PROYECTO:

INTEGRACIÓN DE UNA RED CORPORATIVA UNIFICADA

PRESENTACIÓN

REALIZADO POR:

OLLER AZNAR, JUAN IGNACIO

JUNIO - 2010

ÍNDICE

Oller Aznar, Juan Ignacio

PRESENTACIÓN DEL PROYECTO

VISIÓN GENERAL

En el presente proyecto se trata de presentar el modo de **realizar el despliegue de una plataforma de producción y gestión** para una gran empresa.

En la **solución propuesta** se realiza el estudio de una serie de máquinas, sistemas operativos y aplicaciones que efectuarán las labores de servicio al usuario y a los distintos segmentos de la empresa y por otro lado se estudian las aplicaciones y servicios que deberán ejercer labores de infraestructura para que todos esos sistemas lleguen a ser productivos.

En la **solución desarrollada** se genera el despliegue de una serie de aplicaciones que se han seleccionado como las mejores a todos los efectos. Entre los puntos que se estudian, destacarán la continuidad de negocio y la seguridad de los datos.

El proyecto desarrollado constará de las siguientes partes:

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.

Entre las aplicaciones y servicios descritos en el punto anterior se trataran, planificarán y desplegarán sistemas tales como:

- **LDAP Nativo** para validación de máquinas y usuarios en el dominio.
- **DNS interno** para la gestión de resolución de nombres del dominio.
- **NTP** (Network Time Protocol) para la sincronización de los sistemas.
- **NFS y SMB** para los servidores de archivos distribuido para Unix y para Windows.
- **Sistemas de monitorización** para la gestión SNMP de sistemas hardware y de los sistemas software.
- **Servidores Web** para servir las aplicaciones asociadas a la gestión de la empresa.
- **Sistema de copias de seguridad** de sistema operativo, aplicaciones y bases de datos.

BREVE ANOTACIÓN PREVIA A LA PRESENTACIÓN

Finalmente se ha decidido encaminar el proyecto más hacia la **implantación de una solución basada en software libre** en detrimento de la parte que trataba el **despliegue de la red corporativa**.

DESGLOSE DE OBJETIVOS

Los **parámetros usados para la selección de las máquinas destinadas a dar servicio** en este proyecto, tanto en lo referente a la red de servicio como la de gestión, son sobre todos destinados a aportar rendimiento y redundancia a fallos, buscándose máquinas capaces de trabajar incluso con averías severas o mientras se les cambian piezas. También se mirará la posibilidad de clusterizarlas.

A la hora de seleccionar las **cabinas de almacenamiento**, se ha buscado una solución de alto rendimiento pero que permita ampliaciones modulares y la implementación de varios tipos de discos para así usar los de alto rendimiento para las aplicaciones que lo necesiten (Ej.: bases de datos) mientras que los repositorios de datos con poca tasa de acceso se destinarán a espacios de almacenamiento con menores prestaciones pero con igual fiabilidad frente a fallos. Así mismo, la explotación será dotada de aplicaciones que permitirán una gestión eficiente de las cabinas de discos.

La selección de las **librerías de cintas para el sistema de almacenamiento definitivo** se basa y de la solución de copias de seguridad se basa en una arquitectura de backup para el nodo central, otra para nodo respaldo y otras cuatro para los nodos locales. Cada nodo tendrá un entorno de copias de seguridad independiente, con sus servidores de backup y al menos una librería de cintas. La selección también tiene en cuenta que los dispositivos seleccionados son sistemas modulares y de una arquitectura 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. La administración de la selección se podrá realizar en remoto de manera centralizada o de manera local y descentralizada.

Las políticas de **copias de seguridad** de los sistemas operativos, aplicaciones, bases de datos y cabinas de discos se han planificado cuidadosamente intentando buscar una mayor optimización de los sistemas y del ancho de banda durante las transferencias intentando buscar el equilibrio y la eliminación de los cuellos de botella durante las copias de respaldo.

Para seleccionar las **aplicaciones y modificaciones de los sistema**s, así como las aplicaciones destinadas a aportar continuidad de servicio y redundancia frente a fallos se han seguido los criterios de buscar los sistemas que mejor se integrarán con la arquitectura existente. Entre las herramientas dedicadas a aportar continuidad de servicio se ha establecido la necesidad de clusterizar la electrónica de red, las conexiones de red, los servidores de aplicaciones y bases de datos así como los de servicios. Así mismo, se ha establecido un sistema de zonas y de sistemas virtuales para generar “jaulas” que favorecerán la continuidad de las aplicaciones de una máquina aunque caigan una o más de ellas.

Para dar **soporte** a todos los puntos anteriores se ha decidido usar una serie de aplicaciones que ayudaran a gestionar cada uno de los nodos del proyecto así como todas las aplicaciones del mismo. La infraestructura de gestión para los entornos de producción, preproducción y desarrollo del Nodo Central esta unificada en una serie de servidores Estos servidores realizan tareas de administración, monitorización, despliegue de software, copias de seguridad etc.

A continuación trataremos cada uno de ellos de manera independiente.

Se ha establecido la necesidad de desplegar un **servicio de LDAP nativo** cuya misión consiste en almacenar el repositorio de usuarios destinados a la administración y operación de los sistemas, así como las cuentas de los usuarios finales y de las distintas aplicaciones. La utilización del LDAP nativo permite gestionar usuarios de una forma centralizada y más segura. Esto 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, permite cumplir los estándares de seguridad de la información exigibles a un entorno de este tipo.

Se ha establecido la necesidad de desplegar un **servicio de resolución de nombres o DNS interno** utilizado exclusivamente dentro de la plataforma de este proyecto, no propagándose hacia el exterior. Este servicio de DNS es utilizado por los administradores de la plataforma, aplicaciones, y sistema de copias de seguridad para acceder a todos los servidores, siendo independiente de los servicios de resolución de nombres de cara al exterior que se desplegaría en un estado futuro o se contrataría a otra empresa.

Para la sincronización de la fecha y hora de todos los sistemas de todos los nodos se ha establecido la necesidad de desplegar un **servicio de configuración de tiempo por red (NTP)**. Este servicio es de vital importancia, sobre todo en los clústeres de aplicaciones y de bases de datos.

Se ha establecido la necesidad de un **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 (/export/home/$user).

Para realizar la **administración remota de los servicios** desde el exterior de la explotación y para enlazar las distintas sedes de la empresa, se ha establecido también la necesidad de implementar un servicio de conexión remota encriptada mediante un acceso seguro e intuitivo desde la propia plataforma y desde Internet a las distintas herramientas de gestión de los sistemas. Así mismo, esta estructura de administración remota basada en una conexión SSL-VPN es plenamente moldeable y adaptable a las necesidades de cada administrador y/o usuario autorizado.

Uno de los servicios mas importantes dentro de la administración es el despliegue de un **sistema de monitorización** con capacidad para la monitorización de sistemas operativos, aplicativos, bases de datos, electrónica de red y hardware de servidores. Este sistema se basará en un sistema capaz de tratar traps SNMP enviados por las máquinas y las aplicaciones cuando estas pasan por algún tipo de problema. Estos traps se mostrarán en tiempo real a los administradores y operadores que podrán trabajar de manera reactiva para atajar los problemas lo antes posible. Además de este uso, el sistema también debe guardar un repositorio histórico de los problemas ocasionados durante la vida útil de los sistemas.

Se ha descrito la necesidad de crear una red **corporativa que interconecte todos los nodos locales** contra un nodo central para unificar criterios, gestionar de manera centralizada los nodos y a la larga ahorrar costes de administración, de hardware y de software.

Así mismo, la **red conectará los nodos para asegurar la supervivencia de la explotación** tras la caída de una o más sedes del proyecto. La arquitectura propuesta describe un nodo central desde el que se puede administrar los demás nodos, uno de respaldo que tomará el relevo del nodo central y será capaz de realizar todas las funciones de este y por último cuatro nodos locales que harán las veces de oficinas

territoriales y que contarán con su propia red y sus propios equipos de gestión para poder operar de manera autónoma en caso de cortes de comunicaciones hacia la red troncal.

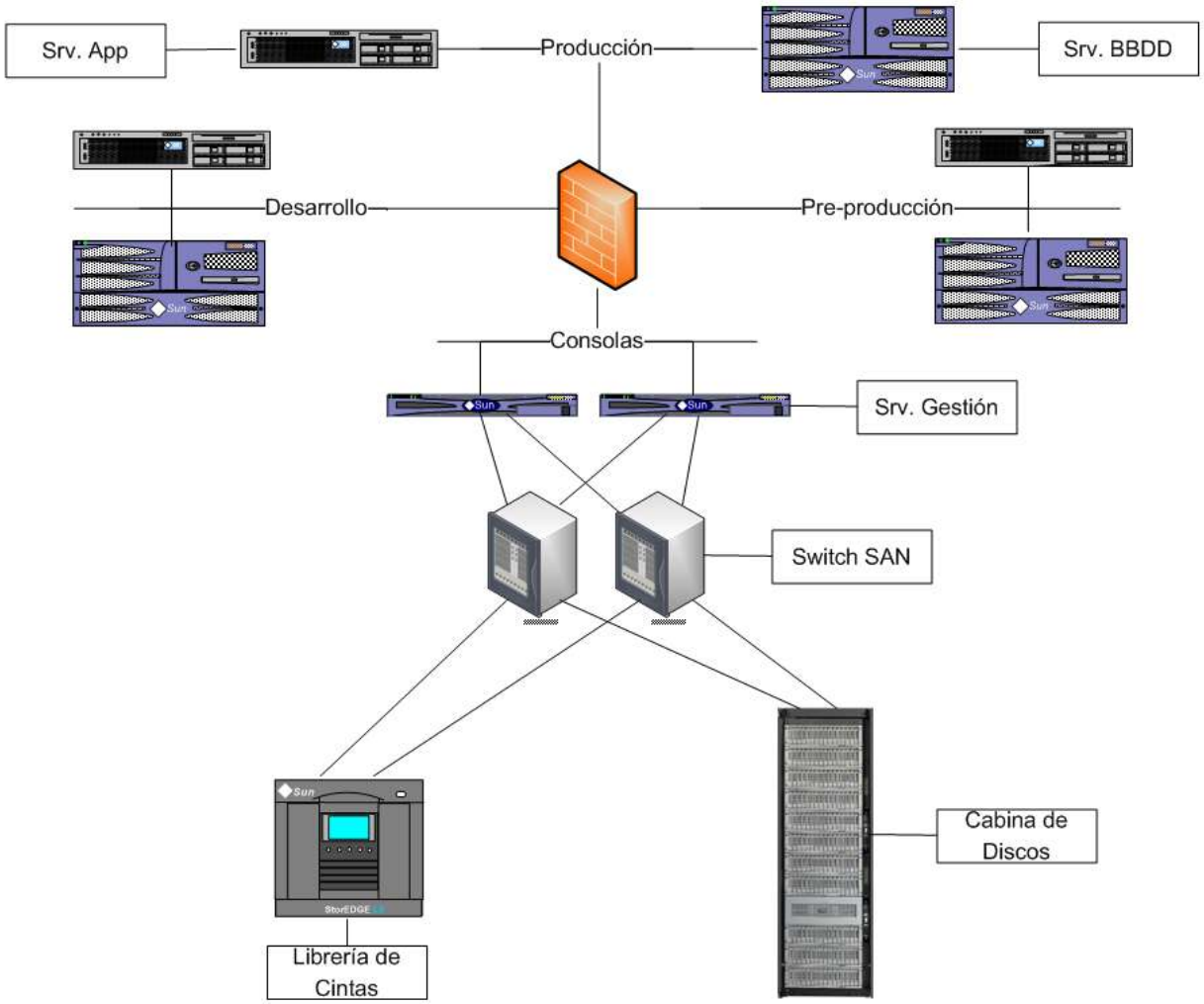
Para asegurar la **independencia de las redes implicadas en el proyecto** y separar de manera bien definida la función de cada una de ellas se han creado una serie de redes gestionadas por redes virtuales y protegidas por reglas de control de acceso y cortafuegos físicos y lógicos a nivel de sistema operativo.

SOLUCIÓN RESUMIDA

A continuación se da un breve repaso a las soluciones que se han considerado convenientes para dar servicio a esta empresa.

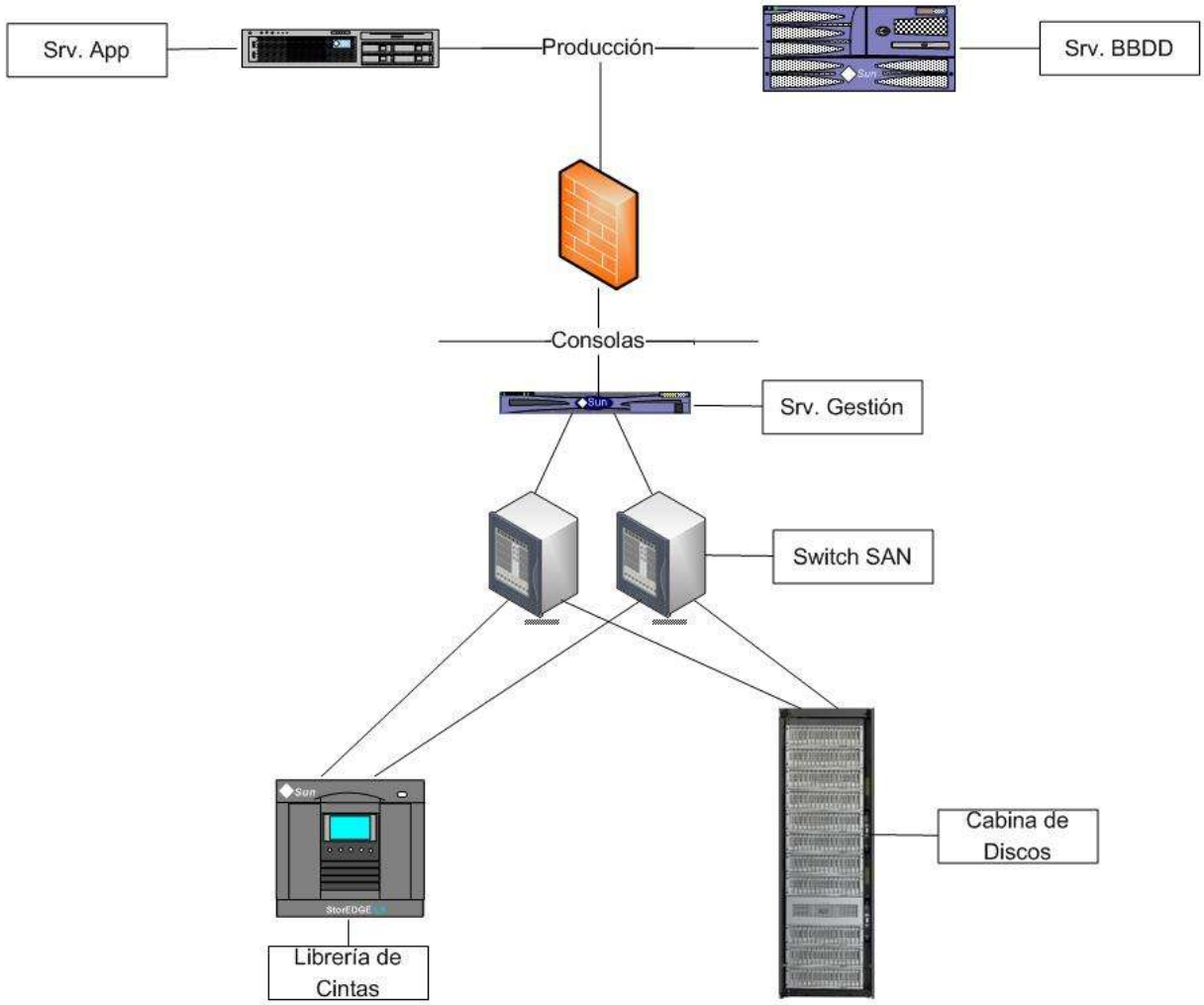
RED CORPORATIVA:

Se ha diseñado también la red corporativa con el objetivo de dar servicio a las aplicaciones y bases de datos que se desplieguen en la empresa. Así como para dar servicio a las aplicaciones ya existentes.



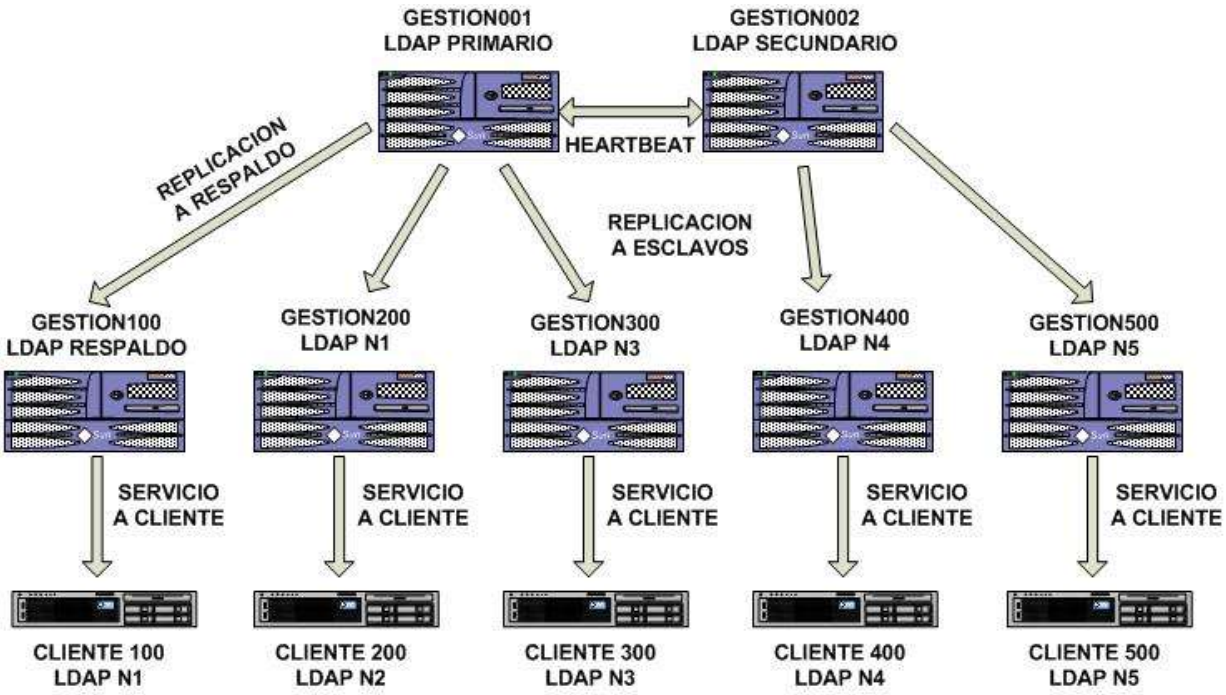
RED CORPORATIVA LOCAL:

Esta red se ha reproducido de manera independiente para los nodos locales para que puedan operar en caso de caída del enlace contra el nodo central. Como es lógico, las máquinas involucradas son mucho menos potentes y mucho menos numerosas.



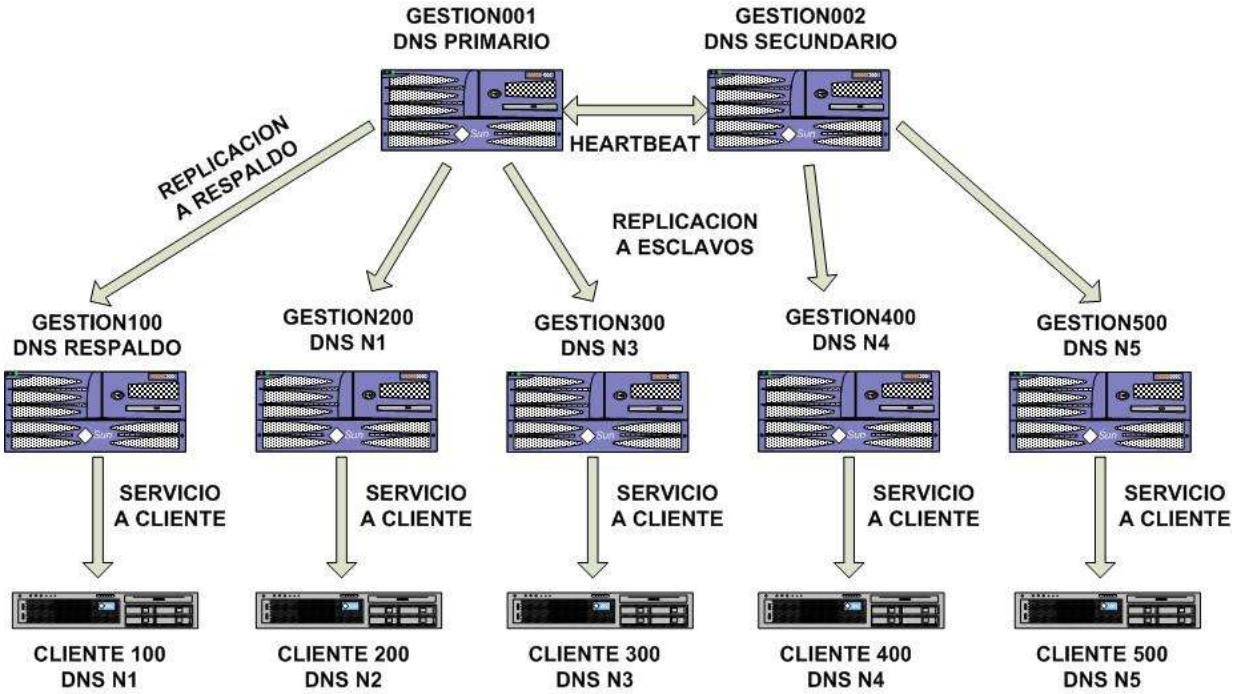
LDAP:

Se ha decidido implantar una estructura multimaster de servidores LDAP con una estructura de árbol hacia los nodos, añadiendo 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.



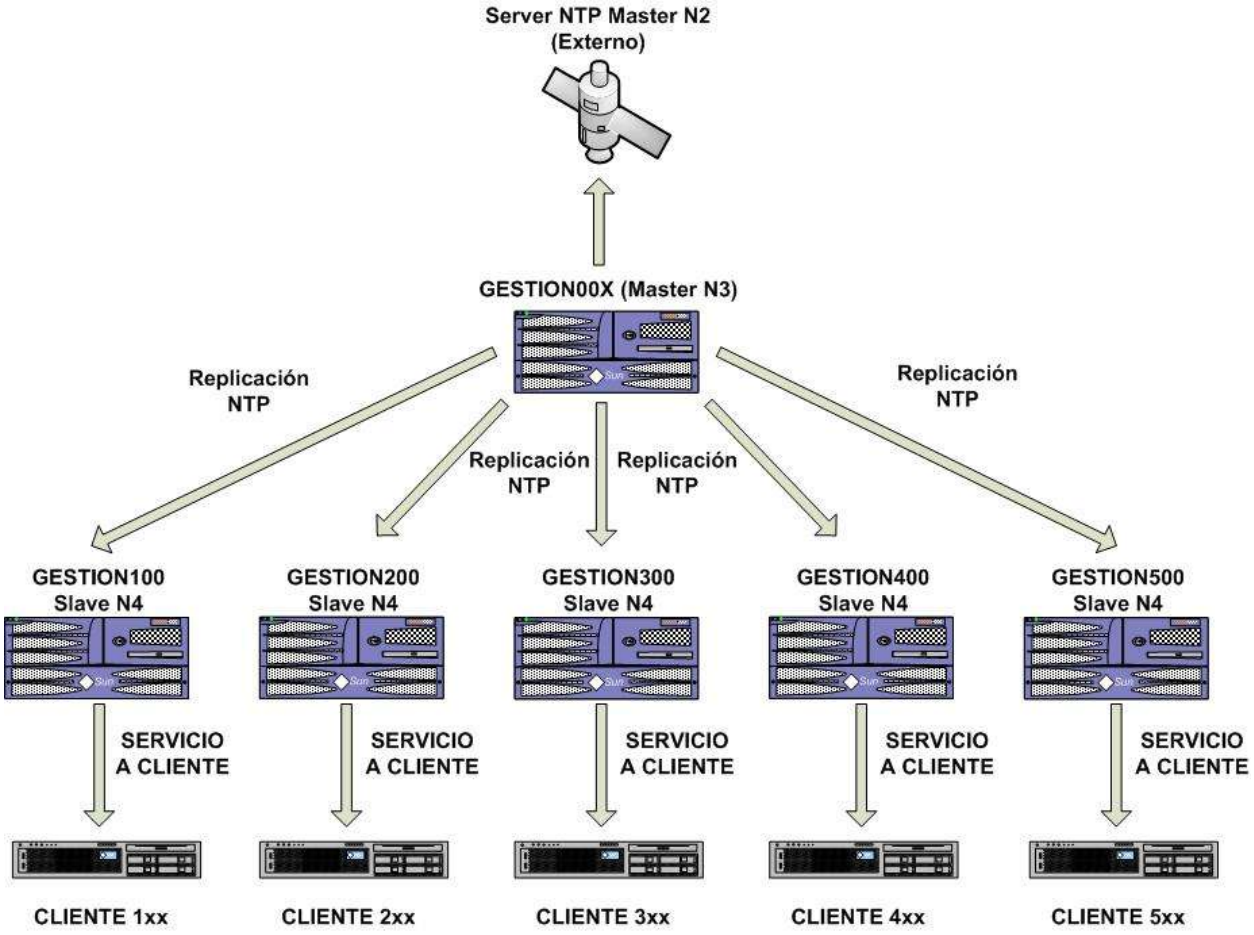
DNS:

Se define un servicio de resolución de nombres con un servidor primario de DNS, que 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.



NTP:

Se establece una red de servidores NTP para la sincronización horaria entre servidores de la explotación. De esta manera se conseguirá que estén sincronizados en tiempo y así los clústeres se sincronicen de manera correcta permitiendo un funcionamiento correcto y preciso.



HTTP:

Se establece una serie de servidores web para servir aplicaciones como los gestores de incidencias y gestores de contraseñas basados en PHP.

NFS y SMB:

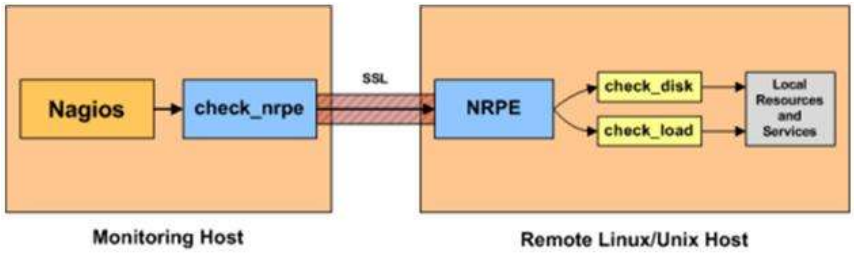
Se crea una red de servidores de archivos distribuidos de red basados en NFS y SMB para gestionar la compartición de ficheros con sistemas UNIX y Windows así como cualquier otro que se conecte a la red en un futuro.

SEGURIDAD:

Se instalan en todos los sistemas GNU/Linux los cortafuegos basados en IPTables con la ayuda de un sistema FWBuilder que mejor la interacción entre el usuario y la máquina y facilita la transición al usuario que hará las veces de mantenedor de la explotación.

MONITORIZACIÓN:

Se ha desplegado una solución de monitorización de la red, los hosts y los servicios basada en software libre utilizando para ello Nagios y Cacti aunque se ha creído que de ser necesario puede ser conveniente desplegar aplicaciones adicionales.



BACKUP:

Se ha diseñado también la red de almacenaje y acceso a discos para poder dar servicio a las aplicaciones y a su vez para permitir la replicación de datos entre dispositivos y frente a cabinas de almacenaje y cabinas de cintas de datos para archivo temporal o definitivo.