IMPLANTACIÓN VDI HORIZON 8 CON MFA DE AZURE

Estudiante: Roberto Tenllado Salazar

Titulación: Grado de Ingeniería Informática

Consultor: Miquel Colobran Huguet

Fecha: Enero 2023

RESÚMEN

La motivación para realizar este proyecto es tratar de explicar las ventajas de una tecnología que ha aparecido hace relativamente poco tiempo, pero que se adapta perfectamente a las nuevas tendencias empresariales en cuanto a modalidad de trabajo. Además, se pretende hacer ver que un sistema VDI es adaptable a cualquier tipo de empresa, pudiendo añadir o quitar servicios según las necesidades específicas de la compañía.

En este proyecto concreto, se explica de forma detallada cómo sería una instalación plenamente funcional en un caso ficticio, siguiendo los estándares en cuanto a metodología. También se pretenden cubrir ciertas buenas prácticas en cuanto a calidad de la solución, como son la alta disponibilidad y seguridad del entorno. Por ello, se explica la necesidad de ciertos requisitos donde todos los servicios están redundados, la red segmentada y se realizan las instalaciones de servidores necesarias para que todos los roles queden duplicados.

Por otra parte, se añade una capa adicional de seguridad explicando cómo se debería realizar la implantación de un sistema de doble factor de autenticación para los usuarios. Para ello, se mezclan las posibilidades que ofrece VMware Horizon con una tecnología tan extendida hoy en día como es Microsoft Azure. De esta forma, los usuarios deben conocer su usuario/*password* y, además, tendrán que aceptar la conexión desde una aplicación instalada en su teléfono móvil. También se trata de facilitar la experiencia de usuario mediante la aplicación de *single sign-on* con el estándar SAML, evitando así tener que realizar validaciones adicionales.

ABSTRACT

The motivation for undertaking this project is to attempt to explain the advantages of a technology that has appeared relatively recently, but that adapts perfectly to the new business trends in forms of working. Furthermore, it intends to make clear that a VDI

system is adaptable to all types of companies, as services can be added or removed according to the specific needs of the company.

In this project specifically, a purely functional installation shall be explained in detail in a fictitious case, and following the standards about methodology. Additionally, certain good practices in terms of the quality of a solution shall be covered, such as the high availability and security of the environment. Thus, the necessity of certain requirements, where all the services are redundant, the network is segmented and the installations of necessary servers so that all the roles are duplicated, shall be explained.

Moreover, an extra layer of security is added, explaining how the implementation of a two-factor authentication system for users should be carried out. To this extent, the possibilities offered by VMware Horizon are mixed with a widespread technology of today, such as Microsoft Azure. In this way, users need to know their username/password and, also, will have to accept the connection from an application installed on their mobile phone. It also attempts to facilitate user experience through single sign-on via the app with the standard SAML, avoiding the necessity of having to complete additional validations.

ÍNDICE

ÍNDICE DE ILUSTRACIONES

1 Introducción

1.1 Justificación del TFG y contexto en el cual se desarrolla

Desde siempre, las empresas han querido que los trabajadores estén físicamente en sus oficinas. Se pensaba que un trabajador en sus instalaciones sería más fácil de controlar y con una menor tendencia a dejar sin hacer sus tareas y, por lo tanto, más productivo.

Sin embargo, esta mentalidad ha ido cambiando con el tiempo y se ha acentuado después de la pandemia del COVID, que obligó a las empresas a tener a sus empleados trabajando desde sus casas. Esta experiencia ha demostrado en la mayoría de los casos que un trabajador en remoto no sólo no es menos productivo, sino que puede serlo incluso más.

Por esta razón, en muchas de las empresas se plantean un modelo de negocio en el que sus empleados trabajan de forma remota, y se está extendiendo la implantación de sistemas VDI. Este sistema permite acceder remotamente a máquinas de la compañía, configuradas con las aplicaciones empresariales necesarias.

Además, este sistema tiene otras ventajas como son la homogeneización del parque de equipos cliente, la facilidad de administración y, una muy importante, el ahorro de costes. En este último punto existen algunas ventajas directas, como son el ahorro de máquinas físicas, y la gestión de la energía, ya que estos sistemas permiten el apagado o encendido de máquinas según la demanda. Pero también existen otros indirectos, como son el ahorro en el alquiler de oficinas, al no necesitar que sean tan grandes como para que quepan todos los empleados.

1.2 Objetivos del TFG

El objetivo principal de este proyecto es explicar el funcionamiento de un sistema VDI (Virtual Desktops Infrastructure), así como la forma en que éste se puede implementar en cualquier tipo de empresa. Dado que no es posible realizarlo en un entorno real

completo, se va a realizar en un entorno simulado definiendo una situación y parámetros iniciales que se puedan ajustar a un gran rango de organizaciones reales.

También es importante que esta implementación cumpla los requisitos de calidad, seguridad y alta disponibilidad que debería cumplir todo servicio informático de una compañía. Por esta razón, también se detallarán metodologías de trabajo y buenas prácticas recomendadas.

Por otro lado, se quiere cuidar un aspecto muy importante hoy en día; la seguridad. Para lo cual, se explicará la forma en que se pueden mezclar distintas tecnologías como son VMware Horizon y Azure, con el fin de que los usuarios tengan un método de autenticación en el que se requieran 2 factores: una password y un código generado aleatoriamente.

Otros objetivos que se pretenden lograr son de tipo personal y profesional. Uno de ellos es explicar el funcionamiento de una tecnología en claro crecimiento y, por otro lado, como decía anteriormente, también creo que es un trabajo enriquecedor profesionalmente, ya que, en informática es importante estar siempre al día de las nuevas posibilidades que van apareciendo. En el caso de un VDI con Horizon, es una tecnología en claro crecimiento, por lo que es un conocimiento muy demandado pensando en la posible aplicación en la vida profesional.

Otro aspecto importante es cómo interactúa un VDI con prácticamente todas las áreas dentro de una empresa, como redes, almacenamiento, virtualización, seguridad, Directorio Activo, etc. Este hecho supone un reto y una gran oportunidad de aprendizaje.

Como explicaba anteriormente, un VDI tiene actualmente mucha demanda y conocerlo es muy positivo para mi carrera profesional. Además, se trata de enriquecer este proyecto añadiendo MFA de Azure, que me permite ampliar aún más mi área de conocimiento en otra de las tecnologías más demandadas hoy en día, como es Microsoft Azure.

En resumen, se pretende determinar una serie de objetivos, numerados a continuación:

- Explicar funcionamiento y formas de implantación VDI

- Cumplir requisitos de calidad de la solución, en cuanto a alta disponibilidad metodología y buenas prácticas
- Cumplir expectativas en cuanto a seguridad de los datos y doble factor de autenticación

1.3 Enfoque y metodología seguida

Para realizar este proyecto se ha seguido una forma de trabajar acorde con los principios de la metodología ágil Kanban. De entre los 12 principios de esta metodología, y habiéndolos adaptado a este tipo de proyecto en algunos casos, destacaría:

- Aceptamos que los requisitos cambian.
- Responsables y desarrolladores trabajan juntos (tomando como responsable el profesor de la asignatura).
- Entrega de software (documentación en este caso) funcional frecuente.
- Individuos motivados.
- Software funcionando (puntos de la documentación completada), medida principal de progreso
- Desarrollo sostenido
- Excelencia técnica y buen diseño
- Maximizar la cantidad de trabajo no realizado
- Reflexionar sobre cómo ser más efectivo.

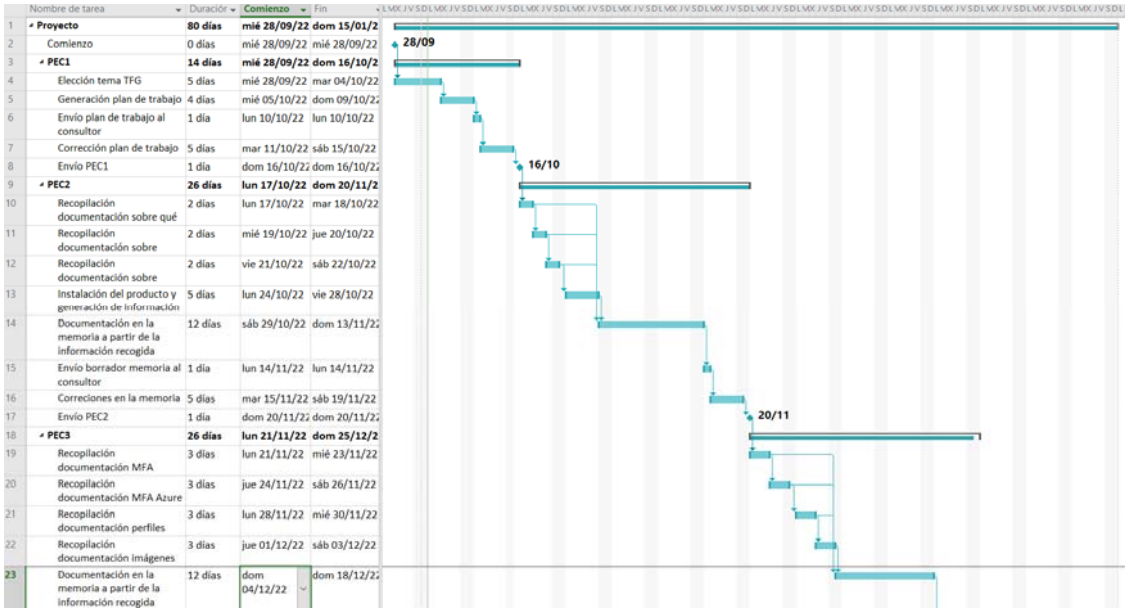
Siguiendo esta filosofía de trabajo, se ha utilizado una herramienta muy útil como Trello, en el que existe un tablero con columnas personalizables. En estas columnas, utilizadas como etapas del trabajo, se han establecido: Ideas, To Do, Doing, Done. De esta forma, se ha podido realizar un seguimiento del trabajo, de forma que rápidamente se pueda ver el estado del proyecto, así como dejar anotados puntos posibles de desarrollo.

Otra herramienta utilizada, que concuerda con el método Kanban y complementa a Trello es Microsoft Project. En ella se han repartido en el tiempo una serie de trabajos a realizar, de forma ordenada. Una de las ventajas de esta herramienta es que se han

podido establecer dependencias entre tareas, así como hitos importantes. Esta planificación está detallada en el punto siguiente.

1.4 Planificación del proyecto

El proyecto se ha dividido basándose en las 3 entregas a realizar durante el semestre, a lo largo de las cuales se cubre el total de los objetivos programados. A continuación, se adjunta un diagrama de Gantt con el detalle de la planificación realizada:



	Nombre de tarea	Duración	Comienzo	Fin
1	**Proyecto**	**80 días**	**mié 28/09/22**	**dom 15/01/2**
2	Comienzo	0 días	mié 28/09/22	mié 28/09/22
3	**PEC1**	**14 días**	**mié 28/09/22**	**dom 16/10/2**
4	Elección tema TFG	5 días	mié 28/09/22	mar 04/10/22
5	Generación plan de trabajo	4 días	mié 05/10/22	dom 09/10/2
6	Envío plan de trabajo al consultor	1 día	lun 10/10/22	lun 10/10/22
7	Corrección plan de trabajo	5 días	mar 11/10/22	sáb 15/10/22
8	Envío PEC1	1 día	dom 16/10/2	dom 16/10/2
9	**PEC2**	**26 días**	**lun 17/10/22**	**dom 20/11/2**
10	Recopilación documentación sobre qué	2 días	lun 17/10/22	mar 18/10/22
11	Recopilación documentación sobre	2 días	mié 19/10/22	jue 20/10/22
12	Recopilación documentación sobre	2 días	vie 21/10/22	sáb 22/10/22
13	Instalación del producto y generación de información	5 días	lun 24/10/22	vie 28/10/22
14	Documentación en la memoria a partir de la información recogida	12 días	sáb 29/10/22	dom 13/11/2
15	Envío borrador memoria al consultor	1 día	lun 14/11/22	lun 14/11/22
16	Correciones en la memoria	5 días	mar 15/11/22	sáb 19/11/22
17	Envío PEC2	1 día	dom 20/11/2	dom 20/11/2
18	**PEC3**	**26 días**	**lun 21/11/22**	**dom 25/12/2**
19	Recopilación documentación MFA	3 días	lun 21/11/22	mié 23/11/22
20	Recopilación documentación MFA Azure	3 días	jue 24/11/22	sáb 26/11/22
21	Recopilación documentación perfiles	3 días	lun 28/11/22	mié 30/11/22
22	Recopilación documentación imágenes	3 días	jue 01/12/22	sáb 03/12/22
23	Documentación en la memoria a partir de la información recogida	12 días	dom 04/12/22	dom 18/12/2

	Nombre de tarea	Duración	Comienzo	Fin
24	Envío borrador memoria al consultor	1 día	lun 19/12/22	lun 19/12/22
25	Correcciones en la memor	5 días	mar 20/12/22	sáb 24/12/22
26	Envío PEC3	0 días	dom 25/12/2	dom 25/12/2
27	Presentación final	10 días	lun 26/12/22	vie 06/01/23
28	Envío presentación consulto	1 día	sáb 07/01/23	sáb 07/01/23
29	Correcciones presentación	7 días	dom 08/01/2	sáb 14/01/23
30	Entrega presentación final	1 día	dom 15/01/2	dom 15/01/2

1.5 Descripción del resto de capítulos de la memoria

En el desarrollo de esta memoria, se comienza explicando la situación actual con respecto a las nuevas ideas sobre forma de trabajar, sobrevenidas en su mayor parte por el impacto del COVID. A partir de ahí, se presentan diferentes soluciones capaces de abordar el problema planteado y se expone en qué consiste VDI. Una vez planteadas las distintas opciones, se explican las ventajas/desventajas que presentan cada una de ellas.

A continuación, se crea un capítulo en el que se explica la situación inicial de la que surge el caso de uso sobre el que va enfocado este TFG. En él se explica el supuesto de una empresa en una situación en la que se encuentran muchas empresas, que se ven en la obligación de tomar una decisión importante. Estas empresas parten de una forma de trabajar consolidada y una inversión en infraestructuras importante.

Tras el planteamiento de la situación inicial, se presenta una propuesta de solución y unos requisitos sobre los que parte este proyecto, con el objetivo de concentrarse lo máximo posible en el producto VMware Horizon y la mejora en cuanto a seguridad con la implantación de MFA con Azure AD.

Una vez establecida la base, se explica en qué consiste la arquitectura de Horizon, explicando cada uno de los roles necesarios para su implantación. Tras esta explicación necesaria para comprender las funciones que llevan a cabo cada uno de los servidores instalados, se explican una serie de servicios y configuraciones previas, necesarios para asegurar el nivel de calidad, seguridad y organización deseado.

En los siguientes capítulos se explicará toda la instalación necesaria, poniendo el detalle de estas instalaciones en los diversos anexos creados al final del documento. Entre las instalaciones, además de la infraestructura, también se encuentran las necesarias para optimizar la plataforma y conseguir la mejor experiencia de usuario posible.

Finalmente, se presenta como quedaría la arquitectura de la empresa, así como la formación necesaria a los usuarios para asegurar en la medida de lo posible el éxito del cambio realizado.

2 La movilidad en el entorno laboral

Cada vez más, las empresas y trabajadores de éstas demandan el poder realizar su trabajo sin la necesidad de estar físicamente en la oficina. Como muchos de los avances tecnológicos, hacer uso de ellos puede resultar una ventaja competitiva importante frente a competidores que las aprovechan. Aprovechar estas tecnologías con respecto a la movilidad, puede ayudar a las empresas a captar talento ya que, por un lado, es una posibilidad muy atractiva para los trabajadores, y por el otro, facilita que los trabajadores no sean ni siquiera del mismo país. También son muy importantes los ahorros de costes que facilitan. En la siguiente imagen se pueden ver las razones más importantes por las que las empresas pueden verse atraídas a facilitar el teletrabajo:

Ilustración 1. Motivos teletrabajo [1]

Desde el punto de vista de los empleados, la posibilidad de trabajar desde casa ofrece algunos beneficios como el bienestar, ya que, permite no tener que desplazarse hasta la oficina, evitando así atascos si se viaja en coche o la incomodidad del transporte público. También permite mayor flexibilidad de horarios y la posibilidad de conciliar el trabajo y la vida familiar, lo que repercute en mayor productividad.

Por culpa del COVID las empresas se vieron obligadas a enviar a los trabajadores a sus casas y facilitarles que pudiesen trabajar desde allí. Esto provocó que las compañías

realizaran una inversión en infraestructuras para permitir el teletrabajo, y que pudiesen comprobar como afectaba esta nueva situación en la productividad de los empleados, así como en los costes de la propia empresa. Desde entonces, se ha ido poco a poco volviendo a la situación anterior en cuanto a restricciones, pero el teletrabajo, en muchos casos, se ha mantenido.

Basta con mirar las condiciones que se ofrecen en las ofertas de trabajo publicadas en sitios como LinkedIn para darse cuenta de que el teletrabajo no ha sido una moda pasajera o algo puntual debido a la situación médica, sino que existe una clara tendencia a que las empresas lo ofrezcan como un incentivo para el trabajador. La siguiente imagen arroja algunos datos que responden a la pregunta "¿está tu empresa considerando introducir el teletrabajo como una política estandarizada?"

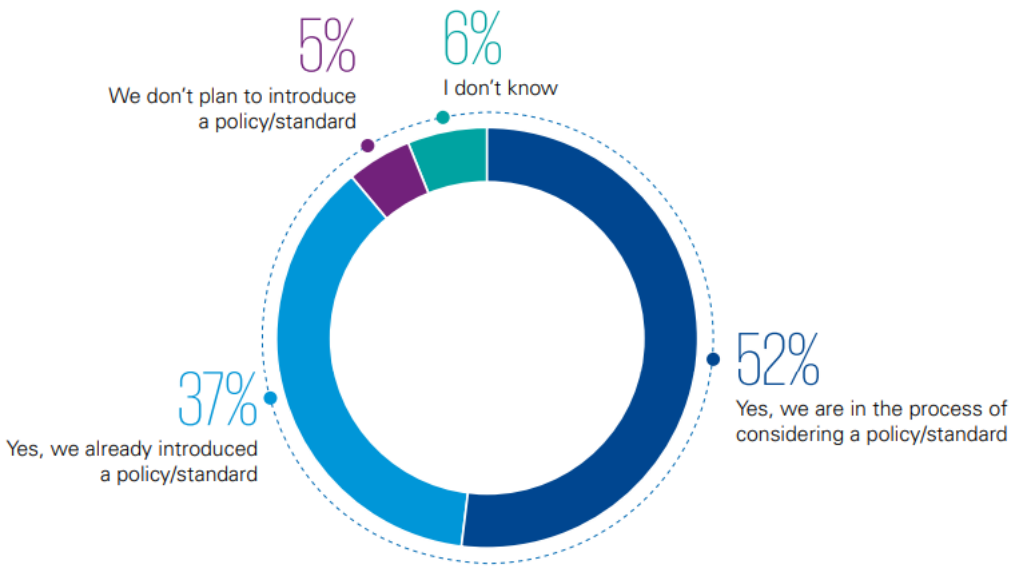


Ilustración 2. Tendencia teletrabajo [2]

También es importante tener en cuenta estos datos respecto al sector al que se dedica la empresa, siendo más sencillo aplicarlo a empresas dedicadas a las telecomunicaciones y tecnología, como muestra la siguiente imagen:

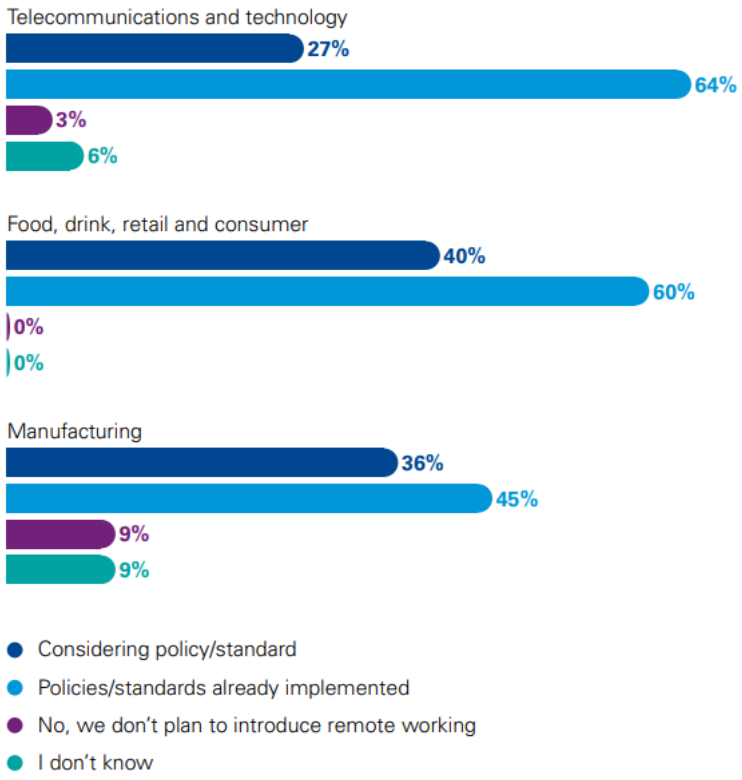


Ilustración 3. Teletrabajo según sectores [3]

3 Qué es VDI

3.1 Tecnologías de escritorios remotos

Hoy en día existen en el mercado diversas opciones que permiten a las empresas habilitar la opción del teletrabajo para sus empleados. Cada una con sus ventajas y desventajas. A continuación, se describen algunas de estas opciones:

- VPN (Red Privada Virtual). Esta tecnología permite crear un túnel seguro a través de Internet, cifrando la comunicación de extremo a extremo (red de la empresa y el dispositivo cliente). De esta forma, un usuario puede conectarse de forma segura a la red interna de la empresa como si estuviese físicamente en ella.
  Una vez dentro de la red, el usuario puede conectarse de forma remota usando Terminal Server, por ejemplo, y trabajar en el PC ubicado en la oficina.
  Con la VPN conectada a la red también puede acceder a las webs internas, así como a los servidores de ficheros.
- Aunque no es un VDI propiamente dicho, en vez de publicar escritorios con aplicaciones a los usuarios, se pueden publicar directamente las aplicaciones. De esta forma, un usuario se podría conectar desde su casa a un portal web y acceder a las diferentes aplicaciones que le permiten realizar sus tareas.
  Es importante recordar que en este caso se estarían publicando solamente aplicaciones, por lo que no habría acceso a la red de la empresa ni a ningún recurso como servidores de ficheros.
- RDS (Remote Desktop Services). Permite la conexión de varios usuarios a la misma máquina de forma concurrente. Teniendo una máquina o varias, según el balanceo de carga necesario, los usuarios pueden conectarse y trabajar en su propia sesión, dentro de la misma máquina
  Para que los usuarios puedan conectarse, las máquinas sobre las que se conectan los usuarios, han de tener todas las aplicaciones instaladas de forma que puedan ser multiusuario.

3.2 Tecnología VDI

Para entender el concepto de VDI, primero hay que comprender de forma básica qué es la virtualización. Tradicionalmente, un PC o un servidor tenía unas características y capacidades como procesadores, RAM… que, a su vez, tenía instalado un sistema operativo y una serie de aplicaciones con las que el usuario interactuaba. Entre el hardware del PC, el software del SO y aplicaciones, existían también una serie de *drivers* que permitían la interacción entre ellos, de forma que este conjunto software-hardware era indivisible.

Gracias a la virtualización se logró separar este conjunto, permitiendo que la asignación de recursos hardware estuviesen controladas por software. Además, las máquinas físicamente están en archivos guardados en carpetas dentro de discos duros de una cabina, un servidor, etc.

VDI viene de las siglas en inglés Virtual Desktops Infraestructure, que hace referencia al sistema por el cual los usuarios pueden hacer uso de escritorios virtuales, que sustituyen a los clásicos PCs. Además, permite acceder a estos a través de un entorno seguro, y desde cualquier lugar y dispositivo. Este hecho trae consigo numerosas ventajas y permite cambiar la forma en la que trabajan los empleados.

La infraestructura VDI se compone de uno o varios servidores físicos donde se instala el hypervisor, que es el software encargado de la virtualización. Una vez instalado, este software toma el control de los recursos de los servidores físicos y los distribuye en las diferentes máquinas virtuales que se irán creando. Dentro del entorno VDI estas máquinas virtuales serán de 2 tipos: los servidores que se reparten los diferentes roles y que permiten al administrador disponer del conjunto de servicios que lo convierten en un entorno funcional, como seguridad, administración, publicación de escritorios, etc. Y las máquinas cliente, sobre las que se conectarán los usuarios.

Esta infraestructura facilita una serie de ventajas como son el ahorro de costes, seguridad y gestión. Sin embargo, la más importante es que permite el acceso a la máquina desde cualquier lugar y dispositivo. Este hecho permite que los empleados de una empresa tengan la oportunidad de teletrabajar, lo que puede reportar un valor

añadido a la empresa. Además, permite que los empleados puedan trabajar desde sus propios dispositivos, lo cual sería útil en aquellas empresas u organismos públicos en las que se contrata personal externo.

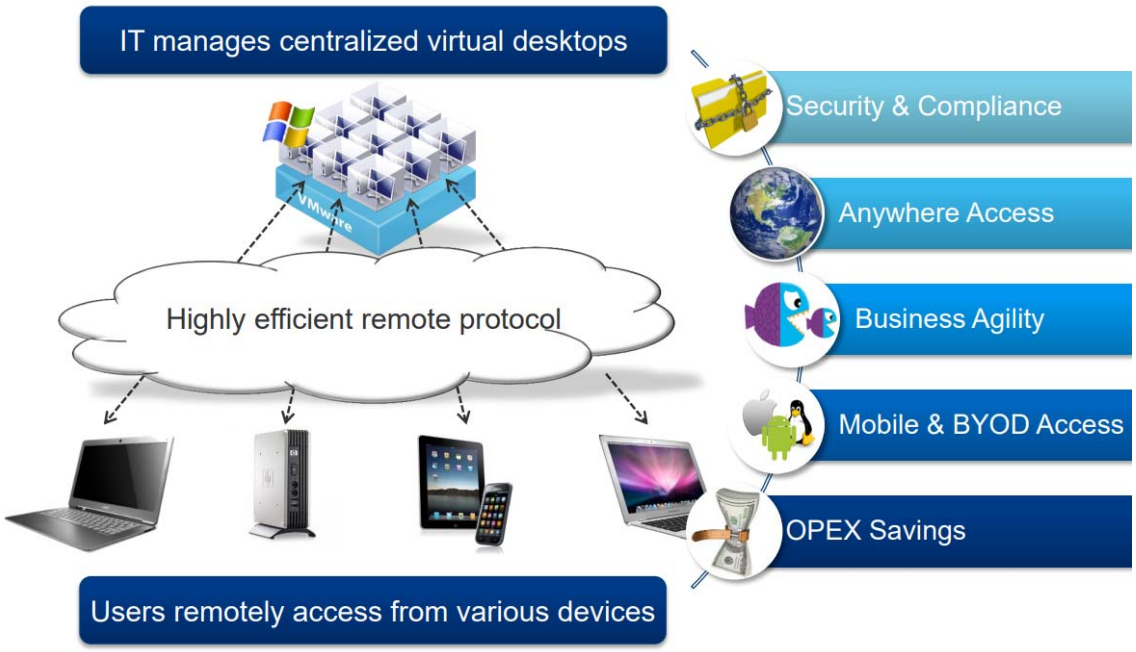


Ilustración 4. Ventajas VDI [4]

Como es normal, existen algunas diferencias entre la forma clásica de trabajar y un VDI. Para evitar que la experiencia de usuario sea diferente, y que esto pueda ser un motivo de rechazo en un primer momento, dentro de la infraestructura VDI, en la que se comparten máquinas virtuales para que accedan los usuarios, 2 opciones de configuración diferentes. Estas 2 opciones se explican a continuación:

- Escritorio virtual persistente. Es la configuración más parecida a la forma tradicional. La máquina a la que se conecta cada usuario es solamente para ese usuario y siempre se conectará a ella, lo que permite una completa personalización por parte del usuario, así como guardar configuraciones y tareas dentro de la propia máquina. En el lado negativo de esta configuración, hay que decir que necesita una mayor cantidad de recursos, ya que hay que tener una máquina virtual por cada usuario y que se pierde control sobre las máquinas por parte de los administradores.
- Escritorio virtual no persistente. Las máquinas son clones hechos desde una imagen maestra, llamada “Golden” y cada vez que una máquina se reinicia, ésta

se destruye y se vuelve a crear una nueva imagen. Esto hace que los usuarios no puedan realizar ciertas personalizaciones, que no puedan guardar documentos fuera de los discos de red y que no puedan instalar nuevo software. A cambio, se ahorran una gran cantidad de recursos, ya que solamente será necesario tener encendidas tantas máquinas virtuales como usuarios concurrentes estén trabajando. También permite a los administradores tener un control total sobre las máquinas, a través de la plantilla "Golden"

En cuanto al ámbito de aplicación de una infraestructura VDI, la puede utilizar prácticamente cualquier organización. Para explicarlo, definiría 4 bloques principales que cubran las necesidades de todas ellas:

- **Teletrabajo/Presencial**. La implantación de una infraestructura VDI es aplicable principalmente a cualquier empresa que quiera dotar a sus trabajadores de la posibilidad de trabajar desde ubicaciones remotas. Pero también, es aplicable a compañías que quieran que sus empleados trabajen presencialmente y quieran beneficiarse del ahorro de costes que supone el hecho de no necesitar equipos cliente potentes, capaces de correr las aplicaciones necesarias para el desempeño de sus funciones.
- **Tamaño**. Gracias a la oferta existente en el mercado de este tipo de sistemas, y a las diferentes configuraciones posibles en cuanto a capacidad de máquinas cliente, servidores, tolerancia a fallos… se ajusta a cualquier compañía, independientemente del tamaño. Se puede implementar tanto en una compañía con miles de empleados, repartidos por todo el mundo, como en una con tan solo 50 empleados, todos pertenecientes a la misma sede.
- **Grados de confidencialidad**. No todas las empresas tienen los mismos niveles de confidencialidad, aun siendo la seguridad importante para todas ellas. Un sistema VDI puede aplicar diversas capas de seguridad, adaptándose a las necesidades del cliente. Por ejemplo, en una empresa puede ser necesario una DMZ con un servidor que actúe de proxy inverso en ella, tráfico SSL y doble factor de autenticación, mientras que en otra es necesaria solamente asegurar el tráfico SSL.

- **Empresa pública/privada**. Esta solución se adapta perfectamente a empresas privadas, así como a organismos públicos, donde cada vez se da con más frecuencia el teletrabajo y disponen de recursos económicos y humanos para invertir en tecnología. Además, estos organismos suelen tener acuerdos con los fabricantes, que les permite disponer de licencias a un menor coste.

3.3 Tendencias actuales en tecnologías de escritorios remotos

Cada tecnología tiene sus puntos fuertes, por lo que es importante definir bien las necesidades que se quieren cubrir y conocer las características que ofrece cada uno de los productos, antes de tomar una decisión. A continuación, vamos a describir algunas de las posibilidades más frecuentes.

Una de las limitaciones más comunes viene dada por el presupuesto disponible para la implantación de la nueva solución. En este sentido, se podrían clasificar las opciones según su precio, en el que aparecerían de más barato a más caro: VPN, RDS, VDI. Sin embargo, además del precio también hay que tener en cuenta la necesidad que se quiere cubrir, por lo que el precio no puede ser un factor definitivo, si esa solución no resuelve el problema en su totalidad.

Otro de los factores a tener en cuenta es si la empresa no quiere adquirir máquinas cliente capaces de correr las aplicaciones que utilizan los usuarios en su trabajo. En una solución con VPN, tan solo se permite el acceso a la red interna, pero los usuarios han de disponer de máquinas con recursos suficientes como para poder ejecutar estas aplicaciones.

En VDI o RDS no habría este problema, ya que los usuarios se conectan a una máquina, que es la que realmente realiza el trabajo. Sin embargo, en RDS la máquina es compartida con otros usuarios, y aunque esté bien balanceada la carga en varias máquinas, un usuario siempre depende de que otro conectado a la misma ejecuta una tarea que consuma demasiados recursos y deje al resto sin poder trabajar.

Este problema descrito en el párrafo anterior no ocurriría con VDI al disponer cada usuario de su propia máquina, y con unos recursos asignados según su perfil de trabajo. Además, en RDS para poder realizar múltiples conexiones concurrentes, la máquina ha de tener un SO de servidor, lo que penaliza la experiencia de usuario.

Otro punto importante es la personalización que se puede dar a cada usuario. En una conexión VPN, no hay personalización específica porque tan solo es una conexión a la red interna. Sin embargo, se podría tener un PC encendido para cada usuario y que estos se conectasen desde casa a ellos, a través de la VPN. El problema de esta configuración es el gasto eléctrico que requiere, así como el mantener un PC en las oficinas solamente para poderse conectar de forma remota, posiblemente desde un portátil también facilitado por la empresa.

De nuevo, el problema planteado con VPN no ocurre con RDS ni VDI, aunque en RDS seguiríamos teniendo el problema de los recursos compartidos. En cuanto a la personalización de perfiles, al ser distintos usuarios entrando en la máquina, en RDS cada uno podría configurar sus preferencias, sin embargo, habría que poner atención al tamaño de cada perfil de usuario que podría comprometer el espacio disponible de la unidad de disco donde se guardasen estos perfiles.

Con VDI no tendríamos estos problemas de personalización ni de espacio en disco. Además, podríamos generar ciertas personalizaciones y aplicarlas solamente a ciertos tipos de usuario, según pertenencia a grupos, a perfil de imagen, etc.

4 Comparativas soluciones VDI

En el mercado se puede encontrar una gran cantidad de productos que permiten implantar una solución VDI. Cada uno de ellos tiene sus propias peculiaridades, con sus ventajas e inconvenientes, que lo pueden hacer más apto para determinado entorno. No existe una solución idónea para todos los escenarios posibles, por lo que es importante que antes de adquirir un determinado producto, se compare y, si es posible, se realice una prueba de concepto con distintas soluciones.

Aquí vamos a hacer una breve comparación entre los productos más extendidos en el mercado, primero presentando cada uno de los 3 productos que se comparan, y luego se explicarán las principales diferencias entre ellos.

4.1 Citrix

Citrix Systems es una de las empresas líderes en el sector, quizá la más extendida del mundo con 100 millones de usuarios en más de 100 países, según los datos recogidos en su web empresarial. Fundada en 1989, tiene una larga experiencia en productos de trabajo digital y ha sido reconocido con diferentes premios internacionales en este ámbito.

Los productos de VDI de Citrix han pasado por diferentes nombres, debido principalmente a la adquisición de varias empresas y proyectos, como es el caso de Xen, de código abierto y adquirido en 2007.

También dispone de un protocolo propio para este tipo de comunicaciones: “ICA” (Arquitectura de Cómputo Independiente), más eficiente en el tráfico de datos entre servidor y clientes. Entre sus ventajas, permite que en un servidor corran diversas aplicaciones y que sean accesibles desde un cliente que use este protocolo.

El último producto de Citrix es Virtual Apps and Desktops 7, muy enfocado a entornos Cloud, aunque también es compatible con instalaciones OnPremise. Este producto supone una solución integral de administración, seguridad y escritorios virtuales. La

arquitectura de esta solución se puede ver en la imagen siguiente, y cuenta con una seria de elementos que permiten la securización de conexiones provenientes de Internet, así como validación de usuarios con un Directorio Activo de Windows.

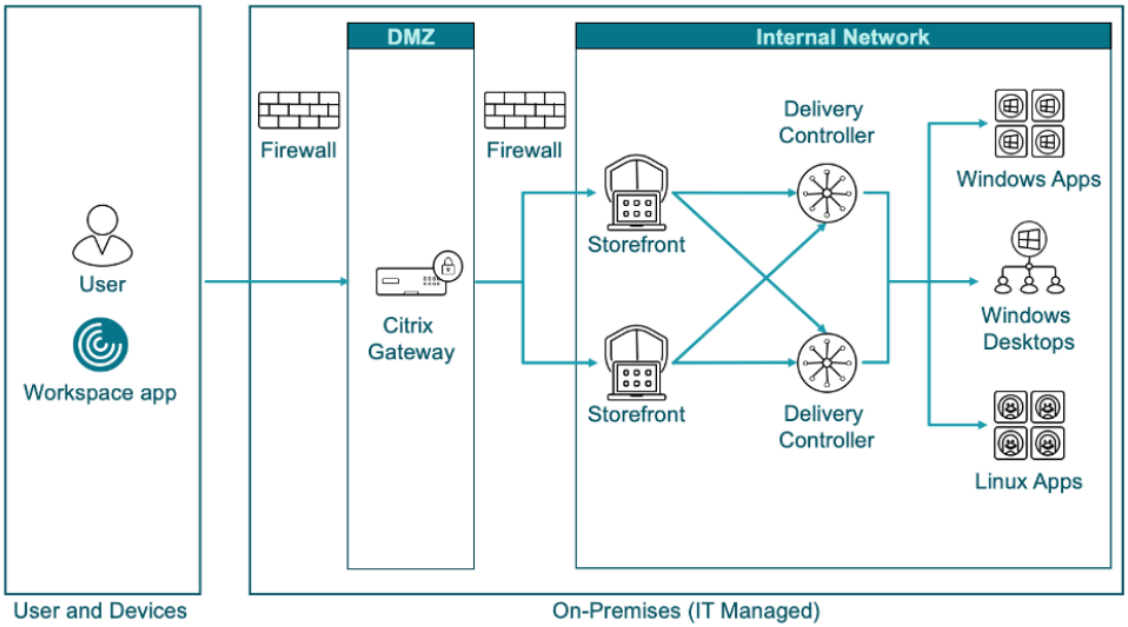


Ilustración 5. Arquitectura Citrix [5]

4.2 VMware Horizon

VMware Horizon es un producto de VMware Inc., una empresa filial de EMC Corporation que, a su vez, fue adquirida hace unos años por Dell Inc. VMware fue creada en 1998 y es líder mundial en virtualización de máquinas, reconocida con diversos premios internacionales.

Su producto más reconocido es VMware vSphere, creado en el año 2009 y que ha ido incorporando más capas de virtualización. En su comienzo este software solamente era capaz de virtualizar máquinas, tanto clientes como servidores. Gracias al éxito que tuvo desde sus inicios, la compañía continuó creciendo e hizo algunas adquisiciones estratégicas como Nicira en 2012, especialista en la virtualización de redes, o de AirWatch en 2014. Este hecho junto a desarrollos propios, ha permitido que hoy en día se pueda virtualizar todo lo necesario en una empresa, como máquinas servidoras, clientes, networking, almacenamiento, etc.

Debido a la estrecha relación entre entornos VDI y virtualización de máquinas, en el que eran líderes del sector, VMware lanzó en 2014 su producto VMware Horizon para poder proveer a sus clientes de una arquitectura de escritorios virtuales.

Su último producto es VMware Horizon 8, con una arquitectura como la que se muestra en la imagen a continuación. Esta arquitectura permite integrarse en una empresa que cuente con la virtualización proporcionada por vSpere, y permita a sus clientes una administración centralizada, así como conexiones seguras.

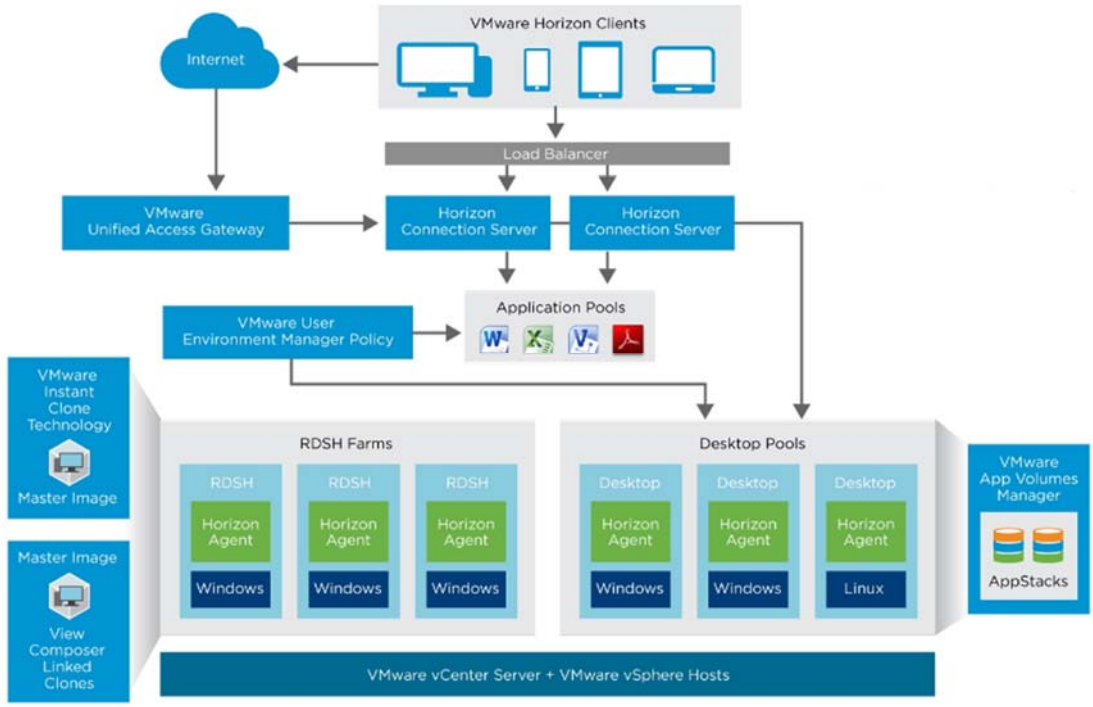


Ilustración 6. Arquitectura Horizon [6]

4.3 Microsoft Remote Desktop Services (RDS)

RDS es un producto de Microsoft, una de las empresas más valiosas a nivel mundial y líder en sistemas operativos, aplicaciones ofimáticas, etc. También dispone de otros productos de desarrollo propio o a través de adquisiciones como LinkedIn o Skype.

Microsoft también dispone de experiencia en la virtualización de máquinas a través de su producto Hyper-V, incluido de forma gratuita dentro de una licencia de servidor. Este

sistema de virtualización dispone de la tecnología necesaria para virtualizar distintas capas además de las máquinas, como la red o el almacenamiento.

RDS permite la conexión de varios usuarios a una sola máquina, de forma simultánea. De esta forma, se pueden usar aplicaciones, hardware, etc… sin la necesidad de adquirir más licencias o máquinas y, además, provee un acceso desde distintos dispositivos de forma remota.

Para realizar las conexiones, se utiliza el protocolo propietario de Microsoft "RDP". Este protocolo establece un canal en el que la información gráfica es codificada y enviada en ambos sentidos. Es decir, un canal desde el servidor al cliente y otro desde el cliente al servidor, en el que se envían las pulsaciones de teclas y movimientos y pulsaciones del ratón hasta el servidor.

En la imagen siguiente, se puede ver cómo funciona una arquitectura RDS. Las conexiones de los clientes son redirigidas desde la ubicación de estos hasta el servidor o la granja de servidores, en la que están instaladas las aplicaciones y que serán sobre los que se conectan los usuarios.

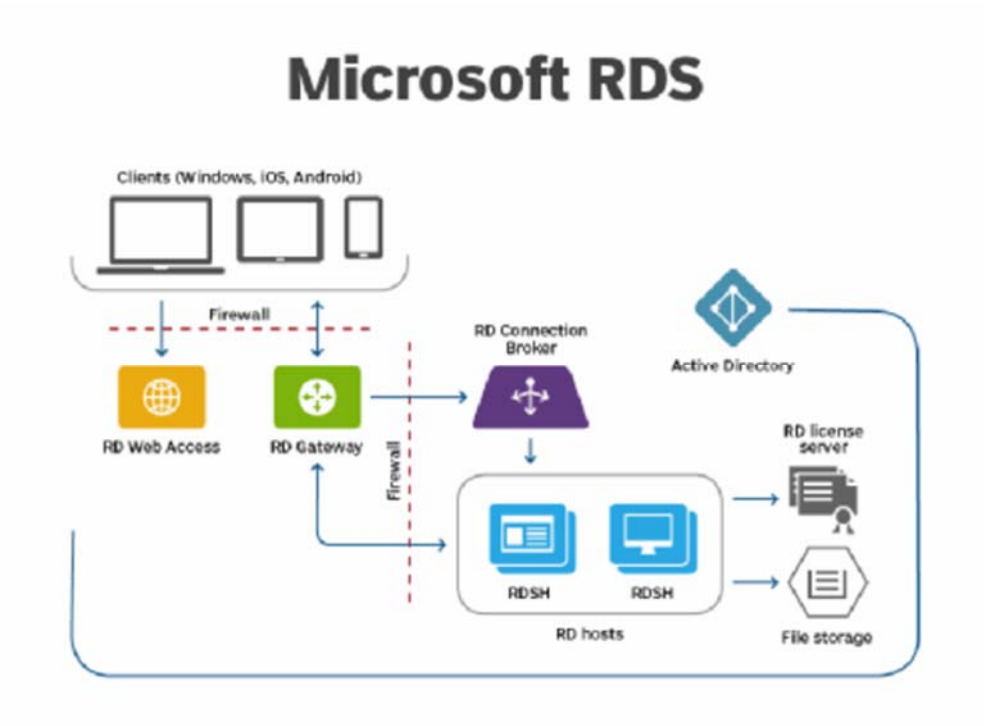


Ilustración 7. Arquitectura RDS [7]

4.4 Comparativa

4.4.1 RDS vs vmWare Horizon y Citrix

Primero habría que hacer una separación entre los 3 productos, separando por un lado Citrix y VMware y, por otro lado, RDS. Esta separación se debe a que, con el primer grupo, los usuarios no comparten máquina en ningún caso, cada cliente se conecta a una máquina propia para esa sesión, aunque en la próxima sesión se conecten a una máquina en la que anteriormente estuvo otro usuario. Sin embargo, en RDS los usuarios comparten la máquina, siendo sesiones concurrentes dentro de una misma máquina.

Entre las diferencias de un sistema y otro, se encuentra el hecho de que para poder ejecutar las sesiones concurrentes de RDS, se tiene que realizar sobre un entorno servidor, mientras que en las otras 2 son escritorios de cliente. Este puede ser un hecho relevante desde el punto de vista de los usuarios, ya que se pueden encontrar con que algunas aplicaciones no se pueden instalar.

Otro punto que podría ser problemático en RDS es el hecho de que compartan máquina, lo que puede dar lugar a situaciones como que un usuario no puede reiniciar lo que él percibe como “su” máquina después de instalar una aplicación, ya que este reinicio afectaría a los demás usuarios conectados al mismo servidor.

En cambio, RDS permite publicar aplicaciones y proporcionar escritorios a distintos usuarios con un coste económico mucho menos elevado. Este hecho, desde el punto de vista empresarial, y dependiendo del servicio que se quiera dar y el número de usuarios a los que se quiere dar este servicio, puede ser un punto muy importante.

4.4.2 VMware Horizon vs Citrix

Como se explica anteriormente, no hay una solución válida de VDI puro, como son estos 2 productos, para cualquier tipo de entorno. Cada solución tiene sus propias ventajas y desventajas, y dentro de los entornos, cada uno tiene sus propias peculiaridades y prioridades. Por ello, para establecer una comparativa entre ambos productos, se han

seleccionado una serie de criterios sobre los que hacer una comparación directa. Estos criterios son los siguientes:

- Tamaño de la organización
    - Vmware Horizon: Mediana y grandes compañías
    - Citrix: Pequeñas, medianas y grandes compañías, cloud
- Hypervisores soportados
    - Vmware Horizon
        - VMware vSphere
    - Citrix
        - Microsoft Azure Resource Manager
        - Citrix Hypervisor (XenServer)
        - VMware vSphere
        - Microsoft System Center Virtual Machine Manager
        - Amazon Web Wervices
        - Nutanix Acropolis
        - Oracle Cloud Infraestructure
- Complejidad de la arquitectura
    - Vmware Horizon. Horizon es sencillo y rápido de implementar y mantener
    - Citrix. Su implementación y mantenimiento es complejo, pero también permite una mayor granularidad en su configuración
- Mecanismos de aprovisionamiento de máquinas
    - Ambas soluciones se basan clones desde una imagen base
- Precio
    - Para tener el mismo nivel de herramientas, las licencias de Horizon son más caras que las de Citrix. Además, hay que tener en cuenta que VMware vSphere es un requisito de Horizon, por lo que este coste también habría que sumarlo.

Como se puede observar en los datos anteriores, depende en gran medida de las necesidades y la infraestructura actual de la empresa, la decisión entre uno de los 2 productos. Por un lado, podemos ver que Horizon no está pensado para pequeños entornos, por lo que es una medida que puede decidir a muchos clientes.

También es importante el Hypervisor que vamos a usar, ya que Horizon tan solo soporta el suyo propio, aunque éste sea, quizá, el más potente y más extendido hoy en día. Esto es importante tanto a nivel de la calidad del servicio que vamos a dar, como del precio que tendrá la solución en caso de que no se disponga de VMware vSphere.

En cuanto a las opciones que provee cada uno de ellos, ambos son muy parecidos, pudiendo sobresalir uno en unos casos y el otro producto en otros. Por ejemplo, Citrix dispone de una opción de actualización de parches de las máquinas mediante streaming, que no dispone Horizon y hay que actualizar la imagen Golden y redistribuir las máquinas. Sin embargo, Horizon dispone de un protocolo de aceleración de gráficos 3D (PCoIP) mucho más optimizado que el de Citrix (HDX).

4.5 Resumen de comparativa

A continuación, se incluye una tabla comparativa entre las 3 tecnologías:

Propiedad	RDS	VMware Horizon	Citrix
SO compartido	SO servidor	SO servidor/cliente	SO servidor/cliente
Tipo máquina cliente	Física/Virtual	Virtual	Virtual
Precio	Económico	Medio/Alto	Alto
Tamaño empresa	Pequeña/media	Todos los tamaños	Media/Grande
Hipervisores soportados	N/A	Gran variedad de Hipervisores	VMware
Complejidad	Pequeña	Muy grande	Media/Grande

5 Situación inicial

El caso de uso planteado va orientado a aquellas empresas que ya dispongan de una infraestructura plenamente funcional y que entre sus objetivos se encuentran el proporcionar a sus empleados una arquitectura que les permita poder trabajar desde sus casas y, además, que le ofrezca la posibilidad de ahorrar costes.

La mayoría de empresas ya se encuentran en esta situación, con toda la infraestructura de servidores, red, bases de datos… ya funcionando en producción y no necesitan una instalación desde cero, sino adaptar lo que tienen para disponer de los nuevos servicios. Entre las posibles organizaciones se encuentran tanto empresas privadas como organismos públicos que disponen de personal interno y trabajadores externos, que han sido contratadas para realizar proyectos concretos o para mantener los sistemas existentes.

5.1 Planteamiento del caso de uso

El escenario que se plantea es el de un organismo público que a raíz de la pandemia han comprobado que el teletrabajo funciona y, desde la dirección, se quiere fomentar. Entre las debilidades que se han identificado en dicho escenario, se pueden encontrar:

- Las máquinas cliente están amortizadas y no se quiere realizar una gran inversión en la adquisición de nuevas máquinas
- No se quiere realizar una inversión en dotar a los trabajadores de portátiles con capacidad suficiente para trabajar desde casa, así como la adquisición de licencias para la conexión VPN
- El gran número de trabajadores entre internos y externos de los distintos departamentos (sistemas, desarrolladores, etc.), compromete el espacio existente en las oficinas.
- El gasto que viene derivado de mantener el equipamiento de los trabajadores externos (luz, máquinas cliente)

Ante esta situación, se quiere dotar a la organización de un sistema que permita el acceso remoto de los trabajadores, tanto internos como externos, que sea capaz de salvar los problemas detectados, y dando prioridad a la seguridad de los datos con los que se trabaja.

5.2 Descripción de la propuesta

Una vez vistas las debilidades del caso de uso y atendiendo a las prioridades marcadas por la organización, descritas en el punto anterior, se propone la implantación de un sistema VDI con VMware Horizon, que facilite el acceso corporativo desde cualquier lugar y que aproveche las infraestructuras existentes.

Este sistema permitirá a la empresa dotar de la posibilidad de teletrabajo a sus usuarios, pudiendo así reducir el número de máquinas físicas disponibles en las oficinas. Esto supone una doble ventaja, ya que elimina la necesidad de tener un equipo físico por usuario, así como un espacio reservado para cada uno, ya que los equipos que quedasen disponibles se podrían usar como “puestos calientes” para los trabajadores “in situ”.

También permite conectarse desde casa a la red empresarial sin la necesidad de disponer de una máquina con unos requisitos que permitan la realización de sus tareas, ya que toda la carga de trabajo se realizará en las máquinas virtuales. Este sistema también permite personalizar el tipo de máquina que usa cada perfil de usuario, ya que las necesidades no serán las mismas para un usuario administrativo que para un desarrollador de software.

Para cumplir con el requisito de la seguridad, se propone que los usuarios deban iniciar sesión mediante un doble factor de autenticación. Este se realizará usando las credenciales de Dominio y un número aleatorio generado por una aplicación móvil. Para ello, se utilizará MFA de Azure AD.

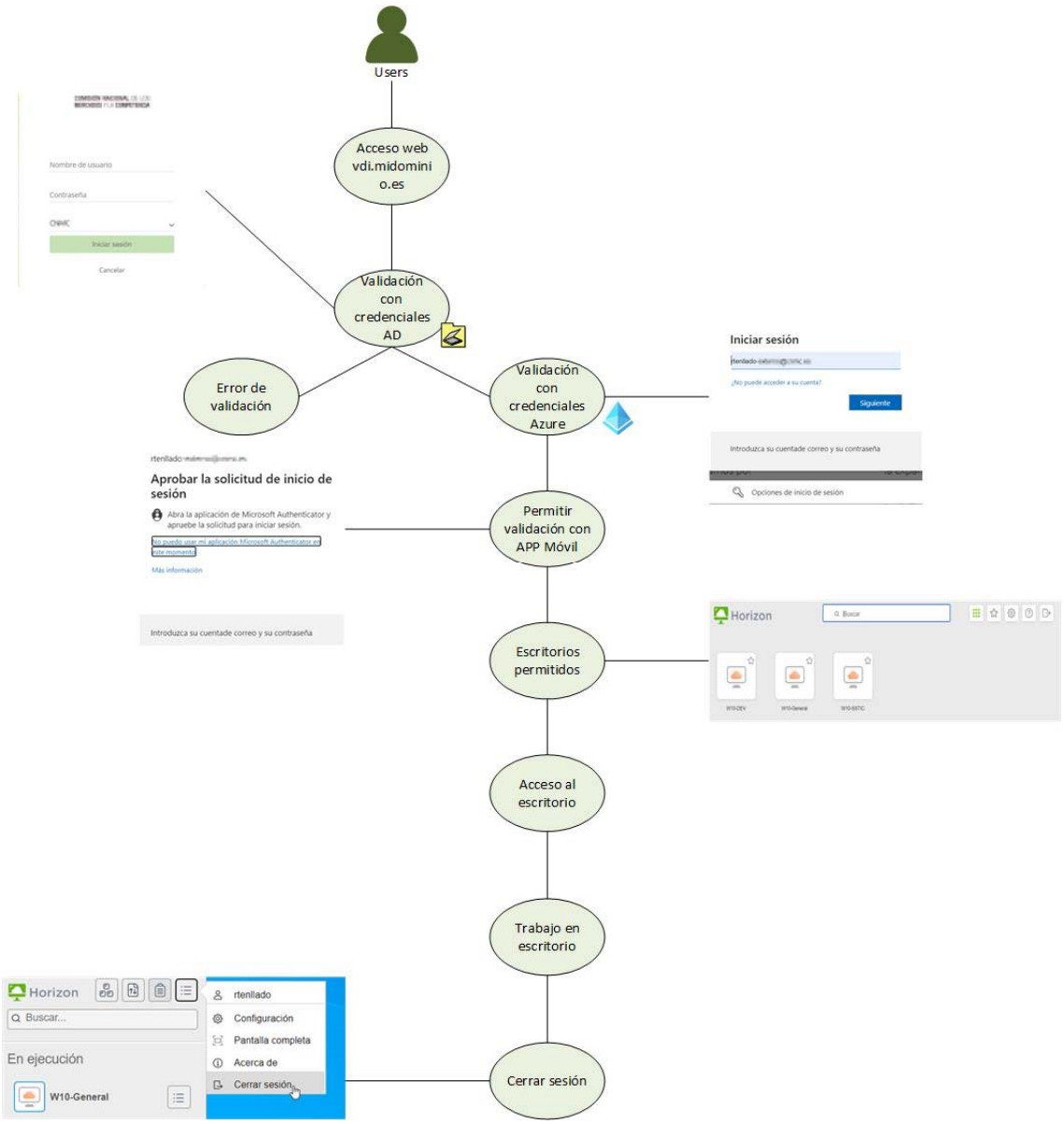
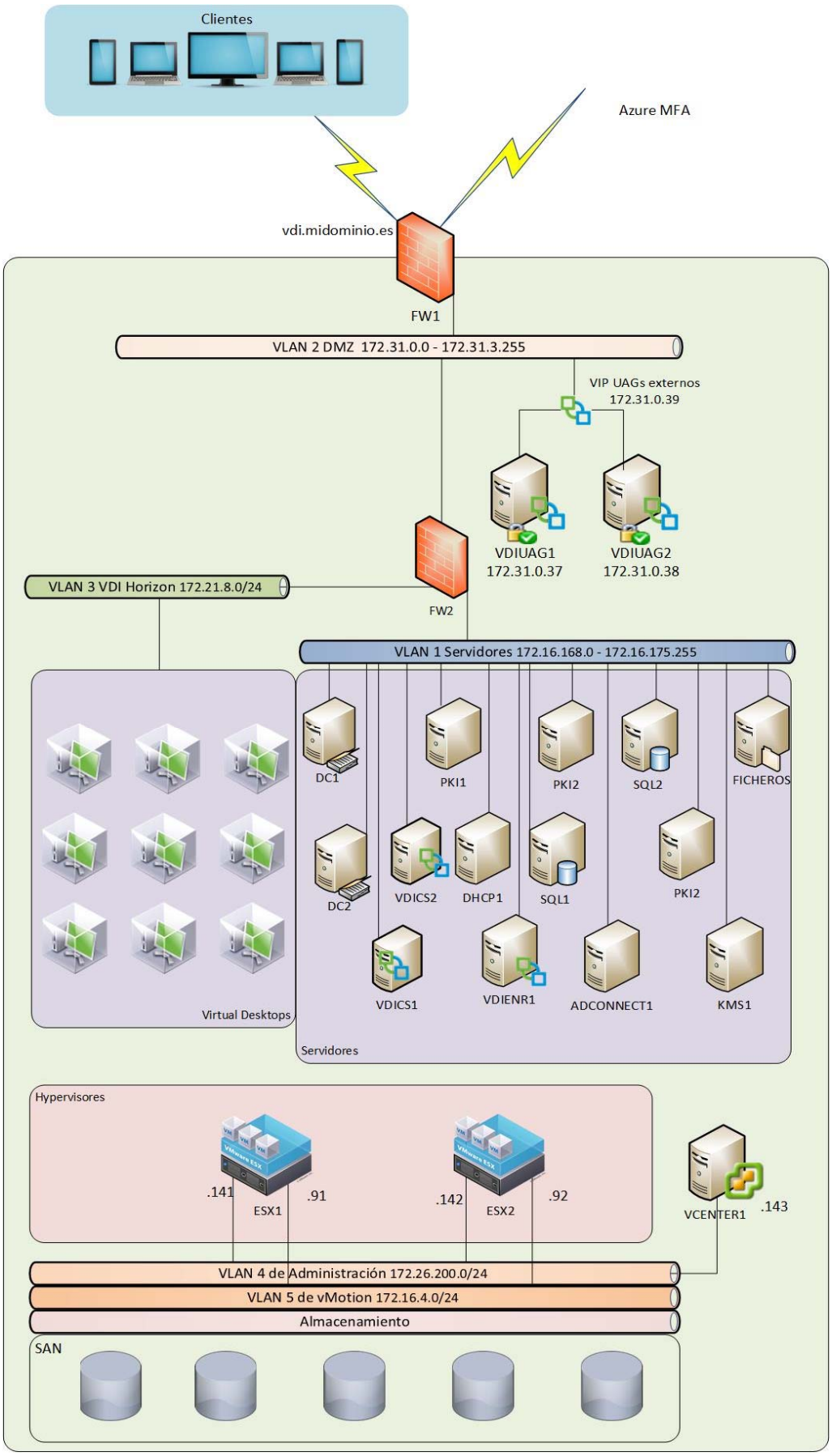


Ilustración 8. Propuesta caso de uso

En la imagen anterior se muestra un diagrama que resume y explica la propuesta en cuanto a funcionalidad, seguridad y casos de uso.

5.3 Arquitectura de red objetivo

Con el fin de facilitar la comprensión de esta propuesta, en cuanto a los distintos elementos que se van a ir añadiendo, se incluye una imagen con la arquitectura final que se pretende lograr:


Clientes
Azure MFA
vdi.midominio.es
FW1
VLAN 2 DMZ 172.31.0.0 - 172.31.3.255
VIP UAGs externos
172.31.0.39
VDIUAG1
172.31.0.37
VDIUAG2
172.31.0.38
VLAN 3 VDI Horizon 172.21.8.0/24
FW2
VLAN 1 Servidores 172.16.168.0 - 172.16.175.255
DC1
PKI1
PKI2
SQL2
FICHEROS
DC2
VDICS2
DHCP1
SQL1
PKI2
VDICS1
VDIENR1
ADCONNECT1
KMS1
Virtual Desktops
Servidores
Hypervisores
.141
ESX1
.91
.142
ESX2
.92
VCENTER1
.143
VLAN 4 de Administración 172.26.200.0/24
VLAN 5 de vMotion 172.16.4.0/24
Almacenamiento
SAN

6 Requisitos previos

En el caso de uso descrito, la empresa dispone de una infraestructura de red existente. A continuación, se listan las partes de esta infraestructura que son requisito para poder realizar las instalaciones y configuraciones descritas en este documento.

6.1 Servicios

A continuación, se detallan los servicios y servidores necesarios, previos a la instalación de vmWare Horizon:

- Dominio de Windows (Active directory): “midominio.local”
- Dominio enrutable en Internet: “midominio.es”
- Cabina de almacenamiento. En ella se guardarán los discos de las máquinas virtuales y se compartirán los Shares de red explicados más adelante dentro de este documento
- Tenant de Microsoft 365 con Azure AD. Es necesario tener una suscripción de azure AD, donde se realizarán las validaciones de usuario
- ADConnect. Los usuarios del dominio OnPremise deben ser sincronizados con Azure AD, por lo que esta herramienta debe estar instalada previamente
- Servidor KMS. Este servidor se encargará de asignar las licencias de Windows sobre las máquinas virtuales a las que se conectarán los usuarios. El servidor KMS es un requisito de Horizon 8
- Infraestructura VMware. Una infraestructura básica de VMware vSphere es un requisito de Horizon. Las configuraciones adicionales necesarias están descritas en este documento.
- Clúster SQL. Para proveer de alta disponibilidad en la base de datos, se requiere un clúster SQL activo/pasivo

6.2 Arquitectura de red inicial

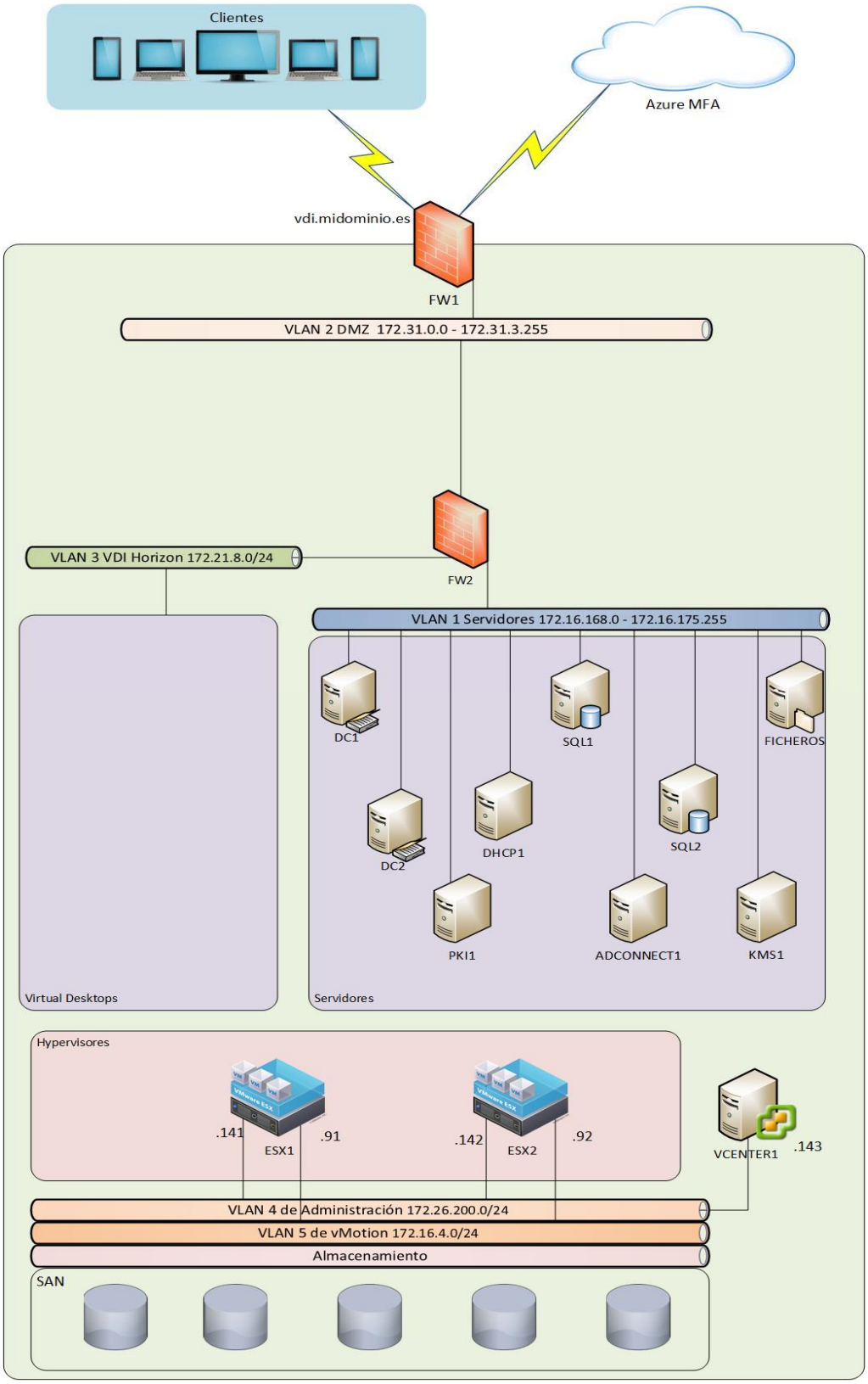


Ilustración 9. Arquitectura inicial

Los distintos elementos representados en la imagen son explicados a continuación:

- **Clientes**: Representa los accesos desde fuera de la organización al servicio VDI. Estos accesos pueden ser desde PCs, portátiles, o dispositivos móviles.
- **URL de Acceso**: Para poder realizar la conexión, los clientes han de introducir en su navegador la URL https://vdi.midominio.es.
- **Azure MFA**: Para securizar el acceso al servicio VDI con un doble factor de autenticación, se utiliza Azure MFA (Multi Factor Authentication), integrado con Horizon usando el protocolo SAML.
- **FW1**: Firewall perimetral, que controla los accesos desde Internet a la red DMZ (Zona desmilitarizada).
- **VLAN2**: Esta VLAN contiene la red de DMZ.
- **FW2**: Este Firewall controla los accesos desde la red DMZ a la red Interna.
- **VLAN1**: Esta VLAN contiene la red donde se ubican los servidores.
- **DC1**: Servidor con el rol de DC (Domain Controller).
- **DC2**: Servidor ocn el rol de DC (Domain Controller)
- **SQL1**: Nodo 1 clúster base de datos SQL.
- **SQL2**: Nodo 2 clúster base de datos SQL
- **FICHEROS**: Servidor NAS donde se guardan los datos de los perfiles móviles de usuario y carpetas redirigidas. Este servidor lo ofrece la cabina de almacenamiento.
- **PKI1**: Entidad certificadora (CA) de Windows, integrada con el Dominio y configurada como Entidad Certificadora Raíz.
- **KMS1**: Servidor KMS, encargado de asignar licencias de Windows a los escritorios virtuales.
- **VLAN3**: VLAN donde se ubican los escritorios virtuales.
- **Virtual Desktops**: Red para máquinas virtuales de Horizon.
- **Hypervisores**: Red de servidores con el software de virtualización VMWARE.
- **VCENTER1**: Servidor de gestión y administración del entorno virtualizado VMWARE.
- **VLAN4**: VLAN dedicada a la gestión del entorno virtualizado VMWARE.

- **VLAN5**: VLAN para el tráfico de red generado por vMOTION (movimiento de máquinas virtuales entre servidores ESXi, sin pérdida de conexión).
- **Almacenamiento**: Red de Fiber Channel.
- **SAN**: Cabina de almacenamiento

6.3 Entorno laboratorio utilizado

Para poder realizar las configuraciones detalladas en este documento, así como las pruebas, capturas de pantalla, etc. Se ha creado un entorno de laboratorio dentro la infraestructura de red de la empresa donde trabajo. Esto ha sido necesario para poder disponer de un entorno lo más parecido posible, así como de las licencias necesarias.

Uno de los elementos necesarios para el laboratorio son las máquinas físicas sobre las que se ha montado toda la infraestructura. En cuanto al hardware de estas máquinas, el entorno de laboratorio está compuesto por los siguientes elementos:

- Chasis HP BladeSystem c7000 G3
- 2 Servidores HP ProLiant BL460c Gen9

Otro de los elementos necesarios es el almacenamiento en el que se han guardado los datos, como el de los archivos que contienen las máquinas virtuales. Para ello, se ha usado la siguiente cabina de discos de tipo SAN:

- DELL EMC Unity 650F

En cuanto a los sistemas operativos de las máquinas utilizadas, se ha diferenciado si la función es de servidor o de cliente:

- Servidores: Windows 2019 Standard en inglés
- Clientes: Windows 10 versión 21H2

También ha sido necesario disponer de una base de datos, para lo que se ha utilizado el clúster activo/pasivo de 2 nodos, ya existente. El SGDB utilizado es el siguiente:

- Microsoft SQL 2019 Standard en inglés

Para la virtualización de máquinas se ha instalado una infraestructura nueva sobre los 2 servidores descritos anteriormente. La versión del hypervisor utilizada es la siguiente:

- VMware ESXi 7.0 Update 2
- VMware vsphere 7.0

Otro elemento utilizado han sido los Firewalls, configurados en clúster, sobre los que ha habido que crear las reglas necesarias para permitir solamente el tráfico deseado. Los Firewalls utilizados son los siguientes:

- Firewall FortiNet 200F

Además de lo anterior, para posibilitar el doble factor de autenticación, integrado con Horizon y usando MFA de Azure, se han usado licencias de tipo “Microsoft Office 365 P3” y el tenant de la empresa.

En cuanto al software específico de VDI se ha utilizado el siguiente software:

- VMware Horizon 8 2111, con los siguientes roles
    - Unified Access Gateway
    - Connection Server
    - Enrollment Server

7 Arquitectura Horizon

La arquitectura de VMware Horizon se puede analizar desde dos enfoques distintos pero complementarios; el conceptual y el lógico. Desde el punto de vista del primero de ellos, se recogen las distintas capas existentes, así como qué elementos corresponden a cada capa. Este enfoque es especialmente útil para comprender con qué otras capas interactúa cada una de ellas y sus dependencias.

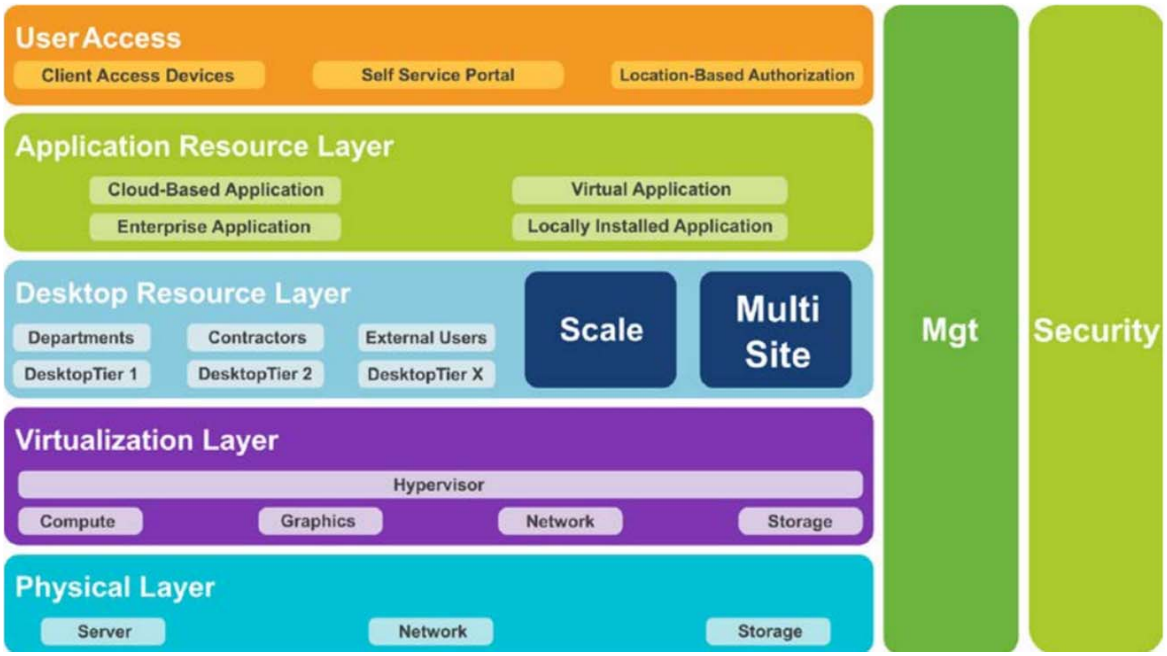


Ilustración 10. Arquitectura conceptual [8]

Fuente: Curso "Horizon 8: Deploy and Manage" realizado el 2022 por VMWARE

La imagen anterior muestra de forma muy clara las distintas capas de la arquitectura conceptual de Horizon. Estas capas son:

- Security. La imagen muestra que esta capa de seguridad engloba todos los elementos que forman parte de una sesión con VDI. Desde los elementos físicos hasta el inicio de sesión de un usuario.
- Management. Al igual que la capa anterior, todos los elementos de una sesión son administrables desde Horizon.

- Physical Layer. En esta capa se encuentra los servidores físicos que albergan las máquinas virtuales, es decir el hardware donde se instalarán los ESX. También se encuentran las conexiones de red y el almacenamiento necesario para guardar máquinas virtuales y otros archivos como los perfiles de usuario.
- Virtualization Layer. En esta capa se encuentra el hipervisor, el elemento que permite abstraer la capa física de los servidores en los que está instalado para poder crear las máquinas virtuales. Este hipervisor también gestiona el procesador, tarjeta gráfica, red y almacenamiento de las máquinas virtuales, por lo que estas también se encuentran en esta capa.
- Desktop Resource Layer. En esta capa se encuentran los distintos perfiles posibles de máquinas que existen en un entorno horizon. En cada uno de estos perfiles hay una configuración específica, adaptada a las necesidades de los usuarios que van a hacer uso de ella. Sobre cada perfil existirá una granja de máquinas para dar respuesta a la demanda existente.
- Application Resource Layer. En esta capa se encuentran las aplicaciones a las que podrán acceder los usuarios a través del entorno VDI. Estas aplicaciones pueden estar ser Cloud, aplicaciones empresariales, publicadas virtualmente o instaladas localmente en las máquinas.
- User Access. En esta capa se encuentran las distintas formas en las que se ofrece el acceso de Horizon, como un portal web o el cliente pesado.

El segundo punto de vista es la arquitectura lógica, donde se recoge la forma que tiene Horizon de realizar las comunicaciones y como se interrelacionan los diferentes dispositivos y roles dentro del entorno.

En un entorno Horizon, existen los siguientes 2 roles básicos:

- Connection Server
- Unified Access Gateway (UAG)

Sin embargo, en este proyecto se desea montar una arquitectura capaz de proveer un doble factor de autenticación, por lo que se hará uso de un tercer rol: “Enrollment Server”.

La imagen a continuación nos permite hacernos una idea general de cómo es una infraestructura Horizon, dónde se ubica cada elemento, con quién se comunica cada rol y cómo se realizan estas comunicaciones.

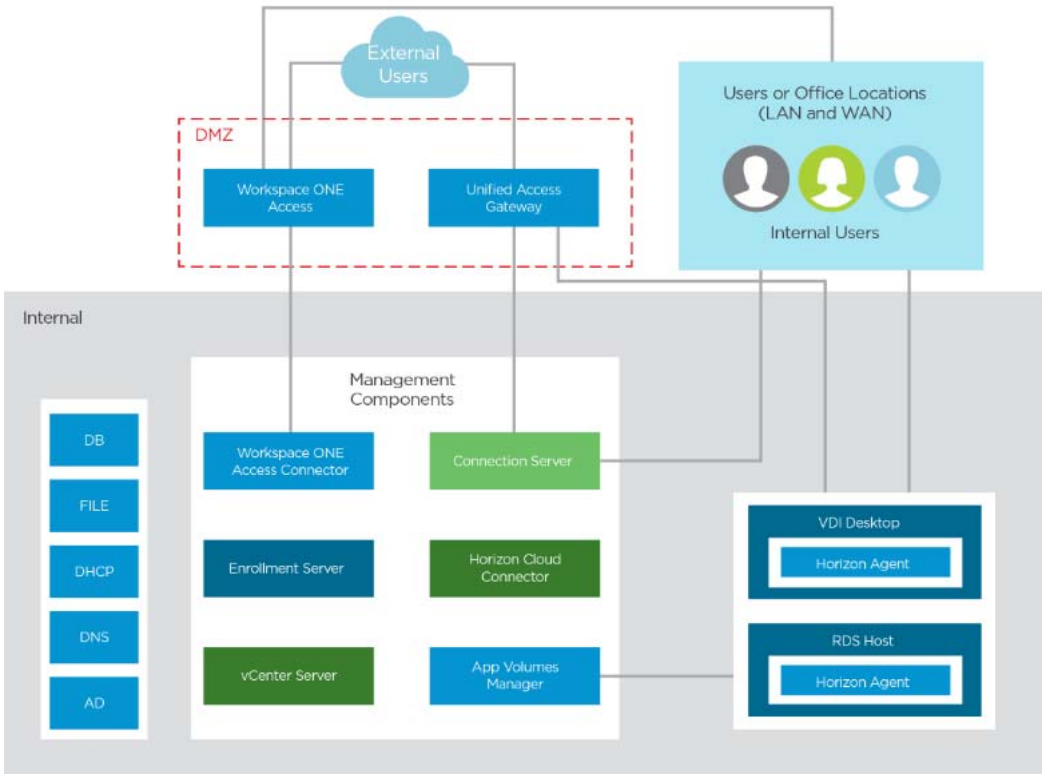


Ilustración 11. Elementos Horizon [9]

Como se puede observar, un usuario que utiliza un PC, teléfono, Tablet o portátil se puede conectar a una máquina virtual a través de Internet o desde dentro de la red corporativa. En el primer caso, la conexión pasará a los servidores UAG, ubicados en la DMZ, que realizarán la validación del usuario con los Connection Server y que le permitirá realizar la conexión con el Agente de Horizon, instalado en la máquina virtual a la que se conectará.

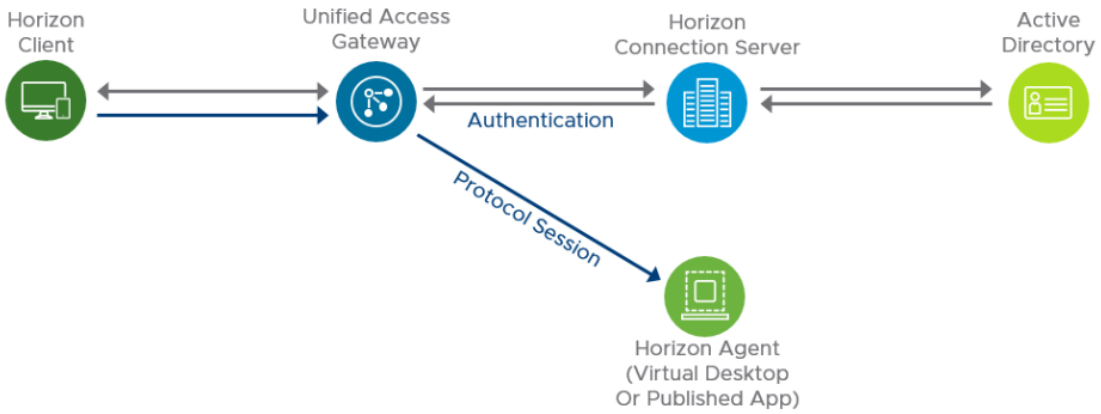


Ilustración 12. Conexión desde Internet [10]

Los usuarios que se conecten desde la red interna se validarán directamente contra los Connection Servers, que serán quienes, a su vez, validarán las credenciales con el Directorio Activo.

A partir de aquí, tanto los usuarios que accedieron desde Internet como los que accedieron a través de la red interna, comparten los siguientes pasos:

- Los Connection Server se encargan de generar y mantener la conexión entre el cliente y el agente, así como de administrarla.
- Los Connection Server también tienen un servicio llamado DEM (Dynamic Environment Manager) que se encarga de gestionar los perfiles de los usuarios, de forma que cuando inicien sesión en la máquina virtual, mantendrán todos los elementos que estén dentro de este perfil, independientemente de la máquina a la que accedan.

7.1 Connection Server

Connection Server es un rol de VMware que se instala sobre un servidor Windows y se encarga de validar a los usuarios a través de Windows Active Directory, así como redirigir las peticiones a las máquinas virtuales. También provee de las siguientes capacidades de administración:

- Autenticación de usuarios

- Concesión de permisos sobre los escritorios virtuales y pools de escritorios
- Incluye la consola de administración del entorno
- Administración de sesiones en escritorios y aplicaciones
- Establecer las conexiones seguras entre usuarios y escritorios y aplicaciones
- Habilitar single sign-on
- Opciones y aplicación de políticas

El servidor con este rol se ubica físicamente en la red interna de la empresa, protegido por un Firewall que separa esta red de la DMZ, y que permitirá las conexiones con otro servidor ubicado en esta DMZ, con el rol de Unified Access Gateway (UAG).

Otras características del Connection Server son:

- Un solo servidor Connection Server soporta hasta un máximo de 4000 sesiones, aunque como buena práctica, es recomendable que no supere las 2000.
- Soporta los siguientes SSOO para escritorios
    - Windows 8, Windows 10
    - Windows Server 2012 R2, Windows 2016, Windows 2019 Server
    - Ubuntu, RHEL, CentOS, SLED, SLES y NeoKylin
- Soporta los siguientes métodos de autenticación
    - True SSO
    - RSA SecurID
    - RADIUS
    - SmartCard
- Requisitos mínimos del servidor Connection Server
    - Procesador:
        - Pentium IV 2.0 GHz
        - Número: 4
        - ESXi: Soportados en la lista de compatibilidad para vSphere 6.5 y superiores
    - Memoria
        - Mínimo: 4GB
        - Para entornos con 50 o más escritorios: 10 GB

- Sistema Operativo
  - Windows 2012 R2 Standard
  - Windows 2016 Standard
  - Windows 2019 Standard
- Red
  - IP estática
  - Resolución DNS normal e inversa

En cuanto a alta disponibilidad de este rol, se pueden instalar servidores adicionales que replicarán automáticamente la configuración existente. Para ello, el primer servidor se instalará como "standard connection server" y el segundo y adicionales como "replica server".

Una vez instalado el segundo servidor (o adicionales) y se hayan replicado, todos quedarán configurados como servidores connection server al mismo nivel, sin distinción de ningún tipo entre el standard y los replica. Esta configuración con varios connection server además de alta disponibilidad, sirve como configuración de escalabilidad, para darle más capacidad al entorno.

En cuanto al balanceo de carga de estos servidores, no hay un método nativo de lograrlo. Sin embargo, sí que existe la opción de agregar un balanceador de carga externo, bien sea por software o por hardware, que se encargará de repartir el tráfico entre todos ellos. Si bien esta opción es muy recomendable, es cierto que tiene un alto coste económico.

7.2 Unified Access Gateway (UAG)

UAG es un rol de VMware que nos permite disponer de un *gateway* seguro, y que funciona como puerta de entrada a los usuarios para conectar con los escritorios y aplicaciones publicadas. Este servidor permite solamente las conexiones de usuarios autenticados.

El servidor UAG se despliega como un appliance, basado en Linux, que se puede descargar desde la página de VMware, y se ubica físicamente en la DMZ de nuestra red. Es decir, está protegido tanto por delante como por detrás por Firewalls que permitirán solamente ciertas conexiones. Para permitir las conexiones validadas hacia la red interna, ha de comunicarse con el servidor Connection Server, a través del protocolo HTTPS.

En esta arquitectura, UAG funciona como un proxy inverso, con el que se logra una capa adicional de seguridad. Los servidores UAG permiten ocultar los escritorios virtuales y aplicaciones publicados por Horizon de los usuarios que acceden desde una red no segura como Internet.

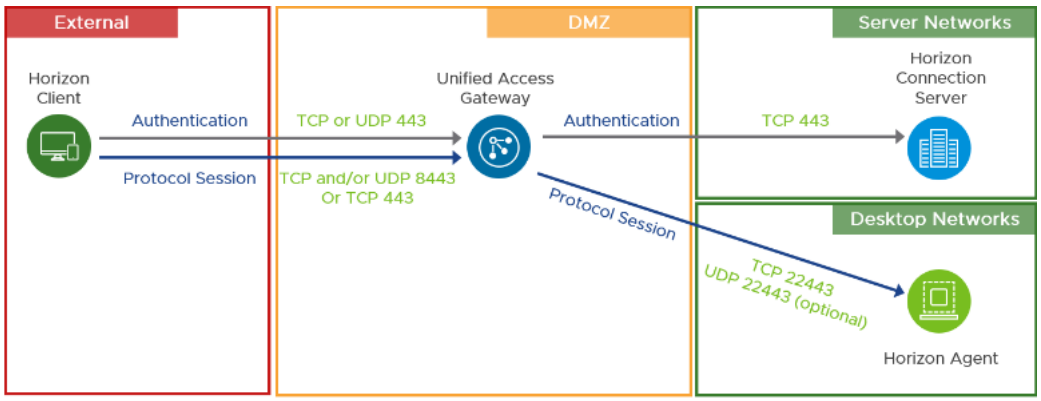


Ilustración 13. UAG en Arquitectura Horizon[11]

Además de las funcionalidades anteriores, UAG permite algunos beneficios adicionales:

- Un servidor UAG se puede configurar para que apunte a un Connection Server o a un balanceador de carga que reparta las conexiones hacia un grupo de Connection Servers.
- A diferencia de otras soluciones de servidores seguros, no se realiza ningún emparejamiento entre UAG y Connection Server por medio de Passwords, lo que permite que sean independientes entre ellos.
- Permite autenticación multifactor (MFA)
- Admite la creación de clusters de UAG, lo que permite tener alta disponibilidad.

Otras características de UAG:

- 3 Niveles de licenciamiento: Standard, Advanced y Enterprise
- Provee de información de las sesiones activas desde su consola de administración
- Permite la monitorización de estado y creación de estadísticas
- Soporta los siguientes métodos de autenticación

- Credenciales de Active Directory
- RSA SecurID
- RADIUS
- SmartCards
- Security Assertion Markup LangUnified Access Gateway (SAML)

Todos estos métodos de autenticación, excepto Smart Card, son redirigidos al servidor Connection Server usando *passthrough*.

En cuanto a alta disponibilidad, se puede formar un clúster activo/pasivo de forma nativa entre todos los servidores UAG, de modo que, si uno de ellos dejase de estar disponible, no se le enviarían conexiones.

Respecto a balanceo de carga, al igual que con los servidores Connection Server, tampoco existe una solución nativa. Aunque de igual modo que los CS, se podría añadir un balanceador de carga externo.

7.3 Horizon Agent

Horizon agent es un software instalado en las máquinas virtuales disponibles para los usuarios. Este agente es el encargado de realizar la comunicación con el cliente, como se muestra en la siguiente imagen.

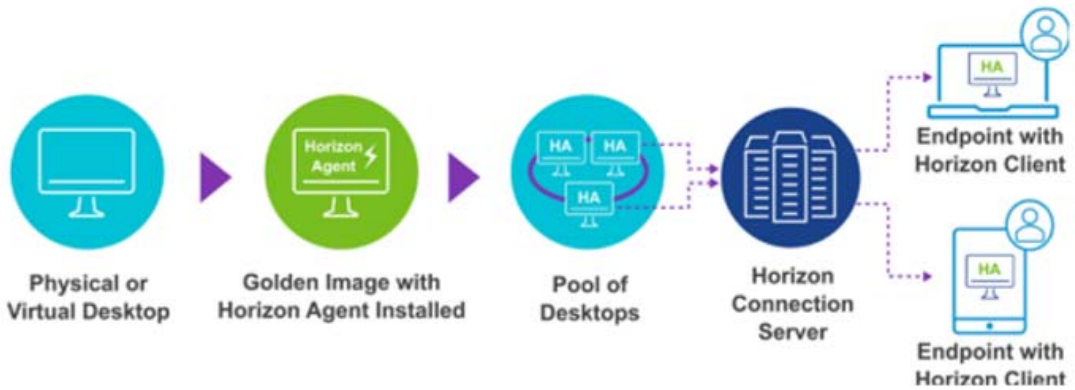


Ilustración 14. Horizon Agent [12]

Fuente: Curso “Horizon 8: Deploy and Manage” realizado el 2022 por VMWARE

Además, este agente permite las siguientes características:

- Monitorización de la conexión
- Impresión virtual
- Administración de usuarios
- Acceso a dispositivos USB locales

Además, el agente de horizon permite la configuración SSO (single sign-on) de forma que no pide una segunda validación al conectarse a las máquinas virtuales.

7.4 Enrollment Server

Los servidores con este rol, permiten generar certificados solicitados por este servidor en nombre de los usuarios cliente de Horizon. Este hecho permite usar certificados generados por una entidad certificadora en la que confían todas las máquinas del dominio, como si fuesen token de sesión. De esta forma, se evita que los usuarios tengan que realizar dobles validaciones, como la que sería necesaria para acceder a la plataforma Horizon VDI y también para validar el usuario dentro del Dominio de Windows.

Estos servidores se ubican físicamente en la red interna de la compañía, ya que deben estar protegidos y, a la vez, tener conexión con la CA encargada de generar los certificados.

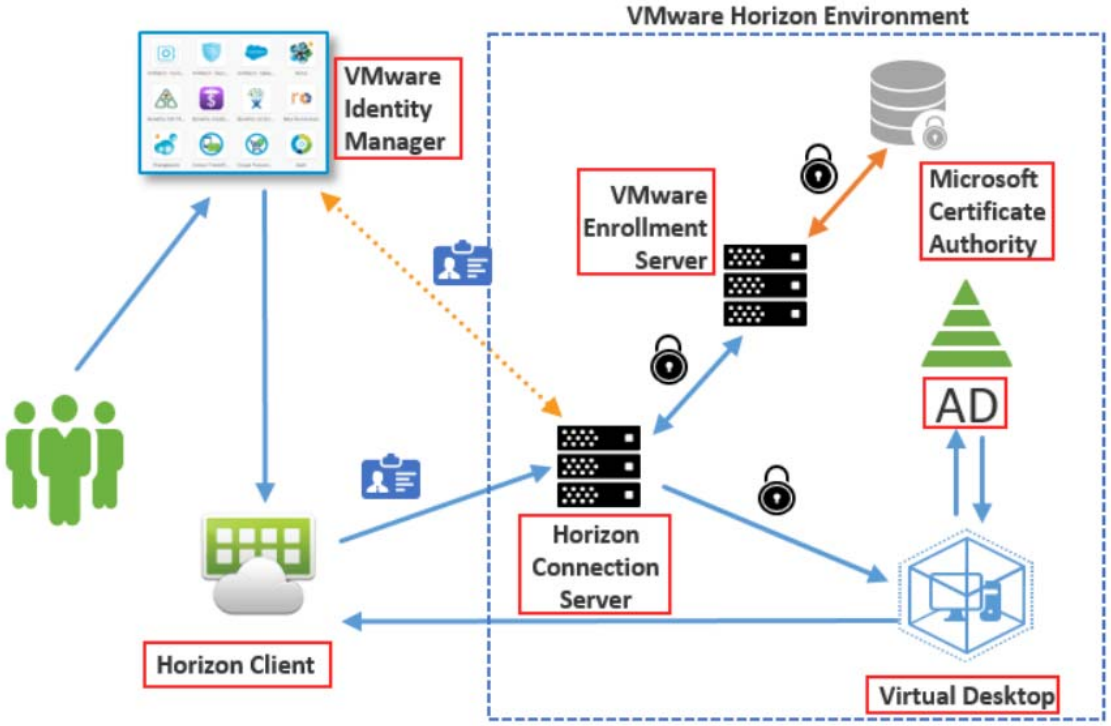


Ilustración 15. Enrollment server [13]

En la imagen anterior se puede observar tanto la ubicación como la interacción que tiene este rol, dentro de una infraestructura Horizon.

Como se mencionaba anteriormente, el propósito de este rol es dotar de SSO a los usuarios y reducir el número de validaciones. Esto lo convierte en un "servicio" importante pero no necesario, ya que los usuarios podrían seguir accediendo a sus escritorios incluso si no hubiese ningún servidor con este rol disponible. Sin embargo, se recomienda dotar de alta disponibilidad a todo lo que sea posible, y en este caso, se puede añadir tolerancia a fallos a este rol.

Para lograr el propósito mencionado en el párrafo anterior, bastaría con disponer de 2 servidores con el rol de "Enrollment server". Sin embargo, estos servidores funcionan como activo/pasivo, siendo uno de ellos el primario y el que realiza las peticiones. Esto tiene como consecuencia que no dispondríamos de balanceo de carga, sino que solamente nos daría alta disponibilidad. Sí es configurable cual es el servidor primario y cual está disponible para *failover*.

8 Configuraciones previas

Siguiendo las buenas prácticas en cuanto a orden, facilidad de administración, y correcto funcionamiento del servicio, se realizan una serie de configuraciones previas a la instalación del producto.

8.1 Directorio Activo y DNS

La posterior instalación de VMware Horizon tendrá un impacto en el Directorio Activo de la empresa, ya que deberá contener los distintos objetos que se irán creando, tanto de máquinas (servidores y clientes), como de los distintos usuarios y grupos que se utilizarán para conceder los permisos de acceso necesario y con los que se ejecutarán los servicios necesarios dentro de Windows.

Con el objetivo de mantener una estructura de DA clara, limpia y que facilite la administración y la escalabilidad, se realizan las siguientes recomendaciones:

1. Crear una estructura de OUs en el DA donde se almacenarán los objetos necesarios para la infraestructura VDI. Como primera medida, sería recomendable crear una OU específica para todos los objetos relacionados con Horizon. Dentro de esta OU, deberían existir las siguientes distinciones:
    - Una OU donde se ubicarán los usuarios y grupos necesarios para la administración de la plataforma, así como para asignar permisos de acceso.
    - Una OU que contendrá la estructura de escritorios, separada por plantillas “Golden”
    - Una OU donde se ubicarán las cuentas de máquina de los servidores Horizon.
2. Siguiendo las buenas prácticas de Microsoft, los permisos se han de conceder a grupos en vez de a usuarios individuales para simplificar las labores de administración. Por este motivo, se creará un grupo por cada uno de los siguientes tipos de permisos:

- Permisos de administración global sobre el entorno Horizon
- Usuarios con permisos de acceso a las máquinas virtuales. Aunque en este proyecto solamente habrá una imagen Golden desde la que se desplegarán las máquinas sobre las que accederán los clientes (VDAs), se ha de crear un grupo diferente por cada una de las imágenes Golden, para diferenciar qué usuarios tendrán acceso a las máquinas creadas desde las distintas imágenes.

3. Las instalaciones no se deben realizar utilizando la cuenta de un usuario real, ya que podría generar futuros errores por motivos como que el usuario deje la compañía, caduque la password, etc. Por este motivo, se recomienda crear una cuenta de usuario específica, con la que se realizarán las distintas instalaciones y configuraciones de Horizon. Además de crear este usuario, sería recomendable usar una nomenclatura de nombres estandarizada, que permitiese reconocer rápidamente la utilidad de este usuario. Este usuario debe ser miembro del grupo creado anteriormente para la administración global del entorno.
4. Se debe crear una cuenta de usuario con la que se crearán y eliminarán las máquinas virtuales. Por defecto, un usuario de dominio no puede añadir más de 10 cuentas de máquina a este dominio, por lo que se necesita un usuario específico para esta tarea, y que se le elimine esta restricción mediante GPO. Además, este usuario ha de tener los siguientes permisos especiales:
    - Listar contenido
    - Leer todas las propiedades
    - Escribir todas las propiedades
    - Leer permisos
    - Restablecer contraseña
    - Crear objeto Equipo
    - Eliminar objeto Equipo
5. Crear registro tipo “A” en DNS público. Para poder acceder a las máquinas virtuales desde cualquier lugar, es necesario que el servicio esté disponible desde Internet. Para ello, necesitamos publicar en un servidor de nombres (DNS) de Internet, el nombre por el que queremos que sea accesible nuestro servicio. En este proyecto, en el que se dispondrá de HA en los servidores visibles desde

Internet (UAG), será necesario, además, otro registro A por cada nodo miembro del clúster.

8.2 Directivas de grupo (GPOs)

Con el fin de optimizar el rendimiento, securizar el entorno y permitir el correcto funcionamiento de algunas aplicaciones, Horizon se puede apoyar en GPOs para facilitar la administración y lograr un rendimiento óptimo. Para ello, es necesario crear y aplicar las siguientes directivas:

1. Crear una GPO que impida el cambio de políticas por parte de los usuarios. Por defecto, las políticas locales se aplican antes que las de dominio, pero se puede evitar este comportamiento por el que se aplican políticas locales. De esta forma, los usuarios que accedan a los escritorios virtuales no podrán hacer cambios con el comando "gpedit.msc", que modifiquen las configuraciones aplicadas por políticas del Dominio.
2. Crear una GPO por la cual, durante el inicio de sesión de los usuarios, se espere a tener acceso completo a la red. Por defecto, la aplicación de políticas no espera a que la red esté completamente disponible. Esto generalmente no es un problema, pero sí lo puede ser en escenarios con perfiles móviles, como ocurre en el caso de un VDI, en el que queremos aplicar el perfil de usuario independientemente de la máquina a la que se conecte. Si no se habilita, además del error comentado, puede ocurrir que, aleatoriamente, al usuario no se le conecte la "Home Folder", si la tiene configurada. Esta unidad, se configura dentro de las propiedades del objeto de usuario de DA.
3. Crear una GPO que permita aplicar las configuraciones de directiva, tanto de máquina como la de usuario. La aplicación de directivas se realiza según el objeto que hay dentro de la OU donde se ha aplicado la respectiva política. Si una GPO con configuraciones de usuario, contiene objetos de máquina no le aplicará, y lo mismo, al contrario. Es por ello, que debemos configurar que a un usuario que inicie sesión en una máquina de VDI, le apliquen las configuraciones respectivas

de usuario. Por ejemplo, la opción de deshabilitar el apagado de máquinas es una configuración de directiva que se aplica a usuarios, pero esto no queremos que se aplique a todas las máquinas en las que inicien sesión los usuarios, sino que solamente lo queremos cuando inicie sesión en una máquina de VDI. Esta configuración se realiza modificando la directiva "Configure user Group Policy Loopback processing mode" a "Merge".

4. Crear una directiva que impida el apagado, reinicio o hibernación de la máquina. Un sistema VDI se basa en que los usuarios se puedan conectar a máquinas de forma aleatoria, sin tener un puesto fijo. Por este motivo, es importante que los usuarios no sean capaces de apagar, reiniciar o hibernar máquinas que puedan impedir que otros usuarios se conecten.

5. Crear una GPO que oculte las unidades locales e impida su acceso por parte de los usuarios. Las máquinas son compartidas, por lo que los usuarios no deben poder hacer modificaciones en la unidad "C:", fuera de las carpetas que corresponden a su perfil. Por este motivo, con esta GPO se previene que los usuarios puedan hacer modificaciones indeseadas.

8.3 DHCP

Las máquinas de virtuales de VDI deberían estar una VLAN específica, diferenciada del resto de la red. Además, no pueden tener una IP fija, ya que realmente son instantáneas de una imagen y se crean y destruyen bajo demanda.

Por los motivos explicados en el párrafo anterior, se hace necesaria la asignación de direcciones IP y el resto de opciones desde un servidor DHCP (Dynamic Host Configuration Protocol). Para ello, necesitamos crear un ámbito nuevo en nuestro servidor DHCP y configurar, dentro de este ámbito, un pool con direcciones válidas dentro de esa VLAN. Además, el pool debe contener el número suficiente de direcciones

IP para que todas las máquinas puedan estar levantadas al mismo tiempo. Si no fuese así, el DHCP no podría asignar más IPs y las máquinas no tendrían conexión a la red.

Además del rango de IPs que podrá asignar el servidor, también habrá que configurar una serie de opciones que permita a los clientes ser plenamente funcionales, como encaminar tráfico de red y resolver nombres. Las opciones que se deberán configurar son:

1. Máscara de red
2. Duración de la concesión para clientes DHCP: 4 días.
    - La opción por defecto es 8 días, sin embargo, al existir una gran cantidad de creación y eliminación de máquinas en este tipo de entornos, es aconsejable reducirlo para mantener actualizada la base de datos de DHCP y que no se llene el ámbito
3. Opciones de ámbito:
    - Router
    - DNS Servers
    - Domain name

8.4 Configuraciones VMWARE vSphere

En el software de virtualización (vSphere) también es necesario que se realicen algunas configuraciones específicas para poder instalar VMware Horizon. Además, al igual que se ha venido haciendo hasta ahora, se debe mantener el orden y la limpieza del entorno, para facilitar la administración y la facilidad de aprendizaje para posibles nuevos administradores.

En este proyecto se pretende usar la “Instant Clone”, que permite la creación de nuevas máquinas para los usuarios a partir de un *snapshot*. Una de las ventajas que proporciona esta tecnología es que las máquinas se crean de forma muy rápida, reduciendo el tiempo que tienen que esperar los usuarios para tener disponible su máquina, y evitando así una posible percepción negativa por parte de estos. Para ello, se necesitan unos

permisos específicos que el propio fabricante de ambos softwares (VMware) nos facilita en una nota técnica (presente en la bibliografía).

Siguiendo el nivel de calidad y metodología descrito en el primer párrafo, se ha de crear un rol en vCenter, específico para esta tarea, que contenta los siguientes permisos:

Grupo de Privilegios en vCenter Server	**Privilegios concedidos**
Folder	Create folder Delete folder
Datastore	Allocate space Browse datastore
Host	In Inventory • Modify Cluster In Configuration • Advanced settings
Virtual machine	In Configuration (all) • Add or remove device • Advanced • Modify device settings • Change CPU count • Change memory • Change settings • Change resource • Configure Host USB device • Configure raw device • Configure managedby

	• Display connection settings • Extend virtual disk • Query fault tolerance compatibility • Query unowned files • Reload from path • Remove disk • Rename • Reset guest information • Set annotation • Toggle disk change tracking • Toggle fork parent • Upgrade virtual machine compatibility In Interaction: • Power Off • Power On • Reset • Suspend • Perform wipe or shrink operations • Device connection In Inventory (all) • Move • Register • Unregister In Snapshot management (all)

	• Create snapshot • Remove snapshot • Rename snapshot • Revert snapshot In Provisioning: • Customize • Deploy template • Read customization specifications • Clone template • Clone Virtual Machine • Allow disk access
Resource	Assign virtual machine to resource pool HotMigrate
Global	Enable methods Disable methods Manage custom attributes Set custom attribute Act as vCenter Server
Network	Assign
Profile Driven Storage	(all--If you are using vSAN datastores or Virtual Volumes)
Storage views	Not required
Cryptographic operations	The following privileges are required if you use instant clones VMs with a Trusted Platform Module (vTPM) device. • Clone

	• Decrypt • Direct Access • Encrypt • Manage KMS • Migrate • Register Host

8.5 Base de datos

VMware Horizon necesita una base de datos para poder almacenar los eventos. De esta forma, aunque complica algo más la arquitectura de la solución, también facilita el tratamiento de los datos, si los comparamos con los que se almacenan en un archivo.

Esta base de datos se ha de crear después de instalar los servidores con el rol de CS y puede ser instalada en un servidor independiente o en un clúster para disponer de alta disponibilidad. Aunque la opción de disponer HA es siempre la más recomendable y la que se ha elegido para este proyecto, se muestran a continuación todas las opciones soportadas:

- Microsoft SQL Server
    - Se puede instalar en versión gratuita de SQL (SQL Express), aunque tiene las siguientes limitaciones:
        - Tamaño máximo por BD 10 GB
        - No tiene agente SQL, por lo que no se podrán automatizar algunas tareas
        - Memoria máxima utilizada por el motor 1 GB
        - Búfer caché máximo 1 MB
- Oracle
- PostgreSQL

En este proyecto, como se comenta en el párrafo anterior, se usará una BD sobre SQL 2019 en 2 nodos físicos, configurados como clúster Activo/Pasivo. Esta configuración nos permite, por un lado, que la base de datos continúe disponible, aunque uno de los nodos físicos tuviese un problema. Por el otro lado, nos permitiría realizar cualquier opción de mantenimiento, como actualizarlo, sin que se viese comprometida la disponibilidad de la base de datos.

8.6 Comunicaciones y seguridad

Al tener la red segmentada en VLANs y existir una DMZ, es necesario realizar algunas configuraciones en nuestros Firewalls (internos y externos). En el caso de los externos, necesitaremos redirigir el tráfico proveniente de Internet a los servidores frontales (UAG). En el caso de los firewalls internos, deberemos permitir un determinado tráfico y puerto.

8.6.1 Configuración Firewall externo

En el Firewall situado entre Internet y nuestra DMZ, se deben configurar las siguientes reglas de NAT (Network Address Translation):

Configuración NAT			
Origen	Destino	Protocolo	Puerto
IP Pública	IP Virtual UAGs	TCP	443
		TCP	8443

Con la creación de estas reglas, conseguimos que las peticiones hechas desde Internet a nuestra dirección pública, sean redirigidas por nuestros Firewalls a los servidores encargados de realizar la validación de usuario. De esta forma, nuestro entorno queda securizado ante posibles peticiones maliciosas.

Además de lo anterior, como se puede observar en la tabla anterior, se han limitado a dos el número de puertos a los que se permite la conexión desde el exterior con nuestros servidores en la DMZ. Los puertos son:

- Puerto 443 se utiliza para el tráfico Web, así como el tráfico de Horizon Client.
- Puerto 8443 lo utiliza el protocolo Blast, mucho más optimizado para el uso de VDIs que el RDP de Microsoft. Algunas de las ventajas que presenta son:
  - Menor consumo de CPU, que permite mayor autonomía en dispositivos móviles
  - Compensación en caso de aumento de latencia en la conexión
  - Monitorización de la conexión
  - Mejoras en la visualización de la imagen, como color de 32 bits o compatibilidad con ClearType
  - Copiar y pegar texto con formato entre cliente y escritorio remoto
  - Posibilidad de usar hasta 4 monitores
  - Redireccionamiento USB

8.6.2 Configuración Firewall interno

En los Firewalls internos, ubicados entre la DMZ y la red interna, se han de crear una serie de reglas que permitan el tráfico necesario entre las máquinas presentes en la mencionada DMZ y las que se encuentran en la red interna de la empresa. A continuación, se muestra una tabla con estas reglas:

Origen	Destino	Protocolo	Puerto
VLAN VDAs Conexión iniciada por “Horizon Agent “	Servidores Horizon Connection Server	TCP	4002
		TCP	4001
		TCP	389
	Servidor de ficheros	TCP	445
	Directorio Activo/DNS	TCP	389
		TCP	636
		TCP	53
Horizon Connection Server	Horizon Agent Red VLAN VDAs	TCP	22443
		TCP	4172
		UDP	4172

		TCP	3389
		TCP	9427
		TCP	32111
		TCP	32111
	vCenter Server	TCP	443
	Unified Access Gateway (UAGs)	TCP	9443
Unified Access Gateway (UAG)	Horizon Connection Server	TCP	443
	Horizon Agent Red VLAN VDAs	TCP	22443
		UDP	22443
		TCP	4172
		UDP	4172
		TCP	3389
		TCP	9427
		TCP	32111
Consola de administración Navegador a la URL Horizon (Opcional)	Horizon Connection Server	TCP	443
	vCenter Server	TCP	443
	Unified Access Gateway (UAGs)	TCP	9443

8.7 Recursos compartidos

Los datos de los perfiles de usuario no pueden ser almacenados en la máquina a la que éstos acceden, ya que la máquina concedida a cada usuario es aleatoria y el usuario necesita tener siempre disponible su perfil. Por este motivo, el perfil de los usuarios ha de ser móvil. Para ello, han de guardarse en un recurso compartido en el servidor de ficheros de la organización.

También han de crearse recursos compartidos para DEM (Dynamic Environment Manager), que se explicará más adelante en el apartado específico de DEM.

Se adjunta una tabla con los recursos compartidos creados en el servidor “ficheros”, así como los permisos concedidos.

Ruta	Permisos share	Permisos NTFS	Propósito

\\ficheros.midominio.local\DEMConfig$	Ap_Horizon_Administradores=Full Control Todos= Change	Ap_Horizon_Administradores = Full Control Ap_Horizon_Usuarios = Read Domain Computers = Read – for DEM computer ADMX	Repositorio de ficheros de configuración de DEM
\\ficheros.midominio.local\DEMPerfiles$	Ap_Horizon_Administradores=Full Control Todos= Change	Ap_Horizon_Administradores = Full Control Ap_Horizon_Usuarios = Read/Execute, Create Folders – this folder only Creator Owner = Full Control	Repositorios de perfiles de usuario
\\ficheros.midominio.local \CR$	Ap_Horizon_Administradores=Full Control Todos= Change	Ap_Horizon_Administradores = Full Control Ap_Horizon_Usuarios = Read/Execute, Create Folders – this folder only Creator Owner = Full Control	Repositorio de carpetas redirigidas de usuario (Escritorio, Descargas, etc…)

8.8 Certificados

Para poder cifrar las conexiones web y usar el protocolo HTTPS, en vez del HTTP, es importante usar certificados en todos los portales web que sean accesibles. Por este motivo, se usan los siguientes certificados:

- Servidores accesibles desde Internet
  - Certificado Wildcard público: Este certificado será el que se utilice en los portales accesibles desde Internet, en los servidores UAG (situados en la DMZ). Cuando se utiliza un certificado en una conexión, este ha de ser expedido por una entidad certificadora reconocida en las máquinas cliente. Ante la imposibilidad de instalar en cualquier máquina cuyo origen sea Internet, un certificado raíz de una entidad certificadora interna, este certificado Wildcard ha de ser de una entidad conocida.

Por ejemplo, desde la consola de certificados de cualquier Windows, se puede ver en qué entidades confía ese sistema operativo. De esa forma, se puede comprobar que cualquier certificado emitido por la FNMT, DigiCert, GlobalSign, etc. será confiable y no aparecerá ningún error en el navegador del cliente cuando inicie la conexión.

Además de lo anterior, el certificado elegido es de tipo “wildcard”, que son válidos para cualquier nombre dentro de un dominio. El motivo de esta elección es que cualquier empresa, además de la nueva plataforma de VDI, probablemente dispondrá de otras páginas accesibles desde Internet, como podría ser la web. En vez de comprar un certificado para el dominio público con un “Subject” (ha de coincidir con la URL) para cada una de estas páginas, se puede comprar este tipo de certificados que será válido para todos los portales que se publiquen en Internet del dominio público.

- Servidores ubicados en la red Interna:
  - Opción 1: Certificado wildcard interno. Este certificado se instalará en los servidores con el rol de Connection Server, solamente accesibles desde la red interna. Al no estar publicado en Internet, no es necesario comprarlo a una entidad certificadora externa, sino que podríamos crearlo desde nuestra entidad integrada con el Dominio. Con ello, conseguiríamos que todas las máquinas que estén unidas al Dominio, ya confíen en esta entidad certificadora, que ha expedido el certificado que estamos usando.

  - Opción 2: Certificado expedido en una entidad open source. Un ejemplo de este tipo de entidades sería “XCA”. Con esta opción, las máquinas no tendrían en su lista de entidades certificadoras raíz reconocidas, solo por el hecho de estar en el Dominio, por lo que tendríamos que distribuir el certificado Raíz de esta entidad a todos los PCs del dominio a través de una GPO.

9 Instalación VMWARE Horizon 8

9.1 Connection Server

Se comenzará con la instalación de los servidores que tendrán el rol de CS. A partir de estos, se irán añadiendo servidores con el resto de roles que permitan disponer de todos los servicios requeridos. A continuación se describen los aspectos básicos de la instalación con el detalle técnico en el Anexo I.

9.1.1 Instalación máquina virtual

1. Se crean dos máquinas virtuales con las siguientes características hardware:
    - CPU: 4vCPUs
    - RAM: 12 GB
    - Disco duro: 100 GB
    - NIC: VMXNET3
1. SO: Windows 2019 Standard Eng

Algunas de las consideraciones básicas que debemos tener en cuenta durante la instalación de estos servidores, como seguridad y organización, son las siguientes:

- Crear cuentas de usuario en AD específicas para cada función. No usar las cuentas de usuarios reales, ni cuentas de administrador del dominio.
- Las cuentas de usuario creadas deben estar en una OU específica para este fin, no mezclarlas con el resto de cuentas de usuario o en ubicaciones por defecto.
- Cuando lo permisos sean para varios o usuarios, o estos sean variables (posibilidad de altas y bajas) trabajar con grupos para facilitar la administración y el mantenimiento.
- Deshabilitar túnel seguro (Secure Tunnel). Por defecto, esta configuración está habilitada y los clientes de Horizon se conectan a los agentes de Horizon

(Escritorios) a través de un túnel Blast o PCoIP, proporcionado por los servidores Connection Server. Sin embargo, es más eficiente que los clientes internos de Horizon se conecten directamente a los agentes de Horizon en lugar de hacerlo a través de los Connection Server.

- Configurar el backup integrado de Horizon, además de otros posibles backups de terceros.
- Para evitar hacer uso de los certificados autofirmados y que al acceder nos aparezca un error con el mensaje de que la página no es segura, es necesario cambiar los certificados. Para ello, haremos uso del certificado Wildcard explicado anteriormente, generado por una entidad certificadora en el que confíen todos los clientes.

9.2 Unified Access Gateway (UAG)

Unified Access Gateway es un appliance, por lo que no requiere instalación, y tampoco licencia Windows, ya que tiene el sistema operativo Photon, basado en Linux. Está diseñado para permitir el acceso remoto sobre la plataforma Horizon, y por este motivo, ha de estar ubicado en una red DMZ, desde la que permitirá solamente el tráfico autorizado de los usuarios autenticados, hacia nuestra red interna.

Este servidor será el encargado de autenticar a los usuarios, y dispone de diferentes métodos de autenticación y MFA (Multi Factor Authentication).

A continuación, se listan algunas de las consideraciones durante la instalación de estos servidores, incluyendo el detalle de la instalación en el Anexo II:

- Como se ha explicado anteriormente, estos servidores se ubicarán en la red de la DMZ.
- Estos servidores han de tener un certificado que no muestre el error de “la página no es segura”. Para ello, se instala en ambos servidores UAG el certificado Wildcard explicado anteriormente.
- Configurar los servidores en HA.

10 Configuración MFA

Los usuarios se conectan a la plataforma Horizon a través de Internet, por lo que, además de las medias de seguridad de la red como Firewalls, UAG en DMZ, etc… se recomienda poner una capa más de seguridad para mantener nuestros sistemas protegidos de las amenazas externas. Para ello, se implementa MFA, es decir, un factor múltiple de autenticación que consiste en algo que el usuario sabe (usuario y password) y algo que el usuario tiene (token).

Los servidores UAG permiten diversos métodos de autenticación y para lograr tener un MFA se han de combinar 2 de ellos. Los métodos soportados por UAG son los siguientes:

- AD Credentials. Son las credenciales de usuario/password necesarias para validarse dentro del Dominio en el que se encuentra la infraestructura Horizon. Este tipo de autenticación es redirigida a los servidores CS usando passthrough.
- RSA Secure ID. Los usuarios han de tener un PIN, para poder acceder a los escritorios virtuales. Este método requiere de un servidor extra (RSA Authentication Manager) y la autenticación se realiza en los servidores CS, por lo que es redirigida de los UAGs a estos usando passthrough.
- RADIUS. Utilizando este mecanismo, Horizon admite un amplio rango de soluciones MFA basadas en Token, como OTP, que es similar al explicado en el punto anterior.
    - Este tipo de autenticación es redirigida a los servidores CS usando passthrough.
- Smart Cards. Esta validación se realiza directamente en el UAG y proporciona SSO a los escritorios virtuales, permitiendo hacia la red interna solamente el tráfico autenticado.
    - Permite la configuración de CRLs para evitar la conexión de usuarios con el certificado caducado o revocado.
- SAML. Autenticación basada en la confianza entre un servidor con un servicio determinado y un proveedor de identidades que realiza la validación.
  Este tipo de autenticación es redirigida a los servidores CS usando passthrough.

El detalle de la instalación está incluido en el Anexo III.

10.1 Requisitos

SAML permite a un servidor o plataforma, que provee de un servicio como VDI, la delegación de la validación de un usuario a un IdP de una organización externa. Una vez realizada esta validación, el IdP devuelve un token que permitirá el acceso al servicio sin la necesidad de volver a pedir credenciales al usuario. Toda esta comunicación se realiza de forma segura.

Trasladando la definición anterior a nuestro proyecto, con SAML podemos aprovechar las ventajas que nos ofrece Azure con respecto a la validación de usuarios y combinarlo con VMware Horizon. Azure AD dispone de nuestra base de datos de usuarios/passwords y de un método de autenticación múltiple basado en token, por lo que al realizarse la validación usando Azure como IdP podremos aprovechar estas ventajas.

Para poder implementar esta infraestructura, es necesario tener en cuenta algunos requisitos:

- Los usuarios que hagan uso de Horizon necesitan licencia P1 de Azure (Incluída en E3 de Office 365)
- Servidor ADConnect para sincronizar usuarios desde DA OnPremise a Azure AD
- Se crea un grupo en AD, que contendrá los usuarios con la autenticación multifactor habilitada en Office 365, para proveer el nivel de seguridad deseado.

10.2 Configuración

Par poder habilitar el doble factor de autenticación al acceder a nuestra plataforma VDI, combinando Horizon y Azure, es necesario realizar 3 tipos de configuración:

- Configuración en Azure AD. Desde aquí se ha de añadir una aplicación empresarial propia, en la que se establecerán los siguientes puntos:
    - Inicio de sesión único con SAML

- Grupo con permisos de acceso
- Se descargará el archivo XML que posteriormente habrá que importar en los servidores UAG

- Configuración de los usuarios. A los usuarios con permisos sobre la plataforma, habrá que habilitarles MFA como tipo de autenticación. Esta configuración se realizará añadiéndoles al grupo creado anteriormente con este fin.
- Configuración en Horizon. Se llevará a cabo en los servidores UAG. Estos son los servidores que atenderán la petición de acceso al entorno VDI y que se encargarán de conectar tanto con Azure como con los internos (CS). Las configuraciones más importantes a tener en cuenta son las siguientes:
  - Importar archivo "XML de metadatos de federación" en ambos servidores UAG.
  - Habilitar método de autenticación SAML

Una vez realizada esta configuración, cada vez que se acceda a Horizon desde Internet (usando tanto Horizon Client como por HTML5), se solicitarán las credenciales de Office 365 y la validación MFA a través de Microsoft Authenticator.

10.3 Microsoft Authenticator

Como se explica anteriormente, una vez realizada la configuración anterior, los usuarios necesitarán realizar una validación adicional. Esta validación puede ser a través de su número de teléfono, mensaje de texto o instalándose la aplicación "Microsoft Authenticator" que le generará un código de 6 cifras y que habrá de introducir después de realizar la validación con su usuario y *password*.

Además, para facilitar la validación al usuario, con esta aplicación móvil inmediatamente después de introducir sus credenciales, le aparecerá en su teléfono un mensaje pidiéndole la confirmación del inicio de sesión, que deberá aprobar y confirmar con sus datos biométricos (huella).

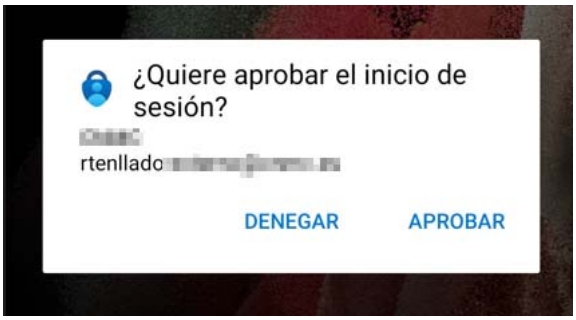


Ilustración 16. Validación APP móvil

Una vez aprobada esta solicitud, el usuario será redirigido a los escritorios virtuales sobre los que tenga permisos, para entrar en uno de ellos y comenzar a trabajar.

11 DYNAMIC ENVIRONMENT MANAGER (DEM)

11.1 Descripción

Uno de los problemas más comunes en un entorno de escritorios virtuales, donde las máquinas se crean y se destruyen según la demanda, es la persistencia de los cambios que realiza el usuario. Esto es una de las diferencias más grandes que van a encontrar los usuarios con respecto a la forma de trabajar más tradicional, en la que cada usuario tenía su propio PC.

Estos cambios pueden ser a nivel de su propio perfil, como una imagen en el escritorio, pero también pueden ser cambios que les afecten en su trabajo, como configuraciones de las aplicaciones empresariales. Un ejemplo de este último, podría ser la conexión a su buzón de Office 365 desde Outlook, un caso en el que, si no se usa ninguna herramienta de gestión de perfiles, los usuarios tendrían que conectárselo cada vez que iniciasen sesión.

Para evitar este problema, VMware Horizon cuenta con la herramienta Dynamic Environment Manager (DEM). Esta herramienta facilita al administrador la gestión de perfiles de usuario y permite poder realizar personalizaciones persistentes, independientemente del escritorio virtual al que se conecte el usuario. Además, también permite administrar estos perfiles de forma dinámica y centralizada mediante GPOs.

Entre las ventajas más importantes que ofrece DEM, se encuentran:

- **Personalización de perfil para todos los dispositivos**. Cada usuario puede realizar sus propias personalizaciones, que le acompañarán independientemente del dispositivo y el lugar desde el que se conecte. Esto facilita transformar lo que, en principio era un problema, en una ventaja, ya que la personalización de su entorno no solo la encontrará en su PC.
- **Centralización y simplificación en la gestión de perfiles**. DEM facilita al administrador de la plataforma de escritorios virtuales su trabajo, de forma que puede gestionar la personalización por usuarios, así como por perfil del

trabajador. De esta forma, se evita el uso de scripts de inicio de sesión, lo que permite facilitar la escalabilidad del entorno, y permite un crecimiento sin que repercuta en la complejidad de la administración.

- **Tiempo de respuesta en el inicio de sesión**. DEM también permite que los escritorios estén disponibles de una forma más veloz, evitando esperas por parte del usuario y perjudicando la calidad en la experiencia del usuario.

11.2 Instalación y Configuración

Para utilizar DEM, es necesario disponer de un almacenamiento centralizado, donde guardar los perfiles de usuario y las configuraciones de éste. Con este fin, se debe disponer de un recurso compartido donde se guardarán todas las configuraciones específicas de la herramienta, en la que tengan acceso todos los usuarios de VDI.

También deberá existir un recurso compartido donde se guarden los archivos específicos del perfil de cada usuario, en el que al igual que en el recurso anterior, tengan permisos todos los usuarios. Es necesario puntualizar que, en este último recurso, a pesar de tener acceso todos los usuarios, sobre cada perfil solamente tendrá permiso el dueño de ese perfil.

Otro punto necesario para el correcto funcionamiento de esta herramienta es la instalación y configuración de una serie de GPOs específicas para este fin. Con ello, se consigue administrar los siguientes aspectos:

- Configuración automática en todos los usuarios del almacenamiento donde se guardan los archivos de perfil de cada usuario
- Generación de archivos de log, configuración de estos y alertas referentes a estos archivos
- Comportamiento de los escritorios en caso de que el usuario no pueda acceder a los recursos compartidos de configuración y almacenamiento de perfiles
- Ubicación de los backups de perfiles de usuario y las opciones relativas a estos, como número de backups guardados y frecuencia de generación

- Configuración de opciones de perfiles almacenados, como compresión de archivos

El detalle y explicación técnica de todas las instalaciones y configuraciones relativas a DEM se encuentran en el anexo sobre DEM.

12 TRUE SSO

Según el objetivo marcado en este proyecto, por el que se dispondrá de MFA, cuando un usuario va a iniciar sesión en Horizon, uno de los servidores frontales (UAG) le solicita las credenciales. Éstas son validadas contra un IdP (proveedor externo de identidad) como es Azure AD, y la conexión se envía a los servidores internos en la red (CS), que al tener una validación integrada con DA, volverán a pedir credenciales, obligando al usuario a introducir 2 veces las mismas credenciales.

Para evitar esto, VMware dispone de la validación "True SSO", que requiere de un servidor "Enrollment Server". Este servidor se encarga de realizar peticiones de certificados, de parte del usuario que se está logando, a una entidad certificadora válida en el Dominio.

Los certificados que solicita este servidor, han de tener un período de validez muy corto por razones de seguridad, válido solamente durante el tiempo que duran las sesiones de los usuarios. De esta forma, cada vez que un usuario quiera volver a iniciar sesión, se volverá a solicitar un certificado a la CA correspondiente.

TRUE SSO necesita que estén permitidas las siguientes comunicaciones:

Origen	Destino	Protocolo	Puerto
Horizon Client	VMware Identity manager	HTTPS	TCP 443
	Horizon Connection Server		
Horizon Connection Server	VMware Identity Manager	HTTPS	TCP 443
	Horizon Enrollment Server		
Horizon Enrollment Server	AD CA		TCP 135
Horizon Agent	Horizon Connection Server		TCP 4002
Horizon Client	Horizon Agent	Blast	TCP/UDP 22443
Horizon Client	Horizon Agent	PCoIP	UDP 4172

Requisitos servidor Enrollment Server:

- Sistema Operativo Windows Server 2012 R2, Windows Server 2016 o Windows Server 2019
- Requisitos mínimos de memoria: 4GB
- El rol puede ser instalado sobre la misma máquina que tiene la función de Enterprise CA
- No se puede instalar sobre las siguientes máquinas
    - Controlador de dominio
    - Connection Server
    - Máquinas con Horizon Client o Horizon Agent instalado
- La máquina ha de ser miembro del dominio de Active Directory
- IPv6 no está soportado, la máquina debe usar IPv4 con IP fija

El detalle de las instalaciones de servidores, así como todas las configuraciones y detalles técnicos se encuentran en el anexo instalación y configuración true SSO.

13 IMAGEN GOLDEN

Para que los usuarios puedan conectarse a las máquinas a través de Horizon, es necesario crear una plantilla o "imagen Golden", que ha de tener toda la configuración y aplicaciones que luego verán los usuarios. Desde esta plantilla, se generan las imágenes que son realmente donde se conectan los usuarios.

Como se ha explicado en el apartado anterior, cuando una máquina se reinicia o se apaga, se vuelve a generar una nueva imagen, por lo que todos los datos que no estén guardados en el perfil móvil del usuario o en unidades de red externas, desaparecerá. Esto también hay que tenerlo en cuenta con respecto a las aplicaciones, si un usuario instala algo en una máquina, la próxima vez que se conecte, puede que no se conecte a la misma máquina, por lo que no aparecería y, además, puede que, aunque la máquina tenga el mismo nombre, se haya reiniciado y tampoco tendría la aplicación instalada.

Por los motivos mencionados anteriormente, es muy importante generar una imagen Golden completa, con todo el software que necesitarán los usuarios y con las configuraciones necesarias para realizar su trabajo.

Lo primero que hay que tener en cuenta, al generar esta imagen son los requisitos necesarios para que sea capaz de soportar toda la carga de trabajo que demandarán los usuarios. Por lo tanto, es necesario hacer un estudio de los requisitos que publican los fabricantes de cada una de las aplicaciones que se instalarán.

Otro punto importante es tener en cuenta la matriz de compatibilidad[1] que publica VMware sobre sistemas operativos soportados, según la versión de Horizon que tengamos instalada. Además de la consulta inicial a esta matriz, también es importante tenerla en cuenta para futuras actualizaciones del sistema operativo.

La seguridad es un punto importante para cualquier empresa, y tener las máquinas actualizadas es una de las tareas básicas en cualquier organización. Teniendo en cuenta lo que se ha visto hasta ahora, las actualizaciones siempre se han de realizar sobre esta

[1] Supported versions of Windows 10 on Horizon Agent Including All VDI Clones (Full Clones, Instant Clones, and Linked Clones on Horizon 7) (2149393) (vmware.com)

imagen Golden, para luego redistribuirla en las máquinas sobre las que se conectarán los usuarios.

Otras tareas a tener en cuenta al instalar y configuración esta imagen, son las siguientes:

- Mantener la organización en el DA, y mover el nuevo objeto de máquina creado a su correspondiente OU
- Instalar el agente de DEM para poder gestionar los perfiles como se ha visto en el punto anterior de este documento
- Ejecutar la herramienta OS Optimization Tool. Esta herramienta permitirá optimizar la imagen para un entorno VDI. Entre otras configuraciones, ejecutará "sysprep.exe" que quitará el SID de la máquina para que sea recreado en el arranque. Además, realizará otras configuraciones como eliminarle la dirección IP, quitar archivos temporales, vaciar la papelera, etc.

El detalle de todas las instalaciones necesarias y las configuraciones descritas se encuentra en el anexo de creación de imagen Golden.

14 CREACIÓN DE POOL DE ESCRITORIOS INSTANT CLONES

14.1 Descripción

Instant Clone es la tecnología por la cual, Horizon provee de forma instantánea a los usuarios escritorios personalizados. Esto lo consigue mediante el clonado de la Golden Image en el momento en el que un usuario realiza el login, dejándola encendida y lista para que el usuario pueda trabajar.

Estas son algunas de las ventajas que presenta esta tecnología:

- Reducción de costes por la administración que realiza en cuanto a máquinas encendidas. También reduce la necesidad de espacio en disco, ya que elimina los archivos de máquinas apagadas
- Despliegue de máquinas de forma sencilla
- Mejora de la seguridad debido a que elimina las máquinas en el momento en que un usuario cierra sesión
- Parcheado de las máquinas más rápida y eficiente, debido a que solamente se requieren los parches en la Golden Image

14.2 Modos de asignación

En Instant Clone se puede elegir entre 2 tipos de asignación de “Pools” de escritorios para los usuarios, cada uno con sus ventajas e inconvenientes. Es importante tener claro cómo funciona cada uno, para poder elegir el que mejor se adapte a las necesidades de nuestra empresa. Estas son las características de cada uno de ellos:

- **Dedicated user assignment**. Cuando un usuario entra a la plataforma, se le asigna una máquina del pool. Esta máquina siempre se le asignará a este usuario y no se le asignará a ningún otro usuario, incluso aunque el usuario no la esté usando y no queden máquinas en el pool.

  - Con este tipo de configuración, se pueden permitir cambios persistentes en las máquinas.

- **Floating user assignment**. Cuando un usuario entra a la plataforma, se le asigna una máquina de forma aleatoria, permitiendo a todos los usuarios de Horizon usar cualquier máquina que esté libre dentro del pool en ese momento. Cuando el usuario vuelva a entrar, se le volverá a asignar una máquina de forma aleatoria.
  - Con este tipo de configuración se pueden ahorrar costes en licencias, ya que hay que tener en cuenta el máximo de conexiones concurrentes que pueden existir en la plataforma.

En nuestro caso, se ha elegido el tipo "Floating user assignment", ya que lo que se pretende es la estandarización de escritorios y el ahorro de costes.

Durante la creación de un pool de escritorios, hay que prestar atención a las siguientes configuraciones:

- Elegir el tipo más adecuado para cumplir los requerimientos empresariales. Como se ha explicado anteriormente, para este proyecto se selecciona "Floating user assignment", sin embargo, el tipo es una decisión importante y debe ir acorde con las necesidades.
- Configurar un patrón adecuado para los nombres con los que se crearán las máquinas virtuales a partir de la nueva imagen.
- Para poder configurar el pool desde la imagen Golden, se ha debido de realizar un *snapshot* previamente. Será éste el que se seleccionará para generar las máquinas virtuales.
- Mantener el orden dentro de la plataforma de virtualización VMware. Para ello, crear una carpeta por cada imagen para que puedan crearse ahí las nuevas máquinas. Igualmente, se debe crear una OU específica para estas máquinas dentro del DA.

Todas las configuraciones necesarias para generar un pool de escritorios están detalladas en el anexo instalación del pool de escritorios.

15 FORMACIÓN DE LOS USUARIOS

Una vez implementada la solución y con todas las funcionalidades operativas, hay que pasar a la puesta en producción. Para ello, es necesario dar a conocer a los usuarios el nuevo sistema, así como facilitar el conocimiento de la plataforma por parte de estos y facilitar el soporte ante cualquier posible incidencia técnica.

Uno de los problemas más comunes en casos de fracaso de proyectos, es la resistencia al cambio por parte de las personas que lo han de utilizar. Esta resistencia viene derivada de la propia naturaleza de las personas, acostumbradas a realizar su trabajo de una determinada forma, y que además les funciona, por lo que suelen ser reticentes a cambiarla.

Otra de las razones por la que los usuarios no tienen una buena predisposición a cambiar sus herramientas de trabajo, es el desconocimiento de la forma de uso. Este desconocimiento provoca que la nueva herramienta sea percibida como poco útil o simplemente como que “no funciona”.

Para evitar estos posibles problemas, que pueden llevar al fracaso del proyecto, se han de dar unas sesiones de formación a todos los usuarios implicados. Estas formaciones deben cubrir los siguientes aspectos:

Motivos por los que se ha implantado y qué ventajas ofrece. Es muy importante que el usuario sea capaz de sentirse parte del proceso de cambio y comprenda las razones que lo han motivado. Este hecho facilitará que no lo vea como un algo molesto y negativo, sino algo que será útil tanto para la empresa como para su trabajo.

Entre las posibles ventajas que se pueden argumentar, se encuentran la posibilidad de que pueda realizar su trabajo desde fuera de la oficina y desde cualquier dispositivo, lo que le puede facilitar la conciliación familiar, por ejemplo. Otro punto positivo para la empresa y por extensión, para el usuario, es el ahorro energético que lleva consigo, en un momento en el que los costes por este apartado se están disparando.

Para lograr este objetivo, bastaría con realizar una sesión de formación de 4 horas, a todos los empleados que vayan a hacer uso de los escritorios virtuales. Esta sesión se

repetirá las veces necesarias, de forma que todos puedan asistir, pero sin que se vea afectada la productividad de la empresa.

El usuario debe conocer las capacidades de la nueva plataforma. Para lograr sacar el máximo rendimiento a la nueva infraestructura, así como permitir que el usuario pueda realizar su trabajo de la mejor forma posible, es necesario que éste conozca las posibilidades que se le ofrecen.

Un ejemplo práctico es que no todos los usuarios trabajan de la misma forma, por lo que es interesante que conozcan hasta qué punto se puede personalizar su perfil, qué herramientas pueden solicitar en sus escritorios, y donde han de guardar sus archivos para que estén disponibles siempre, independientemente de la máquina a la que se conecten.

Otro punto importante es el de la seguridad, motivo por el que los usuarios deberán instalarse una aplicación en su móvil que les generará un código válido durante un corto espacio de tiempo, y que les asegurará un acceso seguro a los datos de la empresa.

Con la finalidad de cumplir este objetivo, se estima que son necesarias 2 sesiones de formación de 4 horas. Al igual que en el punto anterior, deben repartirse los usuarios que acudan a estas sesiones para que no se vea afectado el funcionamiento normal de la empresa.

Conocimiento de los casos de uso que ofrece. Otro de los puntos importantes es que el usuario conozca y domine los posibles casos de uso que se ofrecen, con el objetivo de optimizar el tiempo y la productividad resultante.

Un ejemplo práctico puede ser la forma de utilizar el cliente pesado o el acceso HTML, cuándo es recomendable uno y cuándo otro. También es importante que se conozca la forma en la que funciona un VDI, ya que difiere mucho en algunas situaciones con respecto a la forma en que venían trabajando, utilizando un PC personal. Por ejemplo, en el caso de cambiar un archivo de configuración, esos cambios solamente se guardan en ese PC, con lo que es muy probable que no estén disponibles en su próxima conexión.

Para estas sesiones de formación, se estiman necesarias 2 jornadas de 4 horas para todos los usuarios que vayan a hacer uso de la plataforma. Al igual forma que los puntos

anteriores, los usuarios deben ser distribuidos de manera que no afecte a la productividad de la empresa.

Dónde acudir en caso de problemas. Con el fin de que el usuario tenga la menor cantidad de incidencias informáticas posibles, sobre todo al inicio del proyecto, es necesario que conozca qué hacer si se presenta un error. Estos problemas y, sobre todo, el no saber gestionarlos, puede provocar una reacción negativa del usuario al uso de un escritorio virtual.

Debe existir un CAU que aporte confianza al usuario a través de una atención rápida y efectiva ante la aparición de cualquier problema. Para ello, es importante que exista una base de datos de conocimientos, donde se documenten todas las incidencias que vayan apareciendo y que sirva de referencia a los técnicos a la hora de solucionar un problema.

16 CONCLUSIONES

16.1 Lecciones aprendidas

Para realizar este trabajo ha sido necesario dedicarle mucho tiempo, en el que he podido aprender varias lecciones. Una de ellas es la importancia de tener una buena planificación, necesaria tanto para lograr un resultado de calidad como para poder distribuir de forma óptima el tiempo disponible y compaginarlo adecuadamente con el resto de actividades de la vida diaria.

Además de lo anterior, también he aprendido sobre cómo afrontar un proyecto de este tipo. Entre estas lecciones aprendidas, destacaría como se debe enfocar, no centrándose solamente en aspectos técnicos, sino que el resultado debe ser algo más global. El trabajo final debe explicar de donde surge la idea, por qué puede ser de utilidad para muchas empresas, las diferentes decisiones que se deben adoptar y el impacto que puede tener.

Otro punto que resaltaría en el aprendizaje logrado a lo largo de este tiempo, es el conocimiento adquirido en el campo sobre el que se ha trabajado. Al desarrollar los distintos puntos que componen el TFG, he podido profundizar en diferentes soluciones disponibles en el mercado, por ejemplo, a través de las comparativas. Esto creo que me ha proporcionado una visión más global del sector, y a tener un conocimiento más amplio y completo.

También creo que es importante destacar un punto al que no le prestaba la atención debida, y que de aquí en adelante lo tendré siempre muy presente. El punto referido es a los formatos, la presentación, en definitiva, a los detalles que hacen que el resultado final se presente de forma que el lector perciba que está ante algo trabajado, de calidad. Ahora creo que esto se consigue no solamente con el contenido, sino también con la forma en que se presenta.

16.2 Reflexión crítica sobre el logro de objetivos

La sensación final que me deja este trabajo una vez terminado, es la de haber logrado el objetivo que me marqué en su inicio. Mi intención era exponer las ventajas de este tipo de entornos y explicar con todo el detalle posible como se podía hacer. Además, también pretendía combinar la tecnología elegida con otras de uso muy común, de forma que se viese como este hecho ofrecía mejoras sustanciales en aspectos como la seguridad.

Como explicaba en el párrafo anterior, creo que los objetivos marcados y descritos anteriormente se han logrado. Sin embargo, creo que durante este tiempo y según iba adquiriendo un conocimiento más profundo de la materia, han surgido muchas ideas que no estaban planificadas inicialmente y que creo, hubiesen sido positivas en el resultado final.

A pesar de esas ideas, existía una planificación ya de por sí muy estricta y que, de haberla ajustado más aún, podría haber resultado en un trabajo final de menos calidad. En este caso, se podría decir que se ha tomado la decisión de seguir el camino de la profundidad y riqueza en cuanto a detalles, en lugar de la cantidad y abarcar una cantidad muy grande de campos, pero poco trabajados.

Es posible que, si estas ideas se hubiesen tenido en cuenta desde un principio y se hubiese realizado una planificación teniéndolas en cuenta, se podría haber hecho una mejor programación de trabajos y haber optimizado mejor las horas dedicadas a cada aspecto. Sin embargo, también creo que para haber tenido esas ideas era necesario tener el conocimiento actual sobre la materia y esto lo he logrado realizando este trabajo, lo que me sirve como prueba de que se han logrado los objetivos.

16.3 Seguimiento de la planificación y metodología

La planificación y la metodología son 2 de los pilares sobre las que se asienta el éxito de un trabajo. Creo que es un error muy común comenzar afrontando un reto de este tipo con muchas ganas e ilusión, con la cabeza llena de ideas, que invitan a comenzar a

desarrollarlas sin ninguna planificación ni metodología. Este error puede provocar que se olviden algunas de estas ideas, que se dedique mucho tiempo a un aspecto poco importante, que no se siga un orden lógico o que los cambios provoquen incoherencias sobre el conjunto del trabajo.

En mi caso, creo que habría podido caer fácilmente en los errores comentados anteriormente, sin embargo, el seguimiento de la programación de la asignatura ha sido importante para evitarlos. Tanto el consultor como el enfoque que tiene la propia asignatura, en el que la primera entrega es específica para preparar estos aspectos, ha sido de gran ayuda para no cometerlos.

Una vez realizada la planificación, ha servido como motivación para intentar en todo momento su seguimiento. Además, me ha proporcionado una visión clara de hitos necesarios y el momento en el que debían de estar logrados, para no perjudicar el conjunto del trabajo. Este aspecto, en un trabajo tan largo, creo que es muy relevante y ha sido una de las claves para lograr su consecución.

Por otro lado, elegir una metodología adecuada es otra de las claves que tendrán un peso grande en el resultado final. Para ello, creo que hay que tener en cuenta algunos aspectos como la naturaleza del proyecto que vamos a realizar. En este caso, se ha tenido en cuenta la relevancia de que se producirán constantes cambios en los requisitos, debido al hecho de que no se disponía de experiencia previa en el desarrollo de este tipo de proyectos. Efectivamente, durante el transcurso del trabajo, el consultor ha ido sugiriendo cambios importantes, tanto en el enfoque como en el contenido. Estos cambios no han supuesto un problema gracias a la metodología elegida.

La metodología también es importante en cuanto a la interacción con “el cliente”, personificado en este caso en el consultor que da el visto bueno el trabajo que se está realizando. En una metodología clásica, los requisitos son definidos al inicio del proyecto y no hay, o hay muy pocas, interacciones por lo que se entrega al final el resultado del trabajo. Esta filosofía no encajaba con la forma en la que se estructura la asignatura, con diversas entregas puntuables, por lo que una metodología ágil que permitiese interacciones continuas y disponer de resultados concretos sobre los que seguir evolucionando fue la opción elegida.

Además de lo anterior, se han llevado varias líneas de trabajo de forma concurrente, por lo que disponer de un panel en el que se viesen de forma conjunta lo que se estaba haciendo, en qué situación se encontraba y lo que restaba por hacer era muy importante. En esta línea, Trello ha resultado una herramienta muy útil, que permitía lograr estos objetivos.

En líneas generales, diría que se ha logrado seguir tanto la planificación como la metodología, aunque no ciertas dificultades como pueden ser el tiempo y lograr una planificación precisa con relación a la planificación. Con respecto de la metodología, creo que ha sido una elección acertada el tipo elegido, aunque también ha presentado algunas dificultades como el extra de tiempo que supone su aplicación y el de conocimientos necesarios, aunque ha sido de gran ayuda los adquiridos en algunas asignaturas del grado.

16.4 Líneas de trabajo futuras

Como se mencionaba anteriormente, han existido ideas que surgían durante la realización del proyecto y que no ha sido posible su desarrollo. Sin embargo, creo que es interesante dejarlas reflejadas en el trabajo final.

Una de estas ideas es el detalle de costes que podría suponer la implantación de esta solución. Creo que podría ser muy interesante incluir un presupuesto que de una idea de la inversión necesaria que ha de realizar una empresa. Este presupuesto debería incluir costes de hardware, licencias, formación, etc.

Otro punto en el que se puede trabajar en el futuro es el de la integración de las aplicaciones más comunes en un entorno VDI, así como ventajas y desventajas. Por ejemplo, en muchas empresas se utilizan clientes de correo como Outlook en el que es importante el perfil del usuario para mantener configurado siempre su buzón, así como los archivos locales para evitar una sincronización constante. Otra aplicación

interesante, dentro de este contexto, es Microsoft Teams ya que también requiere de persistencia en cuanto a perfil y existe un paquete específico para su instalación en VDI.

Además de las herramientas explicadas en este documento, existen otras muy interesantes como “Application profiler”, que permite capturar cambios realizados por el usuario en una aplicación determinada. Una vez capturados estos cambios, la herramienta es capaz de generar un archivo de texto que referencia archivos y claves del registro, modificados por el usuario y que se pueden incorporar a su perfil para mantener estas configuraciones a pesar de iniciar sesión en máquinas aleatorias.

Por último, creo que también podría ser interesante desarrollar un apartado en el que se expliquen posibles problemas que podrían aparecer durante la instalación, así como su solución. Como en la mayoría de implantaciones, la práctica no es idéntica a la teoría y existen ciertas particularidades o personalizaciones que pueden generar en situaciones o errores no esperados.

17 Glosario

DA. Estas siglas corresponden a “Directorio Activo”, una base de datos que contiene los objetos de un Dominio de Windows.

VDI. Siglas del término en inglés “Virtual Desktop Infrastructure“, una plataforma que permite la creación bajo demanda de escritorios virtuales, accesibles desde cualquier lugar y dispositivo.

CA. Siglas del término en inglés “Certification Authority”, entidad generadora de certificados digitales para la securización de las conexiones.

Hypervisor. Software que permite la creación y administración de máquinas virtuales, sobre una máquina física que comparte sus recursos.

GPO. Siglas del término en inglés “Group Policy Object”, que permite la generación de ciertas configuraciones para la administración centralizada dentro de un dominio de Windows.

Firewall. Dispositivo para la securización de una red. Existen distintos tipos, tanto software como hardware, que permite controlar el tráfico dentro de una red, así como permitir o denegar el accceso.

VLAN. Siglas del término en inglés “Virtual Local Area Network”. Permite la segmentación de una red física en varias lógicas, ofreciendo mejoras en cuanto a seguridad y rendimiento.

HA. Siglas en inglés de “High Availability”. Este término hace referencia a una configuración por la cual una máquina o un servicio determinado tiene un alto índice de disponibilidad, a pesar de posibles fallos.

MFA. Siglas en inglés de “Multi Factor Authentication”. Mediante este sistema, es necesario presentar credenciales usando más de un método. Generalmente, uno es algo que el usuario sabe y el otro es algo que el usuario tiene.

SAML. Acrónimo de las siglas en inglés "Security Assertion LangUnified Access Gateway". Es un método para asegurar que un usuario es quien dice ser frente a una petición de validación.

CRL. Siglas en inglés de "Certificate Revocation List". Es una lista que publican las entidades certificadoras para anunciar que esos certificados emitidos por ellas mismas, ya no son de confianza.

Certificado revocado. Cuando un usuario tiene un certificado válido dentro de un entorno de seguridad definido y éste abandona la empresa, pierde su certificado o cambia de entorno de seguridad, es necesario convertir ese certificado válido en inválido, de forma inmediata.

Passthrough. Consiste en pasar las credenciales de validación de un servidor a otro, en el que el usuario no se ha validado, de forma segura.

Token. Es un elemento que puede ser software, como un PIN, o un elemento hardware.

RADIUS. Remote Authentication Dial-In User Service. Las credenciales facilitadas a un servidor, son enviadas al RADIUS, habiendo encriptado esta información con una clave que ambos elementos conococen. De esta forma, este puede realizar la validación, así como el control de las sesiones y los permisos concedidos.

CAU. Acrónimo de "Centro de Atención a Usuarios".

IdP. Proveedor de identidad. Realiza las funciones de validación de usuarios.

SSO. Siglas en inglés de "Single Sign-On". Hace referencia a la posibilidad de realizar una sola autenticación y mantener esas credenciales durante toda la sesión.

Appliance. Dispositivo físico que cumple una determinada funcionalidad. Funciona como un paquete completo diseñado para realizar esa tarea específica.

SID. Siglas en inglés de "Security Identifier". Es un código que contiene información relativa al objeto al que hace referencia.

18 Bibliografía

Imagen portada (Septiembre 2022)

Sistemas VDI y teletrabajo, la dupla perfecta en tiempos del COVID-19 | INCIBE

Estudio tendencia teletrabajo (Octubre 2022)

[1][2][3]Current trends in remote working (assets.kpmg)

Las nuevas tendencias de teletrabajo 2022 (workmeter.com)

Qué es VDI (Octubre 2022)

¿Qué es Infraestructura de escritorio virtual (VDI)? | Microsoft Azure

¿Qué es una infraestructura de escritorios virtuales (VDI)? | Glosario de VMware | ES

[4]Virtualizing Tough 3D Workloads with VMware Horizon View and NVIDIA Technologies (gputechconf.com)

Citrix – Vmware (Octubre 2022)

https://www.parallels.com/blogs/ras/citrix-vs-vmware/

https://wire19.com/vdi-options-compared-vmware-horizon-vs-citrix/

https://www.irangers.com/citrix-vs-vmware/

https://www.acecloudhosting.com/blog/citrix-vs-vmware-vdi/

[5]Resumen técnico: Citrix Gateway y Citrix Virtual Apps and Desktops

RDS (Octubre 2022)

https://itopia.com/vdi-vs-rds-which-is-better-for-you/

VDI – RDS (Octubre 2022)

https://www.anuntatech.com/blog/windows-virtual-desktops-vs-horizon-vs-citrix/

[7]https://kryptonsolid.com/que-son-los-servicios-de-escritorio-remoto-rds/

Arquitectura VMware Horizon (Octubre 2022)

[6]https://vinfrastructure.it/2020/10/vmware-horizon-deployment-guide-using-kemp-vlm/

https://techzone.vmware.com/resource/horizon-architecture#scaled-single-site-architecture

[9][10][11]Horizon Architecture | VMware

Arquitectura VMware Horizon - Connection Server/UAG/Agent (Octubre 2022)

https://docs.vmware.com/en/VMware-Horizon/2103/horizon-architecture-planning.pdf

Horizon Architecture | VMware

Arquitectura VMware Horizon - Enrollment Server (Noviembre 2022)

[13]Horizon View 7.5 : Deploy View Enrollment Server 7.5 Part-11 - vGyan.in

Install and Set Up an Enrollment Server (vmware.com)

Configure user Group Policy Loopback processing mode (Noviembre 2022)

https://docs.vmware.com/en/VMware-Horizon-7/7.13/horizon-remote-desktop-features/GUID-E6DE1AAB-75A7-4C05-A97F-

DFEA499DB4FE.html#:~:text=In%20the%20Group%20Policy%20Management,the%20Mode%20drop%2Ddown%20menu

Requisitos previos – VMWARE (Noviembre 2022)

https://docs.vmware.com/en/VMware-Horizon/2106/horizon-installation/GUID-467F552F-3034-4917-A985-B5E5FEC5C68F.html

Requisitos puertos abiertos FW (Diciembre 2022)

https://kb.vmware.com/s/article/1027217?lang=es

Protocolo Blast (Diciembre 2022)

https://docs.vmware.com/es/VMware-Horizon-7/7.13/horizon-architecture-planning/GUID-F64BAD49-78A0-44FE-97EA-76A56FD022D6.html

DEM (Diciembre 2022)

Dynamic Environment Manager | Gestión de perfiles | VMware | ES

TRUE SSO (Diciembre 2022)

https://docs.vmware.com/es/VMware-Horizon-Cloud-Service/services/hzncloudmsazure.admin15/GUID-451AF252-931C-418C-BD7F-288AE170F5A4.html

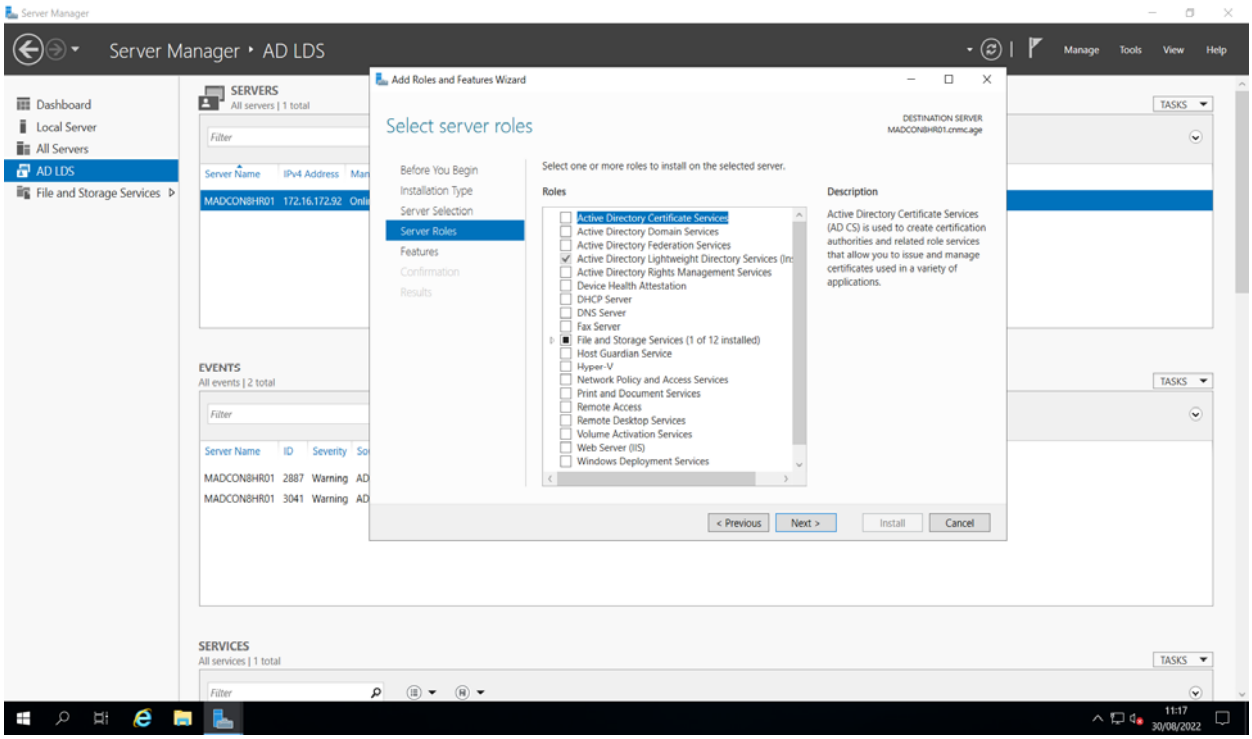
https://www.rocketstothemoon.net/integracion-uag-azure-true-sso/

19 Anexos

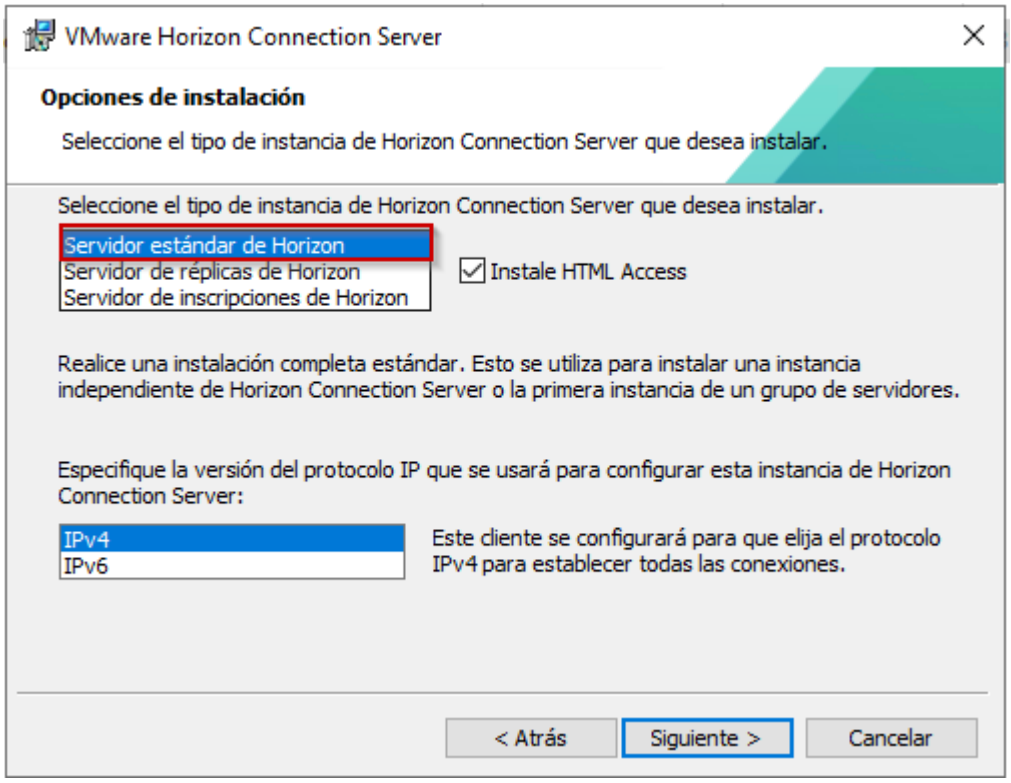
19.1 Anexo I. Instalación servidores CS

19.1.1 Instalación VDICS1

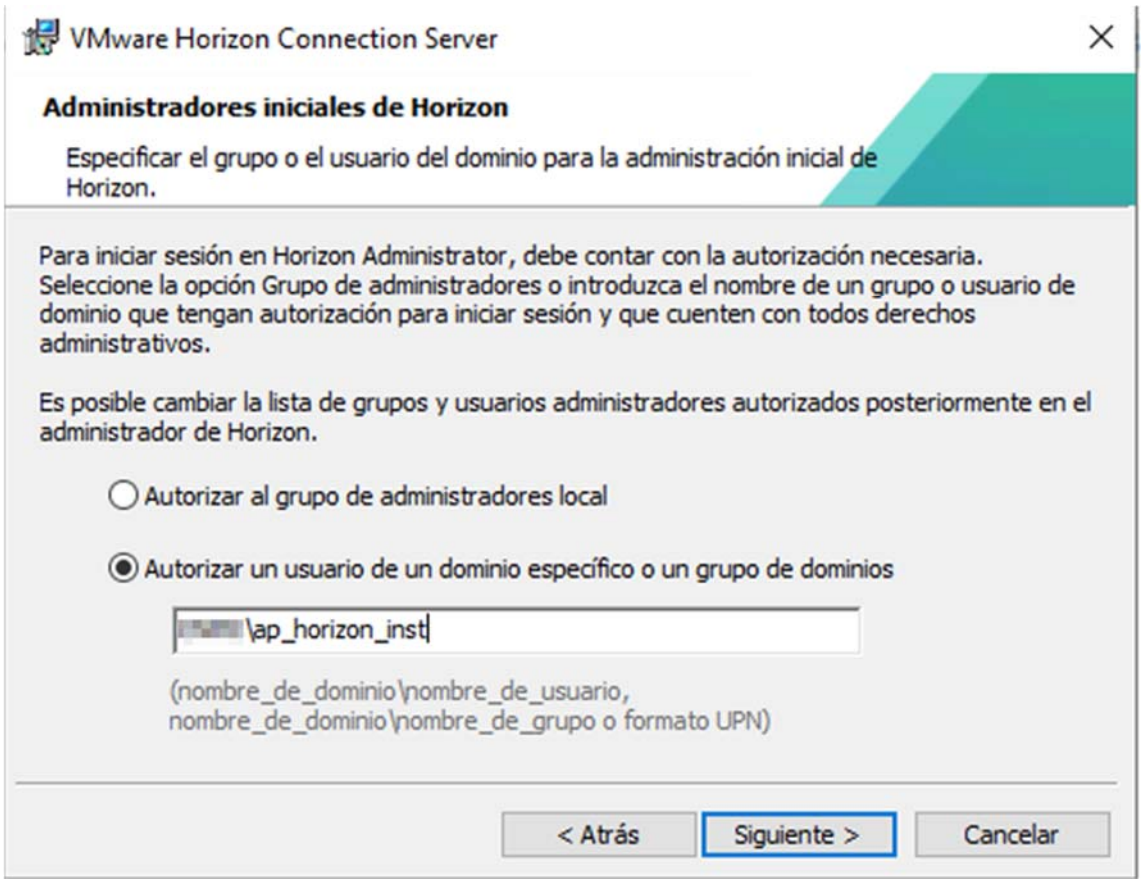
1. Agregar el usuario “AP_Horizon_Inst” como administrador local de ambos servidores
2. Instalar AD LDS y AD LDS Tools



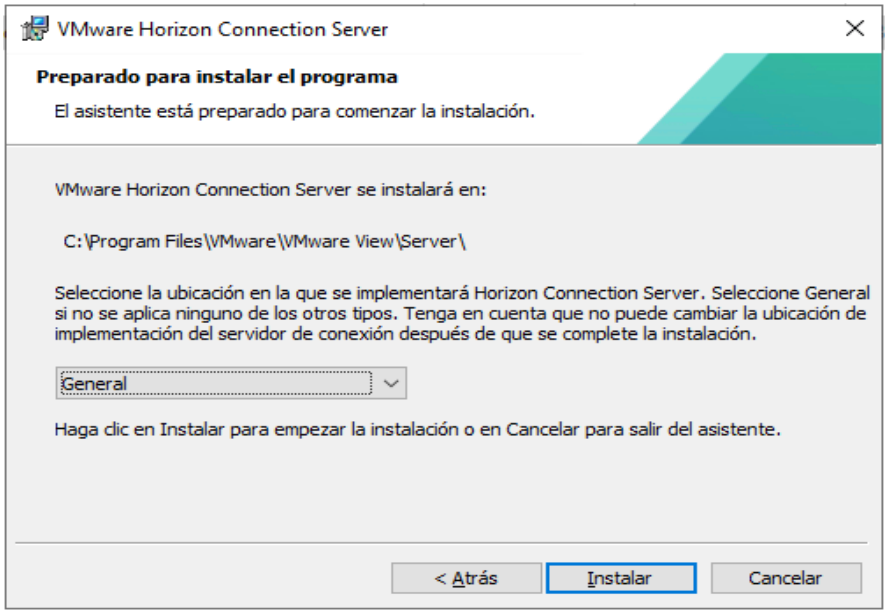
3. Ejecutar como administrador el ejecutable “VMware-Horizon-Connection-Server-x86_64-8.3.0-18294467.exe”
4. Seleccionar “Servidor estándar de Horizon”:



5. Introducir contraseña para proteger las copias de seguridad
6. Seleccionar “Configurar Firewall de Windows automáticamente”
7. Mantener el usuario “AP_Horizon_Inst” como usuario administrador de la consola de Horizon:



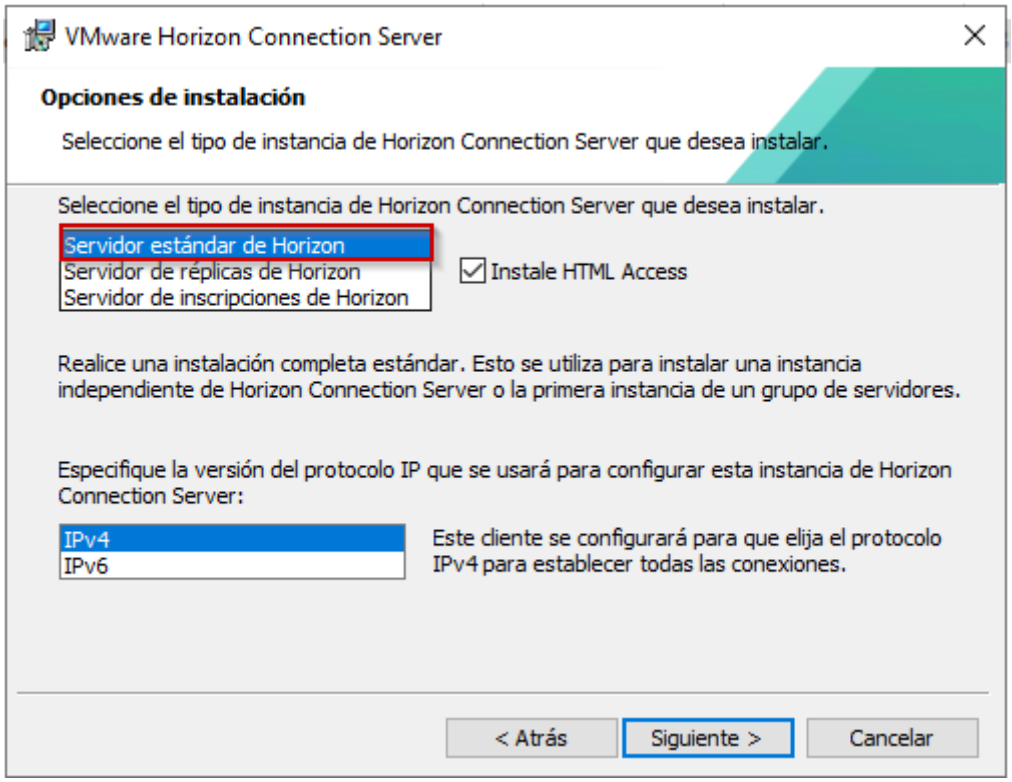
8. Dejar la opción “General” y seleccionar Instalar:



9. Seleccionar “Finalizar”

19.1.2 Instalación VDICS2

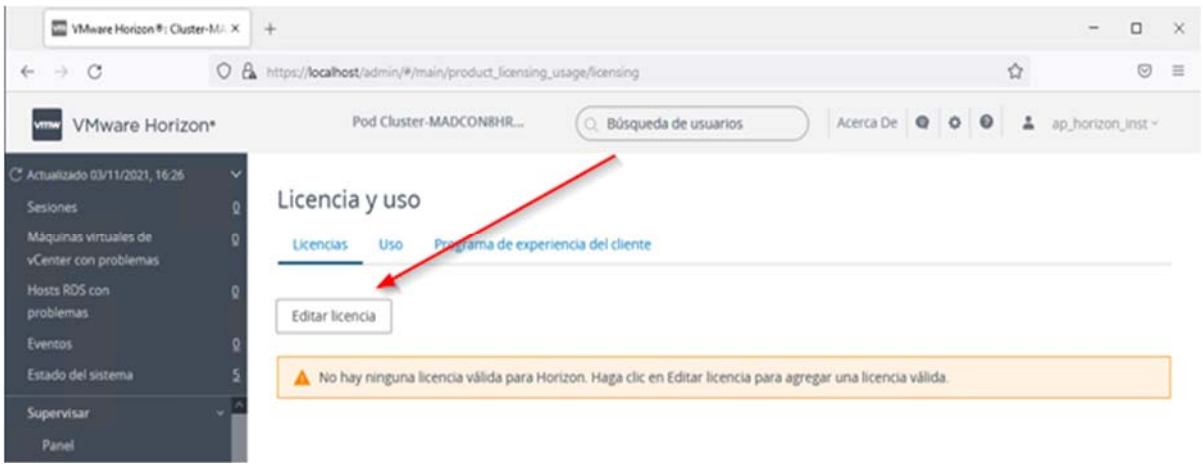
Para el despliegue del segundo connection server, se seguirán los pasos del punto anterior, cambiando la selección a “Servidor de réplicas de Horizon” dentro de “Opciones de instalación”:



19.1.3 Instalación de licencia

1. Acceder a la consola de Administración de Horizon, ubicado en el escritorio del servidor:

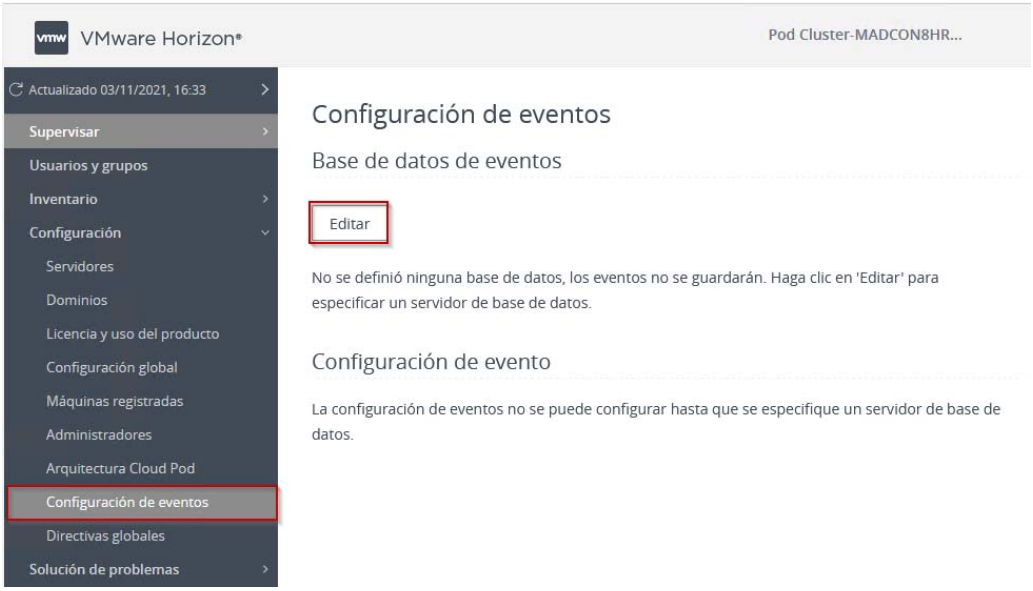
2. Acceder a la consola con el usuario “midominio\Ap_Horizon_Inst”
3. Una vez abierta la consola de administración, se muestra una alerta indicando que se ha de introducir una licencia
4. Seleccionar “Editar licencia” y añadir la clave de licencia



19.1.4 Configuración Base de datos de eventos

1. Acceder a la consola de Administración de Horizon, ubicado en el escritorio del servidor: 

2. Acceder a Configuración -> Configuración de eventos -> Base de datos de eventos -> Editar:



3. Completar los campos correspondientes a la nueva Base de Datos:
    a. Servidor de base de datos: **SQL1**
    b. Tipo de base de datos: **Microsoft SQL Server**

c. Puerto: **55935**

d. Nombre de la base de datos: **db_HorizonEvents**

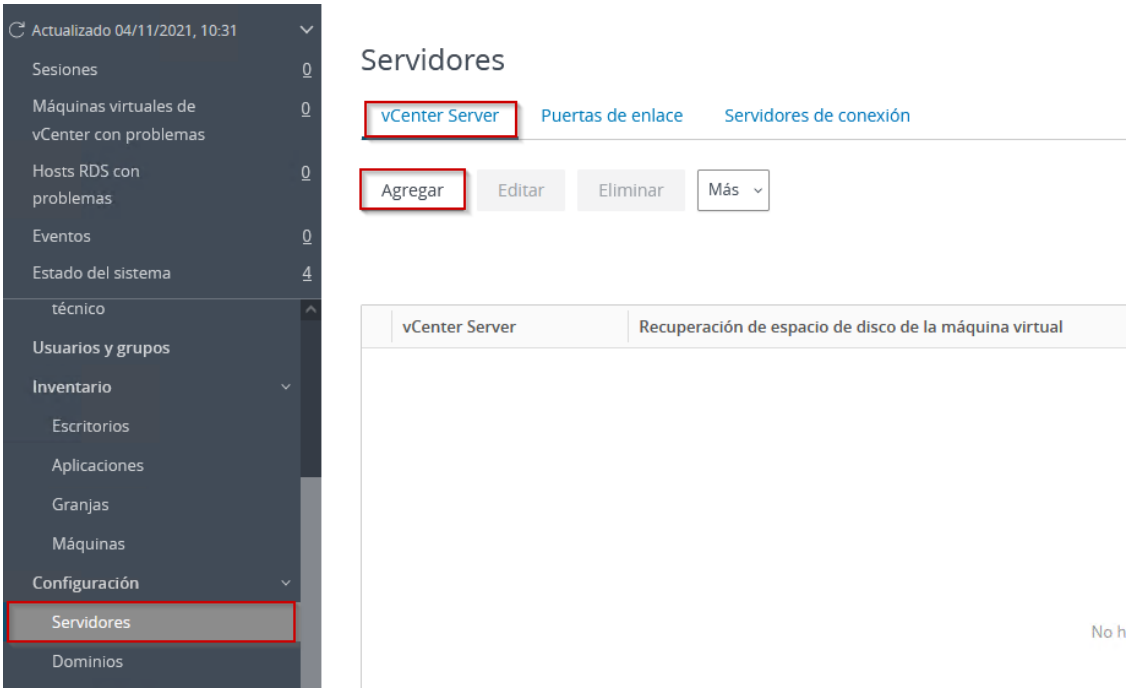
e. Nombre de usuario: **HorizonEvents_LoginOwner**

f. Contraseña: xxx

19.1.5 Agregar servidor vCenter

1. Acceder a la consola de Administración de Horizon, ubicado en el escritorio del servidor: 

2. Seleccionar Servidores -> vCenter Server -> Agregar



3. Informacion de vCenter. Completar los campos correspondientes al servidor:

a. Dirección del servidor: vcenter1

b. Nombre de usuario: cnmc\ap_horizon_ic

c. Contraseña: xxx

d. Puerto: 443

e. Tipo de implementación: General

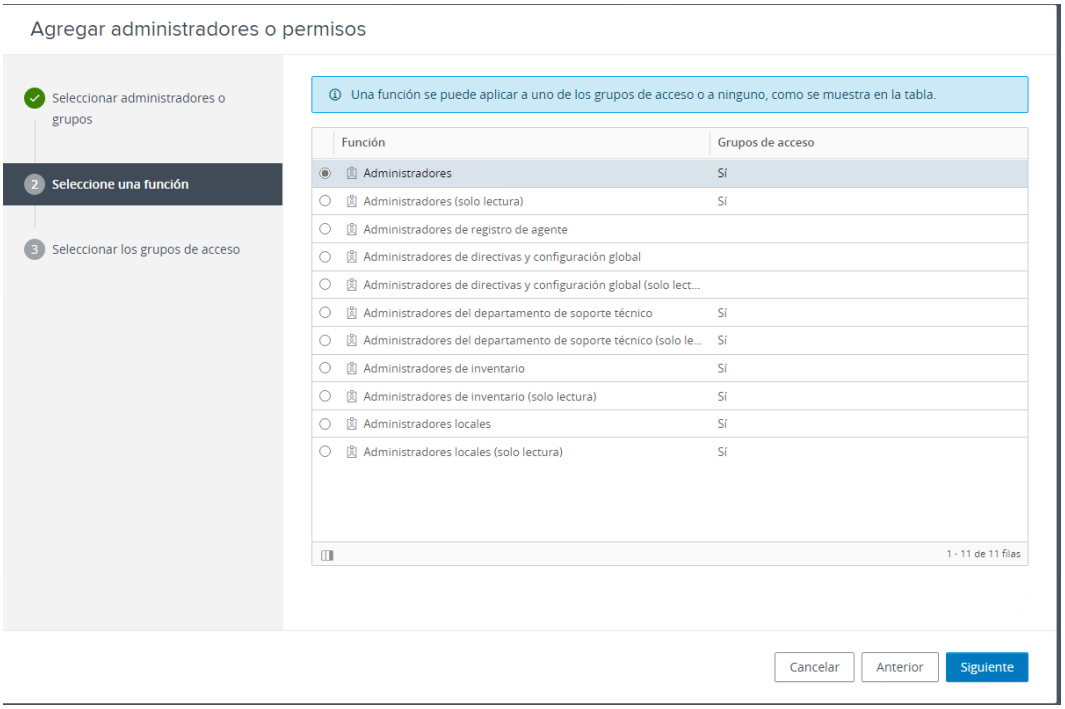
f. El resto, mantener valores por defecto

4. Almacenamiento. Desmarcar la opción “Reclamar espacio de disco de la máquina virtual”, ya que no es necesario en escritorios no persistentes
5. Click en “Enviar”

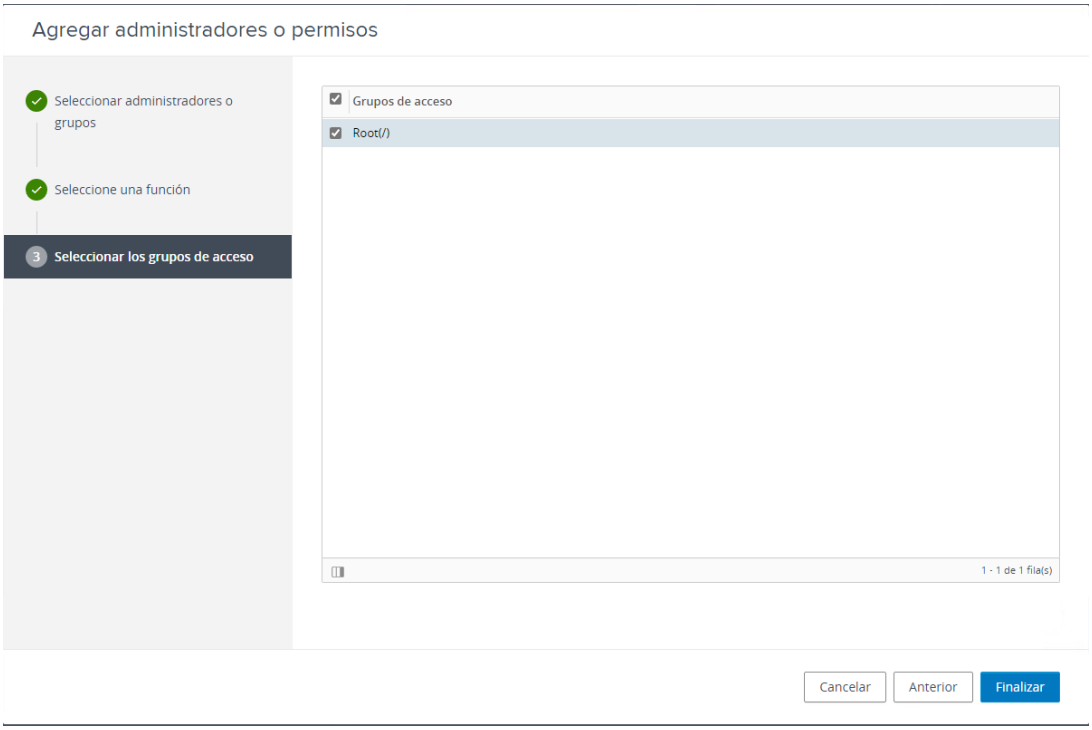
19.1.6 Configurar Administradores de Horizon

1. Acceder a la consola de Administración de Horizon, ubicado en el escritorio del servidor: 

2. Seleccionar Configuración -> Administradores -> Administradores y grupos -> Agregar
3. Agregar el grupo “Ap_Horizon_Administradores”
4. Seleccionar la función “Administradores”



5. Seleccionar el grupo de Acceso “Root (/)”

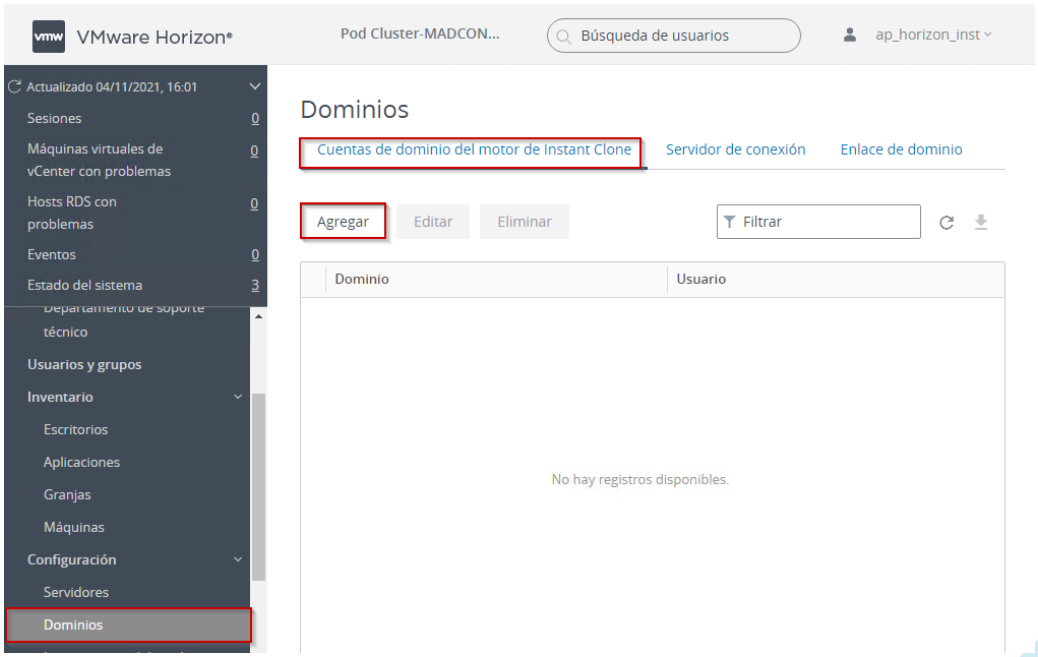


6. Finalizar

19.1.7 Cuentas de dominio para Instant Clones

1. Acceder a la consola de Administración de Horizon, ubicado en el escritorio del servidor: 

2. Seleccionar Dominios -> Cuentas de dominio del motor de Instant Clones -> Agregar

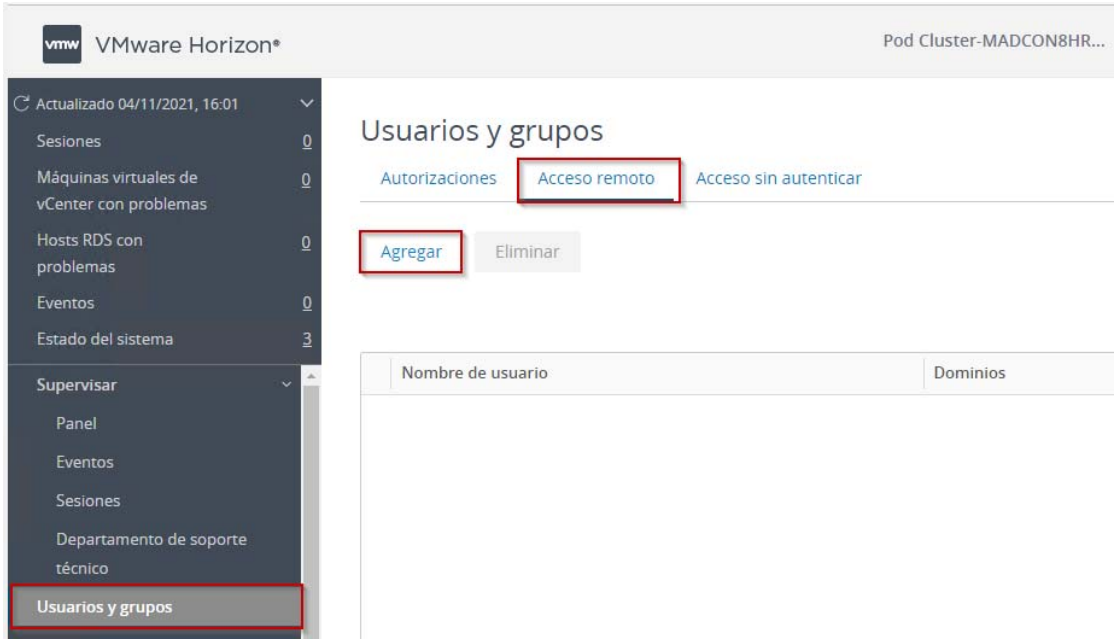


3. Agregar el usuario “Ap_Horizon_Ic”

19.1.8 Restringir acceso remoto a través del Connection Server

1. Acceder a la consola de Administración de Horizon, ubicado en el escritorio del servidor: 

2. Seleccionar Usuarios y grupos -> Acceso remoto -> Agregar -> Seleccionar servidor “VDICS1” -> Editar



3. Seleccionar el dominio “midominio.local” y añadir el grupo “Ap_Horizon_Usuarios”

19.1.9 Deshabilitar túnel seguro (Secure Tunnel)

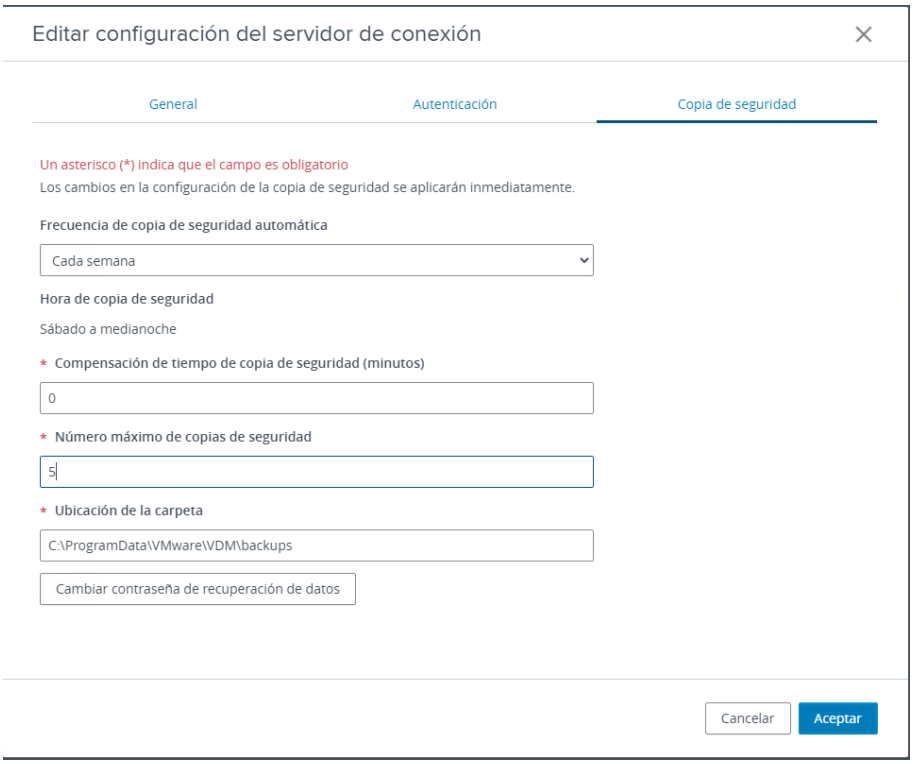
1. Acceder a la consola de Administración de Horizon, ubicado en el escritorio del servidor: 

2. Seleccionar Configuración -> Servidores -> Servidores de conexión -> Seleccionar servidor “VDICS1” -> Editar
3. Seleccionar las siguientes opciones:
    a. Usar conexión de túnel seguro con máquina -> Desmarcado
    b. Puerta de enlace segura PCoIP -> Desmarcado
    c. Puerta de enlace de Blast -> Seleccionar “Usar la puerta de enlace segura de Blast solo en las conexiones HTML de la máquina

19.1.10 Copia de seguridad del servidor Connection Server

1. Acceder a la consola de Administración de Horizon, ubicado en el escritorio del servidor: 

2. Seleccionar Configuración -> Servidores de conexión -> Servidor “VDICS1” -> Editar
3. Configurar la programación de los backups y el período de retención, rellenando los siguientes campos:
    a. Frecuencia de copia de seguridad automática
    b. Número máximo de copias de seguridad
    c. Ubicación de la carpeta



19.1.11 Sustitución certificados SSL

Para realizar el cambio, es importante seguir las siguientes instrucciones, en cada uno de los CS:

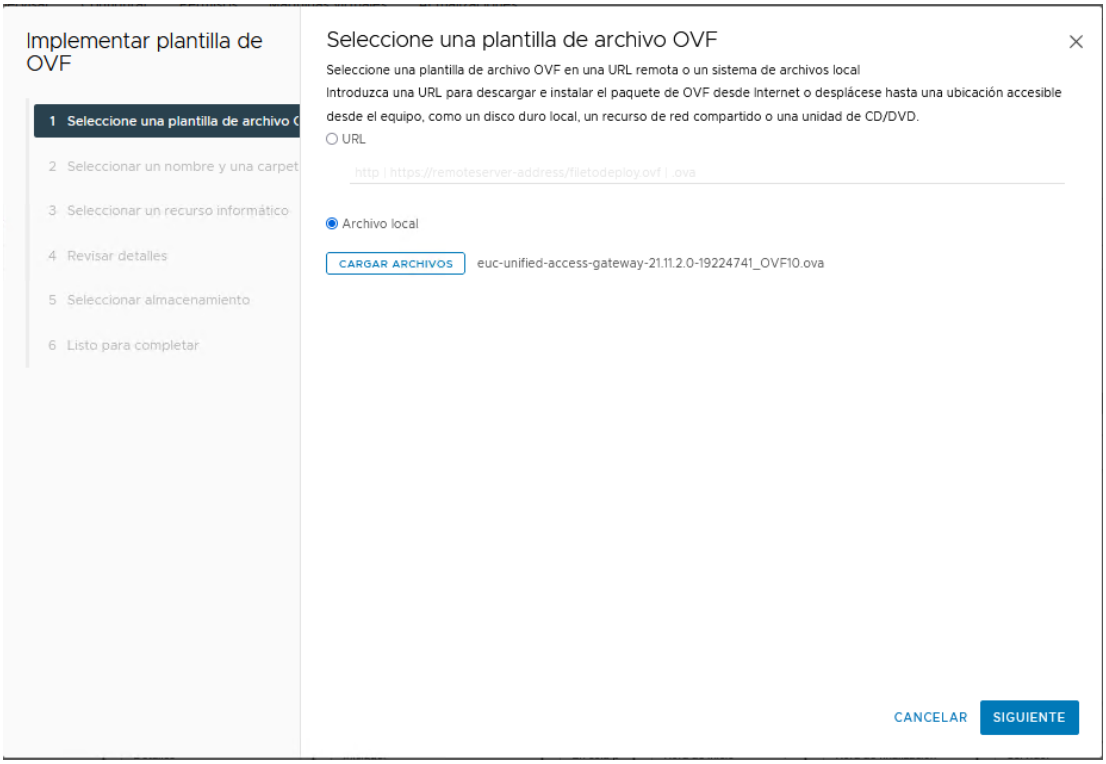
1. Instalar el certificado en los 2 CS
2. Desde la consola de gestión de certificados, ir al contenedor “Personal”
3. Abrir las propiedades del certificado que queremos sustituir (autofirmado) y modificar el campo “Friendly name” por “vdm_old”
4. Abrir las propiedades de nuestro certificado y en el campo “Friendly name” introducir “vdm”
5. Reiniciar el servicio “Componentes de puerta de enlace de seguridad de MVware Horizon View”

19.2 Anexo II. Instalación Servidores UAG

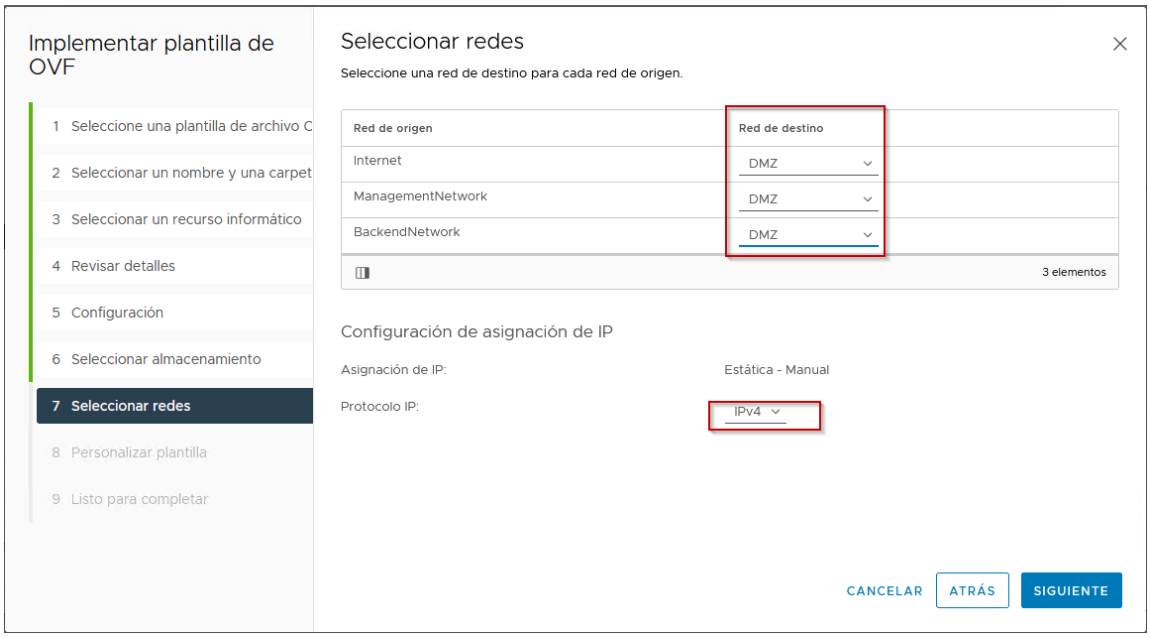
19.2.1 Despliegue de VDIUAG1

1. Descargar la OVA desde: vmware - descarga UAG
2. Dentro de nuestro vCenter, posicionarse en la vista de “Máquinas virtuales y plantillas”

3. Por organización, crear una carpeta llamada “UAG”
4. Clic derecho sobre la carpeta “UAG” y seleccionar “Implementar plantilla de OVF”
5. Cargar el archivo .ova descargado anteriormente



6. Asignar el nombre “VDIUAG1” y seleccionar la carpeta “UAG” creada anteriormente
7. Seleccionar un ESX para que corra la nueva máquina
8. Seleccionar “Single NIC”
9. Seleccionar el almacenamiento en el que se ubicará la máquina virtual
10. Asignar la red de “DMZ” en las 3 redes solicitadas por la plantilla, y el protocolo IPv4



11. En la personalización de la plantilla, configurar los siguientes parámetros:
    a. IPMode for Nic 1 (eth0): STATICV4
    b. NIC 1 (eth0) IPv4 address: 172.31.0.37
    c. DNS server addresses: 172.16.172.90 172.16.172.121
    d. DNS Search Domain: midominio.local
    e. NIC 1 (eth0) IPv4 netmask: 255.255.252.0
    f. IP Default Gateway: 172.31.0.20
    g. Unified Gateway Appliance Name: VDIUAG1
    h. Join the VMware Customer Experience Improvement Program: Desmarcado
    i. Password for the root user of this VM: xxx
    j. Establecer tiempo de expiración de la password
    k. Password for the adin user, which enables REST API access: xxx
    l. System Properties. Enable SSH : Marcado

19.2.2 Despliegue de VDIUAG2

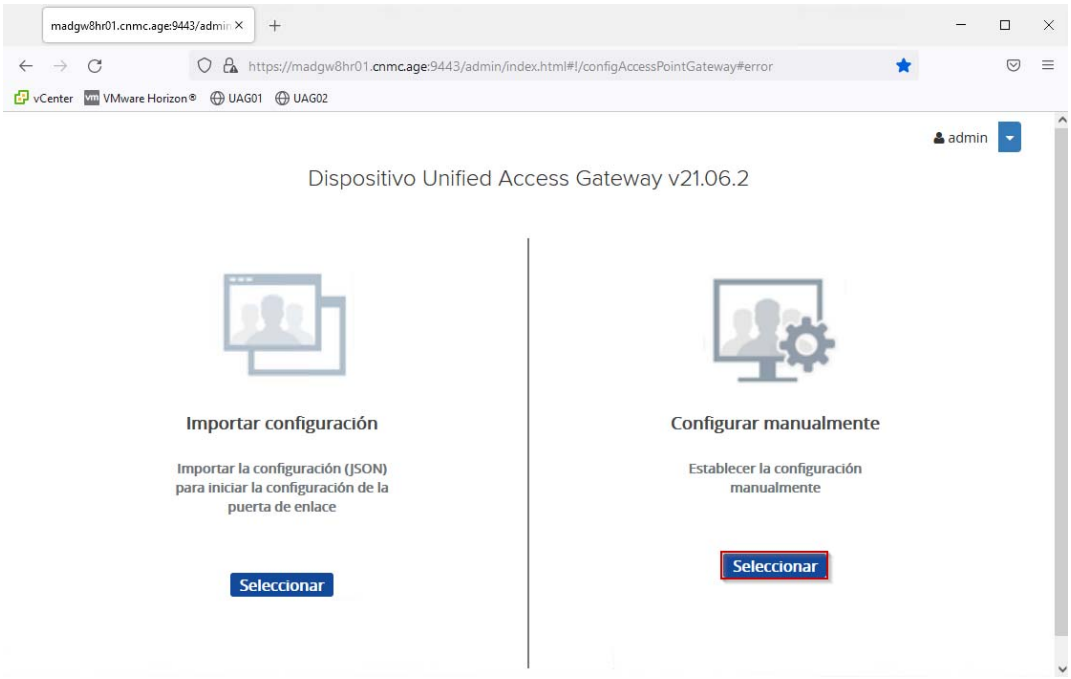
Para el despliegue del segundo UAG, se seguirán los pasos del punto anterior, cambiando los siguientes parámetros:

1. Asignar nombre “VDIUAG2”
2. En la personalización de la plantilla:

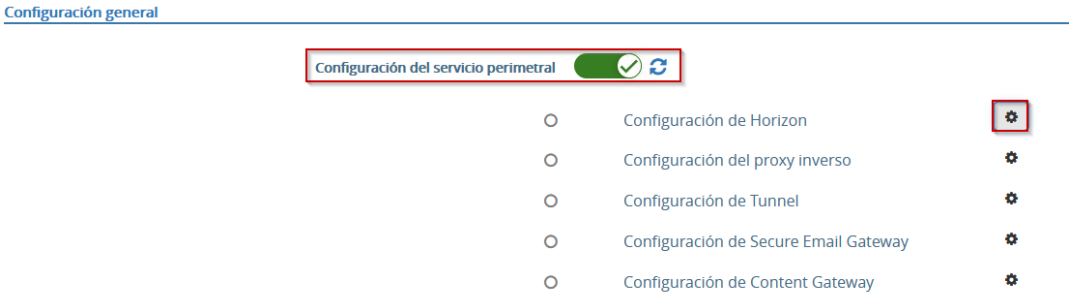
a. NIC 1 (eth0) IPv4 address: 172.31.0.38
b. Unified Gateway Appliance Name: VDIUAG2

19.2.3 Integración de UAG con Horizon

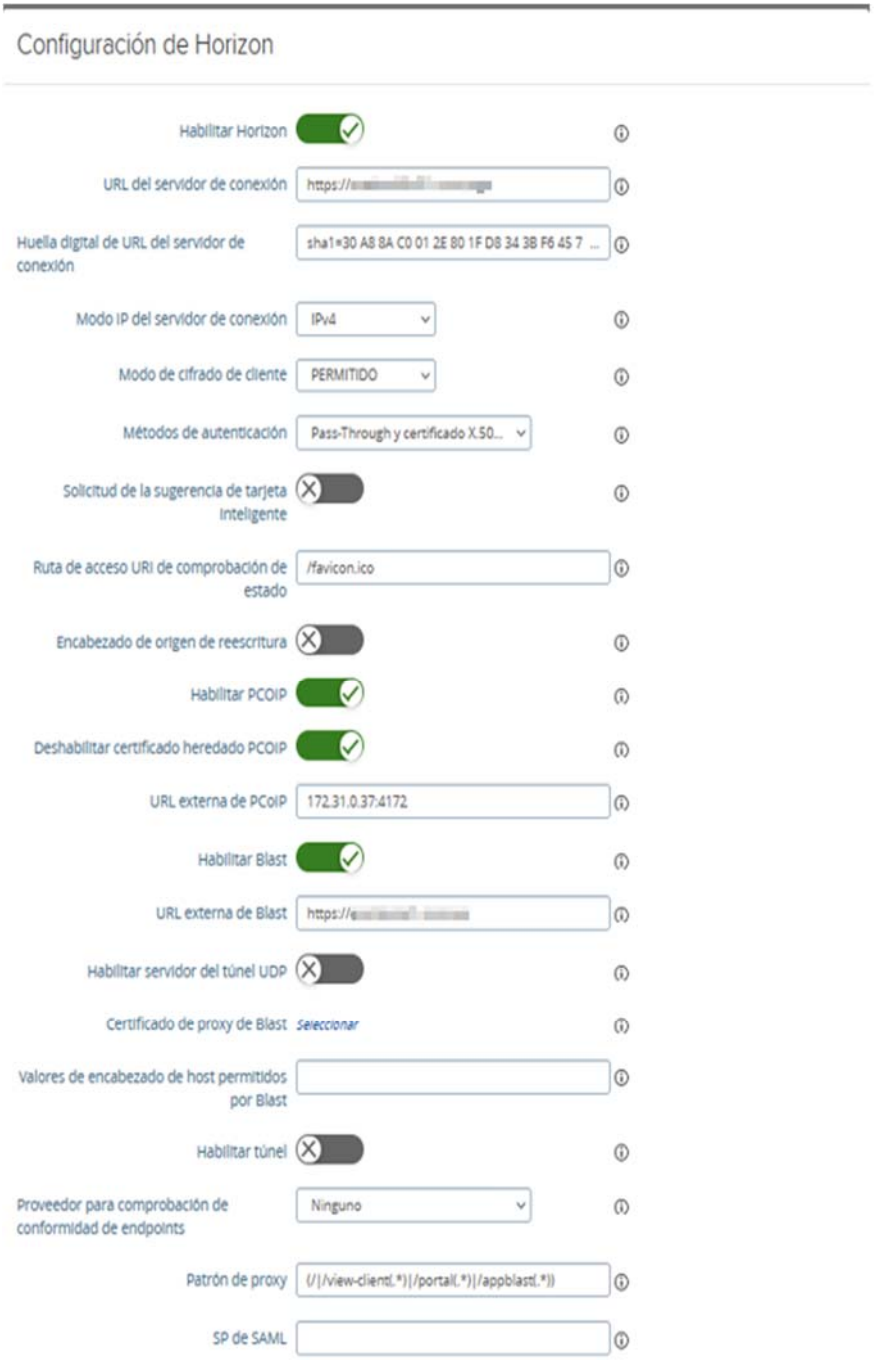
1. En la zona DNS “midominio.local”, añadir el registro de Tipo “A”:
   a. VDIUAG1 – 172.31.0.37
   b. VDIUAG2 – 172.31.0.38
2. Conectarse al UAG desde un Connection server: https://vdiuag1.midominio.local:9443/admin, con las credenciales de “admin”
3. Seleccionar configurar manualmente

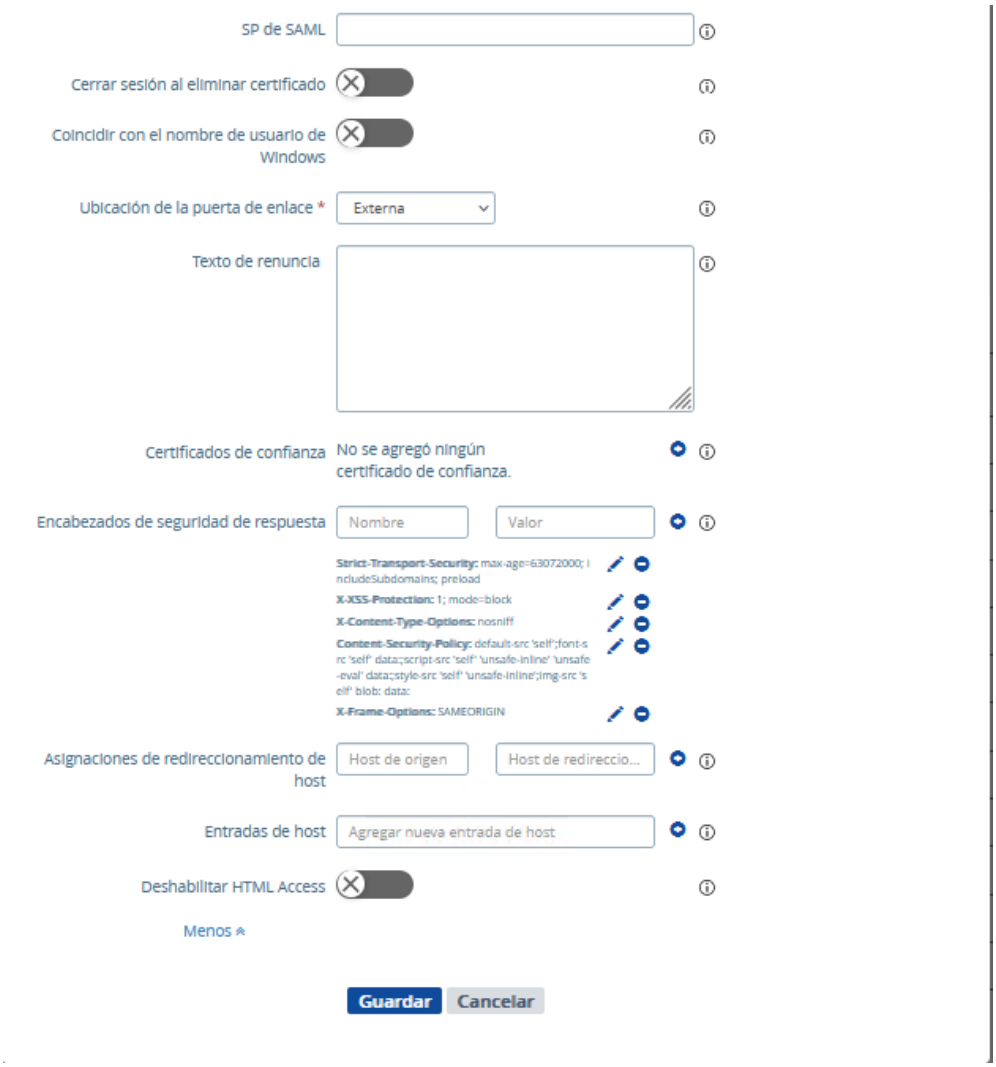


4. Seleccionar Configuración del servicio perimetral (habilitar) -> Configuración de Horizon



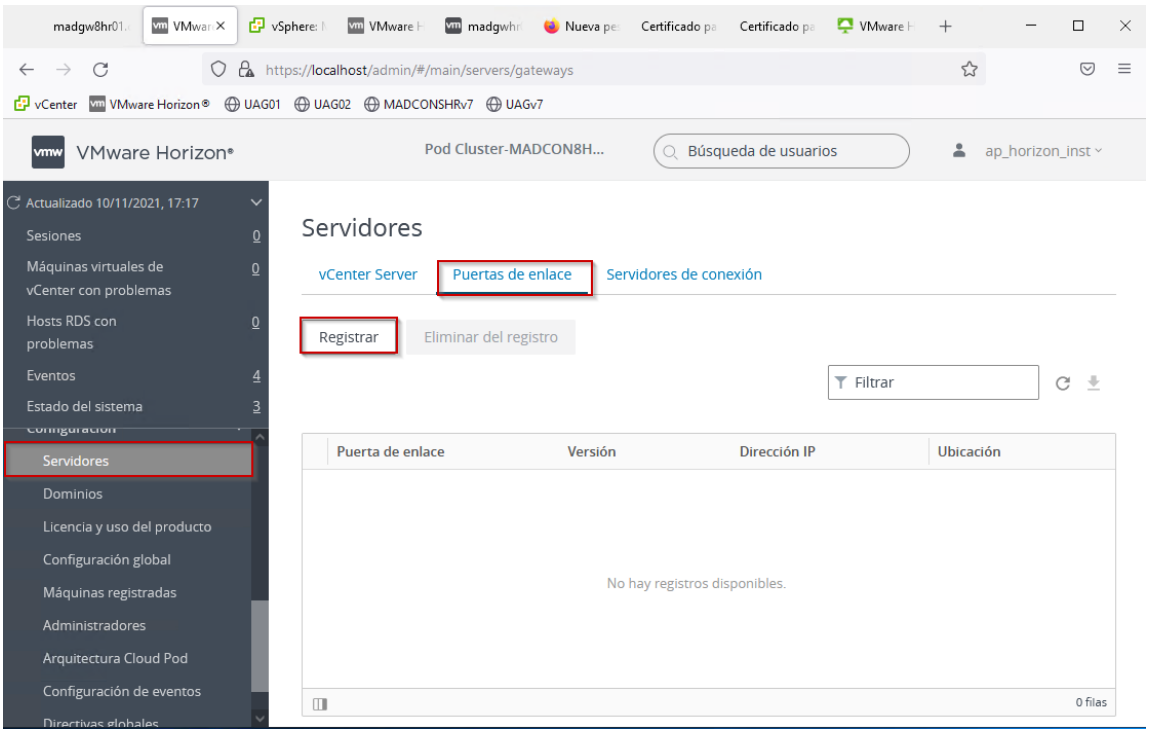
5. Configurar los siguientes parámetros:


Configuración de Horizon
Habilitar Horizon
URL del servidor de conexión
https://
Huella digital de URL del servidor de conexión
sha1=30 A8 8A C0 01 2E 80 1F D8 34 3B F6 45 7 ...
Modo IP del servidor de conexión
IPv4
Modo de cifrado de cliente
PERMITIDO
Métodos de autenticación
Pass-Through y certificado X.50...
Solicitud de la sugerencia de tarjeta inteligente
Ruta de acceso URI de comprobación de estado
/favicon.ico
Encabezado de origen de reescritura
Habilitar PCOIP
Deshabilitar certificado heredado PCOIP
URL externa de PCoIP
172.31.0.37:4172
Habilitar Blast
URL externa de Blast
https://
Habilitar servidor del túnel UDP
Certificado de proxy de Blast
Seleccionar
Valores de encabezado de host permitidos por Blast
Habilitar túnel
Proveedor para comprobación de conformidad de endpoints
Ninguno
Patrón de proxy
(/|/view-client(.*)|/portal(.*)|/appblast(.*))
SP de SAML



19.2.4 Agregar servidores UAG en la consola Horizon

1. Abrir la consola de administración de Horizon desde https://vdics1.midominio.local/admin
2. Seleccionar Configuración -> Servidores -> Puertas de enlace -> Registrar

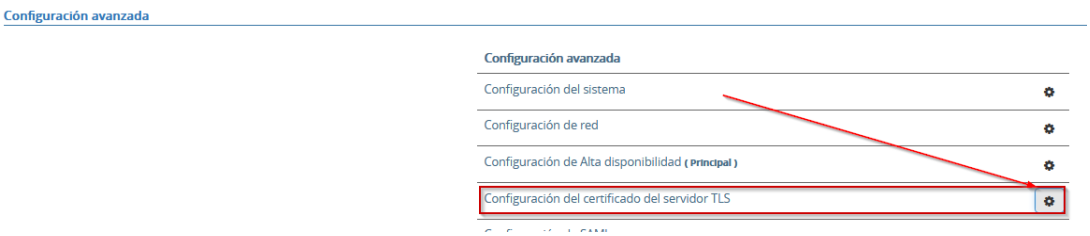


3. Añadir el servidor UAG “VDIUAG1”

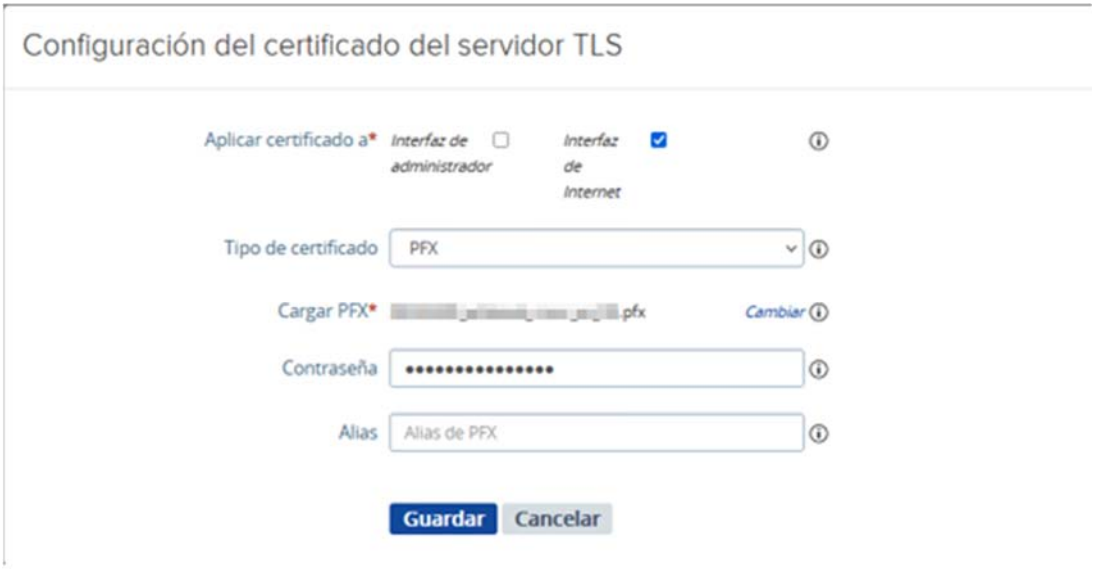
19.2.5 Configuración certificado TLS

Como se ha explicado anteriormente, el servidor al que se conectarán los clientes desde Internet, ha de tener un certificado que no muestre un error porque la página no es segura. Para ello, se instala el wildcard “*.midominio.es” en ambos UAG.

1. Conectarse al UAG: https://vdiuag1.midominio.local:9443/admin, con las credenciales de “admin”
2. Seleccionar “Configuración del certificado del servicio TLS”



3. Seleccionar “Interfaz de Internet” y el certificado wildcard, e introducir su password



19.2.6 Configuración UAG en HA

Como hemos visto anteriormente, en Horizon se pueden configurar nuestros servidores UAG en alta disponibilidad. De este modo, los usuarios podrán seguir accediendo a sus máquinas, aunque uno de nuestro UAG no se encontrase disponible, ya sea por algún problema o por tareas de mantenimiento.

Para conseguir este HA, se ha de realizar la siguiente configuración en ambos servidores:

1. Conectarse a uno de los UAG a través de la URL https://vdiuag1.midominio.local:9443
2. Seleccionar configuración manual
3. Seleccionar Configuración de alta disponibilidad (Sin Configurar)
4. Desplegar “Modo”
5. Introducir los campos
    a. IP Virtual: 172.31.0.39
    b. ID de grupo: 10 (Este número ha de ser un valor entre 1 y 255)
6. El estado de “Seleccionar Configuración de alta disponibilidad” pasará a “Procesando”
7. Una vez realizados los pasos anteriores, el modo cambiará a “Copia de seguridad”

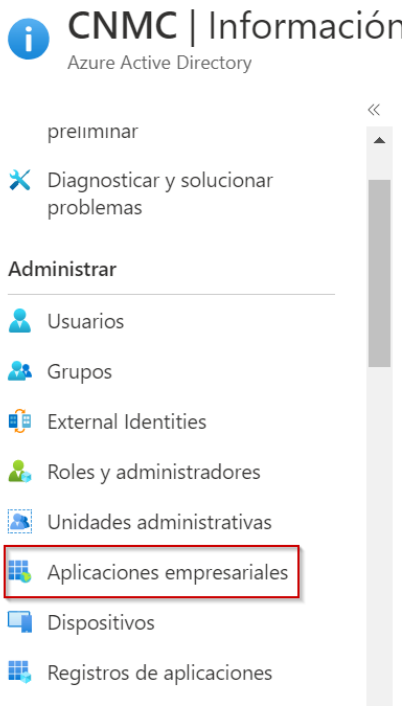
19.3 Anexo III. Configuración MFA

19.3.1 Configuración SAML en Azure AD

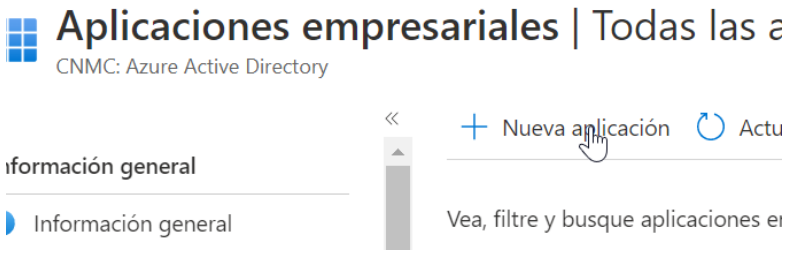
Para la configuración de SAML usando Azure, seguiremos los pasos detallados a continuación:

1. Acceder a https://azure.microsoft.com con usuario administrador y seleccionar "Active Directory"

2. Seleccionar "Aplicaciones empresariales"

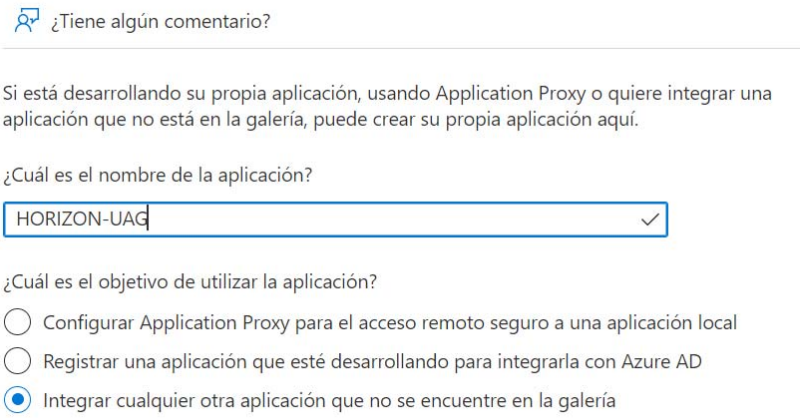


3. Seleccionar "Nueva aplicación":

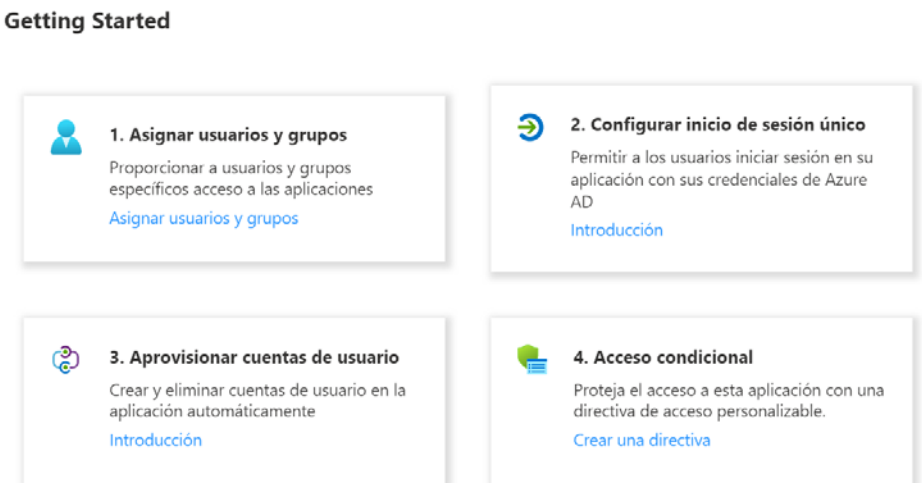


4. Seleccionar “Crear su propia aplicación”:

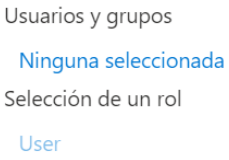
5. Introducir el nombre de la aplicación:



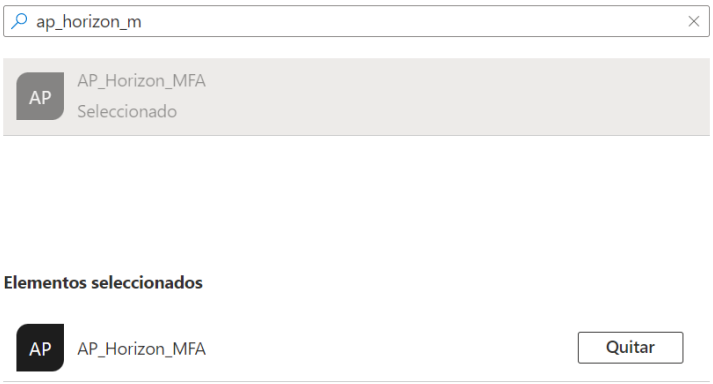
6. Seleccionar “1. Asignar usuarios y grupos”:



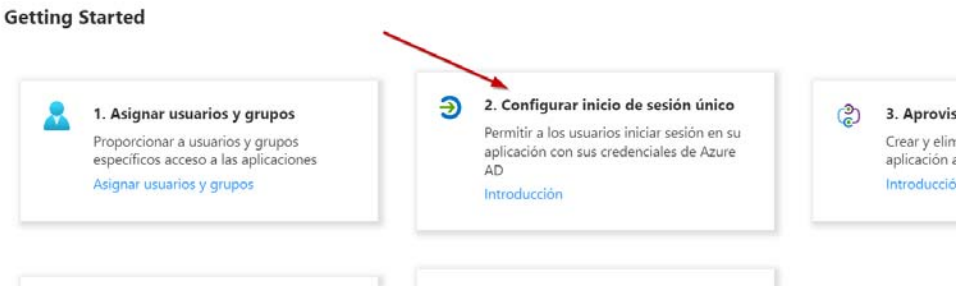
7. Hacer clic en “Ninguna seleccionada”:



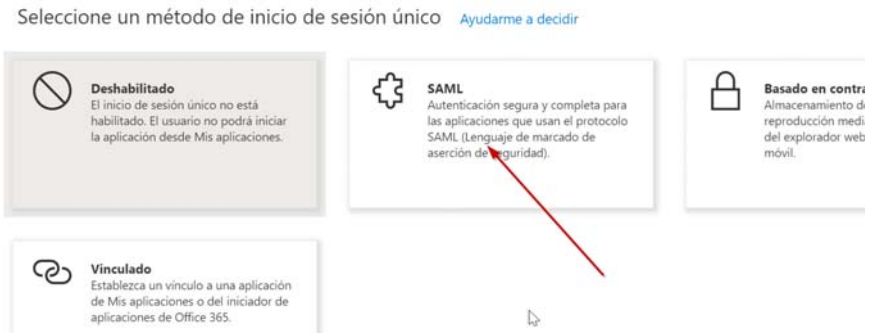
8. Seleccionar “Ap_Horizon_MFA”:



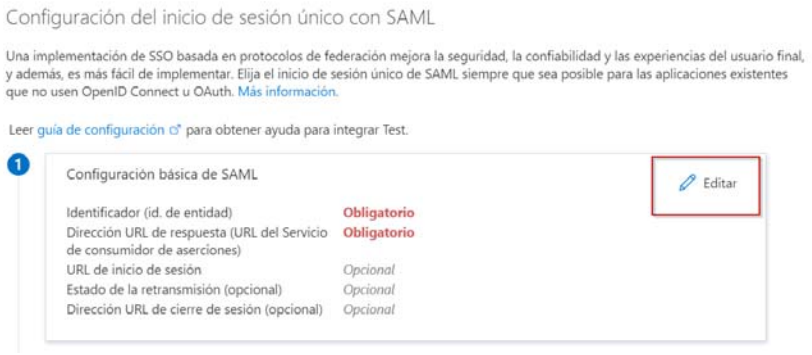
9. Volver a la aplicación “HORIZON-UAG” y clic en “2. Configurar inicio de sesión único”:



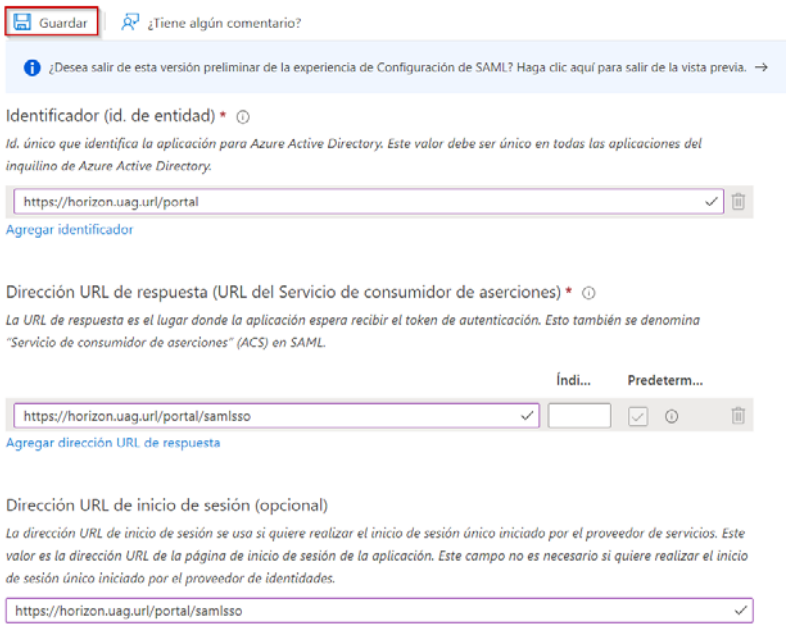
10. Hacer clic en “SAML”:



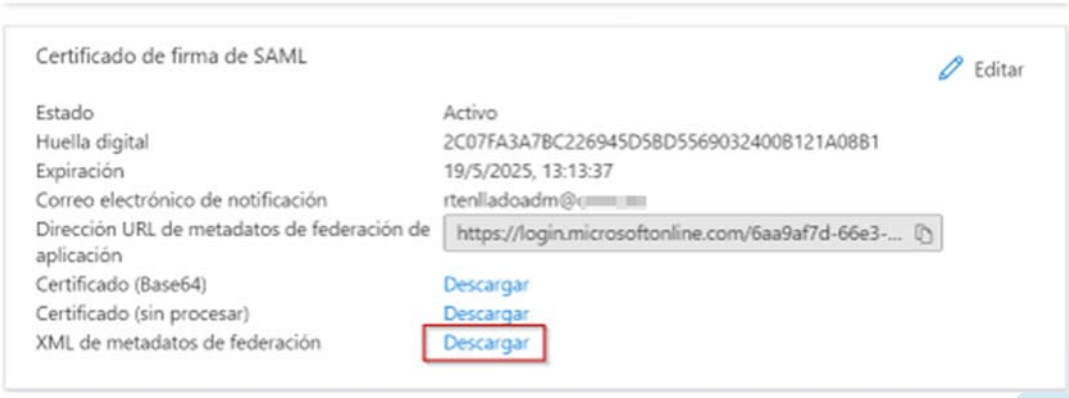
11. Hacer clic en “Configuración básica de SAML – Editar”:



12. Agregar y guardar:
    a. Identificador: https://vdi.midominio.es/portal
    b. Dirección URL de respuesta URL: https://vdi.midominio.es/portal/samlsso
    c. Dirección URL de inicio de sesión: https://vdi.midominio.es/portal/samlsso



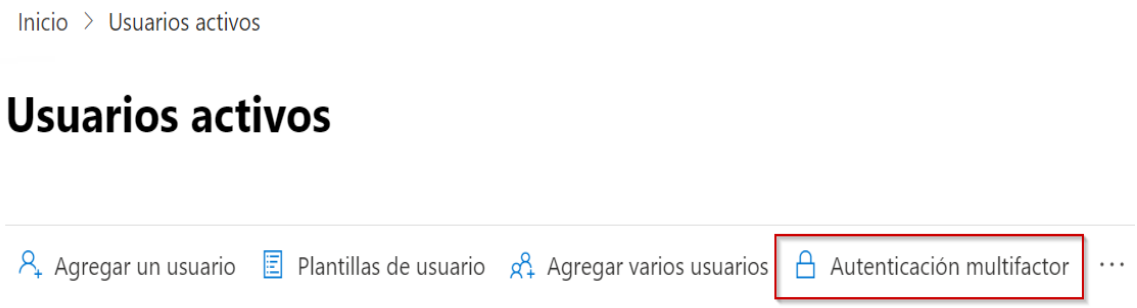
13. Descargar "XML de metadatos de federación":



19.3.2 Configuración MFA Usuarios

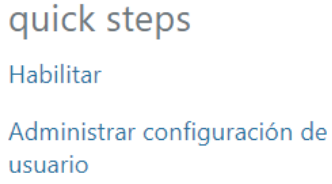
Una vez realizada la configuración anterior, a los miembros del grupo "Ap_Horizon_MFA" hay que configurarles MFA. Para ello:

1. Abrir https://admin.microsoft.com
2. Usuarios -> Usuarios activos -> Autenticación multifactor



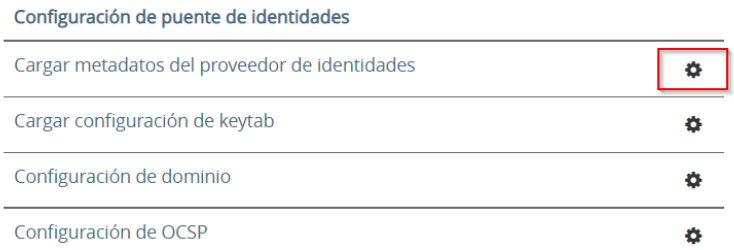
3. Clic en icono de la lupa e introducir el usuario

4. Seleccionar usuario y clic en "Habilitar"

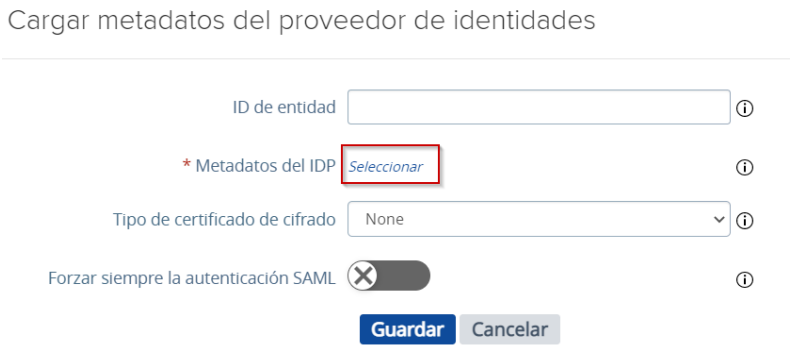


19.3.3 Configuración MFA en UAG

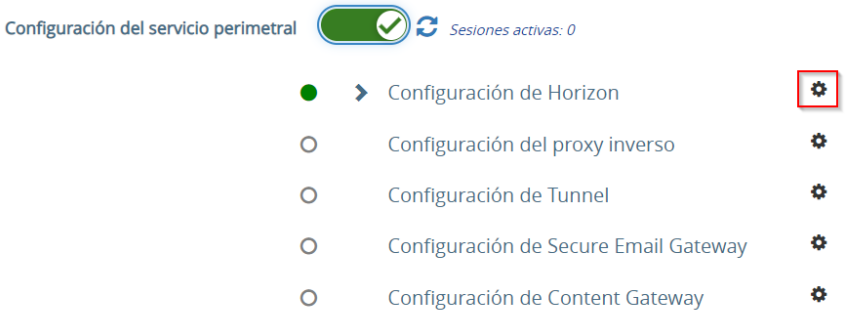
1. Acceder al portal de administración del UAG: https://vdiuag1.midominio.local:9443/admin, con las credenciales de "admin"
2. Clic en Configuración de puente de identidades -> Cargar metadatos del proveedor de identidades



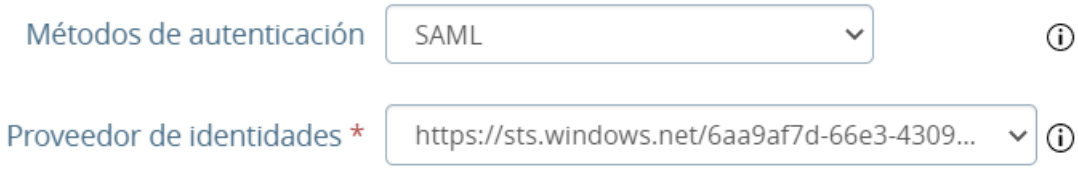
3. Metadatos del IDP -> Seleccionar



4. Cargar el archivo XML "XML de metadatos de federación", descargado anteriormente de Azure y guardar
5. Configuración de servicio perimetral -> Configuración de Horizon



6. Habilitar el método de autenticación SAML



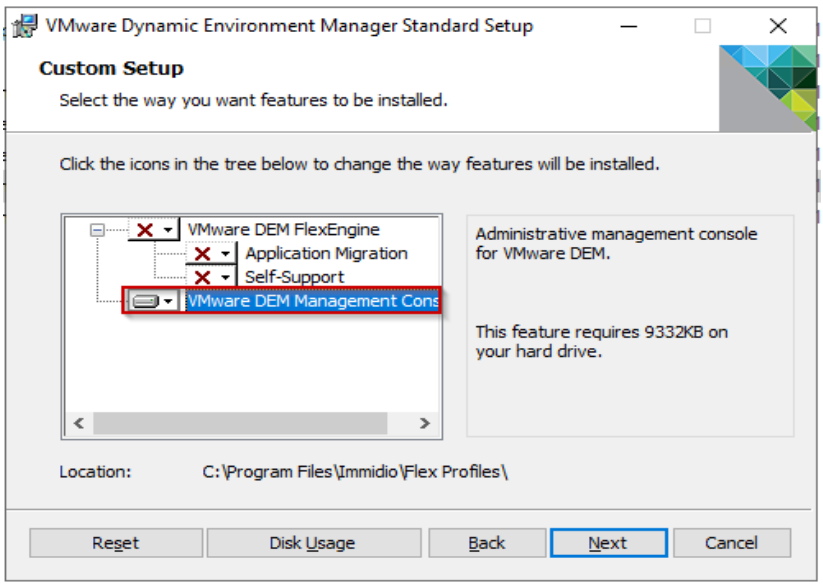
7. Guardar la configuración

19.4 Anexo IV. Instalación y configuración de DEM

Para este fin, se han creado las carpetas compartidas "\\ficheros.midominio.local\DEMConfig$" y "\\ficheros.midominio.local\DEMPerfiles$", explicadas en el apartado "Recursos compartidos".

19.4.1 Instalación consola administración DEM

1. Conectarse al servidor VDICS1, con el rol de connection server y descargar el archivo de instalación
2. Ejecutar el archivo "VMware Dynamic Environment Manager Standard 2106 10.3.msi" descargado
3. En "Choose Setup Type", seleccionar "Custom"
4. Deseleccionar la opción "VMware DEM FlexEngine" y seleccionar "VMware DEM Management Console" y hacer clic en "Next"

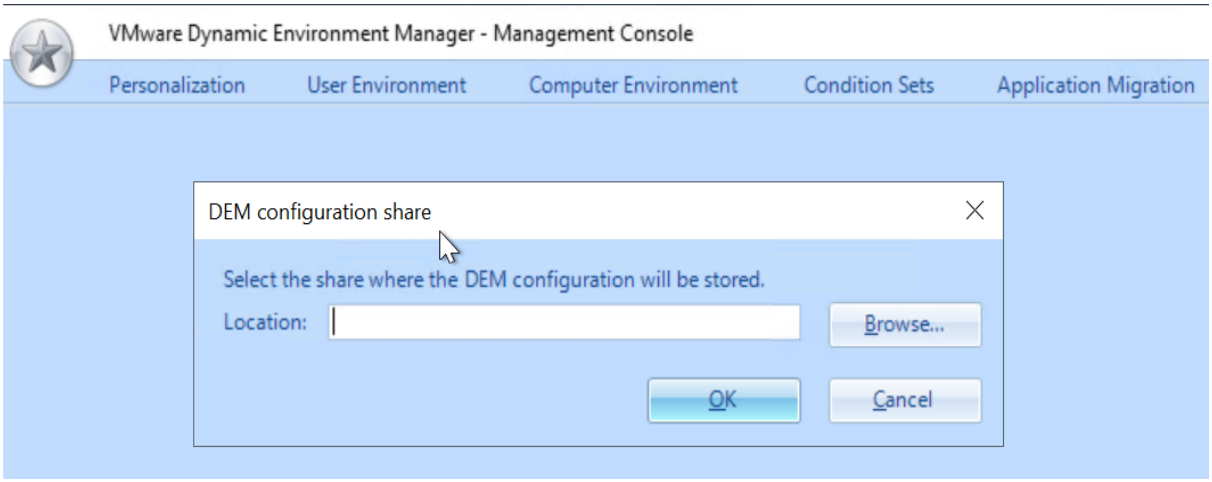


5. Finalizar la instalación

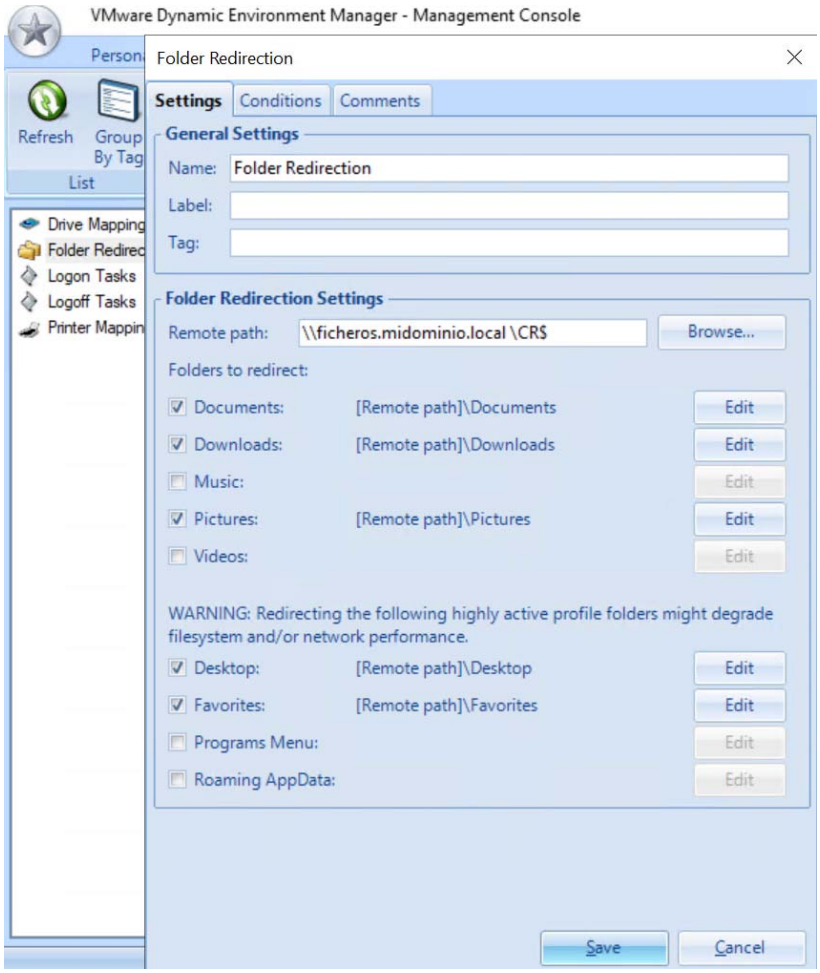
19.4.2 Configuración DEM

1. Conectarse al servidor VDICS1 y abrir la aplicación “Management Console” de DEM

2. Al abrir la consola, introducir la carpeta compartida donde se almacenarán los ficheros de configuración de DEM (\\ficheros.midominio.local\DEMConfig$) y seleccionar OK

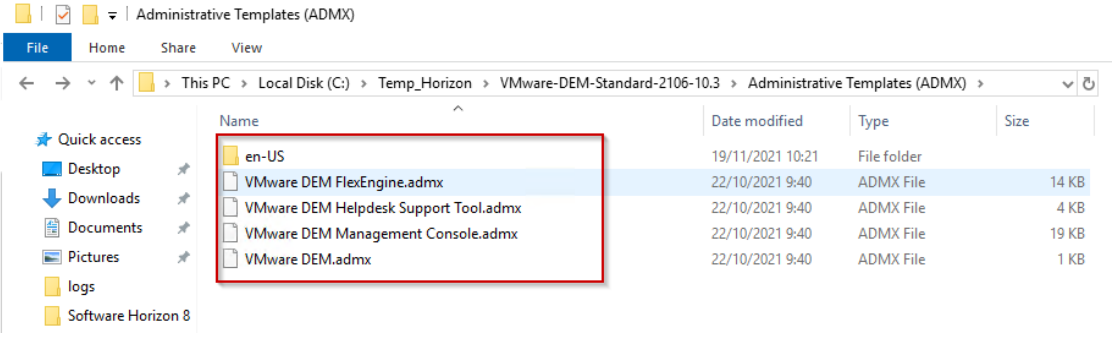


3. User Environment -> Folder Redirection -> Create
4. Marcar las opciones según se muestran en la siguiente captura:



19.4.3 Política de grupo (GPO)

1. Agregar plantillas administrativas de DEM en el Controlador de Dominio



2. Se crea la GPO "GPO Usuarios - DEM Horizon 8" en la OU "OU=VDI,DC=midominio,DC=local". Esta GPO tiene las siguientes configuraciones:

   2.1. Política: Configuración del usuario -> Directivas -> Plantillas Administrativas -> VMware DEM -> Flex Engine -> "DirectFlex - advanced settings"

      2.1.1. Only export at logoff - Deshabilitado

2.1.2. Show DirectFlex notifications - Habilitado

2.1.3. Notification delay in seconds - 5

2.1.4. Hide DirectFlex exit notification - Deshabilitado

2.2. Configuración del usuario -> Directivas -> Plantillas Administrativas -> VMware DEM -> Flex Engine -> "FlexEngine config files"

2.2.1. Central location of Flex config files: \\ficheros.midominio.local\DEMConfig$\General

2.2.2. Process folder recursively: Habilitado

2.3. Configuración del usuario -> Directivas -> Plantillas Administrativas -> VMware DEM -> Flex Engine -> FlexEngine logging

2.3.1. Path and file name of log file: \\ficheros.midominio.local\DEMfiles$\%username%\Logs\Flexengine.log

2.3.2. Log level: Error

2.3.3. Maximum log file size in kB: 1024

2.3.4. Log Total size of profile archive and profile archive backup folders: Deshabilitado

2.4. Configuración del usuario -> Directivas -> Plantillas Administrativas -> VMware DEM -> Flex Engine -> FlexEngine logging to the Windows event log

2.4.1. Configure additional logging:

2.4.2. Asynchronous user environment actions: Deshabilitado

2.4.3. DirectFlex refresh: Deshabilitado

2.4.4. Warm about profile archive sizes:

2.4.4.1. Warm if size of single profile archive exceedes this size in KB : 2048

2.4.4.2. Warm if total size of profile archive folder exceeds this size in KB: 2048

2.4.4.3. Include profile archive backup folder when determining folder size

2.5. Configuración del usuario -> Directivas -> Plantillas Administrativas -> VMware DEM -> Flex Engine -> Paths unavailable at logon

2.5.1. It Flex config files path is not available: Logoff

2.5.2. Optional message to display: WARNING - Path not available

2.5.3. Timeout after which to dismiss message: 10

2.5.4. If profile archive path is not available: Aplly user environment settings

2.6. Configuración del usuario -> Directivas -> Plantillas Administrativas -> VMware DEM -> Flex Engine -> Prevent access to VMware DEM Self-Suport -> Habilitado

2.7. Configuración del usuario -> Directivas -> Plantillas Administrativas -> VMware DEM -> Flex Engine -> Profile archive backups

2.7.1. Location for storing user profile archive backups: \\ficheros.midominio.local\demperfiles$\%username%\Backups

2.7.2. Hide backup folder: Deshabilitado

2.7.3. Number of backups per profile archive: 3

2.7.4. Create single backup per day: Habilitado

2.8. Configuración del usuario -> Directivas -> Plantillas Administrativas -> VMware DEM -> Flex Engine -> Profile archives

2.8.1. Location for storing user profile archives: \\ficheros.midominio.local\demperfiles$\%username%\Archives

2.8.2. Hide profile archive folder: Deshabilitado

2.8.3. Compress profile archives: Habilitado

2.8.4. Retain file modification dates: Deshabilitado

Configuración del usuario -> Directivas -> Plantillas Administrativas -> VMware DEM -> Flex Engine -> Run FlexEngine at logon and logoff -> Habilitado

19.5 Anexo V. Creación de imagen Golden

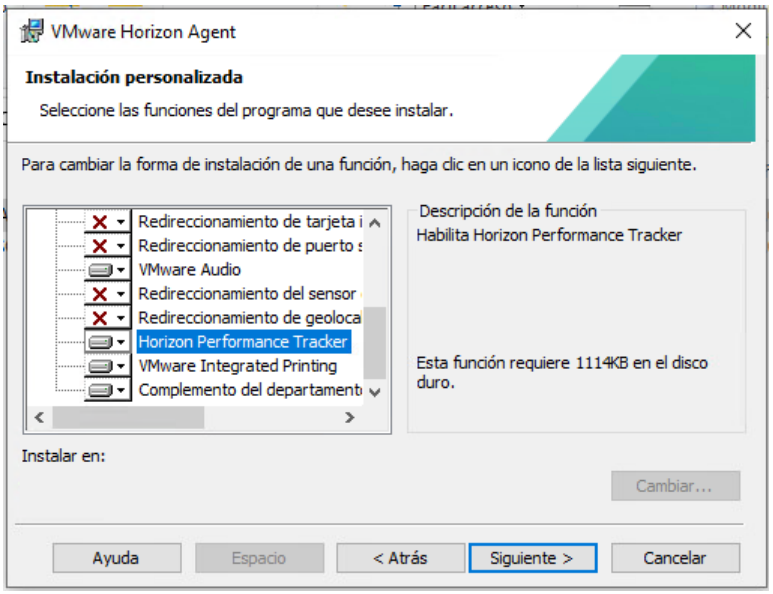
19.5.1 Instalación y configuración

1. Se crea una nueva máquina virtual con las siguientes características

Recurso	Valor
Nombre	Golden01
CPU	4 vCPUs
RAM	8 GB
Disco duro	60 GB
NIC	VMXNET3

Configuración de red	IP: DHCP MASK: DHCP Gateway: DHCP DNS: DHCP

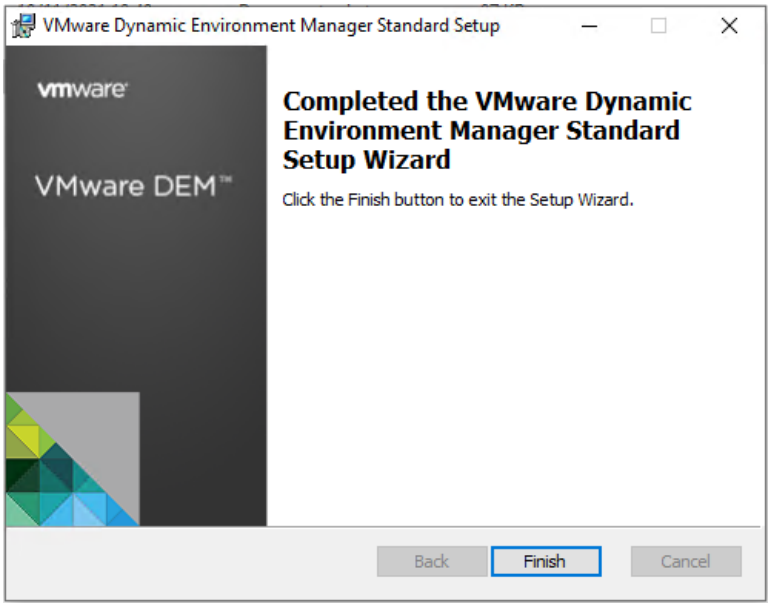
2. Se instala Windows 10 21H2. Es importante que la versión de Windows esté dentro de la matriz de compatibilidad de Horizon
3. Se instalan las últimas actualizaciones de Windows
4. Instalar VMware Tools
5. Agregar máquina al dominio
6. Mover cuenta de máquina a la OU correspondiente, para tener una correcta organización: "OU=General,OU=Clientes,OU=VDI,DC=midominio,DC=local"
7. Ejecutar el archivo "VMware-Horizon-Agent-x86_64-2106-8.3.0-18287218.exe" para instalar el agente de Horizon
8. En "Configuración del protocolo de red", seleccionar "IPv4"
9. Añadir "Horizon Performance Tracker" en las opciones de instalación



10. Clic en "Instalar"

19.5.2 Instalación Agente DEM

1. Con la sesión iniciada en la máquina que contiene la Golden Image, descargar el archivo de instalación
2. Se ejecuta el archivo "VMware Dynamic Enronment Manager Standard 2016 10.3 x64.msi"
3. En "Choose Setup Type", seleccionar "Custom"
4. Clic en "Install" y "Finish"



19.5.3 VMware Horizon OS Optimization Tool

Esta herramienta proporciona una guía paso a paso para crear una imagen Golden. Además, optimiza la máquina para Horizon.

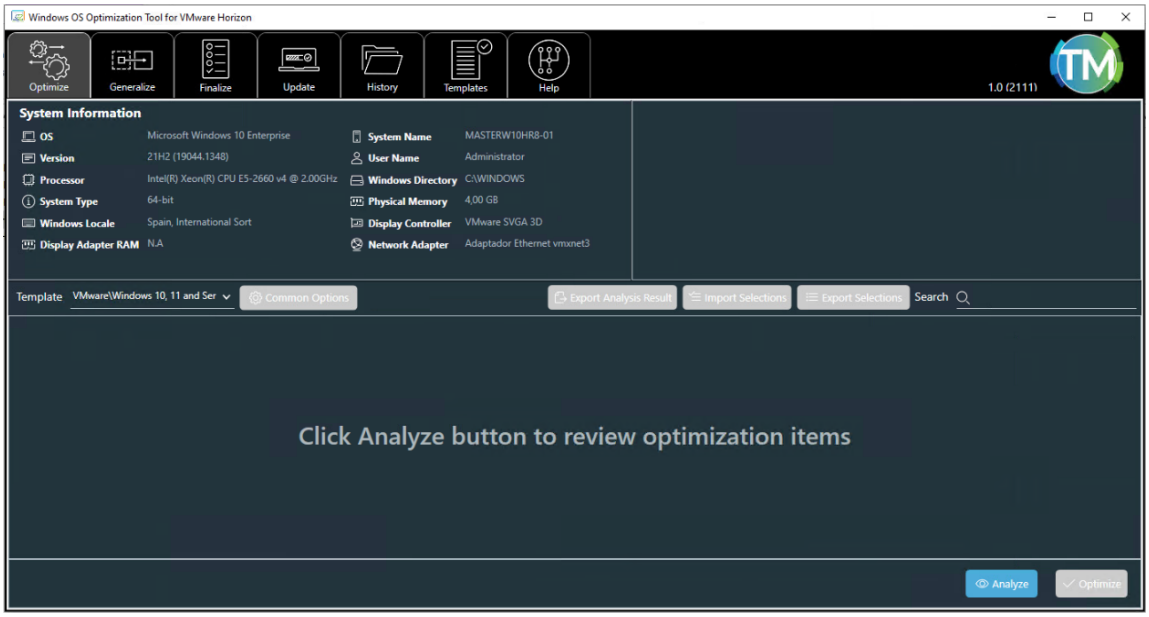
Los pasos recomendados para la creación de una máquina, y que comprueba esta herramienta, son los siguientes:

1. Crear la máquina virtual
2. Instalación de aplicaciones y agentes
3. Optimización
4. Generalización. En este paso realiza un "sysprep" con la opción "Generalize", para que la máquina pueda ser clonada mediante la eliminación del SID. Además,

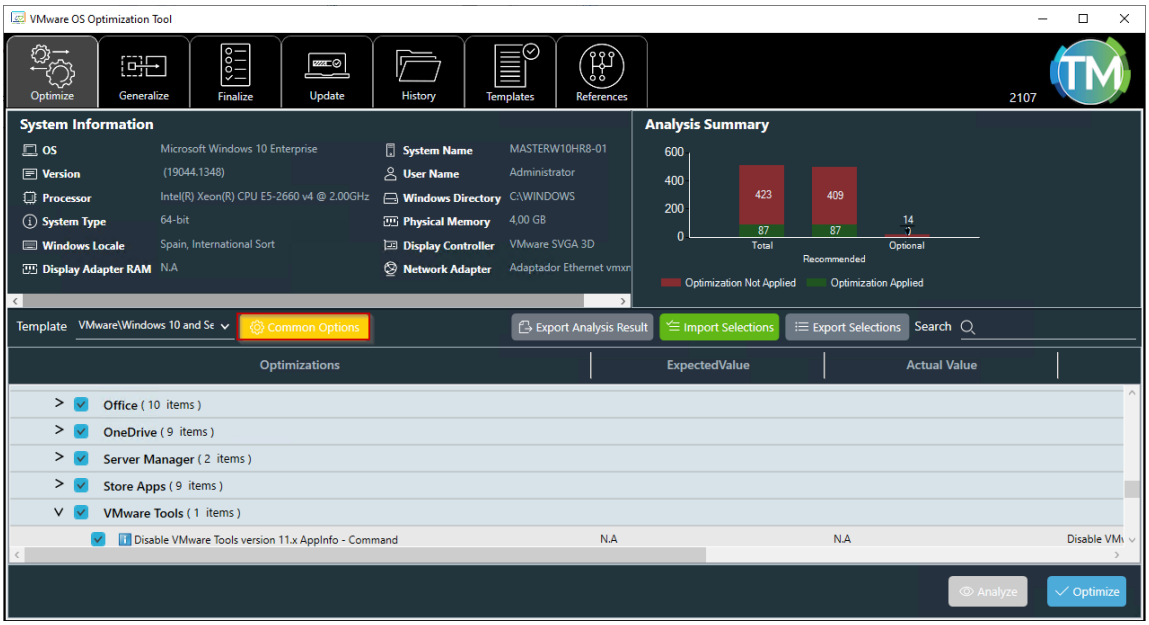
la creación de máquinas a partir de esta se creará desde un archivo editable de respuestas desatendidas.

19.5.3.1 Uso de la herramienta

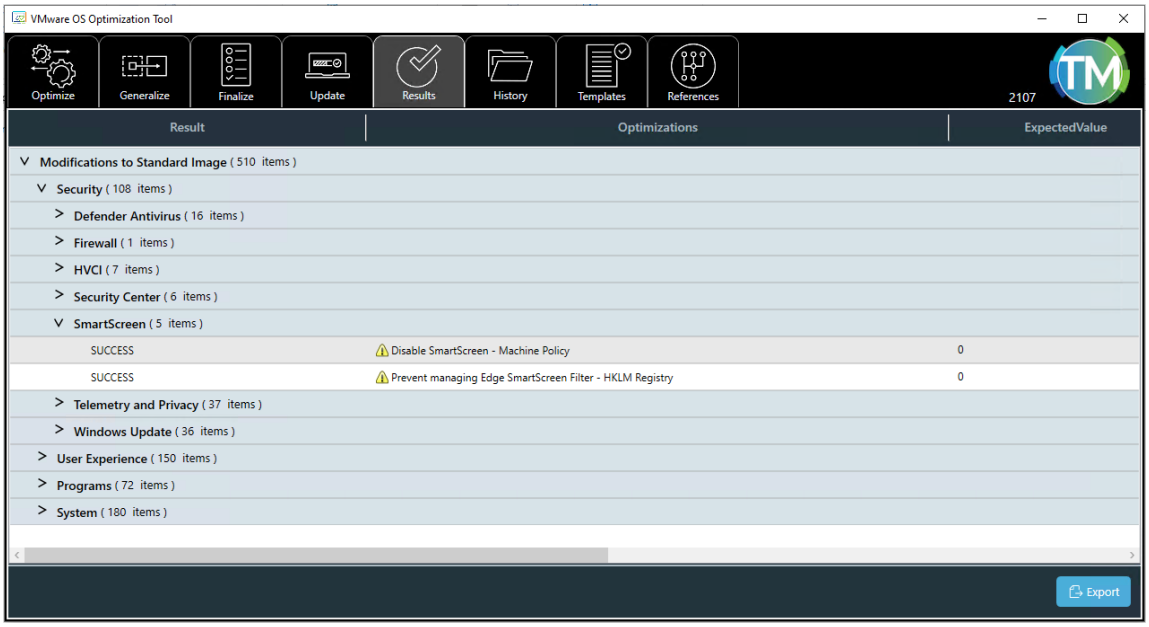
1. Descargar el archivo de instalación de la herramienta VMware Horizon OS Optimization Tool.
2. Ejecutar el archivo descargado "VMwareHorizonOSOptiomizationTool-x86_64-1.0_2111.exe"
3. Seleccionar la opción "Analyze", tal y como se muestra en la captura siguiente:



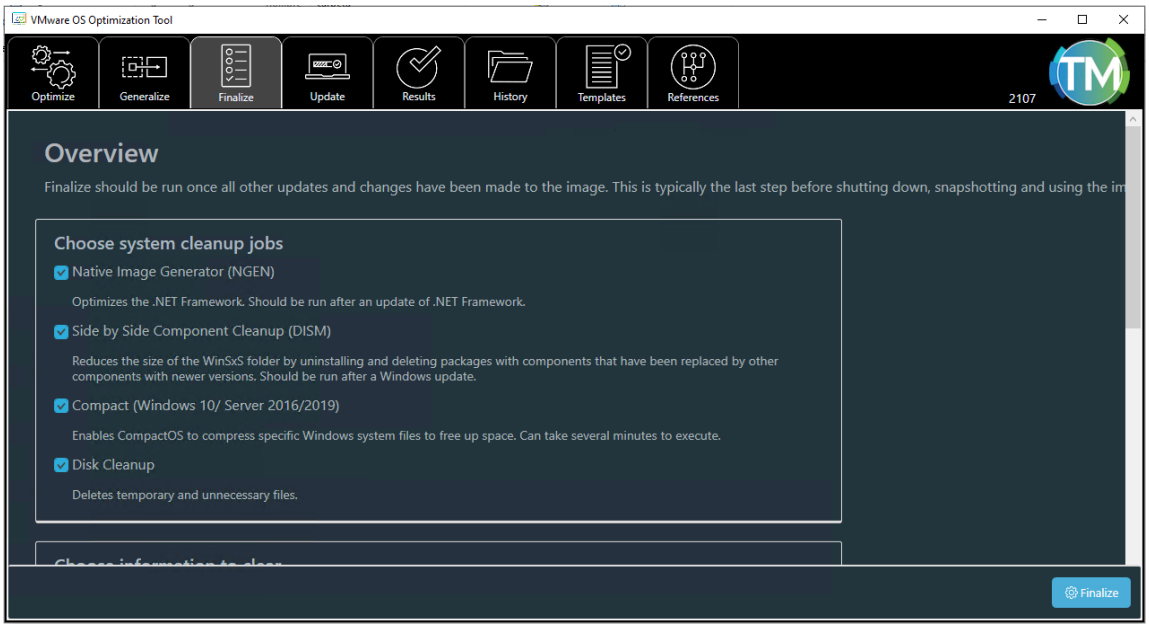
Esto mostrará una lista de posibles optimizaciones a realizar, que se podrán editar desde "Common Options", tal y como se muestra en la imagen



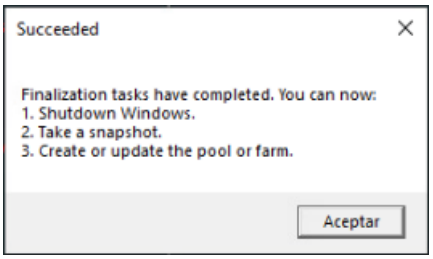
4. Revisar y mantener, si procede, las opciones y seleccionar “Optimize”. Esta acción implementará los cambios y mostrará el resultado de las acciones realizadas



5. Seleccionar “Finalize”. Tener en cuenta que esta acción provocará la pérdida de conexión con la máquina, en caso de estar conectado por RDP. Por ello, es recomendable haberse conectado desde la consola de vCenter



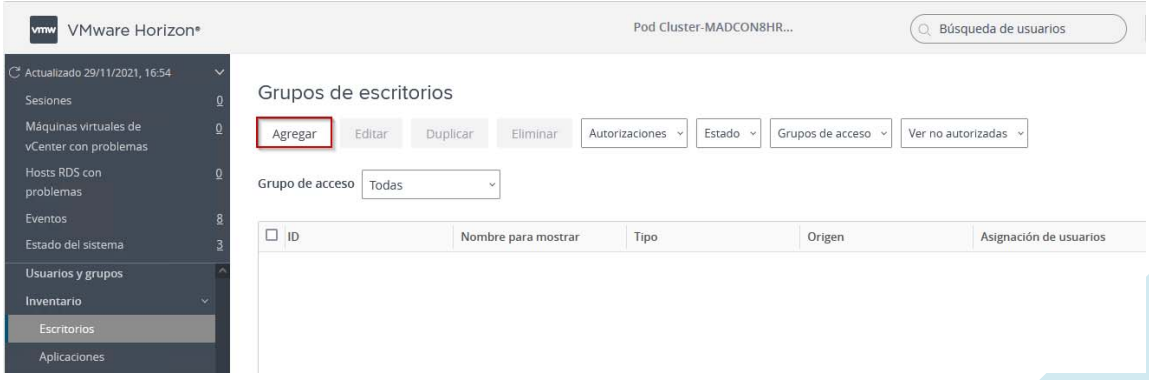
6. Aparecerá la siguiente ventana que indica las acciones a realizar a partir de ese momento



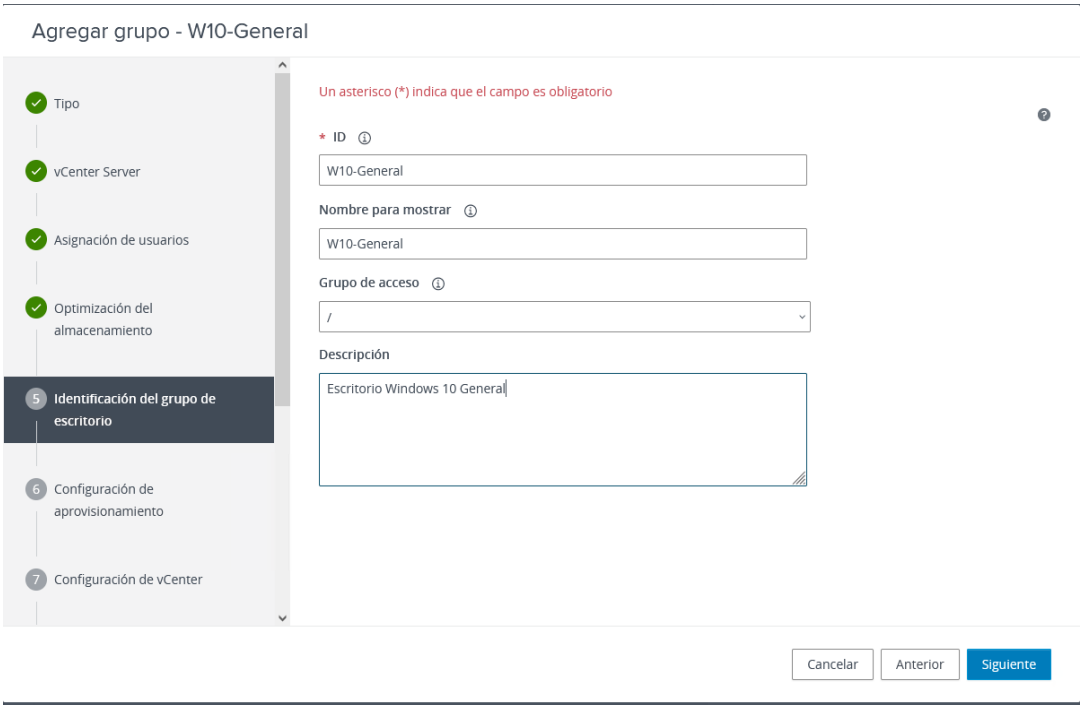
7. Apagar la máquina virtual
8. Realizamos un snapshot con el nombre “Golden01_Snapshot1”

19.6 Anexo VI. Instalación del Pool de Escritorios

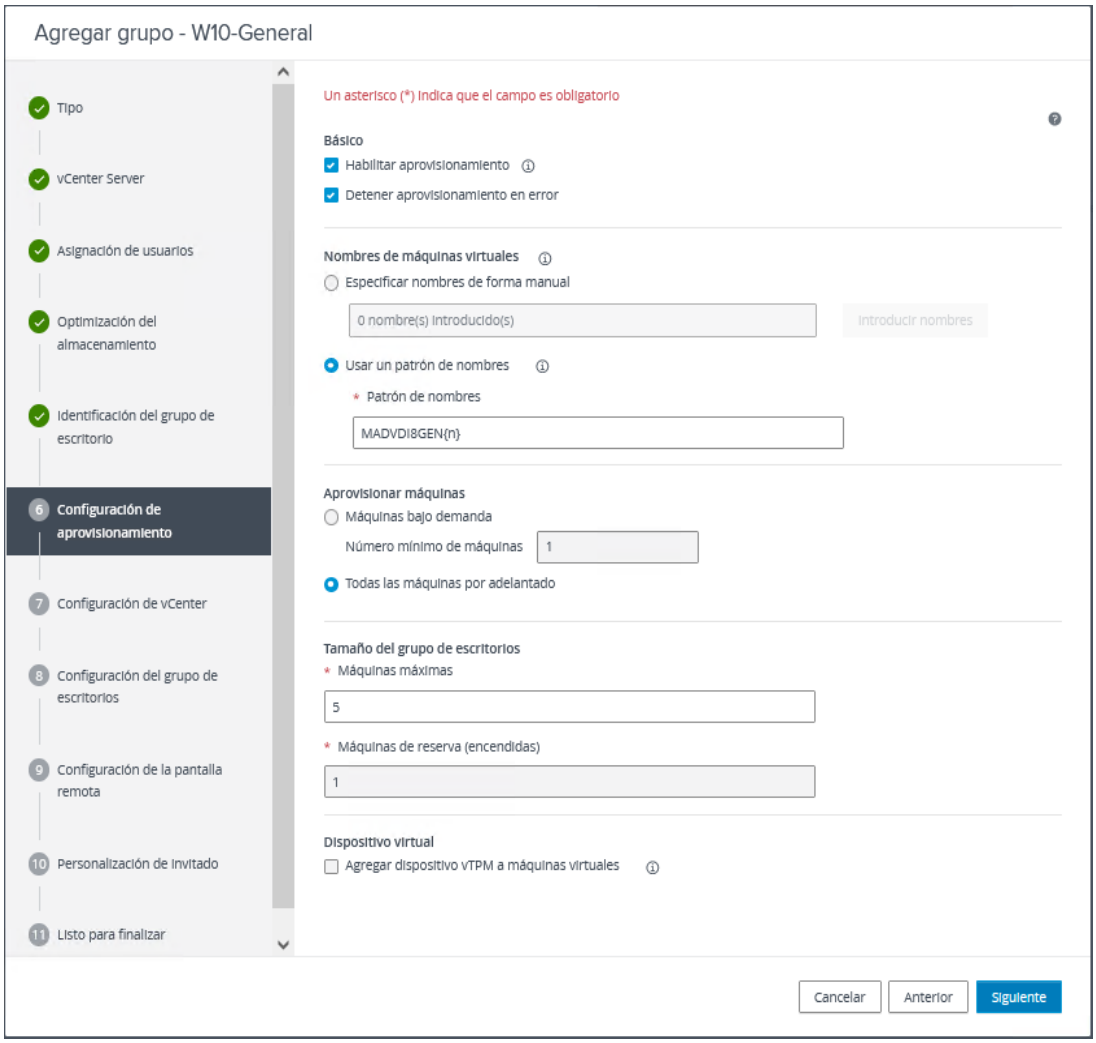
1. Conectarse a la consola de administración de Horizon
2. Inventario -> Escritorios -> Agregar



3. Seleccionar “Grupo de escritorios automatizado”
4. Seleccionar “Clon instantáneo”
5. En asignación de usuarios, seleccionar “Flotante”
6. Desmarcar la opción “Utilizar almacenes de datos diferentes para discos de SO y de réplica”
7. Completar los campos según la imagen adjunta:

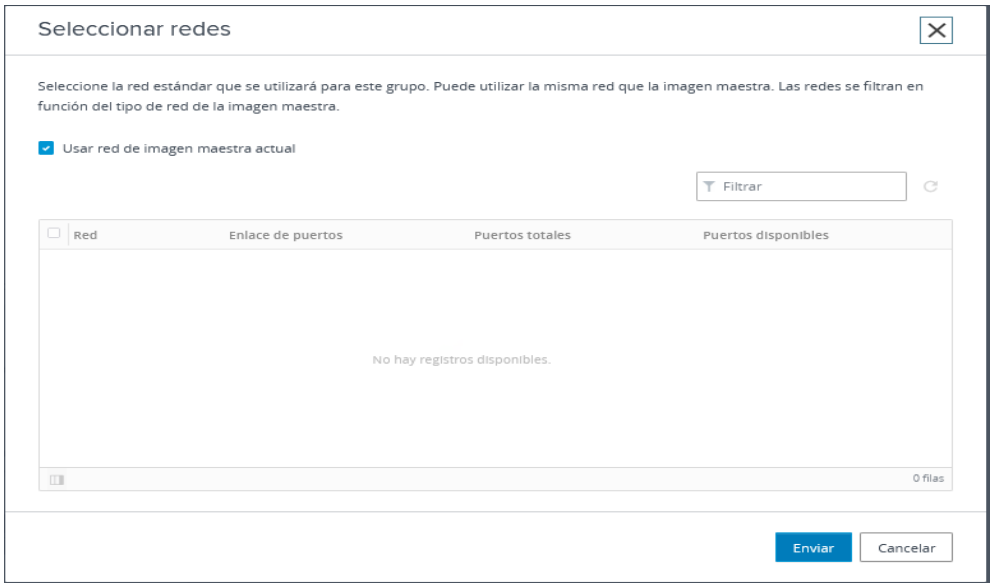


8. Completar los campos según la imagen adjunta:

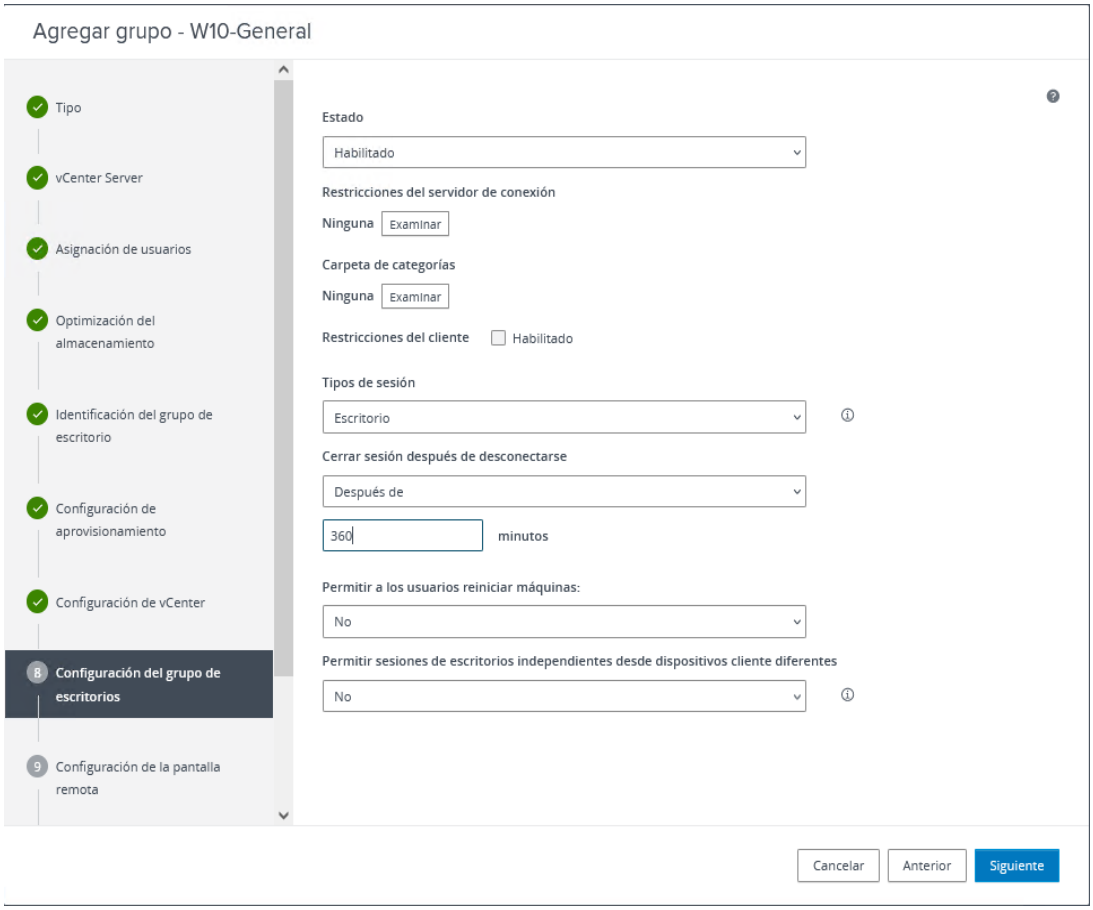


En el campo “patrón de nombres”, el valor {n} hará que se vayan nombrando con números crecientes consecutivos.

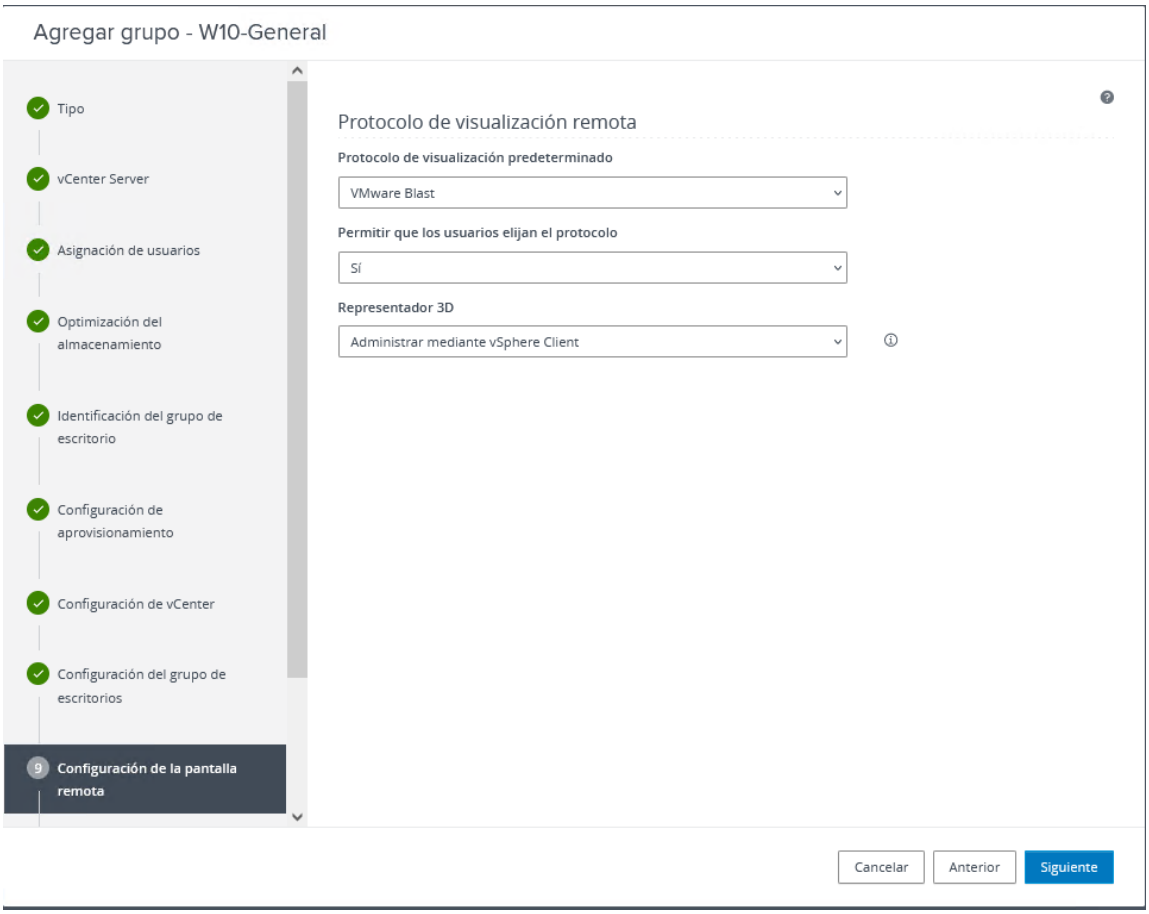
9. Seleccionar la imagen maestra, en este caso la creada anteriormente como “Golden01”
10. En el campo “Instantánea”, clic en “Examinar”
11. Escoger el snapshot a partir del cual se desplegarán los escritorios. En este caso, seleccionaremos el creado anteriormente como “Golden01_Snapshot1”
12. En “Ubicación de la máquina virtual”, clic en “Examinar”. Seleccionar la carpeta de vCenter donde se ubicarán los escritorios virtuales. Este punto no es necesario, pero es importante para tener una correcta organización.
13. En “Almacenes de datos”, seleccionar “Examinar” y seleccionar el DataStore dedicado a las máquinas
14. En “Red” seleccionar “Examinar” y dejar marcado “Usar red de imagen maestra actual”



15. Completar los campos según la imagen adjunta:



16. Mantener las siguientes opciones por defecto:



17. En “Personalización de invitado”, completar los siguientes campos:
    a. Dominio: midominio.local
    b. Contenedor de AD: “OU=General,OU=Clientes,OU=VDI,DC=midominio,DC=local”
    c. Permitir la reutilización de cuentas de equipo existentes: Marcado
    d. Usar ClonePrep: Seleccionado
18. En “Listo para finalizar”, seleccionar “Autorizar usuarios tras agregar grupo”
    a. Seleccionar el grupo que contiene los usuarios con permisos para acceder el pool de escritorios. En nuestro caso “AP_Horizon_Usuarios” que habíamos creado previamente.

En el punto 17.d se puede ver que se usa “ClonePrep”. Esta es una herramienta para “Instant Clones”, y que permite las siguientes personalizaciones:

- Cambiar el nombre a la máquina virtual
- Cambiar la password del administrador local
- Añadir la máquina clonada al dominio de Active Directory

- Activar la licencia de Microsoft usando un servidor KMS, que tal y como se ha referenciado anteriormente, este servidor dentro del proyecto, se llama “KMS1”

19.7 Anexo VII. Instalación y configuración True SSO

19.7.1 CA del Dominio

se crea una CA una subordinada de la principal (PKI1), llamada PKI2. Sobre ésta última, se realizan las siguientes configuraciones:

- Para configurar la CA en modo “no persistente”, ejecutar el siguiente comando desde una consola de comandos abierta desde la máquina CA, con permisos de Administrador:
  - certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS

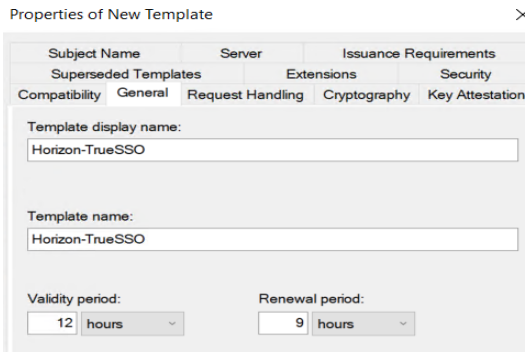
```
C:\Windows\system32>certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBFlags:

Old Value:
  DBFlags REG_DWORD = b0 (176)
    DBFLAGS_MAXCACHESIZEX100 -- 10 (16)
    DBFLAGS_CHECKPOINTDEPTH60MB -- 20 (32)
    DBFLAGS_LOGBUFFERSHUGE -- 80 (128)

New Value:
  DBFlags REG_DWORD = 8b0 (2224)
    DBFLAGS_MAXCACHESIZEX100 -- 10 (16)
    DBFLAGS_CHECKPOINTDEPTH60MB -- 20 (32)
    DBFLAGS_LOGBUFFERSHUGE -- 80 (128)
    DBFLAGS_ENABLEVOLATILEREQUESTS -- 800 (2048)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```

- Reiniciar los servicios de la CA:
  - sc stop certsvc
  - sc start certsvc

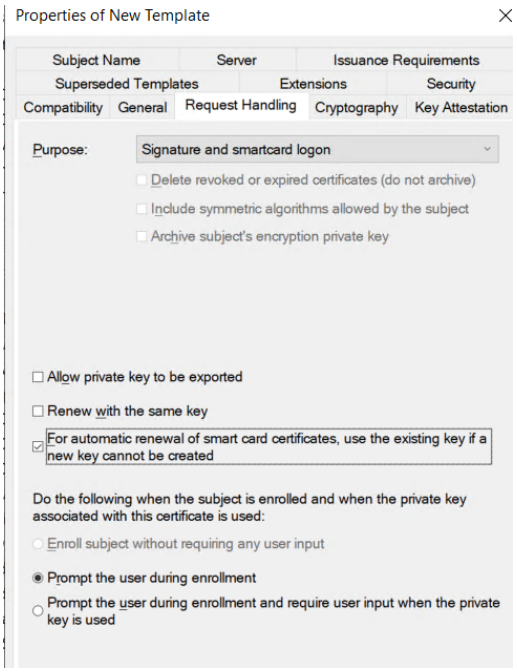
19.7.2 Creación plantillas de certificado para True SSO

1. Abrir la consola de administración de la CA
2. Certificate Templates -> Manage -> Smartcard Logon -> Duplicate Template

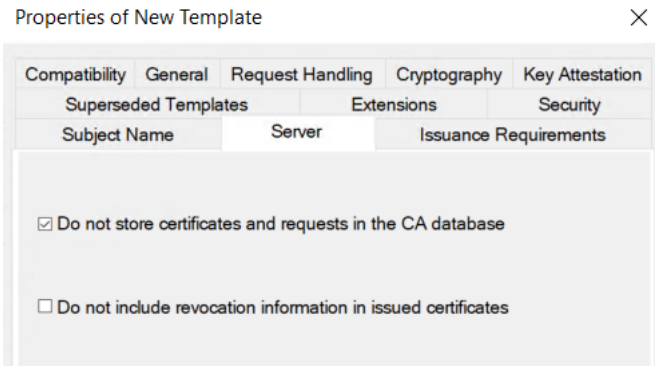
3. Establecer el modo de compatibilidad W10/Windows Server 2016
4. Pestaña General. El campo “validity period” ha de establecer un período de tiempo que cubra la jornada laboral completa de los usuarios. Un período recomendado sería el que se muestra en la captura:



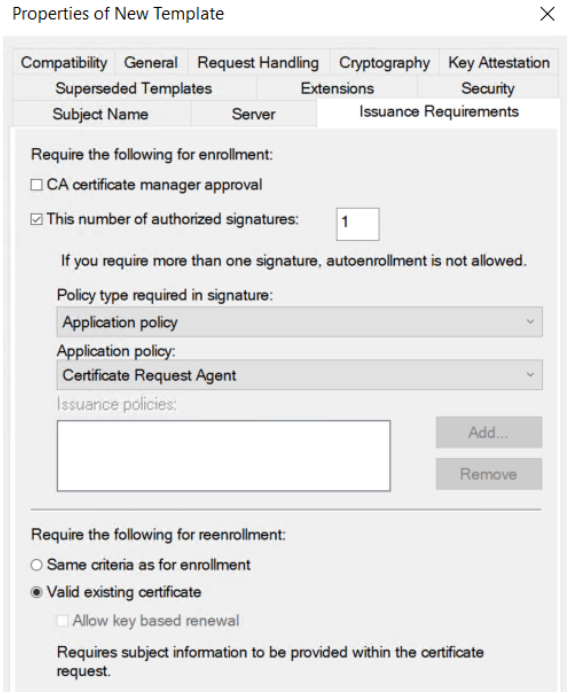
5. Pestaña Request Handling. Establecer según se muestra en la captura:



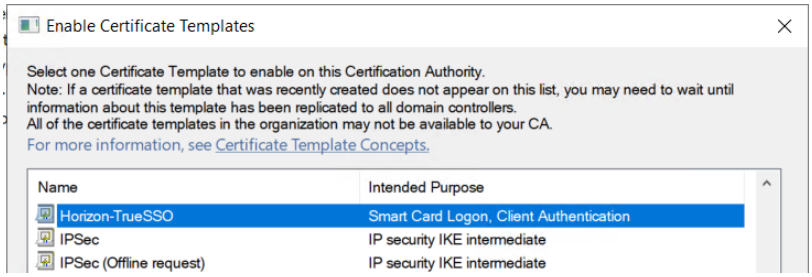
6. Pestaña Cryptography.
    a. Provider Category: Key Storage Provider
    b. Algorith name: RSA
    c. Minimum key size: 2048
    d. Seleccionar “Requests can use any provider available on the subject’s computer”
7. Pestaña Server. Establecer según se muestra en la captura:



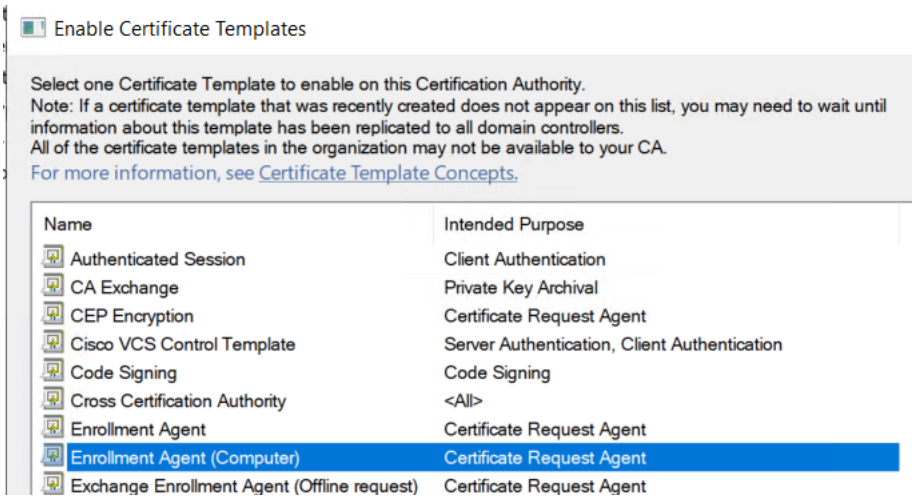
8. Pestaña Issuance Requirements. Establecer según se muestra en la captura:



9. Se crea un nuevo grupo en DA llamado “AP_Horizon_EnrollmentServer”, que contendrá los servidores que pueden hacer enrollment de los certificados de conexión.
10. Pestaña Security. Se añade el grupo creado en el punto anterior (AP_Horizon_EnrollmentServer) con permisos “Read” y “Enroll”
11. Certificate Templates: New -> Certificate Template to Issue
12. Seleccionar la plantilla recién creada



13. Certificate templates -> Manage. Se busca “Enrollment Agent (Computer) -> Propiedades
14. Se añade el grupo recién creado “AP_Horizon_EnrollmentServer”, con permisos “Read” y “Enroll”
15. Certificate Template: New -> Certificate Template to Issue:
16. Agregar la plantilla (Notar que ésta no se ha duplicado, sino que se ha seleccionado directamente)



19.7.3 Servidor Enrollment Server

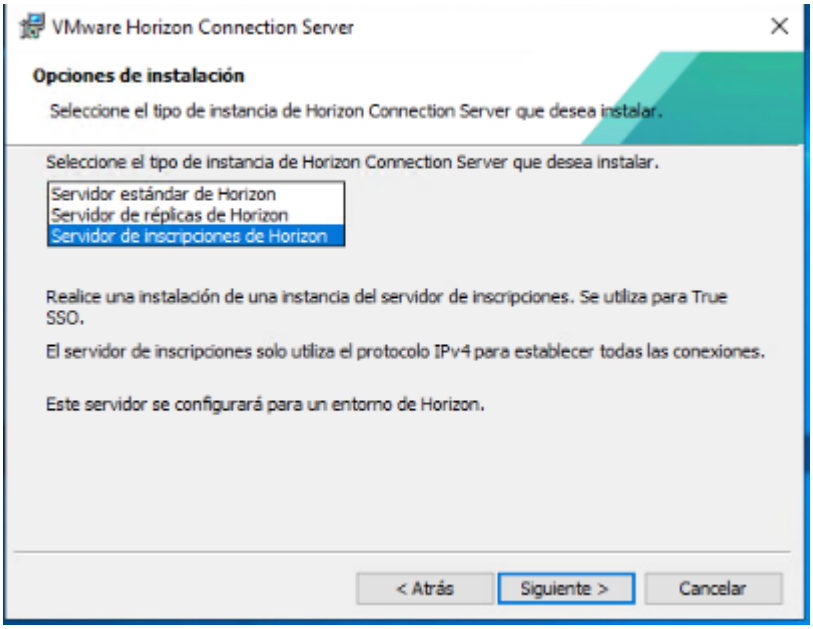
19.7.3.1 Instalación

Para la función de servidor con el rol de Enrollment Server, se instala una máquina virtual con las siguientes características:

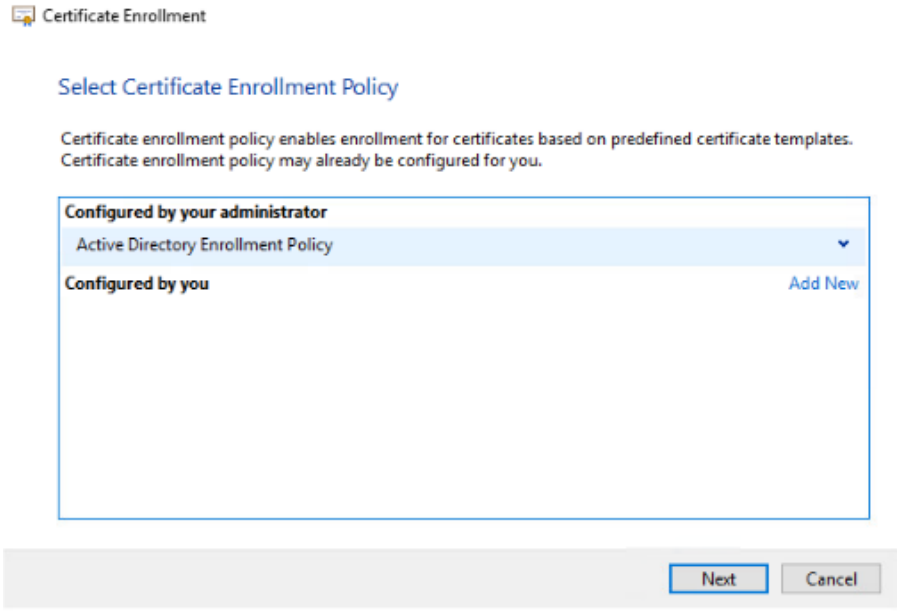
Recurso	Valor
CPU	4 vCPUs
RAM	8 GB
Disco duro	80 GB
NIC	VMXNET3
Configuración de red	IP: 172.16.172.88 MASK: 255.255.248.0 Gateway: 172.16.172.3

	DNS: 172.16.172.90/172.16.172.121

1. Ejecutar el archivo "VMware-Horizon-Connection-Server-x86_64-8.4.0-19067837.exe"
2. Opciones de instalación -> Seleccionar "Servidor de inscripciones de Horizon"



3. Seleccionar "Configurar Firewall de Windows automáticamente":
4. Clic en "Instalar"
5. Clic en "Finalizar"
6. Ejecutar "mmc.exe" con permisos de administrador
7. Archivo -> Agregar o quitar complemento -> Certificados -> Agregar -> Cuenta de equipo
8. Personal -> Todas las tareas -> Solicitar un nuevo certificado
9. Seleccionar "Active Directory Enrollment Policy" y "Next"



10. Seleccionar “Enrollment Agent (Computer)”
11. Click en “Finish”

19.7.4 Export certificado cliente servicio de inscripciones

1. Conectarse al servidor VDICS1, que tiene el rol de Connection Server
2. Ejecutar “mmc.exe” con permisos de administrador
3. Archivo -> Agregar o quitar complemento -> Certificados -> Agregar -> Cuenta de equipo
4. Clic en el contenedor “Certificados de VMware Horizon View” -> Certificados
5. Seleccionar el certificado con el nombre descriptivo “vdm.ec” -> All Tasks -> Export
6. Seleccionar “No, don’t export private key”
7. Seleccionar “Base-64 Encoded X.509 (.CER)”
8. Asignar el nombre al certificado: “enroll_client.cer”
9. Clic en “Finish”

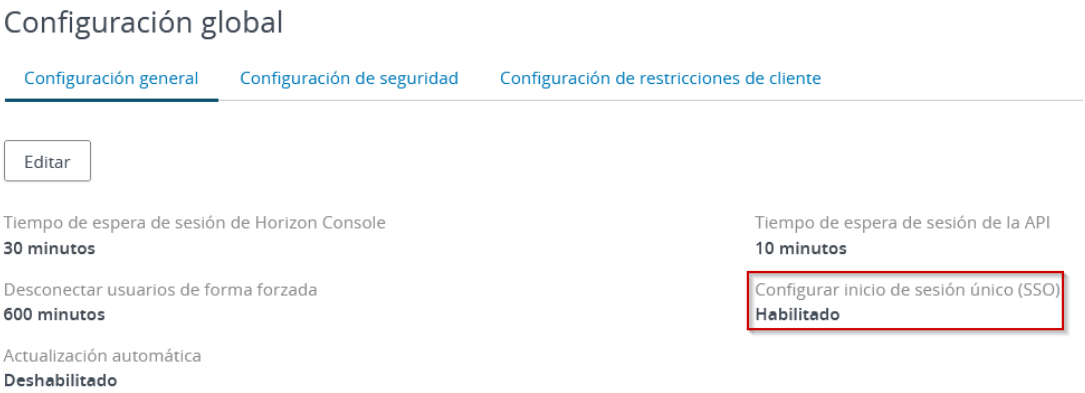
19.7.5 Import certificado cliente en el servidor Enrollment Server

1. Conectarse al servidor VDIENR1, que tiene el rol de Enrollment Server

2. Ejecutar “mmc.exe” con permisos de administrador
3. Archivo -> Agregar o quitar complemento -> Certificados -> Agregar -> Cuenta de equipo
4. Clic en el contenedor “Entidades de certificación raíz de confianza” -> Todas las tareas -> Importar
5. Seleccionar archivo “enroll_client.cer”

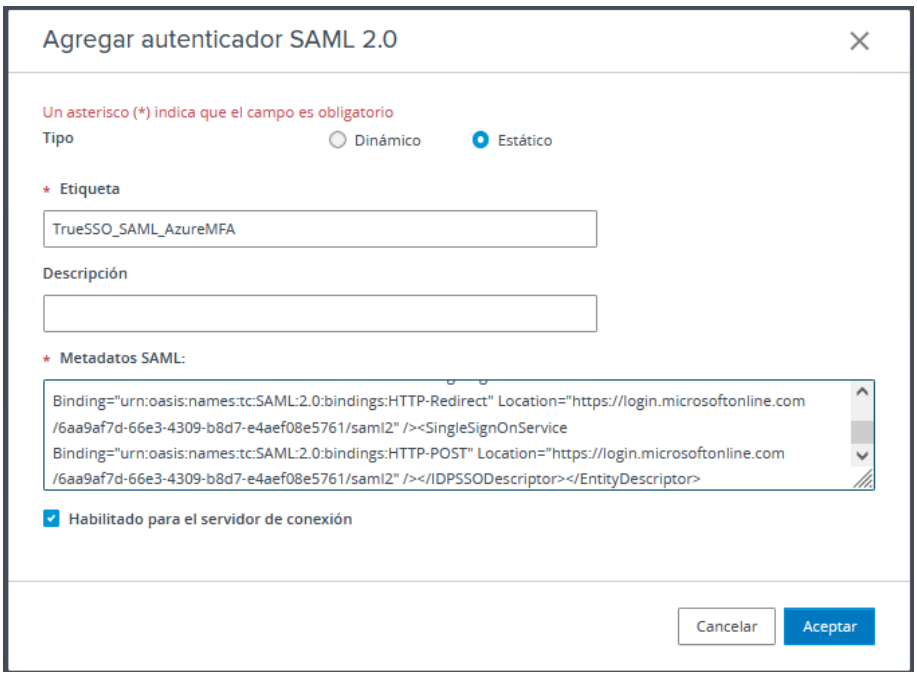
19.7.6 Configuración SAML con TRUE SSO

1. Acceder a la consola de administración de Horizon
2. Configuración global -> Configuración general
3. Comprobar que la configuración “Configuración de inicio de sesión único (SSO)” está HABILITADA

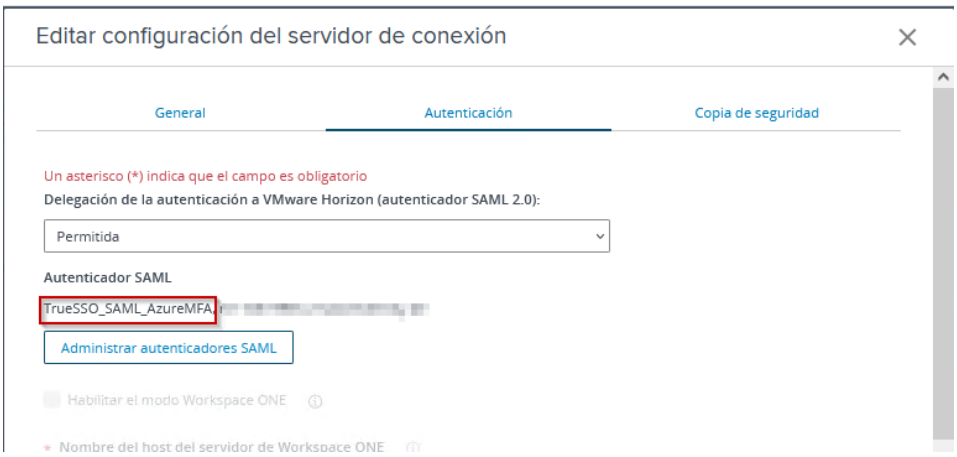


4. Configuración -> Servidores -> Servidores de conexión -> Seleccionar VDICS1 -> Editar
5. Pestaña Autenticación.
    a. Delegación de la autenticación a WMware Horizon (autenticador SAML 2.0): Permitida

6. Seleccionar “Administrar autenticadores SAML” -> Agregar
    a. Marcar Tipo: “Estático”
    b. Etiqueta: TrueSSO_SAML_AzureMFA
    c. Pegar contenido del fichero XML que se descargó desde Azure
    d. Habilitado para el servidor de conexión : Marcado



7. En la pestaña “Autenticación” ya aparecerá el autenticador SAML recién configurado

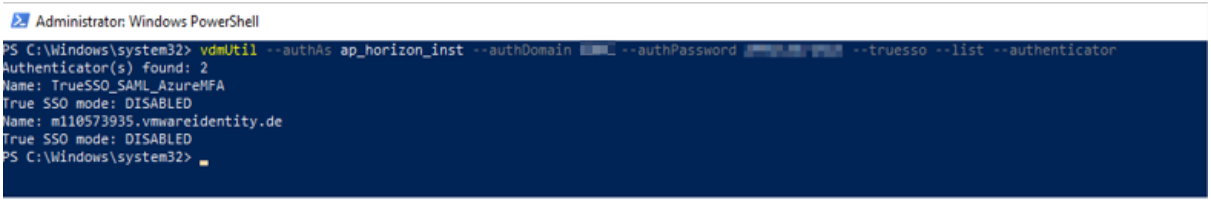


19.7.7 Configuración Connection Server para True SSO

1. Conectarse al servidor VDICS1 por Terminal Server
2. Abrir una consola de PowerShell, con permisos de administrador
3. Para agregar el Enrollment Server, ejecutar el siguiente comando:

   a. vdmUtil --authAs ap_horizon_inst --authDomain MIDOMINIO --authPassword <Password_ap_horizon_inst> --truesso --environment --add --enrollmentServer VDIENR1

4. Para que aparezca la información del Enrolment Server, ejecutar el siguiente comando:
   a. vdmUtil --authAs ap_horizon_inst --authDomain MIDOMINIO --authPassword <Password_ap_horizon_inst> --truesso --environment --list --enrollmentServer VDIENR1 --domain midominio.local
5. Para crear un conector True SSO, con la información de la configuración y habilitarlo, ejecutar el siguiente comando:
   a. vdmUtil --authAs ap_horizon_inst --authDomain MIDOMINIO --authPassword <Password_ap_horizon_inst> --truesso --create --connector midominio.local --template Horizon-TrueSSO --primaryEnrollmentServer VDIENR1 --certificateServer PKI2 --mode enabled
6. Para ver los autenticadores SAML disponibles, ejecutar el siguiente comando:
   a. vdmUtil --authAs ap_horizon_inst --authDomain MIDOMINIO --authPassword <Password_ap_horizon_inst> --truesso --environment --list --enrollmentServer VDIENR1 --domain midominio.local



7. Para habilitar el uso del autenticador en modo True SSO, ejecutar el siguiente comando:
   a. vdmUtil --authAs ap_horizon_inst --authDomain MIDOMINIO --authPassword <Password_ap_horizon_inst> --truesso --authenticator --edit --name TrueSSO_SAML_AzureMFA --truessoMode ENABLED