PROYECTO:

INTEGRACIÓN DE UNA RED CORPORATIVA UNIFICADA

MEMORIA

REALIZADO POR:

OLLER AZNAR, JUAN INGNACIO

JUNIO-2010

Índice

1.Enunciado y objetivo del proyecto

1.1 Enunciado

En el presente proyecto se va a crear una red corporativa que integrará las delegaciones de la empresa contratante dentro de la red que propaga el nodo central. Para ello se utilizarán los equipos y el software que se considere necesario siempre que se adapten a las necesidades y el presupuesto que contempla la empresa que hace las veces de cliente. Por tanto, el cometido del presente escrito es planificar las bases de un proyecto de red informática, los servicios, así como el control de acceso y seguridad de las distintas sedes y los distintos departamentos que cumpla con las expectativas de esta empresa.

1.2 Objetivo

El objetivo del presente proyecto es la adquisición, instalación y puesta en marcha de los sistemas y electrónica de red necesaria para dotar a la empresa de una red cableada que permita la gestión centralizada de todas las sedes de la empresa cliente y que permita también la monitorización y la securización de la misma.

Logísticamente, esta empresa se divide en 5 sedes independientes (contando con la nueva delegación) repartidas por la región y que cuentan con un total de unos 500 escritorios y unos 700 usuarios que utilizarán los llamados “puestos calientes”. Por ello también se deben organizar las estaciones de trabajo en diferentes dependencias que intentaran ajustarse a los distintos departamentos.

Además se trata de dotar de unos sistemas basados en software libre que remplacen los sistemas privativos basados en sistemas Sun/Solaris y Microsoft/Windows usados hasta el momento.

Para realizar el diseño y desarrollar el proyecto se pide definir:

- **Diseño del cableado.**
  - Estructura física de la sede.

  - Distribución de canaletas, toma de comunicaciones y CA, salidas de emergencia, otros.
  - Resumen de tendido de cables y tomas.
  - Esquema de topología de red física y tecnología a utilizar.
  - Estructura general de Backbone, cableado horizontal.
- **Selección de los dispositivos de red**
  - Diagrama jerárquico de los dispositivos de red.
  - Número de subredes necesarias y host en cada una.
  - Elección de MDF e IDFs. Especificaciones ambientales y seguridad.
  - Estructura de cada uno de los rack (MDF e IDF)
  - Elección de las maquinas de red (switches, routers…).
  - Resumen de servidores e impresoras que manejarán.
- **Integración y Configuración de los dispositivos de red.**
  - Elección de software para la configuración de los distintos dispositivos.
  - Desarrollo de configuración de los distintos dispositivos
- **Mantenimiento del sistema.**
- **Elección de software para la configuración de los distintos dispositivos.**
  - Desarrollo de configuración de los distintos dispositivos.
- **Sistemas de servicio a aplicaciones**
  - Diseño funcional de los sistemas de servicio a aplicaciones.
  - Directorio corporativo con LDAP.
  - Sistema de resolución de nombres con DNS.
  - Sistema de asignación de IP con DHCP.
  - Sistema de sincronización de tiempo basado en NTP.
  - Sistema de compartición de ficheros en la red interna.
  - Servidor Web seguro.
  - Servidor de correo.
  - Elección de software para los sistemas citados.
  - Desarrollo de configuración de los sistemas citados.
- **Monitorización de la red**
  - Diagrama de los sistemas de monitorización.
  - Elección de software para la monitorización.
  - Desarrollo de configuración de los sistemas de monitorización.
- **Mantenimiento del sistema**
  - Describir los planes de mantenimiento de los sistemas.

2 Análisis del enunciado

2.1 Ámbito

Este proyecto se enmarca dentro del proyecto de una empresa que está desarrollando para dotar de diversos servicios sus clientes, entre los que se encuentra facilitar un sistema de comunicaciones de mayor alcance y calidad, así como de un sistema de integración de sus nodos locales con un mayor grado de unificación frente al nodo central.

Dentro de este proyecto, nuestra empresa ha sido adjudicataria de la parte del pliego en la que se debe dotar a estos nuevos servicios de la infraestructura de sistemas, redes y almacenamiento necesarios. Además, se deberá procurar que todos los sistemas se integren con las bases de datos y estructuras existentes y en sus distintas ubicaciones. Por esta razón, se deberá tratar con otras empresas que han resultado adjudicatarias de otros segmentos del proyecto global, que implican infraestructura de comunicaciones, infraestructura de aplicaciones.

Así mismo, se deberá procurar que la empresa que quede como adjudicataria del mantenimiento de la explotación tenga la suficiente formación para poder desempeñar las funciones para las que ha sido contratada.

2.2 Propósito

El propósito de este documento es describir tanto las necesidades como la definición de la infraestructura de sistemas y almacenamiento que los arquitectos de nuestra empresa han planificado para los nuevos servicios de la empresa cliente.

2.3 Fuentes de Información

Los detalles incluidos en este documento han sido obtenidos de las siguientes fuentes:

- Documentación del concurso público de la empresa cliente.
- Documentación interna de Sun Microsystems, recogida en los Blueprints y en las páginas de referencia de hardware y software.
- Reuniones mantenidas con el cliente y con el resto de empresas adjudicatarias de cada uno de los lotes que componen el proyecto global.

3 Soluciones posibles

3.1 Visión Global

En esta sección se describe la arquitectura de sistemas, almacenamiento, red de datos y red de gestión que se desplegará por parte de nuestra empresa en el cliente que nos contrata para poder hacer funcionar las bases de datos y aplicaciones desplegadas por el resto de empresas adjudicatarias del resto de partes del concurso del proyecto global.

En el momento actual, se plantea la arquitectura basada en un nodo central (Ed. Pignatelli), un nodo de respaldo (Walqa) y cuatro delegaciones locales situadas en, Calatayud (Zaragoza), Jaca (Huesca), Teruel Capital (Teruel), La Muela (Zaragoza).

El entorno de preproducción del nodo central servirá inicialmente como entorno de pruebas para los servicios que se desean desplegar en este proyecto, será aquí, igualmente donde la empresa adjudicataria del mantenimiento de la explotación será formada por nuestros técnicos en una operativa llamada TOI (Transfer Of Information) frecuente en este tipo de proyectos.

Una vez validadas las pruebas y efectividad del despliegue de nodo central, se realizan los ajustes necesarios a todos los niveles, incluyendo la arquitectura. De esta manera se intenta conseguir que la implantación de los sectores será mas rápida y efectiva.

3.2 Red de Gestión

La infraestructura de gestión para los entornos de producción, preproduccion y desarrollo del Nodo Central esta unificada en una serie de servidores que se describen en un apartado posterior. Estos servidores realizan tareas de administración, monitorización, despliegue de software, copias de seguridad etc. En las siguientes páginas intentaremos describir el alcance de estos servidores:

Los servidores de gestión, además de permitir la gestión de toda la nueva plataforma desplegada en la empresa, soportan una serie de servicios de infraestructura de sistemas, necesarios para que los servicios generales funcionen correctamente.

Estos servicios básicos son los siguientes:

1. LDAP Nativo ➔ Para validación de máquinas y usuarios en el dominio.
2. DNS interno ➔ Gestión de resolución de nombres del dominio.
3. NTP ➔ Network Time Protocol.
4. NFS Y SMB ➔ Compartición de archivos.
5. Sistema de provisión ➔ Instalación distribuida de sistemas operativos, así mismo proveerá de un sistema para la instalación distribuida de parches y aplicaciones.
6. SSL-VPN ➔ Sistema de gestión de sesiones SSL en remoto.
7. Monitorización ➔ Para la gestión SNMP de sistemas hardware y de los sistemas software.
8. http ➔ Servidores Web de uso interno.
9. Syslog ➔ Sistema de gestión de logs.

Ahora tratamos cada uno de estos servicios básicos, desglosando las funcionalidades que proporcionan.

3.3 LDAP Nativo

El servicio de LDAP nativo, es un servicio de directorio con una finalidad equivalente a un Active Directory (AD) de Microsoft, de hecho, el AD es una "piel" sobre un LDAP. Además, esta es totalmente diferente al OID de Oracle, que en esta explotación tiene otra funcionalidad distinta.

La misión de este directorio consiste en almacenar el repositorio de usuarios de GNU/Linux destinados a la administración y operación de los sistemas, mientras que el AD de Microsoft tiene como funcionalidad la de contener las cuentas de los usuarios finales de Windows y el OID de Oracle almacena los usuarios de las distintas aplicaciones. Estos usuarios son totalmente diferentes e independientes entre si.

La utilización del LDAP nativo de GNU/Linux (OpenLDAP), nos permite definir los usuarios de GNU/Linux de una forma centralizada y más segura. Esto nos permite definir un usuario una vez y propagar esta información a todos los sectores y máquinas de cada sector. Además, almacenar estos usuarios de sistemas en un repositorio LDAP, nos permite cumplir los estándares de seguridad de la información exigibles a un entorno de este tipo.

Aunque la información esta centralizada, esta información es replicada a cada uno de los sectores. La administración del LDAP nativo se puede realizar desde el nodo central y opcionalmente desde todos los nodos, aunque es deseable que la gestión del LDAP se ejerza siempre desde los dos servidores principales de central.

La arquitectura de LDAP nativo para los entornos GNU/Linux consiste en dos servidores en configuración multimaster (Gestión 1 y Gestión 2) configurados de forma segura, utilizando una CA interna. Cada sector tendrá un servidor LDAP esclavo que replica la información del nodo central.

Los sistemas GNU/Linux del nodo central consultan a cualquier de los dos servidores de LDAP del central. Los sistemas GNU/Linux de un sector se conectan a su servidor LDAP local, en caso de fallo se conectarían a los servidores centrales. Se consultará en forma balanceada, dejando que central consulte a su servidor principal (Gestión 1), mientras que los sectores consultarán al segundo servidor de central (Gestión 2) en caso de fallo de su servidor de LDAP local (Gestión X1).

La comunicación LDAP nativo se realiza por las redes de gestión, por no ser uno de los servicios de las aplicaciones, sino ser labores de gestión.

3.4 DNS interno

El DNS interno de la explotación, es el servicio de resolución de nombres de los servidores utilizado exclusivamente dentro de la plataforma de este proyecto, no propagándose hacia el exterior, ni si quiera a través de otras redes a las que se pueda conectar nuestra empresa cliente.

Este DNS es completamente independiente del futuro DNS externo, que publicará los nombres de servicios accedidos desde el exterior de la plataforma, como por ejemplo para consultar la base de datos de gestión ciudadana desde la base de datos de tráfico o de hacienda.

Este servicio de DNS es utilizado por los administradores de la plataforma, aplicaciones varias, y NetBackup para acceder a todos los servidores.

La arquitectura del DNS interno consiste en un servidor máster (Gestión 1) y un servidor esclavo (Gestión 2) en el nodo central. Se ha decidido usar la configuración maestro-esclavo, ya que se ha considerado mucho más eficiente que la configuración multimaster y menos propensa a fallos e inconsistencias.

Cada sector tendrá un servidor de DNS interno, que realizará funciones de mantenimiento y replicación, siendo esclavo del servicio de resolución de nombres de central. Todos los servidores esclavos reciben la información de nombres del servidor máster.

Los sistemas GNU/Linux del nodo central consultará a cualquier de los dos servidores de DNS del central. Los sistemas GNU/Linux de un sector se conectan a su servidor DNS local, en caso de fallo se conectarían a los servidores centrales.

Aunque la base de datos de los servidores está centralizada en el nodo central, se puede administrar remotamente desde cualquier lugar de la plataforma mediante conexiones remotas. Incluso se puede hacer uso del sistema SSL-VPN, descrito posteriormente en esta memoria.

La comunicación con el servicio de resolución de nombres de dominio locales se realiza por las redes de gestión, por no ser uno de los servicios de las aplicaciones.

3.5 NTP

El servicio de configuración de tiempo por red (NTP) se considera en esta explotación infraestructura base, ya que permite tener sincronizada la fecha y hora de todos los sistemas GNU/Linux de la plataforma. Esto es de vital importancia, sobre todo en los clusteres de aplicaciones y de bases de datos.

La arquitectura de NTP descrita para esta explotación consiste en dos servidores de nivel "n+1" en el nodo central (Gestión 1 y Gestión 2) sincronizados con servidores de nivel "n" de Internet (RedIris).

Inicialmente se han definido dos servidores de Rediris en Internet, como servidores de nivel 2. Además se configurara un servidor NTP en cada sector que será configurado como servidor de nivel “n+2” y estará ubicado en la máquina de gestión del sector.

La comunicación NTP se realiza por las redes de gestión de la plataforma por no ser un servicio de las aplicaciones orientado a usuario.

3.6 NFS y SMB

El servicio Network File System (NFS) y el servicio Samba basado en SMB permiten compartir sistemas de ficheros entre distintos entornos Unix (Solaris , GNU/Linux, etc) y Windows para el caso de SMB. En la plataforma descrita en este proyecto, se utiliza este servicio para compartir documentación, software y el directorio

HOME de los usuarios administradores y operadores de los sistemas situado comúnmente en (/home/$user).

Esta información compartida es exportada por los servidores de gestión (Gestión 1 y Gestión 2), aunque por lo general es todo automático, en el caso de los HOME habrá que hacer una operativa especial para hacer el fail-over, ya que por motivos de configuración se ha decidido que esta transición sea manual.

El trafico NFS y SMB, como en el resto de servicios de gestión se realiza a través de las redes de gestión. Esto permite no decrementar el rendimiento de la red de servicio por donde solo debe circular el tráfico de las aplicaciones.

3.7 SSL-VPN

Como sistema de conexión segura usaremos un SSL-VPN basado en routers dedicados de Cisco-Systems. Este es un servicio que permite acceso remoto seguro a una amplia variedad de entornos como Unix, GNU/Linux Windows así como a aplicaciones.

El SSL-VPN permite acceso seguro e intuitivo desde la propia plataforma y desde Internet a las distintas herramientas de gestión de los sistemas.

El administrador de estos sistemas de enlace seguro define los host y las aplicaciones que se puede acceder, define los usuarios y grupos de usuarios que pueden acceder a las distintas aplicaciones.

El acceso al servicio es seguro mediante SSL con un certificado de una CA interna.

El servicio SSL está alojado en un router de la familia c28000, este equipo está fuertemente securizado, habilitando únicamente los servicios seguros imprescindibles, además el equipo esta configurado un firewall para generar un sistema confiable.

Este equipo está conectado a la red de gestión del nodo central y a Internet, así como a las líneas dedicadas de telefónica.

3.8 Sistemas de monitorización

Nagios es un sistema de monitorización auspiciado por el proyecto GNU y con funcionalidades para la monitorización de sistemas operativos, aplicativos, bases de datos, electrónica de red y hardware de servidores. Además se utilizará el software de traza de estadísticas de red Cacti para ver en tiempo real el estado de la red y además poder realizar informes y consultar históricos.

La gestión SNMP realizada por ambos sistemas permite detectar problemas hardware, de sistema operativo y aplicativo, que posteriormente los operadores y administradores de la plataforma realicen las acciones correctoras necesarias.

La gestión SNMP está centralizada en el nodo central, mediante un servidor que recogerá toda la información de los agentes SNMP instalados en todos los sistemas de todos los sectores. La gestión centralizada de la monitorización tiene la ventaja de poder obtener una vista global de todos los sectores y preparar plantillas con vistas parciales de la plataforma, de tal modo que un operador de un sector solo podría monitorizar sus equipos.

3.9 Sistemas de almacenamiento y backup

Además de lo expuesto en los puntos anteriores, el proyecto necesita de un sistema de gestión de almacenamiento y de otro de copias de seguridad.

Ambos sistemas, tanto de gestión de almacenamiento como de copia de seguridad a archivo de larga permanencia se encuentran interconectados a través de una red adicional de datos por fibra óptica conectadas mediante el sistema de reparto de fibra de la marca Brocade que se describe posteriormente.

El servicio de gestión de almacenamiento se ha planificado partiendo del modelo de Sun Storagetek basado en cabinas de disco de alto rendimiento de la serie ST6540, ST6520 y software de gestión de Sun Common Array manager (CAM).

El servicio de copias de seguridad se basa en un modelo de almacenamiento en cinta para almacenamiento en armarios ignífugos y en una ubicación externa que garantizan la continuidad del negocio incluso en caso de destrucción completa del centro de datos original y/o centro de respaldo.

El producto elegido para la gestión de las copias de seguridad ha sido Veritas NetBackup que es el producto estrella de la marca Symantec.

La infraestructura de copias de seguridad se expone igualmente de manera detallada en puntos posteriores. Por el momento, se debe saber que la forma en que en que se ha descrito la solución de backup, existe un servidor máster Server de Netbackup en el nodo central, que tiene pleno control de las copias en este nodo y el resto de nodos siguen el mismo modelo, por lo que hay un total de 6 máster servers entre los 6 nodos del proyecto. A demás de estos servidores, tenemos varios media Server distribuidos a lo largo de los distintos nodos.

El servidor máster y los media servers tienen acceso directo a la librería de cintas mediante la SAN, de este modo pueden lanzar copias de seguridad directamente a la librería, el resto de sistemas del nodo central realizaran backup a través de la LAN ya que no requieren tanta celeridad en el proceso de copia y recuperación.

En este proyecto se ha descrito que el tráfico de backup se reparta por las redes de gestión, para no penalizar en el rendimiento de la red de servicio, donde solo circula el tráfico de las aplicaciones.

3.10 Servidores Web de uso interno (http)

Dentro de este proyecto se ha descrito la necesidad de usar sistemas de información para que los distintos grupos se coordinen, se abran incidencias, etc. Esto se hará a través de páginas de tipo dinámico con aplicaciones que facilitarán esta gestión.

Para ello, una serie de máquinas en concreto tendrán que ser configuradas como servidores Web, y tendrán que usar aplicaciones para la gestión de incidencias y/o control de horas, anuncios, etc.

4 División lógica de las redes

En este proyecto se ha descrito la necesidad de proporcionar varias redes diferenciadas para así mejorar el rendimiento y operatividad de los servicios. Por este motivo se han decidido implementar las siguientes redes:

- Red de servicio.
- Red de gestión.
- Red de consolas.
- Red de fibra.

La red de servicio está diseñada para servir la información de las aplicaciones al usuario final y para comunicar los servicios servidor por las aplicaciones de datos entre los distintos servidores. Por ejemplo, la comunicación de las aplicaciones de representación de datos y las bases de datos para hacer las consultas.

La red de gestión está diseñada para proporcionar un interface para la administración de las bases de datos, sistemas y servicios. Así mismo proporcionan la vía de comunicación de los servicios llamados básicos como el NTP, LDAP, etc.

La red de consolas está diseñada para proporcionar una interface de administración adicional y una puerta "trasera" a las máquinas y el sistema operativo.

La red de fibra está diseñada para proporcionar de una vía de comunicación para el tránsito de datos de los servidores que necesitan acceder a datos de las cabinas de almacenamiento y de almacenamiento en cinta.

Todas estas redes se explican con detenimiento en secciones posteriores.

5 Disposición de los nodos del proyecto

Como ya se ha comentado se establece la necesidad de implantar un total de 6 nodos a lo largo del territorio de Aragón para poder cubrir de la mejor manera posible las necesidades de bases de datos y aplicaciones para dar servicio a los distintos departamentos de la empresa. Así mismo se consigue

dividir el trabajo entre los distintos puntos del sistema, y minimizar el impacto en caso de pérdida de comunicación, sobrecarga de trabajo de un nodo o catástrofe.

Uno de los problemas detectados durante la implantación y que han hecho replantearse el modo en que se enfocaba el proyecto es el fallo de comunicación con el exterior por lo que pesar de tener todos los servicios centralizados para conseguir un mejor aprovechamiento en la administración y conseguir así tener un punto de distribución y gestión, los sistemas pueden permanecer operativos durante un tiempo casi ilimitado aunque caigan las comunicaciones con el exterior, como por ejemplo en el caso de una caída de nodo central.

Esta situación de autonomía se ha conseguido mediante mecanismos de replicación de las bases de datos y proporcionando las herramientas de configuración, instalación y administración, que a pesar de estar centralizadas, contienen pequeñas réplicas capaces de actuar de manera autónoma. Un ejemplo de estas herramientas pude ser el sistema de directorio de LDAP o el sistema de gestión de nombres de dominio DNS.

La arquitectura planeada se basa en los siguientes nodos:

- Un nodo central situado en el edificio Pignatelli.
- Un nodo de respaldo situado en el parque tecnológico Walqa de Huesca.
- Un nodo local junto a la sede de la UNED de Calatayud (Zaragoza).
- Un nodo local junto al Ayuntamiento de Jaca (Huesca)
- Un nodo local anexo al CPD del Hospital Obispo Polanco en la ciudad de Teruel.
- Un nodo local en el Parque Empresarial Centrovía en La Muela (Zaragoza).

Las funciones de estos nodos, a pesar de haberse descrito en uno de los puntos previos se exponen más detalladamente en los siguientes puntos.

5.1 Nodo Central

La arquitectura del nodo central para los nuevos servicios solicitados por el cliente, que es en realidad un departamento del Gobierno de Aragón, se compone de las siguientes infraestructuras:

- Gestión.
- Producción.
- Desarrollo.
- Preproducción.

Como este nodo es el troncal, contiene dos entornos adicionales, tal como se ha citado anteriormente:

Desarrollo

Una sección dedicada a la implementación de aplicaciones y primeras simulaciones de la puesta en marcha de las aplicaciones. Sobre esta sección del nodo central, cada proyecto dispone de distintas máquinas o contenedores dentro de las máquinas para que puedan ser desarrolladas sin generar conflictos con otras aplicaciones.

Preproducción

Una sección dedicada al estudio del comportamiento de las aplicaciones sobre un sistema que simula el entorno de producción antes de ser implantado en dicho entorno real.

La mayor carga de trabajo la tiene la propia sección dedicada a producción que es la única que no puede ser detenida ni puede sufrir microcortes de servicio de ahí el empeño puesto en este proyecto en la replicación de máquinas, clusterización de aplicaciones y posibilidad de evacuación de servicios a otras máquinas dentro de la misma localización o incluso al nodo de respaldo.

Nodo de Respaldo

La arquitectura del nodo de respaldo ubicado en Walqa está diseñada para recibir el trabajo de los sistemas de producción de nodo central en caso de catástrofe en este nodo.

Esta necesidad de evacuar los recursos de nodo central al de respaldo viene dado por la necesidad de extender la continuidad de servicio más allá de la supervivencia de las estructuras físicas y también delimitan la necesidad de entornos en nodo de respaldo. Esta necesidad, hará que nodo de respaldo tenga únicamente una red de producción por lo que la red de dicho nodo estará dotada de las siguientes infraestructuras:

- Gestión.
- Producción.

En caso de caída del nodo central, los trabajos que se encuentren en ejecución en la red de producción de dicho nodo serían evacuados al nodo de respaldo a la mayor brevedad posible. Esta brevedad irá determinada por varios puntos que se estudian posteriormente entre los que se encuentran el software empleado para la replicación, el empleado para la clusterización y el estado de los enlaces de comunicaciones entre ambas redes.

Un tema muy relevante a tener en cuenta es que el nodo de respaldo debe ser capaz de soportar los picos debidos a la transición de una carga de trabajo media a una carga de trabajo de mayor densidad cuando se le pase el trabajo de nodo central. Esto establece la necesidad de sobredimensionar las máquinas de nodo de respaldo y de hacer simulacros con una cadencia mínima de uno cada seis meses.

5.2 Nodos locales

Los nodos que quedan a continuación son cuatro nodos de menor tamaño pero parecida importancia ya que cumplen una función:

- Conseguir que las distintas secciones puedan permanecer operativas incluso en caso de caía del nodo central y del nodo de respaldo (hecho altamente improbable), o durante el proceso de conmutación entre nodos (failover) debido a una catástrofe o prueba de evacuación. Esta

autonomía también garantiza la autonomía durante los posibles cortes de red que se produzcan en las comunicaciones internodales.

A continuación trataremos cada uno de ellos a pesar de tener unas características casi idénticas.

5.3 Nodo local de Calatayud

Situada junto al centro de estudios que la Universidad Nacional de Educación a Distancia tiene en la localidad se aprovechan unos locales que se arriendan en una planta baja.

Se ha preparado de tal manera que se eleve el suelo técnico según las especificaciones que se verán en los pliegos de condiciones y se han preparado las salas siguiendo igualmente las premisas de electricidad, temperatura y humedad solicitadas en el mismo grupo de pliegos.

Se ha solicitado también la inclusión de una línea de fuerza segura (SAI) para evitar posibles averías y poder garantizar la continuidad de la explotación, o incluso gestionar un apagado ordenado de los sistemas en caso de caída de las líneas de fuerza del nodo.

En este nodo tenemos, al igual que en el resto de nodos solo una red de producción, lo que excluye las redes de preproducción y desarrollo que solo se podrán encontrar en el nodo central.

5.4 Nodo local de Jaca

El nodo local de Jaca está situado junto al Ayuntamiento de dicho municipio. Concretamente en un edificio dedicado a albergar los archivos de la ciudad. Este edificio es propiedad del ayuntamiento y han habilitado una sala en un entresuelo lo que le da una elevación respecto a la planta calle de aproximadamente 80 cm y esto favorece la supervivencia de las máquinas frente a una posible inundación del pueblo.

Este es el único de todos los CPD del proyecto que no posee suelo técnico ya que el suelo del edificio es de un valor incalculable. Por este motivo, se ha decidido que por un lado, todo el suelo quede cubierto de una serie de losas de un polímero de alta resistencia que preservará el suelo de los arañazos y golpes de las máquinas durante el despliegue y estancia de las mismas y por otro lado, que se haya buscado una solución alternativa para la alimentación y ventilación de las máquinas, por este motivo, en este emplazamiento todo el cableado y ventilación se lanzarán desde el techo utilizando bandejas de cableado estándar.

Este nodo, al poseer una sección dedicada a la documentación de la biblioteca y a otros usos ya poseía una línea de fuerza segura (SAI) para evitar posibles averías y poder garantizar la continuidad de la explotación, o incluso gestionar un apagado ordenado de los sistemas en caso de caída de las líneas de fuerza del nodo.

En este nodo tenemos, al igual que en el resto de nodos solo una red de producción, lo que excluye las redes de preproducción y desarrollo que solo se podrán encontrar en el nodo central.

5.5 Nodo local de Teruel

El nodo local situado en la ciudad de Teruel se encuentra situado en una sala anexo al CPD del Hospital Obispo Polanco, con lo cual las personas que hay destinadas para el mantenimiento de dicho emplazamiento podrán dar soporte puntual al sistema de gestión ciudadana.

Este nodo es el más preparado de todos ya que compartirá alguna de las instalaciones que se pusieron en funcionamiento para el plan de sistemas de Salud de la Diputación General de Aragón.

Este CPD cuenta con comunicaciones de gran ancho de banda, un SAI de gran potencia y sistemas de refrigeración bien dimensionados.

5.6 Nodo local de La Muela

Situada en el Parque Empresarial Centrovía en La Muela y más concretamente en edificio central de oficinas que tiene dicho parque empresarial se aprovechan unos locales que el Ayuntamiento alquila.

Ese ha preparado de tal manera que se eleve el suelo técnico según las especificaciones que se verán en los pliegos de condiciones y se han preparado las salas siguiendo igualmente las premisas de electricidad, temperatura y humedad solicitadas en el mismo grupo de pliegos.

Se ha solicitado también la inclusión de una línea de fuerza segura (SAI) para evitar posibles averías y poder garantizar la continuidad de la explotación, o incluso gestionar un apagado ordenado de los sistemas en caso de caída de las líneas de fuerza del nodo.

En este nodo tenemos, al igual que en el resto de nodos solo una red de producción, lo que excluye las redes de preproducción y desarrollo que solo se podrán encontrar en el nodo central.

6 Elección de los Sistemas

6.1 Elección del Sistema Operativo

En este apartado se va a describir el proceso utilizado para la selección de un sistema operativo adecuado para este proyecto y esta explotación.

Para realizar la elección del sistema operativo, se van a usar criterios basados en las siguientes premisas:

- Interoperatividad con sistemas de DDBB Oracle.
- Rendimiento de las aplicaciones que deberá soportar.
- Seguridad de las aplicaciones y el kernel.
- Plataforma hardware empleada.
- Redundancia ante fallos.
- Auditoría y monitorización del sistema.
- Servicio de soporte a clientes.

Los sistemas operativos barajados para la realización de este proyecto son:

- Microsoft Windows Server 2.003.

- Microsoft Windows Server 2.008.

- Red Hat Enterprise Linux.
- SuSe Linux 10.
- HP-UX 11v2.
- IBM AIX 6.1.
- Sun Solaris 10.

Se han descartado otros sistemas operativos por no tener un servicio de soporte efectivo ya que basan su modelo de desarrollo en voluntarios que no pueden dar las garantías pertinentes de funcionamiento. Entre estos sistemas operativos tenemos por ejemplo:

- OpenGNU/Linux .
- Community Enterprise Operating System (CentOS).
- GNU/Linux DebIan.

A continuación estudiaremos cada uno de los sistemas operativos y sus prestaciones ante cada una de las premisas. Antes de nada, tendremos en cuenta que Microsoft Windows Server 2.003 va a ser "discontinuado" próximamente por lo que es mejor no implantarlo en nuestra explotación ya que esta explotación tiene que mantener cierta estabilidad de aquí a tres años vista.

Interoperatividad con sistemas de DDBB Oracle

La interoperabilidad con el sistema de DDBB Oracle y más concretamente con las versiones 10g y 11g se estudia basándose en el rendimiento ya que todos los sistemas operativos citados tienen soporte para estas versiones de Oracle.

El rendimiento lo basamos en pruebas específicas tanto de los ingenieros de soporte de SGBD y de Sistemas operativos, como en recomendaciones propias de Oracle. Además se hacen pruebas de "capacity" con herramientas propias de Oracle e independientes. Desde Oracle usamos la herramienta "Oracle Benchmark Factory" y como aplicación independiente usamos "Apache J-Meter". La versión de Oracle usada en estas pruebas es la "Oracle 10gR3".

En ambas pruebas, repetidas tres veces para asegurar que no se falsean, se da la siguiente asignación de prioridades:

- Sun Solaris 10.
- Red Hat Enterprise Linux v5.
- HP-UX 11v2.
- IBM AIX 6.1.

- Microsoft Windows Server 2.008.

- SuSe Linux 10.

Rendimiento de las aplicaciones que deberá soportar

A continuación volvemos a repetir las pruebas pero teniendo en cuenta que ahora se mide el rendimiento de estos sistemas mientras interactúan con aplicaciones. Como aplicación vamos a utilizar un "dummy" de java desarrollado con jsp y montado sobre Oracle OAS 10gR2. Nuevamente usamos el "Apache J-Meter", pero cambiamos el "Oracle Benchmark Factory" por el "J-Unit".

Se realizan las pruebas, repetidas nuevamente tres veces, se da el siguiente orden de rendimiento, de mayor a menor:

- Red Hat Enterprise Linux.

- Sun Solaris 10.

- SuSe Linux 10.

- Microsoft Windows Server 2.008.

- HP-UX 11v2.

- IBM AIX 6.1.

Viendo estos resultados y cruzando ambas pruebas se puede concretar que el sistema operativo más indicado tanto para montar Oracle como el servidor de aplicaciones OAS es Sun Solaris 10 seguido a continuación por Red Hat Enterprise Linux, distancia.

Seguridad de las aplicaciones y el kernel

La comparativa de seguridad de las aplicaciones asociadas al sistema operativo y del kernel se va a basar en los criterios descritos por AENOR y el material de la certificación de CCISP.

Todos los sistemas operativos han superado las pruebas de seguridad especificadas por estos estándares.

Los niveles de seguridad propuestos por la NSA (Agencia de Seguridad Nacional de los E.E.U.U.) y el DoD (Departamento de Defensa de los E.E.U.U.) solo son satisfechos por Sun/Solaris 10 y RHEL 5.

Plataforma hardware empleada

La comparativa entre plataformas hardware la basaremos en varios puntos que describimos a continuación:

- Plataforma propietaria ➔ Se valora de manera negativa que la plataforma empleada sea únicamente propietaria.

- Plataforma compartida ➔ Se valora de manera positiva que la plataforma empleada sea general, como AMD e Intel. Y muy especialmente que lo séa realmente compartida, soportando tanto Las anteriormente citadas como plataformas propietarias como Alpha, PA-Risc o Sparc.

- Robustez de sistema ➔ Se valora la resistencia a fallos de la plataforma.

- Escalabilidad ➔ Se valora la posibilidad de poder incrementar la capacidad de los servidores que albergan este sistema operativo.

    - Escalabilidad de memoria.

    - Escalabilidad de microprocesadores/cores.

    - Clusterización.

A continuación haremos un pequeño repaso de cada sistema operativo y su cumplimiento para cada uno de los puntos expuestos arriba.

Microsoft Windows Server 2.003 y Windows Server 2.008

Los sistemas operativos Microsoft Windows, desde el principio han estado ligados a sistemas Intel y posteriormente a AMD. No pueden ser instalados sobre ningún otro tipo de microprocesador a menos que se aplique una capa intermedia para la virtualización del sistema operativo; soluciones de virtualicación tales como VMWare, Virtual Box, etc.

Red Hat Enterprise Linux

Los sistemas operativos basados en GNU/Linux, tienen la ventaja de haber sido diseñados para ser multiplataforma. Pese a ello, no todas las versiones están portadas a todas las arquitecturas hardware disponibles. En este caso, RHEL es uno de los sistemas operativos GNU/Linux que cumplen esta premisa. Está portado para Intel, Sparc y Alpha.

SuSe Linux 10

Suse es otro de los sistemas basados en GNU/Linux. En este caso nos encontramos con un sistema no portado a arquitecturas Sparc ni Alpha.

HP-UX 11v2

El sistema operativo HP-UX es uno de los Unix mas difundidos en el mundo. Es la apuesta de HP para grandes explotaciones y está especializado en el procesamiento de grandes cantidades de datos. Está portado únicamente a PA-Risc (procesador propietario de HP) y a la gama Xeon de Intel.

IBM AIX 6.1

El sistema operativo AIX de IBM es otro sistema operativo propietario basado en UNIX. No es multiplataforma funcionando sobre procesadores propietarios de IBM. Por esta razón se considera un sistema operativo poco deseable para nuestra explotación.

Sun Solaris 10

El sistema operativo Solaris es la apuesta de Sun Microsystems entre los sistemas UNIX. Este sistema soporta arquitecturas Intel y Sparc, que es la arquitectura propietaria de Sun. Así mismo, incorpora propiedades de virtualización tales como Zonas, Containers, Sun Virtual Box e interacción nativa con Xen. Así mismo, se puede hablar de su homónimo libre, OpenGNU/Linux , que nos proporcionará un banco de pruebas que no necesita licenciamiento.

Redundancia ante fallos

En la redundancia ante fallos valoraremos los siguientes puntos que explicamos para que quede claro cuáles son las prioridades:

- Autocorrección de errores de sistema de ficheros ➔ Se valorará la capacidad de reparar errores del sistema de ficheros y la capacidad de recuperarse estos datos en caso de reinicio del sistema o fallo del mismo.

- Autocorrección de errores en el arranque ➔ Se valorará la capacidad del sistema operativo de solucionar los errores en el tiempo de carga del sistema.

A continuación haremos un pequeño repaso de cada sistema operativo y su cumplimiento para cada uno de los puntos expuestos arriba.

Microsoft Windows Server 2.003 y Server 2.008

Los sistemas operativos de Microsoft dedicados al mercado de los servidores incluyen de por si mecanismos de corrección de errores tanto en su sistema de ficheros local, mediante la cuarta revisión del NTFS, NTFSv4 como en su sistema de ficheros compartidos de tipo NFT/DFS.

Así mismo, incorpora sistemas para evitar la carga innecesaria del uso de acceso disco que puede desencadenar errores posteriores, tal como la herramienta de defragmentación de disco.

Para la solución de errores en el arranque, ambos sistemas operativos incorporan la ya conocida opción de arranque en modo a prueba de fallos.

Red Hat Enterprise Linux, SuSe Linux, HP-UX y IBM AIX

En esta ocasión agrupamos los sistemas operativos GNU/Linux y Unix comerciales ya que todos proporcionan las mismas herramientas de solución de errores de sistema de fichero y de arranque del sistema operativo.

Ambos sistemas operativos proporcionan herramientas de redundancia cíclica y corrección de errores en todas las variantes de sus sistemas de ficheros pero entre todos ellos, los que mejor rendimiento dan e incorporan journaling son UFS, EXT3 y RaiserFS. Se descarta la cuarta revisión de EXT por no haber sido suficientemente testeada.

En lo que respecta a la solución de errores en arranque, todos los sistemas operativos UNIX dan la opción de entrar a través del gestor de arranque (Ejm: Grub) en un modo de gestión de errores similar al usado por los sistemas de Microsoft y permite ejecutar chequeos automáticos de sistema de ficheros con fsck y otras herramientas similares.

Servicio de soporte a clientes

En lo que respecta al servicio de soporte a usuario de sistema operativo, podemos decir que todas las empresas poseen servicios de asistencia remota vía voz, correo electrónico, remote-hands (manos remotas) y/o presencial previo pago de los precios establecidos.

7 Desarrollo de la solución elegida

7.1 Máquinas seleccionadas

Para el despliegue del presente proyecto se ha decidido utilizar máquinas de Sun Microsystems, sobre todo por la gran estabilidad de su hardware para el entrono empresarial de alto rendimiento y por otro lado por su gran robustez y buen sistema de garantías y mantenimiento, y por disponer de un partner especializado y de confianza en la ciudad donde se despliega el Nodo central y con cobertura para el resto de nodos, con un tiempo de respuesta de envío de hardware de repuesto, en nivel Premium de garantía de 4 horas, y alcance de 24x7x356 y SLA contratable.

A continuación se exponen las máquinas usadas en el nodo central y otros nodos, listando sus principales atributos.

7.2 Sun Fire Enterprise 20K

La E20K es el producto estrella de Sun Microsystems para el mercado de los Middleware. Combina un total de 36 procesadores de hasta 1.95 GHz de la gama propietaria UltraSPARC IV+ con corrección por ECC.

Hasta 9 placas Uniboard que combina 4 procesadores por panel y hasta 64 GB de memoria RAM. La E20K soporta hasta un máximo de 576 GB de memoria RAM por dominio.

La E20K soporta también hasta 36 placas PCI-X I/O hot swap (manipulables en caliente). De estos slots, 27 son de 90MHz y 9 slots son de 33MHz; soportando conexiones 10/100 BaseT Ethernet, Gigabit Ethernet, UltraSCSI (LVD and HVD), ATM, FC-AL, HSI, y SCI, lo que da un amplio abanico de conexiones disponibles.

Además, las propiedades de hot-swap se extienden a las CPU, memorias, PCI-X, Fuentes de alimentación, ventiladores.

Esta máquina está indicada para aplicaciones de alto rendimiento como bases de datos, serán la Columna vertebral de las bases de datos de producción del entorno central.

7.3 Sun Enterprise T2000

La Sun Enterprise T2000 es un servidor que genera un rendimiento del más alto nivel y la máxima eficacia ecológica junto con virtualización líder de la industria sin costes y memoria de espacio reducido. Estas propiedades convierten al servidor Sun SPARC Enterprise T2000 en ideal para la consolidación de servidores x86/RISC de Web y aplicaciones, así como en la base ideal para crear una infraestructura Web 2.0.

El sistema CMT (Chip Multithreading Technology) de los procesadores UltraSPARC T1 proporcionan hasta 32 hilos de ejecución simultáneos de tipo CoolThreads.

A continuación desglosamos sus propiedades de una manera más técnica mediante el siguiente cuadro de propiedades:

Estas máquinas se usaran para la instalación de frontales Web, aplicaciones clisterizadas, enlaces con bases de datos y todo tipo de aplicaciones que generen gran número de conexiones simultaneas.

7.4 Sun Fire V490

La Sun Enterprise V490 es un servidor que genera un rendimiento de gran eficacia y potencia de procesamiento. Así mismo es la solución hardware para construir una granja de containers basados en zonas de GNU/Linux 10. Estas propiedades convierten al servidor Sun SPARC V490 en ideal para la consolidación de servidores para soportar bases de datos de alto rendimiento.

El mayor problema reseñable puede ser el elevado coste del hardware y actualizaciones del sistema.

Algunas de sus características más importantes es que tiene un rendimiento superior a cinco veces el de la generación anaterior de procesadores de la misma gama y duplicación de memoria en capacidad y velocidad.

Los microprocesadores usados son los potentes UltraSPARC IV+ basados en la tecnología de 90nm a 2.1 GHz de frecuencia. Proceso económicamente eficiente en solo U de montaje en rack.

7.5 Sun Blade X8000 Model P Series

La Sun Blade X8000P es un servidor que genera un rendimiento del más alto nivel y la máxima eficacia ecológica junto con virtualización líder de la industria sin costes y memoria de espacio reducido.

El servidor en carga completa puede contener hasta un total de 240 núcleos de procesador y 1,344 TFLOPs por chasis lo que da tres veces la densidad de los servidores montados en rack y hasta un 43% más de ahorro energético que los servidores montados en rack.

Si lo comparamos con los blades tradicionales podemos observar que da una ventaja de 1,5 veces de espacio de blade que cualquier otro servidor blade. Un espacio entre llamadas de asistencia un 40% más espaciadas y un coste de asistencia un 84% menor que en las blades anteriores, así mismo, da 24 veces más velocidad de implementación que los modelos tradicionales.

7.6 Sun Fire V240

La Sun Enterprise V240 es un servidor que genera un rendimiento de una gran eficacia por un coste moderado. Este sistema está indicado para ser usado como servidor de gestión entre otras cosas por su gran redundancia. Estas propiedades convierten al servidor Sun SPARC V240 en ideal para la consolidación de servidores para soportar aplicaciones de alto rendimiento.

Algunas de sus características más importantes es que tiene un rendimiento superior a cuatro veces el de la generación anterior de procesadores de la misma gama y duplicación de memoria en capacidad y velocidad.

Los microprocesadores usados son los potentes UltraSPARC IV+ basados en la tecnología de 90nm a 2.1 GHz de frecuencia. Proceso económicamente eficiente en solo U de montaje en rack.

7.7 Matriz SCSI Sun StorEdgeTM 3120

La matriz Sun StorEdge 3120 SCSI ofrece un valor excelente para los mercados de almacenamiento de nivel de entrada, ya que ofrece a los usuarios una matriz de almacenamiento modular de bajo perfil y ultracondensada, diseñada para satisfacer las distintas necesidades de entornos en rápido crecimiento.

Al ocupar sólo 1U, puede adaptarse a los espacios más reducidos, mientras que la capacidad para 4 unidades de disco proporciona más de un terabyte por matriz. Esta rentable matriz resulta ideal para ampliar la capacidad de disco de pequeños servidores y también se puede utilizar como una solución de arranque para servidores multidominio de mayor tamaño. El diseño de bus dual le permite arrancar un dominio duplicado por unidad de bastidor (U).

La matriz Sun StorEdge 3120 SCSI está diseñada para ofrecer una alta fiabilidad, robustez y una sencilla capacidad de servicio. La matriz cumple la certificación NEBS de nivel 3 y está conforme con MIL-STD-810F, lo cual asegura el funcionamiento en los entornos más exigentes. Una única interfaz de usuario gráfica permite llevar a cabo de forma intuitiva la configuración y la gestión de toda la familia StorEdge 3000.

7.8 Biblioteca Modular de Cintas Sun StorageTek SL-500

Para el sistema de almacenaje en soporta largo plazo (soporte magnético) se ha seleccionado la biblioteca modular Sun StorageTek SL500, ya que ha sido diseñado para simplificar sus operaciones de copia de seguridad, es facil de conseguir y usar. Tiene repuestos en la península a menos de 3 horas de viaje y ha recibido varios premios.

Este sistema está basado en el sistema de biblioteca modular empresarial y altamente fiable Sun StorageTek SL8500, y pese a que el StorageTek SL500 es de una gama media, mantiene la fiabilidad sin importar la cantidad de módulos de expansión, características redundantes y componentes intercambiables en caliente.

Además permite ser escalado desde de 79 a 460 TB de información, proporcionando un 30% más de capacidad que las bibliotecas de otros fabricantes como HP, DELL, IBM o EMC^2.

Aplicaciones principales:

- Copia de seguridad de datos fiable y ampliable.
- Archivo.
- Consolidación del almacenamiento
- Disastre Recovery (Recuperación de desastres).

Resumen de características:

- Robótica de gama media-alta y mantenimiento sencillo con el objetivo de mejorar la fiabilidad.
- Componentes redundantes intercambiables en caliente que aseguran la disponibilidad.
- Ampliable con facilidad mientras mantiene la fiabilidad y el rendimiento en entornos de alta disponibilidad.
- Salva espacio en su despliegue por permitir ser montado en racks.

- Simplifica y acelera la consolidación con ocho particiones nativas como máximo.

7.9 Selección de los routers

Los routers se utilizan para regenerar señales, concentrar múltiples conexiones y convertir formatos de transmisión que se usan para el envío de los datos. También permiten manejar la transferencias de datos.

Los routers pueden conectarse a una red WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias. Esto es uno de los usos que vamos a tener para estos dispositivos en nuestro proyecto.

Existe gran variedad de marcas y dispositivos de este tipo en el mercado y es necesario estudiar sus especificaciones para no equivocarnos y adaptarlo a las necesidades y exigencias de la red a implementar.

La empresa contratante ha determinado que estos dispositivos sean de la marca CISCO SYSTEMS. En este caso, ya que el mercado es muy amplio, y dentro de las marcas también tienen un gran abanico de posibilidades.

Centrándonos en CISCO, se han elegido los router para que sus características técnicas cubrieran las necesidades del cliente que son conexión Internet, voip y VPN.

Aunque las características de los modelos elegidos las contemplamos en el PLIEGO DE CONDICIONES, señalar que esta elección nos permite un acceso rápido y seguro a las aplicaciones criticas del negocio con una seguridad optimizada, mientras establecen una base sólida para las necesidades avanzadas de comunicación del futuro.

Elección:

De todas las gamas que disponemos de este fabricante se han elegido los router multiservicio integrados de Cisco 2800. Estos equipos están recomendados para pequeña y mediana empresa, son sistemas completamente modulares y además disponen de una gran variedad de componentes adicionales que se pueden añadir conforme evolucionen las necesidades de la empresa sin necesidad de cambiar los equipos de base e incorporan desde origen, el hardware de encriptación y aceleración para construir VPNs (virtual private networks) incorporada.

Como características destacadas de seguridad integra funcionalidad de firewall y la funcionalidad del sistema de prevención de intrusión en línea (IPS - intrusion prevention system). Con esto cubrimos las necesidades de seguridad de la red.

En lo que respecta al número de equipos telefónicos y canales de comunicación de voz, rendimiento de plataforma y capacidad de proceso DSP (Digital Signal Processor), nos permiten comunicaciones IP y de voz asequibles para el cliente y dispodremos de funciones como, voz montada sobre comunicaciones seguras, sistema de puerta de enlace (gateway) de voz, transcodificación y audio-conferencias, combinadas con el proceso de llamadas integrado en Cisco IOS.

Los modelos elegidos son:

- CISCO 2811 y los componentes necesarios para acceso a Internet.
- CISCO 2821-HSEC/K9 y los componentes necesarios para ser servidor VPN.

- CISCO2821-CCME/K9 y los componentes necesarios para gestionar la telefonía.

7.10 Selección de los switch

La empresa contratante determina que estos dispositivos, al igual que los routers sean también de la marca CISCO. Centrándonos en CISCO, debemos seleccionar acorde con los tiempos, unos dispositivos que nos permitan escalar la estructura sin grandes cambios estructurales, deben pertitir tráfico Gigabit, alta disponibilidad y conmutación inteligente para liberar trafico en los router y evitar cuellos de botella, posibilidad de crear intranet, VLAN y aplicaciones de voz. Es importante también que se permita escalar el tráfico a 10G de la manera más barata posible y con los minimos cambios de diseño.

Elección:

De todas las gamas que dispone este fabricante se han elegido la serie Catalyst 6500 y la serie Catalyst 4500, en concreto los modelos de chasis 6506 y chasis 4507R-E. Se han elegido estos chasis porque tanto cubren las especificaciones del cliente, como que, permiten el crecimiento de la empresa entre un 50% y 80%.

Aunque todas las características técnicas de los modelos elegidos las contemplamos en el PLIEGO DE CONDICIONES, señalar que estas elecciones disponen de interfaces Ethernet 10Base-T/100Base-TX/1000Base-TX - RJ-45, admiten alimentación por Ethernet o POE en sus componentes elegidos.

8 Desarrollo de la solución software elegida

8.1 Servicios de directorio

Como herramienta de Servicio de directorio se ha seleccionado el OpenLDAP, ya que es un sistema basado en LDAP (Lightweight Directory Access Protocol) o Protocolo Ligero de Acceso a Directorios que es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido y que permite buscar y ordenar información en un entorno de red.

Es considerado una base de datos a la que pueden realizarse consultas referentes a máquinas, usuarios y grupos de dominio.

Un directorio de OpenLDAP server contiene un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. En el que por ejemplo en esta explotación se guardan, una serie de nombres (personas, máquinas u organizaciones) que están ordenados según una serie de claves como orden alfabético, grupo de pertenencia, etc., en el que cada nombre de máquina, grupo o usuario tiene unos atributos y permisos adjuntos.

Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos y/o organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas).

LDAP almacena la información destinada a la autenticación de los usuarios mediante un nombre de usuario o nick y una contraseña asociada y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, permisos, certificados, ubicación de diversos recursos de la red, etc).

La versión seleccionada para el despliegue en esta explotación el OpenLDAP basada en LDAPv3, la cual es cumple las especificaciones del Internet Engineering Task Force (IETF) y de los famosos Standard Track Request for Comments (RFCs) y más concretamente el documento RFC 4510.

Estructura de directorio

El protocolo LDAP, que sigue la edición de 1993 del modelo X.500. Por este motivo tiene la siguiente estructura:

- Un directorio es un árbol de entradas del directorio.
- Una entrada consta de un conjunto de atributos.
- Un atributo tiene un nombre y uno o más valores.
- Los atributos son definidos en un esquema.

Cada entrada tiene un identificador único: su Nombre distinguido (DN) o Distinguished Name. Este consta de su Relative Distinguished Name (RDN) construido por algunos atributos en la entrada, seguidos del DN de la entrada del padre. Pensar en el nombre distinguido como un completo nombre de archivo y el nombre distinguido relativo como el nombre de archivo relativo en un folder.

La Estructura que se ha decidido para LDAP de este proyecto ha sido bastante simple, ya que es piramidal y se puede decir que es la configuración básica de este tipo de sistemas.

Se ha decidido implementar una solución gestión de usuarios, grupos y máquinas centralizadas en el nodo de Central, con su consabido sistema homónimo en el centro de respaldo, como backup para que se pueda más o menos restablecer el control de los sistemas en caso de caída del nodo central.

Para tener esta configuración se dispondrá de dos servidores en el nodo central que tendrán una configuración multimaster, aunque solo trabajaremos contra el servidor de gestión primario (Gestion001) por motivos de gestión de tareas y especificaciones del modelo ITIL, ya que en realidad podríamos operar sobre cualquier sistema, bien de central o bien de respaldo o resto de nodos.

Además de estos servidores, se ha decidido añadir un servidor de LDAP en cada uno de los nodos del proyecto para evitar problemas. Estos nodos recibirán actualizaciones frecuentes de los servidores de central, además se contará con un script destinado a monitorizar la replicación para asegurar que se están realizando las replicas y actualizaciones de la manera correcta.

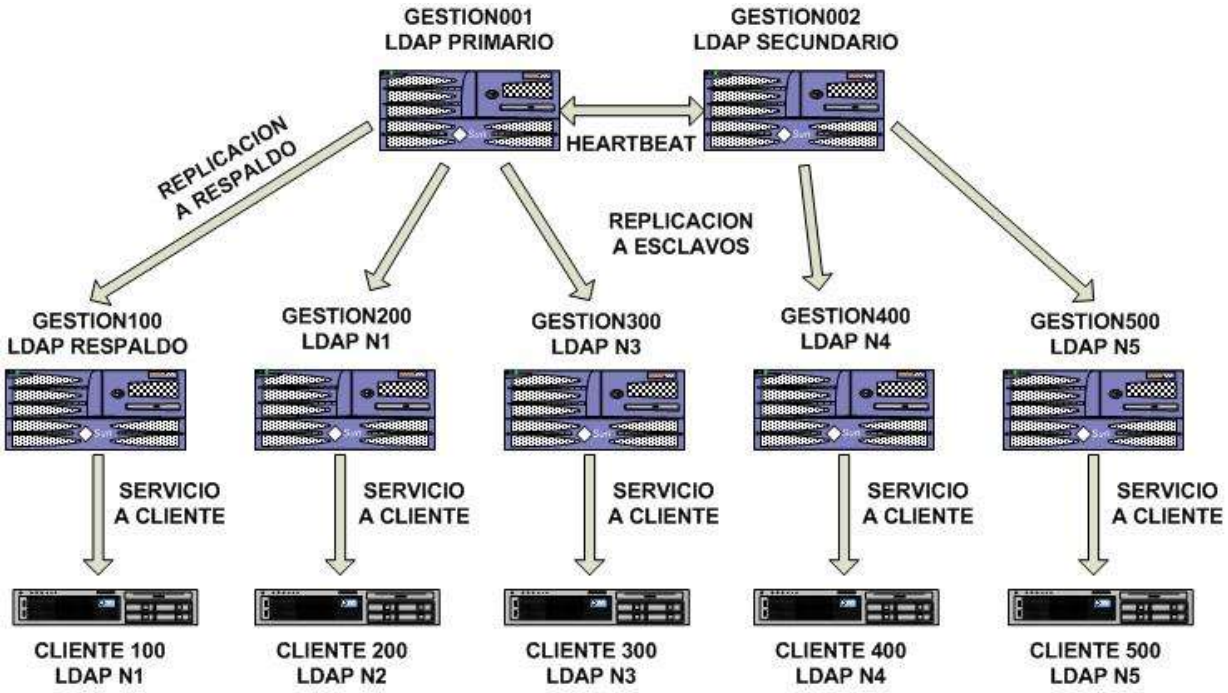
La estructura de máquinas hace que el LDAP esté instalado en las siguientes máquinas:

- Gestion001: Multimaster Primario.
- Gestion002: Multimaster Secundario.
- Gestion100: Servidor de respaldo (Multimaster en RODC).
- Gestión200: Servidor esclavo.
- Gestión300: Servidor esclavo.

- Gestión400: Servidor esclavo.

- Gestión500: Servidor esclavo.

Estos datos más la replicación entre servidores se puede observar en la imagen situada bajo estas líneas.



La comunicación de sincronización y actualización de datos entre las distintas bases de datos de LDAP se realiza mediante protocolo LDAPS a través del puerto 636 mientras que los clientes que usen GNU/Linux con LDAP nativo también se comunicarán vía LDAPS con los servidores de LDAP.

Replicación

Para la replicación entre los nodos multimaster de Gestion001 y Gestion002 con el resto de los servidores de los distintos nodos del proyecto y que tienen la notación GestionX00, se ha decidido que se debe definir desde la herramienta gráfica de SLAPD, con esta herramienta, además es posible ver el estado y resincronizar los directorios y también se han preparado una serie de scripts para esta función.

Todos estos scripts están instalados en el directorio "/export/ldap/" de cada uno de los servidores de gestión implicados en este servicio.

Los scripts para monitorizar la replicación entre directorios son los siguientes:

- repstat.sh: Permite ver el estado de las actualizaciones y si existe retraso entre servidores.

- reptest.sh: Modifica los masters y comprueba que los cambios son propagados adicionalmente encontramos los scripts de backup para el directorio.

- dbbackup.sh: Este script permite realizar una copia de seguridad en formato binario y sin parar el directorio

- ldifbackup.sh: Este script permite realizar una copia de seguridad en formato ldif y parando el directorio.

Además se ha decidido que todos los servidores tengan instalado un filesystem independiente de tipo ZFS llamado "/export/ldap" en el que se encontrarán dos productos relacionados con LDAP:

- Instancia SLAPD: Es el proceso que hace las tareas del servidor de ldap.
- Instancia de administración: Es el proceso que realiza las tareas de servidor para la administración gráfica.

Estructura de directorio

Lo más importante de la gestión de usuarios en este entorno son las restricciones de acceso o control de acceso a los servidores.

Los usuarios de aplicación no deben de entrar a los sistemas vía red por lo que en principio pueden ser usuarios de tipo local. Sólo los usuarios reales tienen que estar permitidos para entrar a los sistemas. A estos últimos usuarios es a los que se les aplica el control de acceso.

El directorio se ha montado según una sencilla división en la cual se crean varios grupos principales:

- Máquinas.
- Usuarios.
- Grupos.
- Servicios.

Además se ha tenido en cuenta la ubicación del objeto creado. Esto quiere decir, que un usuario que tenga control total en el OpenLDAP del nodo de La Muela, no tiene por qué tenerlo en el Nodo de Teruel o en el Nodo de Central.

La estructura del directorio queda reflejada en los anexos.

Todos ellos están adjuntados en los anexos para que el cliente pueda consultarlo si así lo necesita.

Los profiles llevan un campo de nombre en el cual se marca el nombre del Nodo al que pertenecen y una cadena de dos letras que describen el uso de la máquina de manera intuitiva:

- La cadena "ge" indica que son servidores de Gestión.
- La cadena "db" indica que son servidores de Bases de Datos.
- La cadena "if" indica que son servidores de Infraestructuras.
- La cadena "as" indica que son servidores de Aplicaciones.
- La cadena "it" indica que son servidores de Integración.

- La cadena “we” indica que son servidores dedicados a los frontales Web.

Estos profiles definen la forma de autenticación a los servidores. Por ejemplo, para el perfil profile_Calatayud_bd, hacemos que sólo los usuarios que pertenezcan a un determinado grupo puedan conectarse. En este caso los que pertenezcan a los grupos “users_bd” y “nodo_Calatayud”.

```
serviceSearchDescriptor:

passwd:ou=people,o=bdgc?one?(&(memberof=cn=hosp_calatayud,ou=group,o=
bdgc)(memberof=cn=users_bd,ou=group,o= bdgc))

serviceSearchDescriptor:

shadow:ou=people,o= bdgc?one?(&(memberof=cn=hosp_ calatayud,ou=group,o=
bdgc)(memberof=cn=users_bd,ou=group,o= bdgc))
```

De esta forma controlamos el acceso, dependiendo del sector y dependiendo del tipo de servidor. Un usuario debe pertenecer a los dos grupos para poder conectarse.

Los grupos dependientes de la localización disponibles en este proyecto son:

```
dn: cn=central,ou=group,o=bdgc

dn: cn=Respaldo,ou=group,o=bdgc

dn: cn=calatayud,ou=group,o=bdgc

dn: cn=lamuela,ou=group,o=bdgc

dn: cn=jaca,ou=group,o=bdgc

dn: cn=teruel,ou=group,o=bdgc
```

Los grupos dependientes de la aplicación disponibles en este proyecto son:

```
dn: cn=users_ge,ou=group,o=bdgc

dn: cn=users_bd,ou=group,o=bdgc

dn: cn=users_as,ou=group,o=bdgc

dn: cn=users_it,ou=group,o=bdgc

dn: cn=users_we,ou=group,o=bdgc

dn: cn=users_if,ou=group,o=bdgc
```

Además de todos estos grupos dependientes de la aplicación y localización se han descrito dos grupos más para las pruebas de implementación de la maqueta. Estos son:

dn: cn=maqueta,ou=group,o=bdgc

dn: cn=pruebas,ou=group,o=bdgc

Toda la seguridad de acceso recae en los atributos del usuario en el LDAP. Cada usuario pertenecerá a los grupos a los que quiera dársele acceso. Es responsabilidad del administrador del LDAP.

Por esta razón, existen dos tipos de usuarios en la plataforma:

- Usuarios de aplicación: para la manipulación de aplicaciones.
- Usuarios reales: para la conexión a los sistemas.

Las características de cada uno son las que se muestran a continuación:

Usuario.	**Características.**
Aplicación.	Estarán definidos localmente en el "/etc/passwd" de cada servidor. Tendrán password y directorio "home" diferente por cada servidor. No se podrán utilizar para conectarse a los sistemas.
Reales.	Estarán definidos de forma centralizada: LDAP Nativo. Tendrán un único password para todos los sistemas. Tendrán un único directorio "home" exportado por NFS, por lo que será el mismo en todos los sistemas a los que se conecten.

En lo referente al HOME de los usuarios tendremos que hacer una distinción:

- Los directorios home de los usuarios definidos localmente estarán creados localmente en cada máquina.
- Los directorios home de los usuarios centralizados estarán centralizados.

Sobre este tema se habla al final del apartado de LDAP.

A continuación se lista los usuarios de aplicación dados de alta en este proyecto, mientras que los sujetos a personas físicas se preservan en los ficheros encriptados de los servidores para preservar los acuerdos de confidencialidad a los que nos vincula la LOPD.

Aplicación	**Usuario.**
Oracle Database.	oracle

DB de Integración.	bdiapp
DB de BDGC.	bdgcapp
Frontal de aplicación de DB.	Omiapp
Frontal de aplicación de DB.	Intapp
Frontal de aplicación de DB.	Risapp
Frontal de aplicación de DB.	Gdpapp
Frontal de aplicación de DB.	Repapp
Frontal de aplicación de DB.	Rhapapp

A continuación se exponen los de administración de aplicaciones y máquinas:

Aplicación	**Usuario.**
Firewall builder.	Fwbuilder
Firewall local.	Iptables
OpenLDAP.	Ldap

Y por último los de los sistemas de monitorización de aplicaciones y máquinas:

Aplicación	**Usuario.**
DB de Nagios.	Dbnag

Certificados digitales

Otro punto importante es que toda la solución funciona bajo certificados digitales de tipo TLS por lo que es necesario establecer una infraestructura de certificados digitales para los servidores de directorio.

Para ello se ha generado una CA de uso interno en Gestion001 ya que es necesario dar de alta primero el certificado de la CA en "/export/ldap/alias/CA-bdgc", utilizando las utilizadas de la openssl del propio OpenLDAP Desde aquí, pueden generarse los certificados para nuevas instancias y difundirlo a las máquinas pertinentes.

Directorio Home

Los directorios de los usuarios estarán centralizados en los servidores de gestión para facilitar la administración. De esta forma, da igual al servidor que se conecte, su directorio "home" será siempre el mismo.

Para implementar esto, se ha utilizado las características del "automounter" y NFS. La publicación de sus directorios se hará a través del LDAP nativo.

Los directorios base de los usuarios se exportan por NFS desde:

- Usuarios del Nodo Respaldo: Gestion100.
- Usuarios del Nodo Teruel: Gestion200.
- Usuarios de Nodo La Muela: Gestion300.
- Usuarios de Nodo Calatayud: Gestion400.
- Usuarios de Nodo Jaca: Gestion500.
- Resto de usuarios: Gestion001.

8.2 El sistema de resolución de nombres de dominio (DNS)

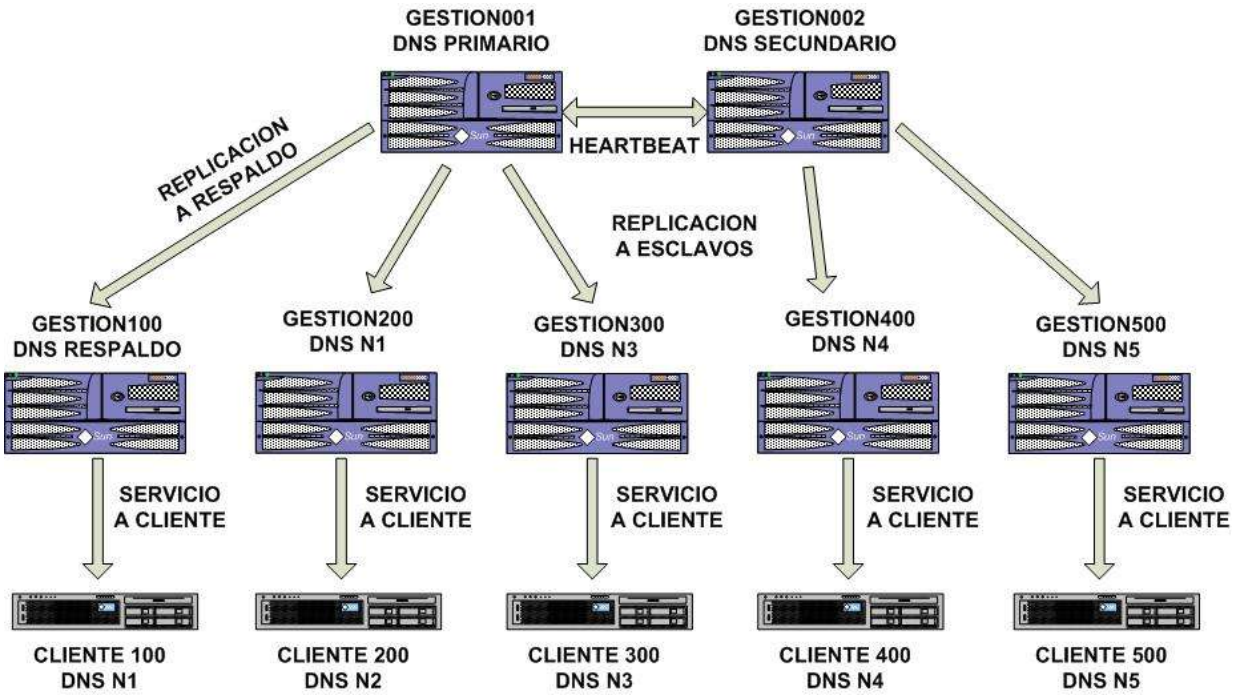
El DNS (Domain Name Server) es un servicio de resolución de nombres cuyo propósito principal es el poder trabajar con nombres de sistemas y dominio en vez de utilizar la dirección IP de máquinas, lo que suaviza bastante la experiencia de uso del usuario y facilita la tarea de administración de la red, aplicaciones y el sistema operativo.

Todo el sistema de DNS se basa en jerarquías de dominios a nivel de Internet. Por lo tanto en nuestro caso para esta explotación, se ha utilizado el dominio. Este dominio es únicamente de uso interno para las redes de gestión de la explotación de Sistema de Bases de Datos de Gestión Ciudadana. Por supuesto, el dominio no es resoluble a nivel de Internet.

El software utilizado para implementar dicho sistema DNS es el mismo “BIND 9.2” disponible de manera nativa en el sistema operativo seleccionado para la gestión del entorno, RHEL.

Estructura jerárquica de la solución

Se define un servidor primario de DNS, alojado en gestion001. Este será el único servidor sobre el que se realizarán los cambios de configuración de zonas. A continuación se definirán una jerarquía de DNS secundarios que dependen del primario. En concreto serán gestion002 y todos los servidores de gestión de los sectores (gestionX00) desplegados en la fase inicial del proyecto y de todos los que se vayan anexando a la estructura.



La arquitectura maestro/esclavo permite que los cambios introducidos en el maestro sean inmediatamente replicados en los esclavos.

Los servidores gestion001 y gestion002 además tendrán configuración para resolver dominios de Internet, aprovechando su conexión hacia afuera. De tal forma que el resto de servidores de DNS (gestionX00) los utilizarán como "resolvers" cuando accedan a dominios de Internet.

En cuanto a la configuración de los servidores como DNS clientes, cada servidor tendrá configurado a su servidor de gestión como servidor de DNS.

Archivos de configuración del DNS

No está contemplado dentro del alcance de este documento realizar ni listar la configuración del documento, a pesar de ello se va a dar un breve repaso a algunos ficheros relevantes para explicar como se ha dejado configurados o los puntos más relevantes de estos.

Las configuraciones detalladas podrán encontrarse dentro del bloque de anexos del proyecto.

El fichero de maestro de configuración del DNS es se encuentra en "/etc/named.conf". Desde este archivo se define el directorio dónde van a estar las zonas configuradas. En nuestro caso, el archivo de zonas de DNS va a ser "/export/dns".

A continuación se va a definir el uso de cada uno de los archivos implicados tanto en la parte del cliente como la parte del servidor.

Archivos de cliente:

Fichero de configuración del cliente.	Comentarios.
/etc/resolv.conf	Fichero de configuración de DNS cliente.

/etc/nsswitch.conf	Fichero dónde se indica los "Data Sources" para el S.O.

Archivos de servidor:

Fichero de configuración del servidor.	Comentarios.
/etc/named.conf	Fichero de configuración global de DNS.
/export/dns/db.127.0.0	Zona inversa para 127.0.0.1.
/export/dns/db.localhost	Zona directa para localhost.
/export/dns/db.bdsgc	Zona directa para el dominio.
/export/dns/db.168.192	Zona inversa para 192.168.0.0.
/export/dns/named.root	Root Servers para la zona "."

Servidor de DNS

Tal como se ha dicho, el sistema de DNS de este proyecto ha sido implementado mediante el modelo de arquitectura Maestro – Esclavo y las modificaciones de información en las zonas ".bdgc" y "db.168.192" sólo se podrán realizar sobre el servidor de DNS establecido en el nodo "gestion001".

El demonio del servicio servidor de DNS es "/usr/sbin/named" y se maneja con el servicio de GNU/Linux : svc:/network/dns/server:default

- Se puede arrancar: svcadm enable dns/Server.
- Se puede parar: svcadm disable dns/Server.
- Se puede releer la configuración para reconfigurar el DNS usando el comando: svcadm restart dns/Server.

A modo de comprobación del correcto funcionamiento puede usarse el comando "nslookup" en cualquier cliente de DNS de la explotación.

Clientes de DNS

Todos los servidores GNU/Linux serán clientes de DNS, al igual que el resto de los sistemas de la explotación, incluyendo a los servidores basados en GNU/Linux RHEL y los servidores basados en Microsoft/Windows.

La configuración de las máquinas cliente se realiza en los ficheros /etc/resolv.conf y /etc/nsswitch.conf.

Dicho sistema se maneja con el servicio de GNU/Linux : svc:/network/dns/client:default

- Se puede arrancar: svcadm enable dns/client.
- Se puede parar: svcadm disable dns/client.

- Se puede releer la configuración para reconfigurar el DNS usando el comando: svcadm restart dns/client.

Modificaciones en las zonas:

Para añadir o quitar información de las zonas, se seguirá el procedimiento descrito en el apartado de manuales de usuario de este mismo proyecto.

Archivos de configuración relevantes:

A continuación se hace un recorrido por los ficheros de configuración más importantes, el resto de los archivos se dejarán como material anexo en los apartados dedicados para dicho propósito.

Se recogen en los anexos de este proyecto.

8.3 Servicio de sincronización de hora mediante protocolo de red (NTP)

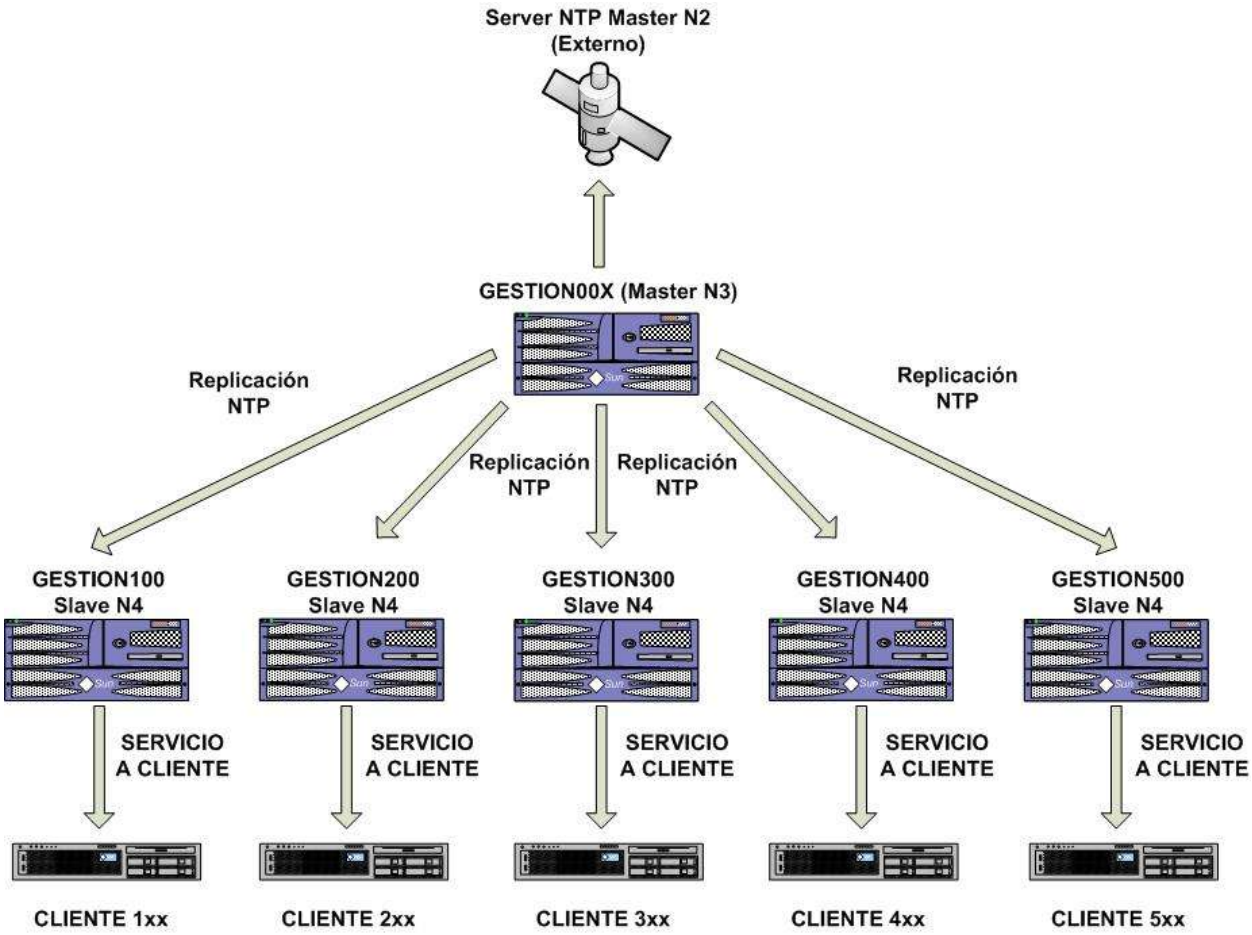
Como solución para realizar la sincronización de todos los sistemas operativos, las aplicaciones y los clústeres, se ha decidido realizar una instalación de dos servidores de NTP en el Nodo Central (Gestion001 y Gestion002) y uno en cada uno de los sectores (GestionX00).

El NTP es el protocolo de tiempo de red (Network Time Protocol). En el mundo en el que vivimos, es tremendamente necesario disponer de una hora correcta e igual entre todos los apartados de la empresa. Por esto, es necesario que todos los sistemas de la misma queden configurados según un único reloj, que para más seguridad debe ser sincronizado con alguna fuente fiable. Esta hora estándar para todos los equipos de la red garantiza que todo lo que se ejecute en la red y que sea dependiente de una sincronización se realizara exactamente cuando deba ejecutarse.

Esto puede hacer por ejemplo que las copias de seguridad se ejecuten en todas las maquinas a la misma hora, o que todos los usuarios reciban un aviso de fin de jornada laboral.

Los sistemas GNU/Linux incluyen gran numero de aplicaciones dedicadas a sincronizar la hora, o simplemente a consultar la fecha y el día. Un ejemplo de dichas utilidades puede ser el comando date o ntpdate. NTP utiliza el puerto UDP 123 como su capa de transporte y el demonio que ejecuta el servicio es el ntpd.

Además, como el NTP es un protocolo de sincronización horaria entre servidores se va a definir una estructura para que todos los servidores de la explotación esten sincronizados en tiempo y así los clusters se sincronicen de manera correcta.



Estructura jerárquica de la solución

Se definirán 2 servidores de primer nivel (nivel n) en el nodo central. Estos serán gestión 1 y gestión 2. Estarán sincronizados con servidores externos. En nuestro caso se han elegido servidores de RedIris. Adicionalmente estarán sincronizados entre ellos (peer).

En cada sector habrá un servidor de NTP adicional (gestiónX00) que estará sincronizado con los dos servidores del nodo central (nivel n+1).

Los servidores finales estarán sincronizados con el servidor de gestión de cada entorno:

- En los sectores con gestionX00.
- En el central con gestion001, gestión 002.

Archivos de configuración del NTP

El fichero de configuración es el "/etc/inet/ntp.conf" para todos los servidores. En caso de cluster, el fichero de configuración de NTP de clúster es "/etc/inet/ntp.cluster".

Los servidores internos apuntados son, como ya se ha dicho los de Gestión de cada entrono, mientras que los externos a los que se consultará son los pertenecientes a redIRIS por lo que quedarán con la siguiente estructura de configuración.

Servidor	Destino
Gestion001	EB-Zaragoza1.rediris.es
Gestion001 (peer)	EB-Madrid1.rediris.es
Gestion002	EB-Zaragoza1.rediris.es
Gestion002 (peer)	EB-Madrid1.rediris.es
Gestion100	Gestion001
Gestion100 (peer)	Gestion002
Gestion200	Gestion001
Gestion200 (peer)	Gestion002
Gestion300	Gestion001
Gestion300 (peer)	Gestion002
Gestion400	Gestion001
Gestion400 (peer)	Gestion002
Gestion500	Gestion001
Gestion500 (peer)	Gestion002

En los Clústeres, se sincroniza con su servidor de gestión y se pone "peer" al otro nodo del clúster.

8.3 Servidores de aplicaciones Web

Apache

En un principio se ha descrito la necesidad de la instalación de un servidor Web en determinadas máquinas destinadas a servir contenido HTML o de otros formatos compatibles con los servidores http. Por este motivo se ha decidido usar Apache.

Apache es un servidor de gran uso y valía y que además se proporciona de manera nativa en GNU/Linux por lo que no habrá de ser instalado ningún otro software adicional.

El proceso para hacer funcionar Apache sobre GNU/Linux es tan simple como levantar el servicio de apache que hay entre los archivos de sistema.

El sistema levantará un aplicativo Web 100% funcional y desde ahí, los administradores de la plataforma deberán programar la Web que deseen mantener.

Otras aplicaciones Web

Además de las clásicas páginas Web de carácter informativo se ha considerado definir una serie de aplicaciones que se deberán instalar para una mejor gestión de la plataforma. A continuación se detallan todas ellas:

- Gestor de incidencias: Se ha decidido usar un gestor de incidencias libre basado en PHP y auspiciado bajo licencia GPL. Este gestor es el GLPI. Los principales motivos son económicos ya que por el momento no se ha destinado presupuesto a la comprar de un gestor completo como Tivoli de IBM, OpenView de HP, etc.

- Gestor de contraseñas: En una explotación tan densa como la que nos ocupa, no se puede gestionar las contraseñas de manera útil sin hacer uso de un software especializado. Por este motivo se ha decido usar el MyPMS que es una aplicación basada en PHP y MySQL de carácter libre y licencia GPL. Este sistema sería sustituido en caso de implementar una solución integral como OpenView ya que también es posible usar una parte de la suite para este propósito.

8.4 Servicio de gestión de archivos de red (NFS y SMB)

NFS

El servidor de archivos distribuidos de red NFS o Network File Systems está integrado de manera nativa en GNU/Linux por lo que simplemente se deberá configurar un arranque automático del servicio para que levante junto a la máquina y se deberá revisar que estos tres servicios estén funcionando.

- Cliente LDAP.

- AutoFS.

- Cliente NFS.

Todo lo que se debe saber sobre este sistema se puede leer en el manual de usuario.

Samba

Para la configuración del servidor de archivos de red se ha decidido usar Samba que es un servicio orientado a la comparición de recursos en redes Unix y Microsoft. Este servicio permite compartir archivos e impresoras en una red local. Samba, funciona de una manera muy similar a como funciona un controlador de dominio de Microsoft Windows 200x.

La integración de Samba, resulta perfecta en redes Microsoft como servidor independiente de impresión, servidor de comparación de archivos, servidor de dominio, etc.

Otra de las ventajas más notables de Samba es que es plenamente compatible con todas las versiones de UNIX, tanto propietarias (Solaris , HP-UX, etc) como libres (GNU/Linux) siendo semitransparente para el administrador si se encuentra en una maquina con uno u otro UNIX instalado. Esta compatibilidad, se debe a que se usa samba usa el protocolo CIFS/SMB (Common Internet System/Server Message Block). Por último, hay sistemas que si bien no soportan samba como servidores si que lo soportan como clientes por lo que pueden ser integrados igualmente en una red en la que se encuentre instalado un servidor Samba. Entre estos últimos sistemas, se encuentra por ejemplo el VMS.

Como se ha dicho, samba sirve tanto para servir datos como para servir de controlador de impresión. El problema, es que en el caso del servidor de impresión, puede llegar a ser tremendamente complicado instalarlo y administrarlo. Pese a ello, resulta ser una herramienta útil y de gran difusión que cada dia que pasa gana más adeptos.

Tampoco hay que olvidar que Samba, recoge el testigo de NFS (Network File System) y permite, como tal, la comparticion de archivos entre maquinas UNIX.

Instalación y configuración de Samba

La configuración de Samba es bastante sencilla aunque un poco más compleja que la del NFS. Existen tres paquetes del servicio Samba que tienen cada uno una funcionalidad:

- Samba: Es el servicio de servidor.
- Samba-client: Conjunto de utilidades que permiten al sistema hacer de cliente de un servidor SMB.
- Samba-common: Conjunto de herramientas y archivos comunes al cliente y al servidor de Samba.

Una vez instalado en servicio, se puede empezar a configurar el servicio para que funcione apropiadamente. Antes de nada, se debe crear un directorio en el cual se compartirán los archivos que el administrador crea conveniente. Para ello, se usara el comando mkdir, asignando a todos los usuarios el derecho de leer, escribir, y ejecutar sobre dicha carpeta. El lugar mas apropiado para dicho directorio es el directorio /home/samba, aunque dependerá mucho de la carga que tenga el mismo.

8.3 Seguridad de la máquina

IPTables

IPTables es un cortafuegos disponible para muchos clones de Unix (GNU/Linux, IRIX, FreeBSD, NetBSD, HP-UX...), es un software gratuito y tiene unas excelentes características técnicas.

Este cortafuegos permite filtrar el tráfico en función de diferentes campos de la cabecera IP de una trama, como las clases de seguridad, las direcciones origen y destino y el protocolo o diferentes bits de estado. Además es posible utilizarlo como redirector de tráfico para configurar proxies transparentes, efectuar NAT e IP Accounting, y ofrece también mecanismos de comunicación con el espacio de usuario. Además IP Filter es stateful y soporta además IPv6.

No obstante, no todo es positivo; el argumento más utilizado por los detractores de IP Filter no es técnico sino jurídico: se trata del tipo de licencia, o de la interpretación de la misma, que hace el autor del software (el australiano Darren Reed), y que aunque distribuye el código fuente de forma gratuita, no permite efectuar modificaciones sobre el mismo. Aunque parezca una tontería, esta postura choca frontalmente con la filosofía de diferentes sistemas Unix para los que el producto está disponible, lo que ha generado problemas de distribución y utilización del mismo.

Instalación

IPTables se distribuye oficialmente en formato binario (en forma de paquete), su instalación en un sistema Unix suele ser muy sencilla: por ejemplo, en el caso de GNU/Linux , la única precaución a tener en cuenta es que GNU CC (gcc) no puede compilar IPTables en modo 64 bits.

Configuración

Tras instalar el paquete, se deben definir las reglas de filtrado y NAT en los archivos correspondientes (tal y como se verá), y una vez hecho esto se podrá inicializar el firewall ejecutando una simple orden, que se puede incluir en el arranque de nuestra máquina de la forma habitual.

Gestión

Como ya se ha comentado, una de las grandes diferencias de IPTables con respecto a otros sistemas cortafuegos es que este toma su configuración - su política - de simples ficheros ASCII; realmente esto es una diferencia importante con respecto a otros sistemas cortafuegos, como iptables, que no están orientados a archivo: un script de arranque de IPTables instala políticas leídas del fichero correspondiente, que posee una cierta sintaxis, mientras que uno de iptables ejecuta línea a línea órdenes que conforman la política a implantar.

La segunda diferencia de IPTables con respecto a casi todo el resto de firewalls del mercado sí que es puramente relativa a su gestión, y la encontramos a la hora de implantar en el cortafuegos la política de seguridad definida en nuestro entorno de trabajo: se trata del orden de procesamiento de las reglas de IP Filter, completamente diferente a Firewall-1, ipchains.

En todos estos firewalls se analizan en orden las reglas instaladas hasta que una coincide con el tipo de tráfico sobre el que actuar (hasta que hace match); en ese momento ya no se analizan más reglas, sino que se aplica la acción determinada por la regla coincidente.

IP Filter no sigue este esquema; por contra, se suelen procesar todas las reglas definidas en nuestra configuración, desde la primera a la última, y se aplica la última coincidente con el tipo de tráfico sobre el que se va a actuar.

Frontal de FWBuilder

Como ya se ha dicho en el punto anterior, el Sistema Operativo GNU/Linux tiene incorporado el paquete de software libre “iptables” para hacer las funciones de Firewall.

El iptables es un firewall que permite el control de todo el tráfico TCP/IP. Se trata de un módulo de kernel que se sitúa entre la capa de driver de red y la capa IP. Puede situarse sobre todos los interfaces que se quieran del sistema.

El iptables puede utilizarse como firewall normal (routing) o firewall de host (sin routing). En nuestro caso, que tenemos el “forwarding” desactivado, lo utilizaremos como firewall de host. El FWBuilder es una herramienta gráfica que facilita la generación de los ficheros de configuración de firewalls de varios tipos, incluido el iptables.

La gran ventaja de usar este producto, es la centralización de las políticas de seguridad en una única consola gráfica. A partir de la misma, se generan cada uno de los ficheros de configuración de los ipfilter.

Además, Firewall Builder trabaja con otras herramientas como iptables, ipfw, Cisco PIX, FWSM, OpenBSD pf y listas de acceso de Cisco IOS (ACL) por lo que podremos unificar el manejo de los Switch de las consolas y las redes de los distintos nodos y estar formados para próximas actualizaciones.

Uso en la explotación

El ipfilter estará instalado y configurado en cada una de las máquinas GNU/Linux de este proyecto, y gracias a las nuevas funcionalidades de la aplicación podría extenderse a posibles máquinas Windows que se instalaran en un futuro.

Para la manipulación de la aplicación se ha creado un usuario "iptables" local a cada máquina, con password local, para la carga de las políticas que se describen posteriormente.

La consola de administración de FWBuilder está instalado únicamente en la máquina de seguridad. Es desde aquí desde dónde se ejecuta y dónde se tiene la política de seguridad. Para trabajar con el FWBuilider existe el usuario "fwbuilder" local de la máquina de gestión de seguridad. En el directorio home (/home/fwbuilder) de este usuario se encuentran los ficheros de reglas.

Si el cliente lo prefiere, en el futuro, sería posible separar la administración de los ipfilters de cada zona de forma independiente, para lo cual, sería necesario instalar el FWBuilder en las máquinas de gestión de cada zona.

8.6 Servicio de monitorización (Nagios y Cacti)

Nagios es un sistema open source que goza de gran popularidad entre todos aquellos administradores que quieren monitorizar una red,, Monitoriza los hosts y servicios que se especifiquen, alertando cuando alguno de ellos no esta dando servicio y nuevamente vuelve al estado correcto.

En este proyecto se ha optado por ya que es un sistema de gran robustez, fiabilidad y de gran difusión, en continuo desarrollo y además a coste cero.

Nagios nos permite monitorizar lo siguiente en esta explotación:

- Monitorización de servicios de red (SMTP, POP3, HTTP, NTTP, ICMP, SNMP).
- Monitorización de los recursos de un host (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos, incluso Microsoft Windows con el plugin NRPE_NT.
- Monitorización de bases de datos, en nuestro caso Oracle
- Monitorización remota, a través de túneles SSL cifrados o SSH.

También nos va a permitir realizar el diseño de nuevos plugins para gestionar mejor nuestros propios chequeos de servicios dependiendo de las necesidades que se vayan descubriendo durante la implementación.

En el caso de esta explotación se ha decidido instalar dos máquinas blade de la X8000 con una versión de Nagios para GNU/Linux RHEL sobre X64. Estas dos máquinas están en cluster y en caso de fallo de una se podrá seguir viendo la monitorización desde la otra.

Como la base de datos de Nagios está montada sobre MySQL se ha tenido que montar un clúster de MySQL entre ambos nodos, aunque a diferencia de los clústeres de producción, este clúster no goza ni de la misma estabilidad ni de un sistema de garantía y soporte.

Requisitos

Para poder monitorizar los distintos sistemas necesitamos preparar las máquinas y equipos de comunicación para que dejen al programa consultar los datos que necesite consultar. Por este motivo hay que dejar abierto en los firewalls pertinentes el puerto que utilizaremos en la explotación para tráfico del protocolo simple de administración de tráfico de red (SNMP), que en esta explotación ha sido cambiado a otro puerto por motivos de seguridad.

Además habrá que instalar un software especial en las máquinas para que puedan comunicar e interpretar las peticiones con el software de monitorización.

Este software es distinto en función del sistema operativo que se pretende monitorizar, por eso tenemos 3 tipos en estas máquinas en función de si son sistemas de red, sistemas Windows o sistemas Unix/linux.

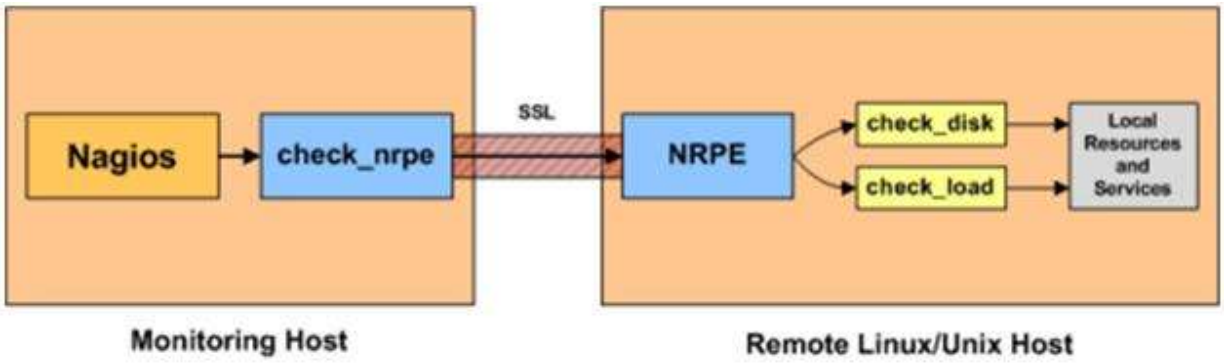
A continuación explicamos que hace falta en cada uno de los casos.

Sistemas Unix y GNU/Linux

Estos sistemas tendrán pocos requisitos ya que Nagios ha sido desarrollado sobre GNU/Linux Debian y tiene una gran integración con sistemas UNIX y GNU/Linux. En este caso bastará preparar el plugin de sistema operativo NRPE que se puede descargar de la página Web del proyecto Nagios3, pero que se proporciona en los DVD/CD de software que se han preparado para este proyecto de implementación de la Red de Base de Datos de Gestión Ciudadana o también se pueden extraer del repositorio que se ha montado en una de las máquinas de gestión de central.

En el esquema situado bajo estas líneas se puede ver el esquema funcional de este sistema de monitorización contra una máquina GNU/Linux o Unix.

Es importante que entre la máquina de monitorización y la máquina monitorizada se pueda conectar vía SSH por lo que habrá que tener en cuenta el usuario de monitorización local de la máquina y que se tengan preparadas las claves RSA pertinentes para que no de problemas en las conexiones.



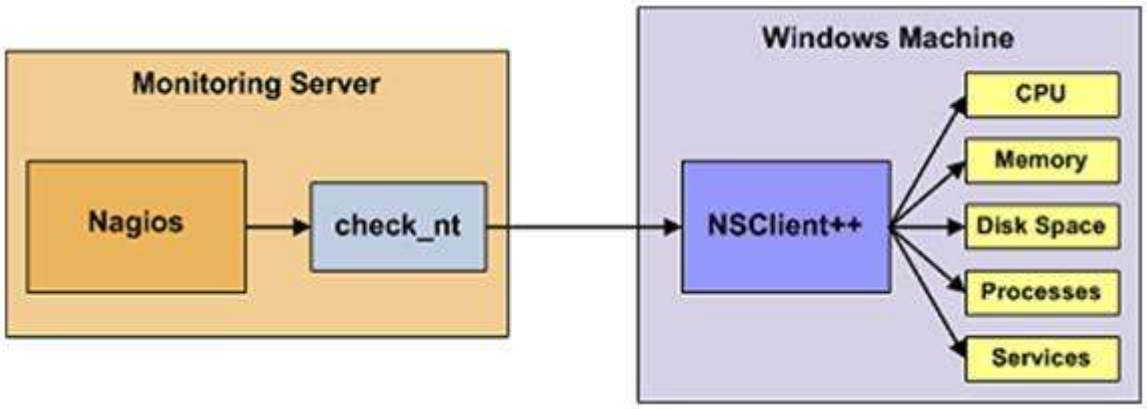
Como se puede ver en el esquema, el sistema de monitorización, por defecto facilita muy pocos datos, esto se solucionará con scripts adicionales y plugins. Todos ellos se reflejarán en los anexos a este proyecto.

Sistemas Microsoft/Windows

Estos sistemas tendrán requisitos adicionales frente a los sistemas GNU/Linux y Unix ya que Nagios ha sido desarrollado sobre GNU/Linux. En este caso se deberá instalar un software llamado NSClient++ que es el equivalente del usado en los sistemas Unix, el NRPE. El NSClient++ se puede descargar de la página Web del proyecto Nagios3, y al igual que su homónimo de los sistemas GNU/Linux y Unix, se proporciona en los DVD/CD de software que se han preparado para este proyecto de implementación de la Red de Base de Datos de Gestión Ciudadana o también se pueden extraer del repositorio que se ha montado en una de las máquinas de gestión de central.

Es importante que entre la máquina de monitorización y la máquina monitorizada se pueda conectar directamente, y aunque en los requerimientos de Nagios3 para Windows no se especifica la necesidad de poder conectar mediante SSH, en este proyecto y por razones de seguridad se ha decidido aplicar esta capa adicional de seguridad ya que a través de los paquetes SNMP enviados por Nagios se puede extraer mucha información valiosa para un atacante al sistema. Para que no haya problemas con la conexión, habrá que tener en cuenta el usuario de monitorización local de la máquina y que se tengan preparadas las claves RSA pertinentes para que no de problemas en las conexiones.

En el esquema situado bajo estas líneas se puede ver el esquema funcional de este sistema de monitorización contra una máquina Microsoft/Windows.



Al igual que en los sistemas Unix y GNU/Linux, el sistema de monitorización, por defecto facilita muy pocos datos, esto se solucionará con scripts adicionales y plugins. Todos ellos se reflejarán en los anexos a este proyecto.

Sistemas de electrónica de red

La monitorización de sistemas de electrónica de red tiene casi menos requisitos que los sistemas GNU/Linux y Unix ya que Nagios solo necesita consultar unos pocos datos en estos sistemas.

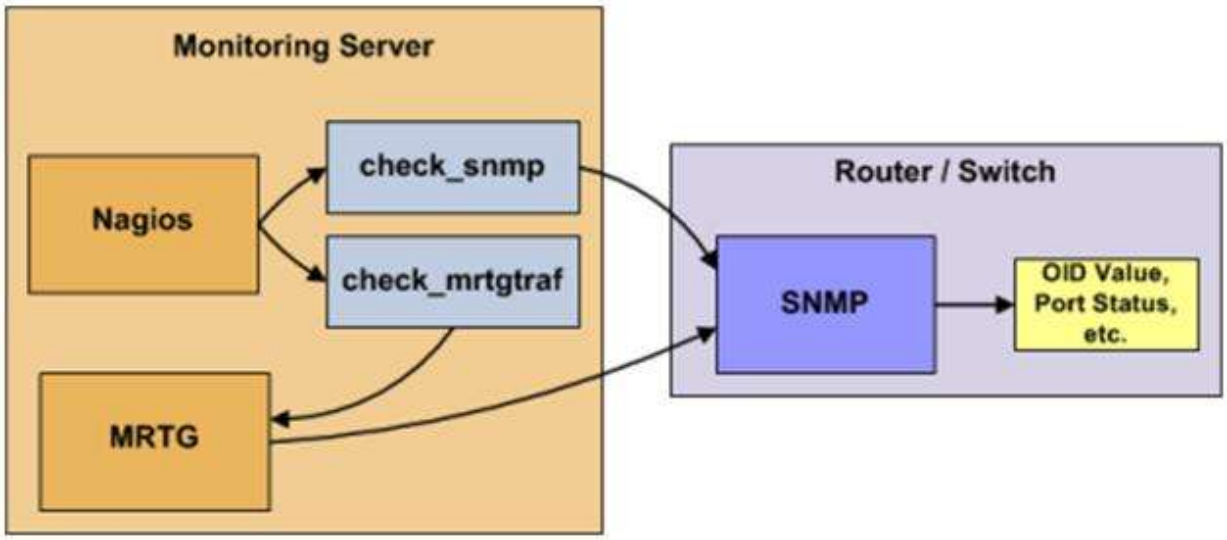
En este caso se deberá instalar un software compatible con SNMP y el aparato en cuestión, este software es el equivalente del usado en los sistemas Unix, el NRPE y el NSClient++ de Windows. Al igual que en los demás casos se puede descargar de la página Web del proyecto Nagios3, y al igual que su homónimo de los sistemas GNU/Linux y Unix, se proporciona en los DVD/CD de software que se han preparado para este proyecto de implementación de la Red de Base de Datos de Gestión Ciudadana o también se pueden extraer del repositorio que se ha montado en una de las máquinas de gestión de central.

Es importante que entre la máquina de monitorización y la máquina monitorizada se pueda conectar directamente, y aunque en los requerimientos de Nagios3 para la monitorización de sistemas de

electrónica de red no se especifica la necesidad de poder conectar mediante SSH, en este proyecto y por razones de seguridad se ha decidido aplicar esta capa adicional de seguridad ya que a través de los paquetes SNMP enviados por Nagios se puede extraer mucha información valiosa para un atacante al sistema.

Para que no haya problemas con la conexión, habrá que tener en cuenta el usuario de monitorización local de la máquina y que se tengan preparadas las claves RSA pertinentes para que no de problemas en las conexiones.

En el esquema situado bajo estas líneas se puede ver el esquema funcional de este sistema de monitorización contra un sistema basado en electrónica de red, que en nuestro caso va a ser siempre basada en los sistemas Cisco Catalyst.



Al igual que en los sistemas Unix, GNU/Linux y Microsoft/Windows, el sistema de monitorización, por defecto facilita muy pocos datos, esto se solucionará con scripts adicionales y plugins. Todos ellos se reflejarán en los anexos a este proyecto.

Monitorización de sistemas gestores de bases de datos

La monitorización de sistemas gestores de bases de datos tiene que ser montada mediante plugins adicionales por encima de los agentes de monitorización NRPE o NSClient++ ya que las bases de datos estarán montadas o bien sobre sistemas Unix y GNU/Linux o bien sobre sistemas Microsoft/Windows por lo que los requisitos para la monitorización de una base de datos son requerimientos adicionales.

El software instalado tanto en el servidor como en el cliente para la monitorización del sistema gestor de base de datos, al igual que en los demás casos se puede descargar de la página Web del proyecto Nagios3, y al igual que su homónimo de los sistemas GNU/Linux y Unix, se proporciona en los DVD/CD de software que se han preparado para este proyecto de implementación de la Red de Base de Datos de Gestión Ciudadana o también se pueden extraer del repositorio que se ha montado en una de las máquinas de gestión de central.

En este caso se deberá monitorizar tres tipos de bases de datos principalmente:

- Bases de datos Oracle.
- Bases de datos MySQL.

- Bases de datos de servicios de directorio.

Monitorización de servicios

Antes de comenzar a explicar los servicios que se monitorizan en esta explotación, se va hacer mención general a unos determinados aclaraciones.

- Host: Llamamos host a cualquier máquina que queramos monitorizar. Estas pueden ser servidores (en cualquier tipo de plataforma), impresoras de red, routers, switches, Urls … Todos ellos deben de tener una ip para poder ser monitorizados.En nuestro caso se ha decidido controlar únicamente máquinas de Bases de datos, de OAS (Orale Aplication Server) y URLS de Aplicaciones Web.

- Service: también llamado servicio, estos se aplicaran sobre uno o varios host. Se encargará de ejecutar un comando sobre un host y nos devolverá el resultado. Existen múltiples servicios, los más comunes son el ping, ssh, estado de discos, estado de los puertos de red, nivel de memoria…

- Tiempos de chequeos: Se establece unos determinados tiempos de chequeo para cada servicio.

Servicios monitorizados

En este primer paso se va a hacer una definición de los servicios monitorizados.

Chequeos de base de datos

- Comunicación con servidor: Este servicio se encarga de comprobar la conectividad entre el servidor de Nagios y la maquina, ejecutando un ping a su dirección ip.

- Acceso vía SSH: Comprueba si es posible acceder a la máquina por ssh.

- Socket para Oracle: Monitoriza el puerto del listener (1521) de la máquina de base de datos a través de su interfaz VIP, esta interfaz es utilizada para las conexiones de BBDD.

    - Estado del Listener: Este tipo de servicio se encarga de ejecutar un tsnping sobre el servicio del listener que se está ejecutando en la máquina de BBDD.

    - Tsnping a Instancia: Se ejecuta un Tnsping al servicio asociado a la instancia de la BBDD de la máquina a controlar.

    - Conexión con BBDD_X: Se encarga de ejecutar una conexión mediante SQL*PLUS a la instancia de la BBDD. Si la consulta es ejecutada correctamente, la base de datos está disponible para los usuarios. Esta conexión se realiza con el usuario soporte.

    - Process Acounting BBDD_X: Mediante la ejecución de una consulta sobre la instancia de la base de datos se obtiene el número de procesos ejecutados contra la BBDD.

    - Bloqueos Base de datos BBDD_X: Se ejecuta una consulta sobre una instancia para detectar si existen algún bloqueo sobre la BBDD.

Chequeos de Oracle Aplication Server

- Puerto Web no Seguro abierto: Este servicio se encargará de chequear si el puerto 80 se encuentra abierto.

- Puerto Web seguro abierto: Este servicio se encargará de chequear si el puerto 443 se encuentra abierto.

- Aplicación Web Online: Mediante este servicio se comprobará si el acceso a una URL está disponible para los usuarios. Para este servicio existen diferentes tipos de chequeos, se detallará para cada uno más adelante.

Las configuraciones de Nagios se dan en los anexos.

8.7 Disposición de los sistemas de backup

En esta sección se pasará a realizar una descripción somera de la arquitectura de backup o de copias de seguridad. Una vez obtenidos los requerimientos de las aplicaciones, los servicios de infraestructura, y los requerimientos expresados por el cliente.

En el momento del despliegue, se ha planteado una arquitectura de backup para el nodo central, otra para nodo respaldo y otras cuatro para los nodos locales. Cada nodo tiene un entorno de copias de seguridad independiente, con sus servidores de backup y al menos una librería de cintas. Estos sistemas estarán dedicados exclusivamente a realizar los backup de los sistemas de su nodo.

La administración se puede realizar a través de las herramientas de administración desde el propio nodo o realizando conexiones remotas a las herramientas desde el nodo central para así poder dar servicio de asesoramiento por parte del equipo de administradores de central.

En los siguientes apartados se describe la arquitectura de copias de seguridad de cada uno de los nodos existentes actualmente. Otro punto importante es que la arquitectura y políticas de copias de seguridad en cada uno de los nodos se pretende que sea bastante similar y homogénea con pequeñas licencias para poder adaptarse en cada nodo para cumplir sus particularidades específicas.

También hay que tener en cuenta que el haber elegido una arquitectura de backup homogénea podrá posibilitar que se lleven piezas de un nodo a otro en caso de necesidad, sacrificando la funcionalidad de copias de seguridad en un nodo mientras otro nodo recibe las piezas pertinentes de ese nodo para poder hacer las copias. Esto no debería ser necesario ya que se ha contratado un sistema de mantenimiento y SLA que aseguran evitar esta posibilidad.

Diseño de la solución en el nodo central

La arquitectura de backup descrita en esta solución contiene dos redes independientes para gestionar el almacenamiento de tipo SAN, que posibilita gestionar datos entre los servidores de backup y la librería de cintas a gran velocidad, y la red de comunicaciones de tipo Local Area Network, que permite la comunicación entre clientes de backup y el servidor máster de backup.

La arquitectura de backup del nodo central es común para los entornos de desarrollo, preproducción y producción aunque se ha definido la necesidad de tener cabinas de cintas adicionales para poder hacer copias de seguridad en caso de caída de la cabina principal.

Otro tema importante a tener en cuenta es que estas cabinas adicionales se pueden apuntar hacia las redes de desarrollo o preproducción para aprovechar por el momento su productividad para conseguir optimizar el rendimiento de la cabina principal optimizando así su ancho de banca y minimizando el tiempo empleado en hacer las copias de seguridad.

El software que se ha utilizado para implementar las copias de seguridad en esta explotación es Symantec Netbackup en su versión 6.5 garantizando también sus actualizaciones durante los próximos tres años desde la firma de la adjudicación del proyecto.

Las librerías sobre la que se realizarán las copias de seguridad a archivo de gran tiempo de permanencia es una librería de cintas L500 que se puede encontrar en dos configuraciones distintas, de dos drives y de seis drives.

Ambas configuraciones utilizarán cintas de tipo LTO3 y además, en caso de decidirse que sea necesario se pueden montar un sistema de puenteo para realizar las copias temporales sobre los discos SATA de la cabina de discos.

Se ha descrito la necesidad de utilizar un servidor master de backup en este nodo que se establecerá en un servidor de gestión que compartirá esta funcionalidad con otros roles como el NTP, LDAP, etc.

Este servidor es el servidor principal del entorno de backup y tiene el control total sobre las librerías de cintas, las políticas de backup y otros servidores de backup secundarios.

Los clientes de backup envían la información al master de backup a través de la red LAN y este servidor gestionara el envío a las unidades de copia de seguridad. Con este propósito, todos los clientes de backup tienen conectados a la red común de backup y a la red de gestión on enlaces de alto rendimiento a un 1Gb.

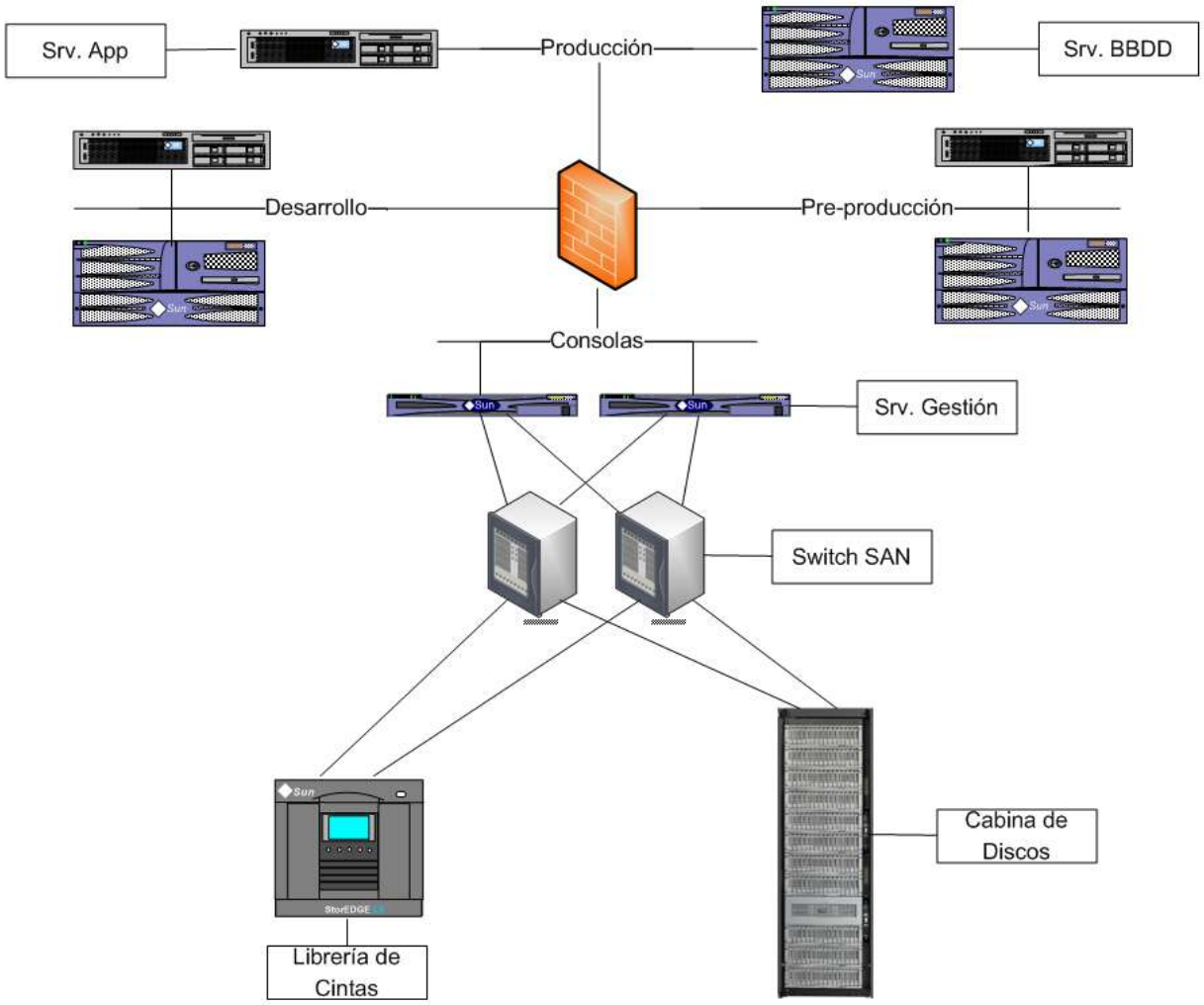
En el proyecto se ha determinado la necesidad de establecer diferentes redes de backup según el dominio de servicio de red al que pertenecen los sistemas. Esto es derivado de los parámetros de seguridad de red. La comunicación entre las distintas redes de backup donde se ubican los clientes y la red de backup donde se encuentra el servidor master, se realizan mediante el ajuste de una serie de parámetros en los firewall de la explotación.

Tal como se ha citado anteriormente, existen unos servidores de almacenamiento intermedios que reciben el nombre de servidores Media Server que son servidores de backup SAN y que pueden copiar sus datos locales directamente a las librerías sin pasar a través del master Server. En esta explotación, estos servidores media Server son los que contienen los sistemas de bases de datos de producción a través de la SAN ya que su importancia hace que sea imprescindible garantizar unas copias de seguridad correctas en todo momento.

Esta característica es necesaria en aquellos sistemas que manejan un volumen de datos elevado, como los servidores de bases de datos de producción.

También se ha establecido la necesidad de realizar las copias de seguridad de las bases de datos de producción en caliente sin necesidad de parar las bases de datos ya que en esta explotación se encuentra la necesidad de dar servicio las 24 horas del día y los 365 días del año.

En el caso de las máquinas de preproducción y desarrollo se ha definido la necesidad de hacer una copia de seguridad a disco, para posteriormente copiar estos datos a cinta. Esta forma de backup permite hacer copias en modo raw que aceleran la gestión de estos backups.



Diseño de la solución en el nodo de respaldo

La arquitectura de backup descrita en este nodo sigue el mismo modelo que el de nodo central. Contiene dos redes independientes para gestionar el almacenamiento de tipo SAN, que posibilita gestionar datos entre los servidores de backup y la librería de cintas a gran velocidad, y la red de comunicaciones de tipo Local Area Network, que permite la comunicación entre clientes de backup y el servidor master de backup.

A diferencia del nodo central, este nodo tiene una sola cabina y solo tiene red de producción.

Al igual que en todos los nodos, el software que se ha utilizado para implementar las copias de seguridad en esta explotación es Symantec Netbackup en su versión 6.5 garantizando también sus actualizaciones durante los próximos tres años desde la firma de la adjudicación del proyecto.

Las librerías sobre la que se realizarán las copias de seguridad a archivo de gran tiempo de permanencia es una librería de cintas L500 en una configuración de seis drives. Esta configuración utiliza cintas de tipo LTO3 y además, en caso de decidirse que sea necesario se pueden montar un sistema de puenteo para realizar las copias temporales sobre los discos SATA de la cabina de discos.

Se ha descrito la necesidad de utilizar un servidor master de backup en este nodo que se establecerá en un servidor de gestión que compartirá esta funcionalidad con otros roles como el NTP, LDAP, etc. El

servidor principal del entorno de backup y tiene el control total sobre las librerías de cintas, las políticas de backup y otros servidores de backup secundarios.

Los clientes de backup envían la información al master de backup a través de la red LAN y este servidor gestionara el envío a las unidades de copia de seguridad. Con este propósito, todos los clientes de backup tienen conectados a la red común de backup y a la red de gestión on enlaces de alto rendimiento a un 1Gb.

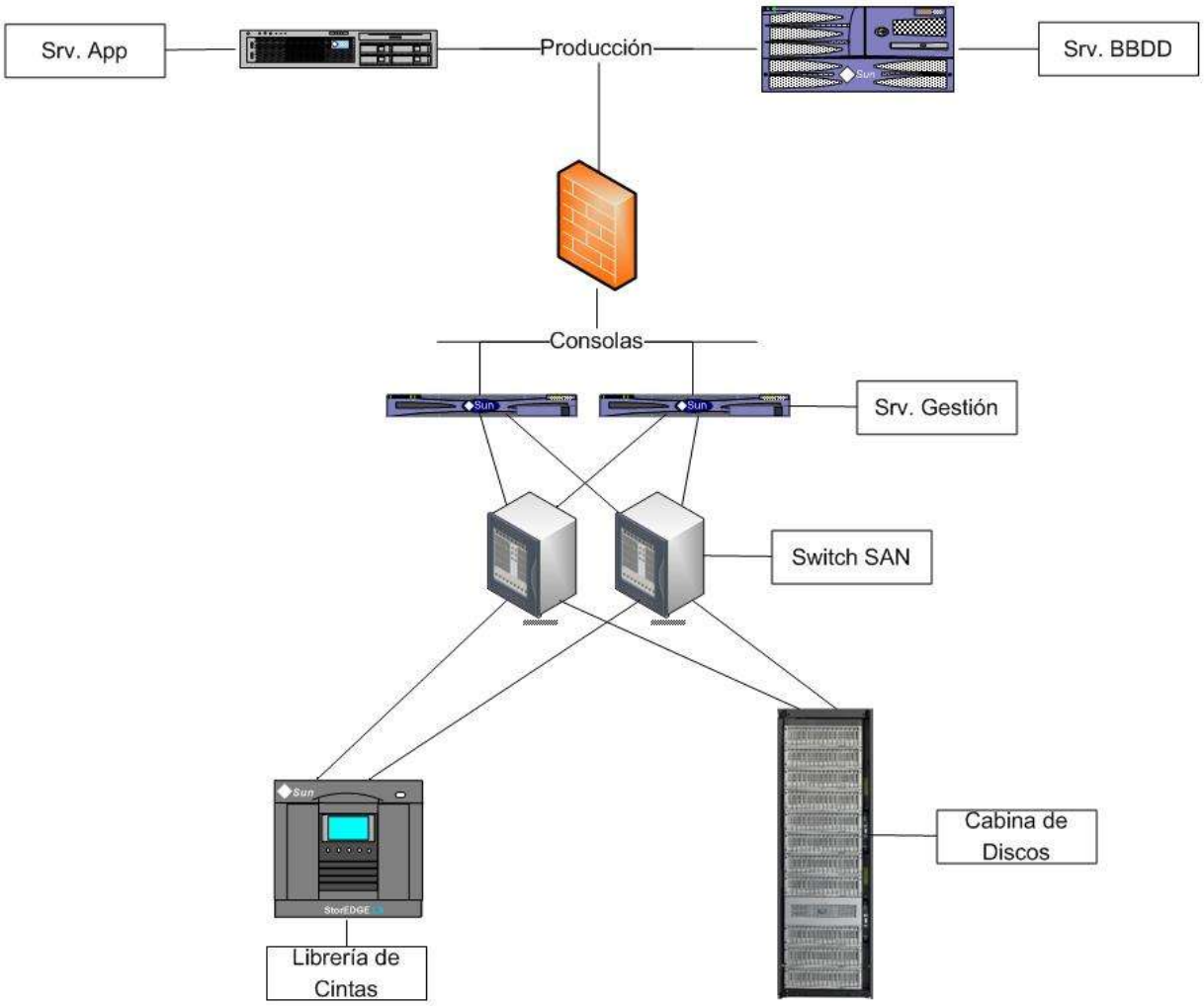
En el proyecto se ha determinado la necesidad de establecer diferentes redes de backup según el dominio de servicio de red al que pertenecen los sistemas. Esto es derivado de los parámetros de seguridad de red. La comunicación entre las distintas redes de backup donde se ubican los clientes y la red de backup donde se encuentra el servidor master, se realizan mediante el ajuste de una serie de parámetros en los firewall de la explotación.

Tal como se ha citado anteriormente, existen unos servidores de almacenamiento intermedios que reciben el nombre de servidores Media Server que son servidores de backup SAN y que pueden copiar sus datos locales directamente a las librerías sin pasar a través del master Server. En esta explotación, estos servidores media Server son los que contienen los sistemas de bases de datos de producción a través de la SAN ya que su importancia hace que sea imprescindible garantizar unas copias de seguridad correctas en todo momento.

Esta característica es necesaria en aquellos sistemas que manejan un volumen de datos elevado, como los servidores de bases de datos de producción.

También se ha establecido la necesidad de realizar las copias de seguridad de las bases de datos de producción en caliente sin necesidad de parar las bases de datos ya que en esta explotación se encuentra la necesidad de dar servicio las 24 horas del día y los 365 días del año.

En el caso de las máquinas de preproducción y desarrollo se ha definido la necesidad de hacer una copia de seguridad a disco, para posteriormente copiar estos datos a cinta. Esta forma de backup permite hacer copias en modo raw que aceleran la gestión de estos backups.



Diseño de la solución en el nodo de Calatayud

La arquitectura de backup descrita en este nodo sigue el mismo modelo que el de nodo central.

Contiene dos redes independientes para gestionar el almacenamiento de tipo SAN, que posibilita gestionar datos entre los servidores de backup y la librería de cintas a gran velocidad, y la red de comunicaciones de tipo Local Area Network, que permite la comunicación entre clientes de backup y el servidor master de backup.

Este nodo tiene una sola cabina para trabajar sobre la red de producción ya que no tiene desarrollo ni preproducción.

El software que se ha utilizado para implementar las copias de seguridad en esta explotación es Symantec Netbackup en su versión 6.5 garantizando también sus actualizaciones durante los próximos tres años desde la firma de la adjudicación del proyecto.

Las librerías sobre la que se realizarán las copias de seguridad a archivo de gran tiempo de permanencia es una librería de cintas L500 en una configuración de seis drives. Esta configuración utiliza cintas de tipo LTO3 y además, en caso de decidirse que sea necesario se pueden montar un sistema de puenteo para realizar las copias temporales sobre los discos SATA de la cabina de discos.

Se ha descrito la necesidad de utilizar un servidor master de backup en este nodo que se establecerá en un servidor de gestión que compartirá esta funcionalidad con otros roles como el NTP, LDAP, etc. El servidor principal del entorno de backup y tiene el control total sobre las librerías de cintas, las políticas de backup y otros servidores de backup secundarios.

Los clientes de backup envían la información al master de backup a través de la red LAN y este servidor gestionara el envío a las unidades de copia de seguridad. Con este propósito, todos los clientes de backup tienen conectados a la red común de backup y a la red de gestión on enlaces de alto rendimiento a un 1Gb.

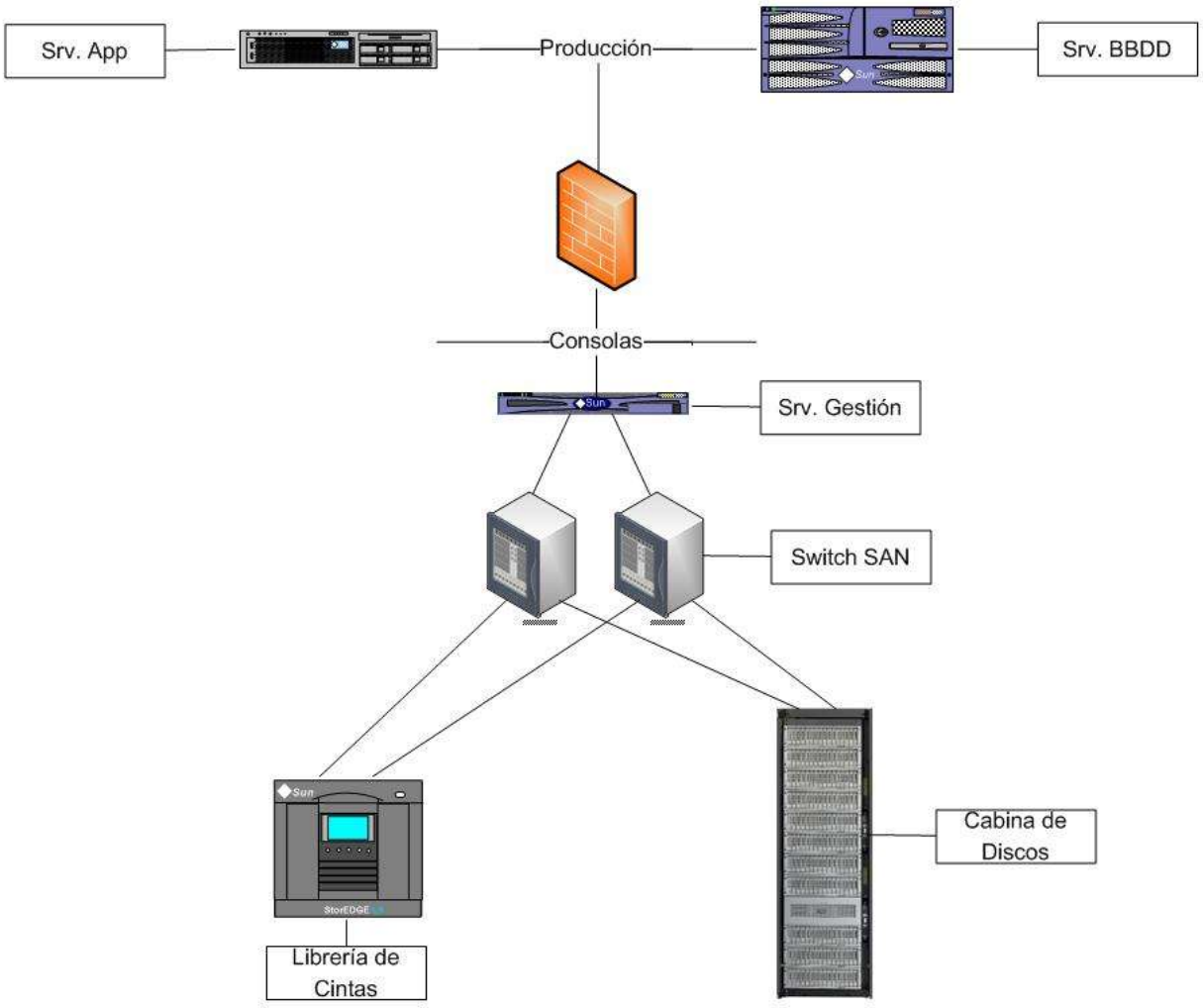
En el proyecto se ha determinado la necesidad de establecer diferentes redes de backup según el dominio de servicio de red al que pertenecen los sistemas. Esto es derivado de los parámetros de seguridad de red. La comunicación entre las distintas redes de backup donde se ubican los clientes y la red de backup donde se encuentra el servidor master, se realizan mediante el ajuste de una serie de parámetros en los firewall de la explotación.

Tal como se ha citado anteriormente, existen unos servidores de almacenamiento intermedios que reciben el nombre de servidores Media Server que son servidores de backup SAN y que pueden copiar sus datos locales directamente a las librerías sin pasar a través del master Server. En esta explotación, estos servidores media Server son los que contienen los sistemas de bases de datos de producción a través de la SAN ya que su importancia hace que sea imprescindible garantizar unas copias de seguridad correctas en todo momento.

Esta característica es necesaria en aquellos sistemas que manejan un volumen de datos elevado, como los servidores de bases de datos de producción.

También se ha establecido la necesidad de realizar las copias de seguridad de las bases de datos de producción en caliente sin necesidad de parar las bases de datos ya que en esta explotación se encuentra la necesidad de dar servicio las 24 horas del día y los 365 días del año.

En el caso de las máquinas de preproducción y desarrollo se ha definido la necesidad de hacer una copia de seguridad a disco, para posteriormente copiar estos datos a cinta. Esta forma de backup permite hacer copias en modo raw que aceleran la gestión de estos backups.



Diseño de la solución en el nodo de Jaca

La arquitectura de backup descrita en este nodo sigue el mismo modelo que el de nodo central. Contiene dos redes independientes para gestionar el almacenamiento de tipo SAN, que posibilita gestionar datos entre los servidores de backup y la librería de cintas a gran velocidad, y la red de comunicaciones de tipo LAN (Local Area Network), que permite la comunicación entre clientes de backup y el servidor master de backup.

A diferencia del nodo central, este nodo tiene una sola cabina de dos drives para trabajar sobre todas las redes como producción, desarrollo y preproducción.

Al igual que en todos los nodos, el software que se ha utilizado para implementar las copias de seguridad en esta explotación es Symantec Netbackup en su versión 6.5 garantizando también sus actualizaciones durante los próximos tres años desde la firma de la adjudicación del proyecto.

Las librerías sobre la que se realizarán las copias de seguridad a archivo de gran tiempo de permanencia es una librería de cintas L500 en una configuración de seis drives. Esta configuración utiliza cintas de tipo LTO3 y además, en caso de decidirse que sea necesario se pueden montar un sistema de puenteo para realizar las copias temporales sobre los discos SATA de la cabina de discos.

Se ha descrito la necesidad de utilizar un servidor master de backup en este nodo que se establecerá en un servidor de gestión que compartirá esta funcionalidad con otros roles como el NTP, LDAP, etc. El

servidor principal del entorno de backup y tiene el control total sobre las librerías de cintas, las políticas de backup y otros servidores de backup secundarios.

Los clientes de backup envían la información al master de backup a través de la red LAN y este servidor gestionara el envío a las unidades de copia de seguridad. Con este propósito, todos los clientes de backup tienen conectados a la red común de backup y a la red de gestión on enlaces de alto rendimiento a un 1Gb.

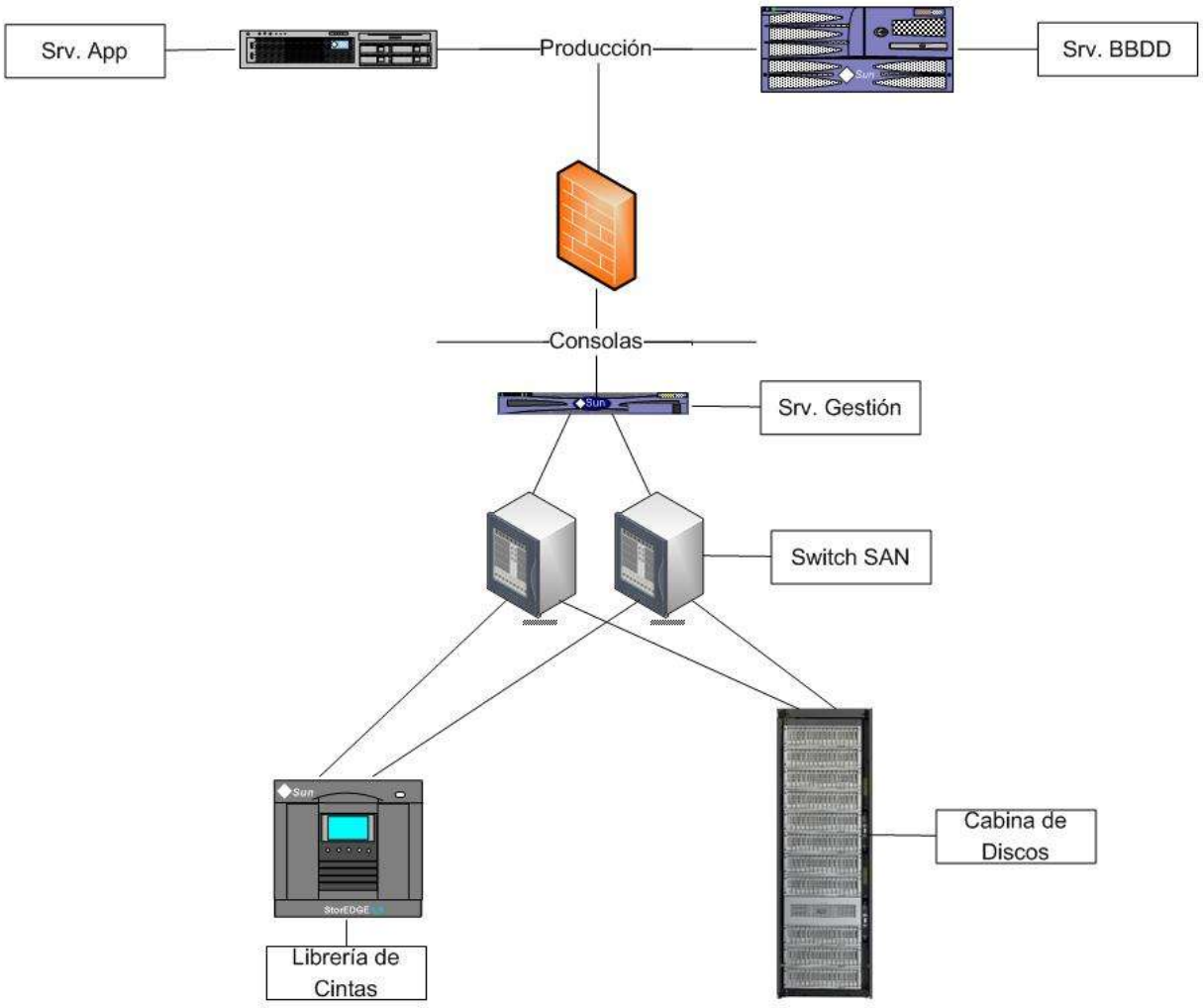
En el proyecto se ha determinado la necesidad de establecer diferentes redes de backup según el dominio de servicio de red al que pertenecen los sistemas. Esto es derivado de los parámetros de seguridad de red. La comunicación entre las distintas redes de backup donde se ubican los clientes y la red de backup donde se encuentra el servidor master, se realizan mediante el ajuste de una serie de parámetros en los firewall de la explotación.

Tal como se ha citado anteriormente, existen unos servidores de almacenamiento intermedios que reciben el nombre de servidores Media Server que son servidores de backup SAN y que pueden copiar sus datos locales directamente a las librerías sin pasar a través del master Server. En esta explotación, estos servidores media Server son los que contienen los sistemas de bases de datos de producción a través de la SAN ya que su importancia hace que sea imprescindible garantizar unas copias de seguridad correctas en todo momento.

Esta característica es necesaria en aquellos sistemas que manejan un volumen de datos elevado, como los servidores de bases de datos de producción.

También se ha establecido la necesidad de realizar las copias de seguridad de las bases de datos de producción en caliente sin necesidad de parar las bases de datos ya que en esta explotación se encuentra la necesidad de dar servicio las 24 horas del día y los 365 días del año.

En el caso de las máquinas de preproducción y desarrollo se ha definido la necesidad de hacer una copia de seguridad a disco, para posteriormente copiar estos datos a cinta. Esta forma de backup permite hacer copias en modo raw que aceleran la gestión de estos backups.



Diseño de la solución en el nodo de Teruel

La arquitectura de backup descrita en este nodo sigue el mismo modelo que el de nodo central. Contiene dos redes independientes para gestionar el almacenamiento de tipo SAN, que posibilita gestionar datos entre los servidores de backup y la librería de cintas a gran velocidad, y la red de comunicaciones de tipo LAN (Local Area Network), que permite la comunicación entre clientes de backup y el servidor master de backup.

Este nodo tiene una sola cabina para trabajar sobre todas las redes como producción, desarrollo y preproducción.

Al igual que en todos los nodos, el software que se ha utilizado para implementar las copias de seguridad en esta explotación es Symantec Netbackup en su versión 6.5 garantizando también sus actualizaciones durante los próximos tres años desde la firma de la adjudicación del proyecto.

Las librerías sobre la que se realizarán las copias de seguridad a archivo de gran tiempo de permanencia es una librería de cintas L500 en una configuración de seis drives. Esta configuración utiliza cintas de tipo LTO3 y además, en caso de decidirse que sea necesario se pueden montar un sistema de puenteo para realizar las copias temporales sobre los discos SATA de la cabina de discos.

Se ha descrito la necesidad de utilizar un servidor master de backup en este nodo que se establecerá en un servidor de gestión que compartirá esta funcionalidad con otros roles como el NTP, LDAP, etc. El

servidor principal del entorno de backup y tiene el control total sobre las librerías de cintas, las políticas de backup y otros servidores de backup secundarios.

Los clientes de backup envían la información al master de backup a través de la red LAN y este servidor gestionara el envío a las unidades de copia de seguridad. Con este propósito, todos los clientes de backup tienen conectados a la red común de backup y a la red de gestión on enlaces de alto rendimiento a un 1Gb.

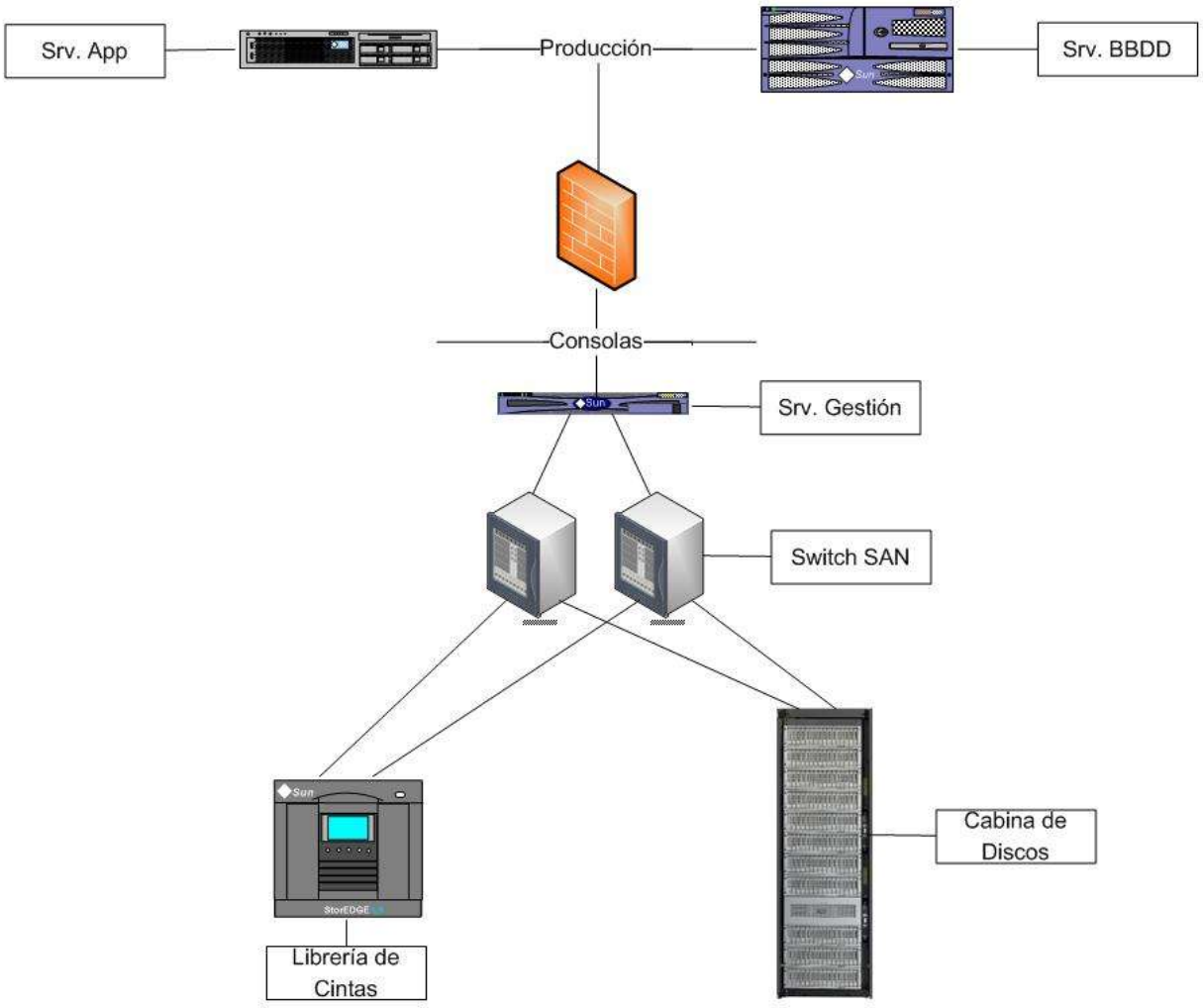
En el proyecto se ha determinado la necesidad de establecer diferentes redes de backup según el dominio de servicio de red al que pertenecen los sistemas. Esto es derivado de los parámetros de seguridad de red. La comunicación entre las distintas redes de backup donde se ubican los clientes y la red de backup donde se encuentra el servidor master, se realizan mediante el ajuste de una serie de parámetros en los firewall de la explotación.

Tal como se ha citado anteriormente, existen unos servidores de almacenamiento intermedios que reciben el nombre de servidores Media Server que son servidores de backup SAN y que pueden copiar sus datos locales directamente a las librerías sin pasar a través del master Server. En esta explotación, estos servidores media Server son los que contienen los sistemas de bases de datos de producción a través de la SAN ya que su importancia hace que sea imprescindible garantizar unas copias de seguridad correctas en todo momento.

Esta característica es necesaria en aquellos sistemas que manejan un volumen de datos elevado, como los servidores de bases de datos de producción.

También se ha establecido la necesidad de realizar las copias de seguridad de las bases de datos de producción en caliente sin necesidad de parar las bases de datos ya que en esta explotación se encuentra la necesidad de dar servicio las 24 horas del día y los 365 días del año.

En el caso de las máquinas de preproducción y desarrollo se ha definido la necesidad de hacer una copia de seguridad a disco, para posteriormente copiar estos datos a cinta. Esta forma de backup permite hacer copias en modo raw que aceleran la gestión de estos backups.



Diseño de la solución en el nodo de La Muela

La arquitectura de backup descrita en este nodo sigue el mismo modelo que el de nodo central. Contiene dos redes independientes para gestionar el almacenamiento de tipo SAN, que posibilita gestionar datos entre los servidores de backup y la librería de cintas a gran velocidad, y la red de comunicaciones de tipo LAN (Local Area Network), que permite la comunicación entre clientes de backup y el servidor master de backup.

Este nodo tiene una sola cabina de un drive para trabajar sobre todas las redes como producción, desarrollo y preproducción.

Al igual que en todos los nodos, el software que se ha utilizado para implementar las copias de seguridad en esta explotación es Symantec Netbackup en su versión 6.5 garantizando también sus actualizaciones durante los próximos tres años desde la firma de la adjudicación del proyecto.

Las librerías sobre la que se realizarán las copias de seguridad a archivo de gran tiempo de permanencia es una librería de cintas L500 en una configuración de seis drives. Esta configuración utiliza cintas de tipo LTO3 y además, en caso de decidirse que sea necesario se pueden montar un sistema de puenteo para realizar las copias temporales sobre los discos SATA de la cabina de discos.

Se ha descrito la necesidad de utilizar un servidor master de backup en este nodo que se establecerá en un servidor de gestión que compartirá esta funcionalidad con otros roles como el NTP, LDAP, etc. El

servidor principal del entorno de backup y tiene el control total sobre las librerías de cintas, las políticas de backup y otros servidores de backup secundarios.

Los clientes de backup envían la información al master de backup a través de la red LAN y este servidor gestionara el envío a las unidades de copia de seguridad. Con este propósito, todos los clientes de backup tienen conectados a la red común de backup y a la red de gestión on enlaces de alto rendimiento a un 1Gb.

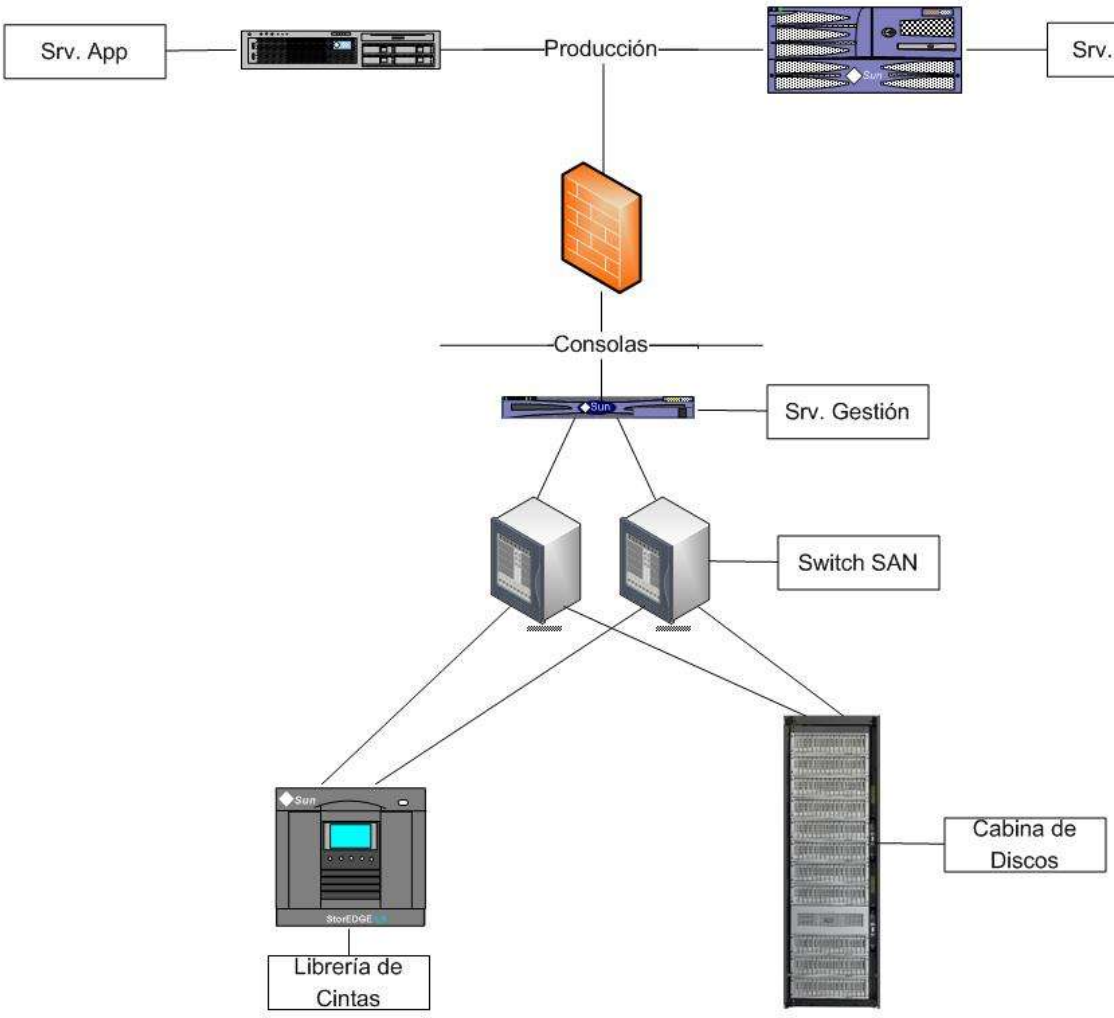
En el proyecto se ha determinado la necesidad de establecer diferentes redes de backup según el dominio de servicio de red al que pertenecen los sistemas. Esto es derivado de los parámetros de seguridad de red. La comunicación entre las distintas redes de backup donde se ubican los clientes y la red de backup donde se encuentra el servidor master, se realizan mediante el ajuste de una serie de parámetros en los firewall de la explotación.

Tal como se ha citado anteriormente, existen unos servidores de almacenamiento intermedios que reciben el nombre de servidores Media Server que son servidores de backup SAN y que pueden copiar sus datos locales directamente a las librerías sin pasar a través del master Server. En esta explotación, estos servidores media Server son los que contienen los sistemas de bases de datos de producción a través de la SAN ya que su importancia hace que sea imprescindible garantizar unas copias de seguridad correctas en todo momento.

Esta característica es necesaria en aquellos sistemas que manejan un volumen de datos elevado, como los servidores de bases de datos de producción.

También se ha establecido la necesidad de realizar las copias de seguridad de las bases de datos de producción en caliente sin necesidad de parar las bases de datos ya que en esta explotación se encuentra la necesidad de dar servicio las 24 horas del día y los 365 días del año.

En el caso de las máquinas de preproducción y desarrollo se ha definido la necesidad de hacer una copia de seguridad a disco, para posteriormente copiar estos datos a cinta. Esta forma de backup permite hacer copias en modo raw que aceleran la gestión de estos backups.



Diseño de las políticas de backup

En los sistemas de todos los nodos se pueden identificar los siguientes tipos de información:

- Datos del sistema operativo (GNU/Linux o GNU/Linux).
- Datos de los binarios de aplicaciones.
- Datos de las base de datos.

Los datos del sistema operativo y los binarios de aplicaciones, incluidos los programas desarrollados para los servidores de aplicaciones, tienen una tasa de modificación baja y una criticidad media.

Esto hace que se defina una política de backup que copie estos datos de forma completa en horario nocturno una vez a la semana durante el fin de semana y de forma incremental acumulativa los días laborables.

Estos tipos de información tienen una naturaleza común por lo que se copiaran en un pool compartido.

Los datos de las bases de datos tienen una tasa de modificación más alta y una criticidad muy alta para esta explotación. La política de copias de seguridad para estos datos es realizar copia completa todos los días en horario nocturno, enviando estos datos a un pool de cintas dedicado.

Las bases de datos de producción realizan copias en caliente sin parar las bases de datos mediante RMAN (Utilidad de Oracle para los backups de bases de datos).

Las bases de datos de preproducción y desarrollo realizan copia en frío con RMAN a disco SATA, y posteriormente se copia a cinta.

Será en estos otros puntos donde se diferencie la gestión de unos nodos frente a otros, dado que como se ha dicho anteriormente, solo nodo central tiene desarrollo y preproducción.

El entorno de desarrollo se ha montado sobre un sistema de contenedores de aplicaciones desarrollado sobre la funcionalidad de GNU/Linux Containers, comúnmente llamadas zonas.

Las zonas, tal como se hablará posteriormente es un sistema de virtualización similar a Hyper-V de Microsoft o VirtualBox de Sun Microsystem, pero que está integrado directamente sobre el kernel de GNU/Linux 10, a partir de la release 11/06.

El backup de este entorno de desarrollo se realizara, haciendo copia total del sistema operativo que hace las veces de host. Para ello previamente realizará la parada de todos los sistemas de desarrollo virtualizados. Este sistema de parada se implementará mediante scripts realizados en Korn Shell para mayor integración sobre el sistema operativo.

Las copias completas se duplicarán de tal forma que se procederá a tener una copia dentro de la librería de cintas y sacar la segunda copia del pool de duplicados a una localización externa segura. Este tema se trata en un apartado posterior para explicar como se gestiona el envío y almacenaje de las copias de seguridad.

La limpieza de los drives LTO3 de la librería es internamente autogestionada por la librería.

Preparación de cintas

Las cintas de backup de este proyecto se agrupan según un criterio de pools de volúmenes por el Media Manager.

La configuración de los “volume pools” y una breve explicación se muestra en la siguiente tabla:

Volume pools	Descripción
Netbackup	Las cintas de este pool se usan para hacer backup de su base de datos.
None	Configurado por defecto.
DataStore	Configurado por defecto.
Catalog	Pool necesario para el backup en caliente de la base de datos de Netbackup.

Unix	Pool de cintas para las copias de Unix/Linux.
Windows	Pool de cintas para las copias de Windows.
Oracle	Pool de cintas para las copias de bases de datos de Oracle.
Duplicación	Pool de duplicación de copias de seguridad.
Semanales	Pool de copias de seguridad semanales.
Anuales	Pool de copias de seguridad de 1, 3 y 5 años.
Scratch	Todas las cintas nuevas están en este pool. Este pool se usa para dar cintas a los pools.
Scratch II	Todas las cintas nuevas están en este pool. Remanente.
Extract	Pool para la extracción. Se usa para aparcar las cintas antes de extraerlas de la cabina.

Las cintas se identifican y son gestionadas de manera automática por la librería de cintas, gracias al código de barras que se ha establecida de manera única en cada uno de los cartuchos.

Al hacer el inventario del robot de cintas y para dar de alta las cintas en el gestor de copias de seguridad se pueden especificar reglas en función de los códigos de barras. Usando para que se muevan a un pool de cintas concreto.

Tal como se ha mostrado en el cuadro situado sobre estas líneas, todas las cintas que se dan de alta como nuevas pertenecen al pool “Scratch”, de donde Netbackup las coge y las usa en función de sus necesidades.

Periodos de retención

Los periodos de retención de cintas establecen el tiempo que tardará una cinta en volver a ser usada desde que se saca de la cabina de cintas y se guarda en un depósito creado para tal propósito.

En la siguiente tabla muestra los periodos de retención definidos por defecto en el sistema de copias de seguridad Netbackup. Estos periodos son los que se ha decidido usar en esta explotación durante la implementación, pero existen hasta 24 niveles de retención que pueden ser modificados por el administrador para adaptarse a cualquier tipo de necesidad.

Nivel de retención	Periodo de retención
0	Una semana
1	Dos semanas
2	Tres semanas

3	Un mes
4	Dos meses
5	Tres meses
6	Seis meses
7	Nueve meses
8	Un año
9	Tres años
10	Cinco Años
11	Infinito (Sin expiración)

Las cintas de una semana se suelen usar para sistemas de desarrollo sin importancia, aunque lo más común para estos backups suele ser las copias de dos semanas o un mes. Las copias para sistemas productivos usadas a diario son las de dos semanas, mientras que las copias de carácter semanal se guardarán durante al menos un mes.

Las copias de mayor alcance se utilizan para temas varios, como el almacenamiento para la continuidad de negocio en caso de catástrofe o para depósitos legales o judiciales.

Las copias de dos meses se envían a otros nodos como se mostrará en un punto posterior, para replicar o guardar copias más o menos actuales de los sistemas. Este envío se realizará de manera cruzada. Enviando las de central a respaldo, las de respaldo a central y las de los nodos a otros nodos y a central.

Las copias de seguridad de 6 meses, uno, tres y cinco años se almacenarán en una empresa especializada en la protección de datos para poder hacer uso de ellas en caso de necesitarse una restauración de urgencia, una evacuación a respaldo cuando falla la replicación y los mecanismos de evacuación a respaldo o para ser usados en caso de necesidad en un juicio u otro evento legal.

Limpieza de las cabinas de cintas

Las librerías de cintas se encargan de manera automática de la limpieza de los drives gracias a la función “auto cleaning” que tiene activada.

Cada una de las cabinas, tiene un slot por drive reservado para la cinta de limpieza. Esto quiere decir que un robot con 2 drives tendrá 2 cintas de limpieza y un drive de 6 cintas tendrá 6 cintas de limpieza. Cada una de las cintas de limpieza tiene un límite de 50 usos.

La extracción de las cintas de limpieza de cada uno de los módulos de backup se debe hacer manualmente a través de la consola de Netbackup o a través de los interfaces hardware situados en la parte frontal de las cabinas de cintas.

Disposición de las copias de RMAN

En la esta sección se detallan brevemente las configuraciones y los scripts utilizados para ejecutar las políticas de copia de seguridad en caliente de Oracle en Netbackup. El agente de Oracle proporcionan una pasarela a RMAN para que pueda hacer backup contra la librería de

Cintas, por lo que hace un paso intermedio que no se hace en las copias de backup de sistema operativo o de datos simples.

A continuación se muestra una relación de servidores de bases de datos de Oracle o que poseen bases de datos Oracle por distintos motivos:

- Sistemas de bases de datos de producción.
- Sistemas de bases de datos de preproducción.
- Sistemas de bases de datos de desarrollo.
- Sistemas de bases de datos implícitos en Netbackup.
- Sistemas de bases de datos implícitos en sistemas de monitorización.

Para que Oracle pueda comunicarse de manera fiable y correcta con NetBackup, las librerías de Oracle deben ser sustituidas por las proporcionadas junto con el agente de Oracle para Netbackup.

Esta cambio se realiza mediante un procedimiento que se pude leer en la documentación anexa en los módulos referentes a las bases de datos de los Anexos por lo que no se perderá el tiempo aquí en describirlo con detalle. Bastará para el lector, saber que este cambio se realiza mediante un link simbólico. Este procedimiento es un linkado de las librerías que se ejecutan durante el proceso de instalación del agente de Netbackup.

Los scripts que son ejecutados desde la política de Netbackup tienen la forma aproximada

/opt/oracle/admin/<SID>/backup/rman/, y se puede sustituir el <SID> de la base de datos pertinente.

Script	Descripción
Bkpdb_<SID>.sh	Backup completo de la base de datos.
Bkpak_<SID>.sh	Backup de los archivos.

La copia de seguridad del catálogo de RMAN se debe realizar cuando este está apagado o fuera de línea (offline), y se lanza desde una política de Netbackup ejecutando los scripts que residen en el servidor de gestión dedicado a las copias de seguridad.

Antes de hacer la copia de seguridad de los ficheros y los directorios que componen el "Oracle Recovery Catalog" usando la política "Oracle_Catalogo_RMAN", se debe proceder a realizar una parada de la base de datos (shutdown) de la base de datos mediante el uso de un script de notificación de Netbackup.

Este script está ubicado en el servidor de copias de seguridad de cada uno de los sectores, incluyendo central y respaldo, y más concretamente en la carpeta de ejecutables de netbackup. (/usr/openv/netbackup/bin).

Existe un script previo a la ejecución del backup. Está destinado a preparar la base de datos de catalogo RMAN para ser copiada. Este script se añadirá también a los scripts situados en los anexos de este proyecto.

Después de hacer la copia de seguridad de los ficheros y los directorios que componen el "Oracle Recovery Catalog" usando la política "Oracle_Catalogo_RMAN", se debe proceder a realizar un arranque de la base de datos (startup) mediante el uso de un script de notificación de Netbackup. Este script ha sido creado para tal propósito y es el llamado "bpend_notify.Oracle_Catalogo_RMAN".

Este script está ubicado en el servidor dedicado a la copia de seguridad y más concretamente en el directorio donde se almacenan los ejecutables del sistema de copias de seguridad Netbackup, el directorio es "/usr/openv/netbackup/bin".

Tras finalizar el backup, el script "bpend" ejecuta una llamada a un script encargado de arrancar la base de datos del catalogo de RMAN, este script es "start_ORMG001.sh" y también se puede ver en los anexos de este proyecto.

El sistema que se ha descrito sobre estas líneas es el encargado de hacer las copias de RMAN o mejor dicho de las bases de datos de Oracle.

Externalización de las cintas de backup

En una explotación como la que nos ocupa, nada puede quedar al azar. Por eso se ha decidido que las cintas de las copias de seguridad son demasiado valiosas para depender de una empresa no especializada como la nuestra.

Por este motivo se ha buscado y se ha determinado que lo mejor es subcontratar este apartado a una empresa que durante los próximos años se encargará de recoger, transportar y almacenar en un dentro seguro las copias de seguridad que se vayan extrayendo de las cabinas de cintas.

Un dato a tener en cuenta es que la empresa dejará una serie de cajas ignífugas en la explotación que los operadores de backup irán llenando con las cintas que extraigan hasta que la empresa contratada para la gestión del backup pase a recogerlas.

Se ha descrito la necesidad de que la recogida se realice al menos una vez a la semana. Siendo el mejor día para la recogida el viernes por la tarde ya que en ese momento ya se han extraído los backups de uno, tres y cinco años que van directamente a un lugar seguro.

A la empresa concesionaria de la gestión de los backups se le ha pedido que sea capaz de transportar los backups en furgones blindados similares a los que se usen en los transportes de dinero de los bancos. Esta necesidad subyace de la delicadeza de los datos que se contienen en algunas cintas ya que contienen datos tales como los números de cuenta, los pagos a haciendo o los datos del INEM.

Siguiendo estas premisas se ha encontrado una empresa que tiene una sede en Aragón, concretamente en el polígono Centrovía de La Muela. Esta empresa es Iron Mountain, una empresa de origen estadounidense que tiene ya una gran andadura en este campo y que cuenta con numerosos galardones por su eficacia en estas tareas.

Además de esta extracción programada y subcontrata, se ha descrito un sistema de intercambio de cintas entre los distintos nodos que componen este proyecto para así ser capaces de recuperar un nodo en caso de catástrofe sacando las cintas del nodo al que fueron enviadas. Este método es por así decirlo el sistema de contingencia por si falla el plan de contingencia de primer nivel.

Estudio de las políticas de backup

A continuación se hace un desglose de cada una de las políticas y como se configuran en el programa de copias de seguridad netbackup.

Estas se dan en los anexos.

9.Bibliografía

Durante la elaboración de este trabajo se han consultado diversas fuentes. Entre ellas podemos citar las que a continuación se detallan, ya que las demás pertenecen a la documentación clasificada de la explotación donde he trabajado durante los últimos años o trabajo en la actualidad.

La organización de esta bibliografía se ha realizado siguiendo un ordenamiento alfabético y no dependiente de la importancia ya que podemos encontrar que temas secundarios como el servidor Web se encuentran por delante del sistema operativo o la base de datos.

DNS: Sistema de resolución de nombres de dominio

- Dns and Bind
  Autor: Cricket Liu, Paul Albitz, Mike Loukides
  Editorial: O'Reilly
  ISBN-10: 8173660492

GNU/Linux

El proyecto GNU-Linux cuenta con incontables colaboradores que apoyan el proyecto de distintas formas. Una de las más conocidas es la documentación. Es imposible por tanto reflejar todas las fuentes empleadas en este proyecto. Seleccionaremos algunas de las más importantes.

- Linux. Guía para administradores de redes.
  Bautts, Tony; Dawson, Terry; Purdy, Gregor N.
  Editorial: Anaya.
  ISBN: 8441518688.

- Red Hat Linux: Manual del administrador.
  Ibrahim Haddad; Richard Peterien.
  Editorial McGraw-Hill.

- Ajuste y planificación con Linux.
  Jason Fink; Matthew Sherer; Clave Informática I+D.
  Pearson Educación.
  ISBN: 8420533882.

- Linux: Manual de referencia.
  Richard Petersen.
  Editorial: McGraw-Hill.
  ISBN: 8448131746.

- Curso de Linux.
  Autor: Schroder, Carla.
  Editorial: Anaya Multimedia.
  ISBN: 8441518572.

- Administración de sistemas Linux.
  Autor: Adelstein, Tom;Lubanovic, Hill.
  Editorial: McGraw-Hill.
  ISBN: 9788441522343.

- Seguridad en servidores Linux.
  Autor: Bauer, Michael D.
  Editorial: Anaya Multimedia.
  ISBN: 8441518777

- Fedora 5 and Red Hat Enterprise Linux 4 Bible.
  Autor: Christopher Negus.
  Editorial: Wiley.
  ISBN-10: 0471754919

Herramientas

- SSH, The Secure Shell: The Definitive Guide
  Autor: Daniel J. Barrett, Richard E. Silverman, Robert G. Byrnes
  Editorial: O'Reilly Media
  ISBN-10: 0596008953

- Network Security with OpenSSL
  Autor: John Viega, Matt Messier, Pravir Chandra
  Editorial: O'Reilly Media
  ISBN-10: 059600270X

- Sendmail, 3rd Edition
  Autor: Bryan Costales, Eric Allman
  Editorial: O'Reilly Media
  ISBN-10: 1565928393

LDAP

- LDAP System Administration
  Autor: Gerald Carter
  Editorial: O'Reilly Media
  ISBN-10: 1565924916

- Implementing LDAP
  Autor: Mark Wilcox
  Editorial: Peer Information
  ISBN-10: 1861002211

- Mastering OpenLDAP: Configuring, Securing and Integrating Directory Services
  Autor: Matt Butcher
  Editorial: Packt Publishing
  ISBN-10: 184719102

- Kerberos: The Definitive Guide
  Autor: Jason Garman
  Editorial: O'Reilly Media
  ISBN-10: 0596004036

- La comunidad de Open LDAP: http://www.openldap.org/

- La comunidad de Open LDAP en castellano: http://www.ldap-es.org/

Nagios

La documentación necesaria para la elaboración de la parte relacionada con la monitorización de sistemas con Nagios se ha extraído de la página Web de dicho proyecto, y más concretamente de la sección de documentación del mismo: http://www.nagios.org/docs/

La documentación empleada ha sido:

- Nagios Version 2.0 Documentation.
- Nagios Version 3.0 Documentation.
- Nagios NDOUTILS Documentation Version 1.4.
- Nagios NDOUtils Database Model.
- Nagios NRPE Documentation.

Adicionalmente se ha contado con los siguientes libros:

- Nagios: System And Network Monitoring.
  Autor: Wolfgang Barth
  Editorial: No Starch Press, Inc
  ISBN: 1593270704

- El Tao de la monitorización de la seguridad en redes.
  Autor: Richard Bejtlich.
  Editorial: Pearson-Addison Wesley.
  ISBN: 0-321-24677-2.

- The Nagios Book
  Autor: Chris Burgués
  Editorial: Free.

- Pro Nagios 2.0
  Autor: Turnbull, James
  Editorial: Pearson-Addison Wesley.
  ISBN: 1-59059-609-9

- Nagios 3 Enterprise Network Monitoring
  Autor: Schubert, Max
  Editorial: Syngress
  ISBN: 978-1-59749-267-6

Por último y en menor medida se ha hecho uso de las siguientes URLs:

- Nagios Community Wiki : http://www.nagioscommunity.org/wiki/

- Nagios Books: http://www.nagiosbook.org/

Samba y NFS

- Using Samba (O'Reilly System Administration)
  Autor: Robert Eckstein, David Collier-Brown, Peter Kelly
  Editorial: O'Reilly Media
  ISBN-10: 1565924495

Scripts

- Learning the bash Shell (In a Nutshell)
  Autor: Cameron Newham.
  Editorial: O'Reilly.
  ISBN-10: 0596009658.

- Learning the vi Editor (6th Edition)
  Autor: Linda Lamb, Arnold Robbins
  Editorial: O'Reilly Media
  ISBN-10: 1565924266

- Classic Shell Scripting
  Autor: Arnold Robbins, Nelson H.F. Beebe
  Editorial: O'Reilly Media
  ISBN-10: 0596005954

- Mastering Regular Expressions
  Autor: Jeffrey Friedl
  Editorial: O'Reilly Media
  ISBN-10: 0596528124

Veritas Netbackup

En el desarrollo de este proyecto se han utilizado los siguientes documentos electrónicos de Veritas NetBackup 6.0 que han sido extraídos del CD de documentación que acompaña a dicho software. Se ha dividido en varios grupos:

- Servidor UNIX (Sun/GNU/Linux).

- Operación del software.

- Cliente Microsoft/Windows.

- Cliente UNIX (Sun/GNU/Linux).

- Operación con BBDD.

Servidor UNIX: (Sun/GNU/Linux)

- MediaMgr_AdminGuide_Unix
- MediaMgr_DeviceConfig_Guide
- NetBackup_AdminGuide_HighAvailability

Operación del software

- NetBackup_AdminGuide_AdvancedClient
- NetBackup_AdminGuide_BMR
- NetBackup_AdminGuide_Encryption
- NetBackup_AdminGuide_NDMP
- NetBackup_AdminGuide_Vault
- NetBackup_Troubleshoot_Guide
- NetBackup_OperGuide_Vault

10. RELACIÓN DE DOCUMENTOS

MEMORIA……...……71 HOJAS DIN A-4
PRESUPUESTO ……..…….. ..11 HOJAS DIN A-4
ANEXOS……...……...…….350 HOJAS DIN A-4

En La Muela a 11 de junio de 2010.

Fdo: Juan Ignacio Oller Aznar
El Proyectista

Fdo: Oller Aznar, Juan Ingnacio

El Proyectista
