Estudio para la Migración de Servidores a un Servicio de Nube Híbrida

Memoria del Trabajo Final del Master Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones

Universitat Oberta de Catalunya. Junio 2014
Autor: Francisco José Peña Sánchez
Tutores: María Francisca Hinarejos Campos y Jordi Cadafalch.

INDICE

Tabla de Ilustraciones

Resumen

La empresa Global Salcai Utinsa se dedica al transporte interurbano de viajeros por carretera, y actualmente es la empresa principal de mayor volumen económico de un grupo de empresas llamado Grupo Global de Empresas.

La conservación y cuidado del Medio Ambiente es una de las grandes preocupaciones de GLOBAL. Y por ello no escatima recursos para ayudar a su conservación. Así, sus vehículos están equipados con motores que cumplen la normativa europea en materia medioambiental; contribuye a la reforestación de Gran Canaria como Patrono Fundador de Foresta (Fundación Canaria para la Reforestación); colabora con las asociaciones ecologistas e instituciones en proyectos de conservación del ecosistema canario y de búsqueda de energías alternativas.

GLOBAL, es puntera en España en nuevas tecnologías, disponiendo de sistemas novedosos ejecutados y desarrollados junto a la Universidad de Las Palmas de Gran Canaria que le permiten prestar un servicio de mejor calidad ofreciendo a los viajeros fórmulas de pago automático y sistemas de prepago, así como la coordinación de la flota a través del programa de Control y Motorización de la misma. Toda su flota está equipada con el Sistema de Ayuda a la Explotación (SAE), una de las herramientas más novedosas y eficaces de GLOBAL.

Actualmente el departamento de Informática utiliza la plataforma de virtualización de VMware vSphere en su Centro de Datos, donde la mayor parte de los servicios para los empleados se ofrecen desde máquinas virtuales. Algunos de estos servicios son accesibles desde Internet a través de tres líneas ADSL, como son el servicio de correo de nóminas, o la petición de servicios de los conductores.

El servicio de correo de nóminas fue una respuesta a la petición de la empresa de eliminar el papel con el que se confecciona las nóminas mensualmente. Este servicio tiene picos de trabajo los fines de mes cuando los empleados descargar las nóminas y para dar una respuesta satisfactoria a este problema, el departamento quería realizar un estudio para la migración de dicha máquina a la nube, siempre y cuando se garantiza la seguridad de los datos.

También se han identificado otros servicios que supondrían una eliminación de papel, como pueden ser la gestión de incidencias de los conductores, el boletín informativo mensual o las circulares internas.

1 INTRODUCCION

Las líneas ADSL se utilizan para la salida a Internet de la propia empresa (gestiones con la administración, bancos, otras empresas…), también la utilizan algunas empresas del grupo y diferentes estaciones de autobuses repartidas por la isla. También se usa para el correo electrónico corporativo. La razón por la cual se usa una estrategia centralizada para dar salida a Internet desde las diferentes estaciones, es filtrar de software malicioso en un único punto en las oficinas centrales.

En ocasiones se producen cuellos de botella en dichas salidas debido a la gran demanda de ancho de banda en estas líneas, ya sea porque se envía algún fichero por correo, o bien porque algunos usuarios se conectan desde el exterior hacia algunos aplicativos para teletrabajo, o descargan ficheros desde los servidores, sobre todo durante el periodo de petición de servicios. En este periodo, muchos de los empleados (en total unos 700), conductores de autobuses, se conectan para descargar el cuadro de horarios para elegir el servicio que más le conviene, siempre y cuando se les asigne mediante un criterio de antigüedad. La empresa considera importante poder dar respuesta a estas limitaciones en cuanto que en ocasiones se ralentiza el trabajo debido a la espera por la respuesta de estas aplicaciones web.

En otras ocasiones, cuando se descargan por ejemplo las nóminas se hace por una ADSL con una subida de 12Mbps/1Mbps. Detrás de esta línea ADSL se encuentra el servidor de correo de nóminas y además este enlace está compartido para dar salida hacia Internet en general, por lo que en ocasiones cuando se producen accesos simultáneos la subida de la ADSL se convierte en un cuello de botella y los usuarios se quejan de lentitud en la conexión. Todo esto a pesar de que se ha limitado la salida para filtrar tráfico indeseado y priorizando el ancho de banda por aplicación.

1.1 Presentación del Estudio

Se pretende realizar un estudio de la migración de la máquina de correo de nóminas, así como la de gestión de incidencias y la creación de un nuevo portal web corporativo. En este estudio no se realizará una migración real de estas máquinas sino un análisis de las posibles opciones de migración para elegir la más adecuada para la empresa, por ello en primer lugar delimitaremos los objetivos y el alcance de este trabajo.

1.2 Definición de Objetivos:

La empresa desea eliminar o al menos reducir estas limitaciones en estos servicios, por lo que se hace necesario realizar un análisis de las limitaciones en cada servicio. A continuación enumeramos las limitaciones más importantes de aquellos servicios a los que se quiere mejorar la experiencia de usuario.

1.2.1.- Limitaciones del equipo servidor de correo de Nóminas.

Está en un equipo virtual, se hacen copias semanales completas de la máquina Virtual y tiene una política de actualización nula. Este equipo es accesible desde el exterior para que los empleados puedan acceder a la nómina. La línea que se utiliza es una ADSL con 12 Mb de bajada y 1 Mb de subida. En ocasiones debido a la gran demanda de los usuarios que quieren ver su nómina se producen picos de entrada en la ADSL que produce que la conexión al mismo se ralentice.

En el siguiente gráfico de la ADSL proporcionado por el Proveedor de Servicios de Internet podemos observar que el tráfico de bajada, es decir, de entrada al servidor de Nóminas (bajada desde el ISP), está promediando picos de más de 3Mbps.

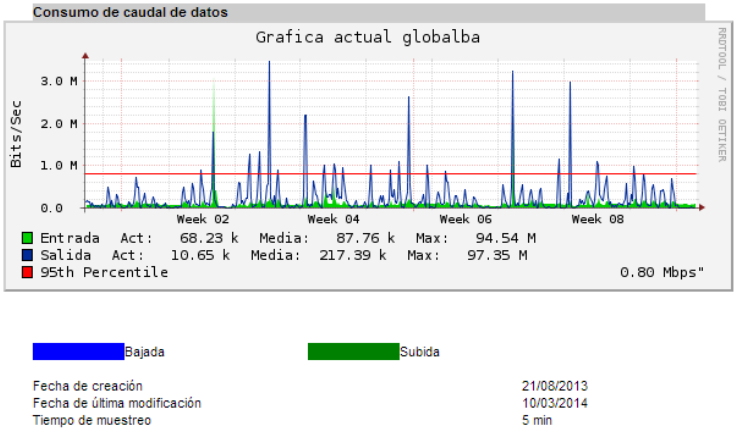

Ilustración 1: Gráfico Mensual de la línea ADSL

En verde se muestra el tráfico de salida del servidor y en azul el de entrada. Un nivel de detalle más bajo nos da una pista de lo que está pasando cuando se conectan varios usuarios para acceder a ver su nómina mensual:

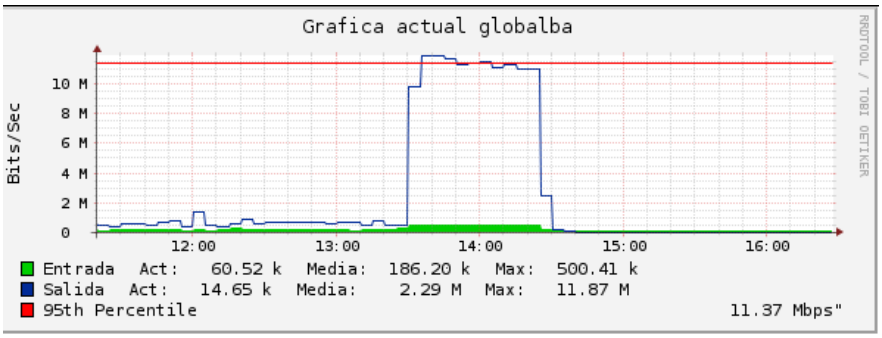

Ilustración 2: Gráfico Diario de la línea ADSL

Los usuarios acceden a través de una página web hacia el servidor de correo Zimbra utilizando un nombre y contraseña. Para el nombre se ha utilizado el código de la empresa e inicialmente, se les ha asignado como contraseña, el número de la Seguridad Social. Este número es personal e intransferible y aparece en la tarjeta sanitaria que posee cada trabajador. Una vez hagan login en el sistema se les pedirá cambiar la contraseña para seguir operando. La conexión siempre se realiza con navegación segura por http-s. El equipo se encuentra detrás de un appliance UTM de la marca sonicwall con capacidad de bloquear malware en general y detectar intentos de penetración de intrusos en la red.

Este equipo sonicwall actualmente también funciona como balanceador de las tres líneas ADSL, de forma que si por cualquier motivo cayera alguna de ellas, la salida se realizaría por alguna de las otras dos. El problema está en que el balanceador tiene sentido para dar mayor disponibilidad para salir hacia Internet pero no sirve para la entrada.

Esto es así, porque cada servicio se encuentra mapeado a una ADSL en concreto, que tiene además asignada una IP pública (se hace NAT). En el caso del correo el nombre asignado a esa IP pública es mail.globalsu.net.

1.2.2- Servidor de Gestión de Incidencias.

Servidor virtualizado con Redmine adaptado a la gestión de incidencias. Este equipo virtual es un nuevo servicio para que los empleados puedan enviar comunicaciones a la empresa desde la web. Las comunicaciones hasta hoy en día se realizan en papel, y todos los días se envían por valija hasta las oficinas centrales. Con esta aplicación los empleados podrían desde cualquier lugar, su casa, el equipo de conductores de cada estación, etc., enviar las comunicaciones como descuadre en la liquidación en los cajeros, problemas con el cajero, errores en la liquidación de abordo, etc. Por ello este equipo debería ser migrado a la nube en un entorno virtual.

1.2.3- Nuevo Portal Web Corporativo (prototipo).

Se hace necesario instalar un portal Web Corporativo que reúna todos estos servicios para los empleados. *La empresa ya hace un par de años manifestó su necesidad de un portal web pero hasta ahora no se ha concretado nada*. En el próximo apartado podemos concretar el alcance que se pretende cubrir en este punto.

1.3 Definición del Alcance

Para cada servicio habría que definir hasta donde se puede actuar para mejorar las prestaciones del mismo en los siguientes aspectos: mantenimiento, escalabilidad, tiempo de inactividad, lentitud, políticas de seguridad y actualizaciones, monitorización de equipos.

1.3.1 Mantenimiento

Los dos servicios, tanto el de Sistema de Correo como el de la Nómina y Gestión de Incidencias son equipos virtuales VMware. Por otro lado, instalar un Portal Web Corporativo, debido a la complejidad y el tiempo de desarrollo que conlleva el crear un portal de calidad, considero que este TFM podría ser un primer paso para avanzar sobre este tema, de forma que más adelante se tome como punto de partida para un proyecto más ambicioso que gestione todas las comunicaciones con los empleados.

1.3.2 Escalabilidad

Dentro de la plataforma VMware vSphere es posible escalar las máquinas virtuales, añadiendo más recursos de hardware a las mismas, pero no es posible asignar mayor caudal de tráfico o de ancho de banda sin tener que aumentar el número o el ancho de banda de las líneas ADSL.

Como ya comentamos el equipo de Nómina se encuentra en una máquina virtual Zimbra accesible por internet que suele tener picos de tráfico los días finales de cada mes. Además sería preferible tener un servicio de push para enviar correos a los terminales móviles de cada empleado.

Los otros dos equipos también necesitan ser accesibles por internet y con las líneas actuales se hace casi imposible dar un servicio con una experiencia de uso de una calidad razonable.

1.3.3 Tiempo de inactividad o lentitud

Los tiempos de inactividad son a menudo producidos debido a los periodos en que se necesite reiniciar el enrutador ADSL porque se quede bloqueado. Este enrutador es un equipo “doméstico” que no ofrece el rendimiento de enrutadores de mayor capacidad de procesamiento y memoria RAM.

La lentitud en las conexiones da una mala imagen del servicio y el usuario se decanta por acceder desde los equipos de las estaciones que conectan internamente sin lentitud, y no lo hace desde sus casas que es lo que se pretendía con este servicio.

1.3.4 Política de Backup

Tanto el equipo de Redmine como el de Nóminas que son equipos virtuales se copian semanalmente de forma completa, y diariamente de forma incremental. La migración a un entorno virtual supondría la definición de estas políticas de copias virtuales en el proveedor.

1.3.5 Política de Actualizaciones

Los equipos actualmente tienen versiones antiguas tanto de Zimbra como de Redmine. Normalmente siguen una política de actualizaciones sólo cuando el software está a punto de ser descatalogado por el fabricante o bien la versión utilizada es vulnerable a algún exploit. El disponer de un servidor virtual en un proveedor en la nube en el que pueda desplegarse en pocos minutos con una versión superior podría mejorar la frecuencia en que se actualizan el sistema y el aplicativo en estas máquinas virtuales.

1.3.6 Monitorización de los equipos.

Para analizar el rendimiento de las máquinas virtuales en la plataforma de virtualización VMware vSphere podemos utilizar la consola llamada vSphere Web Client que tiene una pestaña accesible con análisis de los recursos del sistema, procesamiento, red y memoria.

2. PLANIFICACION

Para planificar este TFM resulta indispensable primeramente qué es lo que se quiere hacer, cuánto tiempo nos llevará realizar los objetivos propuestos. También es posible que más adelante sea necesario cambiarlo y tener que replanificar nuevamente durante la ejecución.

Para realizar la hoja de rutas o plan a seguir, tenemos que definir las actividades a realizar, los requisitos que tiene que cumplir el sistema propuesto, las actividades en secuencia a realizar y por último realizar un calendario en forma de tabla de Hitos y un diagrama de Gantt donde podemos ver las dependencias de estas actividades.

2.1 Requisitos

2.1.1 Disponibilidad y Redundancia

Es casi imposible garantizar el 100% de disponibilidad o tiempo de actividad de la red o de un host, existen los periodos de mantenimiento programado, así como caídas provocadas por fallos de hardware o de software. Aunque un proveedor nos garantice en sus sistemas el 100% de tiempo de actividad, es probable que no sea así, probablemente se acerque al 99,95% o más, pero nunca llegaría al 100% por una cuestión muy simple, las máquinas fallan, la red puede caer, pongamos por ejemplo debido a alguna catástrofe natural. Aun así un porcentaje del 99,95% es un porcentaje muy alto y es lo que suelen ofrecer.

Disponer de la posibilidad de restauración de un host de servidor en la nube en una hora en caso de fallo, tampoco garantiza específicamente la disponibilidad de las cargas de trabajo que existían antes del fallo ya que en ocasiones se necesita redireccionar las mismas al nuevo servidor.

Es recomendable trabajar con proveedor de servicios que puedan garantizar el tiempo de actividad y el rendimiento de las aplicaciones esenciales. También es posible tener en la nube un Centro de Datos Virtual réplica del que tenemos en nuestras instalaciones, o simplemente tener servidores redundados en la nube.

2.1.2 Implementación rápida

La empresa quiere que sus cargas de trabajo funcionen en una solución de Infraestructura como Servicio (IaaS) alojada en cuestión de unos días o menos cargándolas en la nube. Para que la solución pueda ofrecer un rápido despliegue, debería utilizar un interfaz sencillo e intuitivo que permita realizar la operación sin complicación.

2.1.3 Seguridad transparente y gestionable

La conexión a estos servicios debe realizarse cifrada tanto la conexión máquina a máquina (M2M) como la de usuario a máquina. Por otro lado, se necesita poder gestionar los usuarios que pueden conectarse a la nube donde se pueden definir los roles de cada usuario.

Sería preferible que la solución respetase la política de seguridad ya definida en la empresa.

2.1.4 Escalabilidad, Agilidad y Compatibilidad

Hoy en día, todos los proveedores permiten escalar las máquinas virtuales tanto en procesamiento, como en almacenamiento y en tráfico de red.

Por otro lado, sería deseable que las máquinas virtuales que se ejecuten en la red privada sean compatibles con el entorno de ejecución en la nube y se puedan desplegar de forma rápida desde el centro de datos de la empresa al centro de datos en la nube.

Lo más óptimo sería que el proveedor de servicios de nube utilizara el mismo software de virtualización que la empresa. En el caso de la empresa la tecnología de virtualización es VMware 5.5 en ambos lados lo que asegura la compatibilidad, escalabilidad y la agilidad en la migración de máquinas virtuales.

2.1.5 Libertad de elección y portabilidad de las aplicaciones

Idealmente la empresa podría escoger la opción más conveniente entre diferentes proveedores de nube que existen en el mercado sin tener que realizar grandes esfuerzos e inversiones en su Centro de Datos para portar las aplicaciones. Incluso se podría contratar varios servicios de nube con estos proveedores y operar con ellos sin problemas de portabilidad con las máquinas virtuales de uno y otro centro.

2.2 Definición de las Fases del Proyecto y Actividades

En la etapa planificación, es bueno distinguir entre un nivel estratégico, orientado a los productos e hitos principales del trabajo, y un nivel operativo, orientado a las actividades y tareas del equipo. En nuestro caso descompondremos el trabajo en partes o fases **(planificación estratégica)** que en realidad son entregables parciales o generales.

Fase	Descripción
Definición y Planificación	*Definición de los objetivos y del alcance del trabajo, así como la planificación a seguir.*
Análisis del Sistema	*Análisis de los problemas actuales y de la estrategia a seguir y recursos necesarios para solucionarlos.*
Desarrollo de la Solución	Ejecución de la solución propuesta. Parte Operativa.
Seguimiento	Fase que se realiza durante todo el proyecto para ir supervisándolo.
Finalización: Memoria	Memoria Final a entregar para su defensa.
Defensa	Presentación y defensa ante el tribunal

Tabla: **Fases del Proyecto**

A continuación, se descomponen cada parte en actividades (**planificación operativa**), y para cada una de estas actividades se estiman los recursos necesarios y se establece un calendario preliminar en forma de tabla de hitos.

Aunque la duración se mide en días, incluyendo festivos y domingos, el tiempo dedicado en cada actividad es de aproximadamente 1 hora por día al menos. Probablemente la estimación lógica sería cambiar días por horas pero para representar el diagrama de Gantt debemos usar días.

Actividad	Duración	Inicio	Final
PAC1: Definición y planificación	11 días	26/02/2014 8:00	12/03/2014 17:00
Presentación de la propuesta	3 días	26/02/2014 8:00	28/02/2014 17:00
Definición de los objetivos	3 días	01/03/2014 8:00	05/03/2014 17:00
Definición del alcance	3 días	05/03/2014 8:00	07/03/2014 17:00
Planificación	2 días	07/03/2014 8:00	10/03/2014 17:00
Definición de requisitos	1 día	10/03/2014 8:00	10/03/2014 17:00
Definición de las fases del proyecto y actividades	1 día	11/03/2014 8:00	11/03/2014 17:00
Realización de la Tabla de Hitos y el cronograma	1 día	11/03/2014 8:00	11/03/2014 17:00
Análisis de Riesgos	2 días	11/03/2014 8:00	12/03/2014 17:00
PAC2: Análisis del sistema	34 días	12/03/2014 8:00	28/04/2014 17:00
Esquema del sistema actual	2 días	12/03/2014 8:00	13/03/2014 17:00
Análisis de las diferentes opciones de migración	15 días	25/03/2014 8:00	14/04/2014 17:00
Análisis de soluciones existentes.	3 días	15/04/2014 7:00	17/04/2014 17:00
Seguridad en las soluciones	3 días	18/04/2014 7:00	22/04/2014 17:00
Análisis del coste de cada solución	1 día	22/04/2014 8:00	22/04/2014 17:00
Toma de decisión sobre el proveedor de Nube	4 días	23/04/2014 8:00	28/04/2014 17:00
PAC3: Desarrollo de la solución	37 días	10/04/2014 8:00	30/05/2014 17:00
Documentación sobre la solución	2 días	10/04/2014 8:00	11/04/2014 17:00
Preparación del laboratorio de vCloud	11 días	12/04/2014 8:00	28/04/2014 17:00
Pruebas de laboratorio	23 días	29/04/2014 8:00	29/05/2014 17:00
Conclusiones finales	1 día	30/05/2014 8:00	30/05/2014 17:00
PAC4: Memoria Final del TFM	5 días	02/06/2014 8:00	06/06/2014 17:00
Recopilación de la documentación	3 días	02/06/2014 8:00	04/06/2014 17:00
Corrección de la documentación	1 día	05/06/2014 8:00	05/06/2014 17:00
Presentación de la documentación	1 día	06/06/2014 8:00	06/06/2014 17:00
DEFENSA	5 días	06/06/2014 8:00	12/06/2014 17:00
Elaboración de la defensa	5 días	06/06/2014 8:00	12/06/2014 17:00
Presentación del proyecto	1 día	12/06/2014 8:00	12/06/2014 17:00

Tabla de Hitos

2.3 Realización de la Tabla de Hitos y Cronograma.

A partir de la tabla de hitos podemos generar el cronograma del trabajo o diagrama de Gantt, que nos dará una visión de abajo (el nivel de las tareas y actividades) arriba (el nivel de los entregables y objetivos).

Para realizar el digrama de Gant se ha utilizado el software de código fuente abierto *Libre Project*, *que se* puede descargar de la página sourceforge.net. []

Según se puede observar cada etapa en color negro representa el tiempo que ha llevado terminar cada PAC indicada en la tabla de Hitos como PAC1, PAC2, PAC3, PAC4 y DEFENSA.

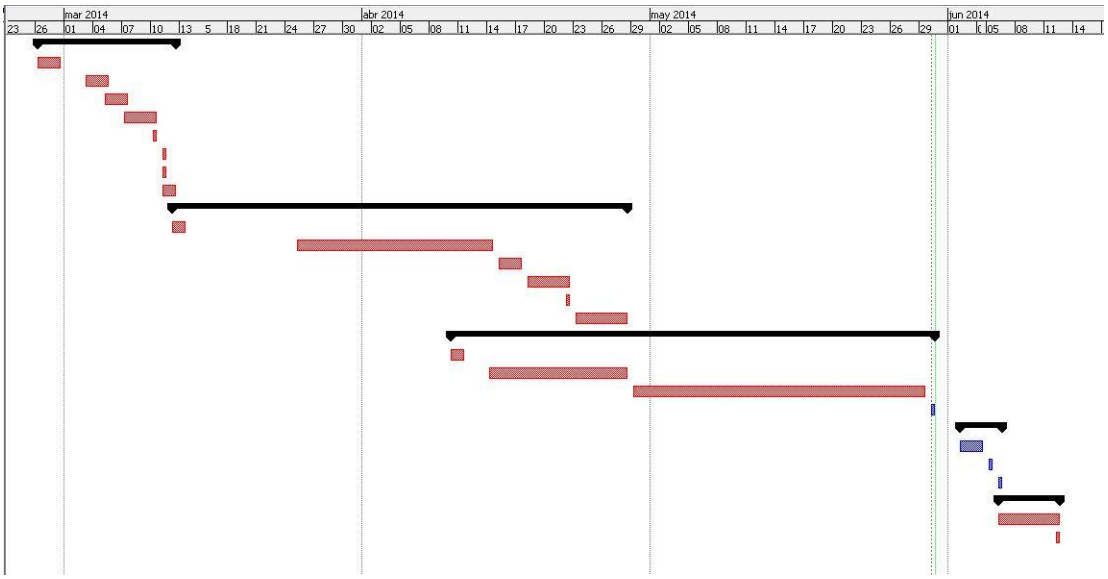

Ilustración 3: Cronograma de la planificación

2.4 Análisis de Riesgos

Hay que tener en cuenta qué riesgos existen a la hora de planificar un proyecto de este tipo para prever posibles problemas futuros. El estudio o análisis de riesgos nos permitirá identificar aquellos riesgos más graves que pueden afectar negativamente al desarrollo del proyecto. Los siguientes tres tipos de riesgos son los que más impacto provocarían en el desarrollo del TFM.

2.4.1 Planificación temporal errónea o demasiado optimista.

Esto afectaría sobre todo a la fecha de finalización del proyecto provocando retrasos y una baja calidad del mismo.

2.4.2 Falta de conocimiento en un área determinada.

Cada proveedor en la Nube utiliza diferente software para realizar la migración de las máquinas que normalmente no se conoce. Esta falta de conocimiento podría ocasionar el incumplimiento de esta actividad en concreto.

En ocasiones, se necesita tener los conocimientos y experiencia sobre un producto de un fabricante, que pueden adquirirse realizando los cursos de certificación que ofrece ese fabricante como en el caso de VMware.

2.4.3 Cambios de Planificación después de la fase de estudio

Aun descartando problemas de fuerza mayor, como enfermedades, accidentes,… no podemos prever que debido a problemas de otra índole como por ejemplo, fallos de hardware o falta de recursos nos ocasione que el proyecto no pueda acabarse en el plazo acordado.

También puede pasar que después de finalizar la fase de estudio de las soluciones a desarrollar se concluya que la solución más óptima para este TFM requiera el tener que rehacer la planificación inicialmente propuesta. Esto fue lo que ocurrió para este TFM, que partiendo de realizar un estudio para migrar hacia la nube pública se decidió que era más óptimo realizar el estudio hacia un servicio de nube híbrida.

3 ANALISIS DEL SISTEMA

La infraestructura utilizada en el Centro de Proceso de Datos de la empresa es VMware vSphere 5.5. Como se comentó en la introducción se emplea tres enrutadores ADSL que mapean los servicios, es decir que realizan NAT desde esos enrutadores a las máquinas virtuales, para que sea posible acceder a los puertos por los que escuchan las aplicaciones que residen en las máquinas virtuales.

3.1 Esquema del Sistema Actual:

En la ilustración 4 se observa como los usuarios acceden a un puerto del enrutador para acceder a la aplicación residente en la máquina virtual. Se marca en rojo para resaltar el hecho de los cuellos de botella que se producen en esa línea cuando muchos usuarios acceden simultáneamente.

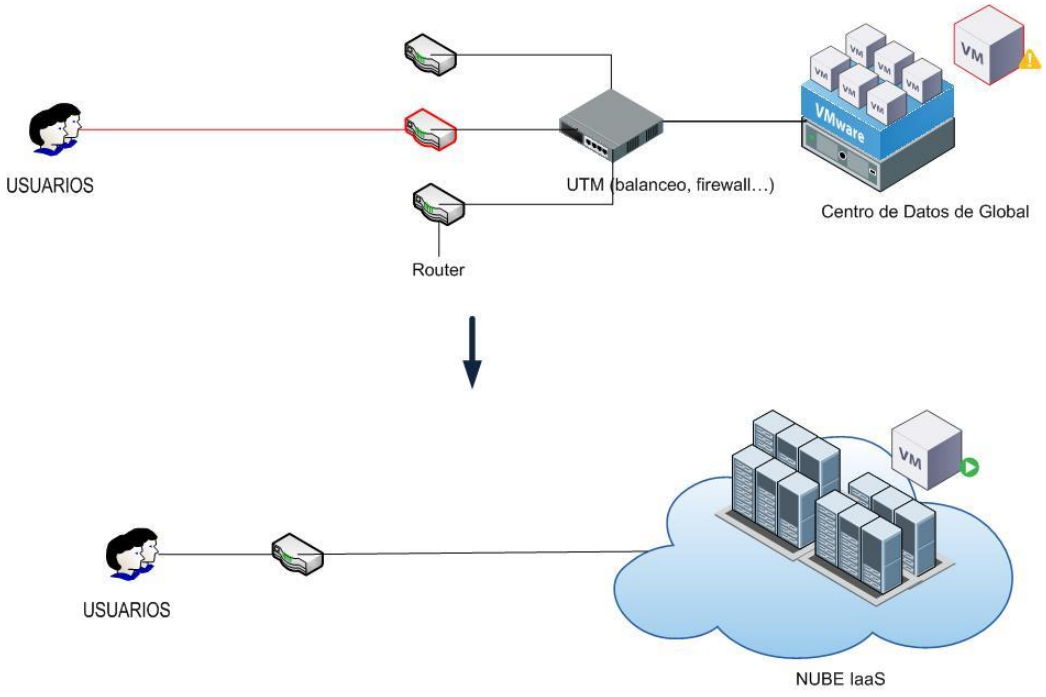

Ilustración 4: Diagrama de Migración de la Red

A continuación vamos a clarificar de la situación de la que se parte, definiendo los equipos afectados que existen en el CPD de Informática y cómo se conectan los usuarios a ellos.

3.1.1 El servidor para las Nóminas.

Este equipo utiliza el sistema de mensajería de código abierto Zimbra en un equipo virtual con Ubuntu Linux 32 bits con 1 CPU virtual (vCPU), con 640Mb de RAM y un Disco Duro de 20 Gb. Actualmente tiene 750 cuentas de correo, una por empleado. Cada buzón de correo tiene una cuota de 200 Mb.

El personal accede al equipo tanto por la sede central o las remotas a través de LAN, como por Internet a un enrutador conectado a una ADSL de 12Mb/800 Kbps, los días finales de cada mes, en los que se produce un aumento de las conexiones de entrada que en ocasiones ralentizan el acceso.

3.1.2 El servidor Gestión de incidencias

Tiene instalado el sistema de Gestión de Proyectos Redmine, aunque modificado para que realice el seguimiento de incidencias. El equipo es una máquina virtual con 1 vCPU, con 1024 Mb de RAM, y un disco duro de 60 Gb. Actualmente tiene creado un Proyecto en el que se ha dado de alta a cada trabajador con una cuenta para que puedan enviar las incidencias que hayan tenido con su trabajo diario. La tipología de incidencias se centra más en las que se producen con los cajeros de autoliquidación disponibles en las diferentes zonas repartidas por la isla.

3.1.4 Acceso interno y externo a los servicios.

Como se ha comentado en los puntos anteriores, los usuarios acceden tanto internamente por la conexión VPN de la sede remota como externamente desde cualquier ubicación a través de los enrutadores que dan acceso a Internet al CPD de Informática, por lo que si trasladásemos estos servicios hacia la nube, todos los accesos se harían a través de Internet hacia el proveedor en la nube.

3.2 Análisis de las diferentes opciones de migración

Los principales modelos de prestación son: []

- Infraestructura como servicio, IaaS, para los recursos de memoria, almacenamiento y red.
- Plataforma como servicio, PaaS, para las herramientas de desarrollo de aplicaciones y los servicios de tiempo de ejecución.
- Software como servicio, SaaS, para las aplicaciones distribuidas como servicio.

Los principales modelos de implementación incluyen soluciones que residen en las instalaciones de la empresa (nube privada), en un proveedor externo (nube pública), o bien una solución combinada (nube híbrida).

Actualmente, la empresa Global desea controlar la gestión y la implementación de sus infraestructuras, por lo que deberían valorar en primer lugar la solución basada en el modelo de nube IaaS, en lugar de las basadas en nube PaaS o SaaS. Una nube IaaS pública ofrece ventajas de agilidad y asequibilidad, sin requerir una inversión mayor en recursos internos de la empresa para crear y gestionar una nube en las instalaciones.

Los principales factores impulsores para la empresa son migrar las máquinas para reducir los costes, aumentar la productividad y mejorar la agilidad de las operaciones de TI. El modelo de prestación que más se ajusta a las necesidades de la empresa es el de Infraestructura como servicio, IaaS.

Dentro de IaaS podemos diferenciar tres tipos, nubes públicas, nube privadas y nubes híbridas. La pregunta lógica a continuación sería: cuál es la solución que mejor se adapta a las necesidades de la empresa. Para ello tenemos que observar los servicios que queremos migrar a la misma.

En primer lugar el servicio más crítico, al que debemos ponerle más grados de seguridad, es al servidor de correos de nóminas, debido a que contiene los datos personales, datos de afiliación a sindicatos y datos económicos, que son según la LOPD datos de nivel alto por lo que hay que salvaguardarlos. Teniendo esto en cuenta trataremos de analizar qué solución de nube sería la más recomendable para migrar el servidor de correo de nóminas a la nube.

Nube pública:

En el caso de migrarlo a la nube pública, los usuarios podrían acceder desde cualquier lugar con lo que se cumpliría el primer requerimiento. La empresa tendría que enviar los datos de las nóminas desde el servidor que las genera y envía por SMTP. Aunque el servidor utiliza protocolo TLS para proporcionar seguridad entre cliente y MTA, existen otras amenazas que pueden afectar a los clientes de correo, como envío de spam, ataques de denegación de servicios (DoS), ataque Man in the Middle (MiM), o simplemente capturar los correos esnifando la red por el puerto de escucha del servidor de Zimbra. Esta solución no es muy segura.

Nube privada:

En este caso los equipos forman parte de una red privada dentro de la nube que el proveedor garantiza que nadie puede acceder salvo la empresa que la contrate. Básicamente tenemos que hacer que los usuarios accedan a esta red a través de nuestra infraestructura ya que en este tipo de nube no hay conexión exterior hacia ella. Esto hace que la VPN contratada para acceder desde la empresa a la nube privada se convierta en un cuello de botella.

Nube hibrida:

Este tipo de nube es la solución combinada de las otras dos, por un lado la empresa puede acceder a la red privada en la nube por VPN y por otro lado los empleados pueden acceder solo a los servicios publicados hacia el exterior desde esta nube híbrida.

Existen varias soluciones de proveedores IaaS que ofrecen servicio de nube híbrida pero en este TFM se compararán las tres soluciones de plataformas de infraestructura emergente más importantes y representativas: VMware vCloud, OpenStack (que también es representativo de otros proyectos de código abierto, como el relacionado con Red Hat KVM), Windows Azure y Amazon AWS.

3.3 Análisis de soluciones existentes

Hoy en día, la computación en la nube evoluciona rápidamente gracias a la amplia gama de tecnologías ya existente y nueva de los fabricantes. Los requisitos para analizar para cualquier solución de computación en la nube híbrida se han acordado de forma general. Se han escogido también los proveedores de computación en la nube más representativos de los tres diferentes modelos escogidos. Todos esos proveedores incluyen amplio acceso a la red, según demanda, a través de una interfaz de autoservicio, y un grupo de recursos compartidos (pool) de TI caracterizados por su rápida elasticidad y que se consumen como un servicio medible de pago por uso. No obstante, a partir de aquí, los modelos de prestación e implementación varían mucho:

3.3.1 Amazon

Amazon Virtual Private Cloud (Amazon VPC) (15)

Amazon Virtual Private Cloud (Amazon VPC) permite aprovisionar una zona aislada de forma lógica dentro la nube de Amazon Web Services (AWS), donde se puede lanzar recursos de una red virtual.

Es fácil personalizar la configuración de red de Amazon VPC. Por ejemplo, se puede crear una subred de cara al público para los servidores web con acceso a Internet y colocar los sistemas como bases de datos o servidores de aplicaciones, en una subred de uso privado sin acceso a Internet. Se puede aprovechar varias capas de seguridad, incluidos grupos de seguridad y listas de control de acceso a red, para ayudar a controlar el acceso a las instancias de Amazon EC2 desde cada subred. Además, también se puede crear una red privada virtual de hardware entre el centro de datos de su empresa y su VPC, y aprovechar la nube de AWS como una ampliación del centro de datos de su empresa. Veamos si cumple los requisitos funcionales definidos para la empresa: (1)

Disponibilidad y Redundancia

Amazon VPC ofrece un Acuerdo de Nivel de Servicios (SLA en inglés) de un único nivel, en comparación con los SLA de múltiples niveles ofrecidos por VMware y otros proveedores del servicio vCloud Datacenter.

El SLA de Amazon basa su compromiso de disponibilidad únicamente en la capacidad para iniciar nuevas instancias. De hecho, Amazon AWS se ha diseñado para permitir que las instancias fallen, lo que significa que los clientes que ejecuten aplicaciones esenciales para el negocio en AWS deben integrar altos niveles de disponibilidad y redundancia en sus aplicaciones.

Aunque existen empresas que pueden permitirse una gran inversión para hacer esto, la empresa y en general cualquier pequeña y mediana empresa lo tendría muy difícil.

Implementación Rápida

AWS permite importar imágenes de máquinas virtuales a instancias de Amazon EC2 y exportarlas de vuelta al entorno de la empresa.

Seguridad empresarial

Amazon ofrece un nivel de seguridad aceptables para las nubes públicas, incluida la gestión básica de usuarios y los controles de acceso basados en roles, además de posibilidad de creación de VPN. Además todo el tráfico se puede cifrar con SSL.

Amazon se ejecutan en una plataforma de virtualización basada en Xen, que tiene las desventajas propias de una arquitectura Dom0 y un sistema operativo principal integrado. El dominio dom0 es típicamente una versión modificada de Linux, NetBSD o Solaris que para entornos muy grandes, donde se ejecutan muchas máquinas por host, Dom0 tiene un cuello de botella, el cual, limita la escalabilidad y reduce el rendimiento del servidor.

Amazon permite el uso compartido de recursos físicos subyacentes, así como el aislamiento de instancias de máquinas virtuales que se ejecutan en la misma máquina física. Sin embargo, este

proveedor no ofrece auténticos grupos de recursos lógicos (pool), dado que deben dedicar los hosts a los clientes para garantizar la disponibilidad de los recursos.

Amazon AWS tampoco ofrece los controles granulares de recursos de vSphere, lo que les impide garantizar los niveles de calidad de servicio para las aplicaciones prioritarias de los clientes.

Escalabilidad, Agilidad y Compatibilidad

Amazon ofrece AWS Virtual Private Cloud (VPC), que incluye una nube privada virtual con la opción de una infraestructura dedicada, utilizando instancias dedicadas. Los clientes pueden migrar cargas de trabajo entre VPC y la infraestructura en la nube pública de AWS, aunque esto requiere cierto grado de configuración de la red y Amazon no lo recomienda.

Aunque los clientes de AWS pueden configurar una red privada virtual (VPN) basada en hardware para conectar la infraestructura de su empresa con Amazon VPC, Amazon no ofrece a los clientes una solución de nube en las instalaciones. Además, debido en gran parte al entorno EC2 patentado por Amazon, actualmente los clientes no pueden migrar fácilmente las aplicaciones entre AWS y las nubes instaladas en las empresas. Amazon no puede ofrecer actualmente una auténtica funcionalidad de Nube Híbrida.

Libertad de elección y portabilidad de las aplicaciones

Amazon ofrece una única solución respectivamente, pero no dan la posibilidad de que el cliente puede elegir otro proveedor de nube y migrar las aplicaciones de una nube a otra. Es decir, el cliente no tiene libertad de elección para cambiar de proveedor en cualquier momento, y si lo hiciera tendría que importar de nuevo las máquinas a su centro de datos para después exportarlas a la nube del proveedor destino. Esas operaciones de importación o exportación pueden necesitar además la conversión desde el formato original que tenían en Amazon al formato de máquina virtual que se utiliza en el destino.

3.3.2 Rackspace

Disponibilidad y Redundancia

Rackspace garantiza el 100 % del tiempo de actividad de la red, salvo en los periodos de mantenimiento programado, así como la restauración de los hosts de servidor en la Nube en una hora en caso de fallo, pero no garantiza *específicamente la disponibilidad de las cargas de trabajo*.

Implementación Rápida

Rackspace utiliza imágenes que cumplan los requisitos de OpenStack (2), esto hace que la implementación no sea rápida.

Seguridad empresarial

Rackspace ofrece un nivel de seguridad aceptables para las nubes públicas, incluida la gestión básica de usuarios y los controles de acceso basados en roles, además de posibilidad de creación de VPN. Además todo el tráfico se puede cifrar con SSL.

Rackspace al igual que Amazon se ejecuta en una plataforma de virtualización basada en Xen, por lo también tiene limitada la escalabilidad y el rendimiento del servidor.

Rackspace permite también el uso compartido de recursos físicos subyacentes, pero tampoco ofrece auténticos grupos de recursos lógicos (pool), y deben dedicar los hosts a los clientes para garantizar la disponibilidad de los recursos.

Rackspace Cloud tampoco ofrecen los controles granulares de recursos de vSphere, lo que les impide garantizar los niveles de calidad de servicio para las aplicaciones prioritarias de los clientes.

Escalabilidad, Agilidad y Compatibilidad

Rackspace, no ofrece una infraestructura dedicada (privada y virtual) que sea compatible con la oferta de nube pública. Aunque Rackspace cuenta con una solución de nube privada basada en VMware, no es compatible con su nube pública y, dado el compromiso de Rackspace con OpenStack, seguirá siendo incompatible en el futuro.

Rackspace no ofrece una auténtica funcionalidad de Nube Híbrida.

Libertad de elección y portabilidad de las aplicaciones

Rackspace al igual que Amazon ofrece una única solución respectivamente por lo que el cliente no puede elegir otro proveedor de nube y migrar las aplicaciones de una nube a otra. Por otra parte, las aplicaciones o máquinas virtuales que residen en Rackspace no se pueden portar sin antes realizar la conversión de formato al que utiliza el otro proveedor.

3.3.3 Vmware y Dell

Al contrario que los otros dos ecosistemas, el ecosistema formado por el tándem VMware y Dell destaca por su programa vCloud Datacenter Services y porque ha creado el programa de proveedor de servicios de nube pública e híbrida para partners.

Veamos si cumple los requisitos funcionales:

Disponibilidad y Redundancia

Dell ofrece acuerdos de nivel de servicio (SLA) en tres niveles diferentes:

1. El primer nivel corresponde a un servicio multicliente de pago por uso que permite que un cliente de una pyme coloque cargas de trabajo de vSphere en la nube de Dell cada mes.

2. El segundo nivel se denomina Reserved y es un servicio multicliente con un compromiso mínimo de un año en el que un cliente puede reservar una cantidad fija de capacidad en la nube para usarla.
3. El tercer nivel, y el más riguroso, se denomina Dedicated. Se trata de un servicio de un único cliente con un compromiso mínimo de 1 año, en el que las cargas de trabajo del cliente pueden ocupar servidores enteros para su entorno de VMware vCloud.

El SLA de Dell es más estricto que la mayoría de los SLA de nube porque especifica la disponibilidad de la carga de trabajo. Si las cargas de trabajo de un cliente no están disponibles al menos el 99,95 % del tiempo, salvo en los periodos de mantenimiento programado por Dell, Dell abonará una cantidad por el tiempo de inactividad que se produzca.

Implementación rápida

Las pymes pueden conseguir que sus cargas de trabajo basadas en el software de VMware vSphere funcionen en una solución IaaS alojada de Dell en cuestión de unas horas o menos simplemente convirtiéndolas al formato de virtualización abierta (OVF) y cargándolas en la nube de Dell.

Seguridad transparente y gestionable

El servicio de centro de datos de vCloud cumple con las normas SAS 70 Tipo II o ISO 27001 e incluye funciones de firewall compatibles con la virtualización y con las aplicaciones, aislamiento de nivel 2, control de acceso basado en funciones e integración de directorio activo. El servicio Dell SecureWorks Active Monitoring proporciona continuamente información de supervisión en tiempo real, correlación de eventos y análisis especializado de la actividad de seguridad para las cargas de trabajo de pymes que se ejecutan en la nube de Dell-VMware.

Dell-VMware ofrece la posibilidad de dedicar la infraestructura en la nube pública a las cargas de trabajo importantes para la empresa y que deban aislarse con fines de cumplimiento normativo o que requieran niveles elevados de calidad de servicio. El nivel de servicio Dedicated permite obtener un rendimiento más predecible al garantizar que los recursos están siempre disponibles cuando se necesitan.

Escalabilidad, Agilidad y Compatibilidad

El programa vCloud Datacenter Services proporciona una serie de servicios de formación y certificación, y requiere a los proveedores de servicios que participen cumplan las normas empresariales de seguridad, agilidad y portabilidad de las aplicaciones.

Libertad de elección y portabilidad de las aplicaciones

Como todas las ofertas de servicios de centros de datos de vCloud están basadas en la misma tecnología compatible de VMware, proporcionan la interoperabilidad y la portabilidad necesarias para que las empresas puedan implementar las cargas de trabajo en la infraestructura de la empresa en nubes públicas y para que puedan migrar las cargas de trabajo de una nube a otra según las necesidades.

En la tabla resumen que se muestra a continuación, he asignado un valor de 0 a 10 para puntuar a cada uno de los proveedores representativos que se han analizado, por cada uno de los requisitos que hemos definido en este estudio de migración a la nube híbrida.

Requisitos de Cloud Híbrida	Vmware vCloud	OpenStack	Amazon AWS
Disponibilidad y redundancia	*8*	*6*	*7*
Implementación rápida			
Seguridad transparente y gestionable	*10*	*6*	*7*
Escalabilidad, Agilidad y Compatibilidad	*8*	*5*	*7*
Libertad de elección y portabilidad de las aplicaciones	*10*	*5*	*5*
Puntuación General	*9*	*5,5*	*6,5*

Tabla Resumen de Análisis de Soluciones Existentes

3.4 Seguridad en las Soluciones

La empresa cuando realizar una migración a la nube obtiene una serie de ventajas, como el ahorro de costes, mejora de la continuidad de negocio, acceso a herramientas que hasta el momento sólo estaban disponibles para la gran empresa, la flexibilidad de despliegue o facilidad para acceder a los datos desde cualquier lugar y dispositivo. Si a todo esto le unimos una mejora para la movilidad de los empleados donde los recursos que necesita para trabajar están accesibles siempre que tenga una conexión a Internet, la nube parece tener sólo ventajas. (9)

Sin embargo, esta ventaja supone una cesión del control de nuestros datos a terceros ya que el servidor donde se guardan no está en nuestras instalaciones y esto lleva a muchas empresas a dudar de si estarán o no seguros alojados en servidores externos.

Todos los proveedores ofrecen copias de seguridad de nuestros datos de forma que en caso de cualquier problema, se pueda volver a tener en marcha los sistemas de forma rápida. En todo caso, implica que se dependa de otros a la hora de restablecerlos, algo que no acaba de convencer a muchas empresas. Un ejemplo puede ser las paradas planificadas por mantenimiento, donde es la empresa proveedora de servicio la que decide en qué momento se ejecutan y no siempre se realizarán los días y horarios adecuados para estas empresas.

En cuanto a la seguridad en la transmisión de los datos, el tráfico de datos suele ir cifrado, de manera que aunque se intercepte, no podrán obtener los datos en claro. Otra cuestión es quién puede acceder a los datos y desde dónde podemos hacerlo. Es bastante improbable que alguien pueda acceder al servidor y robar datos que sean estratégicos, en cambio es mucho más fácil que el robo de datos se produzca por empleados de la propia organización, que por un operador del centro de datos del servidor en la nube.

Por último, tenemos el debate de la continuidad de negocio. Para que nuestro servidor esté siempre disponible en la empresa necesitamos redundancia. Es decir, un servidor principal y otro secundario que

entra en juego cuando el primero ha fallado, pero también redundancia en la fuente de alimentación, en el almacenamiento de los datos, etc. Todo esto hace que los costes de mantener una infraestructura en local sean elevados. Si hablamos de aplicaciones, también tendremos que ir actualizando las versiones de dicha aplicación. La mayoría de las plataformas en la nube garantizan redundancia y alta disponibilidad, en torno al 99'95%, algo muy difícil y sobre todo muy caro de conseguir en las instalaciones de la empresa. Esto hace que la nube resulte más segura y más rápida de restaurar ante cualquier incidente.

Podemos considerar el servicio de nube híbrida como la combinación de nube privada más nube pública. En nuestro caso en la parte pública, tanto en el equipo de nóminas con Zimbra como en el equipo de Gestión de Incidencias y Petición de Servicios utilizan comunicaciones seguras por https. Todos utilizan un usuario y una contraseña para acceder a ellos. En el caso del Portal Web Corporativo se utiliza también https y usuario y contraseña.

Por otro lado en la parte privada, el hecho de utilizar un servicio de nube híbrida supone que la comunicación M2M estará garantizada por el servicio en sí, ya que en ningún momento se expone esa comunicación a Internet, sino que se realiza en la parte privada de la nube híbrida.

3.5 Análisis del coste de cada solución

Aunque los tres proveedores de nubes públicas ofrecen transparencia en los precios, el cálculo de los costes y la facturación de los servicios, se necesita bastante tiempo para entender bien todos los cargos que se aplicarán después de contratar un servicio de Nube Pública IaaS.

Por ejemplo, Amazon AWS ofrece capacidad informática a un bajo coste por hora, pero añade otros cargos a la factura del cliente a lo largo del tiempo, incluidos gastos de almacenamiento, transferencia de datos y uso de la red.

En resumen, se deberían comparar detenidamente los costes y tener en cuenta el coste total de propiedad, en lugar de valorar solo los costes iniciales de adquisición del servicio. Todos estos costes que no aparecen al inicio se suman al coste final por lo que para analizar fielmente los costes de cada solución habría que realizar una migración al proveedor en cuestión. En las conclusiones finales del TFM se pueden leer algunos razonamientos en este sentido.

3.6 Toma de decisión sobre qué proveedor de Nube utilizar

Podemos resumir que las necesidades de la empresa pasan por ofrecer un servicio en la web que sea seguro y que se gestione de forma totalmente automatizada, a sus empleados.

La empresa ya utiliza la infraestructura de virtualización Vmware para la mayoría de los servidores de la red local. Algunas máquinas virtuales en esta infraestructura ya reflejan cierto agotamiento debido a que se hace necesario escalarlas, no sólo aprovisionándolas de más recursos de memoria y procesamiento, sino también de ancho de banda para los accesos cada vez más numerosos que se realizan de diferentes dispositivos por parte de los empleados.

De esta forma, la decisión de migrar estos servicios a la nube puede resultar ser muy acertada para la empresa pero ahora bien, la pregunta sería a qué tipo de nube, ¿Pública, Privada o Híbrida?

La Nube pública requiere menor inversión inicial y pone a disposición un *pool* de recursos ilimitado. La Nube Privada ofrece hardware dedicado exclusivo para los servidores virtuales de la empresa, mantenimiento personalizado y configuración a medida.

En cambio la Nube Híbrida ofrece la combinación de dos o más servicios de nube. Las nubes híbridas permiten combinar recursos de una nube privada con una nube pública en momentos puntuales, mejorando así la capacidad de respuesta de las aplicaciones y pagando sólo por los recursos informáticos adicionales cuando se necesitan. A su vez, muchos proveedores son capaces de integrar servicios de Nube para empresas con servicios como housing, servidores dedicados o cualquier otra solución no necesariamente de Nube.

Vmware ofrece los servicios de Nube Híbrida a través de una serie de partners que utilizan su Software vCloud. Con este software, la infraestructura de servidores virtuales de vCloud , los administradores pueden virtualizar parte o toda su infraestructura IT de forma segura en Data Center de última generación en la Nube, todo ello desde una interfaz intuitiva de autoservicio. De esta forma, se obtiene una mejora de la fiabilidad y la escalabilidad, una gestión sencilla y se reduce el coste total de propiedad. (11). El servicio vCloud está construido con tecnología VMware vCloud que posibilita total compatibilidad con cualquier entorno VMware y permite crear una solución nube híbrida como se muestra en la ilustración 5. (8)

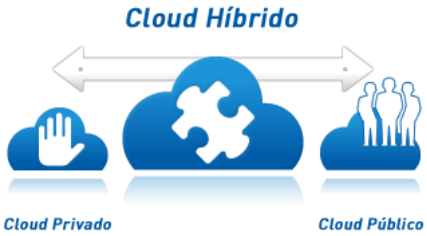

Ilustración 5: Nube Híbrida

La decisión tomada para analizar un servicio de nube híbrida, es la solución de VMware vCloud, pero para probar este servicio no existe ningún proveedor en el mercado que permita realizar pruebas durante un periodo de tiempo como permite otros proveedores como Amazon AWS.

4 DESARROLLO DE LA SOLUCION

Para poder hacer una prueba combinando los sistemas IT internos existentes con el servicio del Proveedor de vCloud para crear una infraestructura híbrida, se creó un laboratorio de evaluación del software VMware vCloud.

Para ello, por una parte hay que descargarse de la página web de VMware el software necesario e instalarlo en modo de evaluación, que normalmente en casi todos los productos es de 60 días. Por otro lado, hay que descargar el sistema operativo de otras máquinas virtuales necesarias para el entorno de ejecución del laboratorio como son el servidor de directorio activo, o para la instalación del vCenter Server. Microsoft Windows Servidor 2008 puede ejecutarse sin activarse durante un periodo de evaluación de 30 días, suficientes para terminar la evaluación.

4.1 Documentación sobre la solución.

He tomado prestado este diagrama de VMware (3) para mostrar y simplificar la solución VMware Cloud. La mayor parte de la nube de VMware vCloud como lo conocemos se encuentra principalmente en el segmento de IaaS.

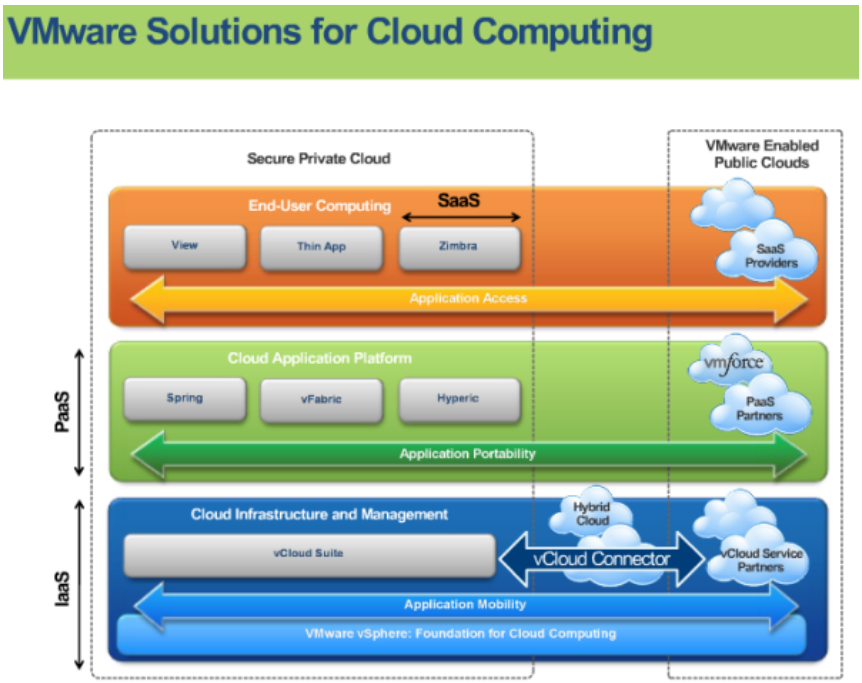

Ilustración 6: VMware Cloud

La suite VMware vCloud consta de:

1. *vSphere Enterprise Plus*
2. *vCloud Director (VCD)*
3. *vCloud Connector (VCC)*
4. *vCloud Networking y Seguridad -Standard y Advanced (anteriormente conocidos como vShield Edge y vShield Manager)*
5. *vCenter Site Recovery Manager (SRM)*
6. *VMware vCenter Operations (vCOps)*
7. *vCenter Chargeback Manager (VCM)*
8. *vCenter Configuration Manager para vSphere*
9. Navigator Infraestructure vCenter
10. vFabric Application Director
11. vCloud Automation Center

La suite vCloud está disponible en tres ediciones: **Standard, Advanced y Enterprise**. El cliente elige una de ellas en función del tipo de carga de trabajo, la escalabilidad y la funcionalidad requerida para su

nube privada. El papel principal de estos componentes lo juegan: vSphere, vCloud Director, vCloud Networking & Security (vCNS) (vShield Manager).

Voy a dar una breve introducción a todos estos componentes, aunque muchos de ellos no lo utilizaremos porque no son necesarios para el propósito del laboratorio de evaluación.

vSphere: Este es el primer bloque de construcción a través del cual se virtualiza el centro de datos para convertirlo un centro de datos virtual. Se puede crear un pool de todos los recursos de memoria y de almacenamiento y procesamiento, de modo que en el futuro pueden auto-aprovisionarse y administrarse a través de una solución de Cloud. En esta capa también se suelen construir los conmutadores virtuales y los conmutadores virtuales distribuidos, grupos de puertos, etc. Aquí su herramienta de gestión es vCenter Server y los servidores físicos de alojamiento de máquinas virtuales (VM) son servidores ESXi. Aquí se crean todos los recursos virtuales. La consola de gestión se llama vSphere Web Client.

vCloud Director: La capa superior en la nube es la capa de vCloud Director que ayuda en el auto-aprovisionamiento y la autogestión de los recursos virtuales que se han creado en la capa de vSphere. Después de la instalación se proporciona dos consolas de HTTP, una para administradores y otra para usuarios. A través de la primera se crea las diferentes partes de una nube como, VDC (Virtual Data Center) de Proveedor, VDC de Organización, vApp, Redes de Organización, Redes Externas, etc. Si trasladamos el lugar de vCenter en el datacenter privado a la herramienta de gestión de la nube, ese lugar sería el de vCloud Director.

vCloud Red y Seguridad: Estos no son más que los dispositivos virtuales vShield Edge y vShield Manager, que proporcionan diferentes servicios de red estándar como enrutamiento, NAT, DHCP, VPN e instalaciones como VXLAN. A través de estos se puede aislar a las redes virtuales de su inquilino del mundo externo. Aquí, la herramienta de gestión sigue siendo vCloud Director, sin embargo se puede configurar una parte básica a través de la consola HTTP de vShield. Estos también se instalan como dispositivos virtuales para facilitar la instalación y configuración.

vCloud Connector: Como su nombre indica sirve para conectarse a otra Nube VMware como nubes privadas compatibles y nubes públicas, y facilita una configuración de Nube Híbrida. También puede conectar su nube privada a una nube asociada VMware vCloud y mover cargas de trabajo (básicamente VM) desde su nube privada a la nube pública.

vCenter Chargeback Manager: componente muy importante de vCloud, ya que proporciona el informe de uso de los diferentes componentes de vSphere y en consecuencia posibilitar hacer la medición financiera y operativa en términos de uso.

SRM: Site Recovery Manager se utiliza en la capa de vSphere para BCP / DRP (Continuidad de Negocio / Proceso de Recuperación de Desastres) donde las máquinas virtuales del sitio primario puede reiniciar automáticamente en el sitio secundario en caso de fallo en el suministro eléctrico por ejemplo. Es un componente opcional.
VMware vCenter Operations: vCOps ayuda al administrador para crear consolas HTTP de control sobre el uso, obtener alertas sobre los problemas, planificación de capacidad, optimización, etc.

vCenter Configuration Manager para vSphere proporciona una configuración continua y gestión del cumplimiento de las políticas definidas para las máquinas virtuales .

Infraestructura vCenter Navigator permite la detección de aplicaciones, el mapeo de dependencia, y la gestión de la infraestructura.

vFabric Application Director proporciona un servicio de aplicación de la publicación de catálogos de múltiples niveles.

vCloud Automation Center permite a los usuarios / administradores / desarrolladores acceder a los menús predefinidos, los catálogos, las opciones de autoservicio para solicitar los recursos y servicios de TI. Esta consola HTTP también permite gestionar cualquier servicio solicitado, es parecido a la consola AWS Console en Amazon Web Services.

Además de éstos, existe también **vCloud API** (Interfaz de Programación de Aplicaciones) que actualmente se limita a VMware y sus socios.

4.2 Preparación del Laboratorio

Para la preparación del laboratorio para evaluar el servicio de Nube Híbrida se ha dispuesto de dos servidores, una estación de trabajo y un portátil que hospedaran a todas las máquinas virtuales necesarias para la evaluación. También se utilizó la cabina de almacenamiento de EMC ya descatalogada por el fabricante CX-320DE y otra cabina de almacenamiento NEC, modelo M-100. Ambas proporcionan Logical Unit Number (LUN) a los servidores. Para la red se utilizó un switch Cisco modelo 300-20 con 20 puerto Gigaethernet y funcionando en nivel 3, por lo que permite realizar enrutamiento de paquetes IP.

4.2.1 Configuración de almacenamiento:

La cabina EMC CX-320DE cuenta con adaptadores de Fibre Channel (FC) red duales en cada unidad procesadora de almacenamiento, los cuales están conectados a un conmutador de FC Brocade.

VMware utiliza como hipervisor al software VMware ESXi. Este software se instala directamente sobre el hardware sin necesidad de un sistema operativo. En realidad, ESXi se deriva del sistema operativo Red Hat Enterprise Linux, pero lo han modificado para permitir ofrecer una capa de virtualización que permita ejecutar varios sistemas operativos (VM) sobre la misma máquina física.

En el caso de la infraestructura de la empresa, los equipos que llevan ESX tienen adaptadores de FC (HBA) que se conectan al conmutador de Fibre Channel por lo que el almacenamiento de la cabina es compartido por todos los servidores ESXis. Esto es fundamental para crear un clúster después en Vmware pero debido a la falta de recursos en este laboratorio no será posible poner los ESXis así.

En primer lugar para nuestro laboratorio, crearemos dos LUNs de 250 GB y 300 Gb en la cabina que asignaremos al Storage Group de laboratorio para que puedan ser vistos por el ESXi instalado sobre el PowerEdge 1950 de este laboratorio.

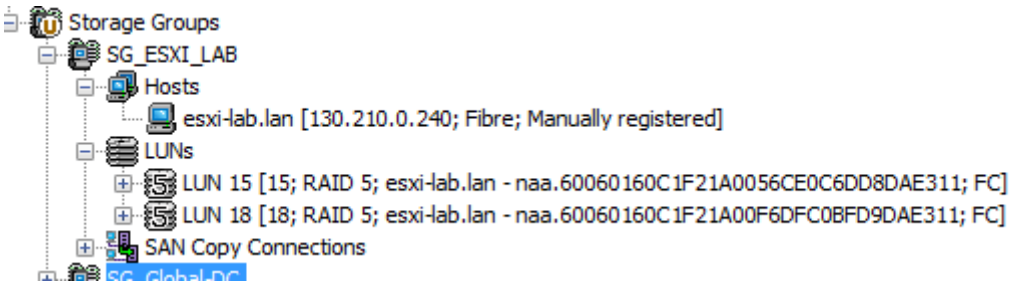

Ilustración 7: LUNs asignadas de la cabina EMC

Como comentaba antes, para simular un clúster hemos conectado el otro ESXi instalado en el PowerEdge 1850 a una SAN NEC-M100 y le hemos asignado dos LUNs de 400 Gb y 50 Gb. Una vez asignada estas LUNs al clúster VMware, hay que crear las unidades de almacenamiento de VMware o Datastores para que sean formateados con el sistema de ficheros VMFS5 y se pueden configurar máquinas virtuales (VMs).

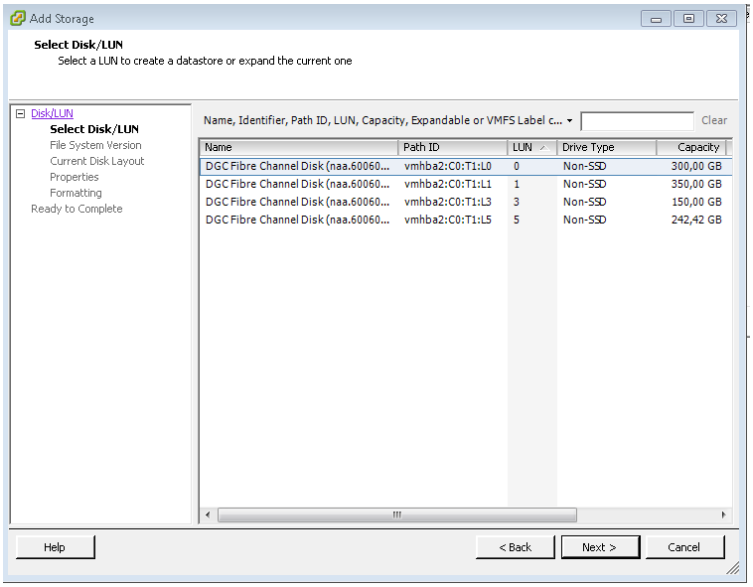

Ilustración 8: Datastores asignados a los ESXis

4.2.2 Descripción del Hardware Utilizado

A continuación paso a describir la configuración utilizada para la creación de un laboratorio para probar la nube híbrida ofrecido por VMware, llamada vCloud.

En el ilustración 9 tenemos el esquema por bloques del laboratorio desplegado para realizar la evaluación de VMware vCloud Hybrid Services (vCHS).

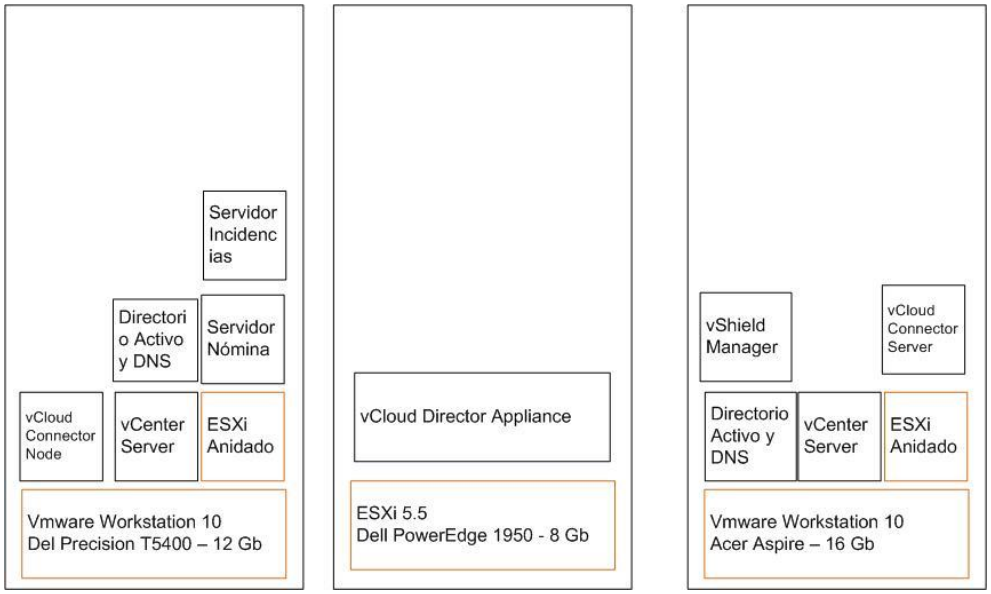

Ilustración 9: Diagrama de bloques del Laboratorio

Esta configuración se ha realizado con dos servidores físicos, una estación de trabajo y un portátil recién adquirido para poder alojar a todos los componentes. En la ilustración 9 sólo aparece un servidor físcio ya que aunque se configuraron dos, el segundo de ellos debido a que dispone de poca memoria RAM (2 GB) y a que se trata de un sistema que tiene procesadores que no soportan virtualización (VT), no se pudo instalar ninguna máquina virtual en él.

Como es lógico VMware no soporta esta configuración para entornos en producción. Sin embargo casi todo funciona para fines de prueba con este hardware limitado. Paso a describir cada componente hardware utilizado:

Hardware de Servidor utilizado:

- Dell PowerEdge 1950
  - 2 Socket Quad Core Processor Intel Xeon E5450
  - 8 GB de RAM
  - Dos Discos Internos SATA en RAID1
  - DRAC
  - Dos tarjetas de red Gigabit
- Dell PowerEdge 1850 (Añadido finalmente para realizar un clúster)
  - 2 Socket Processor Inter Xeon
  - 2 GB de RAM
  - Dos disco internos SCSI Ultra320 de 73 GB
  - Dos tarjetas de red gigabit

- Dell Precission T5400
    - 2 dual-socket Quad-Core Inter Xeon
    - 12 GB de RAM
    - Dos Disco Internos SATA de 400 GB y 150 GB
    - 1 Tarjeta de Red Gigabit
- Acer Aspire E1-772G
    - 1 socket Dual-Core Intel I5 5200
    - 16 GB RAM
    - 1 Disco SATA 1 TB
    - 1 Tarjeta de red Gigabit

Hardware de Red utilizado:

- Cisco conmutador 300-20 trabajando como router (conmutador de Nivel 3).

Hardware de Almacenamiento utilizado:

- EMC CX-320DE con dos LUNs asignadas
- NEC-M100 con dos LUNs asignadas
- Local VMFS sobre el servidor físico

Software Utilizado:

- VMware vSphere vCenter
- VMware vSphere ESXi 5.5
- VMware vCloud Director 1.0 (incluye VMware vShield Edge)
- VMware vShield Manager 4.1 (Virtual Appliance)
- VMware vCloud Connector Server
- VMware vCloud Connector Node
- VMware Workstation 10
- Microsoft Windows 2008 32-bit con AD/DNS server
- Microsoft Windows 2008 R2 64-bit para vCenter server

4.2.2 Máquinas Virtuales en la Nube Local (Nube Privada).

Para la Nube privada se instalaron las siguientes máquinas virtuales con estas características: (4)

SRV-DA

- Hardware
    - 1 vCPU
    - 1 Gb RAM
    - 20 GB HD
- Software
    - Windows 2008 32 bits
    - Instalación Servidor de Directorio Activo y DNS (se creó el dominio ***tfm-ecomercio.com)***

VCENTER_LAN

- Hardware
  - 2 vCPU
  - 4 Gb RAM
  - 40 GB HD
- Software
  - Windows 2008 R2 64 bits
  - Vmware Vcenter 5.5

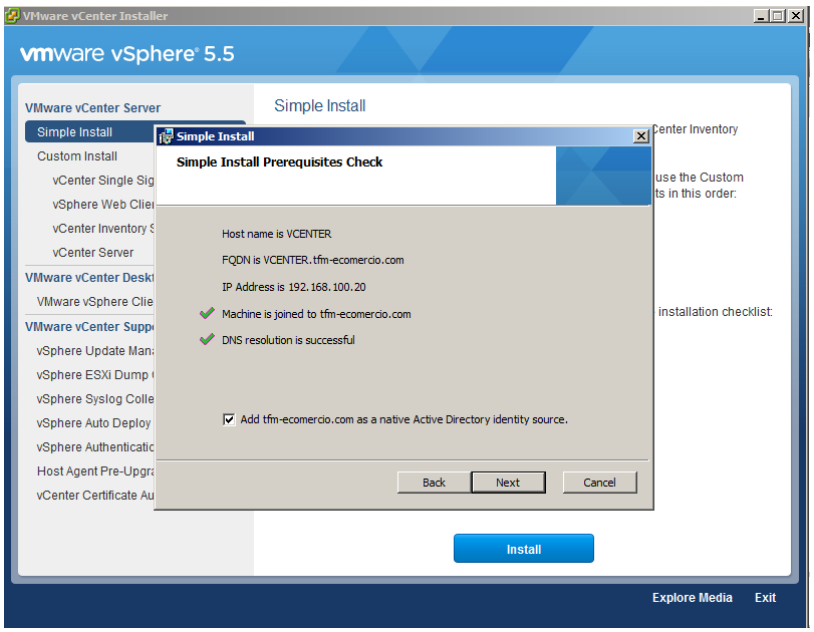

Ilustración 10: vCenter Nube Local

ESXi

- Hardware
  - 2 CPU Intel Xeon Quad Core
  - 8 GB RAM
  - 384 Gb Datastore1
  - 248 Gb DataStore2
- Software
  - Vmware ESXi 5.5
  - Instalación de ESXi 5.5

Añadir host ESXi 5.5 al servidor vCenter desde la consola vSphere Web Client.

4.2.3 Máquinas Virtuales en la Nube Pública

Para la nube pública se instalaron las siguientes Máquinas Virtuales: (7)

SRV-DA

- Hardware
  - 1 vCPU
  - 1 Gb RAM
  - 20 GB HD
- Software

- Windows 2008 32 bits
- Instalación Servidor de Directorio Activo y DNS (se creó el dominio **tfmvcloud.com)**

VCENTER_vCHS

- Hardware
  - 2 vCPU
  - 4 Gb RAM
  - 40 GB HD
- Software
  - Windows 2008 R2 64 bits
  - Vmware Vcenter 5.5

ESXi 5.5 Anidado

- Hardware
  - 2 vCPU
  - 8 GB RAM
  - 200 Gb Datastore1
- Software
  - Vmware ESXi 5.5

ESXi 5.5

- Hardware
  - 2 CPU Intel Xeon Quad-Core
  - 8 GB RAM
  - 350 Gb Datastore1
  - 150 Gb DataStore2
- Software
  - Vmware ESXi 5.5

ESXi .4.1

- Hardware
  - 2 CPU Intel Xeon
  - 4 GB RAM
  - 40 Gb Datastore1
  - 400 Gb DataStore2
- Software
  - Vmware ESXi 4.1

4.2.4 Descripción de la Red de Laboratorio

Se han utilizado tres subredes diferentes para interconectar los diferentes máquinas entre sí, uno de las redes simulará una red pública en la nube, mientras que las dos restantes simulan redes internas a la empresa. A continuación se expone la numeración utilizada para cada una de las subredes creadas y en la ilustración 11 un diagrama de cómo están interconectados los componentes de la red de laboratorio.

Subredes Utilizadas:

- 192.168.100.0/24 – Red Privada
- 192.168.200.0/24 – Red Gestión Almacenamiento ESXi físicos
- 192.168.201.0/24 – Red Pública de la Nube

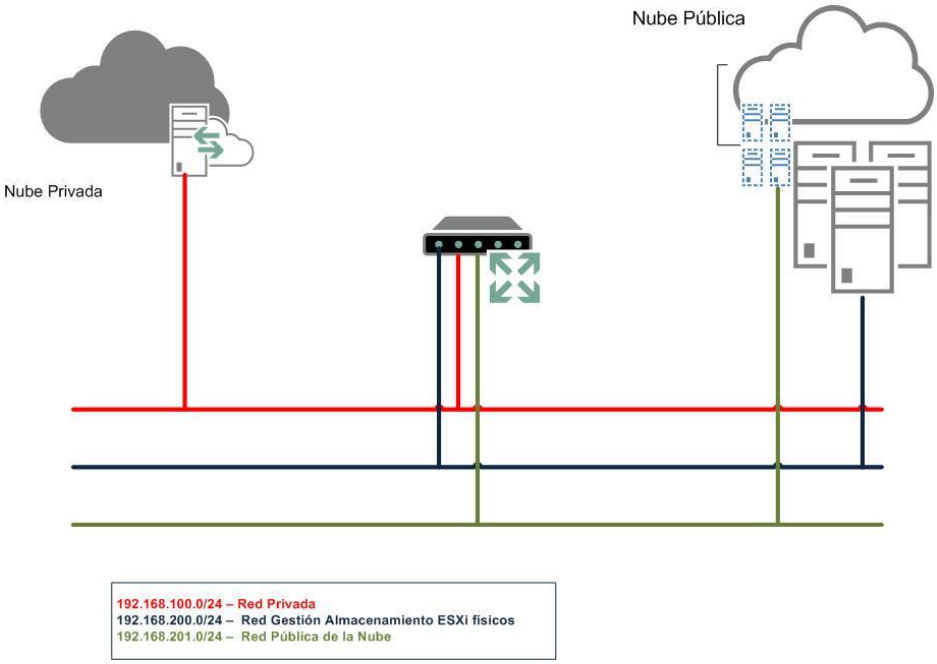

Ilustración 11: Red de Laboratorio

Diagrama de despliegue de las Máquinas Virtuales

El entorno de laboratorio simulará dos redes, una privada y otra pública que se conectarán con el servicio de Nube Híbrida vCHS para traspasar, crear, copiar, provisionar, etc. máquinas virtuales dentro de un entorno seguro y altamente escalable.

Para tener una idea más clara de donde se instalarán las máquinas virtuales, he confeccionado el siguiente diagrama:

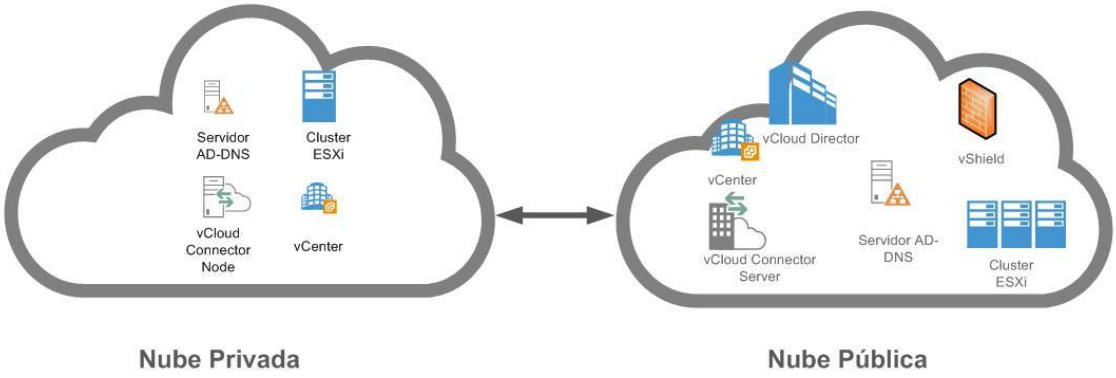

Ilustración 12: Distribución de las Máquinas Virtuales

El equipo Dell Precision T5400 con 12 Gb de RAM será el equipo que alojará la Nube Privada. En este equipo es donde se instalarán las siguientes MVs: Servidor de Directorio Activo, servidor vCenter, ESXi 5.5 virtualizado con Almacenamiento local, y la MV vCloud Connector Node.

El resto de equipos simularán la nube pública, con las siguientes máquinas virtuales, vCenter Server, vShield Manager, vCloud Director y servidor de Directorio Activo – DNS. El clúster de ESXi está formado

por los dos servidores físicos Dell PowerEdge conectadas cada una a una SAN FC y por un ESXi virtualizado en el entorno de virtualización Vmware Workstation 10 (ESX anidado).

El hecho de no tener un clúster ESXi preparado y habilitado, es decir que todos los hosts ESXi estén conectadas a la misma SAN y "vean" las mismas LUNs, limita las pruebas del laboratorio en cuanto al almacenamiento en la parte de la nube pública, al no poder contar con dos de las características más importantes del clúster: High Availability (HA) y Distribuited Resources Scheduler (DRS) en el clúster.

4.3 Pruebas de Laboratorio

Una vez preparado el laboratorio con todas las máquinas virtuales ejecutándose cada una en su entorno, el siguiente paso es configurar la nube privada, la nube pública y la híbrida.

4.3.1 Configuración de la Nube Privada

Este sería el primer bloque del diagrama por bloques de la ilustración 9. Una vez descargado el VMware Workstation 10 nos permitirá instalarlo y funcionar con él durante 60 días en modo de evaluación. (10)

Lo primero que debemos realizar es definir la red privada, en este caso usaremos la red 192.168.100.0/24 con el nombre VMnet0. A esta red también se conecta el equipo anfitrión o host de forma que podamos usar el navegador y compartir recursos directamente con las máquinas virtuales que crearemos después.

En la ilustración 13 vemos que la red VMnet0 está conectada directamente a la red del host de forma que puedan acceder a Internet directamente sin necesidad de realizar NAT.

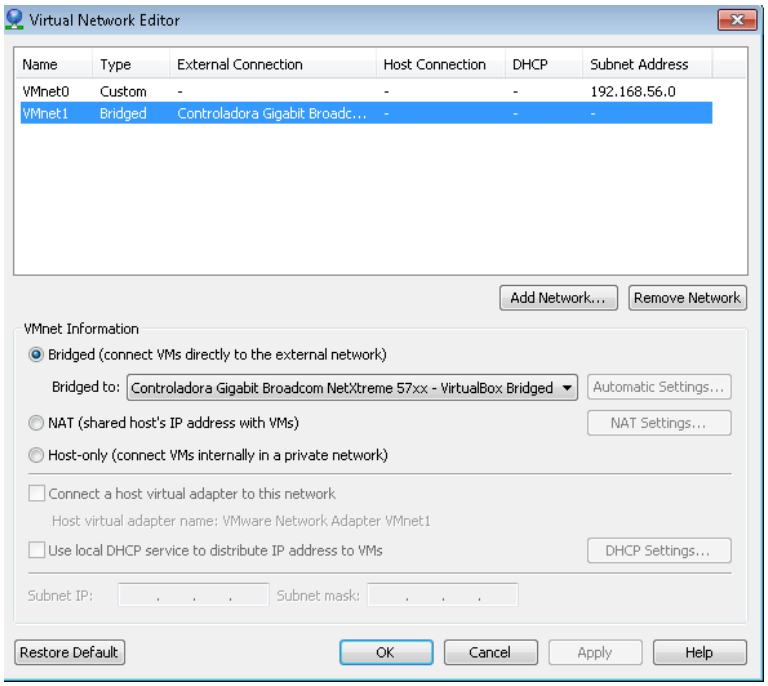

Ilustración 13: Red Local del Host y las Máquinas Virtuales

El equipo host tiene 12 GB de RAM por lo que a la hora de virtualizar nuestras máquinas hay que tener cuidado con la cantidad de memoria que le asignemos a las mismas.

La primera máquina a instalar será el hipervisor VMware ESXi 5.5 dentro del entorno de virtualización Vmware Workstation 10. Vmware llama a este servidor ESXi como ESXi anidado (nested) debido a que el servidor ESXi en un entorno de producción, es el equipo anfitrión para la infraestructura de virtualización Vmware.

La limitación de los ESXi anidados es que en ellos no se pueden virtualizar máquinas de 64 bits. Además para que no nos consuma demasiada RAM del equipo sólo le asignaremos 2 Gb de RAM.

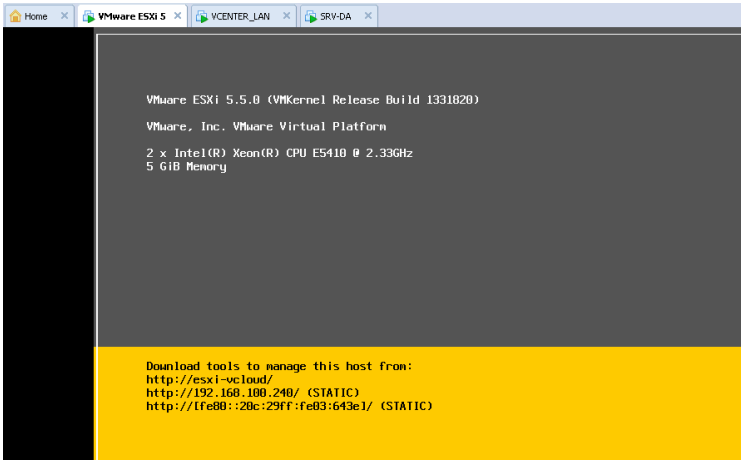

Ilustración 14: Host ESXi 5.5 virtualizado en VMworkstation

Una vez virtualizada esta máquina, con el software VMware vSphere Client podemos acceder a la misma para desplegar en ella una máquina virtual de 1Gb de RAM con Microsoft Windows 2008 de 32 bits. Esta máquina será el Servidor de Directorio Activo y DNS. [1]

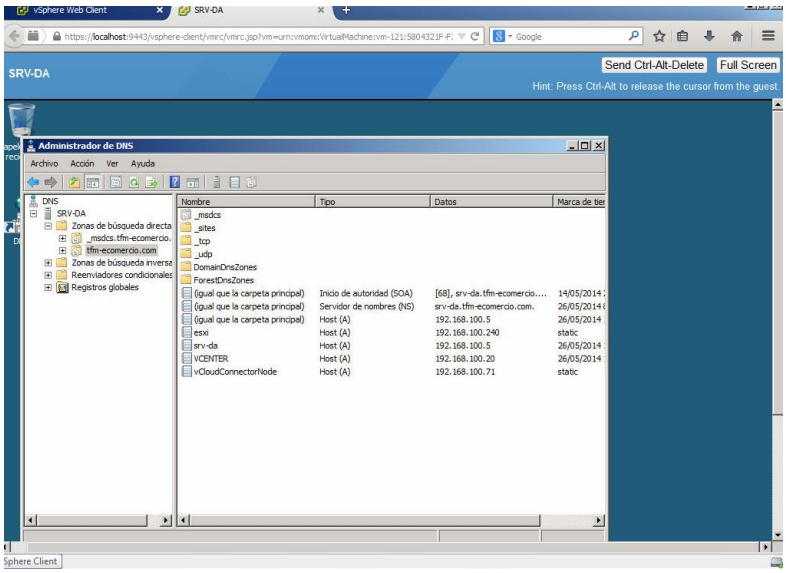

Ilustración 15: Servidor de Directorio Activo-DNS tfm-ecomercio.com

[1] *Nota: El servidor de directorio Activo-DNS se migra desde VMWorkstation hasta el servidor de infraestructura ESXi. Para ello usamos la herramienta VMware Converter Standalone.*

Para el Vmware Virtual Center instalaremos una máquina virtual con 4 Gb de RAM y con sistema operativo Microsoft Windows 2008 R2 64 bits.

La otra máquina virtual que se instalará en la parte 6 será el equipo con el software vCloud Connector Node. En la ilustración 16 podemos ver cómo queda la parte privada de nuestro laboratorio:

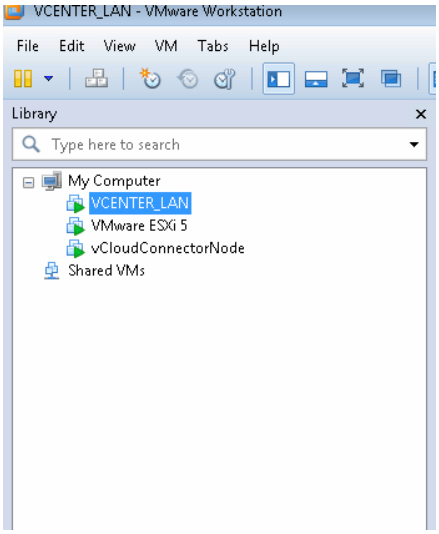

Ilustración 16: Entorno de la Nube Privada

4.3.2- Configuración de la Nube Pública

Para la nube pública tenemos que tener en cuenta varios aspectos de instalación y configuración que vienen detallados en las guía de instalación de cada componente. Es importante leerlos con detenimiento ya que en muchas ocasiones debido a incompatibilidades de las máquinas virtuales y del entorno en que se despliega, es posible tener que repetir el proceso para que cumpla con las exigencias de las mismas. En otras ocasiones, la limitación impuesta por el hardware, por la falta de recursos principalmente de memoria RAM, ha hecho necesario redesplegar alguna máquina virtual en otro hosts o en el mismo entorno del VMware Workstation 10.

En alguna otra ocasión, las limitaciones se han producido por falta de vCPU con lo que se ha tenido que quitar CPU virtuales (vCPU) para que dicha máquina virtual pudiese funcionar razonablemente bien y coexistiendo con el resto de las máquinas virtuales necesarias para la simulación.

Instalaremos una máquina virtual con Microsoft Windows Server 2008 de 32 bits con 1 Gb de RAM y 20 Gb de disco duro como servidor de Directorio Activo –DNS. En la ilustración 17 vemos la máquina virtual ya encendida:

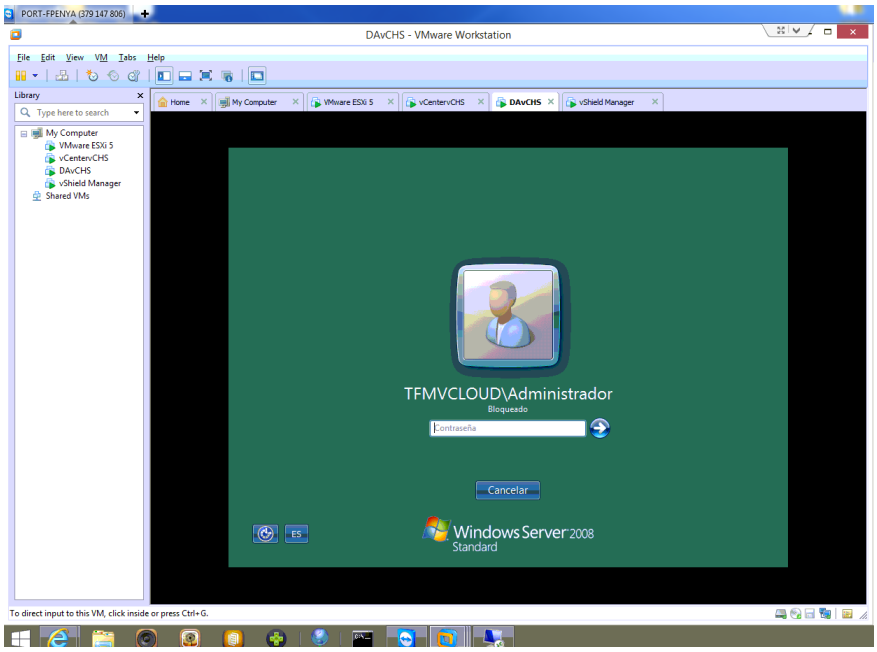

Ilustración 17: Directorio Activo-DNS tfmvcloud.com

Daremos de alta en el DNS los equipos que pertenecen a nuestro dominio en la nube tfmvcloud.com, en la siguiente figura tenemos los nombre de los equipos.

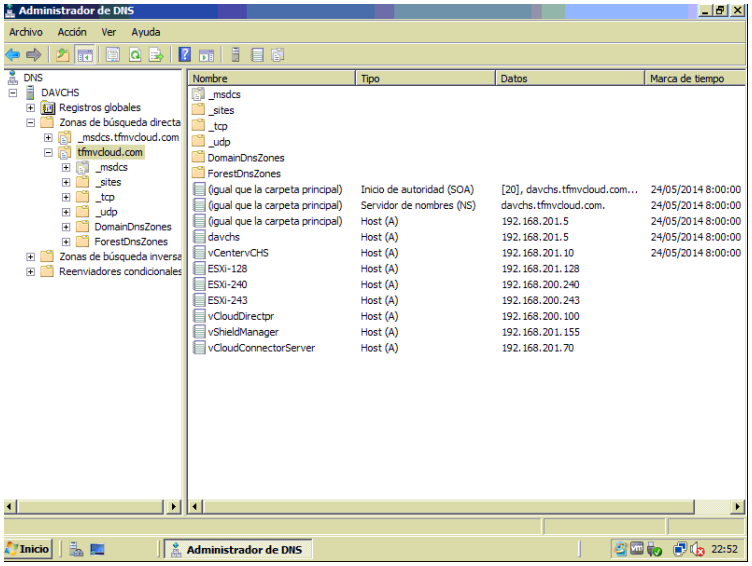

Ilustración 18: Listado de máquinas en el DNS tfmvcloud.com

Se instalarán los 3 ESXi que van a forma parte de nuestra nube pública, dos de ellos se instalarán en máquinas físicas y el tercero será un ESXi anidado en el entorno Vmware Workstation 10. No disponemos de mucha hardware en cada servidor físico por lo que se hizo necesario la creación del ESXi anidado para poder desplegar en el más adelante el vCloud Connector Server.

En la siguiente figura se pueden ver en la esquina inferior izquierda las IP de los tres hosts ESXi, y en el recuadro central otros objetos de alto nivel como son las máquinas virtuales, los datastores y los conmutadores virtuales utilizados.

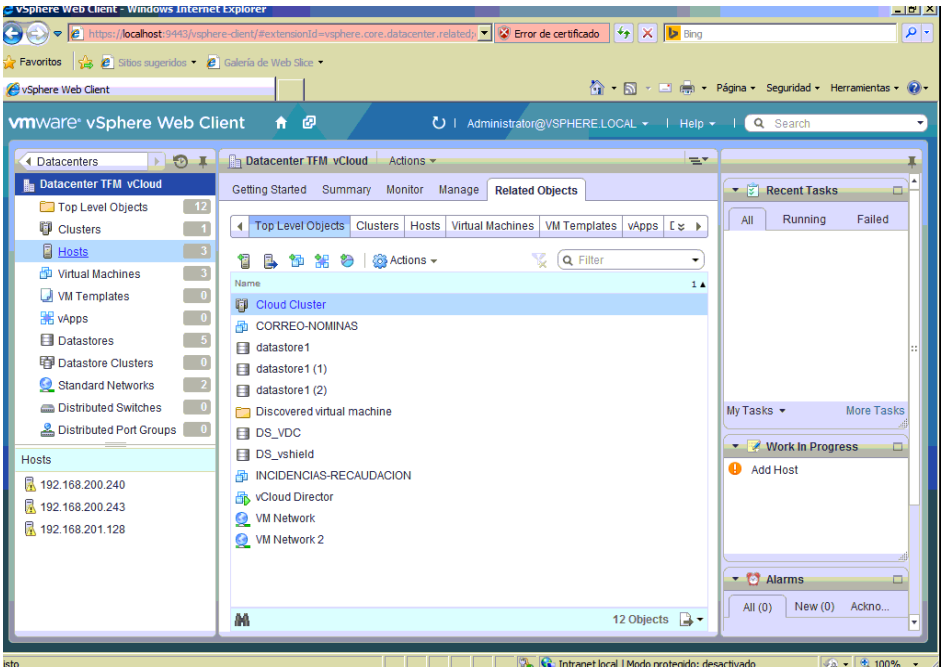

Ilustración 19: Objetos mostrados por el vSphere Web Client

En esta parte del laboratorio tenemos que desplegar el software de VMware vCloud Director, el cual es el software que proporciona a las empresas la posibilidad de construir nubes privadas seguras al aunar los recursos de infraestructura en un Centro de Datos Virtual (Virtual Datacenter), y exponerlos a los usuarios a través de portales basados en la Web e interfaces de servicios basados en catálogos completamente automatizados. (13)

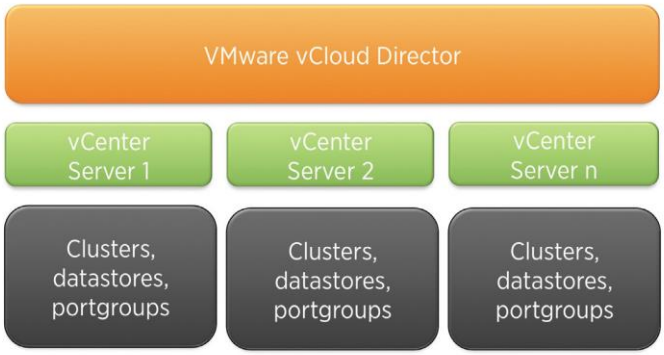

Ilustración 20: Relación entre el VMware vCloud Director y el vCenter

Para instalar el vCloud Director descargamos de la web de VMware el appliance y hacemos el despliegue del mismo sobre el ESXi-240 que tiene 8 Gb de RAM. (7)

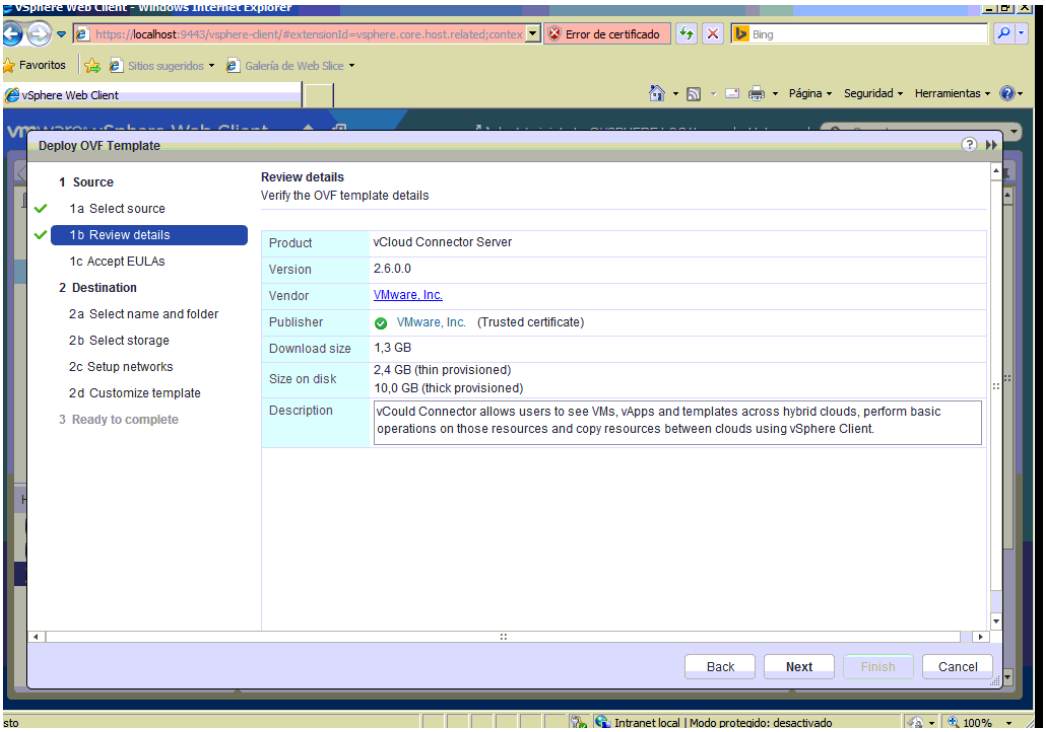

Ilustración 21: Despliegue de vCloud Director

En este apartado se describe cómo instalar el appliance vShield Manager para su uso con vCloud Director, aunque el nombre del producto ha cambiado ahora a VMware vCloud Networking y Seguridad. Los requisitos previos para desplegarlo son: (5)

- Uno o más servidores ESXi en ejecución que están siendo gestionados por vCenter Server.
- Está previsto utilizar vShield Manager con vCloud Director por lo que los ESXi deben estar en un clúster para poder configurar en ese clúster la característica VXLAN-networking.
- Además los ESXi-anfitriones deben estar conectados a un Distributed Switch (dSwitch).

El primero de los requisitos ya se cumple, por lo que quedaría el resto. vShield Manager está integrado en la suite VMware vShield, que es un conjunto de dispositivos virtuales de seguridad integradas para la integración de VMware vCenter Server. vShield es un componente crítico de seguridad para la protección de los centros de datos virtualizados de los ataques y del mal uso. (3)

Debido a las limitaciones de nuestro entorno no ha sido posible desplegar esta máquina en el clúster ESX sino en el entorno de virtualización VMworkstation por lo que no dispondremos de las dos últimas características de esta máquinas pero aun así para los propósitos de evaluación de las características generales de la nube híbrida podemos continuar con la instalación del vCD sin esas características.

Para poder desplegar el appliance VShield Manager en un entorno VMworkstation, una vez descargada de internet hay que primero convertirla a OVF para poder importarla. Para ello se utilizó la herramienta gratuita de Vmware, OVF Tools.

Una vez convertida ya se puede importar a nuestro entorno e iniciar la máquina. Una vez iniciada, entramos con el usuario admin y password wmware y lanzamos el script *setup* que nos pedirá la configuración de red para esta máquina. En el siguiente gráfico vemos la máquina ya desplegada en nuestro entorno. (10)

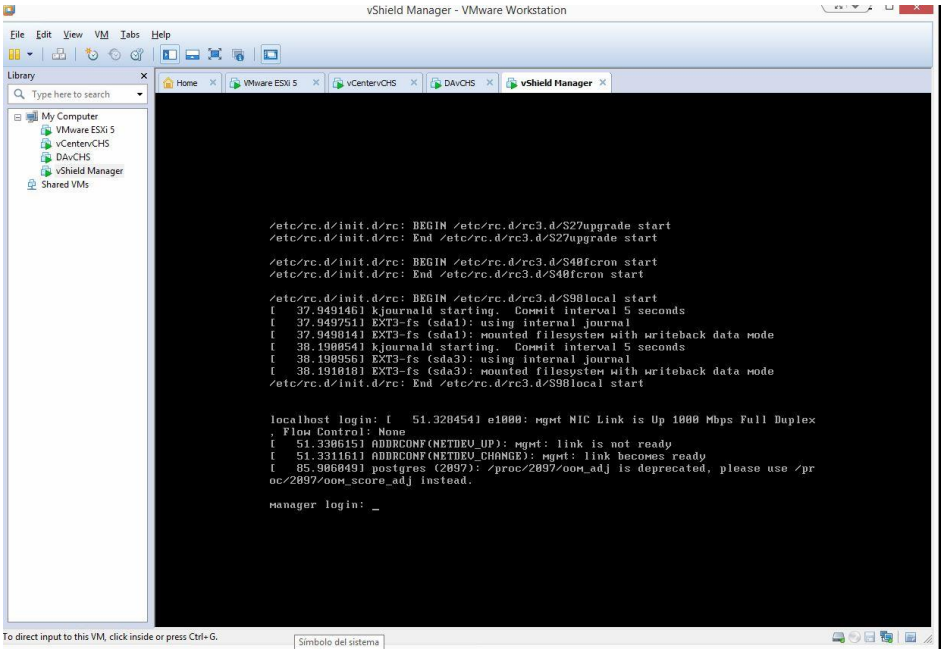

Ilustración 22: vShield Manager en tfmvcloud.com

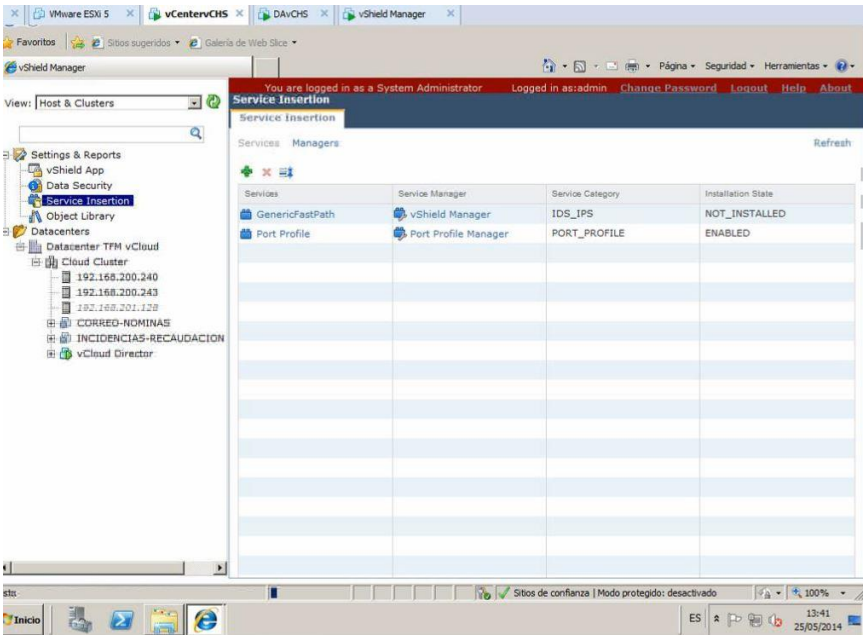

Ilustración 23: Consola http de vShield Manager

Para facilitar la comprensión de lo que se intenta construir he tomado prestado este gráfico extraído de la guía de vCloud Connector que nos muestra paso a paso el flujo de comunicaciones entre las diferentes componentes: (4) (3)

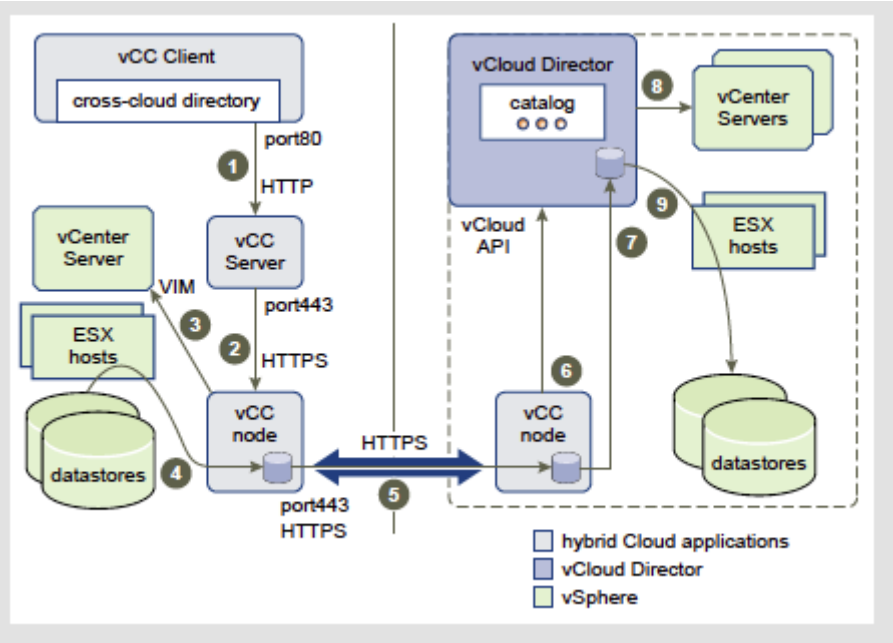

Ilustración 24: Flujo de comunicaciones en la Nube vCloud

Leyenda:

1. *Transferencia de peticiones de los clientes utilizando la vCloud Connector IU.*
2. *vCloud Connector Server le comunica a vCloud Connector Node que transfiera la vApp.*
3. *vClod Connector Node le comunica a vCenter Server que "exporte el contenido" usando la API de VIM.*
4. *El contenido se traslada desde los almacenes de datos a la caché de vCloud Connector Node.*
5. *El contenido se transfiere desde la fuente al nodo destino mediante checkpoint-restart*[2]
6. *vCloud Connector Node en el destino llama a la API vCloud Director "importar".*
7. *Se realiza la transferencia del contenido desde la caché del vCloud Connector Node de destino al vCloud Director.*
8. *vCloud Director envía el comando para la importación al vCenter apropiado.*
9. *Se transfiere el contenido del vCloud Director a la red del almacén de datos de destino y se pone a disposición a través del catálogo de vCloud Director.*

Las tareas restantes para conseguir configurar la Nube Pública son las siguientes: Agregar el vCenter, crear un Virtual DataCenter (VDC), crear las redes externas y el pool de redes, crear las organizaciones y usuarios. Por último crear los VDC de la organización (por ejemplo por departamentos o aplicaciones) y crear los catálogos para desplegar vApps (máquina virtual o conjunto de máquinas virtuales empaquetadas). (13)

4.3.2.1 Agregar el Servidor vCenter

El servidor VCENTER del domino tfmvcloud.com proporciona los recursos de procesamiento, almacenamiento y red para la nube. VMware vCloud Director puede usar uno o más servidores vCenter

[2] [2] *Checkpoint restart permite reiniciar las comunicaciones que fueron interrumpidas. Las comunicaciones empiezan en el punto donde fueron interrumpida en lugar de empezar desde el principio de nuevo.*

para crear una nube, en una nube a escala muy grande puede soportar hasta 25 servidores vCenter controlados simultáneamente.

Para agregar un servidor vCenter debemos acceder a la consola web del servidor vCD, y seleccionar "*Adjuntar un vCenter*".

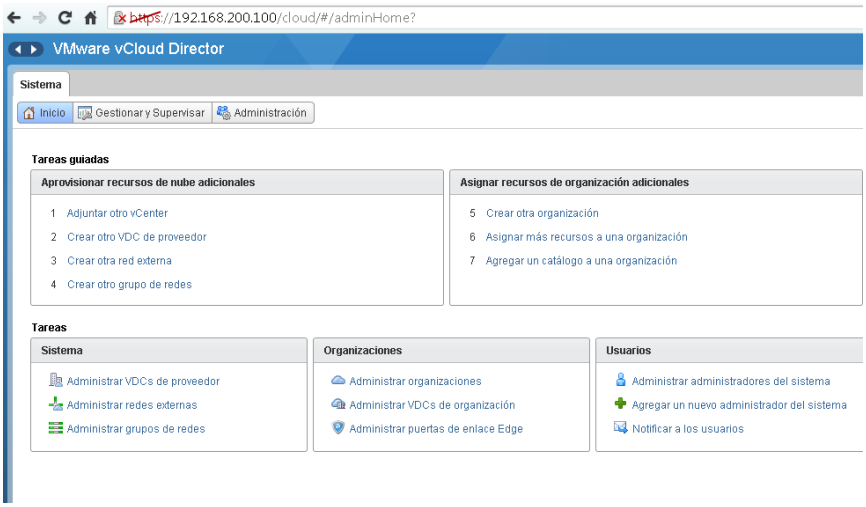

Ilustración 25: Agregando un vCenter al vCD

4.3.2.2 Configurar un Virtual Datacenter (VDC) de Proveedor.

En un servicio de la nube dedicado, hay que crear un centro de datos virtual para poder utilizar la infraestructura de recursos. Se puede agrupar los recursos en uno o más centros de datos virtuales, dependiendo de las necesidades. Por ejemplo, se puede crear un centro de datos virtual para la empresa o se pueden crear diferentes centros de datos virtuales para diferentes departamentos, equipos de proyecto o sitios geográficos. Cuando se crea un centro de datos virtual, hay que configurar la computación, almacenamiento y recursos de red. Si se asignan una o más direcciones IP públicas para el centro de datos virtual, se crea una red adicional que puede proporcionar acceso a Internet a las máquinas virtuales conectadas a ella.

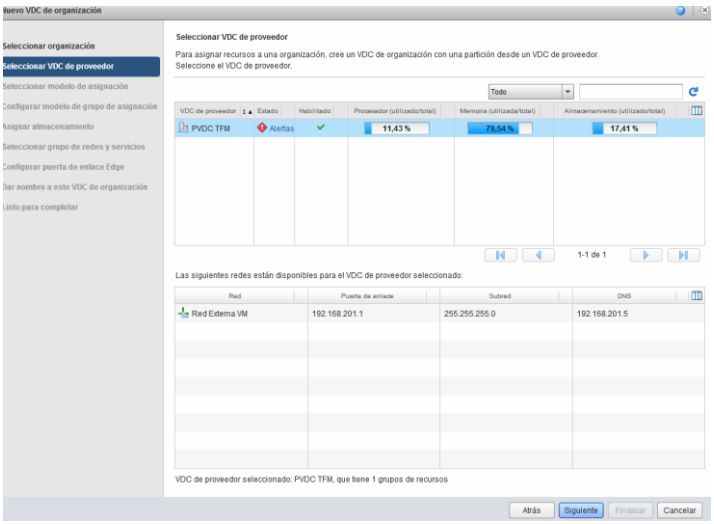

Ilustración 26: Configurar un VDC de proveedor

4.3.2.3 Crear Redes Externas

Las redes externas se utilizan en VMware vCloud Director para dar conectividad externa a vApps. Las vApps residen en Organizaciones (que se presentarán más adelante), por lo que en cierto sentido, estas redes son "externas" a la Organización.
Una red externa es un grupo de puertos (portgroup) en vSphere que lleva el tráfico de máquina virtual externa. Este grupo de puertos puede estar asociado a una VLAN para asegurar el aislamiento de la red.
En nuestro laboratorio hemos creado una red externa con el mismo rango de IP del dominio tfmvcloud.com, 192.168.201.50-80 ya que no se dispone de IP públicas para esta prueba.

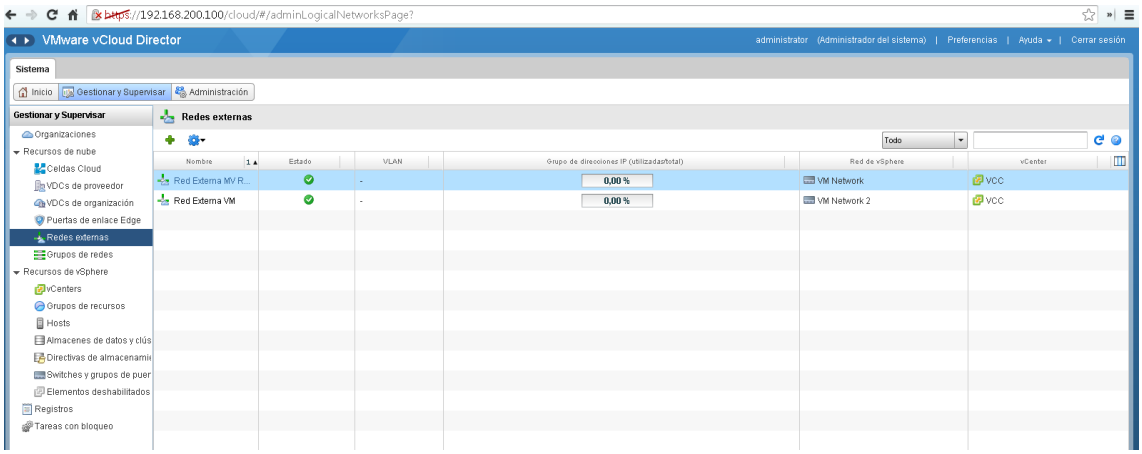

Ilustración 27: Crear Redes Externas

4.3.2.4 Crear un Pool de Redes

Los Pools de redes son redes de nivel 2 aisladas que proporcionan los componentes básicos necesarios para crear redes de organización y de vApp. Son el factor clave para el auto-aprovisionamiento de las redes en la nube. Las redes de organización se utilizan para dar conectividad a vApps dentro de una organización mientras que las redes de vApp se utilizan para dar conectividad a las máquinas virtuales dentro de una vApp.

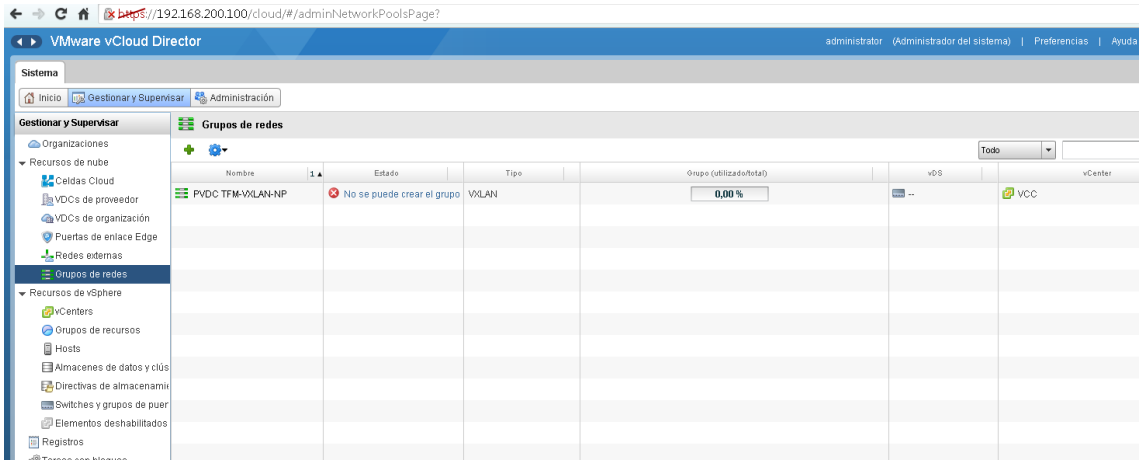

Ilustración 28: Crear un pool de redes

4.3.2.5 Crear Organizaciones y Usuarios

VMware vCloud Director permite crear organizaciones para separar grupos de usuarios entre sí y aplicar diferentes políticas de control por ejemplo, se pueden crear organizaciones separadas para el departamento de financiero, para el de recursos humanos, y otro para el del informática por ejemplo. Cada organización puede contener diferentes grupos de usuarios, y tiene su propio conjunto de recursos y políticas.

VMware vCloud Director crea una URL distinta para cada organización en la que los usuarios de esa Organización inician sesión. Dentro de las organizaciones, se pueden crear usuarios y grupos. En este laboratorio la URL de la organización creada tiene la forma https://192.168.200.100/cloud/org/RRHH .

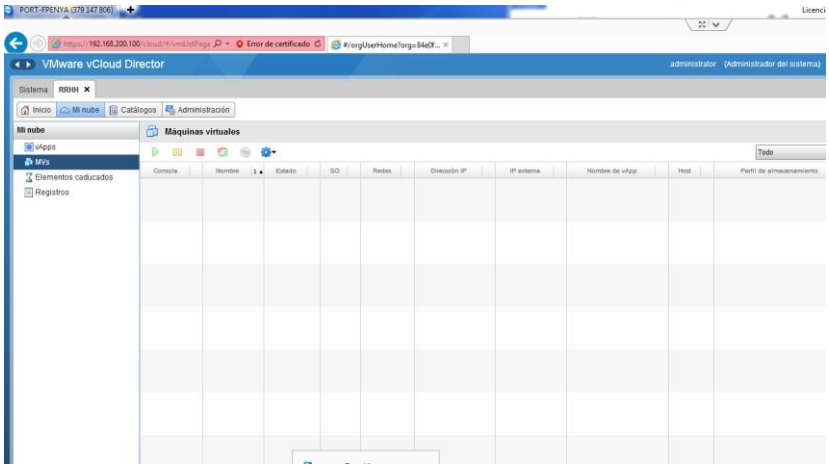

Ilustración 29: Crear una organización

4.3.2.6 Crear VDC de Organizaciones.

Se crean Virtual Datacenter (VDC) de Organizaciones para que las organizaciones puedan utilizar los recursos de los Proveedores de VDC. Una VDC de Organización es un contenedor de recursos que contiene los recursos informáticos y de almacenamiento, un SLA y el coste específico asociado, dependiendo del proveedor de VDC a partir del cual se crea.

Una VDC de Organización puede llegar a ser tan grande como el tamaño del VDC del Proveedor. Una organización puede utilizar los recursos a través de múltiples VDC de Organización creados a partir de múltiples VDC de Proveedor.

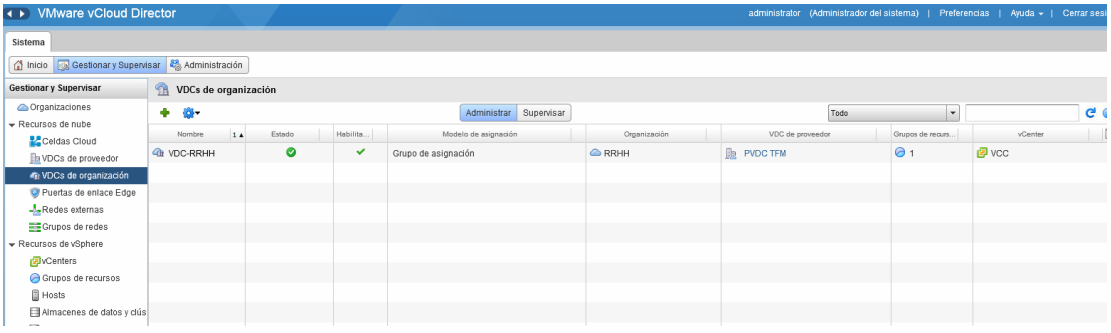

Ilustración 30: Crear VDC de organizaciones

4.3.2.7 Crear Catálogos

Los Catálogos se utilizan para ofrecer vApps y medios de instalación (ISO, disquetes) a los usuarios finales para autoservicio. El departamento de informática puede construir entornos de máquinas y aplicaciones virtuales mediante la creación de las mismas y subirlas al catálogo.

Los Catálogos son creados por los administradores de organización o autores catálogo, y pueden ser compartidos o publicados. Cuando un catálogo es compartido puede ser configurado para ser accesible por uno o más miembros de una organización. Cuando un Catálogo se publica, se puede acceder desde otras organizaciones en la nube privada. Se pueden crear vApps en los Catálogos Organización utilizando tres maneras:

1. Copiando máquinas virtuales y plantillas desde vSphere. Un administrador de la nube puede copiar máquinas virtuales y las plantillas desde la infraestructura vSphere subyacente.

2. Copia vApp desde un disco local. Un administrador Organización puede copiar una vApp en formato OVF desde un disco local a la nube privada.

3. Crear vApps desde cero en la nube privada, es decir, crear máquinas virtuales, instalar el Sistema operativo invitado (SMO) y la aplicación. Esto se puede hacer por un administrador Organización, Catálogo de autor, o autor de vApp. Sólo los administradores de la organización y los autores catálogo pueden agregar elementos al Catálogo.

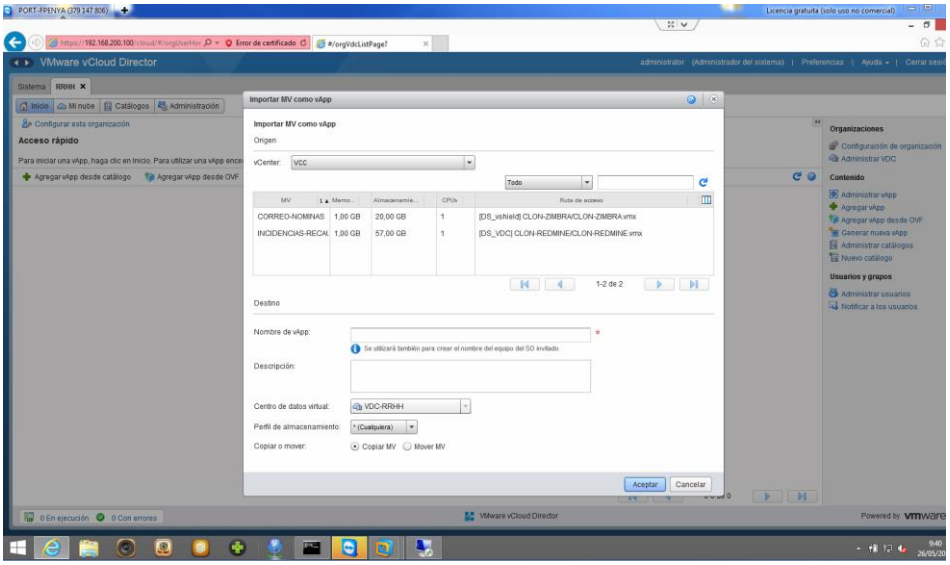

Ilustración 31: Importar MV al vApp

4.3.3 Configuración de la Nube Híbrida.

vCloud Connector proporciona una única interfaz de usuario para supervisar múltiples nubes públicas y privadas y para la transferencia de contenidos de una nube a otra. Permite conectar múltiples nubes, tanto internas como externas, en una única interfaz de usuario. También con vCloud Connector se puede administrar las máquinas virtuales, implementar plantillas, y transferir máquinas virtuales, vApps y plantillas de una nube a otra.

vCloud conector también proporciona las siguientes características clave:

- Content Sync que permite configurar una biblioteca de contenido para distribuir y sincronizar las plantillas a través de las nubes.
- Datacenter Extension que permite extender el centro de datos privado a un vCloud público.
- Offline Data Transfer que permite transferir grandes cantidades de datos desde el centro de datos privado a un Servicio Nube Híbrida (Hybrid vCloud).

vCloud Connector consta de tres componentes distintos: la interfaz de usuario, el software servidor y el software de los nodos como se pueden apreciar en el siguiente gráfico:

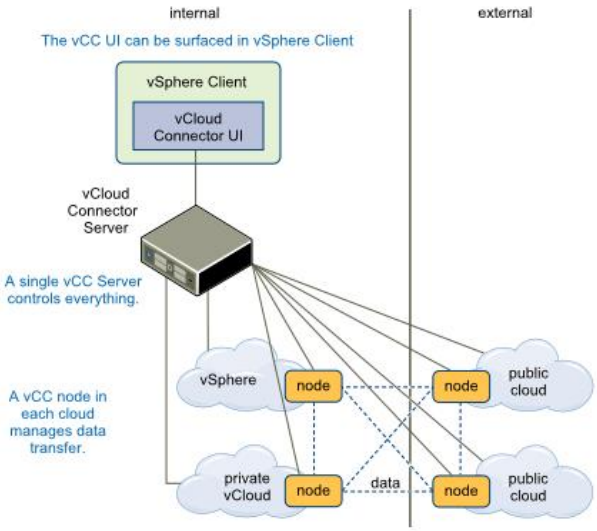

Ilustración 32: Componentes de vCloud Connector

vCloud Connector UI

Es la interfaz de usuario del software vCloud Connector Server. Se registra y se accede desde el cliente vSphere. Durante el proceso de configuración, se decide dónde registrar esta interfaz de usuario.

vCloud Connector Server

Es una aplicación virtual que coordina la actividad de vCloud Connector, controla los nodos vCloud Connector, y produce la interfaz de usuario vCloud Connector. Sólo necesita un servidor de vCloud Connector.

vCloud Connector Node

Son dispositivos virtuales que manejan la transferencia de contenido de una nube a otra. Un nodo vCloud Connector debe estar instalado en cada vSphere o nube basada en vCloud Director que supervisa vCloud Connector.

4.3.3.1 Parte Pública

En las nubes públicas basadas en vCloud Director, el proveedor de servicio puede instalar un nodo de vCloud Connector como un nodo multiusuario para múltiples clientes a utilizar para que cada cliente no tenga que instalar un nodo. Esta configuración también puede ser utilizada por los administradores

privados de vCloud Director que tienen múltiples organizaciones. En el Servicio híbrido vCloud, un nodo multiusuario vCloud Connector se instala por VMware por defecto.[3]

Tanto el Servidor vCloud Connector como el Nodo vCloud Connector están empaquetados como dispositivos virtuales (appliances). El servidor sólo se puede instalar en una Nube vSphere o en una Nube vCloud Director. (6) En la siguiente figura se puede observar la MV vCloud Connector desplegada desde el vSphere Web Client en la red VCLOUDTFM:

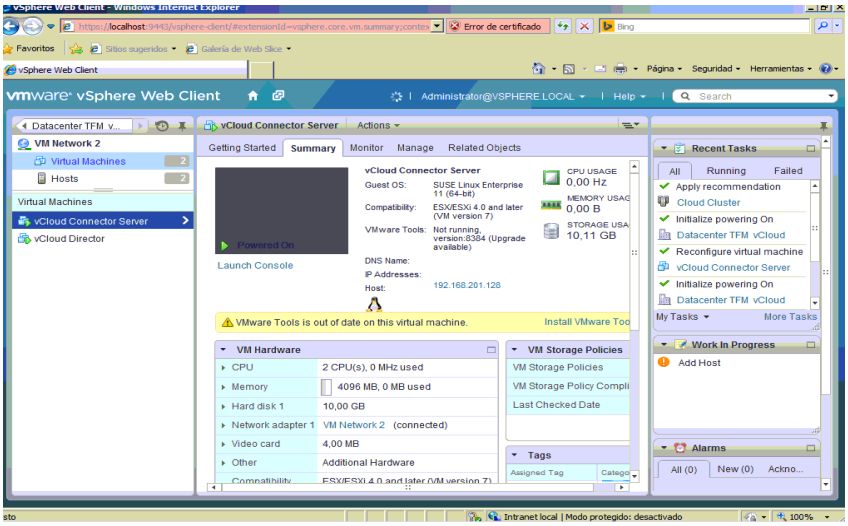

Ilustración 33: Appliance vCloud Connector Server

Todas las comunicaciones con el servidor de vCloud Conector se realizan con SSL y utilizan un certificado autofirmado (que se puede reemplazar con otro de plena confianza). Todas las comunicaciones con los nodos vCC son por defecto con SSL. Para registrar un nodo con un proveedor de servicios se utiliza la dirección URL del nodo de la forma https://vccnode.cloud.com. Una vez desplegada el appliance del vCloud Connector Server podemos enlazarlo tanto con un vSphere como con un vCloud Director.

En este laboratorio usaremos el vCloud Connector Server para enlazarlo con el vCloud Director del dominio en la nube tfmvcloud.com por lo que tendremos que registrarlo desde la interfaz Web.

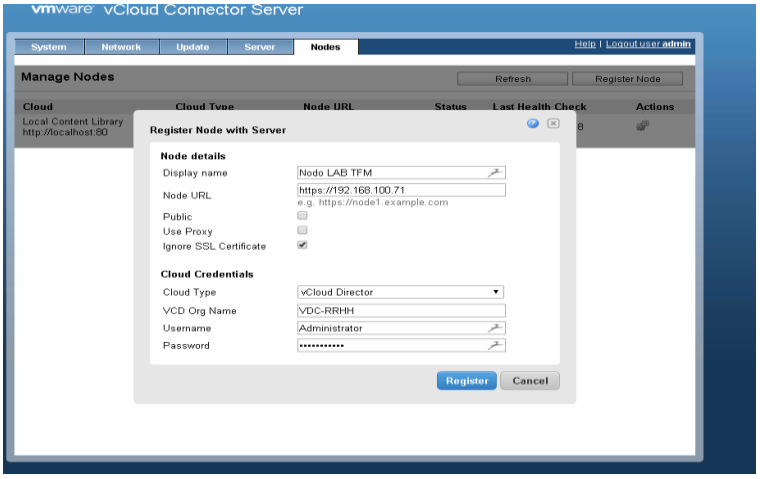

Ilustración 34: Registro de vCloud Connector Server en vCloud Director

[3] *En nubes vCloud Director, no es necesario instalar un nodo para cada organización. Los nodos vCloud Connector son multiusuario, es decir, un nodo puede ser utilizado por múltiples organizaciones para transferir contenido hacia y desde la nube. Se puede optar por instalar un nodo en la nube para que múltiples organizaciones la utilicen. Para agregar un instancia de servicio híbrido a la vCloud Connector IU, no es necesario instalar un nodo en el servicio Híbrido vCloud, sino utilizar el nodo multiusuario anterior que se instala por defecto con VMware.*

4.3.3.2 Parte Privada

Para la parte de la nube privada tenemos dos opciones, o bien desplegar un vCloud Connector Node o bien utilizar el plugin de vCloud Hybrid Services. El problema es que si utilizamos el plugin tenemos que descargar el certificado desde la página https://vchs.vmware.com a la cual se accede con un usuario/password. Para poder iniciar sesión se tiene que comprar la aplicación a Vmware por lo que sólo está disponible para producción y no podemos descargarlo para nuestro laboratorio. Por ese motivo en este laboratorio para poder simular la conexión con la Nube vCloud Director se ha utilizado el vCloud Connector Node.

Una vez desplegado en nuestra LAN privada el appliance virtual vCloud Connector Node, el siguiente paso sería registrarlo en la nube, que es el del tipo vCloud Director. Realmente lo importante no es dónde se ejecutará el vCloud Connector Node sino el tipo de nube y la URL. Incluso se puede registrar con un vSphere en su lugar (vSphere funciona como una nube en si misma).

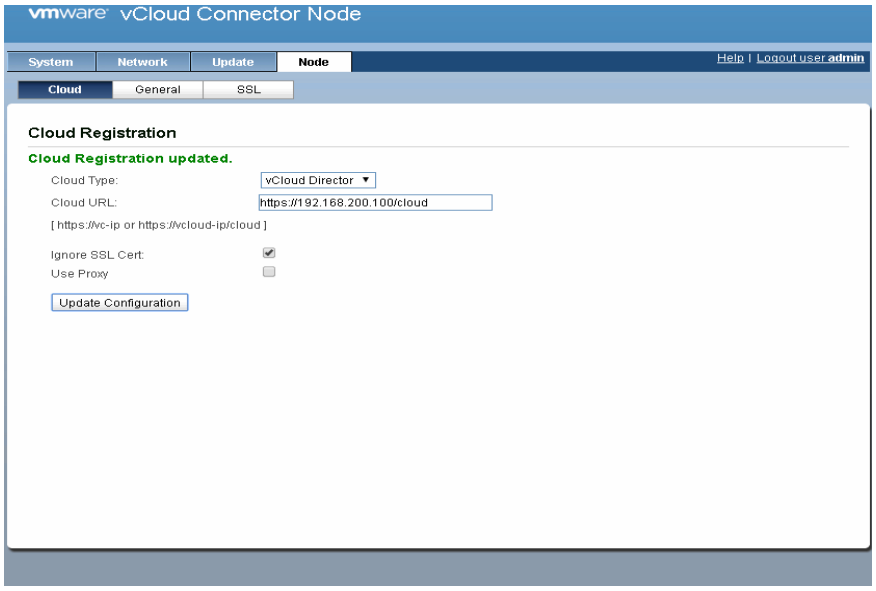

Ilustración 35: Registro de vCloud Connector Node en vCloud Director

Una vez el vCloud Connector Node se haya registrado con el tipo de nube, se puede configurar el vCloud Conector Server para que acceda al nodo. Para ello tenemos que registrar el vCloud Connector Node con el vCloud Connector Server.

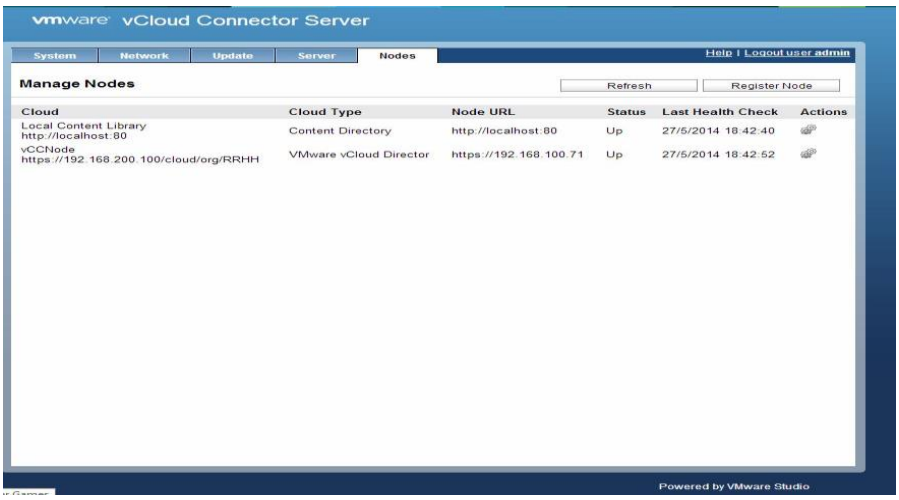

Ilustración 36: Registro de vCloud Connector Node en vCloud Connector Server

Asimismo el vCloud Connector Server se puede registrar a si mismo con el vCenter de la nube tfmvcloud.com para permitir acceder a los recursos de la Nube. (7)

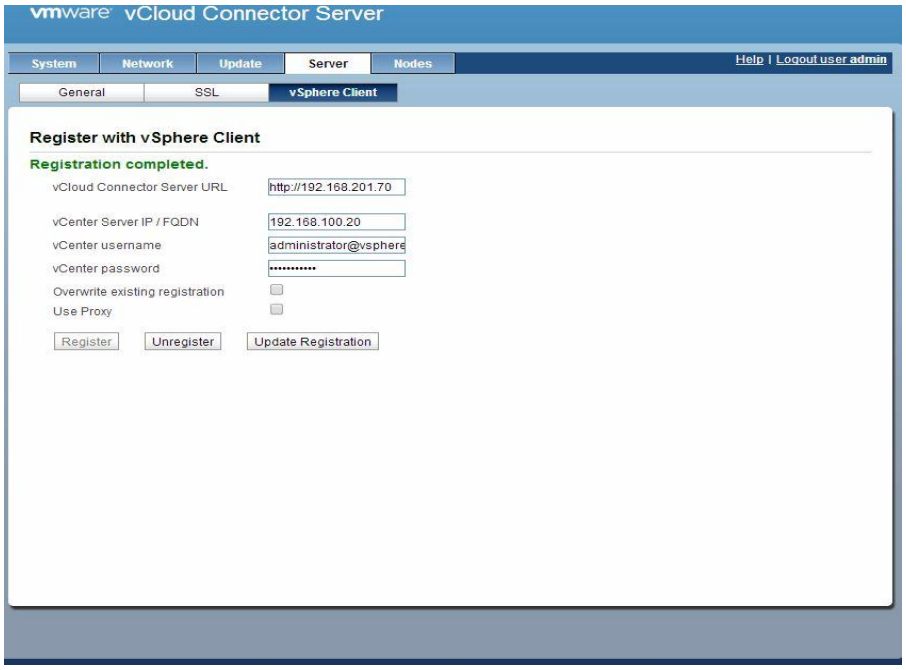

Ilustración 37: Registro de vCloud Connector Server en vCenter de tfm-ecomercio.com

Este proceso de registro añade además un icono vCloud Director en el vSphere Client, que no es más que un puntero a la página web del vCloud Director donde definimos nuestra VDC de organización: https://192.168.200.100/cloud/org/RRHH

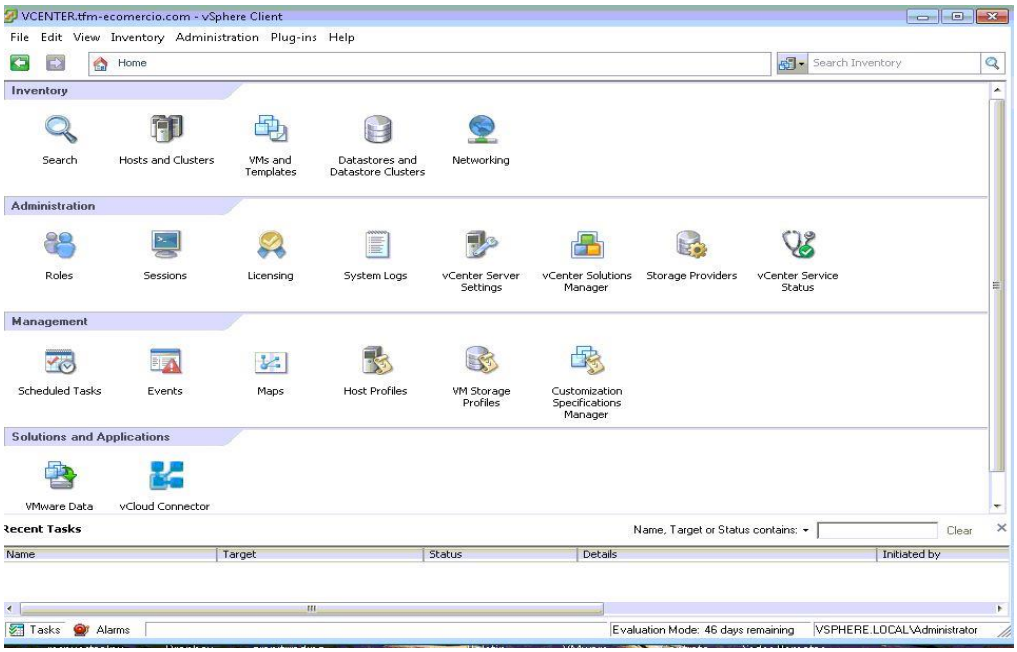

Ilustración 38: Plugin en vSphere Client después del registro

Podemos acceder desde este puntero del vSphere Client al vCloud Connector Node y desde allí podemos añadir Proveedores de Nubes. (4)

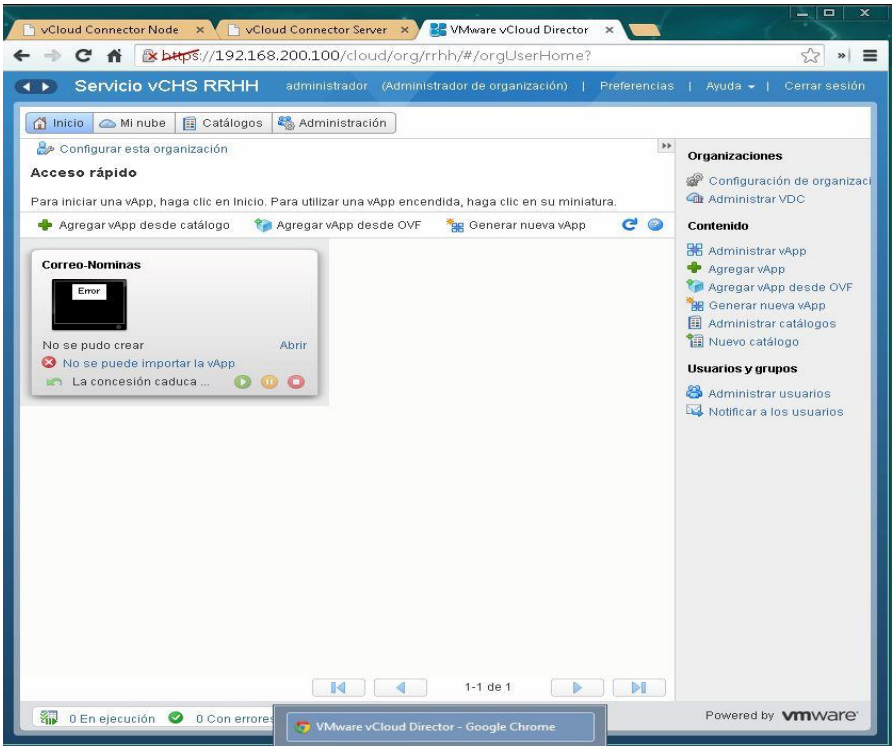

Ilustración 39: Mi Organización "Servicio vCHS RRHH"

Una vez añadida, desde aquí podemos ver la Nube Privada, la Organización y los Virtual Datacenters.

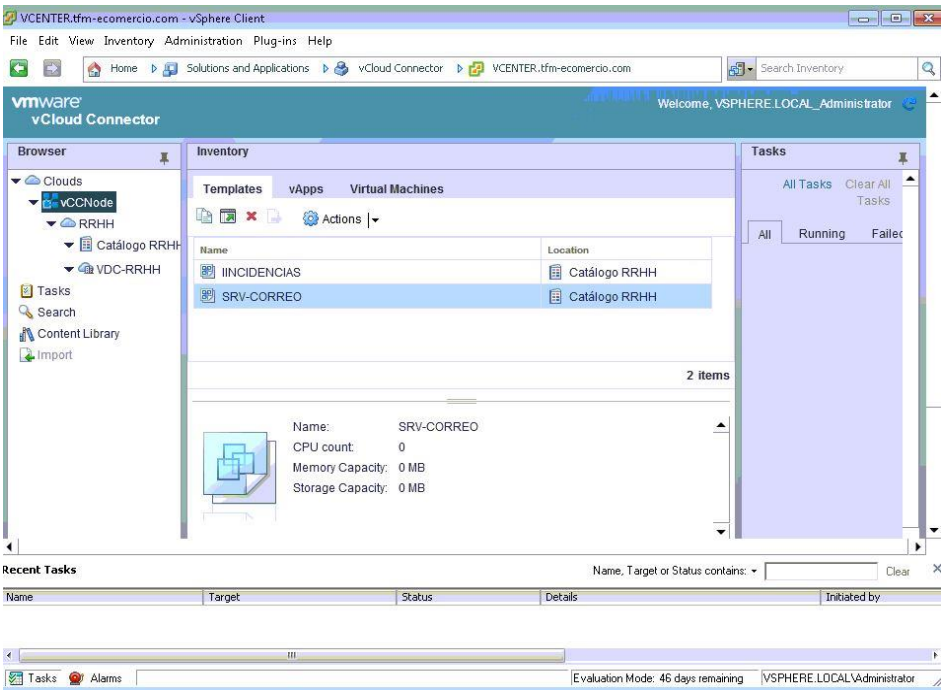

Ilustración 40: MV accedidas a través del plugin vCN

Una vez configurado, un usuario vSphere puede examinar el Catálogo de vCloud Director y desplegar una vApp desde allí, o bien copiarla y desplegarla una vez haya sido subido. También está la opción de borrar la plantilla del catálogo vCD.

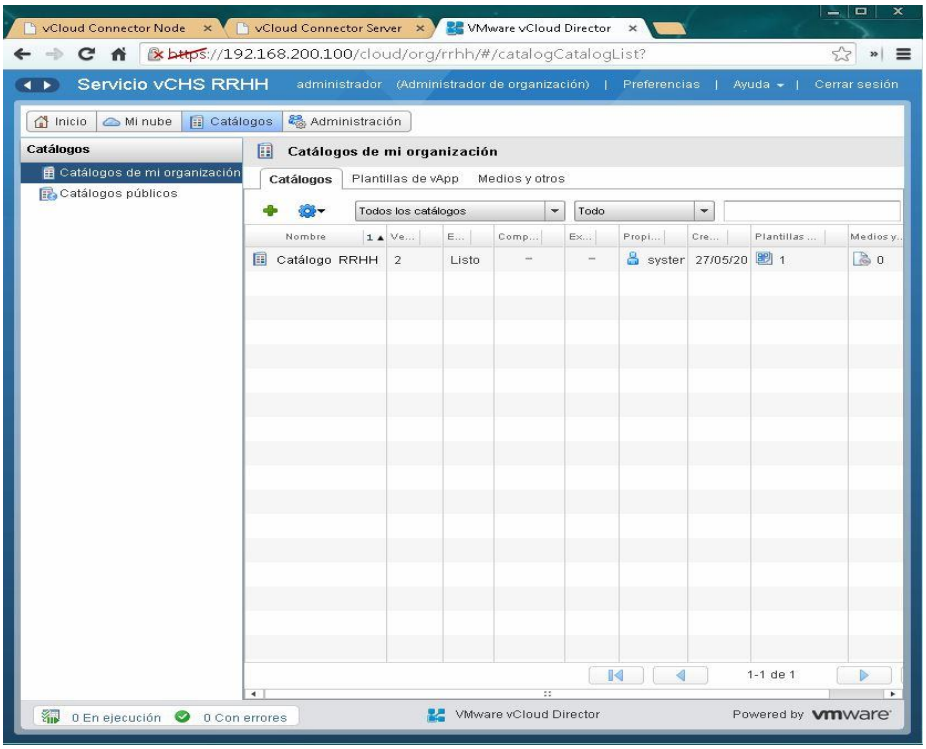

Ilustración 41: Catálogos creados de prueba

Ejemplo subiendo una Plantilla de vApp:

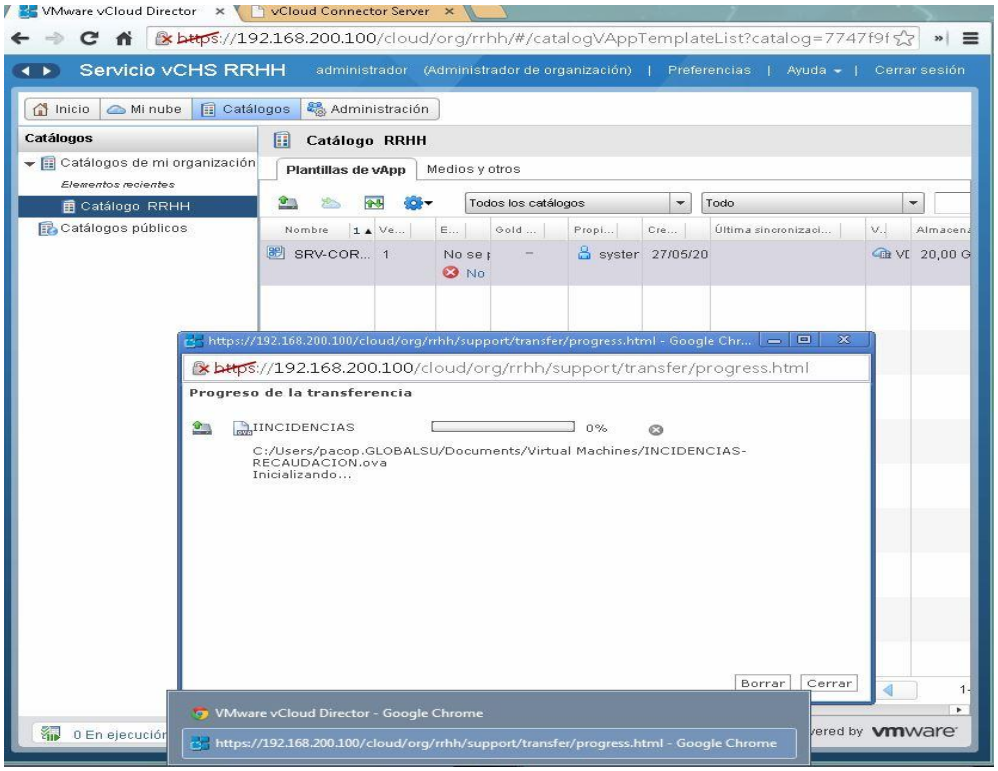

Ilustración 42: Transferencia de una plantilla desde el vCloud Connector Node

4.3.4 Conclusiones de la instalación

Configurar e instalar vCloud Hybrid Services no es una tarea sencilla, incluso para que aquellas personas familiarizadas con el entorno de virtualización VMware vSphere. También evaluar el producto vCloud Director en un entorno de laboratorio es posible como ha quedado demostrado pero exige tener gran cantidad de recursos, sobre todo de memoria RAM, si se desea probar los servicios más importantes de vCHS razonablemente.

La transición de una Nube Privada a una Nube Pública o Híbrida dependerá de muchos factores y tanto AWS como VMware ofrecen grandes soluciones en sus respectivos ecosistemas. AWS sigue siendo el líder en el mercado de computación en la nube pero desde hace poco tiempo Dell-VMware ha aparecido para hacerle competencia y en un futuro inmediato, en mi modesta opinión, se hablará bastante de los servicios que ofrece VMware en la nube.

Aquí expondremos algunos de los razonamientos que pueden decantar la balanza por el lado de VMware en lugar de AWS: (12)

Redundancia a nivel de Máquina Virtual

VCHS incluye de forma *gratuita* y sin configuración la capacidad redundante hot standby para maximizar el tiempo de actividad de la aplicación. De forma que si hay una caída de servicio, inmediatamente reinicia todas las máquinas virtuales afectadas en el mismo clúster VCHS.

Por el contrario, AWS no ofrece ninguna capacidad redundante, sin control automático, y ningún reinicio rápido de las máquinas virtuales. Para la redundancia se tiene que comprar instancias adicionales y comprar y administrar un equilibrador de carga (suponiendo que el tráfico de aplicación se pueda equilibrar).

Gestión proactiva *gratuita* del rendimiento automático gratuito

La misma tecnología de VMware que vela por fallo del servidor en vCHS también supervisa el rendimiento general y la salud de los servidores. Si un servidor concreto está sobrecargado, vCHS migra automáticamente en vivo las máquinas virtuales a un servidor del clúster con más capacidad. No hay tiempo de inactividad y no "pausa" la aplicación.

Los usuarios de AWS deben diseñar estratégicas para que el rendimiento de sus instancias y seguirlas de cerca durante su ciclo de vida o puede que sus servicios no funcionen bien.

Servicio sin interrupciones

Cuando AWS tiene que hacer el mantenimiento preventivo en un servidor (por ejemplo, aplicar un parche de seguridad al hipervisor), la instancia tiene que pararse.

vCHS usa la migración en vivo para mover máquinas virtuales a un servidor con capacidad del servidor redundante, a continuación, se realiza el mantenimiento en el servidor afectado. Las aplicaciones no se detienen porque VMware tenga que realizar este mantenimiento del servidor.

Crear una máquina virtual de cualquier tamaño

Con vCHS, se puede elegir las dimensiones de la máquina virtual que se desee hasta los máximos de CPU, memoria y disco físicos. Todas las máquinas virtuales se ejecutan en los servidores físicos con conectividad agregada 20Gbps, a diferencia de los servidores de AWS con sólo 100Mbps o tarjetas de red de 1 Gbps.

En AWS, hay que decidir en un árbol de hasta 29 opciones de instancia para elegir acertadamente porque no se puede cambiar más adelante. Si te equivocas, habrá que escoger una nueva instancia y averiguar si se puede ejecutar lo que queremos en ella.

Cambiar el tamaño de una máquina virtual o un disco mientras se está ejecutando

En vCHS se puede agregar CPU virtual, memoria y espacio en disco para cualquier máquina virtual en ejecución. Soporte del sistema operativo para la adición de CPU, memoria y disco está presente en las distribuciones de Linux y se incluye en las versiones de Windows desde el año 2008.

Las instancias de AWS no se puede ampliar, y la garantía de que pueden escalar efectivamente requiere una planificación cuidadosa (escoger correctamente el tipo de instancia y un tamaño de disco fijo) y escribir código para hacer el intercambio de estado (añadiendo instancias paralelas).

Rendimiento superior de disco sin tener que pagar por aprovisionamiento de IOPs

El disco estándar en vCHS es una mezcla de los SSD (flash) y discos de gama alta de empresa. En cambio, en AWS se puede comprar muy caro almacenamiento SSD o conformarse con el servicio EBS de AWS que está basado en discos SATA de bajo rendimiento.

Importar Máquinas Virtuales sin necesidad de conversión y con el pleno apoyo del proveedor de aplicaciones

En vCHS se puede ejecutar cualquier VM que se ejecute en vSphere, Workstation o fusión sin ninguna conversión en un formato propietario - y es apoyado por el proveedor de software para su aplicación. También se puede transferir y ejecutar prácticamente cualquier máquina física x86 que ejecute cualquier sistema operativo de DOS en adelante, sin tener que cambiar a un kernel especial o volver a la plataforma.

Con AWS, hay que convertir la máquina virtual y luego convertirlo de nuevo si desea exportar la máquina virtual. Si una máquina virtual es dependiente de cualquiera de los servicios de AWS, no se puede ejecutar en el centro de datos de la empresa más adelante, ya que no existen y utilizan APIs propietarias.

Utilizar las herramientas de gestión que ya se usan en la empresa

Puede administrar vCHS desde el cliente vSphere (web o Windows), vCloud Automation Center (vCAC) y vCenter Operations (vCOps). ***Esto es una gran ventaja para las empresas, ya que significa que se puede gestionar la infraestructura de nube con un enfoque de "arréglelo usted mismo", junto al rendimiento y la disponibilidad que es radicalmente diferente al enfoque de AWS y su modo de operación.***

Finalmente la conclusión extraída de esta evaluación es que el producto de VMware vCloud Director cumple todos los requerimientos definidos para una migración de máquinas virtuales de la empresa pero sobre todo es altamente recomendable para aquellas empresas que ya dispongan del entorno de virtualización vSphere en su infraestructura.

Por supuesto, no es necesario instalar todas estas máquinas para obtener servicios de nube híbrida de VMware, si acaso un vCloud Connector Node únicamente en las instalaciones de la empresa.

5 CONCLUSIONES DEL ESTUDIO

Las pruebas realizadas en este laboratorio para el estudio de la migración a un servicio de nube híbrida han proporcionado una visión general y positiva sobre las características del servicio de nube híbrida VMware. Sobre todo el hecho de se pueda gestionar dentro del entorno de virtualización VMware ya existente, proporciona muchas ventajas adicionales.

El hecho de tener las máquinas en este servicio hace posible que puede usarse la misma política de copias de seguridad ya existente en la empresa o aún mejor, realizar las copias en un recurso de almacenamiento en la nube y no hacerlo en el almacenamiento local del centro de datos de la empresa (parte privada).

Por otro lado, se pueden dar de alta usuarios para que accedan a los servicios en la nube, asignándole roles diferentes según sus necesidades. También es posible añadir usuarios ya existentes en el directorio activo de la parte privada, y asignarle después estos roles. Esto es una ventaja ya que simplifica la gestión de los usuarios.

Todos los accesos se realizan de forma segura utilizando SSL. Si contratamos el servicio de nube híbrida de VMware, además nos proporcionar un certificado privado que debemos instalar en nuestro navegador para usar el plugin de vCloud Hybrid Services.

Por el contrario, en cuanto a la seguridad de los datos, existen unos riesgos específicos en la computación en la nube en general. Estos riesgos son la falta de transparencia del proveedor y la falta de control del responsable de los datos, por ejemplo ante las dificultades para conocer en todo momento la ubicación de los datos.

Si existe falta de transparencia por parte del proveedor, porque no da una información clara, precisa y completa sobre todos los elementos inherentes a la prestación, la empresa sólo puede optar por finalizar su contrato sino quiere asumir este riesgo.

Por otro lado, El modelo de *cloud computing* hace posible que tanto los proveedores de servicios como los datos almacenados en la *nube* se encuentren ubicados en cualquier punto del planeta. Pero en todo caso la empresa que contrata estos servicios sigue siendo responsable del tratamiento de los datos. Además la aplicación de la legislación española no puede modificarse aunque los datos personales estén localizados en otros países. (14)

Los países del Espacio Económico Europeo ofrecen garantías suficientes pero si los datos están localizados en países que no pertenecen a ese espacio, dependiendo del país en que se encuentren, éstos deberán proporcionar garantías jurídicas adecuadas. Se considera una garantía adecuada que el país de destino ofrezca un nivel de protección equivalente al del Espacio Económico Europeo y así se haya acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea. También las proporcionadas por empresas ubicadas en los Estados Unidos que hayan suscrito los principios de Puerto Seguro.

En otro caso, la transferencia internacional de datos necesitará autorización del Director de la Agencia Española de Protección de Datos, que podrá otorgarse en caso de que el exportador de datos aporte garantías adecuadas.

Como se pudo ver en el vídeo presentado el proveedor del servicio puede acceder como Administrador de vCloud Director, a la nube de la organización por lo que para garantizar la confidencialidad de los datos, el proveedor del servicio debe comprometerse a garantizar la confidencialidad utilizando los datos sólo para los servicios contratados. Así mismo debe comprometerse a dar instrucciones al personal que depende de él para que mantenga la confidencialidad.

Sólo el personal del proveedor y aquellos usuarios que creemos en el servicio de Nube Híbrido de la organización creado en laboratorio tiene acceso a las máquinas virtuales pero no tienen acceso a los sistemas operativos ni aplicativos de las mismas. Por esta razón, podemos concluir que se conserva el nivel de privacidad de la información de la empresa.

Finalmente resaltar que la computación en la Nube Híbrida ofrece lo mejor de los dos mundos, por un lado la escalabilidad infinita de recursos de la nube y por otro, la gestión transparente y segura para los usuarios de la red privada.

Bibliografía

1, T. (s.f.). *Taneja Group.* Recuperado el 10 de 2013, de www.tanejagroup.com

2, O. (s.f.). Obtenido de http://docs.openstack.org/grizzly/openstack-image/content/ch_creating_images_manually.html

3, V. (s.f.). *VMware.* Obtenido de http://www.vmware.com/

4, A. (s.f.). Obtenido de http://www.vdicloud.nl/2011/03/18/part-1-setting-up-a-vmware-vcloud-home-lab/

5, B. (s.f.). Obtenido de http://www.vmwarebits.com/install-vshield-manager

6, C. K. (s.f.). Obtenido de http://kendrickcoleman.com/index.php/Tech-Blog/how-to-install-vcloud-director-15-from-beginning-to-end.html

7, C. C. (s.f.). Obtenido de http://www.chriscolotti.us/vmware/vcloud-hybrid-service-tutorials/

8, c. (s.f.). *http://www.colt.net/*. Obtenido de http://www.colt.net/cdnucm/groups/public/@cdn/@public/documents/generalcontent/colt_ceano_infraestructura.pdf

9, S. F. (s.f.). Recuperado el Mayo de 2014, de http://www.scoop.it/t/home-computing-labs

10, E. D. (s.f.). Obtenido de http://www.yellow-bricks.com/2010/09/13/creating-a-vcd-lab-on-your-maclaptop/

11, L. V. (s.f.). Obtenido de http://www.vmwarelearning.com/Q7ib/features-of-the-vcloud-hybrid-service-vchs-gateway/

12, L. M. (s.f.). Obtenido de http://blogs.vmware.com/vcloud/2014/03/vcloud-hybrid-service-different-10-cloud-capabilities-vcloud-hybrid-service-dont-exist-aws.html

13, V. (s.f.). Obtenido de https://www.vmware.com/products/vcloud-hybrid-service/resources.html

14, A. (s.f.). Obtenido de http://www.agpd.es

15, A. A. (s.f.). *Amazon AWS*. Recuperado el Mayo de 2014