

STSM**MAIL**PLATFORM

PLATAFORMA AVANZADA
DE CORREO ELECTRÓNICO

DOCUMENTACIÓN TÉCNICA DICIEMBRE 2008



Tel.Fax: 966 446 046
www.soltecsis.com
comercial@soltecsis.com

STSMAILPLATFORM

ÍNDICE

1. INTRODUCCIÓN	04
2. ARQUITECTURA DEL SISTEMA	06
2.1. MAILBOX STORE CLUSTER	08
2.2. GRANJAS DE FRONTALES	08
2.3. WEBMAIL CLUSTER	10
2.4. REDES DE LA PLATAFORMA	10
2.5. MONITORIZACIÓN	11
2.6. SISTEMA DE APROVISIONAMIENTO	12
3. PLATAFORMAS DE PARTIDA	14
4. ADMINISTRACIÓN REMOTA	18
4.1. REGLETAS DE CONTROL DE CORRIENTE ePOWER.	19
4.2. SWITCHER KVM-IP	20

STSM**MAIL**PLATFORM

1. INTRODUCCIÓN

STSMAILPLATFORM

1. INTRODUCCIÓN

El abanico de servicios que Internet pone hoy en día a disposición de los usuarios es cada vez más amplio y variado. No obstante, estudios estadísticos del uso de servicios muestran que el **correo electrónico** sigue siendo, con gran diferencia, **el servicio más utilizado en Internet**.

Este dato estadístico es de utilidad para percibir la creciente importancia y relevancia que el servicio de correo electrónico tiene tanto en el sector empresarial como particular. Cada vez hay más empresas que dependen en gran medida del correo electrónico para poder desempeñar su área de negocio y para las cuales el no disponer de este servicio durante horas o días les puede suponer pérdidas económicas y de mercado considerables.

Por lo tanto, a la hora elegir un sistema de correo electrónico para nuestra empresa es de vital importancia tener muy presente tanto la calidad que a través del mismo es posible prestar al usuario final, como los mecanismos utilizados por el mismo para garantizar la máxima disponibilidad del servicio. La arquitectura de la solución de correo electrónico expuesta en este documento ha sido diseñada teniendo muy presentes estos requerimientos.

En el presente documento se describen los detalles tecnológicos más sobresalientes de que consta la plataforma de correo electrónico **STS-MAIL PLATFORM** ofertada por **SOLTECSIS SOLUCIONES TECNOLÓGICAS, S.L.** Como veremos, se trata de un completo sistema dotado con los **últimos avances** en lo que a materia de correo electrónico se refiere.

Uno de los puntos más fuertes de la plataforma es la opción de hacer uso de su arquitectura en **cluster** de **alta escalabilidad** y **alta disponibilidad**, gracias a la cual es posible disponer de un sistema de correo capaz de crecer con facilidad para soportar la carga creciente de usuarios, así como evitar la interrupción del servicio en el caso de que se produzca una avería de cualquier índole en un uno de los módulos de la plataforma.

La arquitectura de la plataforma es tan versátil que permite que la solución de correo electrónico **STS-MAIL PLATFORM** sea factible para cualquier empresa. Desde **pequeñas/medianas empresas** con unos pocos cientos o miles de buzones, para las cuales puede ser suficiente un único servidor de correo o un cluster de dos nodos, hasta **grandes empresas o ISPs** (*Internet Services Provider*) con cientos de miles o **millones de buzones**, para las cuales es ideal la arquitectura avanzada basada en granjas de frontales por servicios y el cluster multinodo utilizado para el almacenamiento de los buzones.

STSM**MAIL**PLATFORM

2. ARQUITECTURA DEL SISTEMA

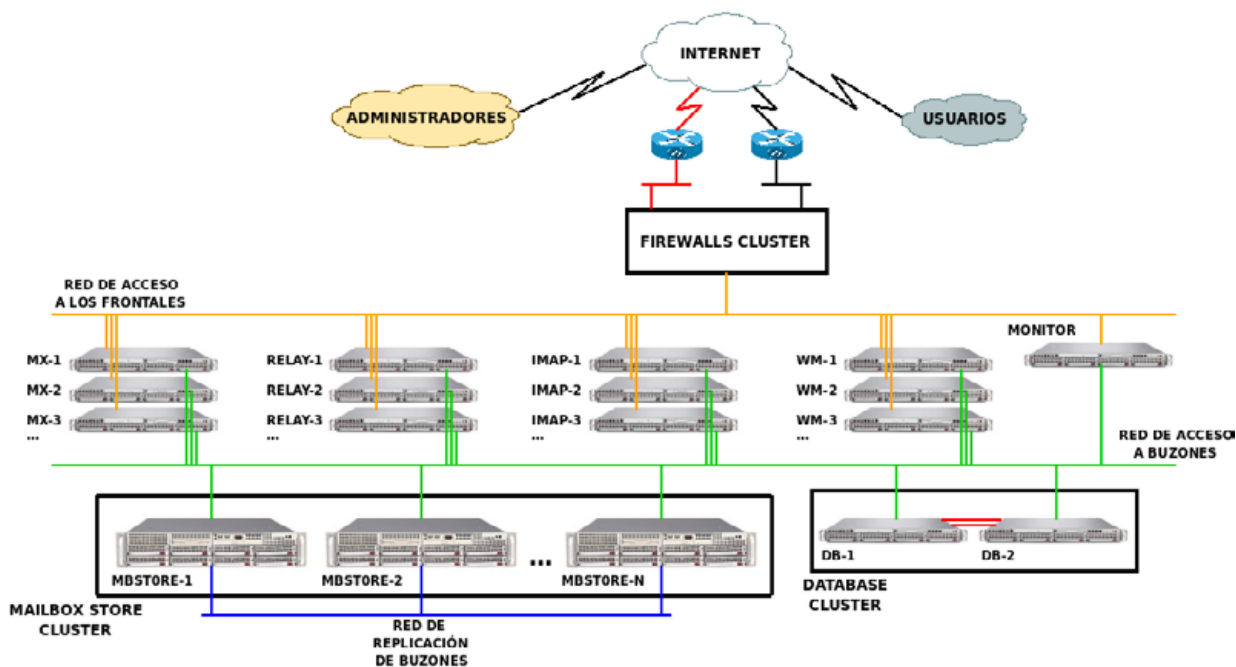
STSMAILPLATFORM

2. ARQUITECTURA DEL SISTEMA

Como ya hemos resaltado en el apartado anterior, uno de los requisitos más importantes con los que debe de cumplir un sistema de correo hoy en día es que sea capaz de crecer de un modo sencillo para soportar la carga originada por el número creciente de usuarios (**ALTA ESCALABILIDAD**), así como garantizar una continuidad del servicio incluso ante el evento de que se produzca una avería de cualquier índole en cualquiera de los módulos que constituyen el sistema (**ALTA DISPONIBILIDAD**).

A continuación veremos como la arquitectura de la plataforma de correo electrónico **STS-MAIL PLATFORM** cumple plenamente con estos requisitos.

El siguiente diagrama se expone la arquitectura de red para la plataforma en su **versión más avanzada**:



No es necesario que una plataforma de correo de partida tenga la estructura expuesta en el diagrama anterior. Como veremos más adelante, una plataforma de partida puede estar constituida por un único nodo (sin alta disponibilidad) o por dos nodos o más nodos.

Por lo tanto, el diagrama no se corresponde al 100% con la plataforma de correo que cubre las necesidades de una empresa dada en una fase inicial de puesta en marcha del sistema, pero permite apreciar de un vistazo las enormes posibilidades de crecimiento y tolerancia a fallos de que consta la arquitectura con la que se ha diseñado la plataforma.

Se ve claramente que no existe **ningún punto de fallo único** dado que todos los elementos a través de los cuales se suministran los servicios de correo están formados por dos o más nodos.

STSMAILPLATFORM

2. ARQUITECTURA DEL SISTEMA

2.1. MAILBOX STORE CLUSTER.

Analizando el diagrama de abajo hacia arriba vemos que en primer lugar tenemos un cluster para el almacenamiento de los buzones de correo (**MAILBOX STORE CLUSTER**). Este cluster está formado por un mínimo de dos nodos y se puede ir ampliando con más nodos a medida que la carga de la plataforma lo vaya requiriendo.

Los buzones se reparten de forma equitativa por todos los nodos del cluster, de este modo se consigue a su vez un reparto de carga por todos los nodos. Además, cada nodo del cluster replica sus respectivos buzones en un nodo hermano, de tal modo que si uno de los nodos del cluster deja de funcionar por el motivo que sea, el nodo hermano asume su papel permitiendo la continuidad en el acceso a los buzones del nodo caído.

Todos los nodos del cluster funcionan de forma activa sirviendo el conjunto de buzones que tiene asignado cada uno de ellos. Por lo tanto, este es un cluster en el cual todos sus nodos son activos, **no existen nodos pasivos** que no hacen nada a no ser que su correspondiente nodo activo falle. Gracias a esto **se utiliza toda la potencia de proceso de los servidores de la plataforma**.

Como se puede ver, el cluster de almacenamiento de buzones cumple con los requisitos de alta escalabilidad y alta disponibilidad, dado que es posible añadir nuevos nodos al cluster si se detecta que este va cargado en CPU, disco, etc., con el fin de repartir la carga de proceso y, aunque se produzca una avería grave en uno de los nodos del cluster, el servicio no se ve interrumpido por ello.

Tal y como iremos viendo a lo largo del documento, la plataforma ha sido diseñada para que todos los subsistemas que la constituyen cumplan con estos objetivos de alta escalabilidad y alta disponibilidad.

Existe una red que interconecta los nodos de este cluster entre si (la red que se muestra en color azul en el diagrama), la cual es utilizada en exclusiva por estos para la replicación de los buzones entre nodos hermanos.

2.2. GRANJAS DE FRONTALES.

El acceso por parte de los usuarios a los servicios de la plataforma de correo se lleva a cabo a través de las **granjas de frontales**, las cuales se agrupan en el diagrama por tipos de servicios. Podemos ver granjas de frontales MX, granjas de frontales para el RELAY SMTP, granjas para el acceso a los buzones mediante IMAP, IMAPS, POP, POPs, etc. y granjas de frontales que permiten el acceso al servicio WebMail.

Los frontales MX son dispositivos **UM-MAILSAFE APPLIANCE** de los cuales podemos encontrar una descripción detallada en el documento anexo **UM-MAILSAFE_Appliance.pdf**. Estos dispositivos reciben los mensajes destinados a los buzones correspondientes a los dominios albergados en la

STSMAILPLATFORM

2. ARQUITECTURA DEL SISTEMA

plataforma. En ellos se llevan a cabo todas las comprobaciones antivirus/antispam sobre los mensajes entrantes antes de proceder a su entrega en el buzón del destinatario. Si dicho buzón existe y el mensaje entrante supera todos los tests antivirus/antispam, entonces se procede al almacenamiento del mismo en el nodo del cluster para el almacenaje de buzones que alberga el buzón.

Los frontales para el RELAY SMTP son utilizados por los usuarios para mandar correo a Internet. El envío se lleva a cabo mediante previa autenticación del usuario que desea hacer uso del servicio.

Los frontales IMAP son utilizados para el acceso al contenido de los buzones mediante cualquiera de los protocolos de acceso a buzones permitidos (IMAP, IMAPS, POP, POPS).

Los frontales WM (WebMail) son utilizados para procesar las peticiones de servicio generadas por los usuarios cuando acceden a la interfaz WebMail. El software WebMail se sirve de una base de datos para almacenar las propiedades particulares de cada usuario que accede a la interfaz. El motor de dicha base de datos se encuentra albergado en el **DATABASE CLUSTER** que aparece en el diagrama, de tal modo que este también se encuentra en alta disponibilidad.

Al igual que el cluster para almacenamiento de buzones, las granjas de frontales cumplen con los requisitos de alta escalabilidad y alta disponibilidad, dado que es posible añadir más frontales de un tipo dado para repartir la carga de proceso y si falla uno de los frontales están el resto para seguir prestando el servicio.

Con el fin de poder hacer un reparto equitativo de la carga sobre los nodos de las distintas granjas de frontales, se recomienda que el sistema de firewalls disponga de capacidades de **balanceo de carga** para poder repartir las peticiones entrantes a un servicio dado entre los diferentes nodos existentes en la granja asociada a dicho servicio. Por ejemplo, que los accesos a buzones IMAP se repartan entre distintos nodos que constituyen la granja de frontales IMAP. Además, el FW tiene que ser capaz de detectar cuando uno de los nodos de la granja está caído para no enviar más peticiones a este, así como detectar cuando el nodo vuelve a estar operativo para volver a enviar peticiones al mismo.

En el documento **UM-FireWall.pdf** anexo a esta propuesta se describe en detalle el sistema de cluster de firewalls en alta disponibilidad **UM-FireWall** el cual dispone de las capacidades de balanceo de carga descritas en el apartado anterior, entre otras muchas características más.

STSMAILPLATFORM

2. ARQUITECTURA DEL SISTEMA

2.3. WEBMAIL CLUSTER.

Como ya hemos indicado, en el diagrama se puede apreciar la existencia de una granja de frontales web, utilizados para la prestación del servicio WebMail. Cada nodo de dicha granja de frontales dispone de todos los elementos necesarios (Apache, PHP, etc.) para la prestación del servicio WebMail, así como de los módulos adicionales necesarios para la prestación de los servicios adicionales disponibles a través del WebMail (libreta de direcciones, sistema de ficheros web, notas, etc.).

Como interfaz WebMail se puede utilizar tanto el *IMP*, que funciona bajo la infraestructura PHP HORDE, como el *SquirrelMail* o cualquier otro que cumpla con los requisitos del cliente.

Estos entornos WebMail suelen centralizar los datos particulares de cada usuario en una base de datos, la cual se configura en cluster tal y como se muestra en el diagrama.

Los usuarios acceden a la interfaz WebMail a través de la granja de frontales web y estos, a su vez, acceden a los buzones almacenados en el cluster de almacenamiento para mostrar el contenido de los mismos al usuario final y al cluster de bases de datos para almacenar las opciones de configuración particulares de cada usuario.

2.4. REDES DE LA PLATAFORMA.

Las mismas características de escalabilidad y alta disponibilidad que hemos visto para los diferentes subsistemas que constituyen la plataforma se pueden aplicar a los elementos de red que permiten la comunicación entre dichos subsistemas o módulos.

Como se puede apreciar en el diagrama, todos los nodos de todas las granjas de frontales se encuentran conectados a dos redes. Una de estas (la de color verde) les une directamente con el cluster de almacenamiento de buzones y es utilizada para el acceso directo a los buzones. La otra red (la de color naranja) es utilizada para la interacción de los usuarios finales con los servicios prestados por cada granja de frontales.

Mirando el diagrama se puede pensar que dichas redes pueden llegar a convertirse en el cuello de botella de la plataforma, pero esto no es así dado que la arquitectura de la plataforma permite añadir varias redes de color naranja o verde tanto para repartir la carga de red por las mismas si se detecta saturación en alguno de los enlaces, como para garantizar que la caída de una de las redes no pueda significar la interrupción del servicio prestado.

STSMAILPLATFORM

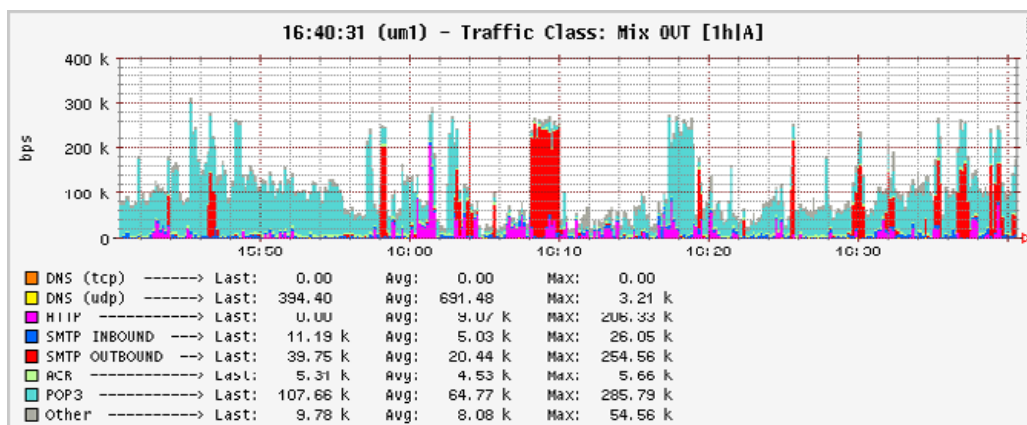
2. ARQUITECTURA DEL SISTEMA

2.5 MONITORIZACIÓN.

En el gráfico se puede ver como existe un equipo destinado a la monitorización de todos los equipos y sistemas que forman parte de la plataforma de correo.

La monitorización se lleva a cabo a través del módulo *Monitor* del sistema **SOLTECSIS MANAGEMENT CONSOLE**. Este es un sistema muy eficaz que permite generar gráficas de estado de los recursos (CPU, memoria, carga de disco, tráfico de red, etc.) de todos los equipos con datos muy precisos que permiten identificar con facilidad si alguno de los elementos de la plataforma está empezando a saturarse.

A continuación se muestra uno de los gráficos de estado que es posible generar en el cual es posible apreciar el tráfico de salida hacia Internet de uno de los servidores de la plataforma, clasificado por colores.



Se trata de una herramienta de enorme utilidad dado que permite monitorizar con gran precisión el estado de la plataforma y llevar a cabo ampliaciones a tiempo para evitar posibles saturaciones en los servicios prestados a los usuarios.

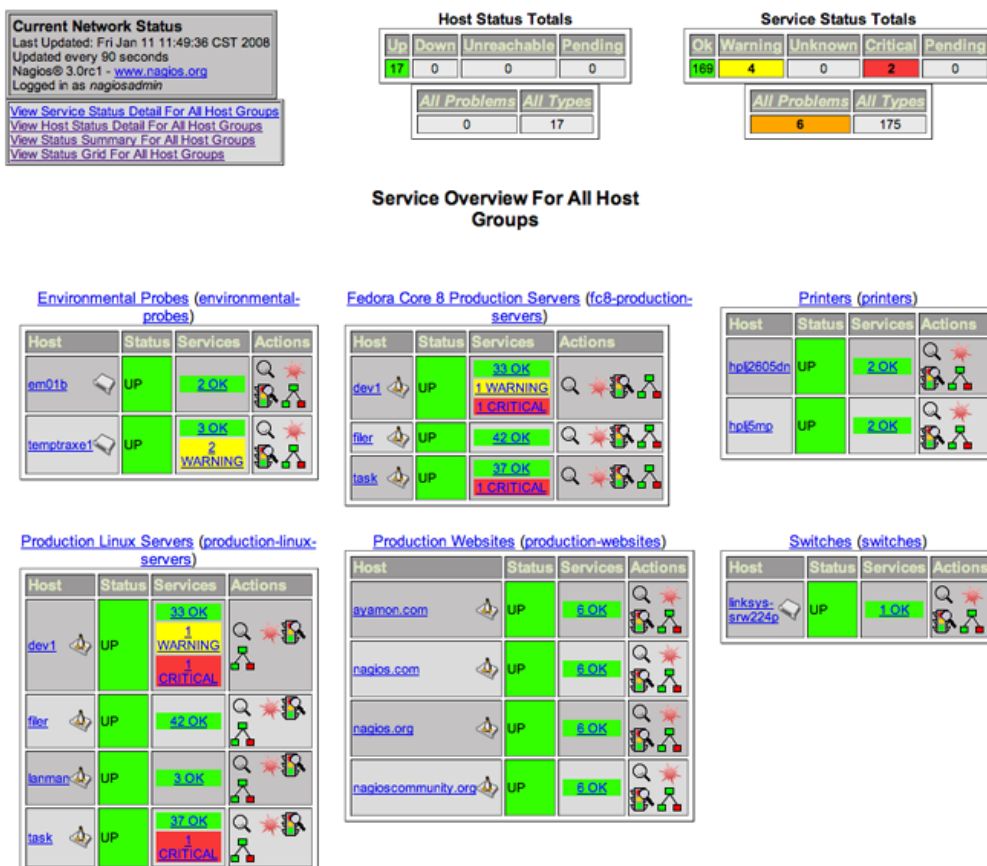
En la sección 8 del documento adjunto **UM-Firewall.pdf** se puede ver una explicación muy detallada de esta herramienta junto con varias capturas de pantalla que muestran las gráficas de estado generadas así como la apariencia y potencia del entorno de monitorización.

Para tener un control en tiempo real del estado de todos los servicios y recursos de la plataforma, se instala también el sistema de monitorización **Nagios**, gracias al cual vamos a poder monitorizar que los servicios de todos los equipos de la plataforma están operativos así como controlar el estado de los recursos (por ejemplo, si una partición de disco está a punto de llenarse, si la cantidad de procesos en memoria es excesiva, etc.). Este sistema permite la generación de alertas por e-mail o SMS, incluso el escalado de alertas para si una avería no se solventa en un tiempo predeterminado se escale a otros operadores.

STSMAILPLATFORM

2. ARQUITECTURA DEL SISTEMA

A continuación se muestra una captura de pantalla en la que se muestra como se puede controlar desde el Nagios el estado de un conjunto de servidores.



Aunque el equipo para monitorización y gestión de buzones no aparece en cluster en el diagrama, no existe ningún problema en montarlo en cluster para garantizar la alta disponibilidad del mismo.

2.6. SISTEMA DE APROVISIONAMIENTO.

El equipo de monitorización se utiliza también para albergar la interfaz de administración web que permite la gestión (altas, modificaciones, bajas, etc.) de los dominios y buzones que alberga la plataforma de correo. Esta interfaz es utilizada por los administradores de la plataforma como medio de acceso al **sistema de aprovisionamiento cliente/servidor** utilizado para la administración de los dominios y buzones de la plataforma.

Para la gestión (altas, modificaciones, bajas, etc.) de los dominios y buzones se hace uso del módulo *Mailbox* para la *SOLTECSIS Management Console*. Gracias a este módulo es posible gestionar todos los buzones desde una sencilla interfaz web, tal y como se muestra en el documento adjunto **UMMC.pdf**.

STSMAILPLATFORM

2. ARQUITECTURA DEL SISTEMA

Este módulo se sirve de un sistema cliente/servidor para el aprovisionamiento automatizado de buzones a lo largo de todos los equipos que forman parte de la plataforma. Por ejemplo, cuando damos de alta un buzón a través de la interfaz *SOLTECSIS Management Console*, la interfaz pasa la petición a un proceso local el cual se encarga de mandar las correspondientes peticiones de servicio a los demonios de aprovisionamiento corriendo en cada uno de los equipos de la plataforma para realizar las acciones asociadas como son crear el buzón correspondiente en el nodo del cluster de almacenamiento de buzones, crear el usuario en las base de datos para permitir el envío de correo autenticado a Internet y el acceso autenticado a los buzones, etc.

Del mismo modo, cuando se da una baja o modificación en cualquiera de los buzones existentes, el sistema de aprovisionamiento cliente/servidor se encarga de llevar a cabo todas las acciones oportunas en los equipos de la plataforma afectados por dicha acción.

El sistema es capaz incluso de **encolar peticiones de servicio de aprovisionamiento**, manteniendo la secuencia lógica de los comandos, con el fin de ser procesadas de forma automatizada más tarde si alguno de los equipos a los cuales va destinada la petición no está operativo.

Por ejemplo, imaginemos que uno de los frontales para RELAY SMTP está detenido porque se está llevando a cabo una ampliación de hardware. Si mientras dura la intervención se da de alta un nuevo buzón, la petición de servicio destinada a este frontal se encolará hasta que este responda.

Por lo tanto, **el propio sistema de aprovisionamiento dispone también de mecanismos de tolerancia a fallos**.

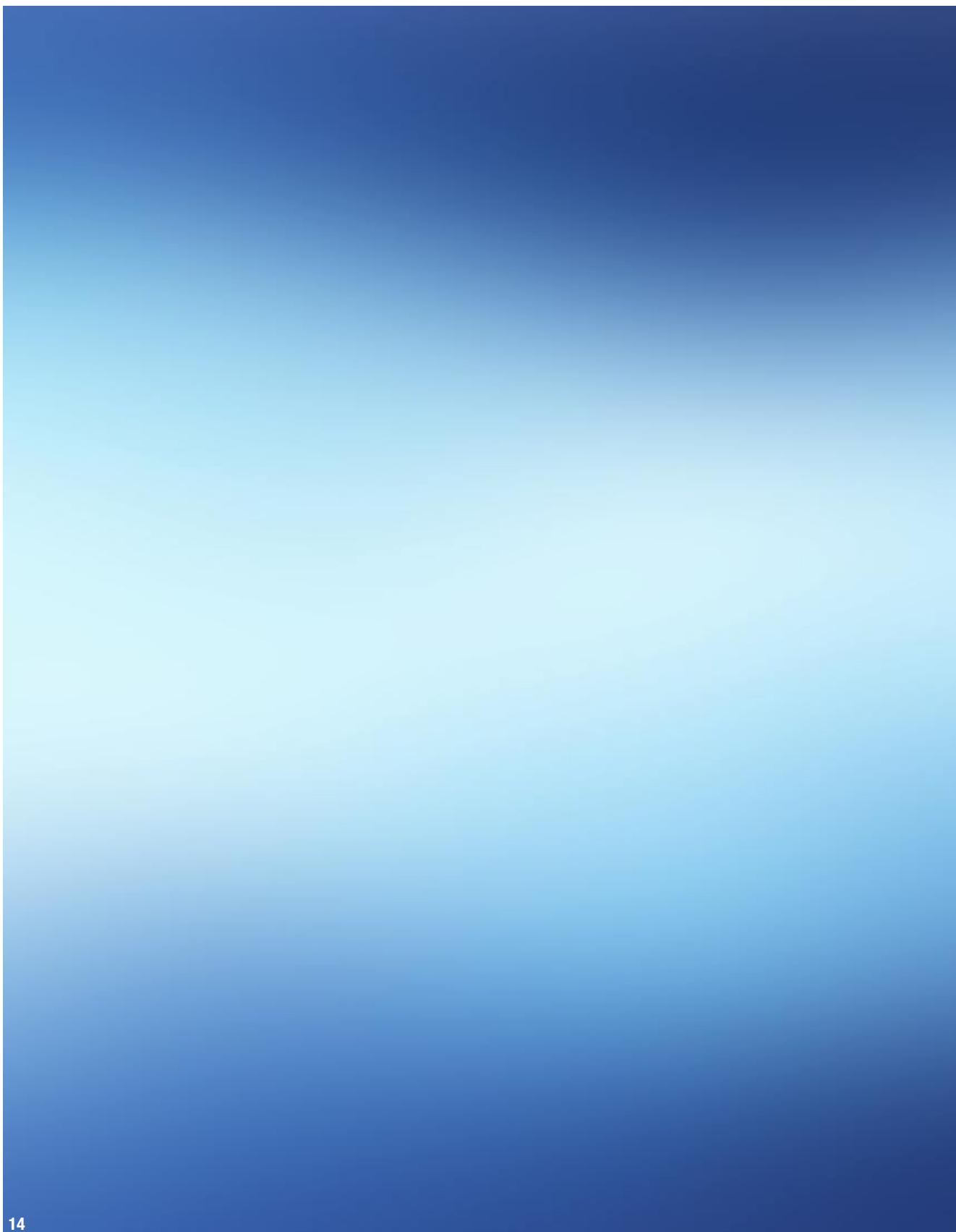
Gracias a este eficaz sistema de aprovisionamiento se consigue una gestión sencilla, limpia y en tiempo real de los buzones albergados en la plataforma.

Este sistema permite también automatizar tareas tales como pueden ser, por ejemplo, el cambio de cuota de todos o un conjunto de buzones de uno o varios dominios, el alta de cientos o miles de buzones en cuestión de pocos segundos, etc.

Se pueden generar scripts que lleven a cabo tareas de forma automatizada inyectando las peticiones de servicio necesarias a través del punto de entrada de aprovisionamiento.

STSM**AIL**PLATFORM

3. PLATAFORMAS DE PARTIDA



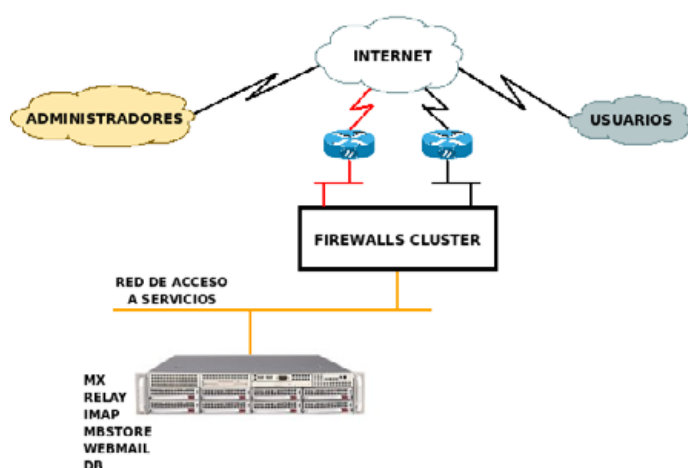
STSMAILPLATFORM

3. PLATAFORMAS DE PARTIDA

Tal y como se resaltó en la sección anterior, la plataforma de correo de partida por la cual opte un cliente no tiene el porque de ser tan compleja como la expuesta en el gráfico explicativo que se ha utilizado para facilitar la comprensión de las enormes capacidades de ampliación y tolerancia a fallos de que dispone el sistema de correo propuesto en el presente documento.

La plataforma inicial de cada cliente puede tener diseños diferentes en función de los requerimientos y cantidad de buzones que esta tenga que albergar.

Si la plataforma que se desea montar va a albergar pocos buzones y no se desea alta disponibilidad para la misma, se puede optar por un diseño en el que todo el servicio lo preste un único servidor.

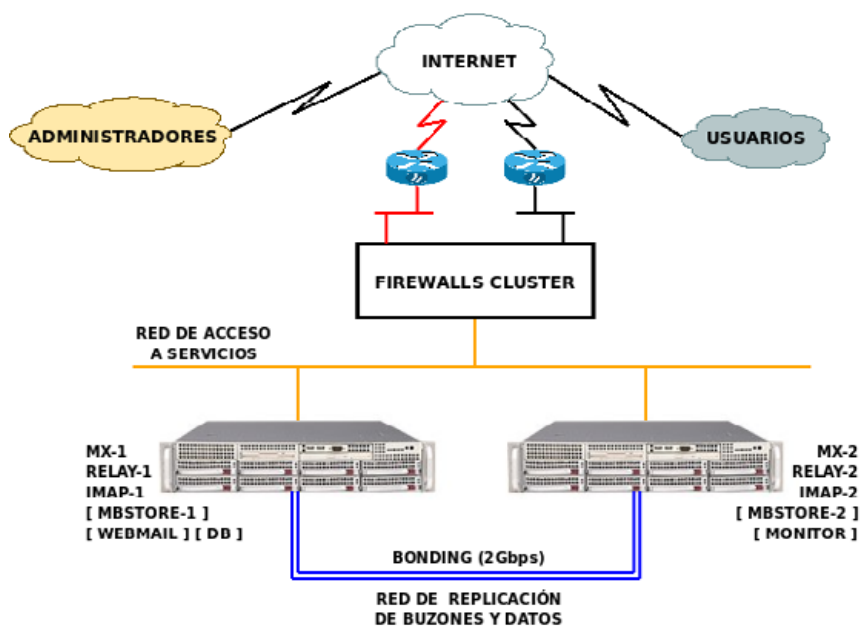


No obstante este diseño únicamente es recomendable para plataformas con pocos buzones y en las cuales una parada del servicio por avería no suponga demasiados problemas. Hay que tener en cuenta que con este diseño se pierde uno de los puntos fuertes de la arquitectura propuesta en el documento, la alta disponibilidad.

STSMAILPLATFORM

3. PLATAFORMAS DE PARTIDA

Como mínimo se recomienda hacer uso de un sistema formado por dos nodos funcionando en modo híbrido, es decir, ambos nodos del cluster prestando todos los servicios. En vez de hacer servir un cluster para el almacenamiento de buzones y luego granjas de frontales para prestar los distintos servicios, todo integrado dentro de un par de equipos tal y como se esboza en el siguiente gráfico.



Como se puede apreciar en el diagrama, cada nodo del cluster es capaz de prestar por sí mismo los servicios propios de la plataforma de correo.

En lo que respecta al almacenamiento de los buzones, cada nodo tiene asignado un conjunto del total de los buzones existentes y, además, cada nodo es hermano del otro nodo desde el punto de vista de replicación de los buzones. Es decir, cada nodo replica en tiempo real en uno de sus sistemas de ficheros los buzones del nodo hermano, de tal modo que si el hermano falla el nodo que queda operativo es capaz de acceder a la última instancia de los buzones del nodo hermano justo antes de su caída y permitir el acceso a los mismos.

Dicha replicación en tiempo real se lleva a cabo mediante el módulo DRBD (*Data Replication Block Device*), el cual permite hacer mirror de todo un sistema de ficheros en otro equipo a través de una red.

Para evitar que este tráfico de replicación viaje a través de la misma red a través de la cual los usuarios acceden a los servicios de correo, se puede configurar una interfaz de **bonding** (también conocida como *port trunking* o *link aggregation*) entre ambos nodos del cluster haciendo servir dos interfaces de red gigabit y un par de cables de red cruzados. Con esta configuración se consigue un ancho de banda de replicación de 2Gbps, además de tolerancia a fallos en dicho enlace dado que si falla una de las interfaces gigabit en enlace continúa operativo.

STSMAILPLATFORM

3. PLATAFORMAS DE PARTIDA

Existen varias **unidades lógicas** dentro del cluster que en un momento dado podrán estar funcionando en uno u otro nodo. Una unidad lógica en un cluster es un conjunto de IPs flotantes, servicios y sistemas de ficheros que en un momento dado pueden estar funcionando en uno solo de los nodos del cluster al cual pertenece la unidad en cuestión.

Dichas unidades lógicas son las correspondientes a las dos particiones para el almacenamiento de buzones, el servicio WebMail, la base de datos utilizada por el WebMail y el entorno de monitorización y aprovisionamiento de buzones que explicamos en el apartado anterior. En el gráfico aparecen con su nombre encerrado entre corchetes para resaltar el hecho de que pueden estar funcionando en uno u otro nodo del cluster.

Estas unidades lógicas se sirven de un sistema de ficheros DRBD para mantener copias de sus respectivos datos en ambos nodos del cluster y, como hemos dicho, pueden estar activas en uno u otro nodo del cluster. Se diferencian de los servicios MX, RELAY e IMAP en que estos servicios sí que van a estar operativos en ambos nodos del cluster a la vez de tal modo que se pueda utilizar balanceo de carga para los mismos sobre ambos nodos del cluster tal y como se haría si se dispusiera de las correspondientes granjas de frontales.

STSM**MAIL**PLATFORM

4. ADMINISTRACIÓN REMOTA

STSMAILPLATFORM

4. ADMINISTRACIÓN REMOTA

Todas las comunicaciones (acceso ssh a los servidores, acceso a las interfaces web para la monitorización de la plataforma, acceso a la interfaz de gestión de dominios y buzones, etc.) necesarias para llevar a cabo la administración remota tienen lugar **de forma segura a través de túneles VPN**. El establecimiento de los túneles VPN se lleva a cabo de forma autenticada asignando a cada administrador que precise conectar a la plataforma su correspondiente **certificado digital**. Dichos túneles es posible establecerlos desde equipos cliente con sistema operativo Linux o con sistema operativo Windows. El servicio terminador de túneles se puede instalar en la unidad lógica del cluster para la monitorización, de tal modo que este mismo servicio funcione en alta disponibilidad al igual que todos los servicios de la plataforma. Con el fin de mejorar la administración remota de la plataforma y reducir los tiempos de respuesta y resolución de averías, a continuación se describe un par de dispositivos adicionales de gran utilidad.

4.1. REGLETAS DE CONTROL DE CORRIENTE ePOWER.

Este tipo de regletas de enchufes es de gran utilidad dado que permiten el apagado/encendido de cualquiera de los cuatro enchufes de que consta, a través de una dirección IP. La regleta posee una interfaz de red ethernet a través de la cual se conecta a una red IP y desde la cual se puede establecer comunicación con la misma para indicarle que lleve a cabo el apagado/encendido de cualquiera de sus 4 enchufes.



Podemos pensar que a través de la interfaz serie de un SAI ya se pueden llevar a cabo dichas acciones de reinicio eléctrico del equipo conectado a uno de los enchufes, pero ¿qué sucede si el equipo al que se conecta el SAI deja de estar operativo? Nadie lo podrá reiniciar eléctricamente y ya no se podrá reiniciar a ningún otro equipo. La regleta ePower tiene la ventaja de que, al disponer de su propia conexión a la red, se pueden utilizar sus funcionalidades de reinicio eléctrico de enchufes desde cualquiera de los PCs conectados a su misma red.

STSMAILPLATFORM

4. ADMINISTRACIÓN REMOTA

Para poder obtener control sobre más tomas de corriente, se puede optar por una solución **ePower Master/Slave** que nos permite controlar hasta un total de 32 tomas de corriente mediante una arquitectura escalable de 4 módulos con 8 tomas de corriente por cada módulo, partiendo siempre de un módulo master al cual es posible conectar 3 módulos slave adicionales.



Es más económico un módulo master con 8 tomas de corriente que la adquisición de dos regletas ePower. Además, el espacio necesario para un módulo es mucho menor que el necesario para dos regletas, dado que cada módulo ocupa una única unidad de rack. También hay que tener en cuenta que una vez adquirido el módulo master, los módulos slave son más económicos y la solución master/slave tiene la ventaja añadida de que con una única IP se puede controlar hasta 32 tomas de corriente.

4.2. SWITCHER KVM-IP.

Este tipo de dispositivos se utiliza para acceder a la consola (teclado, monitor y ratón) de varios equipos a través de un único teclado, monitor y ratón. Posee una entrada a la cual conectamos nuestro teclado, monitor y ratón; y varias entradas más (en función del modelo elegido: 8, 16, 24, etc.) a las cuales se conectan el teclado, salida VGA y ratón de los equipos a los cuales deseamos acceder por consola.



La conmutación de la consola de un equipo a otro se lleva a cabo mediante la pulsación de un botón que va pasando por todos los equipos disponibles.

Una variante de este tipo de dispositivos, muy interesante y útil para la administración remota, son los Switchers KVM sobre IP. Estos dispositivos disponen de una conexión de red para conectarlos a una de nuestras redes y permiten la conexión a la consola de nuestros equipos desde cualquier parte de Internet que nuestro sistema de firewalls permita.

STSMAILPLATFORM

4. ADMINISTRACIÓN REMOTA

Para entender mejor su gran utilidad, imaginemos el caso en el que un servidor que tenemos instalado en un país extranjero se queda bloqueado y no tenemos modo alguno de acceder al mismo dado que no responde a ningún intento de conexión a través de Internet. Si dispusiéramos de un switcher KVM sobre IP conectado a dicho equipo, nos podríamos conectar al mismo por Internet para ver la consola del equipo bloqueado e intentar solventar el problema. Podríamos incluso llevar a cabo la reinstalación completa del sistema operativo de un servidor en el caso de que alguien nos pudiera poner el CD de instalación en la unidad de lectura de CDs.

Un switcher KVM sobre IP combinado con un sistema de apagado/encendido eléctrico como el ePower expuesto en este mismo documento, nos permiten un ***control remoto total*** de nuestros servidores, dado que, en caso de ser necesario, podemos llegar a reiniciar eléctricamente de forma remota un servidor bloqueado con el fin de intentar que retorne a un estado estable viendo a través del *KVM-IP* lo mismo que veríamos si estuviéramos enfrente de la consola del equipo.

