



VIRTUALIZAR UN PUESTO DE USUARIO

Nombre Estudiante: Santiago Cebrián García

Plan de Estudios del Estudiante: Máster Universitario en Ingeniería de Telecomunicación UOC-URL

Telemática

Nombre Consultor/a: Xavi Vilajosana Guillen

Nombre Profesor/a responsable de la asignatura: José López Vicario

Fecha Entrega: 23/05/2018



Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada [3.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

FICHA DEL TRABAJO FINAL

Título del trabajo:	<i>Virtualizar puesto de usuario</i>
Nombre del autor:	<i>Santiago Cebrián García</i>
Nombre del consultor/a:	<i>José López Vicario</i>
Nombre del PRA:	<i>Xavi Vilajosana Guillen</i>
Fecha de entrega (mm/aaaa):	18/04/2018
Titulación:	<i>Máster Universitario en Ingeniería de Telecomunicación UOC-URL</i>
Área del Trabajo Final:	<i>Telemática</i>
Idioma del trabajo:	<i>Castellano</i>
Palabras clave	<i>Virtualización</i>
<p>Resumen del Trabajo (máximo 250 palabras): <i>Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.</i></p>	
<p>El proyecto presenta un breve análisis entre distintas tecnologías de virtualización como son VMware, Microsoft, Citrix... Realiza una comparación entre ellas y se destaca los puntos fuertes y desventajas eligiendo Citrix, por características como:</p> <ul style="list-style-type: none"> • Facilidad de implantación • Estabilidad • Flexibilidad • Centralización <p>Por ello, se realiza una propuesta para virtualizar un puesto de trabajo usando Citrix como solución para una empresa que esté interesada en el proyecto. En los contenidos del proyecto, se detalla su arquitectura, diseño, objetivos, utilidad...La solución adoptada también tiene en cuenta la posibilidad de distintas sedes para la empresa.</p> <p>En este proyecto se pretende dar una idea general del funcionamiento de la virtualización para su utilización en el aprendizaje y el desarrollo de personas interesadas en este tema. Así, este proyecto podrá ser utilizado tanto de una forma teórica como practica en la introducción a la virtualización.</p> <p>En la actualidad, las empresas suelen tener distintas sedes repartidas por la geografía mundial. Por ello, surge la necesidad de centralizar los sistemas y dotar de una mayor versatilidad a los usuarios. Por ello, distintas empresas han sacado soluciones para virtualizar el puesto de un usuario, destacando algunas como Citrix, VMware, Microsoft, etc.</p>	

Abstract (in English, 250 words or less):

The project introduces a brief analysis between different virtualization technologies such as VMware, Microsoft, Citrix ... It makes a comparison between them and highlights the strengths and disadvantages by choosing Citrix, for characteristics such as:

- Facility of implementation
- Stability
- Flexibility
- Centralization

Therefore, a proposal is made to virtualize a job using Citrix as a solution for a company that is interested in the project. In the contents of the project, its architecture, design, objectives, utility are detailed ... The solution adopted also takes into account the possibility of different sites for the company.

This project aims to give a general idea of the operation of virtualization for its use in the learning and development of people interested in this topic. Thus, this project can be used both in a theoretical and practical way in the introduction to virtualization.

At present, companies usually have different offices spread across the world geography. Therefore, there is a need to centralize systems and provide greater versatility to users. Therefore, different companies have taken solutions to virtualize the position of a user, highlighting some as Citrix, VMware, Microsoft, etc.

Índice

1. Introducción.....	1
1.1 Contexto y justificación del Trabajo.....	1
1.2 Objetivos del Trabajo.....	1
1.3 Enfoque y método seguido.....	3
1.4 Planificación del Trabajo.....	3
1.5 Breve resumen de productos obtenidos.....	4
1.6 Breve descripción de los otros capítulos de la memoria.....	4
2. Conceptos teóricos.....	5
2.1 Comparación entre los distintos fabricantes.....	6
3. Elementos e introducción a Citrix.....	10
3.1 XenAPP y XenDesktop.....	10
3.2 VDI (Virtual Desktop Infrastructure).....	11
3.3 Arquitectura FMA (FlexCast Management Architecture).....	12
3.4 Protocolo ICA.....	13
3.5 Capas definidas.....	14
4. Diseño propuesto:.....	23
4.1 Esquema y diseño actual.....	23
4.2 Requisitos planteados.....	24
4.3 Diseño a realizar.....	25
4.4 Distribución y diseño capa cliente.....	26
4.5 Distribución y diseño capa acceso.....	26
4.6 Distribución y diseño Control layer.....	28
4.7 Distribución y diseño Resource layers.....	33
4.8 Distribución y diseño Hardware layer.....	35
5. Implementación.....	36
5.1 Implementación a realizar.....	36
5.2 Implementación del StoreFront y Netscaler Gateway.....	36
5.3 Implementación Delivery Controller.....	54
5.4 Configuraciones de Directorio Activo.....	62
5.5 WSUS y seguridad.....	65
5.6 Despliegue de equipos.....	66
5.7 Creación de catálogos.....	71
5.8 Asignación Delivery Groups.....	74
5.9 Pruebas y validaciones.....	74
5.10 Pruebas de funcionalidad.....	75
5.11 Pruebas de rendimiento y cuantitativas.....	77
5.12 Mejoras y escalabilidad.....	79
6. Presupuesto.....	80
6.1 Costes empleados.....	80
6.2 Costes licenciamiento.....	80
6.3 Costes totales.....	81
7. Conclusiones.....	82
8. Glosario.....	84
9. Bibliografía.....	85

Lista de figuras

- Figura 1.1 Diagrama de Grant
- Figura 3.1 Capas de la infraestructura
- Figura 3.2 Arquitectura FMA
- Figura 3.3 Conexiones ICA
- Figura 3.4 Modelo Encapsulado ICA
- Figura 3.5 Acceso al entorno
- Figura 3.6 Vista de usuario de un StoreFront
- Figura 3.7 Esquema Provision Services
- Figura 3.8 Proceso instalación y configuración MCS
- Figura 3.9 Resumen de layers del entorno
- Figura 4.1 Implantación StoreFront
- Figura 4.2 GPOs del Directorio Activo
- Figura 4.3 Configuración de bucle invertido
- Figura 5.1 Implantación de forma gráfica
- Figura 5.2 Diagrama implementación StoreFront
- Figura 5.3 Create RSA Key
- Figura 5.4 Complimentar Create RSA Key
- Figura 5.5 Complimentar CSR
- Figura 5.6 Datos a cumplimentar para certificado storefront
- Figura 5.7 Panel Netscaler SSL
- Figura 5.8 Certificados .txt instalados
- Figura 5.9 Panel de instalación certificado
- Figura 5.10 Datos a cumplimentar para instalar
- Figura 5.11 Datos a cumplimentar para instalar certificado
- Figura 5.12 Como linkar certificado con CA
- Figura 5.13 Configuración IIS
- Figura 5.14 Binding para insertar certificado
- Figura 5.15 Crear Store en consola StoreFront
- Figura 5.16 Nombre del Store a crear
- Figura 5.17 Añadir Delivery Controller
- Figura 5.18 Remote Access en conexión externa
- Figura 5.19 Añadir Netscaler Gateway

Figura 5.20 Secure Ticket Authority

Figura 5.21 Autenticación StoreFront

Figura 5.22 Método de autenticación

Figura 5.23 Como añadir dispositivos móviles

Figura 5.24 Stores configurados

Figura 5.25 Añadir servidores a Netscaler

Figura 5.26 Añadir Virtual Server StoreFront a Netscaler

Figura 5.27 Añadir Wildcard a Virtual Server

Figura 5.28 Añadir Política

Figura 5.29 Configuración política rewrite

Figura 5.30 Configuración Virtual Server DeliveryController

Figura 5.31 Configuración Virtual Server Access Gateway

Figura 5.32 Política de Autenticación

Figura 5.33 Política de sesión StoreFront Externo

Figura 5.34 Política de sesión Citrix Receiver

Figura 5.35 Configuración STA

Figura 5.36 Instalación Delivery Controller

Figura 5.37 Instalación SQL express

Figura 5.38 Puertos necesarios

Figura 5.39 Puertos necesarios Servidor de Licencias

Figura 5.40 Configuración Servidor de Licencias

Figura 5.41 Agregar fichero de licencias

Figura 5.42 Servicio Citrix Licensing

Figura 5.43 Citrix Studio Site Setup

Figura 5.44 Nombre de la granja

Figura 5.45 Configuración conexión servidor de licencias

Figura 5.46 Configuración conexión vcenter

Figura 5.47 Configuración Recursos

Figura 5.48 Configuración de servicios

Figura 5.49 Configuración del equipo GPO XenApp

Figura 5.50 Configuración del equipo GPO XenApp

Figura 5.51 Configuración del equipo GPO XenDesktop

Figura 5.52 Configuración del equipo GPO XenDesktop

Figura 5.53 Permisos Network/CTXProfile

Figura 5.54 Añadir plantilla .adm
Figura 5.55 Instalación Agente VDA
Figura 5.56 Instalación Agente VDA
Figura 5.57 Creación Imagen Maestra
Figura 5.58 Habilitar pvDisk
Figura 5.59 Puertos requeridos para plataforma VDI
Figura 5.60 Resumen instalación
Figura 5.61 Actualizar personal vDisk
Figura 5.62 Citrix Personal vDisk
Figura 5.63 Crear Catálogo de máquinas
Figura 5.64 Elección Windows Desktop OS
Figura 5.65 Citrix Machine Creation Services (MSC)
Figura 5.66 Master Imagen (snapshot)
Figura 5.67 Configuración Virtual Machine
Figura 5.68 Configuración Computer Accounts
Figura 5.69 Crear Delivery group
Figura 5.70 Pantalla bienvenida
Figura 5.71 Escritorio inicial

Lista de Tablas

Tabla 1.1 Planificación

Tabla 2.1 Comparativa entre fabricantes

Tabla 2.2 Comparación Integración uniforme con clientes pesados

Tabla 2.3 Comparación Simplicidad

Tabla 2.4 Comparación Rendimiento

Tabla 4.1 Sedes y clínicas de la empresa

Tabla 4.2 Servidores StoreFront definidos

Tabla 4.3 Servidor de Licencias definido

Tabla 4.4 Servidores Delivery Controller definidos

Tabla 4.5 Servidores XenApp diseñados

Tabla 4.6 Resumen de requerimientos

Tabla 6.1 Costes en base a la planificación y consultores contratados

Tabla 6.2 Coste licenciamiento

Tabla 6.3 Coste total

1. Introducción

1.1 Contexto y justificación del Trabajo

Para este proyecto, se va a realizar un despliegue para una empresa de seguros médicos, concretamente, SegurPat, con 2 sedes principales, Madrid y Barcelona. Además, dispone de distintas clínicas repartidas por España, reuniendo alrededor de 2.000 trabajadores.

Para optimizar y modernizar la infraestructura de IT, se requiere optimizar los puestos de usuario y tener un sistema centralizado en una de las sedes, donde se elige Barcelona.

Tras analizar ventajas e inconvenientes de los distintos fabricantes, se decide utilizar Citrix para virtualizar el puesto de trabajo.

1.2 Objetivos del Trabajo

En este proyecto se pretende dar una idea general del funcionamiento de la virtualización para su utilización en el aprendizaje y el desarrollo de personas interesadas en este tema. Así, este proyecto podrá ser utilizado tanto de una forma teórica como practica en la introducción a la virtualización.

En la actualidad, las empresas suelen tener distintas sedes repartidas por la geografía mundial. Por ello, surge la necesidad de centralizar los sistemas y dotar de una mayor versatilidad a los usuarios. Por ello, distintas empresas han sacado soluciones para virtualizar el puesto de un usuario, destacando algunas como Citrix, VMware, Microsoft, etc.

Para este proyecto, la empresa quiere aplicar una solución que permita modernizar su infraestructura, teletrabajar y mejorar la movilidad de sus empleados y aumentar la velocidad en montar un puesto de usuario para nuevas incorporaciones.

La solución implantada, debe permitir lo siguiente:

- Flexibilidad: Permitir a los usuarios trabajar desde cualquier dispositivo (Ipad, PC, móvil, etc).
- Seguridad: Estos sistemas, deben dotar a la infraestructura de una gran seguridad, permitiendo al usuario trabajar como si estuviese en la propia sede “principal”.
- Administración global y centralizada: Permite a los técnicos de sistemas, administrar y controlar la infraestructura desde una sede, (updates, despliegues, etc).
- Optimización de los recursos disponibles.

- Reducción de costes: Al simplificar los servicios de IT también se produce un ahorro en costes.
- Facilitar el despliegue masivo de escritorios y aplicaciones
- Mejorar el mantenimiento, la actualización de escritorios y aplicaciones y reducir las incidencias de los usuarios.

A parte de los objetivos de este tipo de tecnologías, se definen una serie de necesidades para este TFM:

- Los usuarios deben ejecutar escritorios XenDesktop convirtiendo el puesto de trabajo en un terminal remoto.
- Los usuarios, con frecuencia, requieren de configuraciones específicas y guardar datos. Para ello, se crean los perfiles de usuario al acceder a una máquina.
- Los sistemas diseñados, deben permitir a los usuarios utilizar aplicaciones no instaladas en local.
- Como requisito principal se necesita que la administración esté centralizada, de manera que los técnicos de sistemas puedan realizar sus tareas desde sus propios dispositivos sin necesidad de desplazarse o utilizar servidores dedicados para ello.
- Citrix debe permitir la reconexión de una sesión en caso de alguna caída para evitar la pérdida del trabajo no guardado en ese momento. Este periodo de tiempo será de 5 minutos, en base a lo indicado por el departamento de seguridad de la compañía.
- Mapeo de unidades con los servidores utilizados.
- A nivel técnico es necesario que los despliegues se realicen en alta disponibilidad (HA) para todos los elementos de la plataforma posible, evitando, que ante imprevistos el servicio se vea afectado.
- La solución implantada debe plantear la posibilidad de crecimiento. Se estima que la empresa crezca y los estudios indican que, en 2 años, la empresa estará formada por 2.250 empleados.
- Mejorar la seguridad de la compañía. Para ello, se limitará los accesos publicados a internet. Se limitarán las comunicaciones que se abran y se controlará el tráfico que pase por el firewall con el equipo de comunicaciones de SerguPat.
- Se realizará integración con la SAN corporativa basada en NetApp.

1.3 Enfoque y método seguido

Actualmente, la empresa no utiliza la virtualización del puesto de usuario y es por ello, que, para optimizar el trabajo, mejorar el rendimiento y centralizar el sistema, se va a realizar el desarrollo y la implantación de una solución para virtualizar los puestos de trabajo mediante el uso de Citrix.

El proyecto constará de cinco fases:

- a. Estudio y análisis actual.
- b. Análisis y diseño: Requisitos de la infraestructura, dimensionar máquinas virtuales, asegurar alta disponibilidad (HA), securización de acceso (certificados, encriptaciones), balanceo, etc.
- c. Implementación: Despliegue de toda la infraestructura y sus configuraciones.
- d. Fase de pruebas finales y validación: Testeo de rendimientos y latencias.
- e. Documentación.

1.4 Planificación del Trabajo

Se adjunta la planificación en forma de tabla:

Tarea	Fecha Inicio	Fecha Fin	Duración
Presentación del Proyecto	mié 28/02/18	mié 28/02/18	0 días
Inicio PEC1	mié 28/02/18	mié 07/03/18	6 días
Definición del proyecto	mié 28/02/18	vie 02/03/18	2 días
Análisis y objetivos definidos	vie 02/03/18	mié 07/03/18	4 días
Entrega PEC1	mié 07/03/18	mié 07/03/18	0 días
Inicio PEC2	jue 08/03/18	mar 17/04/18	29 días
Identificar y definir aspectos relevantes	jue 08/03/18	mié 14/03/18	5 días
Usar herramientas TIC adecuadas	mié 14/03/18	jue 15/03/18	2 días
Desarrollo de la solución propuesta	jue 15/03/18	mar 17/04/18	24 días
Presentar resultados parciales	dom 15/04/18	mar 17/04/18	2 días
Entrega PEC2	mar 17/04/18	mar 17/04/18	0 días
Inicio PEC3	mié 18/04/18	mié 23/05/18	26 días
Revisión de los resultados presentados	mié 18/04/18	vie 20/04/18	2 días
Inclusión elementos innovadores en la solución propuesta	mié 18/04/18	mar 15/05/18	20 días
Desarrollo segunda entrega	mié 18/04/18	mar 15/05/18	20 días
Revisión de la segunda entrega	mar 15/05/18	mié 23/05/18	7 días
Entrega PEC3	mié 23/05/18	mié 23/05/18	0 días
Inicio de la memoria	mar 01/05/18	dom 10/06/18	30 días
Entrega de la memoria final	dom 10/06/18	dom 10/06/18	0 días
Entrega de la presentación	dom 17/06/18	dom 17/06/18	0 días
Inicio del tribunal	lun 18/06/18	dom 24/06/18	6 días
Final del tribunal	dom 24/06/18	dom 24/06/18	0 días

Tabla 1.1 Planificación

Se adjunta el diagrama de Grant de la PEC1:

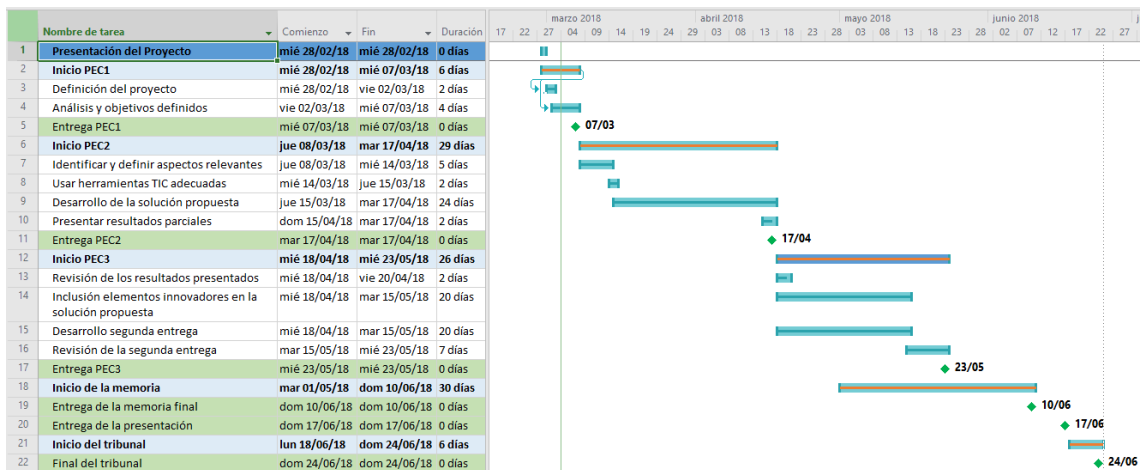


Figura 1.1 Diagrama de Grant

1.5 Breve resumen de productos obtenidos

El proyecto presenta un breve análisis entre distintas tecnologías de virtualización como son VMware, Microsoft, Citrix... Realiza una comparación entre ellas y se destaca los puntos fuertes y desventajas eligiendo Citrix, por características como:

- Facilidad de implantación
- Estabilidad
- Flexibilidad
- Centralización

Por ello, se realiza una propuesta para virtualizar un puesto de trabajo usando Citrix como solución para una empresa que esté interesada en el proyecto. En los contenidos del proyecto, se detalla su arquitectura, diseño, objetivos, utilidad...La solución adoptada también tiene en cuenta la posibilidad de distintas sedes para la empresa.

1.6 Breve descripción de los otros capítulos de la memoria

Una primera aproximación o índice de lo que contendría la memoria del proyecto a realizar, sería la siguiente:

1. Introducción
2. Comparación entre fabricantes
3. Elementos e introducción a Citrix
4. Diseño y arquitectura propuesta
5. Implementación
6. Presupuesto y costes
7. Conclusiones
8. Glosario
9. Bibliografía
10. Anexos

2. Conceptos teóricos

La virtualización con el paso de los años se ha convertido en un elemento clave para las empresas y la evolución del mundo informático. La virtualización es la piedra angular de cualquier técnica de diseño para todas las arquitecturas de nube. Se entiende por virtualización, como la abstracción de los recursos IT físicos tanto de las personas como de las aplicaciones que los utilizan. La virtualización permite a los servidores, elementos de almacenamiento y otros elementos hardware ser tratados como una pila de recursos, estos recursos pueden ser distribuidos según la demanda.

Esta tecnología, permite crear múltiples entornos. Se pueden diferenciar distintas tecnologías de virtualización:

- Sistema Operativo.
- Aplicaciones.
- Red.
- Almacenamiento.
- Hardware.

En este proyecto, la empresa busca modernizar sus sistemas y su infraestructura de TI, por ello, se decide usar la virtualización. Además, quiere permitir el teletrabajo y mejorar la movilidad de sus empleados, por lo que la virtualización es la tecnología adecuada para este tipo de objetivos. Aplicando esta tecnología, se reducen considerablemente los costes y se permite desplegar puestos en un tiempo reducido. Entre sus principales ventajas destacan las siguientes:

- Elimina el sobreaprovisionamiento, usando servidores a plena capacidad y apagando los que no tienen prácticamente uso.
- Aumenta la eficiencia energética, debido a la reducción del número de servidores.
- Reduce los requisitos de hardware de la infraestructura. Cuenta con una independencia de las máquinas virtuales del hardware físico del que disponen.
- Reduce el coste en aplicaciones porque aumenta la capacidad de un host para alojar sistemas operativos.
- Reduce considerablemente el tiempo empleado en labores de aprovisionamiento y mantenimiento de la infraestructura.

Además de esto, proporciona alta disponibilidad de las máquinas virtuales y por tanto de las aplicaciones, asegurando que se cumplan los niveles de servicios contratados haciendo que los servicios

permanezcan operativos como mínimo el tiempo indicado en la configuración.

En el caso de interrupciones imprevistas de los sistemas, ya sea por fallo de uno de los servidores o por fallo de uno de los sistemas operativos, se mejora el tiempo de respuesta, reduciendo considerablemente el tiempo de inactividad.

Existen diferentes fabricantes para el uso de la virtualización, donde destacan Microsoft, VMWare o Citrix. De estos, Citrix destaca con productos que introducen unas soluciones de mejora distintas a sus competidores incorporando XenApp, XenDesktop y XenServer. Por el contrario, VMWare destaca con el producto View y la virtualización de servidores, al igual que Microsoft con RDS. De esta manera, el mercado tiene una gran variedad de productos y fabricantes donde puede buscar la solución que mejor se ajuste a sus necesidades.

Centrándonos en estos productos y medios de virtualización sus principales características son las siguientes:

- XenApp y XenDesktop de Citrix: Destaca por la posibilidad de utilizar publicaciones y streaming de aplicaciones. Utiliza un protocolo ICA/HDX y otorga la posibilidad de virtualizar aplicaciones y escritorios.
- VMWARE Horizon View: Al igual que Citrix, ofrece la posibilidad de virtualizar aplicaciones y escritorios, por el contrario, solo permite el streaming de aplicaciones.
- Microsoft RDS: Como ocurre en los anteriores, permite virtualizar escritorios y aplicaciones. Utiliza un protocolo Terminal Server/Remote FX propio de Microsoft. Al igual que Horizon View, sólo permite el streaming de aplicaciones.

2.1 Comparación entre los distintos fabricantes

Teniendo en cuenta la descripción previa, se puede profundizar más en las principales diferencias que ofrecen los productos de cada uno. Respecto a la virtualización del puesto de trabajo, hay 3 fabricantes que destacan por encima del resto en base a sus costes, software y volumen de empresas que usan sus productos. Se adjunta una imagen que refleja el uso de estos fabricantes en el mercado:

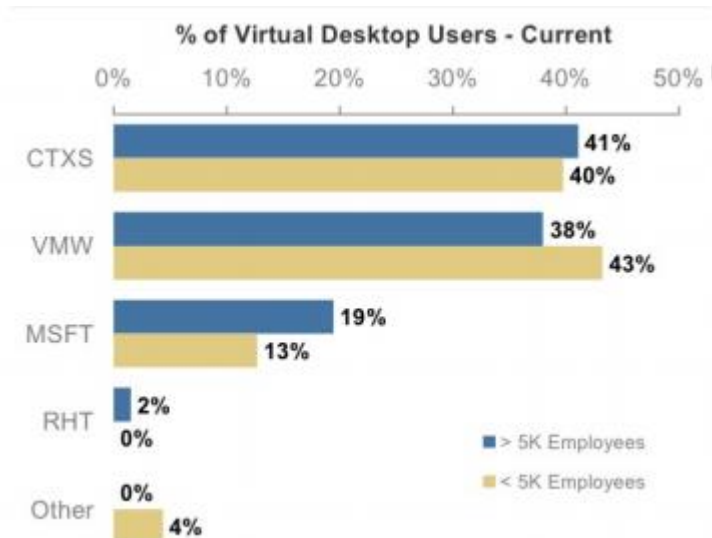


Figura 2.1 Comparativa Virtual Desktop User, Fuente: Morgan Stanley

Por ello, se adjunta una tabla con las principales diferencias entre ellos:
Para ello, se adjunta una tabla con las principales diferencias:

Características	VMWare	Microsoft	Citrix
VDIs de Windows y Linux	Sólo Windows	Sólo Windows	Ambas
Estabilidad	Alta	Alta	Muy alta
Facilidad de Implantación	Alta	Alta	Muy alta
Consola de centralización	Limitado	Si	Si
Acceso a aplicaciones virtuales (Windows y Linux)	Sólo Windows	Sólo Windows	Ambas

Tabla 2.1 Comparativa entre fabricantes

Aparte de estas características, se pueden hacer diferencias en otros aspectos como se presentan en las siguientes tablas:

INTEGRACIÓN UNIFORME CON CLIENTES PESADOS			
Características	VMWare	Microsoft	Citrix
Inicio instantáneo de aplicaciones con lanzamiento previo y permanencia de sesión	-	-	X
Integración de aplicaciones Windows virtualizadas, así como aplicaciones SaaS/Web en el menú Inicio	-	X	X
Compatibilidad con Windows Aero	-	X	X
Acceso sin inconvenientes a aplicaciones locales desde VDI o sesiones de escritorio compartido alojadas	-	-	X

Tabla 2.2 Comparación Integración uniforme con clientes pesados

SIMPLICIDAD			
Características	VMWare	Microsoft	Citrix
Desbloqueo y reinicio de password autoservicio del usuario	-	X	X
HDX™ Mobile optimiza las aplicaciones Windows para entornos de pantalla táctil móviles	X	-	X
Sencillez y coherencia en los dispositivos	limitado	limitado	X
Configuración automatizada basada en el correo del usuario	-	-	X
Interfaz de usuario personalizable para marca corporativa, elementos emergentes y flujos de trabajo	limitado	limitado	X
Facilidad de despliegue e implantación	X	-	X
Amplia compatibilidad escritorio y aplicaciones	X	-	X
Ruta óptima mediante Storefront y Netscaler Gateway	-	-	X

Tabla 2.3 Comparación Simplicidad

RENDIMIENTO			
Características	VMWare	Microsoft	Citrix
Guardado de sesiones y perfiles de usuario	-	X	X
Rendimiento optimizado en sesiones de usuario con conexiones de larga distancia con un ancho de banda limitado y una latencia alta	X	-	X
Rendimiento de aplicaciones casi nativo en redes con una alta latencia y alta pérdida de paquetes con HDX	-	-	X
Admite la aceleración de gráficos con GPUs suministrados por Intel, AMD y NVIDIA	X	-	X
Entrega de imágenes de alta resolución mediante la compatibilidad de uso compartido de Intel Iris Pro Virtual GPU (GVT-g)	-	-	X
Impresión sin controladores y sin preocupaciones desde cualquier dispositivo y con un consumo mínimo de ancho de banda	X	X	X
Optimización para soluciones de Unified Communications como Skype for Business o Cisco Jabber, reduce la latencia con procesamiento de medios locales de voz y video	Limitado a VDI	X	X

Tabla 2.4 Comparación Rendimiento

Por el contrario, Citrix y la virtualización, también cuentan con algunas desventajas respecto a sus principales competidores:

- Cualquier problema que afecte al servidor afectará a múltiples usuarios. Por esa razón, es una buena idea configurar servidores redundantes como mecanismo de seguridad
- Los administradores tendrán que aprender las capacidades del software de VDI y sus limitaciones.
- Se depende en gran medida de las comunicaciones y la configuración crece en importancia. En caso de realizar malas configuraciones los riesgos de seguridad crecen.

Teniendo en cuenta las tablas anteriores, donde se realiza una comparación con distintas características entre los principales fabricantes del mercado, se determina que Citrix destaca en aspectos muy importantes en cuanto a la virtualización para un puesto de usuario, donde destacan las siguientes:

- Estabilidad: Citrix goza de una gran estabilidad antes latencias altas y bajos anchos de banda.
- Flexibilidad: Con el paso de los años, los dispositivos móviles distintas al PC gozan de una gran importancia en las empresas. Por ello, es fundamental disponer de un acceso óptimo desde cualquier dispositivo, Tablet, móvil, pc, etc. Citrix en este aspecto, destaca ante el resto de los fabricantes.
- Implantación: La forma de desplegar el producto y su plataforma es mucho más sencillo respecto al resto, lo cual, provoca que tenga una gran facilidad de implantación respecto a sus competidores.
- Centralización: Dispone de una única consola de administración.
- Troubleshooting: Al tener una estructura más sencilla, los problemas de infraestructura suelen ser más sencillos de resolver.

En conclusión y resumiendo lo visto entre estos fabricantes, existen tres aspectos diferenciales. El primero, Citrix ofrece a cada usuario el tipo de virtualización que mejor se adapta a su entorno, a través de VDI, shared desktops, virtualización local de la aplicación u otras alternativas. En segundo lugar, permite mantener intacta la experiencia del usuario, resultando de gran valor en proyectos que requieran acceso remoto. Por último, son el único fabricante que puede abordar el proyecto de extremo a extremo.

Por estas razones, se ha decidido implementar el proyecto mediante el uso de Citrix, usando XenApp y XenDesktop y no otros productos de diferentes fabricantes.

3. Elementos e introducción a Citrix

3.1 XenAPP y XenDesktop

Para realizar el proyecto se van a usar dos productos de Citrix visto de manera sencilla anteriormente, XenApp y XenDesktop. Estas tecnologías, se caracterizan por lo siguiente:

- XenApp: Permite virtualizar cualquier aplicación de Windows y centralizarla de manera que pueda gestionarse desde una única consola. Este producto, ofrece la posibilidad de entregar aplicaciones bajo demanda al usuario, de manera instantánea y en forma de servicio. Da flexibilidad, permitiendo que el usuario este en cualquier lugar y usando cualquier tipo de dispositivo. XenApp reduce los gastos de la gestión de aplicaciones hasta un 50%, aumenta la capacidad de respuesta entregando las aplicaciones a los usuarios, y mejora la seguridad de aplicaciones y datos.
- XenDesktop: Ofrece la posibilidad de virtualizar los puestos de trabajo de los usuarios, transformando los escritorios en un servicio para cada usuario, permitiendo que el usuario esté en cualquier lugar y usando cualquier dispositivo. Habitualmente, es conocido como VDI o puesto virtual.

A nivel de infraestructura, se puede dividir en dos partes. Una primera, formada por lo parte a nivel de usuario, donde se ofrece el acceso a los escritorios y aplicaciones a los usuarios. En segundo lugar, estaría la parte de administración del servicio para los usuarios encargados de administrar la plataforma.

Con esto, podemos realizar una división en cinco capas, mostrando de manera sencilla la estructura a desplegar y los componentes que forman parte de la misma.

- Access layer: La forman los sistemas de acceso a la infraestructura diseñada.
- User layer: Formada por los dispositivos desde los cuales, se accede a las aplicaciones y escritorios que han sido virtualizados.
- Hardware layer: Está compuesta por toda la infraestructura a nivel físico, es decir, el “hierro” de la plataforma. Esta capa principalmente se divide en dos, el almacenamiento y el host.
- Control layer: Se compone de los servidores y la consola de administración.

- Resource layer: Esta capa, se forma por los escritorios y aplicaciones como recursos a servir.

Se adjunta una imagen mostrando las capas descritas:

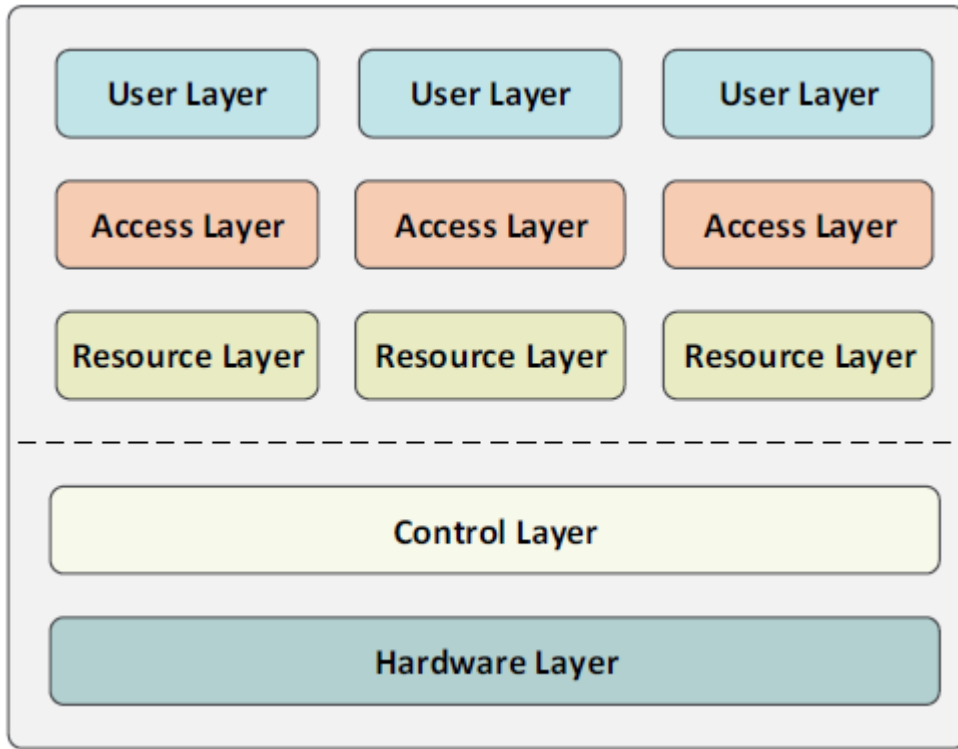


Figura 3.1 Capas de la infraestructura

3.2 VDI (Virtual Desktop Infrastructure)

La virtualización de un escritorio tiene distintas funcionalidades y características a las de un servidor de aplicación. Aunque tienen cosas en común, la esencia de este tipo de virtualización se basa en la creación de una máquina virtual que se ejecuta en un servidor virtualizado (VDI Server), es decir, un PC virtual.

Esta VDI, mantendrá las características de rendimiento y el sistema operativo habitual de un ordenador. Para acceder a la VDI, será necesario habilitar las comunicaciones correspondientes y ejecutar el software de cliente de terminal remoto. Este acceso, recibe el nombre de acceso por RDP.

A diferencia de un ordenador tradicional, los discos no están en el propio equipo de manera física, sino que se presentan a la máquina virtual de distintas formas, por ejemplo, por fibra. Este modo de presentar los discos permite que, en caso de pérdida o daño del equipo, no se pierdan los datos guardados en el disco. Además, nos permite la conexión al equipo desde cualquier punto y diferentes dispositivos, siempre que disponga de las herramientas adecuadas para iniciar una conexión por RDP.

La tecnología basada en VDIs introduce novedades y ventajas importantes en el mundo de la virtualización. A modo económico, se reducen los costes y se produce un gran ahorro. Esta reducción económica, principalmente, se debe a la menor dependencia de la evolución de aplicaciones y sistema operativo. Otra de las principales ventajas es que permite el rehusar equipos existentes incluso permitiendo el ahorro de licencias en determinados casos.

Las VDIs, añaden una gran mejora y simplificación de los PC escritorio y su gestión. Permite que se reduzcan los costes de mantenimiento y se facilite la resolución de incidencias. Hay que tener en cuenta que los discos son virtuales y los equipos suelen estar basados en las mismas plantillas facilitando también el despliegue y la rapidez en la creación de máquinas nuevas.

En cuanto a seguridad, introducen mejoras que aumentan la dificultad de robo de claves y datos. Por ejemplo, no se disponen de datos locales que puedan ser robados o motivo de pérdida por avería o extravío.

Se optimiza el trabajo para los usuarios y se les permite el acceso desde cualquier lugar, ofreciendo la posibilidad de continuar sus trabajos fuera de su puesto habitual. Las averías e incidencias se reducen ayudando a la optimización del trabajo.

3.3 Arquitectura FMA (FlexCast Management Architecture)

La arquitectura FMA es la base de las tecnologías Citrix XenApp 7.6 y XenDesktop 7.6. Este tipo de arquitectura está orientada a servicios permiten la interoperabilidad y administración modular de las diversas tecnologías de Citrix. FMA, da la posibilidad de tener una plataforma con aplicaciones y escritorios, servicios, aprovisionamiento flexible, administración en la nube y movilidad.

Además, FMA sustituye a la arquitectura IMA (Independent Management Architecture), usada en versiones anteriores de XenApp como la 6.5. Esta arquitectura se refleja en la siguiente figura:

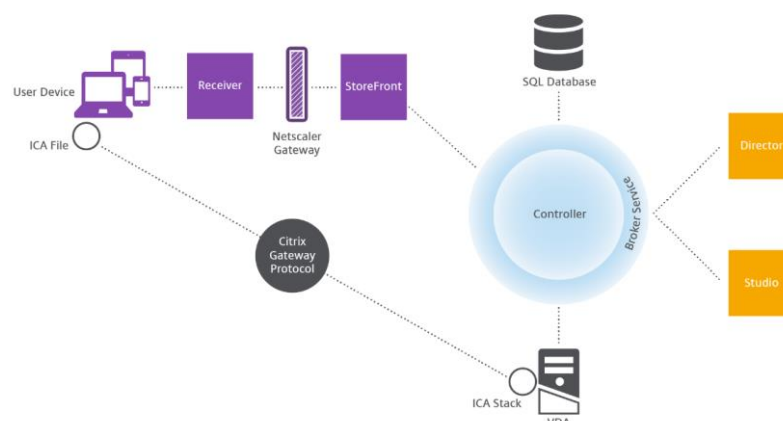


Figura 3.2 Arquitectura FMA

3.4 Protocolo ICA

El protocolo ICA (Independent Computing Architecture) es la base de la tecnología Citrix y la que ofrece más ventajas respecto al resto de sus competidores. Es un protocolo basado en TCP que trabaja en la capa de Presentación (nivel 6) del modelo OSI y por el puerto 1494 o por el 2598 si se utiliza "Session Reliability".

El protocolo ICA es altamente interactivo, sin embargo, es considerablemente menor el consumo de ancho de banda con respecto al existente con RDP, el cual, requiere constantemente por pequeño que sea, una comunicación de tipo cliente / Servidor.

ICA, permite la compresión de toda la información que es transmitida consiguiendo una conexión entre el cliente y el servidor mucho más eficiente. Además, está optimizado para conexiones lentas de hasta 14 kbps y con una latencia alta. Se adjunta imagen con estas conexiones:

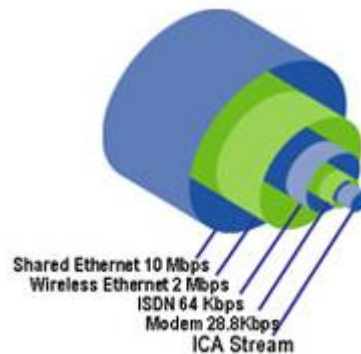


Figura 3.3 Conexiones ICA

Este modelo, también usa canales para redirigir contenidos como se puede mostrar en la siguiente figura donde se aprecia este modelo de encapsulado:

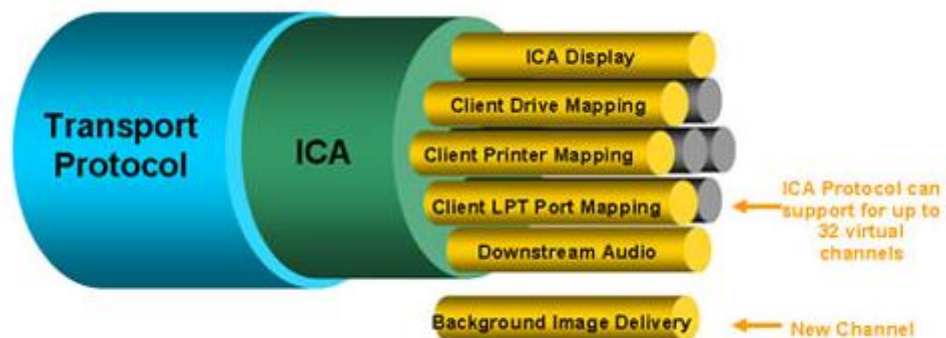


Figura 3.4 Modelo Encapsulado ICA

Esto permite que se consuma únicamente aquello que varía en la pantalla, y transmite únicamente aquello que cambia.

A diferencia del protocolo RDP, el consumo de ancho de banda del protocolo ICA puede variar de 4/8KB a 20KB como máximo de consumo de ancho de banda por conexión existente. Por el contrario, RDP tiene un consumo fijo de 26KB de ancho de banda por conexión establecida.

Con las nuevas funcionalidades HDX (High Definition Experience), ICA también ha evolucionado y ha sido optimizado. Con ello, se han generado nuevas características, de las que destacan las siguientes:

- HDX RichGraphics with RemoteFX: optimiza el rendimiento de gráficos 2D y 3D.
- HDX Realtime: audio bidireccional con lo que se permiten aplicaciones del tipo comunicaciones integradas.
- HDX Plug&Play: permite la conexión de multi-monitor y otros dispositivos locales.

3.5 Capas definidas

Como se comentaba en el punto 3.1, existen distintas capas en el entorno a diseñar y en las cuales, cada una tiene un objetivo diferente.

User layer

Esta capa queda definida como la Access layer del usuario a la plataforma Citrix. La componen todos los elementos que requiere el usuario para realizar el acceso al entorno. Esto podría ser, el Software Citrix Receiver y que es necesario para realizar el acceso, Delivery Group (grupos de publicación de acceso a los recursos) y los puestos de usuario, tablets, smartphones, etc. El acceso al entorno puede realizarse de manera externa o interna como se refleja en la siguiente imagen:

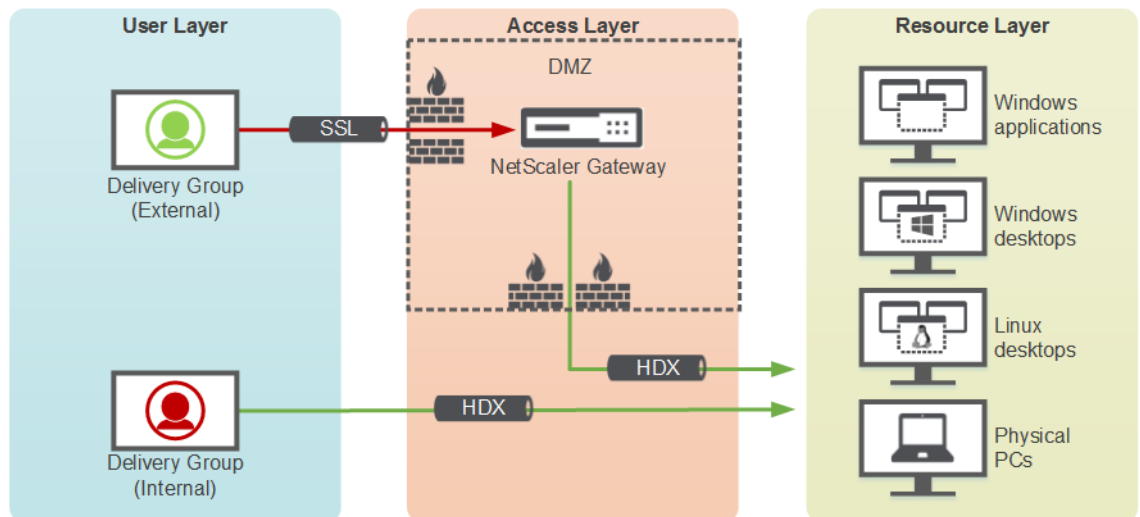


Figura 3.5 Acceso al entorno

Externa: Las conexiones externas son todas las que provienen de fuera de la red de la empresa y requieren de un acceso a la DMZ.

Interna: Conexiones internas para usuarios que ya están en la red de la compañía y no requieren pasar por DMZ.

Access layer

La Access layer permite la autenticación del usuario permitiendo o denegando las conexiones al entorno. Esta operativa, se puede realizar desde el Netscaler Gateway o desde el Storefront. Además, hemos de tener en cuenta que existen conexiones externas e internas. Esta capa, proporciona la comunicación entre la User layer y la Resource layers. Entre los elementos principales, destacan los siguientes:

- Netscaler Gateway: Permite al personal acceder a cualquier aplicación, desde cualquier dispositivo, mediante una sola URL. Con el uso del AD del entorno, permite diferenciar los usuarios y permitir o denegar la conexión al entorno. Por lo tanto, este elemento de la infraestructura se encarga de la autenticación a la red. Este elemento, se encuentra en la DMZ y es un dispositivo VPN SSL, permitiendo que un usuario externo al firewall de la empresa pueda acceder de forma segura si cumple los requisitos AD marcados.
- StoreFront y en versiones anteriores de XenApp, Web Interface: Realiza la autenticación de accesos internos provenientes del acceso Web o a través Citrix Receiver. Además, se encarga de listar de manera gráfica las aplicaciones publicadas al usuario mediante grupos de directorio activo. La comunicación del listado de aplicaciones se consigue a través del Delivery Controller, el cual, dispone de dicha información y la proporciona al StoreFront. Se adjunta una imagen del StoreFront de un entorno:



Figura 3.6 Vista de usuario de un StoreFront

El acceso al entorno puede realizarse mediante distintas formas más o menos restrictivas, por ejemplo, Token, Smart Card o Kerberos. Las políticas utilizadas deben poder detectar tanto conexiones internas como externas.

Control layer

Esta capa es el núcleo del entorno Citrix a desplegar, donde se encuentran los siguientes elementos:

- Servidor de Licencias Citrix: Administra las licencias del fabricante y se comunica con el Delivery Controller para asignar y liberar a los usuarios las licencias con cada inicio de sesión. También, realiza una conexión con la consola del Citrix Studio, utilizada para asignar archivos de licencias.
- Servidor de Licencias TsCal (Terminar Server): Todas las conexiones Citrix requieren de una sesión TsCal, la cual, requiere de una licencia Terminar Server.
- Base de Datos: Se necesita de una BBDD de tipo SQL donde se pueda almacenar toda la información generada, sesiones, configuraciones, etc. Esta BBDD, no suele ser de tamaños grandes. Es importante que la base de datos quede desplegada en alta disponibilidad.

- Citrix Studio: Studio es la principal consola de administración para gestionar sitios de XenApp y XenDesktop. Esta intuitiva consola de Windows se utiliza para tareas como la configuración inicial del sitio, aprovisionamiento de la máquina y publicación de aplicaciones y escritorios. Da la posibilidad de publicar a los usuarios escritorios o aplicaciones.
- Citrix Director: Es la consola de administración de virtualización diaria para tareas rutinarias en XenApp y XenDesktop. Los administradores y personal del servicio de asistencia telefónica usan esta consola basada en web para las actividades de administración y monitorización habituales, como la visualización y control de sesiones de usuario, informes sobre uso del entorno y notificaciones y alertas.
- Deliver Controller o Broker: Es el principal elemento de administración de XenApp y XenDesktop. Generalmente, se dispone de varios servidores Deliver Controller. Se compone de servicios que comunican con el hipervisor para distribuir escritorios y aplicaciones. Este elemento, actúa como intermediario entre el usuario y el recurso a usar, distribuyendo la carga de las conexiones entre los servidores disponibles. Al diseñar los Controller del entorno se debe tener en cuenta lo siguiente:
 - Redundancia: Se recomienda que un sitio de producción siempre tenga al menos dos Controllers en diferentes servidores físicos. De este modo, si falla un Controller, los otros pueden gestionar las conexiones y administrar el sitio.
 - Escalabilidad: A medida que aumenta la actividad de un sitio, también aumenta el uso de CPU en el Controller y la actividad de la base de datos de SQL Server. Los Controllers adicionales ofrecen la capacidad de administrar más usuarios y más solicitudes de aplicaciones y escritorios, además de mejorar la capacidad general de respuesta.

Además de los elementos comentados deben tenerse en cuenta otros como las directivas a aplicar, los DNS, DHCPs y el directorio activo (AD) y su contenido.

Resource layers

Esta capa está compuesta por los recursos que los usuarios tienen a su disposición para ser publicados. De cara a realizar esta tarea, se deben considerar los catálogos que ofrece Citrix, centrados en XenDesktop y XenApp. Cada uno de ellos, ofrece diferentes herramientas.

Para XenApp, se ofrecen las siguientes posibilidades:

- Hosted: las aplicaciones se encuentran instaladas y publicadas en un servidor funcionando como de Xenapp 7.6. Las aplicaciones se ejecutan en el servidor y se distribuyen mediante grupos de usuarios. Esta opción es la más idónea para aplicaciones empresariales con un volumen de uso entre el 50%-75% del conjunto de usuarios.
- Streamed: las aplicaciones se entregan de forma dinámica al servidor/ escritorio físico/virtual, con una solución similar a Microsoft-App-v, permite que las aplicaciones estén disponibles para los usuarios finales sin estar instaladas en los equipos finales. Esta solución requiere de productos e infraestructura adicionales, pero es la opción más óptima respecto al número de Golden Images.
- VDI de Servidor: consiste en utilizar un servidor Xenapp para entregar escritorios a los usuarios. En este tipo de escritorios no existe ningún tipo de personalización ya que no deja de ser una sesión de terminal server compartida en un Servidor
- User-Based: se trata de aplicaciones que, por el pequeño porcentaje de usuarios, no tiene sentido que sean administradas por el Departamento de IT. Los usuarios que requieran estas aplicaciones tienen dos opciones:
 - Xendesktop Pvdisk: solicitar un escritorio personal con Personal Vdisk (PvDisk), e instalar la aplicación, de este modo quedaría instalada en su Pvdisk, como si se tratase de un PC al uso.
 - Xendesktop: solicitar un escritorio normal, tipo Pool con acceso a las aplicaciones instaladas en el puesto físico, con el uso de la política "Local App Access".
- Installed: las aplicaciones se instalan en la Golden Image para su posterior despliegue. A pesar de que esta opción puede dar lugar a un mayor número de imágenes de escritorio maestro si los conjuntos de aplicaciones entre los grupos de usuarios difieren en gran medida, es el método recomendado debido a su simplicidad. Esta es la mejor opción para las aplicaciones utilizadas por el 75% + del conjunto de los usuarios.

Para XenDesktop, se ofrecen las siguientes posibilidades:

- Escritorio Existing: es lo más parecido a un puesto físico pero gestionado desde Xendesktop. Al igual que con los escritorios locales tradicionales, los cambios y las actualizaciones son

permanentes y deben gestionarse individualmente o colectivamente utilizando herramientas de distribución de terceros. La administración de los escritorios virtuales Existing a través de Xendesktop le permite tener un mayor control sobre sus estados de energía; Por ejemplo, puede configurar Xendesktop para apagar máquinas virtuales cuando los usuarios desconecten para minimizar el consumo innecesario de energía en el centro de datos.

- Escritorio estático no persistente: la primera vez que un usuario inicia una sesión para usar uno de estos escritorios, el usuario recibe un escritorio de un grupo de escritorios basados en una única imagen maestra. Después del primer uso, cada vez que el usuario inicia sesión para usar uno de estos escritorios, el usuario se conecta al mismo escritorio que le fue asignado la primera vez. Todos los cambios realizados en el escritorio se pierden cuando la máquina se reinicia.
- Escritorios aleatorios no persistentes: también conocidos como escritorios VDI Pool o Random. Cada vez que un usuario inicia una sesión, se conecta a un escritorio seleccionado de forma aleatoria dentro de un grupo de escritorios basado en una única imagen maestra. Todos los cambios realizados en el escritorio se pierden cuando la máquina se reinicia.
- Escritorio estático persistente: también conocido como VDI con Personal vDisk. A diferencia de otros tipos de escritorios VDI, los usuarios pueden personalizar completamente estos escritorios. La primera vez que un usuario inicia una sesión para usar uno de estos escritorios, el usuario recibe un escritorio de un grupo de escritorios basados en una única imagen maestra. Después del primer uso, cada vez que el usuario inicia sesión para usar uno de estos escritorios, el usuario se conecta al mismo escritorio que le fue asignado la primera vez. Los cambios en el escritorio se conservan cuando la máquina se reinicia porque están almacenados en un disco, este disco se llama Personal vDisk.
- Escritorio Remote PC Access: el acceso con Remote PC permite a un usuario final iniciar sesión de forma remota desde cualquier lugar, en un equipo físico Windows de la oficina. El Virtual Delivery Agent (VDA) debe estar instalado, el cual se registra con el Delivery Controller y administra la conexión HDX entre el equipo y los dispositivos finales.

También se debe tener en cuenta el aprovisionamiento. Este es independiente del sistema operativo seleccionado. En el caso de Citrix, se incluyen dos soluciones:

- Provisioning Services (PVS): La tecnología de distribución por streaming de Provisioning Services permite aprovisionar y

reaprovisionar los equipos en tiempo real desde una misma imagen de disco compartida. De esta forma, los administradores no necesitan administrar ni instalar revisiones para cada sistema individualmente. Toda la administración de imágenes se realiza en la imagen maestra. Es posible usar la unidad de disco duro local de cada sistema para el almacenamiento en caché de los datos en ejecución o, en algunos casos, es posible quitarla completamente del sistema, a fin de reducir el uso de energía, la frecuencia de errores del sistema y los riesgos a la seguridad.

Al utilizar Provisioning Services, cualquier disco virtual puede configurarse en Standard Image Mode. Un disco virtual en Standard Image Mode permite que muchos equipos se inicien de forma simultánea desde ese disco, lo que reduce de manera significativa la cantidad de imágenes que deben mantenerse y la cantidad de almacenamiento requerido. El disco virtual tiene un formato de solo lectura y los dispositivos de destino no pueden modificar la imagen. Se adjunta una imagen con el esquema del PVS:

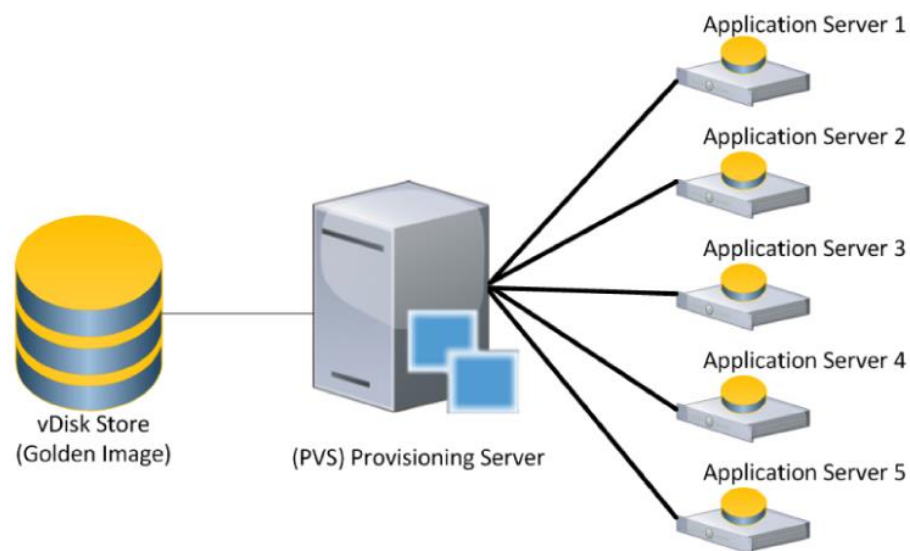


Figura 3.7 Esquema Provision Services

- Machine Creation Services (MCS): Para aprovisionar las máquinas, se proporciona una imagen maestra (o instantánea) como guía para crear máquinas virtuales idénticas en el catálogo. Antes de crear el catálogo, primero se deben usar las herramientas en el hipervisor o servicio de nube para crear y configurar la imagen maestra (lo que incluye instalar un Virtual Delivery Agent o VDA en la imagen). A continuación, cuando se crea el catálogo de máquinas en Studio, se selecciona esa imagen (o una instantánea de ella), se especifica la cantidad de máquinas virtuales que se van a crear en el catálogo y se configura más información.

Para implementar aplicaciones en catálogos de máquinas administradas por MCS, debe trabajar con Configuration Manager y Citrix Studio. En la siguiente figura, se describe el proceso de instalación:

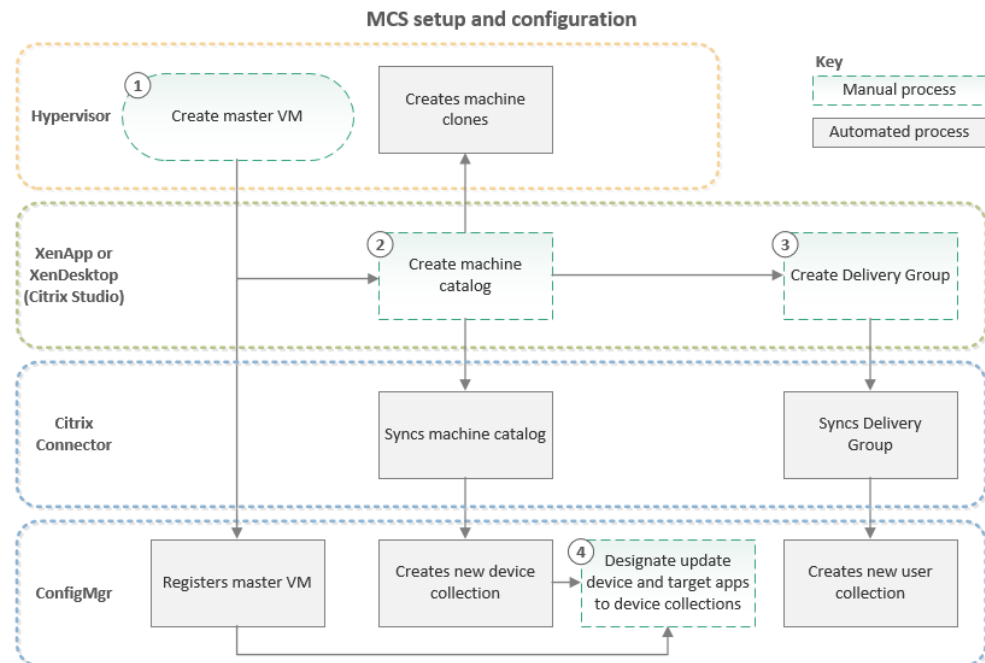


Figura 3.8 Proceso instalación y configuración MCS

Hardware layer

La capa Hardware está compuesta por los servidores y almacenamiento necesarios para la implementación de la solución de virtualización de escritorio y aplicaciones.

La elección del tipo de almacenamiento tiene un impacto directo sobre la elección de la infraestructura servidora y viceversa:

- Almacenamiento: está considerado como una de las partes más importantes en las soluciones de virtualización de escritorio/aplicaciones, no solo afecta al coste del proyecto sino también a las limitaciones para la elección de la infraestructura servidora. Por lo que la elección de almacenamiento es el primer paso en el diseño de la Capa Hardware. Además del tipo de almacenamiento escogido, hay que poner especial atención al dimensionamiento (espacio e IOPS) con el fin de proporcionar un servicio adecuado. Cada operación de lectura / escritura en el disco debe esperar en la cola antes de ser atendida. Si la capacidad de la infraestructura de almacenamiento no es suficientemente alta, una solicitud de IO aumenta el tiempo de espera, lo que afecta negativamente a la experiencia del usuario.
- Servidores: en la capa Hardware de una solución de virtualización de escritorio y/o aplicaciones, se debe elegir el tipo de

infraestructura servidora, generalmente suele estar entre servidores Blade o tipo rack.

Por último, se adjunta una figura de la estructura explicada y sus capas:

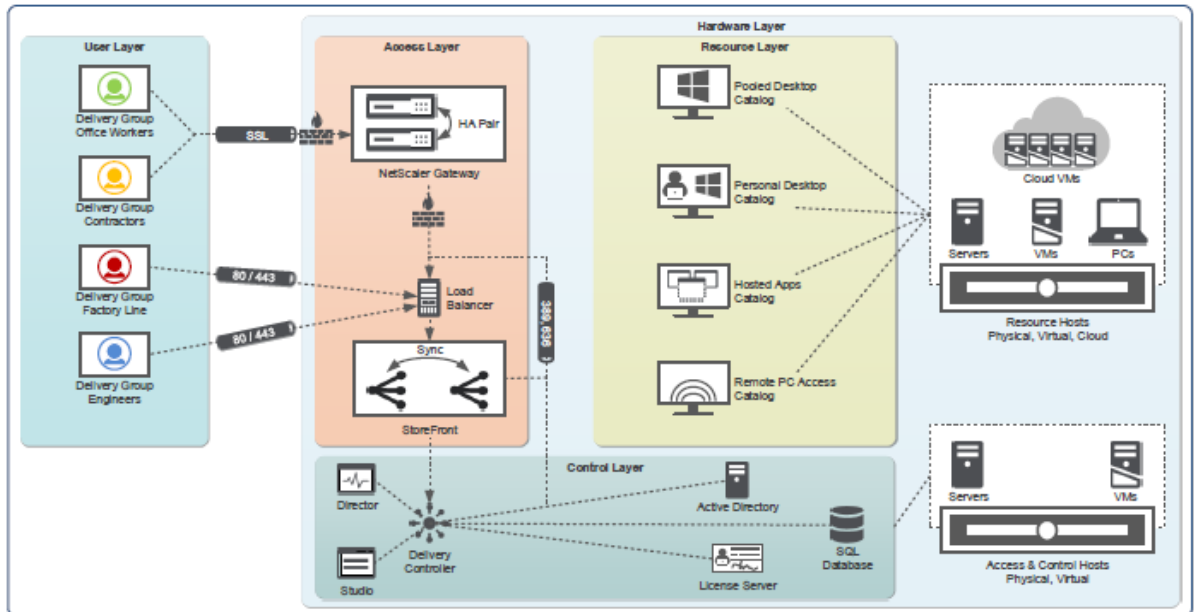


Figura 3.9 Resumen de layers del entorno

4. Diseño propuesto:

Para este proyecto se va a realizar un despliegue para una empresa de seguros médicos (SegurPat) con 2 sedes principales, Madrid y Barcelona y distintas clínicas repartidas por España, para la cual, trabajan alrededor de 2.000 personas.

Para optimizar el trabajo, se requiere optimizar los puestos de usuario y tener un sistema centralizado en una de las sedes, donde se elige Barcelona.

Tras analizar ventajas e inconvenientes de los distintos fabricantes, se decide utilizar Citrix para virtualizar el puesto de trabajo.

4.1 Esquema y diseño actual

En la actualidad, la empresa se compone de las siguientes sedes, número de trabajadores y roles:

Sedes y clínicas	Número de trabajadores	Roles
Barcelona	900	Departamento de Sistemas Recursos Humanos Administración Médicos Recepcionistas Usuarios VIP (directores)
Madrid	500	Departamento de Sistemas Administración Médicos Recepcionistas Usuarios VIP (directores)
Valencia	200	Médicos Recepcionistas Enfermeros
Sevilla Bilbao Málaga	100	Médicos Recepcionistas Enfermeros
Toledo Zaragoza	50	Médicos Recepcionistas Enfermeros

Tabla 4.1 Sedes y clínicas de la empresa

La empresa, dispone de 3 centros de procesamiento de datos (CPDs), 2 en Barcelona y 1 en Madrid, lugares donde se acumula el mayor número de trabajadores.

Para el almacenamiento, se dispone de 3 cabinas NetApp, 2 en Barcelona y 1 en Madrid, es decir, una por cada CPD. El CPD1 de Barcelona se toma como principal y está configurado como activo/pasivo con el CPD2 de Barcelona, de tal manera, que si un centro tuviese problemas se podrían balancear de manera rápida e incluso automática el servicio al CPD2 (secundario).

Se dispone de una red de backup por posibles problemas que pudiese haber. Además, existe conexión mediante switches utilizando una red Ethernet. También, se dispone de una red ADSL para conexiones de VPN, lo que permite conectarse a la red si fallase Citrix.

Respecto a la virtualización, se utilizan host de VMWare con un total de hasta 30 host ESX que permiten el desarrollo y despliegue de la infraestructura Citrix.

Cada CPD contiene un Chasis de servidores Blade Cisco UCS. En cuanto a las licencias, se dispone de 2000 licencias TsCAL de usuario nominal, necesarias para las conexiones de usuario.

Para el correcto desarrollo, se van a montar 6 controladores de dominio integrados en un AD de Microsoft versión Windows 2016.

4.2 Requisitos planteados

Para realizar el desarrollo, se deben cumplir los requisitos planteados:

- Los usuarios deben ejecutar escritorios XenDesktop convirtiendo el puesto de trabajo en un terminal remoto. Esto permite que puedan acceder desde cualquier dispositivo.
- Los usuarios, con frecuencia, requieren de configuraciones específicas y guardar datos. Para ello, se crean los perfiles de usuario al acceder a una máquina. Estos perfiles son necesarios para multitud de aplicaciones, Outlook, SAS, Business Objects, etc.
- Los sistemas diseñados, deben permitir a los usuarios utilizar aplicaciones no instaladas en local. Esta conexión y accesos se tramitarán mediante grupos de acceso creados en AD, los cuales, servirán para que cada usuario visualice lo que corresponda cuando accede al StoreFront.
- Centralizar el sistema y la red. Como requisito principal se necesita que la administración esté centralizada, de manera que los técnicos de sistemas puedan realizar sus tareas desde sus propios dispositivos sin necesidad de desplazarse o utilizar servidores dedicados para ello.

- No tener pérdida de sesión tras un fallo de conexión, ya sea por fallo de la red u otro motivo. Citrix debe permitir la reconexión de una sesión en caso de alguna caída para evitar la pérdida del trabajo no guardado en ese momento. Este periodo de tiempo será de 5 minutos, en base a lo indicado por el departamento de seguridad de la compañía.
- Mapeo de unidades con los servidores utilizados. Debe poderse realizar tareas entre unos equipos y otros, permitir el copy/paste u otros procesos que sean necesarios y de uso habitual para los usuarios.
- A nivel técnico es necesario que los despliegues se realicen en alta disponibilidad (HA) para todos los elementos de la plataforma posible, evitando, que antes imprevistos el servicio se vea afectado.
- La solución implantada debe plantear la posibilidad de crecimiento. Debe tener en cuenta que tanto a nivel de usuarios, como a nivel de aplicaciones la infraestructura puede ampliarse, por ello, es necesario disponer de un sistema escalable. Se estima que la empresa crezca y los estudios indican que, en 2 años, la empresa estará formada por 2.250 empleados.
- Mejorar la seguridad de la compañía. Para ello, se limitará los accesos publicados a internet. Se limitarán las comunicaciones que se abran y se controlará el tráfico que pase por el firewall con el equipo de comunicaciones de SerguPat.
- Se realizará integración con la SAN corporativa basada en NetApp. Todas las necesidades de discos de red se ofrecerán a través de la plataforma de SAN Corporativa basada en tecnología Netapp.

4.3 Diseño a realizar

Se plantea un proyecto para 2000 empleados y con posibilidad de crecimiento tanto a nivel de usuarios, como aplicaciones, clínicas o nuevas sedes. Por ello, la escalabilidad es una de las principales características que debe tenerse en cuenta en el diseño.

También, se requiere de una alta disponibilidad y tener bien fijada las soluciones antes imprevistos o fallos que pudiesen afectar al servicio.

Realizar un buen diseño, reducirá costes y ahorrará trabajo a la hora de implementar. Durante la fase piloto del proyecto, se permitirá realizar algunas correcciones que puedan mejorar y optimizar el resultado final.

4.4 Distribución y diseño capa cliente

Para agrupar y definir los puestos de usuario, se ha decidido utilizar equipos con versiones actuales, predominando Windows 10. A la hora de agruparlos se ha decidido distinguir 3 grupos diferenciados:

1. Equipos fuera de red: Estos equipos se desplegarán de forma manual y son elementos que estarán fuera de la red de la compañía. Se podrán descargar desde la página de acceso a la plataforma Citrix.
2. Equipos internos de red: Estos equipos con acceso a la red de la compañía tendrán un despliegue automático y vendrán configuración mediante el AD 2016 que se desarrollará.
3. Resto de dispositivos: El resto de “equipos” serán los dispositivos como Tablet, telefonía móvil, etc, los cuales, podrán realizar conexiones mediante el uso del Citrix Receiver.

A la hora de implementar la capa cliente se requiere utilizar una de las versiones de Citrix Receiver recientes y que sea compatible con las versiones de los puestos usuario. En este caso, se ha elegido una de las últimas versiones, Citrix Receiver 4.11, la cual, es compatible con Windows 10, 8.1, 7, 2008R2 y con servidores Windows 2012, Windows 2012R2 y Windows 2016. Esta elección depende del momento actual, ya que no tendría sentido usar versiones anticuadas para implementar un proyecto actual y nuevo.

4.5 Distribución y diseño capa acceso

Como se vio en la parte descriptiva, el Access layer depende del StoreFront y el Netscaler Gateway. Por ello, se han definido el siguiente grupo de servidores para cada caso:

Respecto al StoreFront se van a implementar los siguientes servidores:

NOMBRE	SO	DISCO C:	RAM	CPU
STOREINTB101	Windows Server 2016	50 Gb	16	4
STOREINTB202	Windows Server 2016	50 Gb	16	4
STOREEXTB101	Windows Server 2016	50 Gb	16	4
STOREEXTB202	Windows Server 2016	50 Gb	16	4

Tabla 4.2 Servidores StoreFront definidos

El nombre debe ser descriptivo y en este caso se ha optado por marcar un primer término que defina el servidor “STORE”, una segunda parte indicando si es un servidor interno (INT) o externo (EXT), un siguiente término “B1” o “B2” indicando el CPD en el que se encuentra el servidor y el número posterior “01” o “02”.

El Sistema Operativo elegido es Windows Server 2016, con un disco C: que tenga una capacidad de almacenamiento de 50Gb, memoria Ram de 16Gb y 4 CPU.

Está diseñado para ser activo/activo, estando un nodo en B1 y otro nodo en B2.

Respecto al Netscaler, se cuenta con una configuración activa/pasiva de manera que tengamos alta disponibilidad, es decir, distinto al caso del StoreFront. El sistema operativo de estos equipos es CentOS y son servidores físicos, uno en B1 y otro en B2 para tener uno por cada CPD. El Netscaler nos permitirá balancear la carga de usuarios y distribuir la carga a los servidores de StoreFront mediante el método de menor cantidad de conexiones Least Connection y el tipo de persistencia CookieInsert ambos recomendados por el proveedor.

Además, tiene como función realizar conexiones SSL de manera segura e integrar los certificados en su plataforma, importando e instalando el adecuado para cada servicio configurado. Para ello, lo primero es importar el certificado a Netscaler, esto puede realizarse mediante comandos o de manera gráfica usando la interfaz de administración.

Otra de las funciones de este elemento del Access layer, es autenticar usuarios. Para ello, se configura el Secure Ticket Authority (STA), el cual, está alojado en servidores XenDesktop y XenApp. Emite tickets de sesión en respuesta a las solicitudes de conexión. Estos tickets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de XenDesktop y XenApp.

En el caso del StoreFront permitirá que los usuarios no necesiten iniciar sesión de nuevo para acceder a sus escritorios y aplicaciones. Se adjunta una imagen con la implantación habitual de los StoreFront:

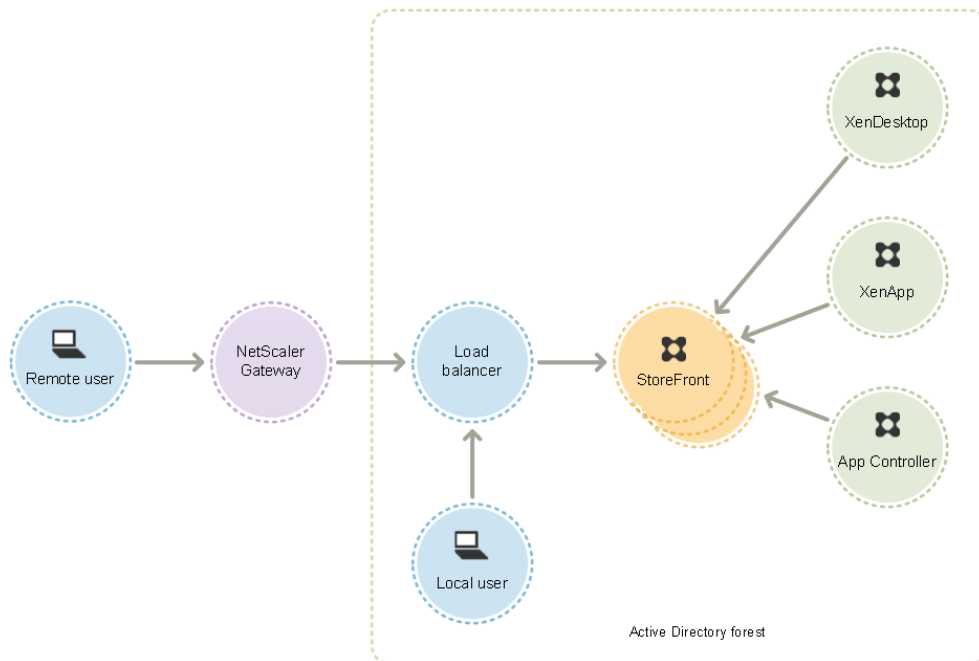


Figura 4.1 Implantación StoreFront

Los servidores StoreFront deben residir ya sea en el dominio de Active Directory que contiene las cuentas de los usuarios o en un dominio que tiene una relación de confianza con el dominio de las cuentas de usuario. Todos los servidores StoreFront pertenecientes a un grupo deben residir en el mismo dominio.

4.6 Distribución y diseño Control layer

Como se vio en los conceptos teóricos, en esta capa uno de los elementos necesarios es el servidor de licencias. Para ofrecer este servicio, el proveedor facilita la posibilidad de no hacerlo en alta disponibilidad ya que, ante cualquier fallo del servidor, se permite el uso de un periodo de gracia de 30 días, permitiendo recuperar el sistema en ese plazo de tiempo. Por ello, se ha decidido implantar el siguiente servidor:

NOMBRE	SO	DISCO C:	RAM	CPU
PROB1LICEN01	Windows Server 2016	40Gb	8	2

Tabla 4.3 Servidor de Licencias definido

Se ha incluido en B1 ya que es el CPD donde estarán los servidores activos. Se comprarán un total de 2250 licencias de tipo Xendesktop Enterprise User/device permitiendo que todos los usuarios tengan su licencia y dejando 250 libre para posibles variaciones.

El servidor de licencias, en caso de actualización, respalda el uso de productos y archivos de licencias antiguos. No obstante, los productos nuevos requieren el servidor de licencias más reciente para poder extraer correctamente las licencias.

Otro de los elementos de esta capa es el delivery controller, el cual, es la pieza fundamental y que va a permitir distribuir aplicaciones y escritorios a los usuarios. En este caso, se ha decidido implantar los siguientes servidores:

NOMBRE	SO	DISCO C:	RAM	CPU
PROB1CONT01	Windows Server 2016	50Gb	16	4
PROB1CONT02	Windows Server 2016	50Gb	16	4
PROB1CONT03	Windows Server 2016	50Gb	16	4
PROB1CONT04	Windows Server 2016	50Gb	16	4
PROB2CONT01	Windows Server 2016	50Gb	16	4
PROB2CONT02	Windows Server 2016	50Gb	16	4
PROB2CONT03	Windows Server 2016	50Gb	16	4
PROB2CONT04	Windows Server 2016	50Gb	16	4

Tabla 4.4 Servidores Delivery Controller definidos

Estos servidores permitirán realizar las funciones de bróker/controller. También, se instalará en ellos el Citrix Studio y Citrix director, herramientas que se vieron en el apartado teórico.

Además de esto, será necesario configurar la base de datos Citrix. Está formada por 3 SQL Server 2016:

- Sitio: También conocida como Configuración del sitio, esta base de datos almacena la configuración activa del sitio, el estado actual de la sesión y la información de conexión.
- Registro de configuración: También conocida como Registro, esta base de datos almacena información acerca de actividades de tipo administrativo y los cambios de configuración del sitio. Esta base de datos se usa cuando la función Registro de configuración está habilitada (opción predeterminada).
- Supervisión: Esta base de datos almacena los datos que utiliza Director, como la información de conexión y de sesión.

Todos los Delivery Controller se comunican con la BBDD del sitio. Un Controller se puede desconectar o apagar sin que esta acción afecte a los otros Controllers del sitio. No obstante, esto significa que la base de datos del sitio representa un punto único de fallo. Si el servidor de base de datos da error, las conexiones existentes seguirán funcionando hasta que el usuario cierre sesión o se desconecte. En cambio, no se podrán establecer conexiones nuevas si el servidor de base de datos no está disponible, excepto en algunos casos cuando está configurada la concesión de conexiones.

Otro de los elementos clave en la arquitectura es el directorio activo, donde los equipos y usuarios van a estar agrupados en unidades

organizativas (OU). Además, estarán configuradas bajo una GPO diferente que permitirá diferenciar perfiles de usuario y aplicaciones y servirá para optimizar cada aplicación.

A nivel de estructura, se configurará una OU principal y a partir de esta se irán definiendo nuevas OU para ir definiendo la función de los servidores o grupos de seguridad que cuelguen de la unidad organizativa. Por ello, será necesario definir OU para cuentas de servicio, cuentas de usuario en función de la clínica o sede donde se encuentren, OU para administración, OU para equipos VDI, OU para servidores de aplicaciones, etc.

Cada unidad organizativa creada tendrá una función y sobre ella, aplicarán GPO iguales y otras diferentes. En el caso de Citrix, realiza algunas recomendaciones como cortar las herencias para que se obtenga un control mayor sobre lo que ocurre en los equipos, grupos o usuarios, esta recomendación contrasta con la de Microsoft, que recomienda no usar el corte de herencias. A parte, se recomienda el modo loopback que reemplaza las políticas de usuario por las de equipo y viceversa. A la hora de elegir este modo, existen dos formas diferentes de aplicarlo:

- Combinar: Mezcla las GPO de usuario que normalmente se le aplican a estos con las GPO de usuarios definidas para los servidores de la OU servidores.
- Sustituir: Las GPO que normalmente se le aplican a los usuarios no serán tenidas en cuenta. Solo se aplicarán las GPO de usuarios vinculadas a la OU servidores.

Por tanto, permite asignar GPO de usuarios a todos los servidores destino sin preocuparnos en que OU está el usuario, ni cuales son las directivas que tiene establecidas en origen.

Para aplicar este método, se debe realizar en la ruta siguiente:

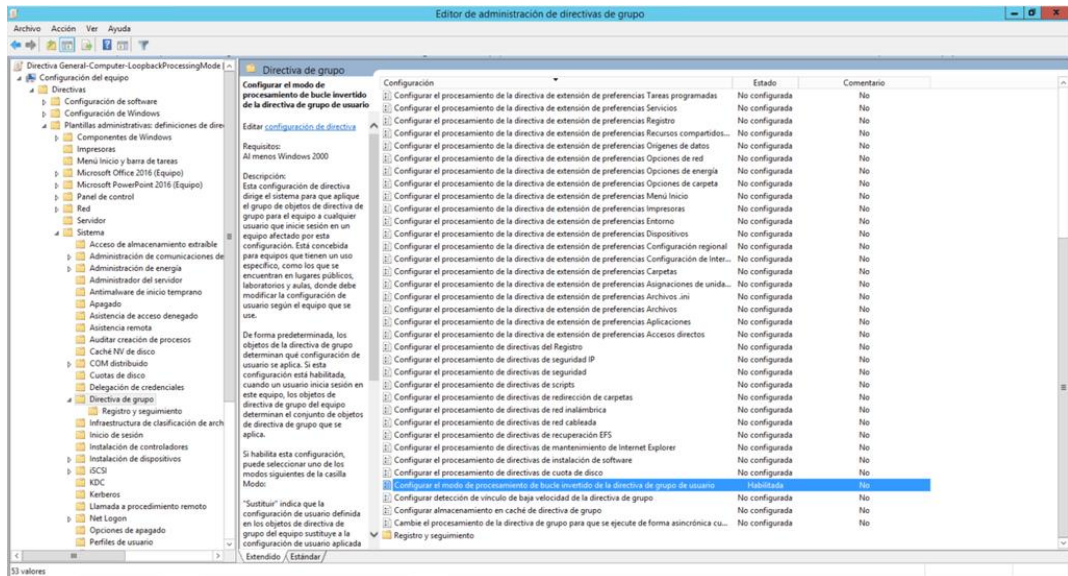


Figura 4.2 GPOs del Directorio Activo

Y se debe aplicar la configuración deseada en la siguiente imagen:

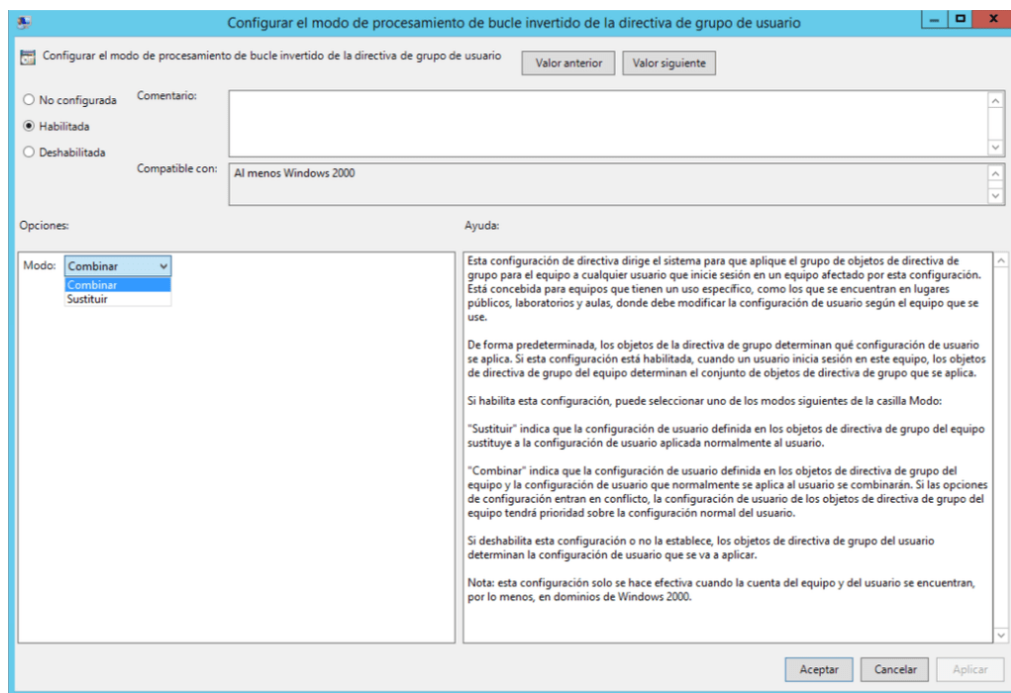


Figura 4.3 Configuración de bucle invertido

También es importante la configuración de usuario y el perfil en los servidores Citrix, por ello, se recomienda usar Profile Management. Citrix recomienda instalar la misma versión de Profile Management en todos los dispositivos de usuario y agregar la misma versión del archivo .adm o .admx a cada objeto de directiva de grupo en todos los controladores de dominio. De esta manera, se evita que se dañen los datos de los perfiles, que puede ocurrir cuando existen distintas estructuras del almacén de usuarios. Se va a definir un perfil de usuario con un tamaño máximo de 120Mb, es decir, teniendo en cuenta unos 2.000 usuarios, un total de 240Gb.

Otro punto importante es la asignación de IPs a los equipos, el cual, se va a realizar mediante DHCP. Para ello, será necesario crear un Scope con un rango de IPs a asignar para cuando se creen servidores de aplicaciones o VDIs. También, se podrán realizar reservas de IPs si es necesario mediante el nombre del equipo y el uso de la MAC.

En las políticas de usuario, será necesario aplicar configuraciones de tiempo por inactividad. En este caso, se ha decidido fijar un tiempo de 3 horas para servidores de aplicaciones para poner al usuario en disconnected y 1 minuto para hacer logoff de la sesión desconectada previamente. Este tiempo, se puede modificar posteriormente o para servidores concretos si se estima oportuno.

A nivel de VDIs, también se ha decidido fijar un tiempo de inactividad de 3 horas para desconectar la sesión y 1 minuto para deslogar la sesión desconectada.

En el StoreFront, se ha decidido marcar un tiempo inferior, estimado en 30 minutos. Pasado este tiempo de inactividad, la sesión se cerrará.

A parte, se ha decidido aplicar una política de reinicios de la plataforma durante la noche, donde una noche se reiniciarán los servidores pares de la granja Citrix y otra los impares. Esta configuración, se realizará mediante WorkersGroups y políticas Citrix de XenApp. El principal motivo es que se vayan aplicando las configuraciones necesarias y parches que se vayan instalando en la granja. Es posible que algún servidor de aplicación no pueda incluirse en esta política para evitar que se reinicie. Esto lo marcará si alguna aplicación no puede o debe reiniciarse porque necesite estar 24 horas encendida para lanzar informes o procesos más pesados de lo habitual.

Además de estas configuraciones y políticas, se deberá aplicar algunas tareas programadas que mejoren y optimicen el rendimiento. Una de ellas, es el borrado de perfiles de usuario en desuso. Esto permitirá liberar espacio en los servidores Citrix que no esté siendo usado, optimizando y usando el almacenamiento adecuado.

En esta capa, también será necesario configurar el antivirus, donde se ha elegido MacAfee y se desplegará una de las versiones actuales del momento. Se aplicarán algunas de las recomendaciones del fabricante:

- Instalar y escanear en eventos de escritura o cuándo los ficheros son modificados. Por defecto se escanea en las acciones de lectura y escritura.
- No escanear el disco de Pagefile y el directorio de Print Spooler. En algún momento, puede añadirse algún directorio extra que recomiende Citrix.

- Escanear los discos locales y dejar deshabilitado el escaneo a nivel de red.

4.7 Distribución y diseño Resource layers

Como se indicó con anterioridad en puntos anteriores, para los escritorios de los usuarios se va a usar Windows 10 como principal sistema operativo. En algunos casos, podrán desplegarse alguno distinto por algún motivo particular, pero por plantilla el puesto de usuario tendrá Windows 10. Dentro de los escritorios diseñados, se van a distinguir 3 tipos:

- Escritorios para empleados de dirección y TI: En este caso, los usuarios van a trabajar con sus VDIs y van a necesitar guardar cambios y configuraciones. Estos usuarios van a ser VIP y se tendrá que tener un especial cuidado con sus equipos, por lo tanto, es necesario separar tanto equipo como usuarios del resto.
- Escritorios estáticos: Estos equipos estarán asignados en un puesto físico habitual donde el empleado trabaje a diario desde este punto. El usuario podrá guardar configuraciones a diario.
- Escritorios dinámicos: Estos equipos estarán dedicados para empleados que puedan ir variando y que no siempre estén en el puesto. Serán equipos virtuales donde no será necesario guardar cambio y el mismo equipo lo pondrán usar distintas personas.

Por ello, para XenDesktop, se estima que sean necesarios 1.500 equipos que estarán divididos en los 3 escritorios comentados con anterioridad.

Las VDIs a desplegar van a tener una memoria RAM de 4Gb y serán Windows 10 con 2 CPUs. Se ha estimado que serán necesarias 1000 VDIs estáticas, 400 VDIs dinámicas y 100 VDIs VIPs. Lógicamente, estos números podrán variar y modificarse según necesidades ya que el diseño tendrá como una de sus características principales, permitir la escalabilidad y modificar el dimensionamiento según necesidades del momento. Estos equipos, van a tener un disco C: de 50Gb.

Además, será necesario crear un Delivery Group por diseño de equipo, es decir, 3 en total. De esta manera, los usuarios podrán acceder a los recursos de la granja. Por ello, se ha decidido implementar los siguientes Delivery Group:

- XenD_VIP: Para publicar equipos VIP.
- XenD_Dinamic: Para publicar equipos dinámicos.
- Xend_Static: Para publicar equipos estáticos.

Además del XenDesktop, es necesario planificar el despliegue de equipos XenApp, para ello se usarán equipos Windows Server 2016. En

estos servidores, se realizará la instalación de los aplicativos necesarios para las sedes y clínicas de la compañía.

Para realizar un correcto dimensionamiento de XenApp, hay que tener en cuenta el consumo y las características de una sesión de usuario. Por ello, se han tomado como referencia los siguientes valores:

- Paquete office: Se estima que consuma 120Mb de RAM.
- Outlook: Se estima que consuma 150Mb de RAM.
- Aplicación instalada: Esto variará en función de la aplicación y no podemos tener una estimación aproximada.
- Sesión de usuario: Una sesión inactiva tiene un consumo de 60Mb de RAM.
- Internet Explorer: Tiene un consumo de 70Mb de RAM.

Además de esto, hay que tener en cuenta que los usuarios pueden abrir aplicaciones simultaneas a la vez aunque no es lo recomendable, no se puede controlar el uso que le dé el usuario, por lo tanto, hay que dejar un margen considerable para realizar la estimación de consumo.

Con todo esto, se ha realizado una estimación para el uso que harán los 500 usuarios que consuman XenApp, es decir, los restantes que no hacen uso de VDIs. Por ello, se ha tomado como consumo por usuario 700Mb, esto es así de los datos ofrecidos con anterioridad y de una estimación realizada para el uso de 2 aplicaciones corporativas simultáneas con un consumo de 100Mb de RAM y haber dejado un margen más de 100Mb libres. Es por ello, que para 500 usuarios se obtiene lo siguiente:

$$500 \text{ usuarios} \times 700\text{MB} = 350\text{Gb}$$
$$350\text{Gb} / 1,024 = 341,18\text{Gb}$$

Debemos tener en cuenta, que esto es una estimación al alza y que durante la fase piloto y de pruebas se podrán ajustar estos valores teniendo unos resultados más exactos del dimensionamiento a realizar.

Con todo ello, y teniendo en cuenta que el sistema operativo tiene un consumo de unos 2Gb de RAM, que el servidor se va a desplegar con 24Gb de RAM, se obtiene que:

$$24\text{Gb} - 2\text{Gb} = 22\text{Gb}$$
$$22\text{Gb}/0,700\text{Gb} = 31,4 \text{ sesiones por máquina}$$

Por ello, y redondeando a 31 sesiones de usuario como máximo en cada máquina virtual, se obtiene, que para 500 usuarios se necesitan 16,129 servidores, es decir, volviendo a redondear al alza, 17 servidores para la granja XenApp. Estos servidores serán del tipo descritos a continuación en la siguiente tabla:

NOMBRE	SO	DISCO C:	DISCO PAGINACIÓN	CPU
CTXB1APP01	Windows Server 2016	50Gb	20Gb	4

Tabla 4.5 Servidores XenApp diseñados

Como en las VDIs será necesario asignarle un Delivery Group que en este caso se ha denominado Xen_App para el despliegue de servidores de aplicación.

4.8 Distribución y diseño Hardware layer

La plataforma se va a desplegar en el CPD1 de Barcelona, es decir, en el activo. Hay que tener que todo el almacenamiento estará replicado en el CPD2 de Barcelona y para cualquier imprevisto se podría realizar el balanceo de la granja al CPD2.

A nivel de almacenamiento y con todo lo visto con anterioridad, se va a requerir lo siguiente:

Tipo de servidor	Almacenamiento
XenApp	1190Gb
XenDesktop	75000Gb
Usuarios	240Gb
Licenciamiento	40Gb
Delivery Controller	400Gb
StoreFront	200Gb
BBDD	50Gb

Tabla 4.6 Resumen de requerimientos

Esto es asumible en vista a la infraestructura diseñada, teniendo en cuenta las cabinas NetApp y que se disponen de 30 host ESX para el rendimiento de las máquinas.

5. Implementación

5.1 Implementación a realizar

En la siguiente figura se muestra un esquema con del diseño que he planteado, tanto para el acceso externo como interno:

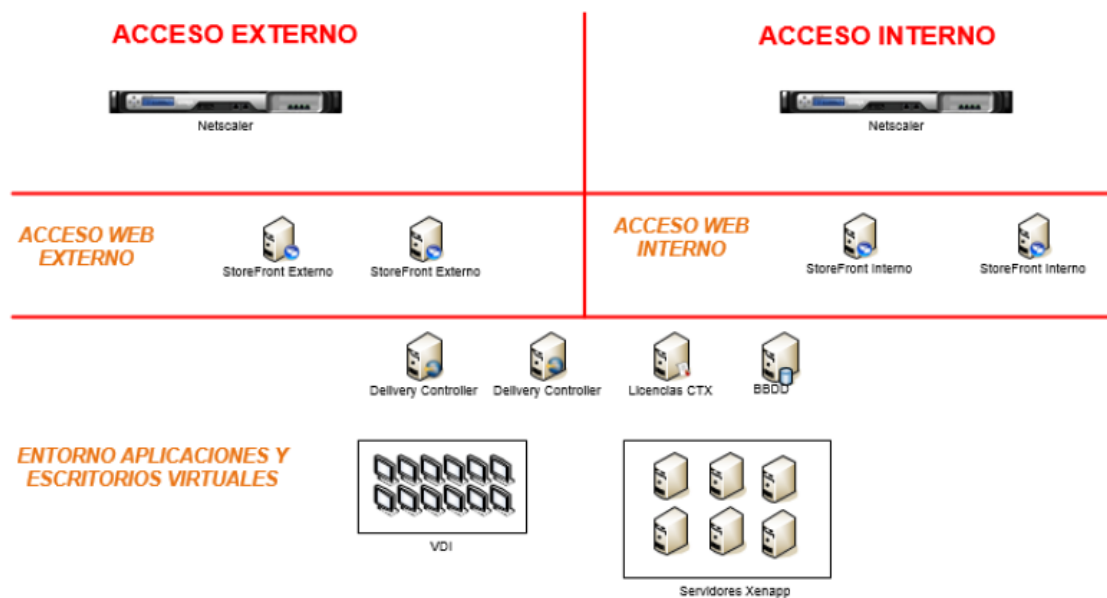


Figura 5.1 Implantación de forma gráfica

5.2 Implementación del StoreFront y Netscaler Gateway

Lo primero sería comprobar que el StoreFront este unido al dominio de Microsoft Active Directory. Este, contiene las cuentas de los usuarios o a un dominio que tiene una relación de confianza con el dominio de las cuentas de usuario. Como nota importante, cabe destacar que un StoreFront no se puede instalar en un controlador de dominio. En nuestro caso, se han diseñado servidores específicos para ello.

Para realizar la instalación es requisito previo tener instalado el .NET Framework 4.5.1.

Para realizar la configuración del storeFront se incluye un diagrama con los pasos a seguir:

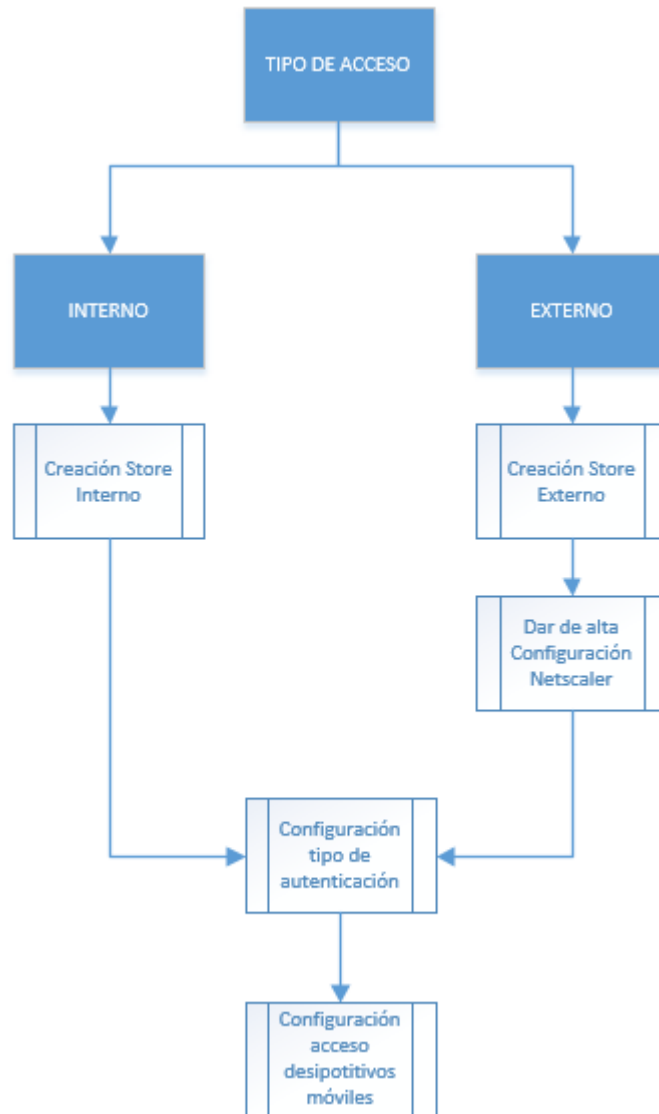


Figura 5.2 Diagrama implementación StoreFront

Para iniciar la instalación debemos configurar e instalar un certificado en Netscaler para tener realizar la conexión en modo seguro SSL. Para ello, se deben realizar los siguientes pasos:

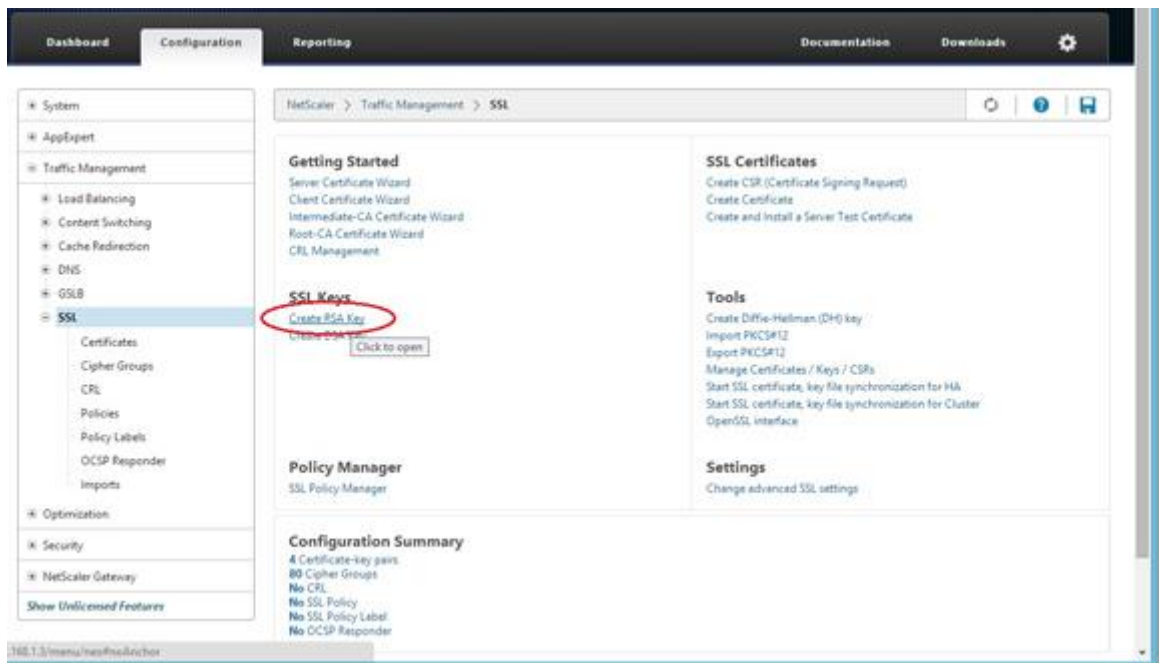


Figura 5.3 Create RSA Key

Se debe pulsar en Create RSA Key y se avanza a la siguiente pantalla que debe ser cumplimentada con los datos requeridos:

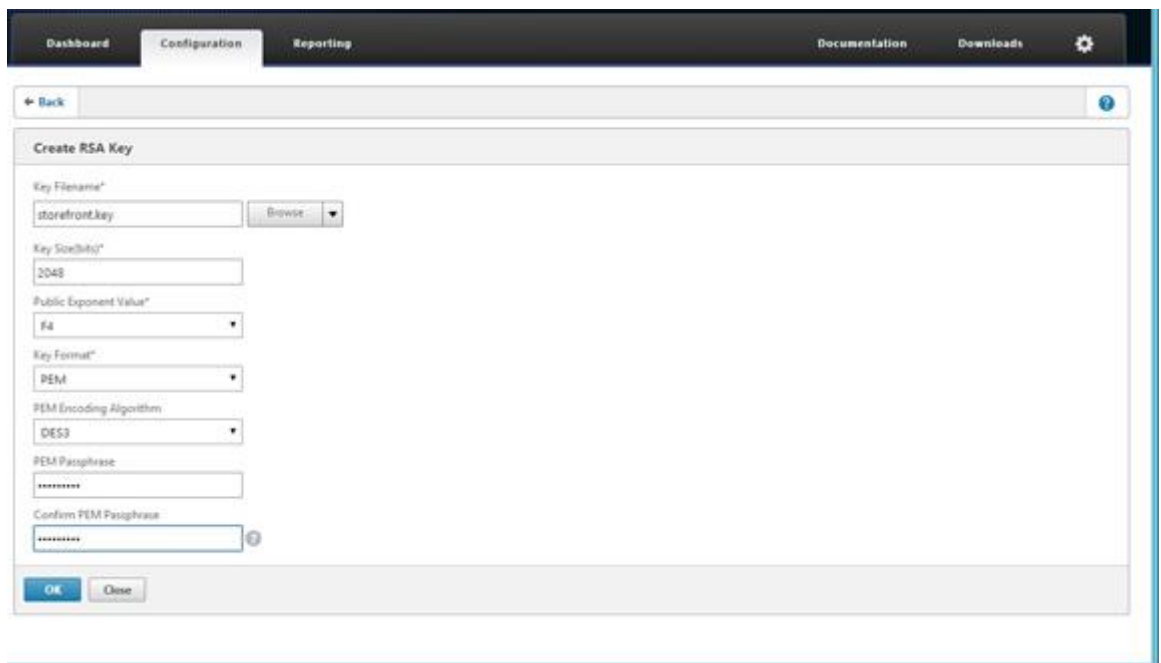


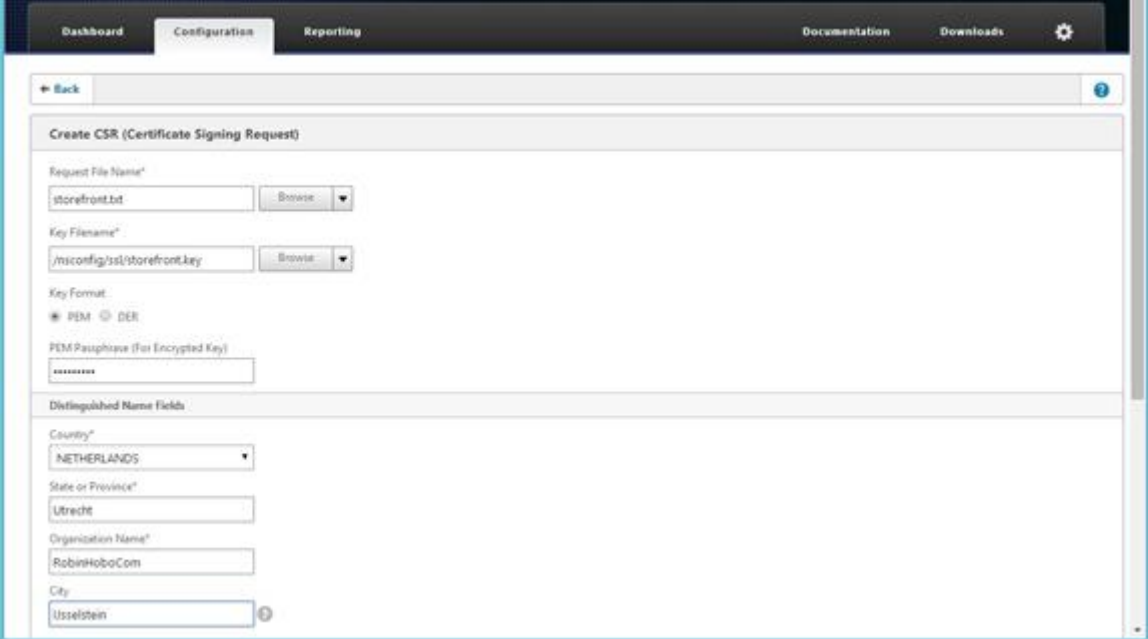
Figura 5.4 Cumplimentar Create RSA Key

Se ha rellenado con los siguientes datos:

- Key Filename: storefront.key
- Key Size (bits): 2048
- Public Exponent Value: F4
- Key Format: PEM
- PEM Encoding Algorithm: DES3

- PEM Passphrase: password elegida
- Verify Passphrase: La misma de arriba

Se pulsa en OK y posteriormente, se crea un CSR:



The screenshot shows a web interface for creating a CSR. The form is titled "Create CSR (Certificate Signing Request)". It has a "Back" button at the top left. The form contains the following fields:

- Request File Name***: storefront.txt
- Key File Name***: /usr/config/ssl/storefront.key
- Key Format**: PEM DER
- PEM Passphrase (For Encrypted Key)**: [password]
- Distinguished Name Fields**:
 - Country***: NETHERLANDS
 - State or Province***: Utrecht
 - Organization Name***: RobinHoboCom
 - City**: Usselstein

Figura 5.5 Complimentar CSR

En este caso, con los siguientes datos:

- Request File Name: storefront.txt
- Key File Name: Se navega hasta el fichero .key del paso anterior
- Key Format: PEM
- PEM Passphrase (For Encrypted Key): Password elegida en el paso anterior

REM DER

PEM Passphrase (For Encrypted Key)

Distinguished Name Fields

Country*

NETHERLANDS

State or Province*

Utrecht

Organization Name*

RobinHoboCom

City

Usselstein

Email Address

admin@hobo.lan

Organization Unit

IT

Common Name

storefront.hobo.lan

Attribute Fields

Challenge Password

Company Name

RobinHoboCom

OK Close

Figura 5.6 Datos a cumplimentar para certificado storefront.segurPat.2k3

- Country: España
- State or Province: Cataluña
- Organization Name: Nombre Compañía
- City: Barcelona
- Email Address: clinica@segurPat
- Organization Unit: SegurPat
- Common Name: storefront.segurPat.2k3
- Challenge Password: Password a elegir
- Company Name: SegurPat

Se pulsa en OK y quedaría el certificado instalado. Posteriormente, sería necesario descargarlo y firmarlo por la CA de la compañía. Para ello, pulsar en Manage Certificates / Keys / CSRs:

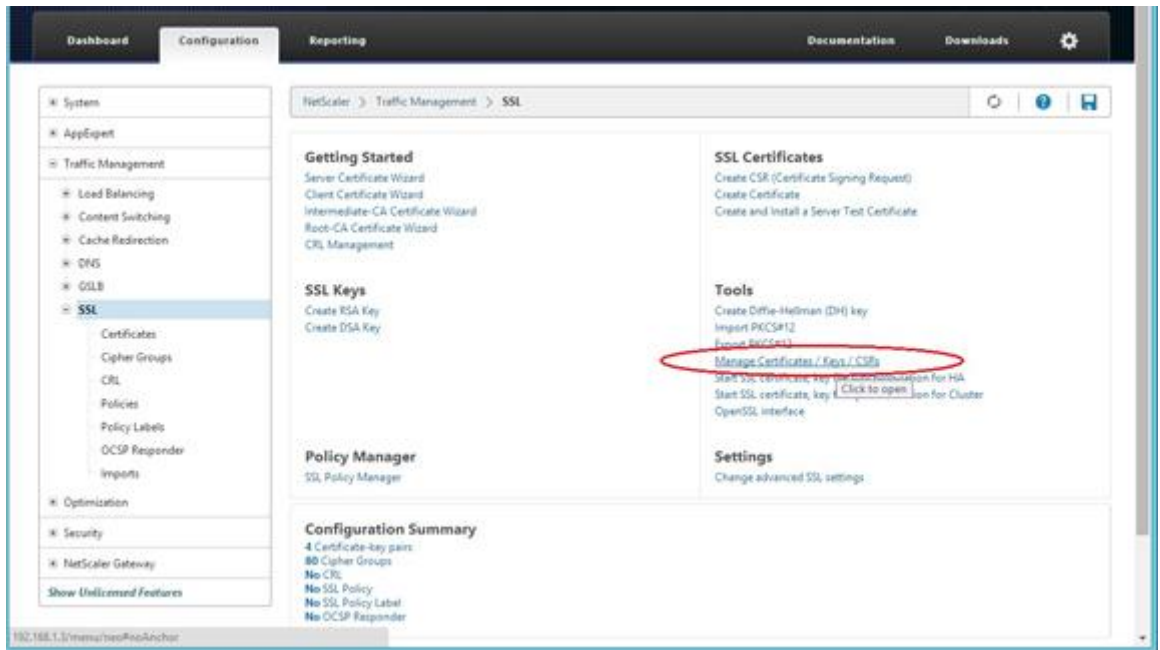


Figura 5.7 Panel Netscaler SSL

Y se descarga el fichero creado, storefront.txt:

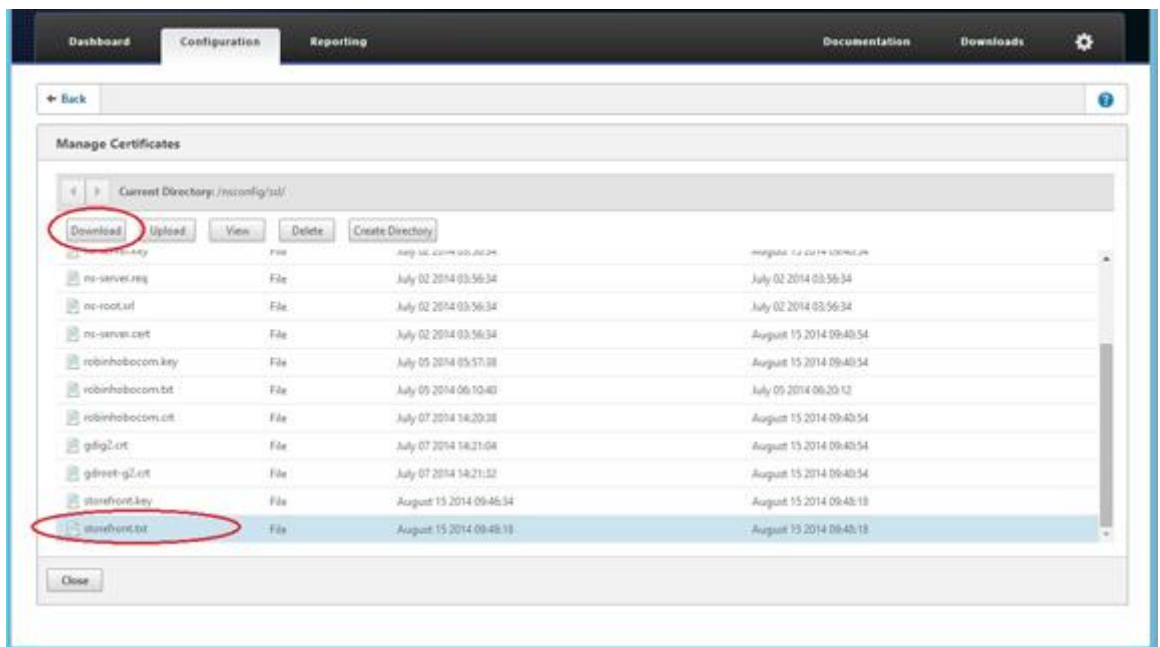


Figura 5.8 Certificados .txt instalados

Una vez se obtenga el fichero, es necesario ir a la página de nuestra CA y realizar los pasos firmar el certificado. Una vez firmado, hay que realizar la instalación en el certificado. Para ello, hay que ir al siguiente apartado, Traffic Management > SSL > Certificates y pulsar en instalar:

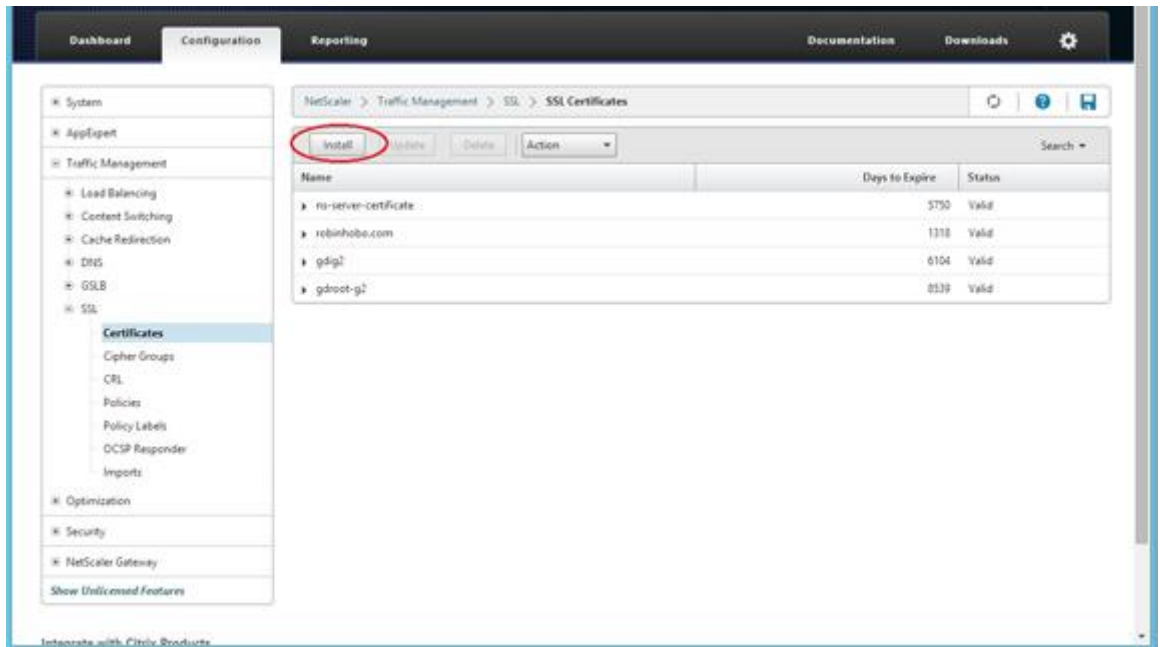


Figura 5.9 Panel de instalación certificado

Se rellenan los datos solicitados para la CA y se da a instalar de nuevo:

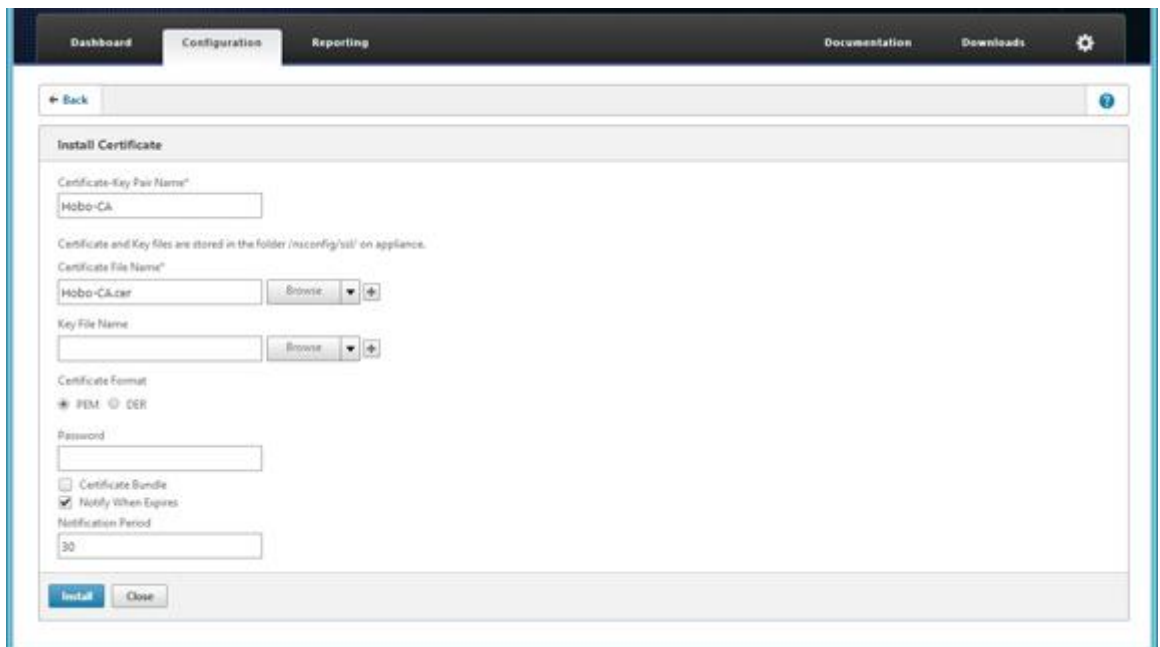


Figura 5.10 Datos a cumplimentar para instalar CA

Una vez instalada la CA, se vuelve a dar a instalar y se rellenan los siguientes datos de nuevo:

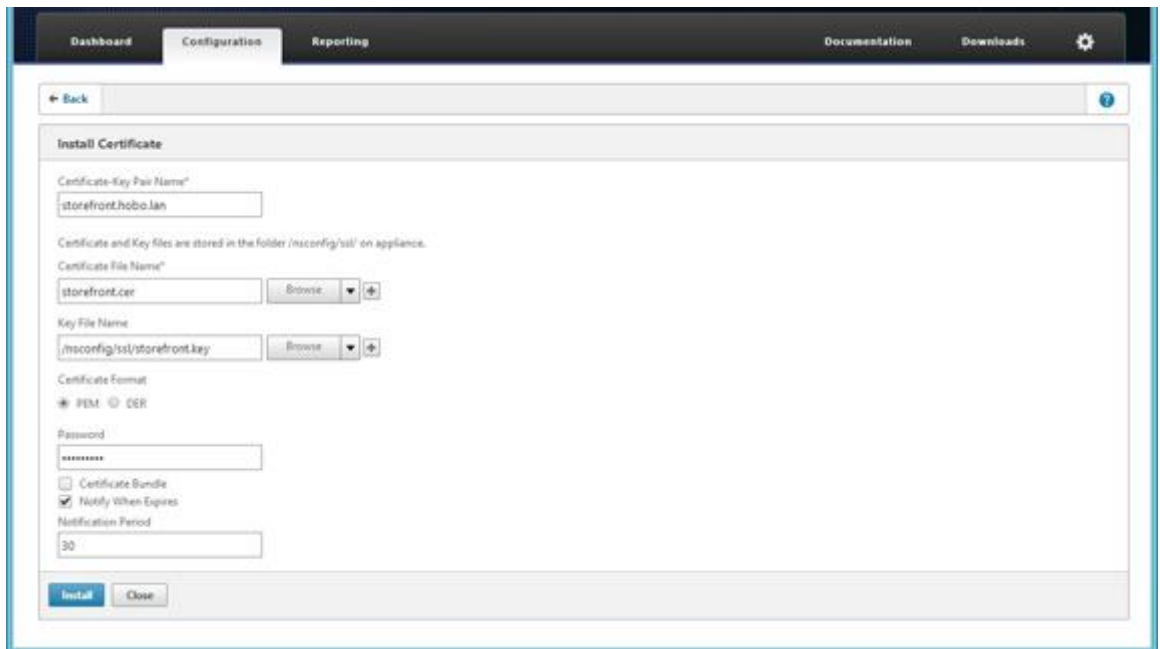


Figura 5.11 Datos a cumplimentar para instalar certificado

En esta ocasión, los datos deben ser los del storefront. Una vez instalado, se debe linkar a la CA, para ello se debe pulsar en “link”:

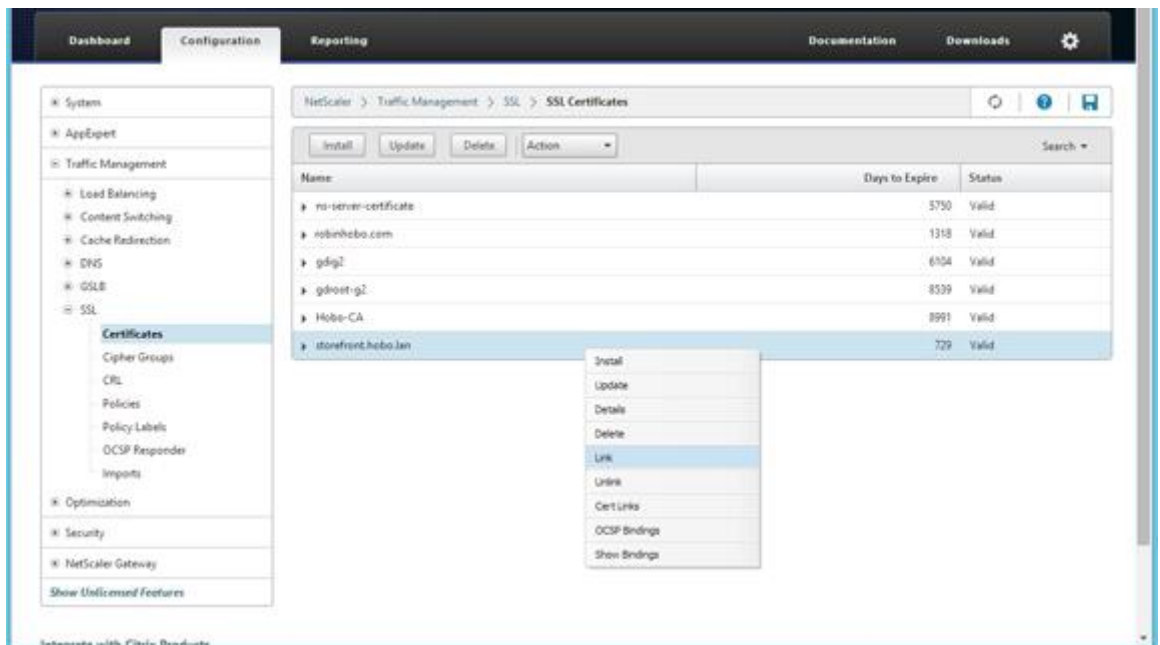


Figura 5.12 Como linkar certificado con CA

Y asignarle la CA.

Una vez instalado el certificado con su CA, se procede a realizar el paso de instalación del StoreFront, en este caso, se ha elegido la versión 2.5.2 y debe instalarse en todos los servidores que vayan a ser usados para esta tarea. Destacar, que esta instalación es válida para los que hacen la función de conexiones internas y externas, no sería necesario distinguir entre ellos.

En primer lugar, se debe ejecutar el .exe y aceptar la licencia y condiciones de uso, para posteriormente, pulsar en instalar y seguir los pasos con “siguiente”. No se adjuntan capturas ya que es una instalación bastante simple.

Una vez realizada la instalación de la consola, se debe incluir el certificado en el IIS.

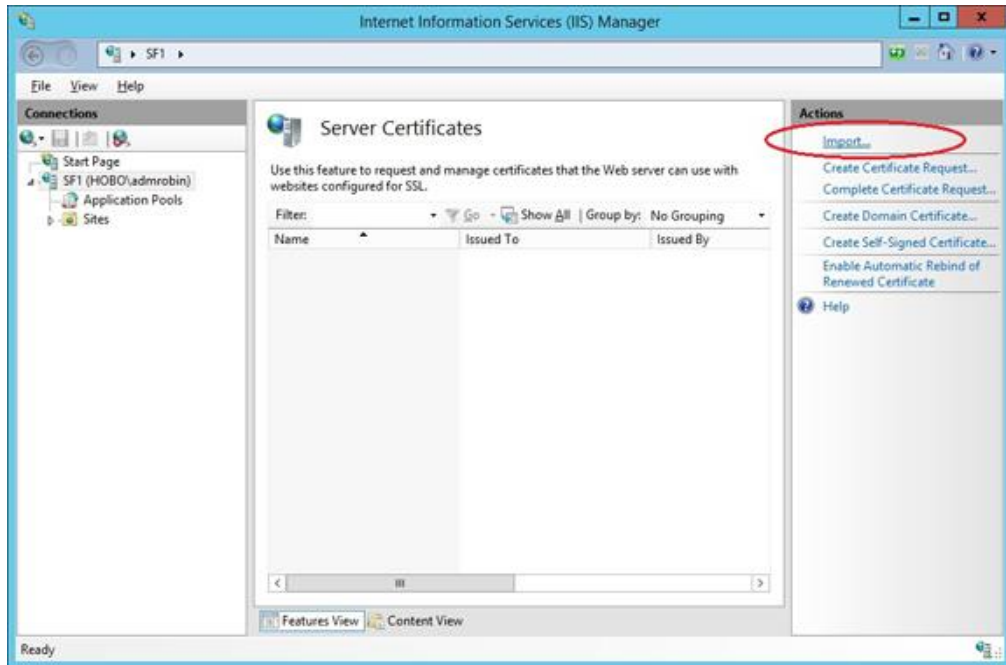


Figura 5.13 Configuración IIS

Y realizar la instalación del binding correspondiente:

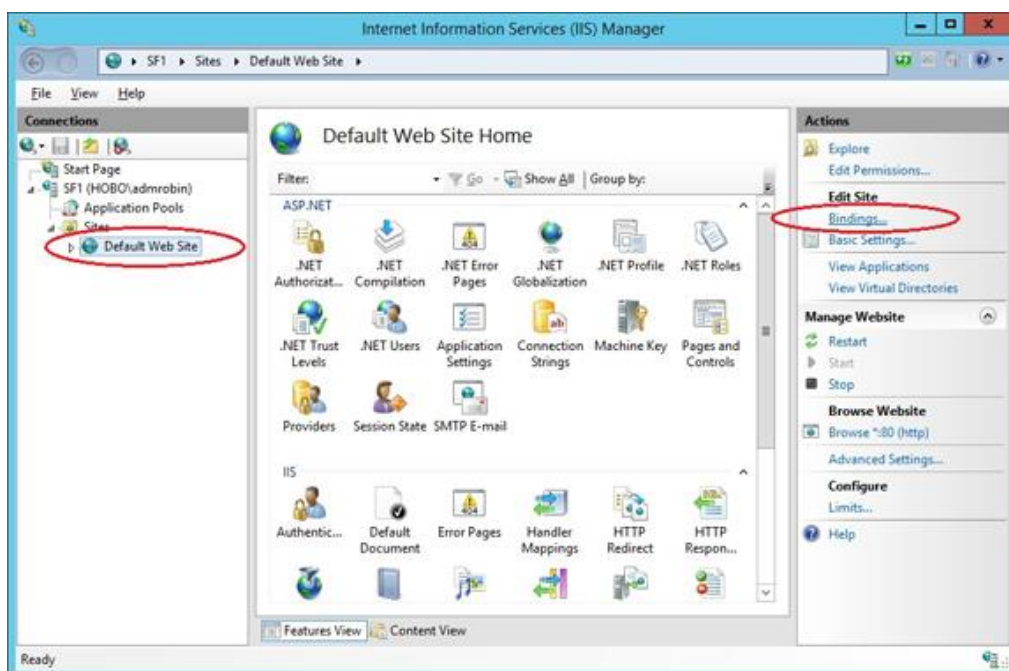


Figura 5.14 Binding para insertar certificado

Una vez se haya instalado el certificado y configurado el IIS, se debe abrir la consola del StoreFront y crear dos stores, uno para la conexión interna y otro para la externa:

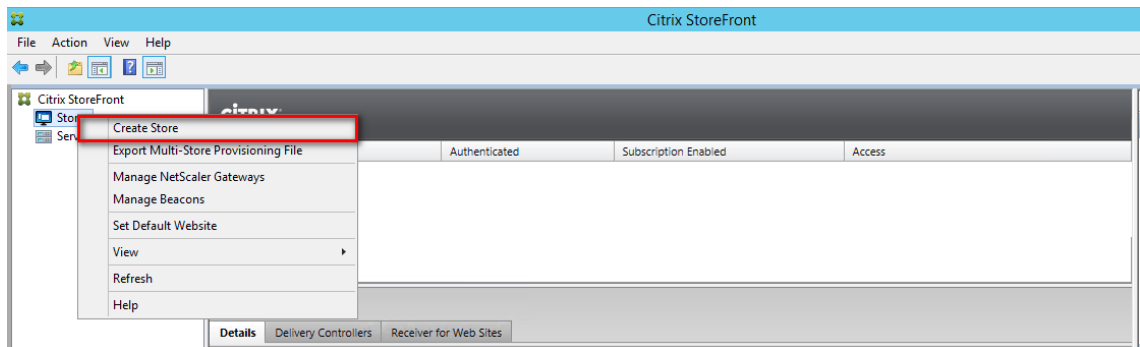


Figura 5.15 Crear Store en consola StoreFront

La creación es sencilla y se deben seguir los pasos que va dando la instalación, marcando el nombre definido para cada uno de ellos:

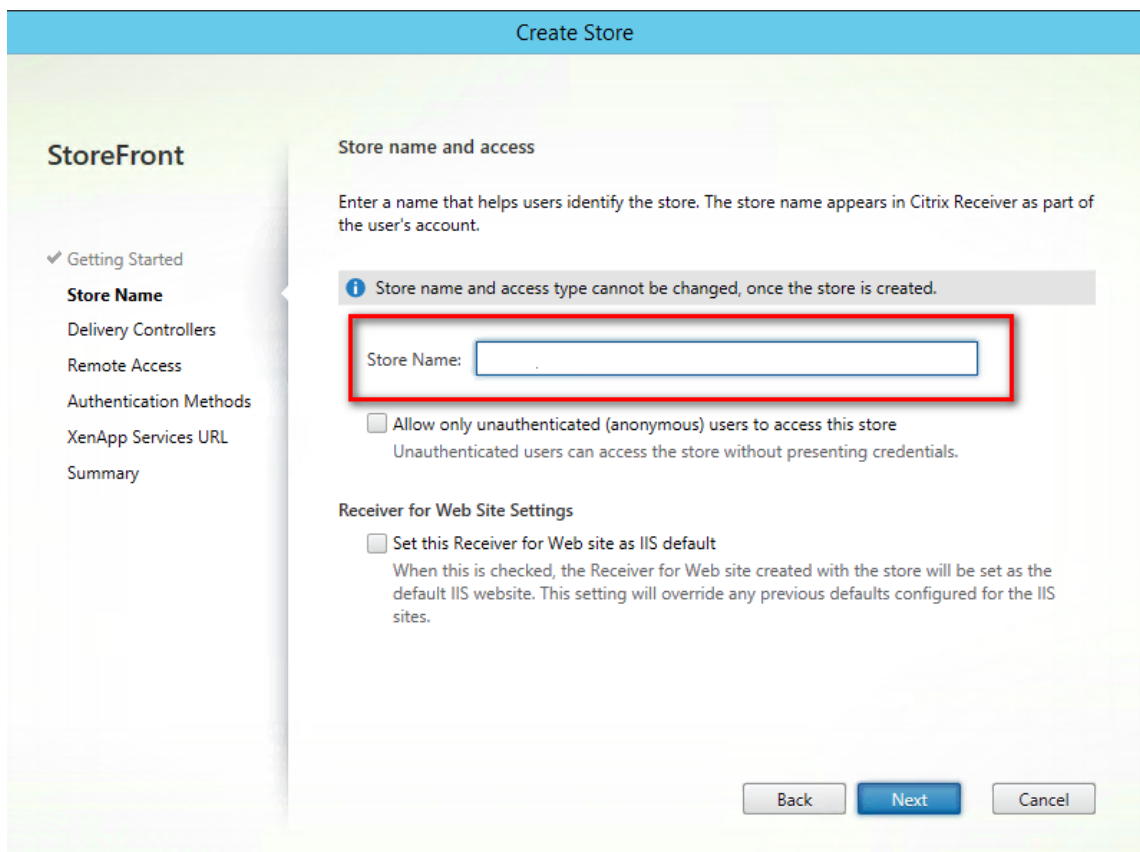


Figura 5.16 Nombre del Store a crear

En el segundo paso se añaden los Delivery Controller:

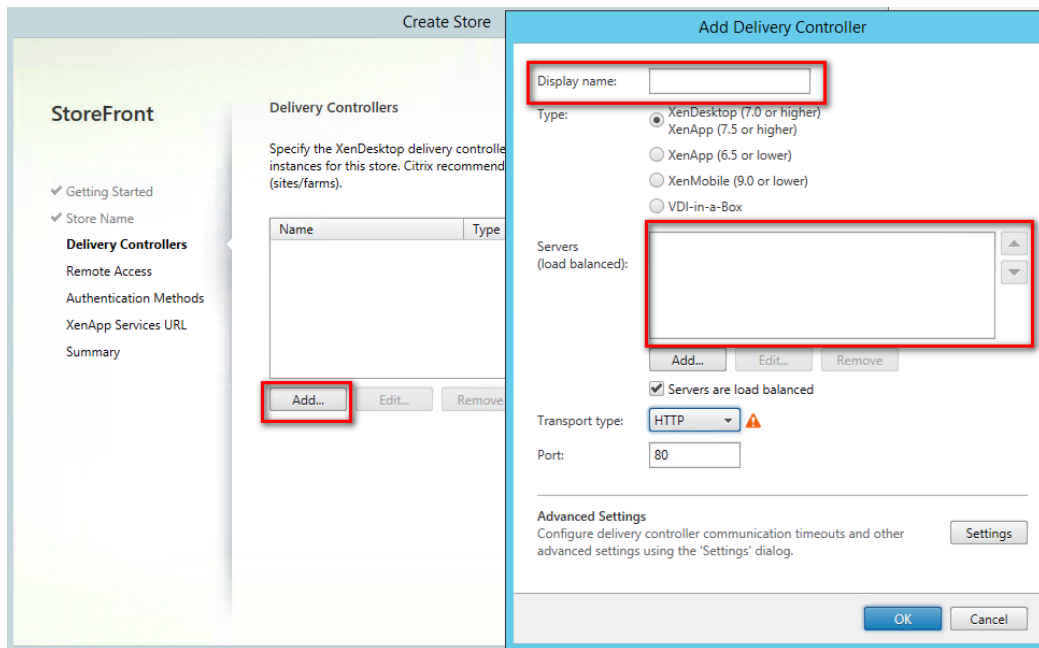


Figura 5.17 Añadir Delivery Controller

Para las conexiones internas y externas en el apartado de “Remote Access” hay una diferencia, para conexiones internas no marcamos la opción “Enable Remote Access” y para conexiones externas si se marca. En este caso, se adjuntan capturas para la configuración externa, puesto que esta parte es distinta y hay que añadirlo también en el Netscaler desde el que se accederá externamente:

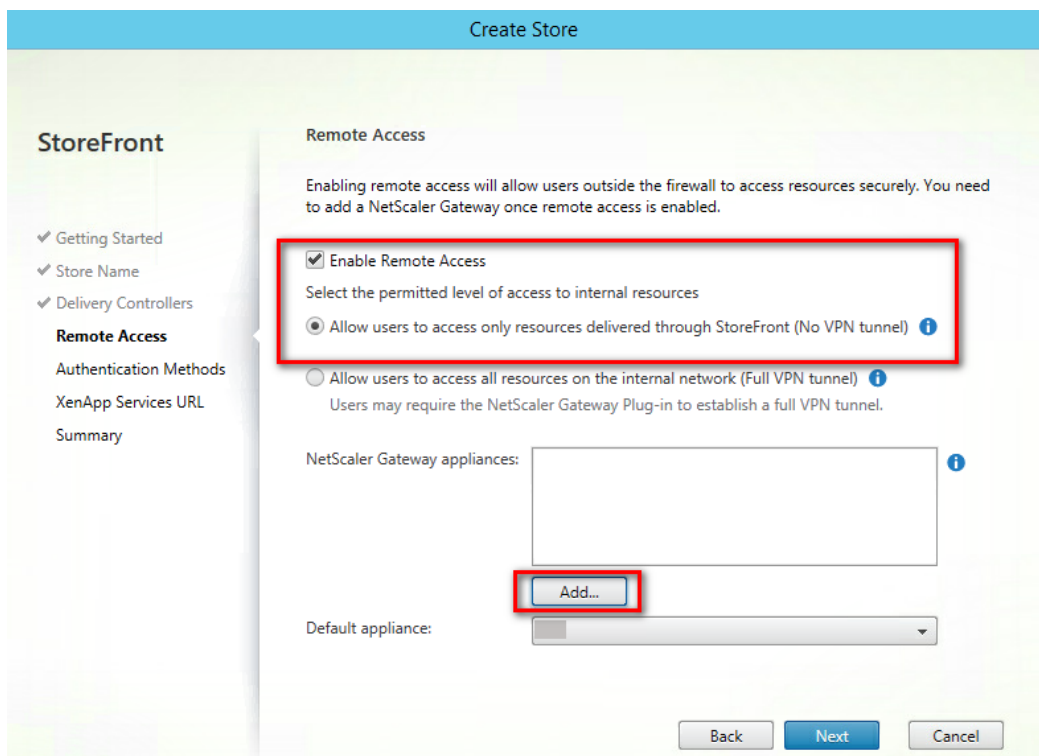


Figura 5.18 Remote Access en conexión externa

Pulsando en “Add” añadimos el “display name”, por ejemplo, NetscalerExt y la URL de acceso externa, por ejemplo, <https://conexion.segurPat.com>. Se adjunta captura:

The screenshot shows the 'Add NetScaler Gateway Appliance' configuration page. The left sidebar is titled 'StoreFront' and has 'General Settings' selected. The main content area is titled 'General Settings' and contains the following fields:

- Display name:** An empty text input field.
- NetScaler Gateway URL:** A text input field containing the value `https://NetScalerGatewayFQDN`.
- Usage or role:** A dropdown menu with the selected option 'Authentication and HDX routing'.

At the bottom right of the page, there are 'Next' and 'Cancel' buttons.

Figura 5.19 Añadir Netscaler Gateway

Después, es necesario añadir los servidores Delivery controller:

The screenshot shows the 'Add NetScaler Gateway Appliance' configuration page, specifically the 'Secure Ticket Authority (STA)' section. The left sidebar is titled 'StoreFront' and has 'Secure Ticket Authority' selected. The main content area is titled 'Secure Ticket Authority (STA)' and contains the following elements:

- Secure Ticket Authority URLs:** A large empty text area with up and down arrow buttons on the right.
- Buttons:** 'Add...', 'Edit...', and 'Remove' buttons are located below the URL list. The 'Add...' button is highlighted with a red box.
- Options:**
 - Load balance multiple STA servers
 - Bypass failed STA for: 1 hours 0 minutes 0 seconds
 - Enable session reliability
 - Request tickets from two STAs, where available

At the bottom right of the page, there are 'Back', 'Next', and 'Cancel' buttons.

Figura 5.20 Secure Ticket Authority

El siguiente punto, es para configurar la forma de autenticar usuarios externos, que, en este caso, será mediante el método Callback. Será necesario, una VIP (Virtual Server IP) que comunicará con los servidores, en este caso, 10.98.6.20. También hay que añadir la URL configurada anteriormente <https://conexion.segurPat.com> para verificar de donde provienen las peticiones:

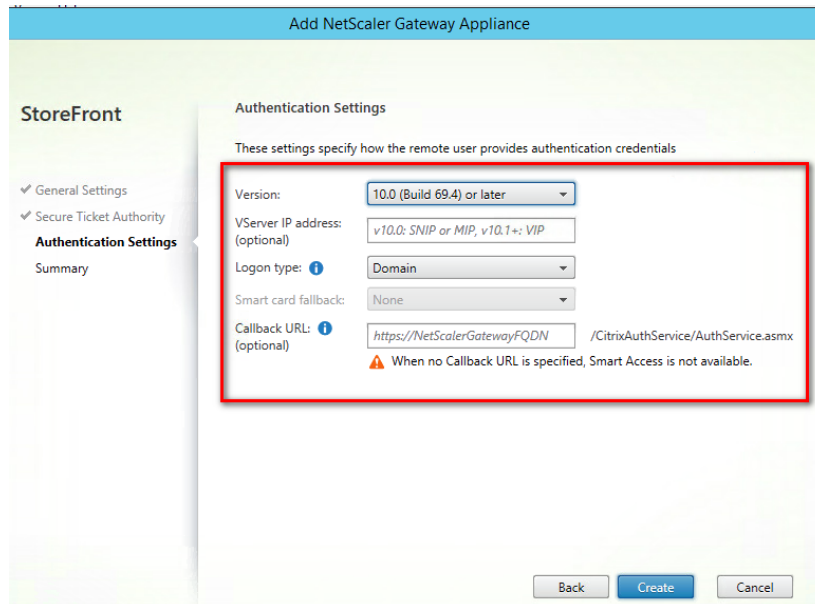


Figura 5.21 Autenticación StoreFront

A partir de este paso, la configuración del StoreFront interno y externo vuelve a ser igual.

Para autenticar los usuarios, se va a usar el dominio y el AD, por ello, es necesario marcar las siguientes opciones:

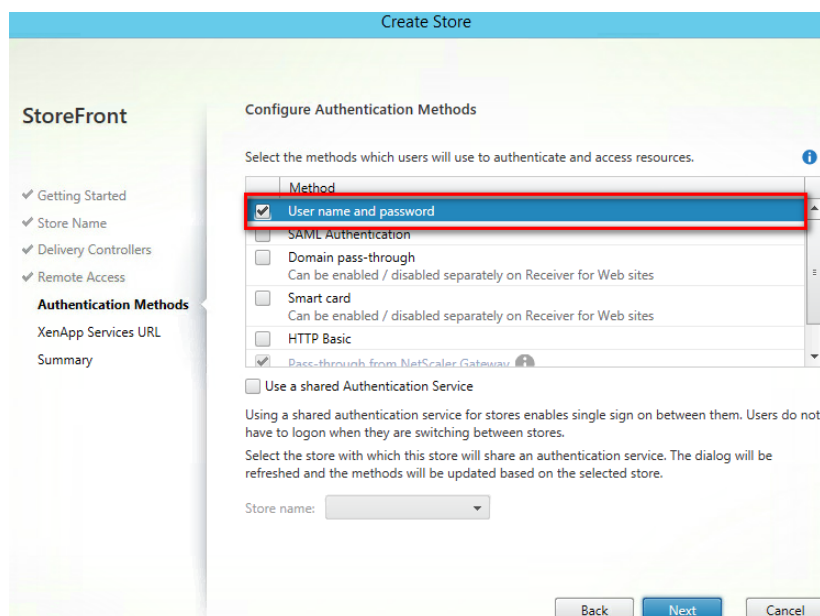


Figura 5.22 Método de autenticación

También, será necesario añadir el acceso para dispositivos móviles, sobre todo para el uso de usuarios VIP:

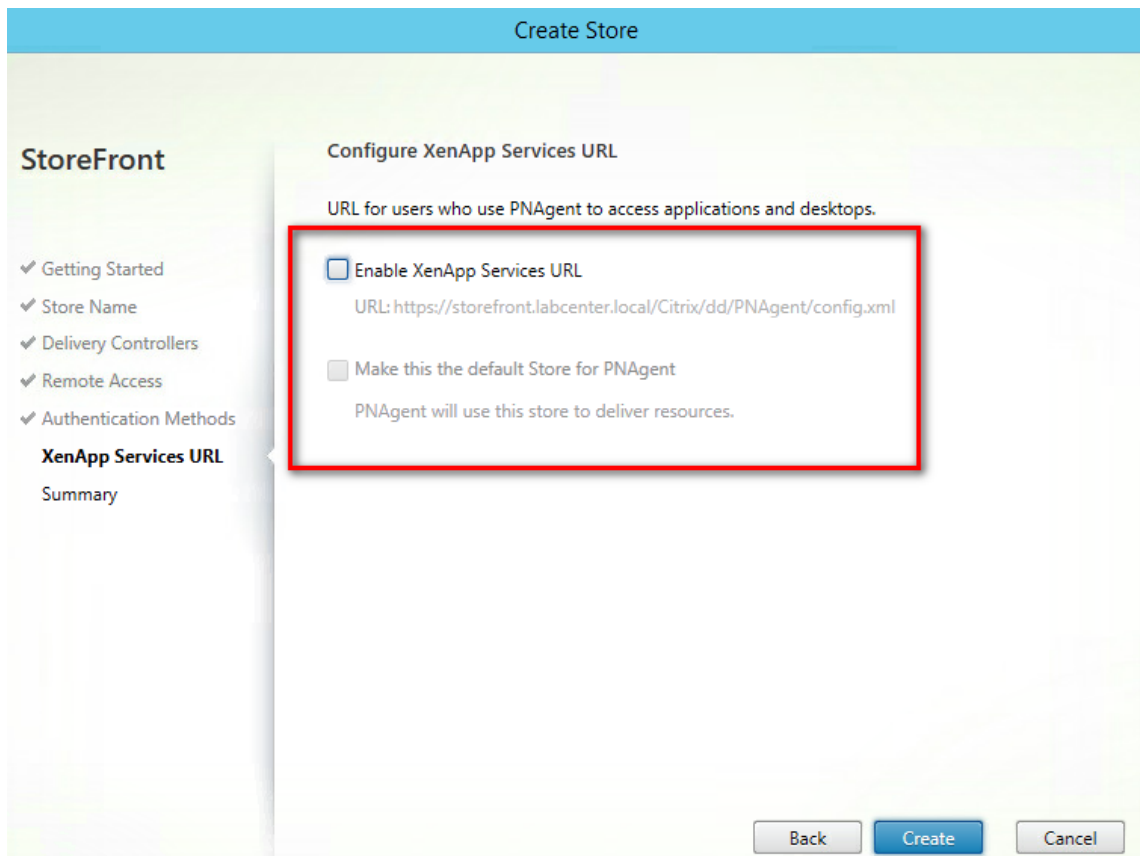


Figura 5.23 Como añadir dispositivos móviles

Una vez finalizado estos pasos, la consola debería quedar como la siguiente imagen:

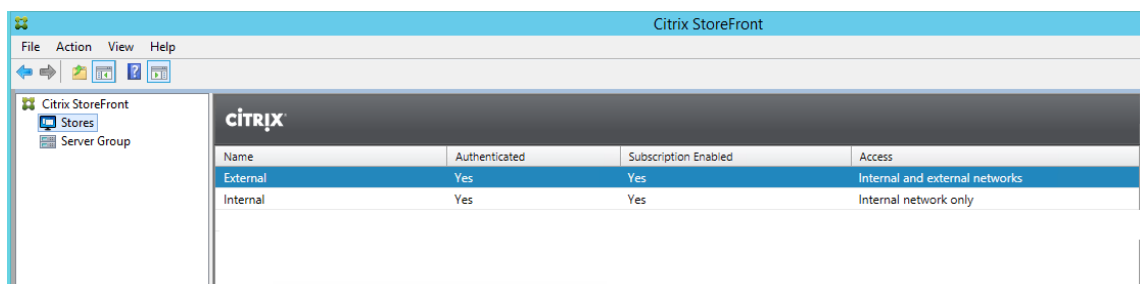


Figura 5.24 Stores configurados

Con el StoreFront configurado en su consola y el certificado incluido, es necesario realizar el balanceo y configurar los servicios en Netscaler: Para ello, lo primero será incluir los servidores a configurar en la herramienta de la siguiente manera:

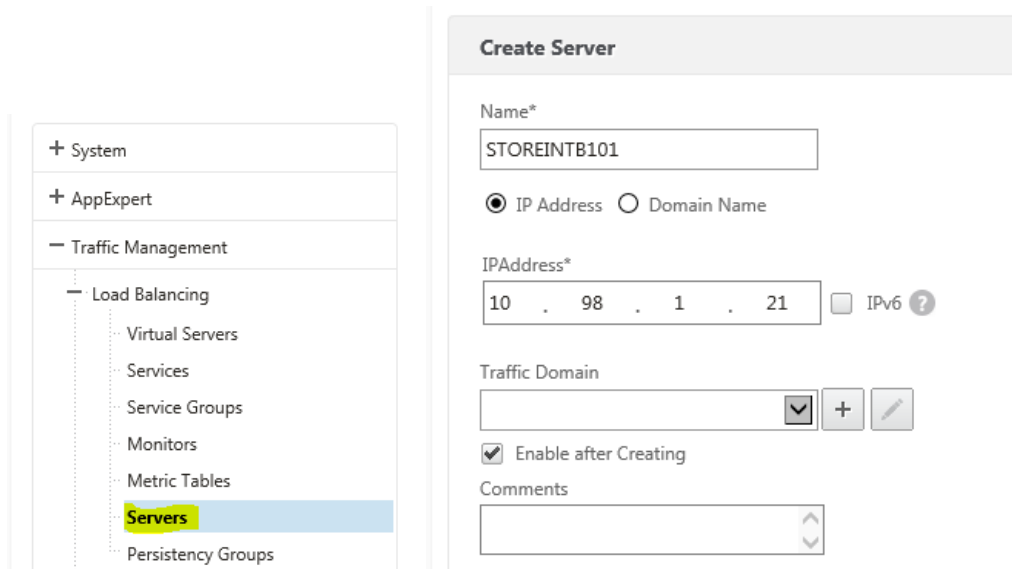


Figura 5.25 Añadir servidores a Netscaler

Una vez incluidos, se deben balancear los 4 servidores que harán uso de StoreFront, los cuales, soportan el acceso interno y externo. Para ello, se crea el Virtual Server por el puerto 443:

Load Balancing Virtual Server

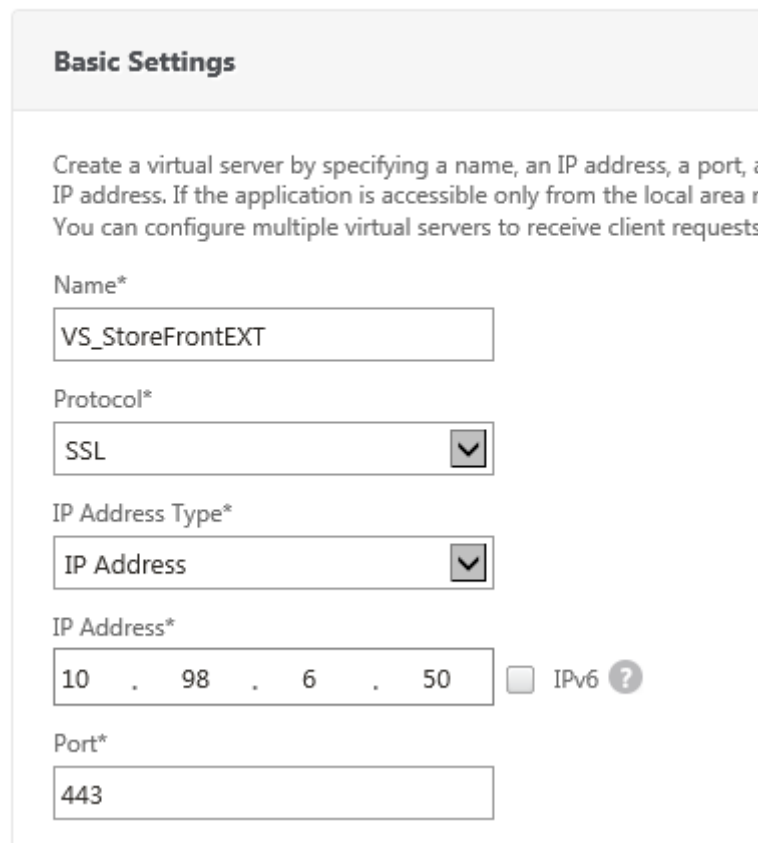


Figura 5.26 Añadir Virtual Server StoreFront a Netscaler

Una vez creado, es necesario añadir los servidores al Virtual Server mediante el uso de un Service Group. Además, al tener una conexión

segura y por el puerto 443 es necesario añadir el certificado, usando el wildcard:

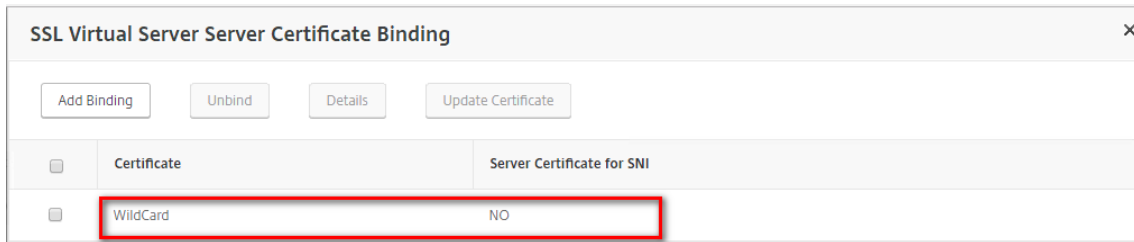


Figura 5.27 Añadir Wildcard a Virtual Server

En el caso del StoreFront interno es necesario añadir una política de rewrite con la configuración mostrada en la figura 5.27:

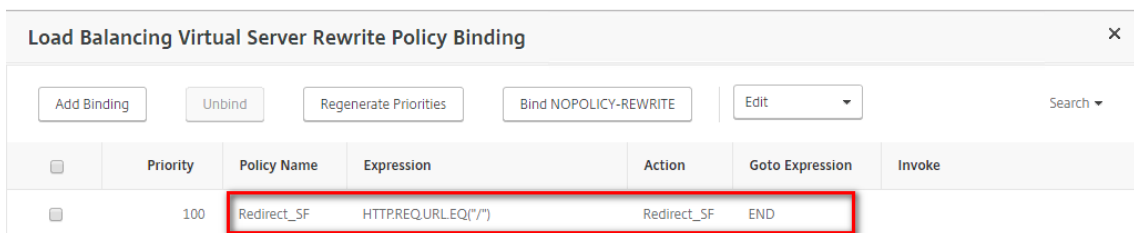


Figura 5.28 Añadir Política

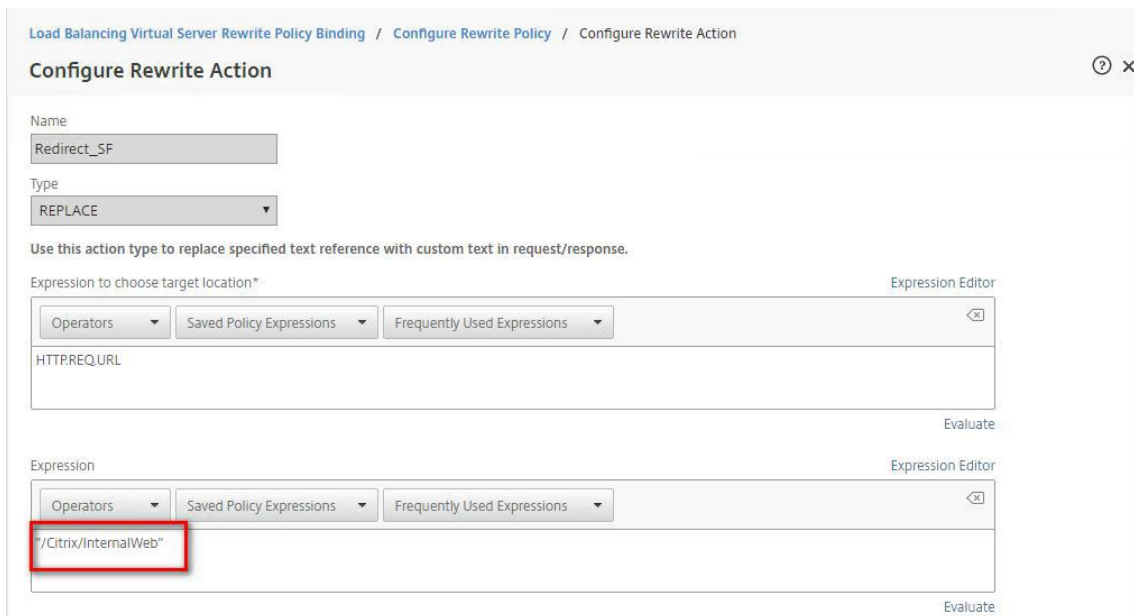


Figura 5.29 Configuración política rewrite

Con ello, quedaría configurado el balanceo de los StoreFront en Netscaler. Posteriormente, se debe incluir los DeliveryController en un balanceo de Netscaler con la siguiente configuración y mediante el uso de una VIP:

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol. If the application is accessible only from the local area network, you can configure multiple virtual servers to receive client requests.

Name*

Protocol*

 ?

IP Address Type*

IP Address*

 IPv6

Port*

Figura 5.30 Configuración Virtual Server DeliveryController

Una vez configurado, se añaden los servidores y el certificado wildcard.

También, es necesario crear el acceso externo Access Gateway y para ello, hay que crear un virtual server con este servicio:

← Back

VPN Virtual Server

Basic Settings

Name*
 ✕ ?

IP Address Type*
 ▼

IPAddress*
 IPv6

Port*

▶ More

Figura 5.31 Configuración Virtual Server Access Gateway

Dentro de la pestaña "Políticas" definimos una política de autenticación para cada uno de los dominios que va a validar Netscaler, ya que se encargará de realizar la validación. La política de autenticación se va a ejecutar de manera incondicional por lo que se evalúa la condición que siempre devuelve "True" (ns_true).

VPN Virtual Server Authentication LDAP Policy Binding				
Priority	Policy Name	Expression	Server	
100	Poi_LDAP_SSL	ns_true	Prof_LDAP_SSL	

Figura 5.32 Política de Autenticación

Hay que añadir las políticas de sesión, las cuales, sirven para establecer el modo en que sirven a los sitios de StoreFront, dependiendo de la petición que llegue, quedando definidas dos tipos:

- Acceso Web: Se configura como https://VS_StoreFrontEXT/Citrix/Web de tal manera que redirecciona al StoreFront externo.

VPN Virtual Server Session Policy Binding				
Priority	Policy Name	Expression	Profile	
100	Pol_Clientless	REQ.HTTPHEADER User-Agent NOTCONTAINS CitrixReceiver	Prof_Clientless	

Figura 5.33 Política de sesión StoreFront Externo

- Acceso con el cliente Citrix Receiver, donde se configura un perfil de sesión idéntico a la parte web, pero ahora cambiando el "Web Interface Address" a la ruta del fichero XML del sitio de servicios <https://StoreFrontExt/Citrix/PNAgent/config.xml>

VPN Virtual Server Session Policy Binding				
Priority	Policy Name	Expression	Profile	
90	Pol_Storefront	REQ.HTTPHEADER User-Agent CONTAINS CitrixReceiver	Prof_Storefront	

Figura 5.34 Política de sesión Citrix Receiver

En la pestaña "Published Applications" del servidor virtual, se definen los STAs de validación del logon de los usuarios. Es recomendable, usar los mismos STAs y en el mismo orden que los definidos en StoreFront.

VPN Virtual Server STA Server Binding				
Secure Ticket Authority Server	Secure Ticket Authority Server Address Type	State	Auth ID	
http://10.58.22.11	IPV4	UP	STA19591907	
http://10.58.22.10	IPV4	UP	STA986310240	

Figura 5.35 Configuración STA

5.3 Implementación Delivery Controller

Se introduce la ISO del producto Citrix y se ejecuta el .exe para realizar la instalación del software. Se selecciona Delivery Controller y se marca las opciones que se desean instalar, en este caso, Studio y Director:

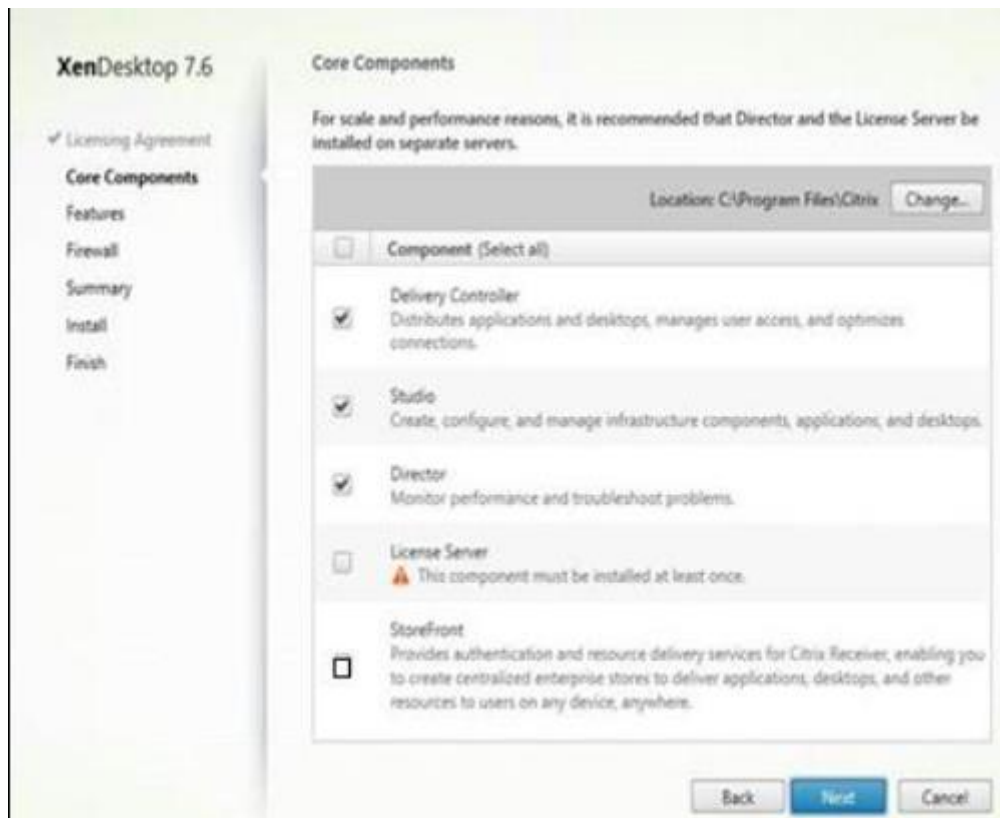


Figura 5.36 Instalación Delivery Controller

Delivery Controller: Es la pieza fundamental y el sistema que va a permitir distribuir aplicaciones y escritorios a los usuarios. administración de acceso y optimización.

Studio: Es la consola desde se va a realizar la administración. Desde ahí, se gestiona la presentación de aplicaciones y desktops, y en general los componentes de la infraestructura.

Director: Es la consola que permite supervisar el rendimiento, y resolver problemas o localizar un problema.

Servidor de licencias: Se indica el modo de licenciamiento.

Esta instalación tiene un tiempo estimado de 15 minutos. Una vez terminada la instalación se muestra la pantalla principal para empezar a configurar el producto.

En esta configuración, para el SQL se procede a realizar una instalación de SQL express, el cual, se instala en uno de los Delivery Controller.

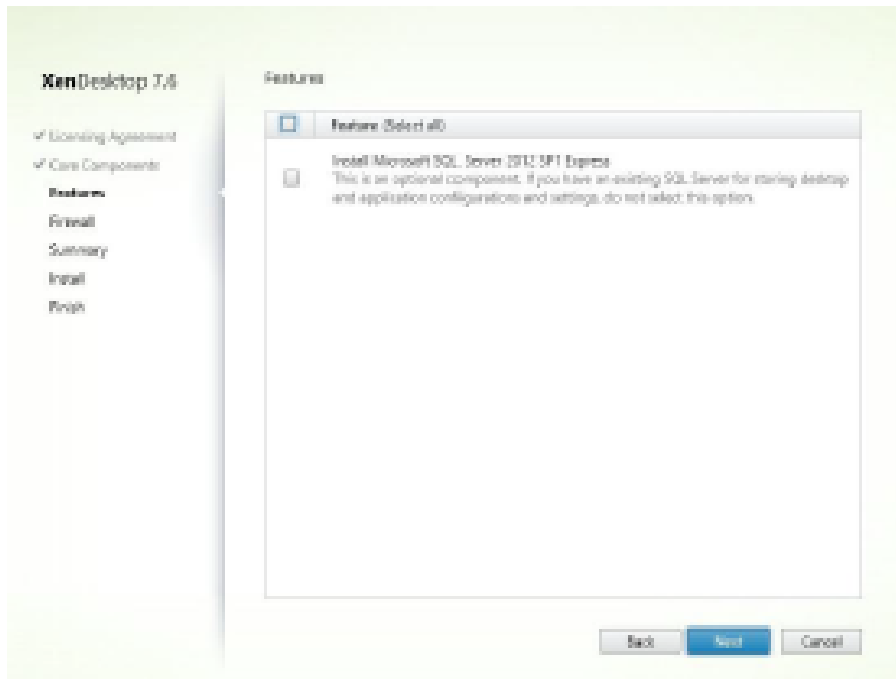


Figura 5.37 Instalación SQL express

Posteriormente, se fijan los puertos utilizados y necesarios para realizar esta instalación:

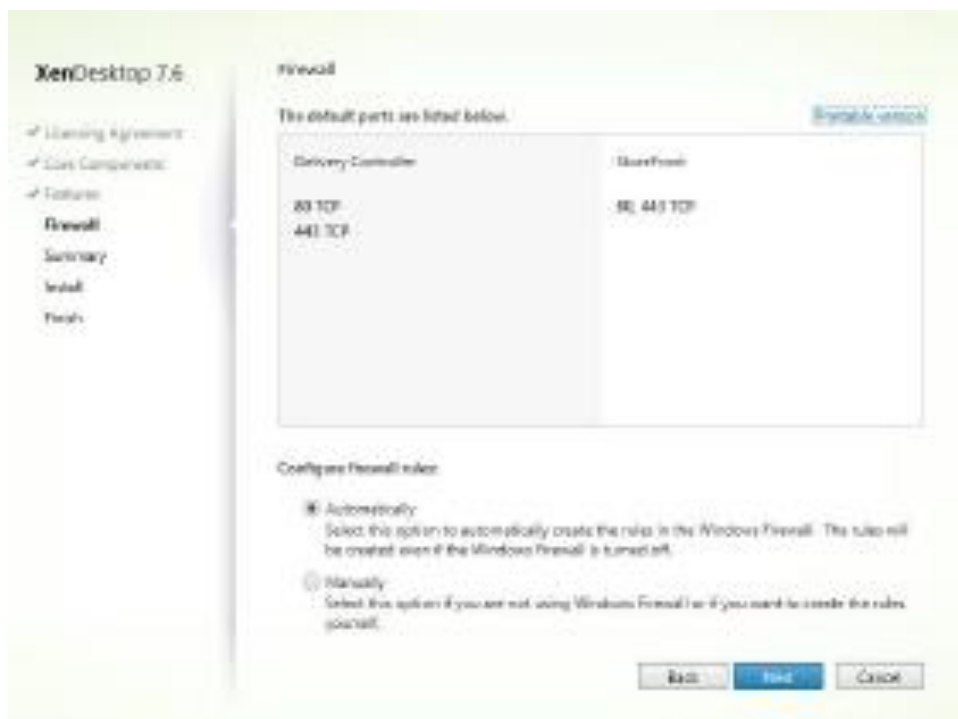


Figura 5.38 Puertos necesarios

Para el servidor de licencias y la granja XenApp serán necesarios los siguientes puertos:

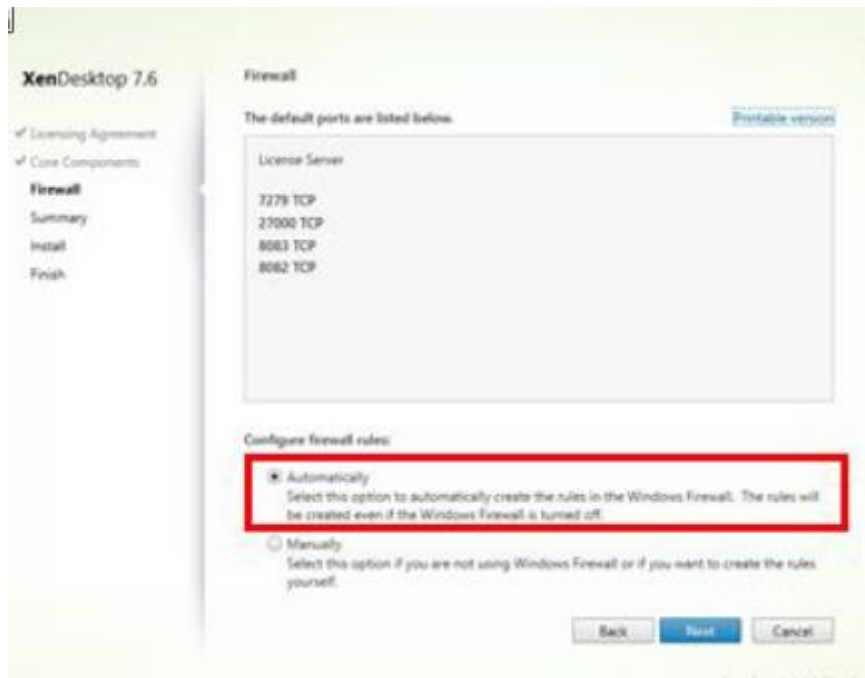


Figura 5.39 Puertos necesarios Servidor de Licencias

Una vez realizada la instalación, para realizar la configuración del servidor de licencias, se debe acceder a la consola de administración:

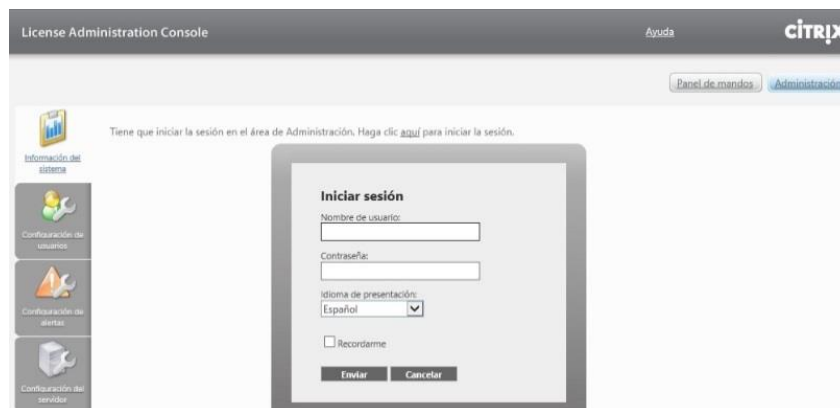


Figura 5.40 Configuración Servidor de Licencias

Desde la pestaña administración, agregamos el fichero de licencias, este tipo de archivos tiene la siguiente extensión: “.lic”.



Figura 5.41 Agregar fichero de licencias

Y una vez realizado, se reinicia el servicio de Windows “Citrix Licensing” donde tiene que estar con arranque automático y el sistema una vez reiniciado debe detectarlo:

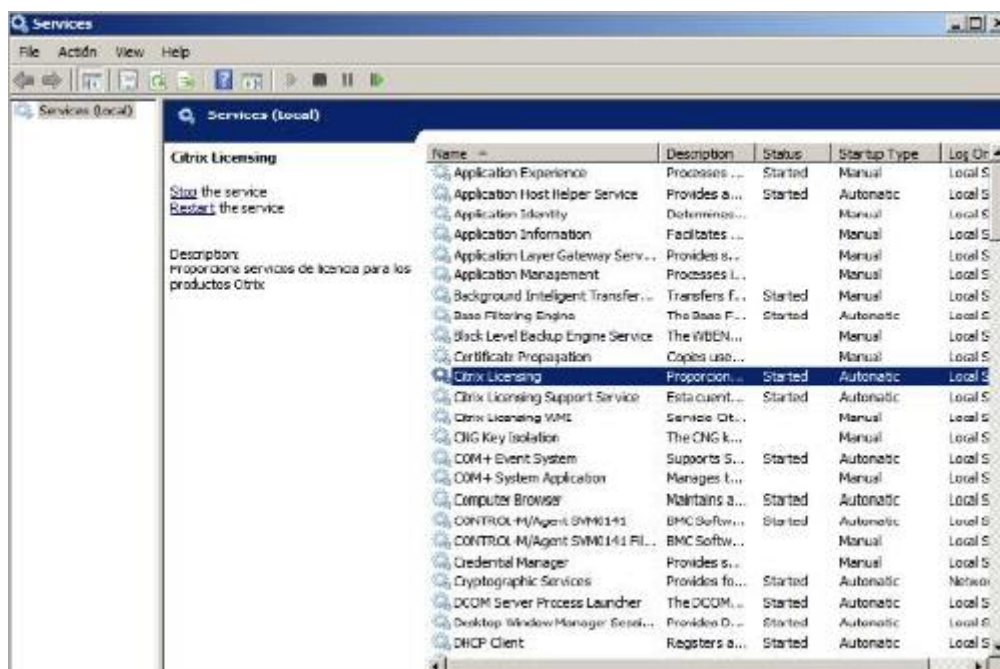


Figura 5.42 Servicio Citrix Licensing

Con el servicio de licencias instalados, se debe crear y configurar la granja. Para ello, desde el Citrix Studio se pincha en Site Setup y se le

indica un nombre a la nueva granja, en nuestro caso, será Citrix_SegurPart:

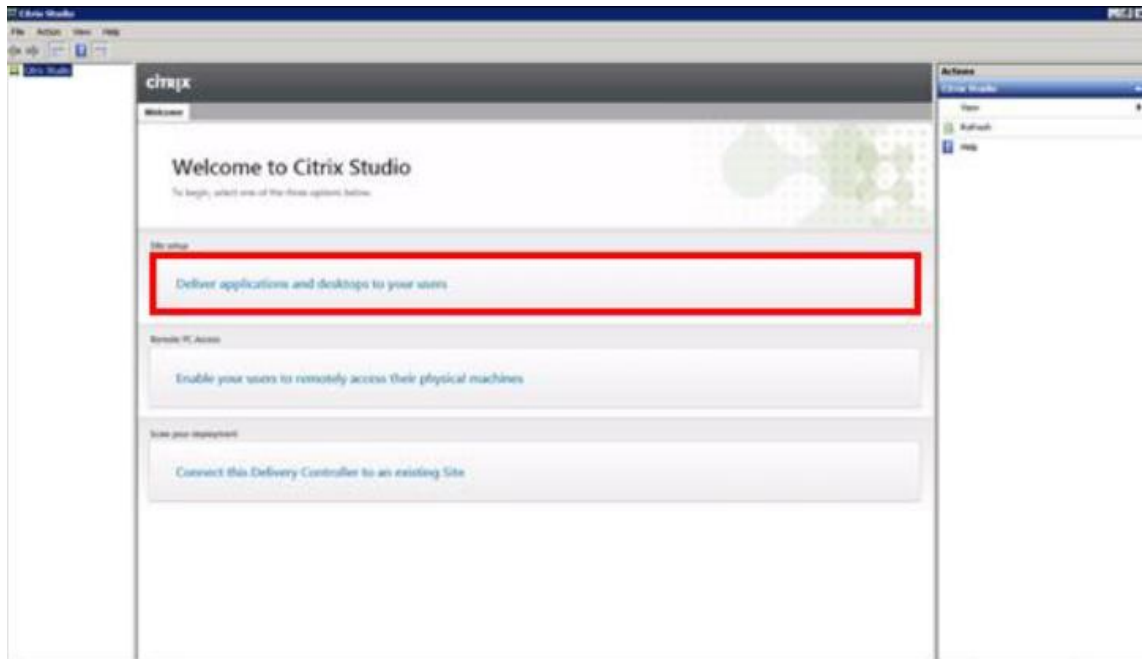


Figura 5.43 Citrix Studio Site Setup

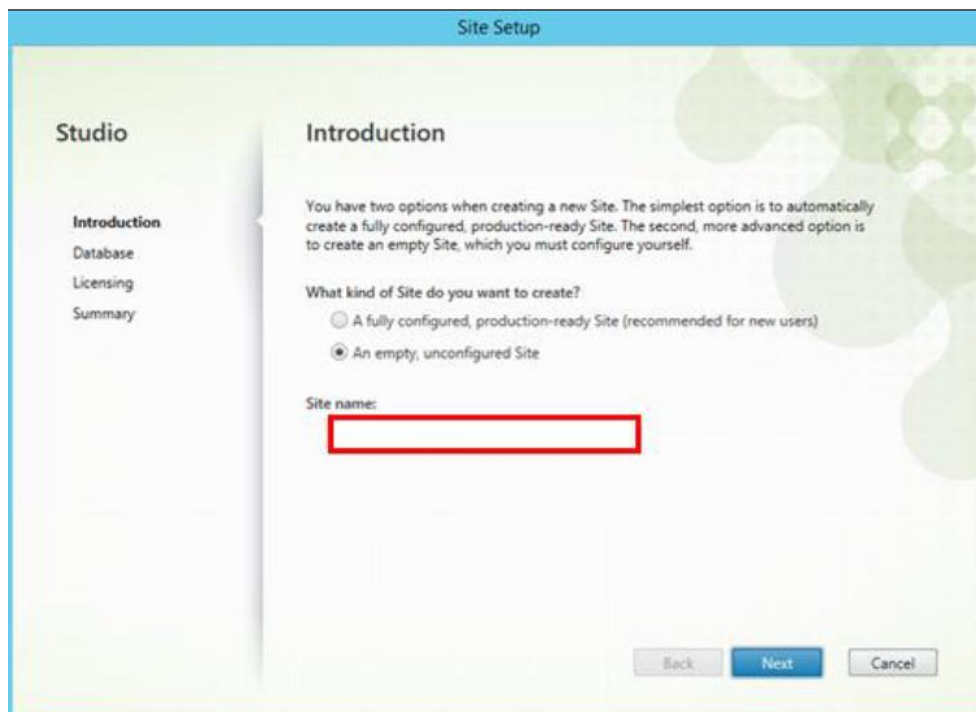


Figura 5.44 Nombre de la granja

Posteriormente, la instalación requiere que se indique la Base de datos, en este caso, BBDD_Citrix y después se requiere la conexión al servidor de licencias, que en este caso, es el servidor PROB1LICEN01 con una edición Enterprise Edition y un tipo de licencia User/Device:

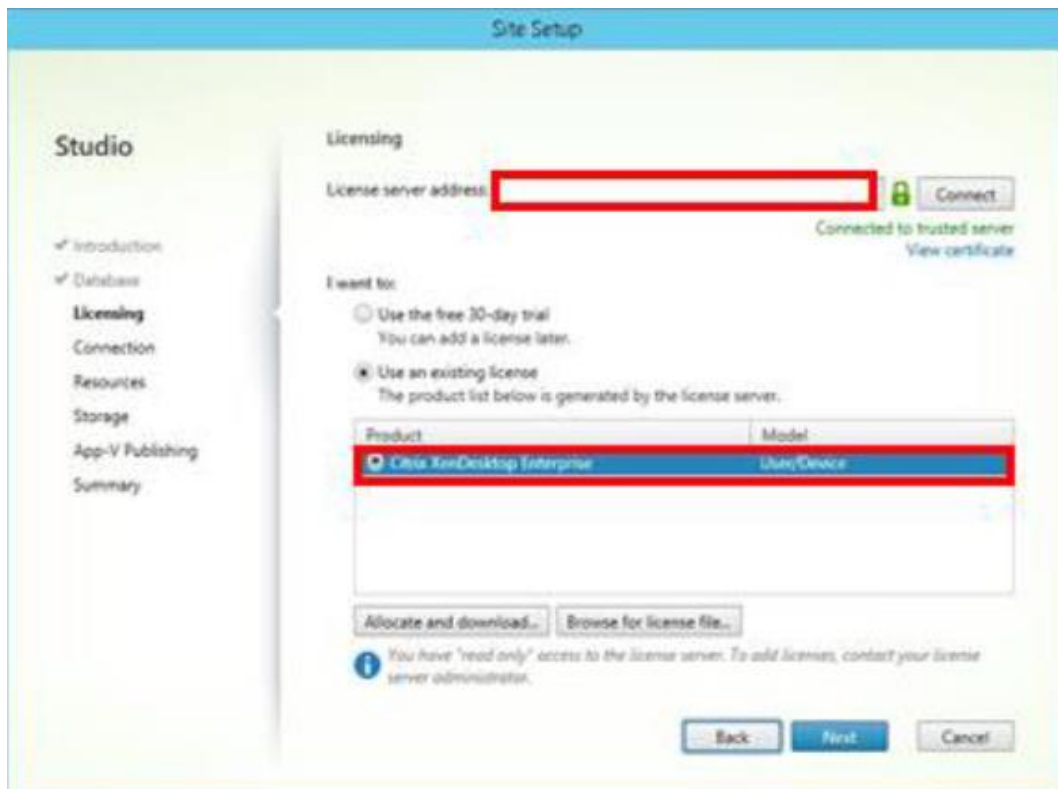


Figura 5.45 Configuración conexión servidor de licencias

El puerto a configurar, por defecto, es el 27000, de manera que quedaría configurado como PROB1LICEN01:27000.

Ahora, se debe crear y configurar la conexión con las máquinas virtuales a desplegar posteriormente. Citrix ofrece muchas opciones de virtualización para realizar la conexión (XenServer, Hyper-v, vSphere...). En este caso, se ha elegido la siguiente configuración:

- Tipo Host: VMWare.
- Dirección de la conexión: <https://vcenter.vmware/sdk>
- Nombre de usuario: En este caso, se usa una cuenta de servicio "srvsetupvcenter" con contraseña sin caducidad.
- Nombre de la conexión: Conexión.

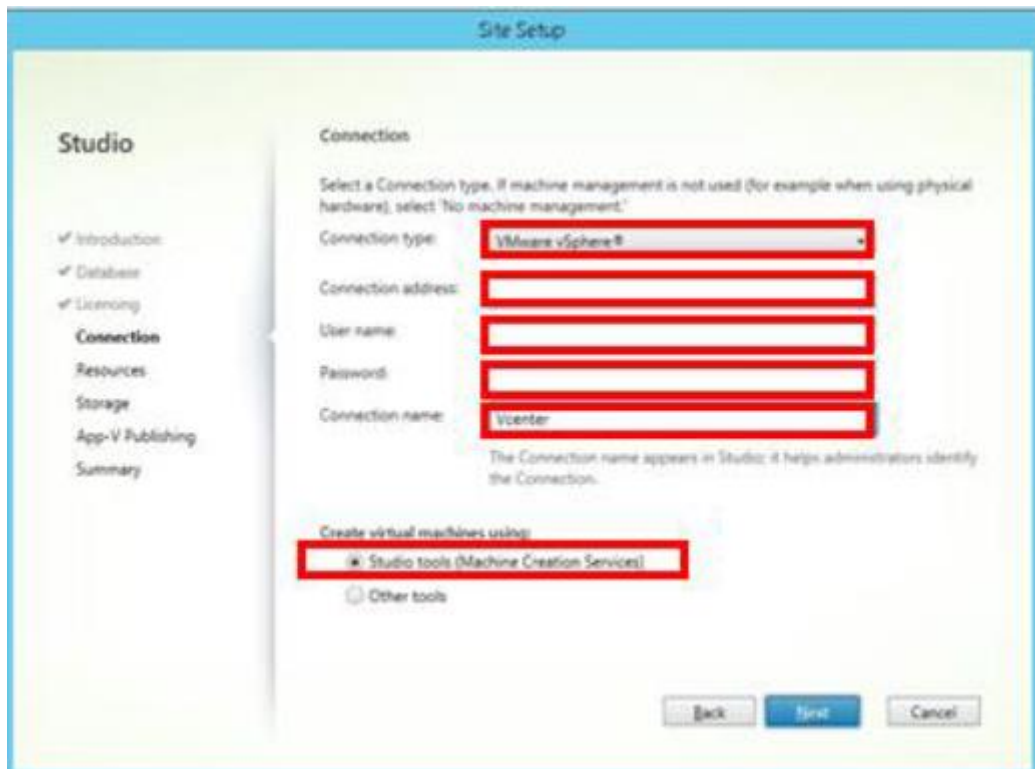


Figura 5.46 Configuración conexión vcenter

Una vez conectado con el vCenter Server u otro tipo de conexión, se requiere indicar la red o redes a utilizar. Se indica un nombre y se pulsa en Examinar para buscar el clúster.



Figura 5.47 Configuración Recursos

A continuación, se debe indicar el almacenamiento para almacenar las máquinas virtuales.

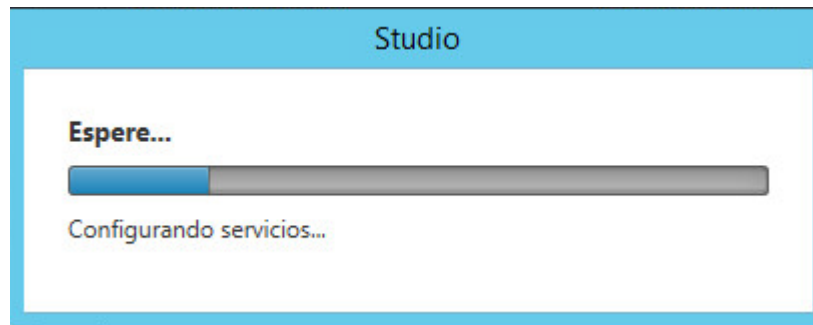


Figura 5.48 Configuración de servicios

Se terminan de configurar los servicios y si todo ha ido correcto, se termina la instalación. Una vez realizado, se debe realizar la instalación de los siguientes Delivery Controller.

5.4 Configuraciones de Directorio Activo

Para configurar correctamente la infraestructura de Citrix, es necesario crear una nueva estructura de unidades organizativas. Además, será necesario configurar distintas políticas de dominio, llamadas GPO. Dos de las primeras GPOs que deben definirse son las de XenApp y XenDesktop. Estas políticas son bastante extensas por lo que se ha añadido alguna imagen con alguna de sus particularidades:

Configuración del equipo (habilitada)		
Directivas		
Configuración de Windows		
Configuración de seguridad		
Directivas locales/Directiva de auditoría		
Directiva		Configuración
Auditar eventos de inicio de sesión		Acleros, errores
Directivas locales/Asignación de derechos de usuario		
Directiva		Configuración
Permitir inicio de sesión a través de Servicios de Terminal Server		Domain Users
Directivas locales/Opciones de seguridad		
Inicio de sesión interactivo		
Directiva		Configuración
Inicio de sesión interactivo: requerir tarjeta inteligente		Deshabilitado
Servicios del sistema		
Programador de aplicaciones multimedia (Modo de inicio: Deshabilitado)		
Permisos		
Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\SYSTEM	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Auditoría		
Tipo	Nombre	Acceso
Errores	Todos	Control total
Firewall de Windows (Modo de inicio: Manual)		
Permisos		
Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\SYSTEM	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer

Figura 5.49 Configuración del equipo GPO XenApp

Tipo	Nombre	Acceso
Errores	Todos	Control total
Reconocimiento de ubicación de red (Modo de inicio: Deshabilitado)		
Permisos	Sin permisos especificados	
Auditoría	Sin auditoría especificada	
Temas (Modo de inicio: Deshabilitado)		
Permisos	Sin permisos especificados	
Auditoría	Sin auditoría especificada	
Windows Defender (Modo de inicio: Deshabilitado)		
Permisos	Sin permisos especificados	
Auditoría	Sin auditoría especificada	
Windows Update (Modo de inicio: Deshabilitado)		
Permisos	Sin permisos especificados	
Auditoría	Sin auditoría especificada	
Directivas de clave pública/Entidades de certificación raíz de confianza		
Propiedades		
Directiva	Configuración	
Permitir a los usuarios seleccionar nuevas entidades de certificación raíz de confianza	Habilitado	
Los equipos cliente pueden confiar en los siguientes almacenes de certificados	Entidades de certificación raíz de terceros y entidades de certificación raíz de empresa	
Para realizar la autenticación de usuarios y equipos basada en certificados, los CA deben cumplir los siguientes criterios	Sólo los registrados en Active Directory	
Plantillas administrativas		
Definiciones de directiva (archivos ADMX) recuperados del almacén central.		
Citrix/Profile Management		
Directiva	Configuración	Comentario
Grupos procesados	Habilitado	

Figura 5.50 Configuración del equipo GPO XenApp

Directiva	Configuración	Comentario
Citrix/Profile Management/Configuración multiplantilla		
Habilitar configuración multiplantilla	Deshabilitado	
Ruta de definiciones multiplantilla	Deshabilitado	
Citrix/Profile Management/Gestión de perfiles		
Directiva		
Eliminar perfiles guardados en caché local al cerrar la sesión	Deshabilitado	
Gestión de conflictos de perfiles locales	Habilitado	
Si existen tanto el perfil de usuario local de Windows como el perfil de usuario de Citrix en el almacén de usuarios:		Eliminar el perfil local
Directiva		
Migración de perfiles existentes	Habilitado	
Tipos de perfiles de usuario que se migran si el almacén de usuarios está vacío:		Móviles
Citrix/Profile Management/Parámetros avanzados		
Directiva	Configuración	Comentario

Figura 5.51 Configuración del equipo GPO XenDesktop

Directiva	Configuración	Comentario
Network/Background Intelligent Transfer Service		
Directiva	Configuración	Comentario
Maximum network bandwidth that BITS uses	Deshabilitado	
Network/Offline Files		
Directiva	Configuración	Comentario
Prohibit user configuration of Offline Files	Habilitado	
Prevents users from changing any cache configuration settings.		
System		
Directiva	Configuración	Comentario
Remove Boot / Shutdown / Logon / Logoff status messages	Habilitado	
System/Group Policy		
Directiva	Configuración	Comentario
User Group Policy loopback processing mode	Habilitado	
Mode:	Merge	
System/Internet Communication Management/Internet Communication settings		
Directiva	Configuración	Comentario
Turn off Help and Support Center "Did you know?" content	Habilitado	
Turn off Help and Support Center Microsoft Knowledge Base search	Habilitado	
Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Habilitado	
Turn off Internet File Association service	Habilitado	
Turn off the Windows Messenger Customer Experience Improvement Program	Habilitado	
Turn off Windows Error Reporting	Habilitado	
Turn off Windows Update device driver searching	Habilitado	
System/System Restore		
Directiva	Configuración	Comentario
Turn off System Restore	Habilitado	
System/User Profiles		
Directiva	Configuración	Comentario
Delete cached copies of roaming profiles	Habilitado	
Do not check for user ownership of Roaming Profile Folders	Habilitado	
Do not detect slow network connections	Habilitado	
Only allow local user profiles	Habilitado	
Windows Components/Internet Explorer		

Figura 5.52 Configuración del equipo GPO XenDesktop

También, será necesario aplicar una GPO para los perfiles de usuario. Para ello, se define un repositorio Network/CTXProfile con unos permisos específicos.

Será necesario incluir full control para todos los usuarios en el share y en NTFS incluir permisos especiales para los usuarios autenticados.

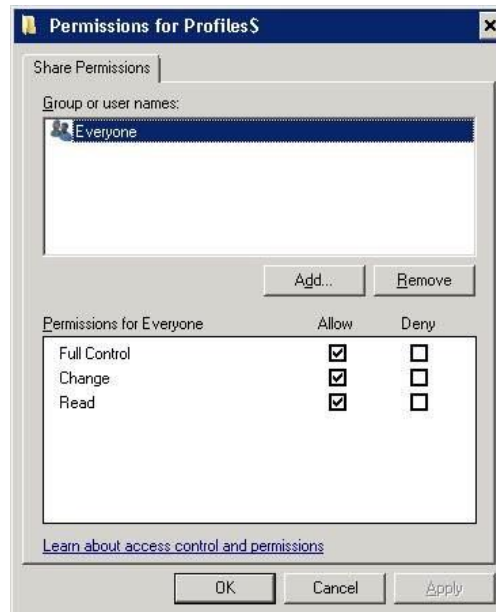


Figura 5.53 Permisos Network/CTXProfile

Para poder configurar la GPO, es necesario agregar la plantilla .adm. Esta plantilla se puede encontrar en el propio software de Xendesktop 7.X:

- o ...\\x64\\ProfileManagement\\ADM_Templates\\en

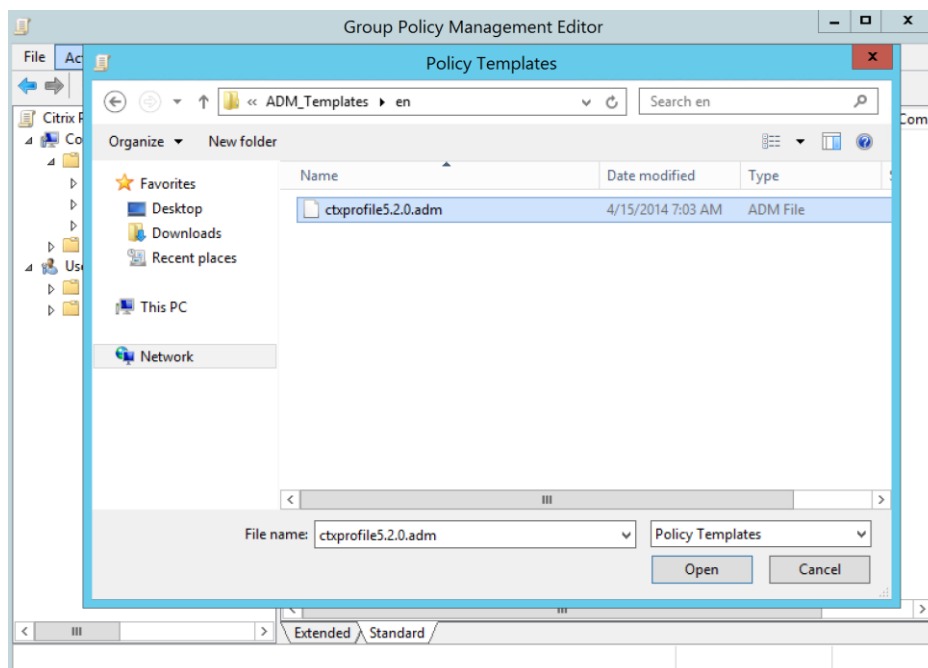


Figura 5.54 Añadir plantilla .adm

Una vez agregada la plantilla, se debe configurar la política, donde se destacan algunos de los principales puntos implementados:

- Se marca como disabled la opción Processed groups para que aplique a todos los usuarios.
- Con el fin de acelerar el cierre de sesión, se ha configurado Process Internet cookies files on logoff como enabled.
- Se configura a 180 segundos la opción delay before deleting cached profile para que se borren los perfiles de los usuarios tras haber hecho logoff pasado este tiempo.
- Se habilita la opción de eliminar perfiles cacheados.
- Se define Path to user store para almacenar los perfiles de usuario. La ruta definida es CTXProfile\$\SAMAccountName#. Este punto puede ampliarse revisando <https://docs.citrix.com/en-us/profile-management/5/upm-specify-user-store-path-den.html>
- Se deshabilita la opción Process logons of local administrators para evitar que esta GPO afecte a administradores locales.

Puede ampliarse información y ver más sobre esta GPO en <http://www.carlstalhood.com/citrix-profile-management/>

5.5 WSUS y seguridad

Una vez finalizado los pasos anteriores, es fundamental, dejar los servidores al corriente de parches de seguridad. Para ello, la empresa va a disponer de un servidor con la herramienta de WSUS, la cual, permite instalar de manera automática todas las actualizaciones de manera rápida en todos los equipos generados hasta ahora. Además, los responsables de seguridad deben instalar el antivirus y configurarlo en los equipos desplegados.

Citrix, recomienda la exclusión de análisis sobre algunos directorios, los cuales, se muestran a continuación:

Director and StoreFront:

```
\inetpub\temp\IIS Temporary Compressed Files
\Windows\system32\inetsrv\w3wp.exe
\Windows\SysWOW64\inetsrv\w3wp.exe
\Program\Files\Citrix\Receiver
\StoreFront\Services\SubscriptionsStoreService
```

Controller:

\\Windows\system32\csrss.exe
\\Windows\system32\winlogon.exe
\\Windows\system32\userinit.exe
\\Windows\system32\smss.exe
\\Program Files\Citrix\Group Policy\Client-Side
\\Extension\CitrixCseEngine.exe
\\Program Files (x86)\Citrix\System32\wfshell.exe
\\Program Files (x86)\Citrix\system32\ctxmlss.exe
\\Program Files (x86)\Citrix\System32\CtxSvcHost.exe
\\Program Files (x86)\Citrix\system32\mfcom.exe
\\Program Files (x86)\Citrix\System32\Citrix\Ima\ImaSrv.exe
\\Program Files (x86)\Citrix\System32\Citrix\Ima\IMAAdvanceSrv.exe
\\Program Files (x86)\Citrix\HealthMon\HCAService.exe
\\Program Files (x86)\Citrix\Streaming Client\RadeSvc.exe
\\Program Files (x86)\Citrix\Streaming Client\RadeHlprSvc.exe
\\Program Files (x86)\Citrix\Independent Management
\\Architecture\RadeOffline.mdb
\\Program Files (x86)\Citrix\Independent Management
\\Architecture\imalhc.mdb

Además de esto, se recomienda realizar el escaneo fuera del horario laboral. En este caso, supone que debe ser posterior a las 18:30 y previo a las 8:00, horario considerado no productivo en la empresa.

5.6 Despliegue de equipos

Para los equipos de usuario es necesario determinar y fijar el proceso de despliegue de VDIs. En este caso, para los puestos VIP, se va a utilizar pvDisk para permitir que los usuarios puedan guardar sus configuraciones una vez asignada la VDI.

La función Personal vDisk conserva la administración de imágenes únicas para escritorios agrupados y distribuidos por streaming, al tiempo que permite a los usuarios instalar aplicaciones y cambiar la configuración de sus escritorios. A diferencia de las implementaciones de VDI tradicionales con escritorios agrupados, donde los usuarios pierden sus personalizaciones y sus aplicaciones personales cuando el administrador modifica la imagen maestra, las implementaciones con discos Personal vDisk conservan dichos cambios. Esto significa que los administradores pueden administrar de manera centralizada y sencilla las imágenes maestras, al mismo tiempo que proporcionan a los usuarios una experiencia de escritorio personalizada.

Los discos Personal vDisk permiten esta separación al redirigir todos los cambios que efectúa el usuario en la máquina virtual a un disco aparte (el disco Personal vDisk) asociado a la máquina virtual del usuario. El contenido del disco Personal vDisk se fusiona en tiempo de ejecución con el contenido de la imagen publicada para proporcionar una

experiencia unificada. De este modo, los usuarios pueden seguir accediendo a las aplicaciones aprovisionadas por el administrador en la imagen maestra.

Para realizar el despliegue, es necesario realizar los siguientes pasos:

1. Instalar Windows 10
2. Instalar el Agent VDA abriendo la ISO y ejecutando el software dedicado para esta tarea.

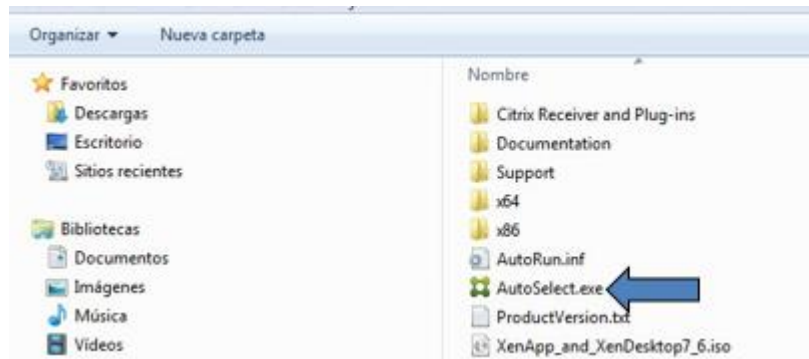


Figura 5.55 Instalación Agente VDA

3. Seleccionar la instalación XenDesktop y Agent VDA:

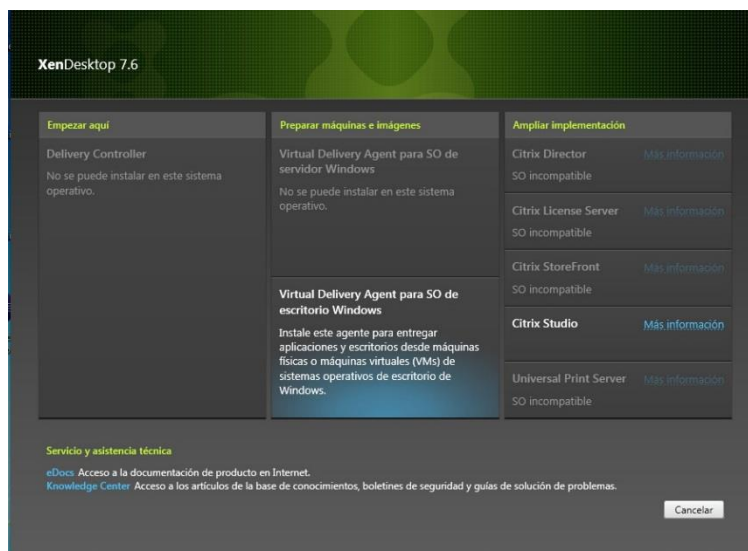


Figura 5.56 Instalación Agente VDA

4. Se crea una imagen maestra y se pulsa en “siguiente”:

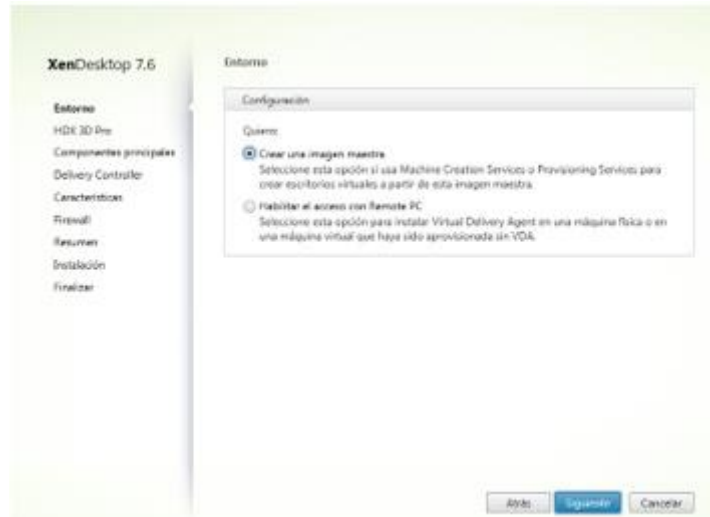


Figura 5.57 Creación Imagen Maestra

5. Se selecciona el agente estándar y se añaden los delivery de la granja generada.
6. Para las VDIs VIP se va a habilitar la opción pvDISK. Una vez habilitado pvDisk en la instalación, cada vez que se abra la GoldImage para realizar algún cambio, se solicitará la actualización del inventario del software base que tiene instalado el puesto.

Este servicio cada vez que se realiza un cambio en la GoldImage realiza la actualización del inventario y se almacenan los cambios que tiene la GoldImage. A partir de este punto, todo el software que se instale un usuario, quedará almacenado en su personal vDisk (disco p:\)

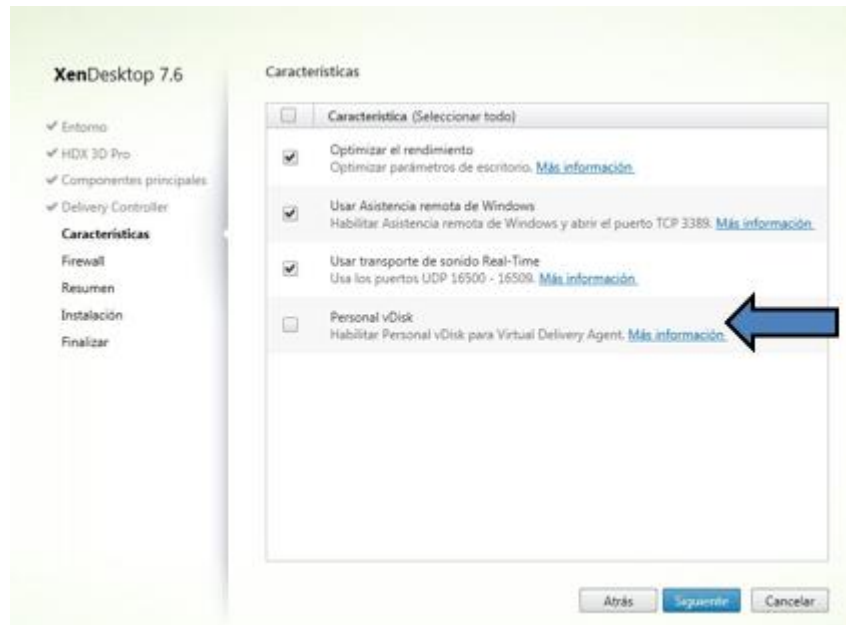


Figura 5.58 Habilitar pvDisk

Para que el proceso funcione, es necesario abrir en los firewall los siguientes puertos de la plataforma VDI:

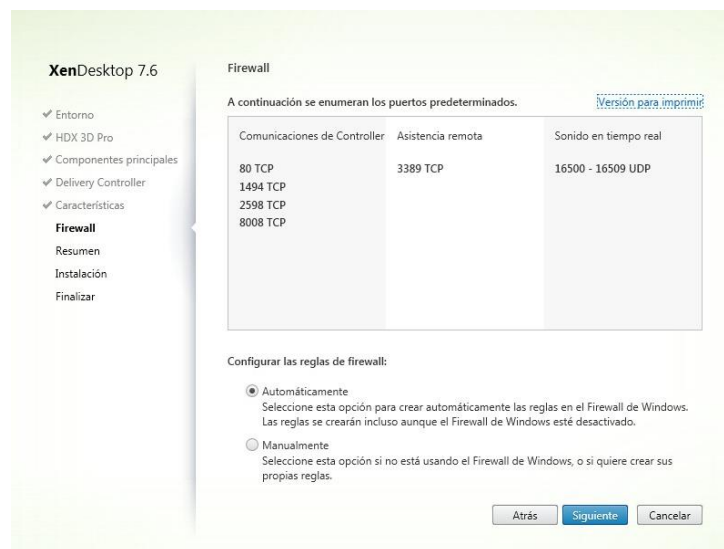


Figura 5.59 Puertos requeridos para plataforma VDI

A continuación, se muestra el resumen de la instalación. Se pulsa en instalar y por último, reiniciar:

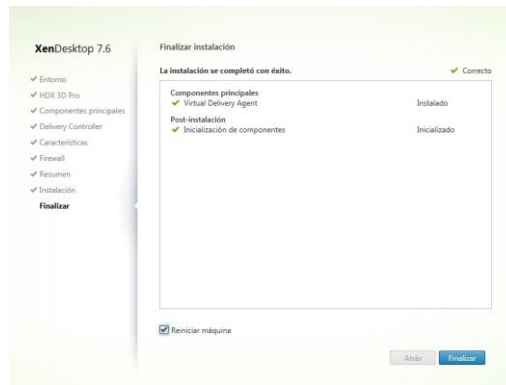


Figura 5.60 Resumen instalación

Tras ello, es necesario instalar el software que llevará el puesto, es decir, Office, navegadores, antivirus, etc.

Por último, es necesario cerrar la imagen, es necesario:

- Aplicar scripts de optimización para Windows 10 y servicios de Citrix. Estos scripts ya están preparados y están a disposición del departamento de Windows. Simplemente hay que ejecutarlos.
- Limpiar antivirus para posterior clonado de imágenes. Ejecutar el script para preparar la imagen. Debido al clonado de la GoldImage se necesita preparar el antivirus antes de cerrar la plantilla, para que, después en los puestos virtuales clones no se dupliquen las cuentas de máquinas y aparezcan los puestos VDI correctamente en la consola.
- En el caso de los puestos VDI para TI, actualizar inventario personal vDisk. En este punto, antes de apagar la GoldImage se necesita actualizar el inventario de todo el software base instalado. Cuando se apaga la máquina, se solicita la realización del inventario, no obstante, también es posible lanzarla, como se muestra a continuación:



Figura 5.61 Actualizar personal vDisk

Se realiza el inventario y al finalizar es necesario tener marcado el check de “apagar el sistema al completar la actualización”:

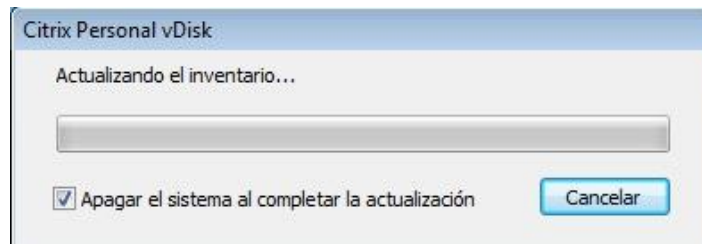


Figura 5.62 Citrix Personal vDisk

5.7 Creación de catálogos

Una vez se ha generado las Master Imagen, es necesario crear los catálogos de equipos. Para ello, se debe abrir el Desktop Studio y realizar los siguientes pasos:

- Crear un catálogo de máquinas sobre la opción de "Machine Catalogs":

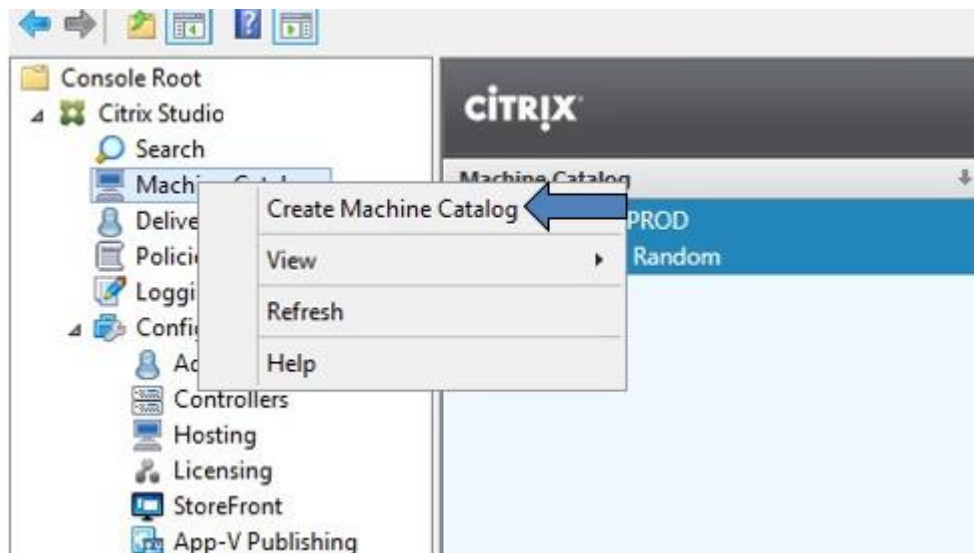


Figura 5.63 Crear Catálogo de máquinas

- Para las VDIs se selecciona "Windows Desktop OS":

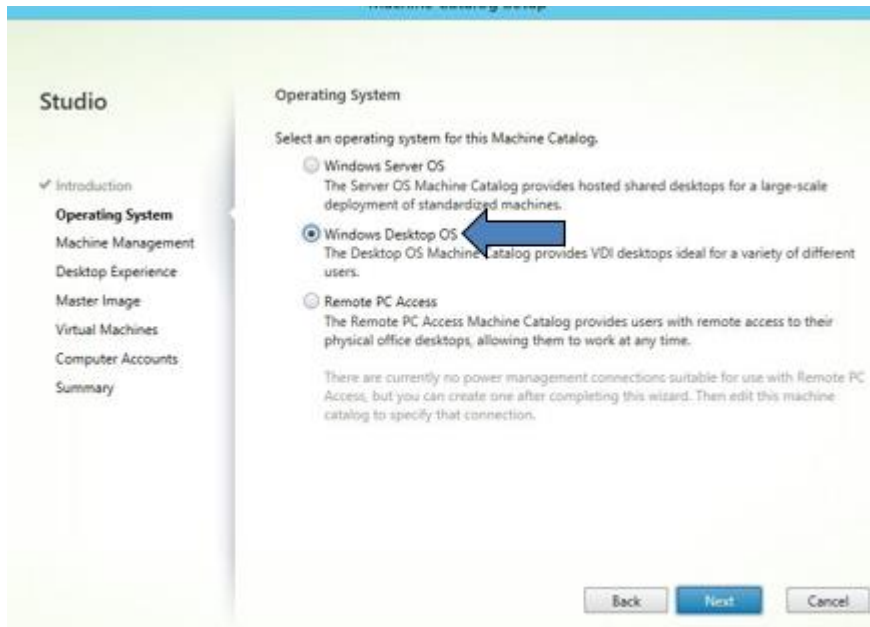


Figura 5.64 Elección Windows Desktop OS

- Se selecciona el recurso dónde se van a desplegar las VM's, y se pulsa en "Next":

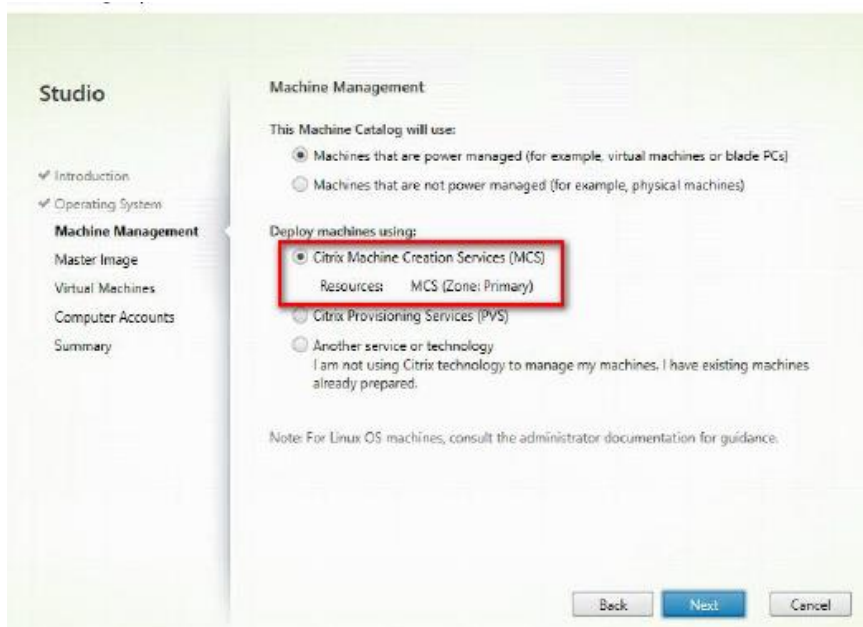


Figura 5.65 Citrix Machine Creation Services (MCS)

- Se marca el tipo de catálogo en función de la VDI y se selecciona la Master Imagen:

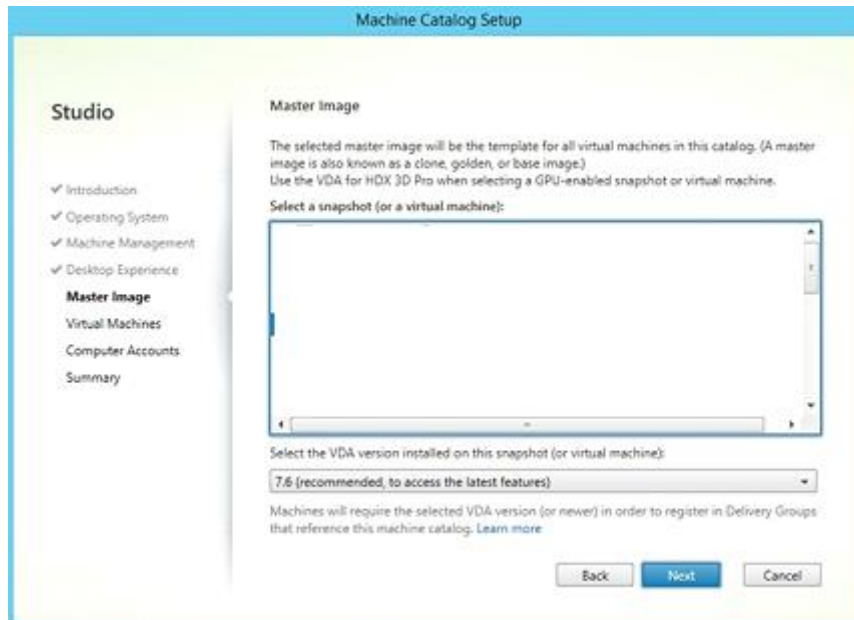


Figura 5.66 Master Imagen (snapshot)

- En el siguiente punto, se asignan los recursos a los puestos virtuales, CPU, memoria y tamaño del disco personal pvDisk en caso de disponer de el:

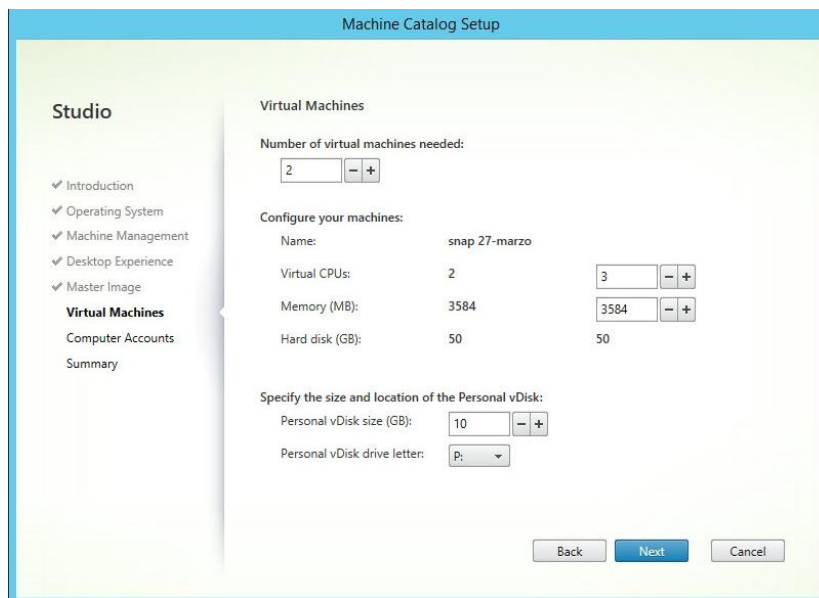


Figura 5.67 Configuración Virtual Machine

- Se crean las cuentas de máquinas en las OU's de Active Directory. El nombre va a ser igual que la cuenta que se genera en Active Directory:

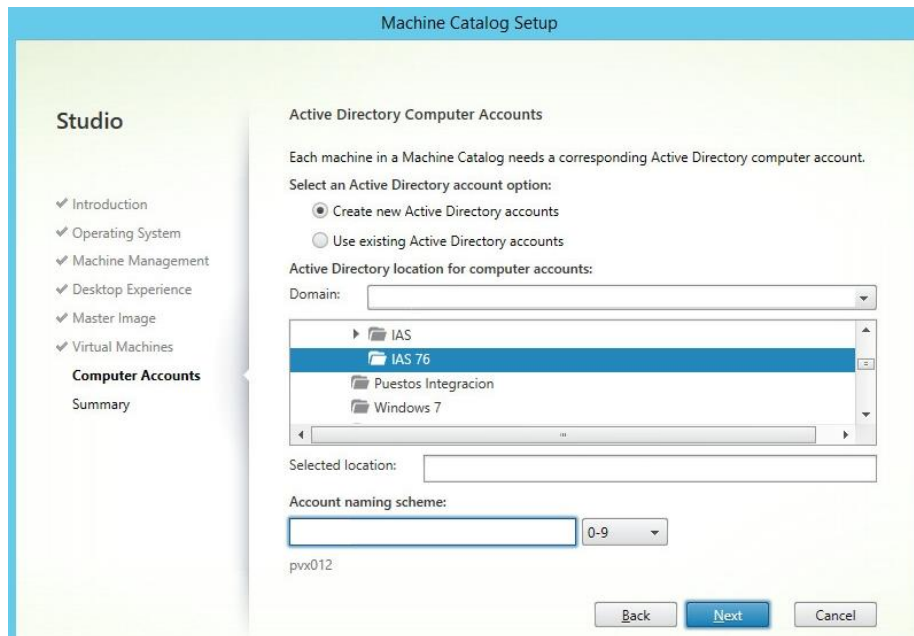


Figura 5.68 Configuración Computer Accounts

- El último paso es poner el nombre del catálogo y darle a finalizar:

5.8 Asignación Delivery Groups

La última parte del proceso es asignar un delivery group a los catálogos que se generen. Para ello, en la consola de Citrix Studio, crear un nuevo delivery group:

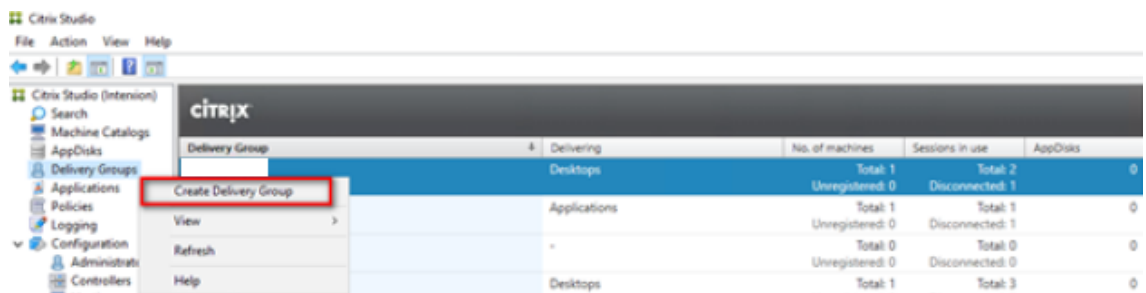


Figura 5.69 Crear Delivery group

5.9 Pruebas y validaciones

El objetivo de estas pruebas es validar la plataforma generada y verificar que cumple con los requisitos indicados. Con ello, se busca que la reacción en la puesta a producción sea más eficaz y rápida. Además, permitirá encontrar puntos débiles en el diseño implantado y una revisión avanzada de la infraestructura. Esto es muy importante a la hora de explotar la infraestructura ya que no estamos exentos a elementos externos, como por ejemplo un corte de corriente.

Para realizar las pruebas, se ha generado un usuario de test “usuario01” con el que se da acceso a la plataforma:

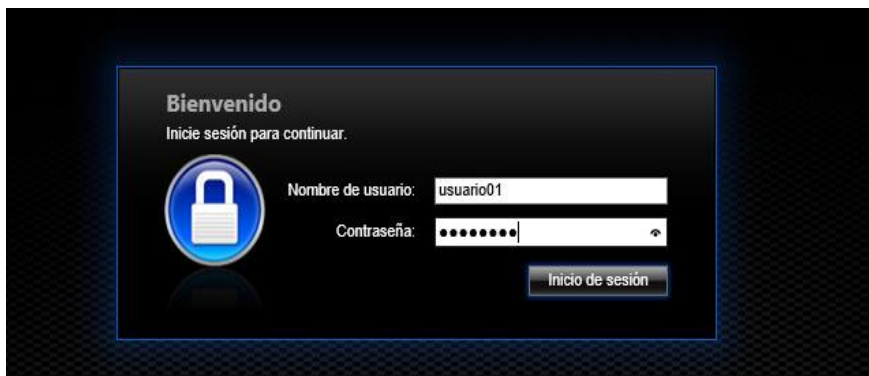


Figura 5.70 Pantalla bienvenida

No se ha realizado, pero si fuese necesario y desde el departamento de seguridad lo solicitasen, se podría añadir un disclaimer para que los usuarios tuviesen que aceptar unas condiciones para acceder.

Una vez logado, se muestra el acceso publicado al usuario de pruebas:

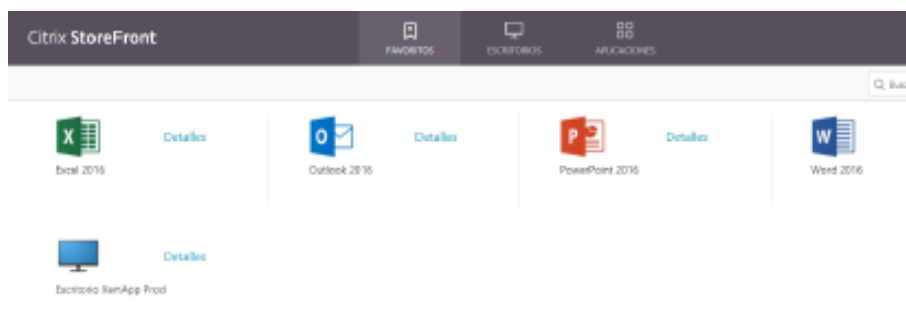


Figura 5.71 Escritorio inicial

Se le han publicado diversas aplicaciones a través de grupos de directorio activo que dan acceso a las aplicaciones.

Se observa que a nivel de rendimiento tanto los servidores de aplicaciones como las VDIs muestran valores correctos, es decir, valores de CPU por debajo del 10% y niveles de memoria utilizada que no llegan al 40%, por lo que se deduce que no tienen problemas de dimensionamiento. La apertura de iconos es correcta y cargan a una velocidad fluida.

5.10 Pruebas de funcionalidad

A continuación, se detallan las pruebas realizadas:

Prueba 1: Si falla un Controller

Para poner a prueba los Delivery Controller, se provoca un fallo en uno de ellos. El resultado ha sido el esperado, permitiendo que las VDIs y aplicaciones que estaban en uso se mantengan funcionando. Además, a pesar de este error, al tener un servicio de alta disponibilidad, se observa

que pueden seguir iniciándose aplicaciones y accesos de VDIs conectando con otros servidores.

En este caso, los usuarios no se ven afectados.

Prueba 2: Fallo en todos los Delivery Controller

En este caso, se ha provocado que fallen todos los servidores de la granja. El resultado es el esperado, los usuarios que actualmente están conectados no se ven afectados, pero no se permite la conexión de nuevos usuarios.

Para esta prueba, todos los usuarios que quieran acceder a alguna aplicación o VDI se verá afectado. Para recuperar el servicio, es necesario, recuperar al menos un servidor Delivery Controller.

Prueba 3: Si falla un StoreFront interno

Tras la caída de uno de los nodos internos que dan el servicio de StoreFront, los usuarios conectados no sufren ningún problema y se mantienen conectados. Los usuarios que intentan acceder tampoco tienen problema porque el otro nodo con este servicio asume la carga y se mantiene funcionando sin problemas.

En este caso, los usuarios no se ven afectados. Esta prueba se ha comprobado con un StoreFront externo siendo el mismo resultado, como era de esperar.

Prueba 4: Fallo en todos los StoreFront internos

Se comprueba que no se pueden iniciar aplicaciones nuevas y que los usuarios se quedan sin poder acceder. Los usuarios que estaban conectados y con aplicaciones abiertas, no se ven afectados y se mantienen trabajando con normalidad.

Los usuarios que intentan acceder, no lo pueden hacer hasta que se recupere uno de los servidores que da este servicio. Se comprueba que en un servidor StoreFront externo el resultado es el mismo, como era de esperar.

Prueba 5: Fallo en la BBDD

En este caso, los usuarios no se ven afectados ni notan el fallo en la BBDD. A nivel de administración de sistemas, es necesario recuperarla lo antes posible, ya que no se pueden realizar cambios de configuración desde la consola Citrix Studio.

Prueba 6: Fallo en uno de los Netscaler

Los usuarios conectados se mantienen con las aplicaciones o VDIs abiertas y no experimentan ningún corte. Además, pueden seguir iniciándose las sesiones. El Netscaler está configurado en alta disponibilidad por lo que no se sufre corte.

Prueba 7: Fallo en todos los Netscaler

Se cae el servicio y el acceso a la red. Es necesario recuperar el servicio para que los usuarios vuelvan a poder conectar. Los usuarios que estén haciendo uso antes de la caída no sufren corte y se mantienen trabajando con normalidad.

Prueba 8: Fallo en el servidor de Licencias

Hay un tiempo estimado de 96 horas para recuperar el servidor, puesto que es el tiempo que da Citrix sin una afectación mayor. Los usuarios no notan nada y siguen trabajando con total normalidad.

Prueba 9: Fallo de los perfiles de usuario

Los usuarios tienen fallos para iniciar sesión porque no se puede cargar su perfil de usuario.

Para solventar los problemas es necesario recuperar el servicio de ficheros.

Prueba 10: Fallo en un servidor de aplicaciones XenApp

Al fallar los usuarios se quedan “colgados” y pierden la conexión con el servidor. Por lo tanto, es necesario que cierren sesión e inicien de nuevo para logarse en otro servidor Citrix. A veces, es necesario matar la sesión del usuario desde la consola de XenApp. Esta tarea se debe realizar por un administrador de sistemas.

5.11 Pruebas de rendimiento y cuantitativas

Para la realización de estas pruebas, el entorno piloto reflejaba la arquitectura de acceso de la solución a pasar a producción.

Dentro de este ámbito se ha llevado a cabo varias pruebas de carga. Se han generado cargas para 5, 30, y 50 usuarios en un servidor y pruebas para 30 usuarios concurrentes en 5 servidores sobre el mismo host.

Prueba 1: 5 Usuarios concurrentes sobre 1 servidor virtual

El funcionamiento fue correcto durante toda la prueba. Los tiempos de respuesta fueron rápidos y en ningún momento, se pasó en cuanto a CPU's de 30% de utilización y el uso de memoria no pasó de 6GB de RAM. Hubo muy poca utilización de pagefile.

Esta prueba se realizó con finalidad de confirmar el funcionamiento correcto de la plataforma y verificar que los tiempos de respuesta eran los esperados. Se confirmó que los tiempos de respuesta no fueron mayores a un segundo

Prueba 2: 30 Usuarios concurrentes sobre 1 servidor virtual

El funcionamiento fue correcto durante toda la prueba. Los tiempos de respuesta estuvieron todos por debajo de 2.4 segundos. CPU por debajo del 50% y con una media de 20% de uso promedio. El uso de memoria no pasó de 9GB de RAM. Hubo muy poca utilización de pagefile.

Esta prueba tenía como finalidad simular el servidor con 30 usuarios concurrentes para probar que el funcionamiento del servidor era adecuado. Se confirmó que los tiempos de respuesta estuvieron dentro los límites de lo aceptable (por debajo de 2.5 segundos) y que el servidor todavía tenía recursos disponibles para su uso.

Prueba 3: 50 Usuarios concurrentes sobre 1 servidor virtual

El funcionamiento empezó a fallar durante la prueba, viéndose errores de sesión. Los tiempos de respuesta se dispararon a medias de 8-16 segundos para aplicaciones de productividad. CPU de forma constante en 70% - 80% con picos puntuales de másd el 90%, con uso de memoria no pasó de 10-11GB de RAM.

Se cargó el servidor con 50 usuarios concurrentes y se observó que el uso de procesadores estaba de manera constante por encima del 70%. Aunque el consumo de memoria estuvo de forma confortable dentro de los límites del servidor (por debajo de 11Gb de RAM), esto no se podría garantizar para aplicaciones con alto consumo de memoria. Se observó que las aplicaciones empezaron a dar timeout por tiempos de espera y se observaron fallos de conectividad de las sesiones. Los tiempos de respuesta con medias de entre 8 y 15 segundos demuestran que el servidor está funcionando por encima de sus posibilidades.

Prueba 4: 30 Usuarios concurrentes sobre 5 servidores virtuales

El funcionamiento fue correcto durante toda la prueba. Los tiempos de respuesta estuvieron todos por debajo de 2 segundos, que es el límite superior de lo aceptable para este tipo de entornos. CPU por debajo del

30% de utilización. El uso de memoria no pasó de 5GB de RAM. Hubo muy poca utilización de pagefile

Se confirmó la escalabilidad lineal de XenApp y que todos los servidores consumen alrededor del mismo número de recursos.

5.12 Mejoras y escalabilidad

En una plataforma que está en constante cambio y evolución es muy aconsejable disponer de entornos independientes para poder llevar a cabo las pruebas necesarias. Por lo tanto, se propone crear además del actual entorno de producción, un entorno de preproducción sin descartar un entorno de desarrollo. Quedando configurado del siguiente modo:

- Preproducción: Entorno donde se ejecutarán todas las pruebas de aplicaciones, cambios de configuración, parcheado, etc. Deberá ser un entorno lo más parecido posible al productivo y que sea de fácil reciclado. En este entorno se les da acceso a ciertos usuarios clave que ejecutaran las aplicaciones como si fueran productivas.
- Producción: Serán las máquinas destinadas a todos los usuarios finales. Cualquier cambio de configuración en este entorno deberá ser validado previamente en los otros dos entornos.

6. Presupuesto

6.1 Costes empleados

Este proyecto requerirá de un técnico senior y de un técnico junior, ambos de una empresa externa. Ambos, necesitarán ayudas en momentos determinados del departamento de sistemas de la empresa. SecurPat ha llegado a un acuerdo con una empresa externa donde el consultor externo cobrará 75€ la hora y el consultor junior 45€ la hora.

La planificación fijada, es la siguiente:

- a. Estudio y análisis actual.
- b. Análisis y diseño: Requisitos de la infraestructura, dimensionar máquinas virtuales, asegurar alta disponibilidad (HA), securización de acceso (certificados, encriptaciones), balanceo, etc.
- c. Implementación: Despliegue de todas la infraestructura y sus configuraciones.
- d. Fase de pruebas finales y validación: Testeo de rendimientos y latencias.
- e. Documentación.

En base a ambos, se obtiene la siguiente tabla con los costes por el servicio de los consultores:

Fase	Título	Duración	Coste
1	Estudio y análisis actual.	15 días	14.400 €
2	Análisis y diseño: Requisitos de la infraestructura, dimensionar máquinas virtuales, asegurar alta disponibilidad (HA), securización de acceso (certificados, encriptaciones), balanceo, etc.	7 días	6.720 €
3	Implementación: Despliegue de todas la infraestructura y sus configuraciones.	40 días	38.400 €
4	Fase de pruebas finales y validación: Testeo de rendimientos y latencias.	14 días	13.440 €
5	Tras paso de documentación.	7 días	6.720 €
	Total	83 días	79.680 €

Tabla 6.1 Costes en base a la planificación y consultores contratados

6.2 Costes licenciamiento

Además de estos costes, hay que añadir los servicios de licenciamiento que son necesarios obtener. Será necesario conseguir las licencias Citrix y Terminal server, por ello se ha generado la siguiente tabla con los costes adjuntos:

Licencia	Número	Coste por unidad	Coste total
Citrix	2000	100	200.000 €
Microsoft Terminal Server	2000	100	200.000 €
Total	4000	-	400.000 €

Tabla 6.2 Coste licenciamiento

6.3 Costes totales

En este apartado realizamos un cómputo global de todos los costes relacionados con la implantación de la solución planteada:

Concepto	Coste total
Personal	79.680 €
Licenciamiento	400.000 €
Total	479.680 €

Tabla 6.3 Coste total

7. Conclusiones

El principal objetivo de este proyecto era virtualizar y desplegar Citrix en la empresa con distintas clínicas, sedes y 2000 trabajadores. Este objetivo se ha conseguido satisfactoriamente.

Además, la plataforma implantada tiene alta disponibilidad, una gran escalabilidad que permita ir creciendo en un futuro tanto en usuarios, como en aplicaciones.

Con este proyecto, se ha conseguido que la empresa SegurPat mejore su infraestructura de IT, pero también se han conseguido otros requisitos que eran parte importante del proyecto, los cuales, se detallan a continuación:

1. Mediante XenApp se ha conseguido que los usuarios puedan lanzar aplicaciones que no estén instaladas en local, es decir, en sus propios equipos.
En este punto, también se incluye el requisito de VDIs, es decir, posibilidad de ejecución de escritorios remotos por parte de los usuarios, gracias a XenDesktop.
2. Posibilidad de guardar configuración de los usuarios gracias a las políticas aplicadas.
3. Reconexión de un usuario en caso de fallo de red y pérdida de conexión, como se fijó en los objetivos. Esto se permite gracias a las directivas de Citrix aplicadas.
4. Se ha configurado los elementos en alta disponibilidad. Esto permite que los servicios puedan balancearse ante posibles fallos de la plataforma, permitiendo que el servicio no se vea afectado y el usuario no note nada, pudiendo trabajar con normalidad.
5. Otro de los principales objetivos, era implantar una solución centralizada, permitiendo que todo se administrase desde un mismo punto. Este objetivo se ha conseguido con las consolas de XenApp y XenDesktop.
6. Disponer de un sistema escalable. El diseño implantado permite y ha tenido en cuenta la posibilidad de crecer en un futuro. La ampliación de equipos virtuales y nuevas aplicaciones, es rápido y sencillo, permitiendo que ante nuevas incorporaciones de empleados tengan el puesto de usuario configurado en pocos minutos.
7. Mapeo de unidades con los servidores utilizados. Se permite que los usuarios puedan realizar copy/paste y otras tareas necesarias para el día a día.

8. La red implantada es segura y cumple con los requisitos solicitados por el departamento de seguridad de SegurPat, permitiendo el acceso a la red de manera externa e interna y dejando a los empleados que puedan teletrabajar en caso de necesidad.
9. Tener una red segura con los accesos publicados a internet. Ya que tanto las aplicaciones, como los escritorios, se van a publicar hacía internet para poder consumirlas fuera de la red interna se deben realizar las configuraciones de seguridad oportunas.
10. Todas las necesidades de discos de red se ofrecen a través de la plataforma de SAN Corporativa basada en tecnología Netapp.

Gracias a este trabajo, he podido profundizar y aprender diferentes conceptos dentro de los servidores de aplicaciones y usuario. El tener una plataforma actualizado, nos permite aplicar soluciones actuales. Además, es necesario estar en continuo reciclaje debido a los avances tecnológicos que se van produciendo día a día.

No se ha conseguido seguir la planificación como estaba previsto, aunque si que se han cumplido los plazos de vencimiento. Esto es algo que debo mejorar de cara al futuro, acercando las planificaciones a la realidad e intentar cumplir los plazos e hitos marcados.

A futuro se podría explorar en temas de almacenamiento, backups y copias de seguridad, puesto que todas estas tareas e infraestructura es fundamental para cualquier empresa. Hoy en día, las empresas dedican muchos recursos a la seguridad de sus sistemas debido a la multitud de ataques diarios que reciben. Mucha información es sensible y cada día las normas de LOPD son más exigentes, lo que deriva en una mayor inversión económica y de recursos sobre mejorar estas líneas.

8. Glosario

SO - Sistema Operativo
RDS - Remote Server Desktop
ICA - Independent Computing Architecture
VDI - Virtual Desktop Infrastructure
RDP - Remote Desktop Protocol
FMA - FlexCast Management Architecture
IMA - Independent Management Architecture
HDX - High Definition Experience
AD - Active Directory
PVS - Provisioning Services
MCS - Machine Creation Services
CPD - Centro Procesamiento Datos
VIP - Virtual Server IP

9. Bibliografía

[1] Instalar StoreFront

<https://docs.citrix.com/es-es/storefront/3/sf-install-standard.html>

[2] XenApp y XenDesktop

<https://www.citrix.com/products/xenapp-xendesktop/>

[3] Plataformas Citrix

<http://www.robinhobo.com>

[4] Comunicaciones Citrix

<https://blog.citrix24.com/communication-ports-used-by-citrix-technologies/>

[5] Netscaler

<https://support.citrix.com/article/CTX139963>

[6] Licenciamiento

<https://www.citrix.es/products/xenapp-xendesktop/feature-matrix.html>

[7] Store Path

<https://docs.citrix.com/en-us/profile-management/5/upm-specify-user-store-path-den.html>

[8] Profile Management

<http://www.carlstalhood.com/citrix-profile-management/>

[9] pvDISK

<https://docs.citrix.com/es-es/xenapp-and-xendesktop/7-6/cds-pvd-intro.html>