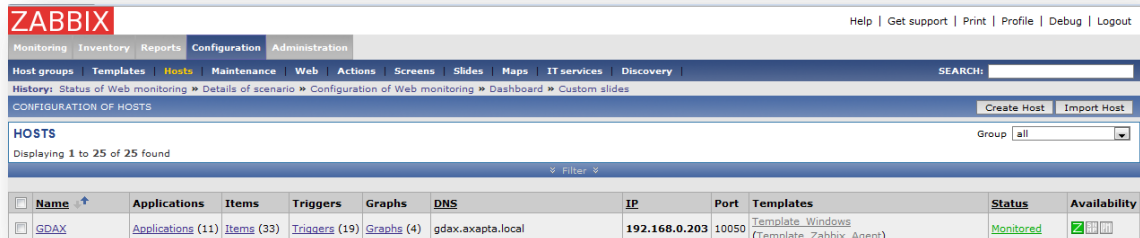
Host group	Disaster	High	Average	Warning	Information	Not classified
Linux servers	0	0	0	0	0	0
Webs Corporativas	0	0	0	0	0	0
Windows servers	0	0	2	0	0	0
Zabbix servers	0	0	0	0	0	0
- Host status:** A table showing the status of individual hosts.

Host group	Without problems	With problems	Total
Linux servers	1	0	1
Webs Corporativas	1	0	1
Windows servers	17	2	19
Zabbix servers	1	0	1

La imagen anterior muestra el panel principal, donde podemos ver a modo de resumen el estado de los servicios monitorizados. En verde se encuentran aquellos elementos en los que no hay ningún problema, mientras que en rojo se destacan aquellos elementos que tienen problemas.

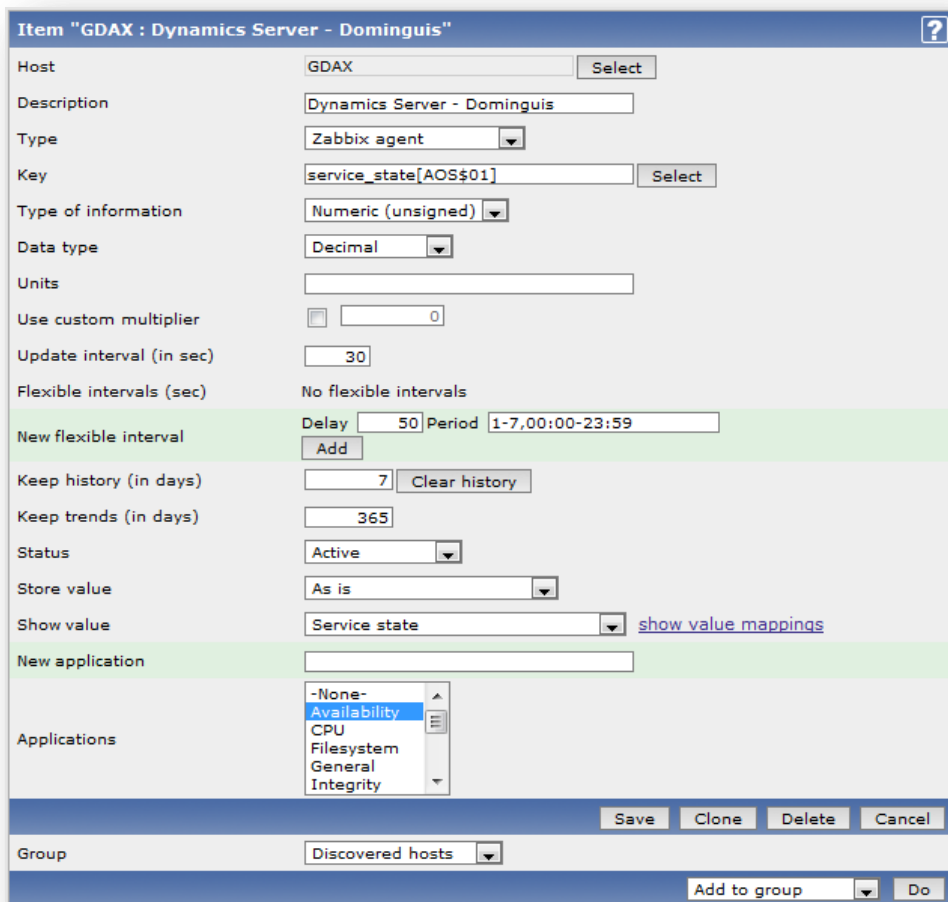
Aplicación de soluciones libres a una empresa TIC

En la siguiente imagen, podemos apreciar en un host que se encuentre monitorizado las aplicaciones, items, triggers y gráficos que tiene asignados a demás de su nombre FQDN (Fully Qualified Domain Name), dirección IP, plantillas asignadas y el estado de la monitorización (activada o desactivada).



Name	Applications	Items	Triggers	Graphs	DNS	IP	Port	Templates	Status	Availability
GDAX	Applications (11)	Items (33)	Triggers (19)	Graphs (4)	gdax.axapta.local	192.168.0.203	10050	Template_Windows (Template_Zabbix_Agent)	Monitored	<input checked="" type="checkbox"/>

En la siguiente captura, se aprecia la creación un ítem nuevo para ser monitorizado. En este caso se trata del estado del servicio de Microsoft Dynamics Axapta. El servicio a monitorizar se llama AOS\$01, y el tipo de información que vamos a obtener es un entero que nos indicará si el servicio está en ejecución o por el contrario está detenido.



Item "GDAX : Dynamics Server - Dominguis"

Host: GDAX [Select]

Description: Dynamics Server - Dominguis

Type: Zabbix agent

Key: service_state[AOS\$01] [Select]

Type of information: Numeric (unsigned)

Data type: Decimal

Units: []

Use custom multiplier: [0]

Update interval (in sec): 30

Flexible intervals (sec): No flexible intervals

New flexible interval: Delay 50 Period 1-7,00:00-23:59 [Add]

Keep history (in days): 7 [Clear history]

Keep trends (in days): 365

Status: Active

Store value: As is

Show value: Service state [show value mappings]

New application: []

Applications: [Availability]

Group: Discovered hosts [Add to group] [Do]

[Save] [Clone] [Delete] [Cancel]

Una vez que ya tenemos el ítem a monitorizar, deberemos crear un disparador o trigger, para que en caso de que el servicio no esté en ejecución se envíe una notificación a los miembros del departamento de TI.

La condición para que se active el disparador es el resultado de la lectura del ítem. El valor 0 indica que el servicio está en ejecución, mientras que un valor distinto de 0 indica que el servicio está detenido.

Trigger "Dynamics Server - Dominguis"

Name: Dynamics Server - Dominguis

Expression (Toggle input method): {GDAX:service_state[AOS\$01].last(0)}#0

The trigger depends on: No dependencies defined

New dependency: Add

Event generation: Normal

Severity: High

Comments: El servicio Dynamics - Dominguis está detenido.

URL:

Disabled:

Buttons: Save, Clone, Delete, Cancel

Aplicación de soluciones libres a una empresa TIC

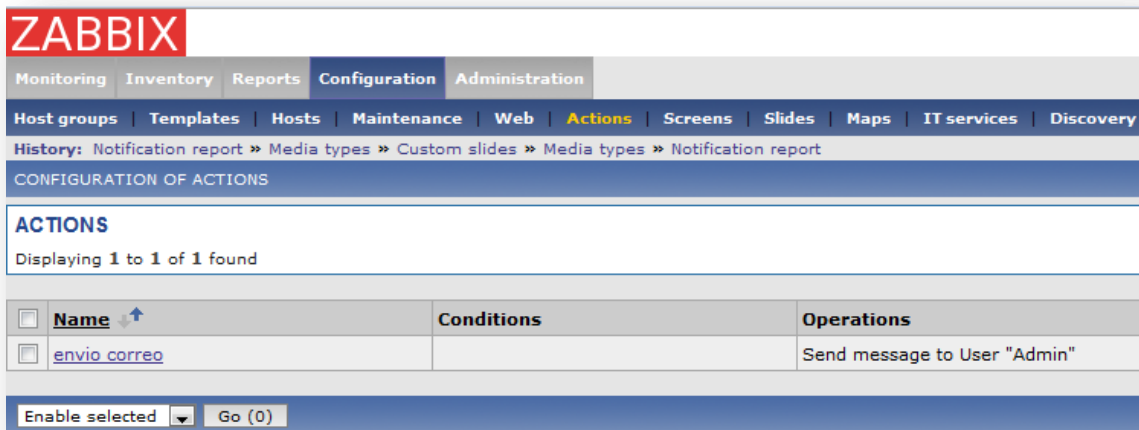
Detalle de los triggers aplicados al servidor GDAX (servicio de Microsoft Dynamics Axapta), uso de CPU, memoria RAM total y disponible, unidades de almacenamiento indicando su espacio total y disponible.

TRIGGERS			
Displaying 1 to 19 of 19 found			
Hosts list	Applications (11)	Items (33)	
		Graphs (4)	
		Host: GDAX	
		DNS: gdx.axapta.local	
<input type="checkbox"/>	Severity	Status	Name
<input type="checkbox"/>	Average	Disabled	Template_Windows:c:\autoexec.bat has been changed on server {HOSTNAME}
<input type="checkbox"/>	High	Disabled	Dynamics Server - Desarrollo
<input type="checkbox"/>	High	Enabled	Dynamics Server - Dominquis
<input type="checkbox"/>	High	Disabled	Dynamics Server - Pruebas
<input type="checkbox"/>	Average	Disabled	Template_Windows:Host information was changed on {HOSTNAME}
<input type="checkbox"/>	Average	Enabled	Template_Windows:Lack of free memory on server {HOSTNAME}
<input type="checkbox"/>	Average	Enabled	Template_Windows:Lack of free swap space on {HOSTNAME}
<input type="checkbox"/>	Average	Enabled	Template_Windows:Low free disk space on {HOSTNAME} volume c:
<input type="checkbox"/>	Average	Enabled	Template_Windows:Low free disk space on {HOSTNAME} volume d:
<input type="checkbox"/>	Average	Enabled	Template_Windows:Low free disk space on {HOSTNAME} volume e:
<input type="checkbox"/>	Average	Enabled	Template_Windows:Low free disk space on {HOSTNAME} volume f:
<input type="checkbox"/>	Average	Enabled	Template_Windows:Low free disk space on {HOSTNAME} volume T:
<input type="checkbox"/>	Average	Enabled	Template_Windows:Low free disk space on {HOSTNAME} volume X:
<input type="checkbox"/>	Average	Enabled	Template_Windows:Processor load is too high on {HOSTNAME}
<input type="checkbox"/>	Average	Enabled	Template_Windows:Server {HOSTNAME} is unreachable
<input type="checkbox"/>	High	Disabled	Template_Zabbix_Agent:Server {HOSTNAME} is unreachable for 3 minutes
<input type="checkbox"/>	Average	Enabled	Template_Windows:Too many processes on {HOSTNAME}

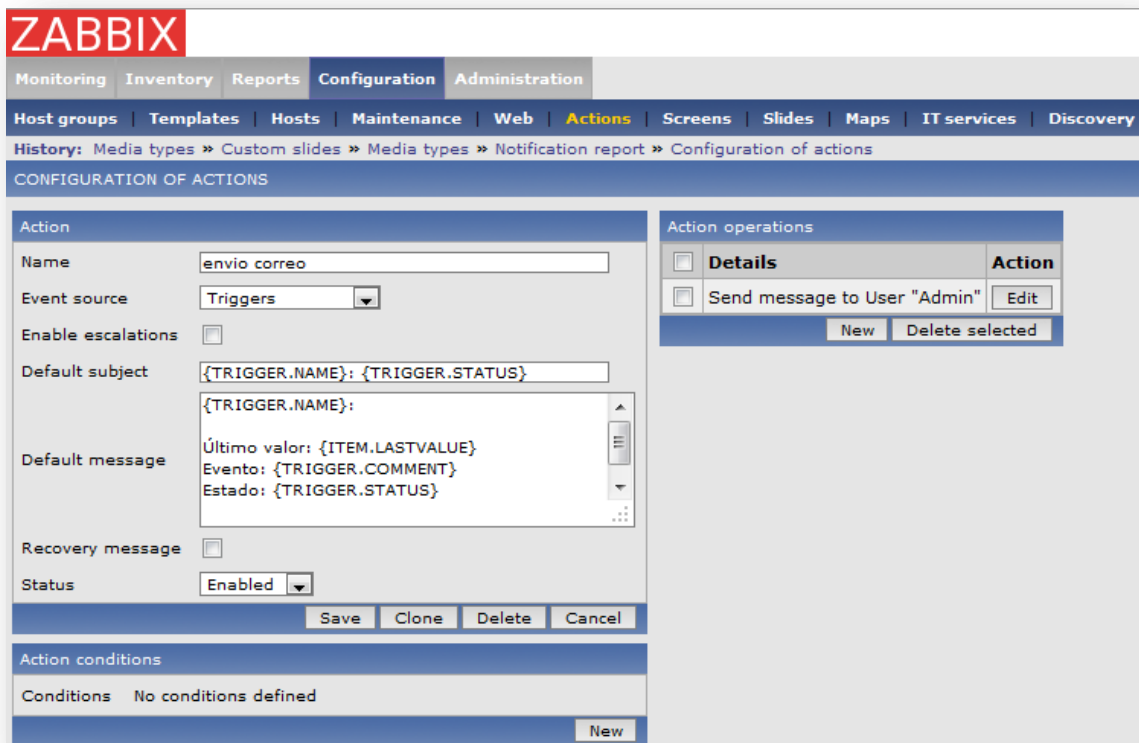
Detalle de las condiciones de los triggers.

Group		all	Host	GDAX
[Hide disabled triggers]				
IP:	192.168.0.203	Port:	10050	Status: Monitored
				Availability: Available
	Expression	Error		
	{GDAX:vfs.file.cksum[c:\autoexec.bat].diff(0)}>0	✘		
	{GDAX:service_state[AQS\$02].last(0)}#0	✔		
	{GDAX:service_state[AQS\$01].last(0)}#0	✔		
	{GDAX:service_state[AQS\$03].last(0)}#0	✔		
	{GDAX:system.uname.diff(0)}>0	✘		
	{GDAX:vm.memory.size[free].last(0)}<10000	✔		
	{GDAX:system.swap.size[free].last(0)}<100000	✔		
	{GDAX:vfs.fs.size[c;free].last(0)}<1073741824	✔		
	{GDAX:vfs.fs.size[d;free].last(0)}<1073741824	✘		
	{GDAX:vfs.fs.size[e;free].last(0)}<1073741824	✔		
	{GDAX:vfs.fs.size[f;free].last(0)}<1073741824	✔		
	{GDAX:vfs.fs.size[t;free].last(0)}<1073741824	✔		
	{GDAX:vfs.fs.size[x;free].last(0)}<1073741824	✔		
	{GDAX:system.cpu.load[avg1].last(0)}>45	✔		
	{GDAX:status.last(0)}=2	✔		
	{GDAX:agent.ping.nodata(3m)}=1	✔		
	{GDAX:proc.num[]}.last(0)>300	✔		

Una vez que disponemos de los disparadores, deberemos asociar la activación de los disparadores con la notificación por correo electrónico del evento en cuestión. Para ello crearemos la acción “Envío correo”.

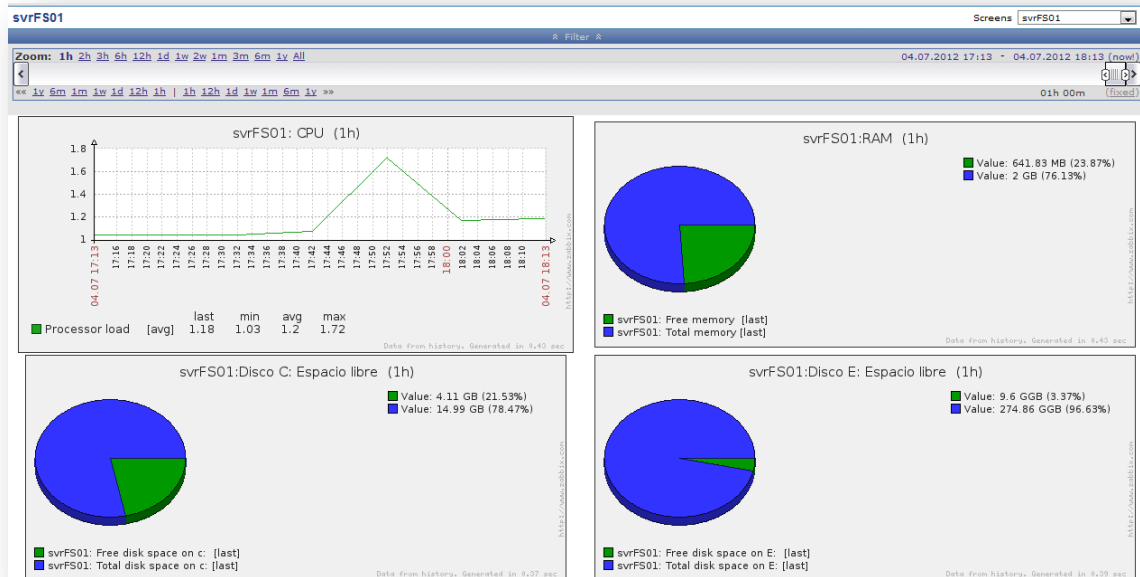


En la acción “Envío correo”, definiremos el asunto del correo, en este caso pondremos el nombre del disparador y su estado. En el cuerpo del mensaje informaremos del último valor obtenido en la lectura, el evento y su estado.



Aplicación de soluciones libres a una empresa TIC

Detalle de un gráfico obtenido a partir de los datos resultantes de la monitorización de los ítems de un servidor de ficheros en red. Podemos apreciar la carga de CPU, la memoria RAM disponible y total, y el estado de las unidades de almacenamiento, mostrando su capacidad total y su espacio disponible.



Detalle de la configuración para la monitorización de un sitio web. Podemos observar el nombre del sitio web, la frecuencia con la que tomaremos muestras (900 segundos), el agente a utilizar y por último los pasos o steps de este escenario de monitorización. En cada uno de ellos podemos apreciar el nombre, el tiempo máximo para obtener la respuesta del sitio web, la URL a la que realizar la petición y por último el estado que debemos obtener para comprobar que el sitio web está “vivo”.

The screenshot shows the configuration window for web monitoring. The 'Scenario' section is filled with the following details:

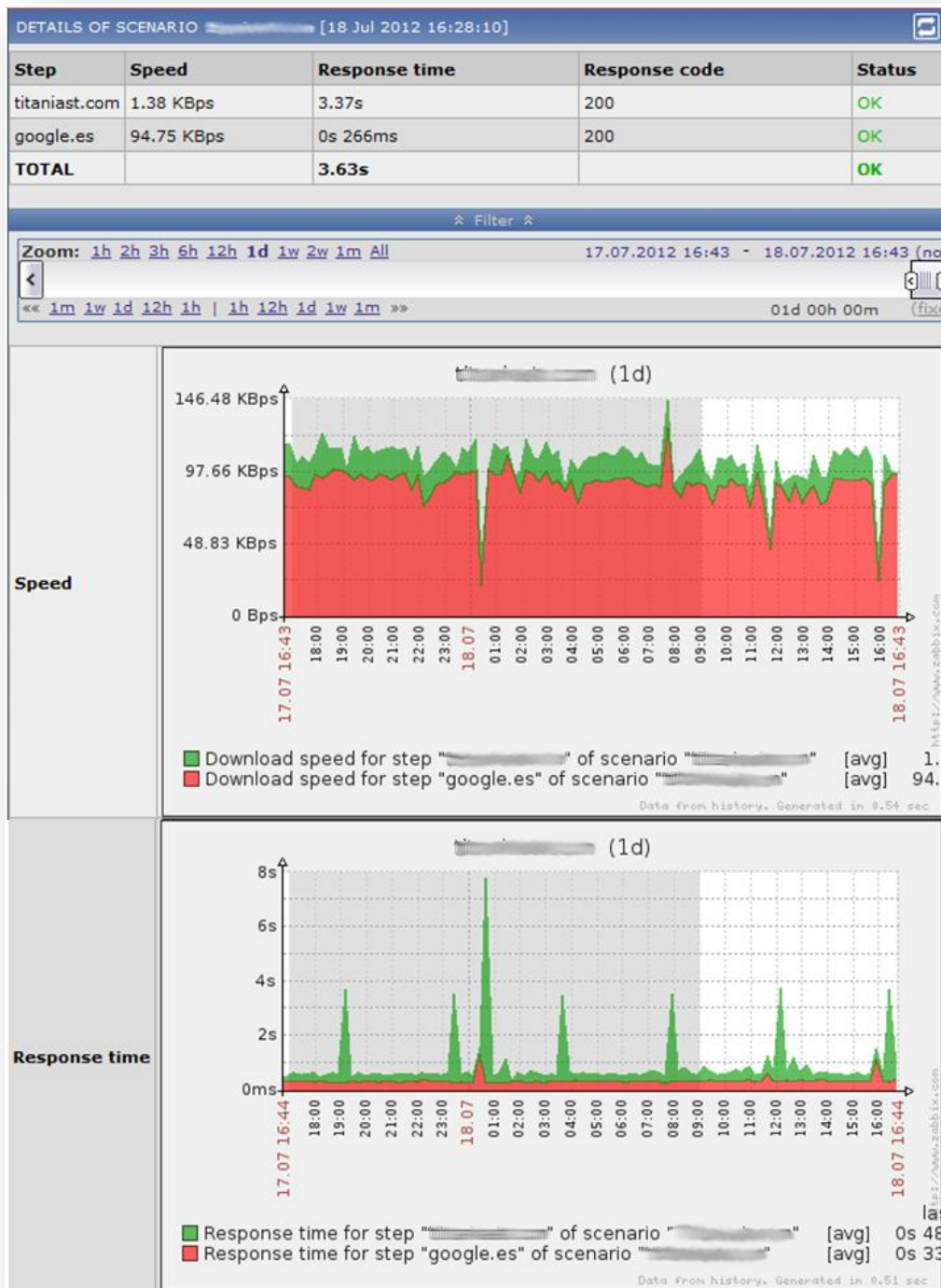
- Application:** Páginas Web
- Name:** titaniast.com
- Authentication:** None
- Update interval (in sec):** 900
- Agent:** Internet Explorer 6.0 on Windows
- Status:** Active

The 'Steps' section contains a table with the following data:

	Name	Timeout	URL	Required	Status	Sort
<input type="checkbox"/>	titaniast.com	15 sec	http://www.titaniast.com/		200	Down
<input type="checkbox"/>	google.es	15 sec	www.google.es		200	Up

Buttons at the bottom include 'Add', 'Delete selected', 'Save', 'Clone', 'Delete', and 'Cancel'.

La siguiente captura muestra el gráfico obtenido a partir de los datos recopilados de la monitorización del sitio web. Podemos apreciar la velocidad, el tiempo de respuesta y el código de respuesta obtenido. En verde se muestran coloreados los datos del sitio web que deseamos monitorizar, mientras que en rojo se muestran los de Google (<http://www.google.es>). Se monitoriza la web corporativa junto con la de Google, porque si ambas se muestran como no accesibles, probablemente tengamos un problema de conectividad hacia internet.



Conclusiones.

Resulta imprescindible disponer de un sistema de monitorización cuando se dispone de cierta cantidad de servidores, para poder conocer en cualquier momento el estado de todos los servicios proporcionados. Quedarse sin espacio de disco duro en un servidor, un servicio crítico detenido o el sitio web corporativo caído, por poner algunos ejemplos, suponen pérdidas millonarias que afectan negativamente al crecimiento del negocio y proporcionan una mala imagen tanto a nivel de empresa como conjunto, como para los responsables del buen funcionamiento de los servicios corporativos.

4.3 Planificación de proyectos.

Por qué planificar.

La planificación consiste en analizar la situación actual junto con los recursos y determinar las acciones necesarias para alcanzar un determinado fin u objetivo. Es necesario tomar decisiones para poder alcanzar nuestros objetivos, pero éstas deben tener cierto orden para poder otorgarles la importancia adecuada en el desarrollo del proyecto.

Habitualmente no se dispone de recursos infinitos para abordar un proyecto, sino que disponemos de recursos ya sean materiales o humanos limitados, por ello es necesaria una correcta planificación.

En un entorno complicado y cambiante como el escenario empresarial actual, un pilar fundamental para cualquier proyecto debería ser la planificación, ya que con ella podremos adaptarnos más fácilmente al cambio, evaluar las dificultades a las que nos enfrentamos y tomar las decisiones más adecuadas conforme a la información que disponemos.

Herramientas para la planificación de proyectos.

En el mercado existe multitud de herramientas para la planificación de proyectos. Podemos distinguir dos grupos de aplicaciones conforme a la forma en la que el usuario puede trabajar con dicha herramienta, acceso vía web o acceso local a la aplicación.

Ventajas e inconvenientes de una aplicación local Vs aplicación web.

Una aplicación local para la planificación de proyectos tiene sentido cuando el proyecto a abordar implica pocos recursos (humanos y/o materiales) y hay muy poca interacción con la planificación. Es simplemente un calendario con una serie de hitos a cumplir para seguir nuestros objetivos.

Una aplicación web proporciona a los participantes del proyecto un mayor dinamismo y flexibilidad. Tiene más sentido la utilización de este tipo de herramientas cuando necesitamos coordinar grandes recursos (humanos y/o materiales) en los que es necesaria una realimentación acerca del estado de las fases de cada proyecto y cuando son abordadas por equipos independientes, para poder conocer el avance global del proyecto a desarrollar. Todo el equipo participa en la planificación del proyecto, y todos los miembros pueden acceder al plan del proyecto, cosa imposible en una aplicación instalada en una estación de trabajo.

Por las razones anteriormente mencionadas, tipo y envergadura de proyectos a tratar, consideramos que la herramienta adecuada para la planificación de proyectos debe ser una aplicación web.



Herramientas de código libre de acceso web a valorar.

Existe un amplio abanico de soluciones web de código libre para la planificación de proyectos, nuestros posibles candidatos son [LibrePlan](#) y [Redmine](#).

Estándares. Protocolos aplicables.

Los estándares a valorar ya se han detallado anteriormente, son la autenticación de usuarios, servidores web y servicios de red.

Estándares y protocolos a utilizar.

Tras la exposición anterior, los protocolos y estándares seleccionados son: autenticación mediante Active Directory, servidor LAMP y protocolo DNS.

La organización dispone de servidores centrales dedicados a la comprobación de las credenciales de los usuarios utilizando Active Directory. Esto se traduce en una única credencial memorizada por el usuario y le proporciona el acceso a todos los servicios ofrecidos por la organización.

La elección de un servidor LAMP se fundamenta principalmente por el buen funcionamiento de estos sistemas y por su coste, mucho menor que cualquier otro servidor web.

El protocolo DNS será utilizado por el servidor para la resolución de nombres, localizando así los servidores de actualizaciones del sistema operativo y de la aplicación.

Descartamos el uso de DHCP en el servidor ya que no nos interesa que la dirección IP varíe, por ello utilizaremos una dirección IP estática.

Comparativa de soluciones de código libre.

LibrePlan	Redmine
<i>A favor:</i>	<i>A favor:</i>
Interfaz gráfica intuitiva Soporte multi empresa Herramienta de informes muy potente Notificaciones vía email Integración con LDAP Calendario y diagramas de Gantt	Soporte para múltiples proyectos Control de acceso basado en roles Integración LDAP Calendario y diagramas de Gantt
<i>En contra</i>	<i>En contra</i>
	Interfaz gráfica Facilidad de uso

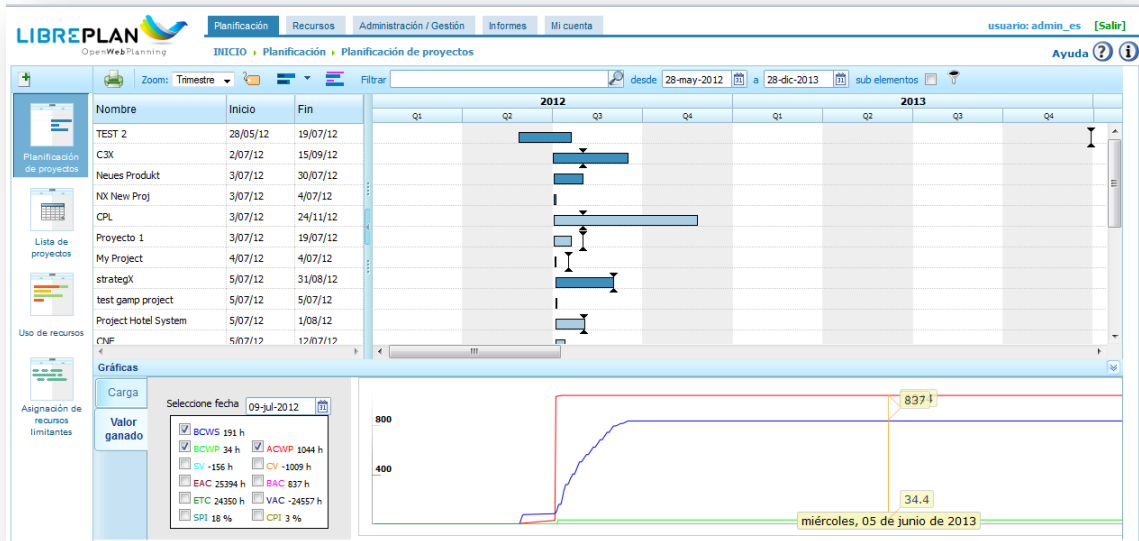
Elección de la herramienta a utilizar.

LibrePlan y Redmine son muy similares respecto a la funcionalidad que ofrecen: soporte para la planificación de múltiples proyectos, control de acceso a la aplicación basado en roles, control de tiempos, medición de progresos, representación en diagramas de Gantt y soporte para la autenticación por medio de LDAP. Pero en la facilidad de uso para el usuario final e instalación para los administradores destaca LibrePlan. Por ello nos decantaremos por esta herramienta.



Un vistazo a LibrePlan.

Vista de planificación de proyectos: en esta vista se puede ver la lista de proyectos planificados y también podremos ver el uso de recursos.



(imagen con datos ficticios)

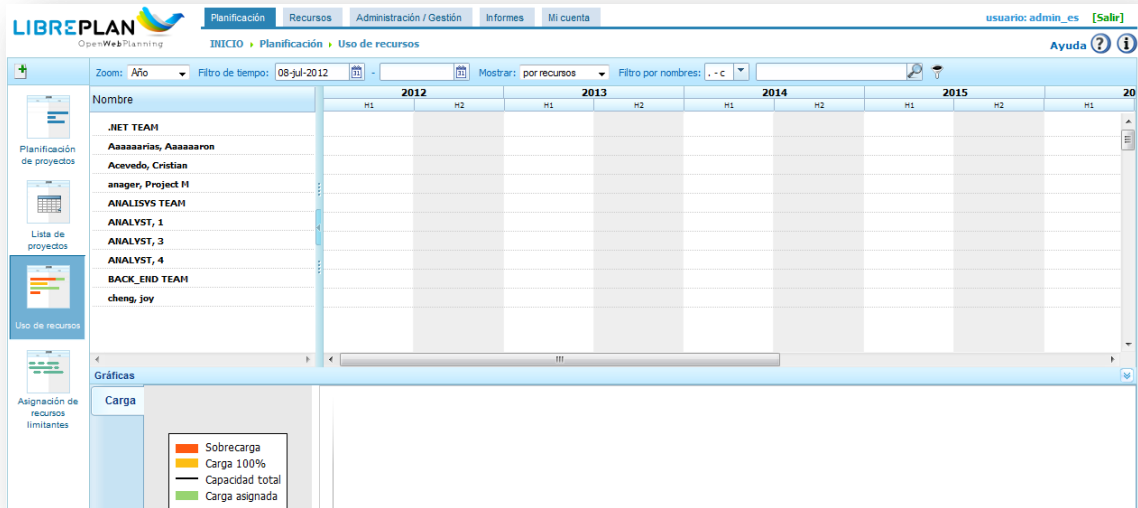
Vista lista de proyectos: en ella podemos apreciar la lista de proyectos creados en LibrePlan. Para cada uno de ellos, disponemos del nombre del proyecto, su código, fecha de inicio, fecha límite, Cliente, presupuesto total, horas y el estado.

Nombre	Código	Fecha de inicio	Fecha límite	Cliente	Presupuesto total	Horas	Estado	Operaciones
B121	ORDER00647	01/09/2012	30/06/2013		0.00	0	OFERTADO	
provame	ORDER00502	28/07/2012	28/08/2012	ING DIRECT	0.00	444	OFERTADO	
Testprojekt 1	ORDER00651	09/07/2012	31/12/2012	ING DIRECT	0.00	0	OFERTADO	
Test_lj	ORDER00649	09/07/2012	17/07/2012		0.00	0	OFERTADO	
casastoria	2012CASA	09/07/2012	08/08/2012	Microsoft	0.00	0	OFERTADO	
EVAL	ORDER00646	09/07/2012			0.00	40	OFERTADO	
AZ1	ORDER00631	09/07/2012	30/07/2012	Accenture	0.00	0	OFERTADO	
Mi	ORDER00644	08/07/2012	30/10/2012	VODAFONE GLOBAL	0.00	0	OFERTADO	
UAP\$\$	ORDER00640	08/07/2012	28/07/2012		0.00	2	OFERTADO	
NRT Test	ORDER00635	08/07/2012	14/07/2012	ING DIRECT	0.00	263	OFERTADO	
BSPLAN	ORDER00627	06/07/2012	31/08/2012		0.00	0	OFERTADO	
Mohan	ORDER00623	06/07/2012	06/06/2013	VODAFONE GLOBAL	0.00	0	OFERTADO	
brn	ORDER00620	06/07/2012	06/12/2012		0.00	0	OFERTADO	
Sewatama - PLTD Trisakti	EMS-SWT-0512	06/07/2012	06/08/2012		0.00	0	OFERTADO	
New Project	ORDER00610	06/07/2012	13/07/2012	Accenture	0.00	263	OFERTADO	

(imagen con datos ficticios)

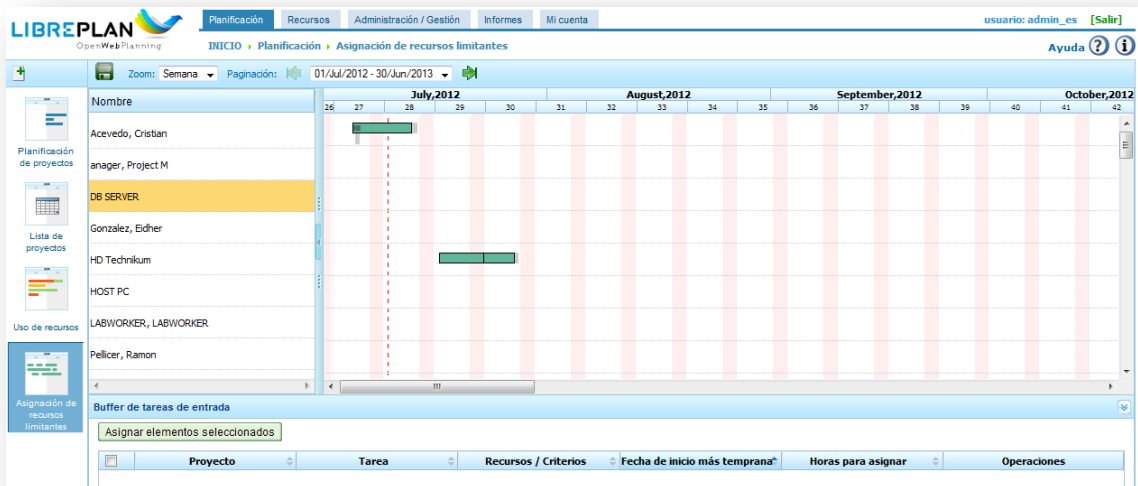
Vista uso de recursos. La aplicación gestiona dos tipos de recursos: trabajadores y máquinas. Ambos recursos son asignables específicamente a una tarea, dependiendo de las necesidades del proyecto a desarrollar.

A los recursos trabajador y recursos máquina se les puede asignar un calendario si así se decide.



(imagen con datos ficticios)

Asignación de recursos limitantes. Los recursos limitantes son un tipo especial de elementos productivos que no pueden tener más de una tarea asignada al mismo tiempo o encontrarse sobrecargados. En el gráfico podemos observar los periodos en los que los recursos se encuentran ocupados.



(imagen con datos ficticios)

Informes. LibrePlan permite la generación de informes. Existen tres tipos de informe predefinidos:

- Horas trabajadas por recurso.

Este informe permite extraer una lista de tareas y tiempo dedicado por parte de los recursos de la organización en un período de tiempo. Hay varios filtros que permiten configurar la consulta para obtener la información deseada y evitar datos superfluos.

Informe de Trabajo
Horas trabajadas por empleado

LIBREPLAN
OpenWebPlanning

Fecha de inicio: 01/05/2012 Fecha de fin: 19/07/2012

ANALYST, 1

09/07/2012

Código/Nombre tarea	Inicio	Fin	Horas	Campos de texto	Etiquetas
WDWW What do we want			8		
Horas totales por día:			8		
Horas totales por empleado:			8		

ANALYST, 3

02/07/2012

Código/Nombre tarea	Inicio	Fin	Horas	Campos de texto	Etiquetas
ORDER00478-00001 conexio			10		
Horas totales por día:			10		
Horas totales por empleado:			10		

(imagen con datos ficticios)

- Total de horas trabajadas por recurso en un mes.

Este informe permite obtener el número total de horas trabajadas por los recursos en un mes. Esto puede ser útil para calcular las horas extras hechas o la cantidad de horas que tiene que ser pagadas por recurso en un mes.

La aplicación permite registrar partes de trabajo tanto para los trabajadores como para las máquinas. Gracias al registro de los partes de trabajo, el informe en el caso de las máquinas indica las horas totales que las máquinas han estado funcionando en un determinado mes.

Informe de trabajo
Horas trabajadas por recurso en un mes

LIBREPLAN
OpenWebPlanning

Año: 2012 Mes: Julio

Nombre	Horas
ANALYST,1	8
joze, joze	500
joze2, joze2	500
ANALYST,4	10
DEV NET, Domenic	9
cheng, joy	8
ANALYST,3	10
Horas totales:	1045

(imagen con datos ficticios)

- Trabajo y progreso del proyecto.

Este informe permite mostrar cuál es el estado global de los proyectos teniendo en cuenta dos variables: el progreso y el coste. Se analiza el estado actual de progreso de un proyecto comparándolo con lo previsto de acuerdo a la planificación y al trabajo dedicado.

Informe de progreso
Planificación del progreso por proyecto

LIBREPLAN
OpenWebPlanning

Tipo de progreso: PROPAGACIÓN
Proyectos: Todo
Fecha de Referencia: 10/07/2012
Fecha inicio: 01/05/2012
Fecha fin: 10/07/2012

CNE

CNE			CNE		
Horas Totales	Estimadas	49	Horas al día	Planificadas	0
	Planificadas	0		Reales	0
Progreso	Calculado	0,05	Diferencia	Coste	0,0000
	Registrado	0,00		Planificada	0,0000
	Planificado	0,00		Proporción coste	0
				Proporción	0

(imagen con datos ficticios)

Conclusiones.

Un elemento clave para el correcto desarrollo de un proyecto y para cumplir los plazos establecidos es la planificación. Con ella y gracias a las nuevas tecnologías, disponemos de herramientas colaborativas que nos facilitan el seguimiento del proyecto. Dichas herramientas nos proporcionan un feedback sobre la situación actual y además podemos participar agregando nuestros progresos, pudiendo así cumplir con los objetivos establecidos de recursos, tiempo y coste.

4.4 Gestión de Incidencias.

Por qué gestionar incidencias de IT.

La mayoría de organizaciones están empujando a sus departamentos de IT para que éstos mejoren los niveles de servicio y mantengan unos entornos complejos. El centro de atención al usuario no puede seguir trabajando de manera reactiva “apagando fuegos” según surjan problemas, sino que deben transformarse para adquirir una pro actividad y ser percibido como un recurso de valor añadido e imprescindible en cualquier organización. Es por ello por lo que surge la necesidad de una aplicación para la gestión de incidencias, que gestione las mismas desde su creación hasta su resolución.

Herramientas para la gestión de incidencias a valorar.

Existe una gran cantidad de software dedicado a ayudar a los departamentos de IT para gestionar las incidencias a las que se enfrentan a diario. Disponemos tanto soluciones comerciales como soluciones de código libre, en las que en ambas, dispondremos de un servidor donde se encontrará instalada la aplicación junto con una base de datos para almacenar los tickets generados, ya sea por parte de los clientes, utilizando una interfaz web tipo kiosco, o por el personal del propio departamento.

Una de las soluciones comerciales más destacables es [ServiceDesk Plus](#). Se trata de una solución completa, que soporta la autenticación de usuarios mediante LDAP, gestión de tickets, SLA (Acuerdos de Nivel de Servicio), inventario de estaciones de trabajo a nivel de software y hardware, informes y bases de conocimiento.

Dentro de las soluciones open source, podemos encontrar [OTRS](#) y [osTicket](#) entre otras muchas soluciones, pero en el caso de OTRS se trata de una solución mucho más potente que osTicket, puesto que soporta la adición de plugins que nos proporcionarán el enriquecimiento de la aplicación, gestión de incidencias, integración con LDAP, base de conocimiento, encuestas, catálogos de servicio, SLA e informes.

Estándares. Protocolos aplicables.

Los estándares a valorar ya se han detallado anteriormente, son la autenticación de usuarios, servidores web y servicios de red.

Estándares y protocolos a utilizar.

Tras la exposición anterior, los protocolos y estándares seleccionados son: autenticación mediante Active Directory, servidor LAMP y protocolo DNS.

La organización dispone de servidores centrales dedicados a la comprobación de las credenciales de los usuarios utilizando Active Directory. Esto se traduce en una única credencial memorizada por el usuario y le proporciona el acceso a todos los servicios ofrecidos por la organización.

La elección de un servidor LAMP se fundamenta principalmente por el buen funcionamiento de estos sistemas y por su coste, mucho menor que cualquier otro servidor web.

El protocolo DNS será utilizado por el servidor para la resolución de nombres, localizando así los servidores de actualizaciones del sistema operativo y de la aplicación.

Descartamos el uso de DHCP en el servidor ya que no nos interesa que la dirección IP varíe, por ello utilizaremos una dirección IP estática.

Comparativa de herramientas para la gestión de incidencias.

ServiceDesk Plus	OTRS	osTicket
<i>A favor:</i>	<i>A favor:</i>	<i>A favor:</i>
Integración con LDAP	Integración con LDAP	Gestión de tickets
Gestión de tickets	Gestión de tickets	Coste
Definición de SLA	Definición de SLA	
Horas dedicadas por incidencia	Horas dedicadas por incidencia	
Inventario de equipos	Bases de conocimiento	
Bases de conocimiento	Personalización	
Informes	Disponibilidad de plugins	
	Informes personalizados	
	Coste	
<i>En contra</i>	<i>En contra</i>	<i>En contra</i>
Coste (solución comercial)		Autenticación local
		Escasa funcionalidad

Elección de la herramienta.

Debido al coste de licenciamiento, la solución comercial ServiceDesk Plus, queda descartada y entre las soluciones open source elegimos la opción de OTRS, puesto que nos proporciona mucha más funcionalidad que osTicket.



Un vistazo a OTRS.

Página principal para los técnicos de IT. En la sección central podemos apreciar los tickets escalados, los tickets nuevos y los tickets abiertos. En la sección derecha podemos apreciar un gráfico con las incidencias creadas (línea azul) y las incidencias cerradas (línea marrón), los eventos entrantes (incidencias) y los técnicos en línea en ese preciso momento.

- Opción Tickets: podremos crear incidencias nuevas.
- Opción FAQ: se accede a la sección de preguntas frecuentes.
- Opción Encuesta: genera/muestra las encuestas.
- Opción Estadísticas: genera/muestra las estadísticas de la aplicación.
- Opción Clientes: accedemos al listado de clientes de la aplicación.
- Opción Administrar: permite cambiar opciones de configuración de la aplicación.
- Opción buscar: permite realizar una búsqueda de un ticket conforme a varios criterios.

Detalle de la generación de un ticket. En cada uno de ellos se establece el cliente, y se asocia a la cola de incidencias, se selecciona el servicio con el que se puede categorizar la incidencia, se establece el propietario (técnico responsable del caso) y por último se establece el asunto y el texto con la descripción de la incidencia.

Create New Phone Ticket

* Tipos: default

* To queue: Incidencias

Servicio: Email

Acuerdo de Nivel de Servicio: -

Propietario: rodriguez antonio (a.rodriguez)

* Asunto: Bloquear Spam

Opciones: [Cliente] [FAQ]

* Texto:

Ha recibido correo basura en su buzón de correo.
Bloquear esas direcciones en el antispam.

Una vez que el ticket ha sido creado, se notifica al técnico por correo electrónico la creación de la incidencia que está a la espera de resolución.

Detalle del cierre de un ticket. Para poder cerrar una incidencia deberemos rellenar el texto con la resolución de la misma, seleccionaremos el estado “Cierre OK” si ha sido satisfactorio o por el contrario “Cierre KO” si no hay solución posible, por ultimo estableceremos las unidades de tiempo dedicadas a la resolución de la incidencia.

The image shows a web form for closing a ticket. It includes the following elements:

- *Asunto:** A text input field containing the word "Cerrar".
- Opciones:** A dropdown menu showing "[FAQ]".
- *Texto:** A rich text editor with a toolbar (bold, italic, underline, strikethrough, bulleted list, numbered list, link, unlink, image, undo, redo, print) and a text area containing the text "Direcciones bloqueadas satisfactoriamente el en antisпам."
- Anexo:** A text input field for attachments, with an "Examinar..." button next to it.
- Tipo de nota:** A dropdown menu set to "nota-interna".
- iente estado:** A dropdown menu set to "3-Cierre OK".
- es de tiempo s de trabajo):** A text input field containing "0.3".
- Enviar:** A button at the bottom of the form.

Detalle de la cola de tickets abiertos. En ella podemos apreciar el número de ticket, el título, el usuario que requiere asistencia, la antigüedad, la fecha de creación, el propietario (técnico asociado a la incidencia), el estado, la empresa y el servicio o categoría al que pertenece.

Status View: Open tickets

Open tickets 31 | Closed tickets 513

Ticket#	De	Antigüedad	Cola	Empresa	Tiempo para Primera Respuesta
2012071010000123 – Email extracto de visa no le llega a Juan Garcia	c.fernandez.lyM	2 h 28 m	Incidencias	lyM	50 h 31 m / 12/07/2012 - 18:25
2012071010000098 – inhabilitar la directiva que conecta la unidad comun	s.saez	5 h 35 m	Incidencias	Herramientas de Gestión Co[.]	46 h 24 m / 12/07/2012 - 14:18
2012070910000055 – Backup para CNT	a.martinez.LAI	1 d 6 h 18 m	Incidencias	LAI	21 h 41 m / 11/07/2012 - 13:35

Detalle de la herramienta de búsqueda. Permite localizar tickets seleccionando un criterio de búsqueda entre los disponibles: número de ticket, propietario, cliente, asunto...

Buscar

Plantilla de búsqueda: - ▾

Crear Nueva

Texto Completo:

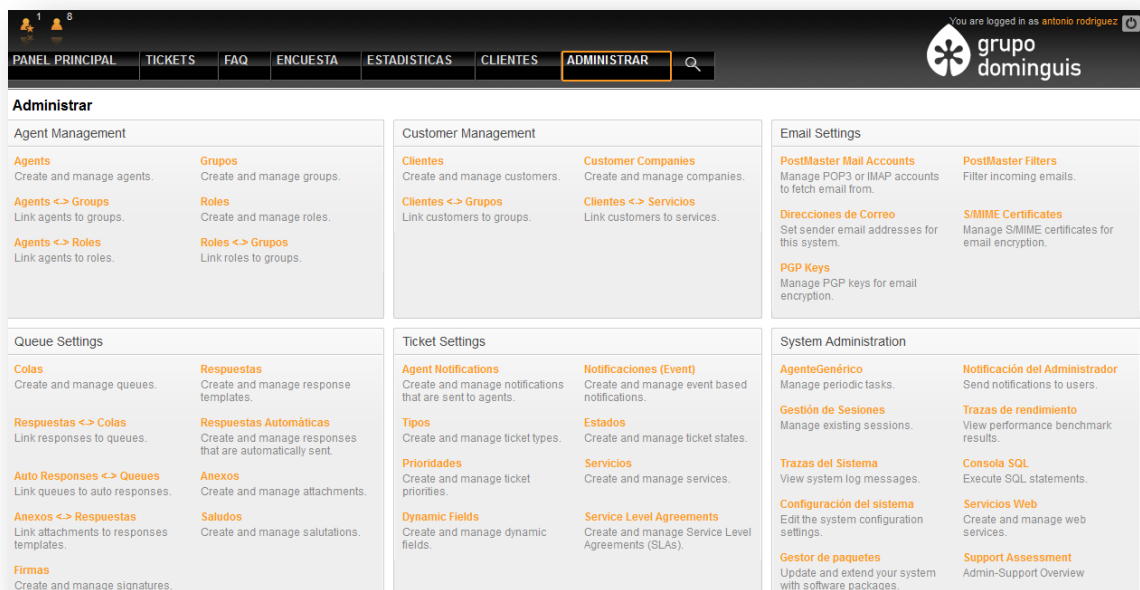
Agregar otro atributo: Ticket Número ▾

Formato de Resultados: Normal ▾

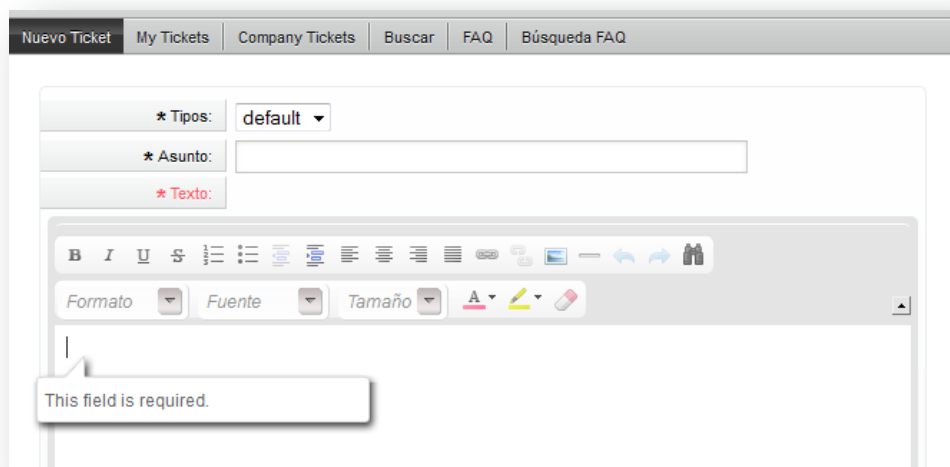
Run search

Detalle del panel de administración. Desde ésta sección se pueden controlar todos los aspectos de funcionamiento de OTRS:

- Agent Management: para la gestión de técnicos y grupos.
- Customer Management: para la gestión de clientes.
- Email settings: para la configuración y opciones de correo electrónico.
- Queue Settings: para la configuración de las colas de incidencias.
- Ticket Settings: para la configuración de los tickets.
- System Administration: todo lo relacionado con la configuración general del sistema.



Creación de un ticket desde la interfaz de cliente. El proceso es muy similar al que se ha visto anteriormente, sólo hay que rellenar el asunto, y el cuerpo de la incidencia. Como nos encontramos en la sesión de un cliente, disponemos de muchas menos opciones que las disponibles en la sesión de un técnico.



Conclusiones.

Cuando se dispone de una cantidad elevada de usuarios, resulta bastante útil hacer uso de una herramienta para la gestión de incidencias. Es muy habitual tener varios tipos de incidencias categorizadas, pero un elemento muy importante es la prioridad de la incidencia. Ya que no es lo mismo una incidencia creada por un usuario que no puede trabajar porque su ordenador ha dejado de funcionar, que una incidencia de un usuario que pide ayuda porque no sabe cómo utilizar el corrector ortográfico de un programa de autoedición. Con ello se definen las prioridades que nos ayudaran a atender aquellas solicitudes que sean más críticas antes de las que tienen una menor importancia.

Muy destacable es la capacidad de trazabilidad o seguimiento de una incidencia. Así se conoce en cualquier momento, el estado de la misma y cualquier persona del departamento técnico, es capaz de conocer e incluso retomar dicha solicitud de servicio.

También este tipo de herramientas poseen la capacidad de generar informes, resultando muy útil cuando es necesario un desglose de incidencias por usuario, por empresa o incluso para conocer el número de horas dedicado a resolver los problemas de los usuarios de una determinada empresa pudiendo así realizar una estimación del coste de los servicios prestados a dicha organización.



Conclusiones

En organizaciones de cierta envergadura, en las que es necesaria una compartición de recursos mediante una red interna, ya sean impresoras, depósitos de información distribuidos, bases de datos, ficheros... es imperativo proporcionar acceso a dichos recursos utilizando los protocolos adecuados para tal fin.

Utilizando dichos servicios, conseguiremos un mayor control sobre los recursos proporcionados, por ejemplo el acceso a depósitos de información o a archivos alojados en un servidor de ficheros, y una gestión más eficiente y centralizada de los mismos, como por ejemplo el uso de un servidor central que almacene las credenciales de los usuarios, para poder verificar su identidad y el nivel efectivo de permisos que dispone sobre ciertos objetos.

También resulta necesaria la utilización de un protocolo de red que permita la configuración dinámica de un host para su acceso a la red (DHCP), restando trabajo de configuración al departamento de IT a la hora de preparar un equipo nuevo para un usuario y un sistema que facilite la traducción de nombres de máquinas por su dirección IP (DNS), ya que resulta mucho más cómodo y fácil recordar un nombre que cuatro octetos separados por puntos.

Pero todo ello, no sirve de nada cuando no se disponen de herramientas para conocer el servicio que se proporciona a los usuarios y que ayuden a la correcta planificación de los proyectos, ajustando los recursos necesarios, ya sean humanos como materiales, para obtener el mayor grado de productividad con el menor coste posible en el desarrollo del proyecto.

Mirando hacia el futuro, las perspectivas de crecimiento de negocio son bastante halagüeñas, debido a la expansión internacional, lo que se traducirá en un incremento en el número de usuarios que harán uso de la infraestructura y servicios proporcionados por la Organización para atender a los nuevos proyectos a desarrollar. Es por ello por lo que será necesaria la puesta en marcha de nuevos servidores distribuidos para la autenticación de usuarios (utilizando Active Directory), y poder así soportar un futuro número de peticiones concurrentes.

También se necesitarán nuevos servidores de ficheros (acceso mediante los protocolos NFS o SMB) para poder almacenar la información relativa a nuevos proyectos de desarrollo: documentación técnica, anexos, informes, ofertas, imágenes, vídeos... y sólo accesible por los integrantes de los proyectos.

Será necesario el despliegue de servidores distribuidos para la gestión de la seguridad en las estaciones de trabajo, que controlen la actualización de las definiciones de virus de las aplicaciones antivirus, posibiliten la flexibilidad y automatización de tareas para reducir los costes, la gestión de la seguridad y la gestión del cumplimiento de las normativas establecidas por la Organización. Deberán notificar a los administradores cualquier amenaza existente en un equipo, que pueda poner en riesgo al resto de las estaciones de trabajo e infraestructura, pues a pesar que un equipo se encuentre en otro país, utilizando las tecnologías de red privada virtual, podrá acceder a los

recursos proporcionados por la organización, pero también puede resultar un foco de infección para el resto de sistemas.

Por otro lado, es una realidad la espectacular evolución de los dispositivos móviles como puedan ser Tablets o Smartphones. Debido al aumento de prestaciones y capacidades de los mismos, cada vez nos encontramos dichos dispositivos tanto en nuestro entorno personal como en el corporativo. Podríamos pensar que los dispositivos anteriormente mencionados no tienen cabida en un entorno empresarial, pero gracias a las tecnologías de virtualización de escritorios, podemos salvar las diferencias frente a un ordenador tradicional, lo que nos permitirá acceder desde un Tablet o Smartphone a todas las aplicaciones corporativas, sin la necesidad de hacer uso de un ordenador tradicional. Un Tablet es mucho más ligero y manejable que un ordenador, aunque sea portátil, y para un usuario que viaje con frecuencia puede ser una solución idónea.

Es por ello, por lo que será necesario desarrollar toda la infraestructura de virtualización de escritorios y aplicaciones, para que los servicios corporativos estén disponibles en los anteriormente mencionados dispositivos móviles, permitiendo por ejemplo la creación de incidencias de IT, consulta del estado de los servidores, acceso al EPR corporativo e interactuar con él, desde cualquier dispositivo y lugar, sin importar el dispositivo hardware que estemos utilizando.

Por último, será necesario encontrar el modo de interconectar el calendario de la herramienta de planificación de proyectos con el calendario personal de cada participante. En caso de que no fuera posible dicha sincronización quizá sea conveniente encontrar otra herramienta que proporcione dicha funcionalidad.

En conclusión, todo este crecimiento e innovación tecnológica se traducirá en un mayor requerimiento de recursos hardware y software, pero con la correcta elección de la solución a utilizar y evaluando tanto las soluciones comerciales como las de código libre, conseguiremos un correcto equilibrio entre el coste necesario para ofrecer el servicio y el rendimiento esperado por los usuarios de la infraestructura TIC.

Bibliografía

Documentación consultada en Julio de 2012.

- Sitio web de Microsoft. <http://www.microsoft.com/es-es/default.aspx>
- Sitio web de Technet de Microsoft. <http://technet.microsoft.com/es-es/>
- Sitio web de IIS. <http://www.iis.net/>
- Wikipedia. <http://www.wikipedia.org/>
- Sitio web de Ubuntu. <https://help.ubuntu.com/>
- Sitio web de VMWare. <http://www.vmware.com/es>
- Sitio web de Qnap. <http://www.qnap.com/>
- Sitio web de SWE y SPW. <http://memex.dsic.upv.es>
- Sitio web de ManageEngine. <http://www.manageengine.com>
- Sitio web de Solarwinds. <http://www.solarwinds.com/>
- Sitio web de Zabbix. <http://www.zabbix.com/>
- Sitio web de Nagios. <http://www.nagios.org/>
- Sitio web de Redmine <http://www.redmine.org/>
- Sitio web de LibrePlan <http://www.libreplan.com>
- Sitio web de OTRS <http://www.otrs.com/es/>
- Sitio web de osTicket <http://osticket.com/>
- Software comercial y libre <http://www.rebellion.org/docs/32693.pdf>