



TGF - Despliegue automatizado por red para la renovación de la infraestructura

Ballester Talavera, José Miguel
Grado en Ingeniería Informática

Consultor: Manuel Jesús Mendoza Flores

Fecha de entrega: 01/2020



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

FICHA DEL TRABAJO FINAL

Título del trabajo:	<i>Despliegue automatizado para la renovación de la infraestructura</i>
Nombre del autor:	<i>José Miguel Ballester Talavera</i>
Nombre del consultor:	<i>Manuel Jesús Mendoza Flores</i>
Fecha de entrega (mm/aaaa):	<i>01/2020</i>
Área del Trabajo Final:	<i>Administración de sistemas</i>
Titulación:	<i>Grado en Ingeniería Informática</i>
Resumen del Trabajo (máximo 250 palabras):	
<p>Con el fin de mejorar la eficiencia laboral y evitar errores humanos se pretende crear un conjunto de servicios y herramientas para el despliegue automatizado de los sistemas operativos utilizados por defecto en las empresas de servicios IT (Microsoft Windows Server y Linux Debian) y aplicación de los ajustes de configuración inicial, facilitando así la renovación de la infraestructura hardware.</p> <p>La instalación y configuración pretende ser desatendida en la mayor parte del proceso, por lo que mediante arranque por red (PXE) se lanzará la instalación del SO con la preasignación de opciones, para minimizar la intervención humana.</p> <p>Una vez instalado el sistema operativo se lanzará la instalación de software y configuraciones adicionales para preparar el servidor para su uso y/o administración remota.</p>	
Abstract (in English, 250 words or less):	
<p>In order to improve work efficiency and avoid human errors, the goal is to create a set of tools for the automated deployment of the operating systems used by default by the IT services companies (Microsoft Windows Server and linux Debian) and their initial configuration settings, thus facilitating the renewal of the hardware infrastructure.</p> <p>The installation and configuration aims to be unattended in most part of the process, so the installation of the OS with the pre-assigned options will be made by network startup (PXE) to minimize human intervention.</p> <p>Once the operating system is installed, the installation of additional software and configurations will be launched to prepare the server for its use or administration.</p>	
Palabras clave (entre 4 y 8):	
Gestión de la infraestructura IT, automatización de sistemas, administración de sistemas, gestión de la configuración.	

Índice

1. Introducción.....	1
1.1 Contexto y justificación del Trabajo.....	1
1.2 Costes y rentabilidad.....	3
1.3 Riesgos.....	5
1.4 Planificación del trabajo.....	7
1.5 Enfoque y método seguido.....	9
1.6 Sumario de productos obtenidos.....	12
1.7 Breve descripción de los otros capítulos de la memoria.....	12
2. Resto de capítulos.....	13
2.1. Qué es el PXE.....	13
2.2. Arranque por red (PXE).....	14
2.3. Configuración del entorno de arranque.....	15
2.3.1 Instalación de los servicios necesarios.....	15
2.3.2 Configuración del servicio WDS para imágenes Windows.....	19
2.3.3 Automatización de la instalación de Windows.....	24
2.3.4 Configuración y arranque del menú iPXE.....	28
2.3.6 Arranque del kernel Linux y automatización de la instalación de Debian.....	34
2.4. Instalación desatendida y post-instalación.....	36
2.4.1 Configuración Windows Server 2019.....	36
2.4.2 Configuración Debian.....	39
3. Conclusiones.....	41
4. Glosario.....	43
5. Bibliografía y enlaces.....	45
6. Anexos.....	46
6.1 Ficheros de configuración de iPXE.....	46
6.2 Fichero de configuración de preseed.cfg.....	49
6.3 Ficheros de configuración WDS (Unattended.xml).....	50
6.4 Fichero de configuración post-instalación Windows.....	52
6.5 Fichero de configuración post-instalación Linux.....	53
6.6 Resumen de ficheros utilizados en la configuración.....	54

Lista de figuras

Logotipo UOC.....	1
CC BY ND.....	ii
Diagrama de Gantt.....	8
Protocolo PXE.....	14
Instalación de servicios desde Server Manager.....	15
Confirmación de la instalación.....	16
Configuración post-instalación.....	16
Creación scope servidor DHCP.....	16
Configuración del rango DHCP.....	16
Servidor WDS no configurado.....	17
Menu contextual configuración WDS.....	17
Opciones de integración con AD.....	17
Opciones de WDS para el DHCP.....	17
Configuración ProxyDHCP.....	18
Proceso de instalación.....	18
Arranque manual del servicio.....	18
Ficheros del DVD Windows Server.....	19
Añadir imagen de arranque.....	19
Selección del fichero de imagen de arranque.....	19
Nombre de la imagen de S.O.....	20
Imagen importada a WDS.....	20
Añadir imagen de instalación.....	20
Creación del grupo.....	20
Selección del fichero de imagen de instalación.....	20
Selección de arquitectura y versión.....	21
Proceso de importación.....	21
Imagen de instalación importada.....	21
Prueba de arranque BIOS.....	21
Captura de paquetes BIOS.....	22
Captura de paquetes BIOS (2).....	22
Prueba de arranque UEFI.....	22
Captura del arranque UEFI.....	22
Carga de la instalación por red.....	22
Inicio de la instalación.....	22
Selección de idioma y teclado.....	23
Solicitud de credenciales.....	23
Instalación ADK (ruta por defecto).....	24
Opciones de instalación de ADK.....	25
Windows System Image Manager.....	25
Creación del catálogo.....	25
Apertura fichero de imagen.....	25
Selección arquitectura de la imagen.....	26
Añadir componentes al fichero XML.....	26
Atributos de los componentes.....	26
Componentes añadidos.....	26
Configuración del fichero respuestas.....	27

Habilitar uso por imagen.....	27
Configuración del fichero de respuestas.....	27
Ficheros iPXE.....	29
Configuración del servicio DHCP.....	29
Deshabilitar opción 60.....	29
Creación nuevas clases.....	29
Clase iPXE.....	30
Clase PXE Arquitectura UEFI.....	30
Creación nueva política DHCP.....	30
Selección de clases creadas.....	30
Selección de condiciones.....	31
Configuración del atributo 60.....	31
Configuración del atributo 67.....	31
Configuración atributos UEFI.....	31
Orden de las políticas.....	32
Cambio de claves de registro.....	32
Filtro TFTP.....	32
Arranque servidor UEFI.....	33
Menú de iPXE.....	33
Descarga de netboot desde debian.org.....	34

1. Introducción

1.1 Contexto y justificación del Trabajo

Hoy en día, muchas empresas pueden ofrecer sus servicios mediante Internet, tanto potenciados como a través de éste, siendo un ecosistema que evoluciona a pasos agigantados, así como la tecnología. Cada vez más, el cliente desea una respuesta más rápida y ágil a las interacciones con los servicios ofrecidos online, y las empresas, por su parte, mejorar los beneficios y/o rentabilidad, razón por la cual -además de potenciar el crecimiento- es necesario renovar y ampliar el parque informático para aumentar la potencia, eficiencia y/o la capacidad del servicio ofrecido.

Entre los aspectos negativos que puede encontrarse una empresa en crecimiento figuran diferentes limitaciones y situaciones que ralentizan o suponen una barrera al crecimiento, por ejemplo la disponibilidad de espacio físico o dedicar tiempo y recursos a tareas repetitivas, por ejemplo de instalación y configuración, siendo éstas -además- susceptibles a errores humanos.

Para superar el primer aspecto negativo, la limitación de espacio físico, una opción es aumentar la densidad de potencia o rendimiento, por ejemplo ampliando el hardware y/o renovando cíclicamente el parque informático, con equipos más potentes. Determinados proveedores ofrecen la opción de incluir en un leasing las compras de equipos para evitar un desembolso inicial importante y controlar mejor el retorno de inversión, ya que es posible retornar dichos equipos antes de finalizar el pago íntegro. Y debido a la velocidad a la que aumenta la potencia de cómputo informática, no siempre es lo más rentable utilizar los equipos hasta su deterioro.

Para el segundo punto, el tiempo dedicado a las tareas repetitivas, una de las posibles soluciones y técnicas a aplicar es la automatización, es decir, el reto de unificar muchos procesos manuales en uno o varios procesos automáticos minimizando la intervención manual.

Este segundo punto será el enfoque y la motivación de este trabajo para conseguir una configuración y despliegue de servidores en el menor tiempo posible con una tasa de errores (humanos) mínima. Dichos equipos, tras la instalación del sistema operativo, se les instalará diferente software o configuraciones según la finalidad a la que se vayan a destinar. Adicionalmente, con la tendencia del uso de DVD es a la baja, uno de los objetivos adicionales es minimizar o suprimir el uso de medios físicos (DVD, Usb) a la hora de llevar a cabo la instalación para, por un lado la practicidad y por otro lado la posibilidad de llevar a cabo la instalación remotamente, con herramientas como KVM, iDrac o iLO.

El *estado del arte* -actualmente- contempla multitud de herramientas para ejecutar cada parte en la que está dividido el trabajo, no obstante, son muy pocas -o nulas- las que cubren el proceso completo en la mayoría de sus fases.

Por otro lado, no hay una interoperabilidad completa entre cualquier software y las instalaciones de ambos sistemas operativos Windows y GNU/Linux, es más, dentro del subconjunto de las instalaciones de Linux se utilizan diferentes sistemas para la automatización de la instalación, según a qué familia pertenezca la distribución (por ejemplo: Debian utiliza preseed, Centos utiliza kickstart, etc.).

Por este motivo, el presente trabajo supone un reto de búsqueda, integración y aplicación de configuraciones, además de la prueba y validación de las diferentes configuraciones posibles y disponibles para alcanzar un enfoque hacia la optimización y automatización en la parte más básica de la infraestructura de los sistemas informáticos.

El objetivo de este trabajo es crear y facilitar una guía con la documentación del ensamblaje, configuración de un conjunto de programas, scripts y herramientas para que, tras su implantación, el proceso de renovación de la infraestructura de IT (servidores físicos y/o virtuales) se agilice y sea más eficiente, ahorrando costes, tiempo y errores.

1.2 Costes y rentabilidad

El público objetivo del trabajo no es cualquier empresa o persona particular, en primer lugar ha de evaluarse el tiempo a invertir frente al beneficio resultante, ya que si el tiempo invertido en la reinstalación de máquinas es nula o si la empresa es mayoritariamente consumidora de SaaS, plataformas de aplicaciones encapsuladas para su uso directo, no tiene sentido implementar el presente proyecto en la empresa.

La implantación del servicio cobra sentido en cuanto las horas dedicadas a la parte de infraestructura y preparación de los servidores superan al tiempo de implantación, lo cual es habitual en organizaciones que dispongan de centro de datos propio o que mantengan un parque informático de equipos de usuarios, donde no exista mucha diferenciación entre los equipos, por ejemplo:

- Medianas y grandes empresas
- Universidades
- Laboratorios

En el caso de las pequeñas empresas se debería evaluar si el número de horas dedicadas al plataformado de equipos de usuario compensa el implantar este sistema (tal como se describe en el trabajo), ya que existen las herramientas de imágenes de disco que permiten preparar diferentes imágenes para que al restaurarse dejen un equipo en el punto de renombrar, meter en dominio y la máquina estaría lista para su uso, aplicables tanto localmente como por red, siendo ésta una solución simple y de más rápida implantación.

Pero el verdadero punto a favor del sistema que se presenta es que está formado por capas y no limita la utilización a una determinada herramienta, sino que ofrece una plataforma abierta de estándares (PXE) para poder incorporar otras herramientas -alternativas o complementarias- para utilizar en el momento del arranque del equipo. Por ejemplo poder arrancar remotamente un software de clonado de imágenes de disco (Clonezilla, Norton Ghost, Acronis, etc,) que recupere el fichero de la red y escriba en el disco duro local, sin la necesidad de llevar un pendrive o discos ópticos, en un entorno donde cada vez figuran menos unidades de disco, que puedan desgastarse o deteriorarse. Por otro lado, complementario a la instalación del sistema operativo, sería posible incorporar para el arranque herramientas de diagnóstico y entornos o distribuciones *live* como Windows PE, MemCheck, Hiren's Boot cd, etc.

Una estimación al alza, de la implantación del presente proyecto, partiendo de cero, son aproximadamente 100 horas y una estimación de la instalación de un sistema operativo, configuración posterior e instalación de software adicional son entre 1 y 3 horas. Si se realiza el cálculo sobre un año, el punto a partir del cual la inversión de tiempo estaría amortizada es tras realizar 50 instalaciones o -aproximadamente- entre 2 y 4 al mes. Por tanto, en el caso que el parque informático de la empresa supere los 50-100 equipos, servidores y/o estaciones de trabajo, sería beneficiosa la implantación del proyecto.

Por el contrario si se replican los pasos descritos en el presente trabajo, la estimación de tiempo es inferior a un día laboral, por lo que la rentabilización del tiempo invertido en el despliegue y configuración es casi inmediata.

Dependiendo de la complejidad de instalación y la especialización de los equipos, en aras de minimizar la intervención manual, será posible automatizar en mayor o menor grado el proceso global y con diferente nivel de dificultad. No obstante, el objetivo del trabajo es proporcionar una estructura inicial del proceso de automatización sobre la que es posible añadir variaciones y ajustes -según necesidad- para su adaptación a cada caso de uso.

1.3 Riesgos

Uno de los principales riesgos identificados está derivado de la incertidumbre proveniente de ensamblar y trabajar con software ajeno y/o desconocido, sin saber si alguna de las soluciones disponibles cubrirá todos los requisitos, o si será necesario combinar varias aplicaciones que realicen funciones similares alcanzando un nivel de utilización de recursos subóptimo. Asimismo es posible que al tratarse de entornos heterogéneos no sea posible cubrir y adaptarse a las todas las configuraciones de arquitecturas y los diferentes tipos de servicios o roles de los servidores. Este riesgo, algo difícil de abordar, una posible solución sería limitar -inicialmente- las opciones de operación, por ejemplo, limitar según el tipo de arquitectura o sistema operativo, a unas determinadas opciones que pueden ser diferentes a las de otros conjuntos y gradualmente introducir dichas posibilidades según se realice la configuración del software. O, en casos más drásticos, realizar una configuración de los servicios a más bajo nivel, utilizando software más específico y personalizable, separando los grupos para utilizar diferentes aplicaciones. No obstante, la intención del proyecto -a pesar de la dificultad inicial que conlleve- es que sea fácilmente mantenible, y sea posible incorporar de manera sencilla nuevas versiones y configuraciones de los sistemas operativos que aparezcan a lo largo del tiempo, tras realizar las pruebas y validaciones pertinentes.

Otro posible riesgo es acerca de la escalabilidad, ya que es posible que en determinados momentos se lleven a cabo múltiples instalaciones de forma simultánea, resultando en que el servidor pueda convertirse en el "cuello de botella". Para compensar este riesgo, se deberán evaluar en cada caso el uso las necesidades de recursos dedicados, disponiendo de opciones de mejora tales como discos SSD, controladoras con caché o RAID para la mejora de la capacidad del acceso a disco, agregación de interfaces de red (Nic Teaming, bonding o LACP) para el ancho de banda de la red, además del aumento de la RAM y los recursos de CPU (número de cores) si fuera virtual o el procesador si se tratara de una máquina física.

A medida que transcurra el tiempo, desde la configuración inicial del proyecto, y las imágenes de los sistemas operativos se vuelvan más antiguas, la fase de verificación e instalación de actualizaciones implicará -cada vez- más tiempo, por lo cual es recomendable instalar y configurar un servidor de actualizaciones, como por ejemplo WSUS (Windows Server Update Services) en el caso de Microsoft o un repositorio/caché de paquetes en Linux, para agilizar esta fase y ahorrar ancho de banda.

Un riesgo adicional, de carácter general, es la pérdida del servicio WDS por un posible fallo del propio servidor, pero éste quedaría fuera del alcance del presente trabajo, al criterio del responsable de la implantación o responsable de dicho sistema informático, realizando las pertinentes copias de seguridad. El punto a favor del sistema es que, una vez finalizada la instalación, no queda relación alguna ni conexión necesaria con el servidor, evitando así una interdependencia de servicios si se decide retirar o realizar un mantenimiento.

Un posible riesgo a futuro, es el que podría llegar a aparecer una barrera de adaptación y/o compatibilidad con nuevos sistemas operativos, forzando -en el peor de los casos- a descartar alguna parte de la solución y la necesidad de rehacer la configuración y estructura de aplicaciones, o la imposibilidad de incorporar el nuevo sistema operativo hasta que aparecieran actualizaciones del software que resolvieran la compatibilidad. En este caso el riesgo es futuro, *a posteriori* de la implantación, por lo que -si ocurriera- podría demorarse la implantación del nuevo sistema operativo o abordarse un nuevo proyecto paralelo, a modo *ad-hoc* o con la posibilidad de reemplazo o complemento temporal del anterior.

1.4 Planificación del trabajo

Con las diferentes herramientas evaluadas se realizará la integración y las pruebas entre las diferentes fases, para después proceder a la configuración adaptada al escenario de trabajo.

Las configuraciones que no quedaran cubiertas con los programas y las especificaciones realizadas inicialmente, serían resueltas mediante la creación de scripts en el lenguaje que mejor se adapte a cada sistema operativo (powershell, bash, python, ...) para complementar y completar las tareas adicionales.

Los recursos necesarios serán: un servidor o máquina virtual para ejecutar los diferentes servicios o herramientas utilizadas durante el proceso y otras 2 máquinas para verificar el arranque en las diferentes arquitecturas.

Las principales fases y secciones del trabajo son:

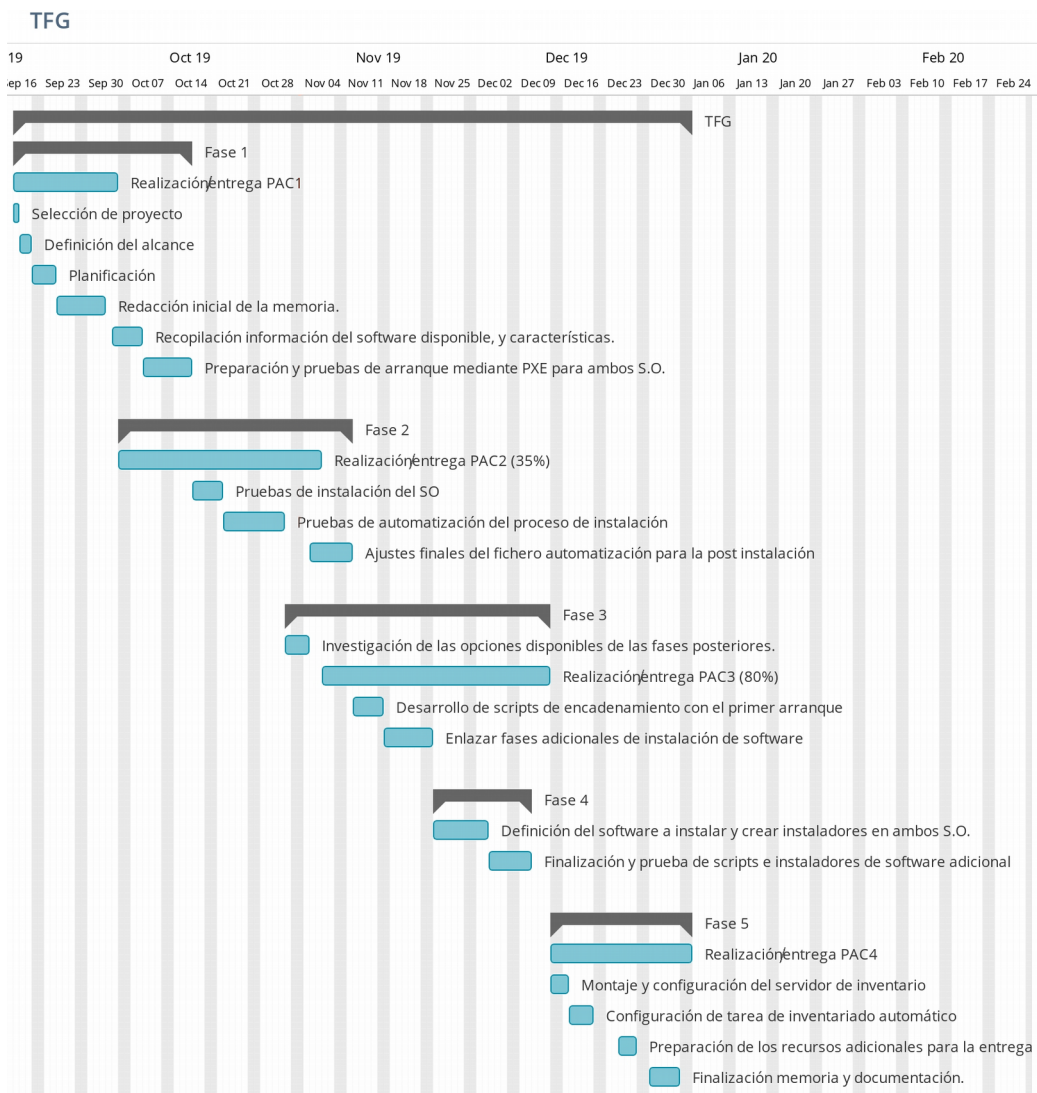
- 1- Arranque por red (DHCP + PXE)
- 2- Instalación del SO (Windows y/o Linux)
- 3- Configuración post-instalación, ajustes y programas del S.O.
- 4- Instalación de software externo al S.O. y configuraciones adicionales
- 5- Registro en herramienta de inventario OCS

Dichas fases se distribuirán en la siguiente planificación temporal:

Fecha	Días	Descripción de la fase
19/09/19	1	Selección de proyecto
21/09/19	2	Definición del alcance
25/09/19	4	Planificación
03/10/19	8	Redacción inicial de la memoria.
04/10/19	1	Entrega PAC1
09/10/19	5	Recopilación información del software disponible, y características
17/10/19	8	Preparación y pruebas de arranque mediante PXE para ambos S.O.
22/10/19	5	Pruebas de instalación del SO
01/11/19	10	Pruebas de automatización del proceso de instalación
05/11/19	4	Investigación de las opciones disponibles de las fases posteriores
07/11/19	2	Realización de la memoria al 35%
08/11/19	1	Entrega PAC2
15/11/19	7	Ajustes finales del fichero automatización para la post instalación
20/11/19	5	Desarrollo de scripts de encadenamiento con el primer arranque
28/11/19	8	Enlazar fases adicionales de instalación de software
07/12/19	9	Definición del software a instalar y crear instaladores en ambos S.O.
12/12/19	5	Realización de la memoria al 80%
13/12/19	1	Entrega PAC3
20/12/19	7	Finalización y prueba de scripts e instaladores de software adicional
23/12/19	3	Montaje y configuración del servidor de inventario
27/12/19	4	Configuración de tarea de inventariado automático de forma periódica
30/12/19	3	Preparación de los recursos adicionales para la entrega
04/01/20	5	Finalización memoria y documentación
05/01/20	1	Entrega PAC4

- PAC1: (16 días) Selección de proyecto, definición del alcance, planificación, redacción inicial de la memoria.
- PAC2: (35 días) Recopilación información del software disponible, y características. Pruebas de integración y configuración de las fases 1, 2. Pruebas iniciales de la fase 3. Investigación de las opciones disponibles de las fases posteriores. Realización de la memoria al 35%.
- PAC3: (35 días) Completar fase 3 (integrándola en las fases anteriores). Comienzo de las pruebas de fase 4, en base a la investigación anteriormente realizada. Realización de la memoria al 80%.
- PAC4: (23 días) Completar fases 4 y 5. Finalización memoria y documentación. Entrega de recursos adicionales.

Diagrama de Gantt:



1.5 Enfoque y método seguido

Como se ha expuesto anteriormente, tras una investigación inicial, en el mercado existen diferentes herramientas para conseguir el objetivo, pero ninguna de ellas cubre la totalidad del proceso que se desea llevar a cabo, por lo que se utilizará un conjunto de varias aplicaciones, configuradas para resolver las necesidades del presente trabajo.

Los requisitos de partida son que sea posible instalar tanto un sistema operativo Microsoft Windows Server como un Linux (Debian) de manera desatendida (parcial o completamente) y que se lleve a cabo una configuración posterior e instalación de programas en el menor tiempo posible, para poder disponer del servidor listo para su uso y/o configuración personalizada.

El trabajo se divide en varias partes (las distintas fases secuenciales del proceso) donde, tras la prueba y evaluación de las opciones disponibles, pros, contras y cómo se integran con los requisitos del proceso general, se describe el proceso de implementación de la configuración final desplegada.

Como ya se indicado anteriormente, existe una variedad de software alternativo, algunas opciones del cual se desglosan a continuación, comparando las funcionalidades y la decisión sobre éste.

- Servicios de clonación de imágenes de disco duro, por ejemplo CloneZilla, Norton Ghost, etc.
 - Ventajas: La mayoría de ellos soportan la transferencia de datos por red (desde un servidor central de almacenamiento) y así evitar llevar un disco duro hasta el equipo. Compatibilidad con múltiples sistemas operativos. Simplicidad de preparación, ejecución y restauración.
 - Desventajas: Nula posibilidad de personalización del resultado, más allá de tamaño de las particiones; copia los mismos datos que figuran en el origen. Baja posibilidad de automatización; hay que lanzar el proceso *in-situ* siguiendo los pasos de forma manual. Arranque desde medio físico, por lo que hay que desplazarse a insertar el disco o pendrive para el arranque de la aplicación. Necesidad de renombrar y personalizar cada máquina tras el clonado.
 - Opción descartada por las anteriores desventajas, ya que la finalidad es que el proceso sea lo mínimamente interactivo, permita la automatización y una mayor personalización del proceso y resultado.

- WDS y MDT: Suite de herramientas gratuitas para realizar imágenes de instalación y desplegar imágenes. WDS se utiliza para desplegar imágenes sobre PXE. MDT es una herramienta complementaria a WDS, para realizar imágenes de instalación. MDT se utiliza para implementar imágenes personalizarlas con secuencias de tareas, lo que lo hace más flexible a WDS. Complementa a WDS porque MDT necesita una imagen de arranque para comenzar. En lugar de tener la imagen de arranque en una memoria USB o DVD, puede implementarse sobre PXE con WDS.
 - Ventajas: Herramientas disponibles para habilitar en una instalación por defecto de Windows Server, incluyendo el servidor PXE. Interfaz gráfica para su configuración y uso, lo cual lo hace más accesible para cualquier administrador.
 - Desventajas: Requiere de un servidor, con una licencia Windows, para utilizar el servicio. Aunque, si en la red existen otros servidores Windows, puede solaparse con servidores de otros servicios pero, dependiendo de la carga que se planee aplicarle, será necesario escalar los recursos adecuadamente.
 - Opción adecuada para su configuración y uso en el proyecto.
- Microsoft System Center Configuration Manager (SCCM): Similar a WDS, no obstante, permite muchas más opciones de configuración para windows, pero requiere de un licenciamiento aparte. SCCM es una herramienta empresarial que incluye herramientas de implementación, administración de parches, distribución de software, etc. La parte de implementación de imágenes de SCCM es similar a MDT.
 - Ventajas: Sistema integral de gestión de configuración y despliegue para equipos Microsoft Windows.
 - Desventajas: Licencia adicional, mayor complejidad de uso y configuración.
 - Opción descartada por la necesidad de interoperabilidad con sistemas Linux, requerir licenciamiento adicional y la no necesidad de funciones de distribución de software.
- The Foreman: Herramienta de gestión de la configuración y servidor de arranque PXE, mediante interfaz web. Conjunto de aplicaciones configuradas sobre servidor Linux. Utiliza puppet para instalar, en el mismo servidor, los servicios necesarios, como DHCP, para realizar el PXE.
 - Ventajas: Servidor Linux con menor huella de consumo de recursos. Mejor interoperabilidad con sistemas Linux.
 - Desventajas: Falta de documentación, guías y manuales, por lo que la curva de aprendizaje es pronunciada. No trae configuración por defecto para el arranque PXE de Debian, y baja compatibilidad con arranque PXE en sistemas Windows.
 - Opción descartada por la baja compatibilidad y opciones respecto al arranque e instalación de sistemas Windows.

- Syslinux sobre WDS:
 - Ventajas: Permite arrancar kernels Linux desde PXE. Dispone de ficheros de configuración para crear un menú con las opciones que aparecerán en el arranque. Incompatibilidad con arranque UEFI.
 - Desventajas: Opciones de arranque limitadas (arranque tipo BIOS) y no es capaz de encadenar a otros ficheros de arranque, únicamente kernels e imágenes ISO.
 - Opción en la que se ha invertido más tiempo, para tratar de hacer funcionar ambos tipos de arranque (BIOS y UEFI), pero por problemas de compatibilidad con UEFI no era completamente funcional y se reemplazó por iPXE. El funcionamiento es similar, no obstante iPXE permite más opciones de encadenamiento tras el arranque.
- Configuración de servicios individuales manualmente:
 - Ventajas: ajuste completo y detallado de los parámetros de funcionamiento. Mayor abanico de opciones y modularidad.
 - Desventajas: Inversión de tiempo desproporcional, obteniendo pequeños avances tras un elevado o dificultoso trabajo. Resultados similares a otras herramientas, pero con una inversión mayor de esfuerzo. Dificultad de configurar y mantener. Necesidad de un elevado conocimiento sobre protocolos de red, arquitectura informática y sistemas operativos.
 - Opción descartada por su complejidad, tanto por la vertiente del montaje como la vertiente de administración.

1.6 Sumario de productos obtenidos

En un teórico escenario profesional, donde el presente trabajo fuera un proyecto real, el resultado sería uno o más servidores, bien sean físicos o virtuales, ejecutando los servicios necesarios configurados para el aportar el valor del proyecto.

En el caso del presente trabajo, el resultado será la propia memoria, detallando el procedimiento de instalación y configuración del servicio. En este caso no es posible realizar un script para llevar a cabo la configuración completa, de forma automatizada, ya que el proceso de configuración de los servicios requiere de múltiples acciones manuales, posee múltiples variables y se trata de un proceso que se implementa -generalmente- una única vez, se realizan los ajustes necesarios y no suele repetirse al completo, por lo que realizar un script que lo automatice sería contraproducente en tiempo y costes.

De manera adicional al procedimiento, se adjuntan -en el apartado anexos- los principales ficheros de configuración una vez ensamblados y probados, además de los scripts utilizados en la configuración post-instalación.

1.7 Breve descripción de los otros capítulos de la memoria

Como se ha esbozado anteriormente, cada subapartado del segundo capítulo se centra en una fase del proceso:

- Detalles del arranque por red mediante PXE
- La configuración inicial del servidor para WDS, que incluye la instalación y configuración del servicio de Windows
- Integración de iPXE en el servidor WDS
- Llamadas a WDS e instalación de Linux desde iPXE
- Enlace de la instalación con los ficheros de automatización
- Detalle de las configuraciones seleccionadas para los ficheros de automatización.

Finalmente, en el apartado 2.4 y 6 (anexos), se muestran ficheros de configuración y scripts, a modo de ejemplo, de la siguiente fase -que queda fuera del alcance del trabajo- donde se aplican configuraciones iniciales para posibilitar el acceso remoto y el inventariado de la máquina.

2. Resto de capítulos

2.1. Qué es el PXE

PXE, o Preboot eXecution Enviroment, es un entorno para el arranque y ejecución de software a través de red, independiente de los dispositivos de almacenamiento disponibles. La especificación de PXE fue desarrollada y publicada por Intel como parte del framework Wired for Management, en diciembre de 1998, haciendo uso de varios protocolos de red (IP, UDP, DHCP y TFTP) para la carga imágenes de arranque. Una vez ejecutada una imagen de arranque, ésta puede lanzar otros cargadores de arranque, por ejemplo, iniciar la instalación de un sistema operativo, cargar una aplicación o incluso la carga un sistema operativo completo. Posteriormente, en 2004, Intel desarrolló EFI (Extensible Firmware Interface) como reemplazo de BIOS en las nuevas arquitecturas, incluyendo PXE como parte del firmware, no obstante en 2005 cesó el desarrollo y se unió al Unified EFI Forum para el desarrollo de UEFI, que acabó siendo el reemplazo de BIOS e incluye soporte PXE.

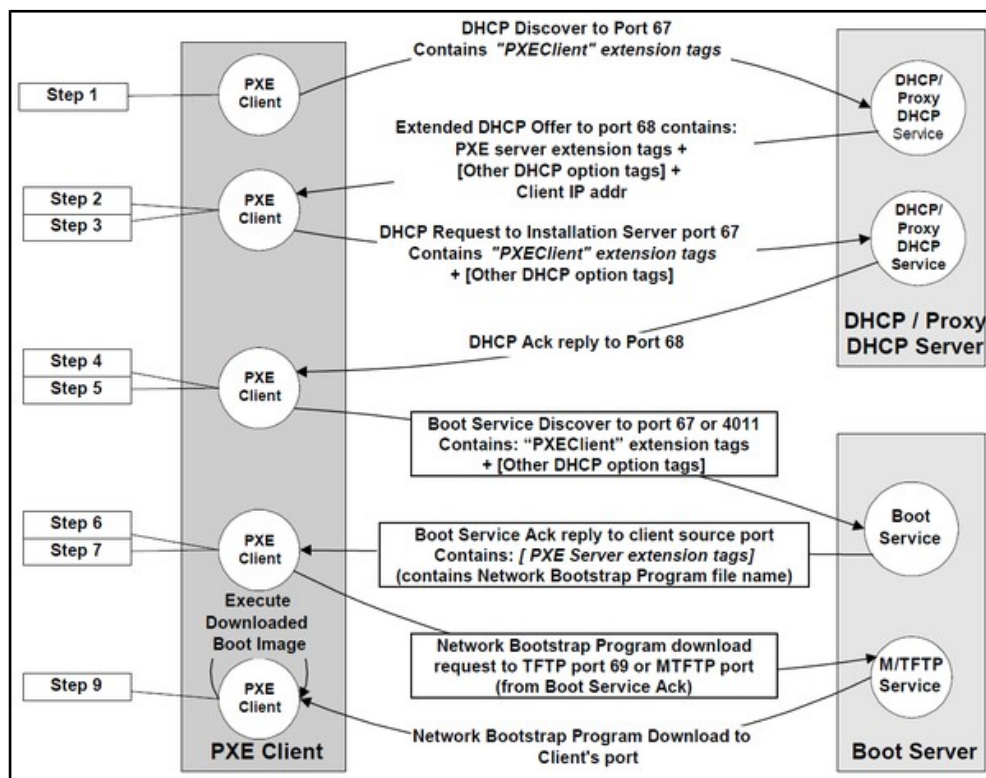
El protocolo PXE consiste en una combinación de los protocolos DHCP y TFTP con mejoras en ambos. DHCP es utilizado para localizar el servidor de arranque apropiado, con TFTP se descarga el programa inicial de bootstrap y archivos adicionales.

El concepto de ProxyDHCP aparece cuando, debido a las restricciones de los entornos corporativos, es difícil introducir parámetros y configuraciones adicionales de forma dinámica en los servidores DHCP, y se procede a separar las funciones: gestión de direcciones IP y gestión de servidores TFTP con la imagen de arranque. En estos casos la petición DHCP recibiría dos respuestas que servirían para realizar el arranque PXE. [1],[2],[3]

2.2. Arranque por red (PXE)

Para iniciar una sesión de arranque con PXE el firmware (BIOS) envía un paquete de tipo DHCPDISCOVER extendido con opciones específicas de PXE al puerto 67/UDP (puerto estándar del servicio DHCP). Estas opciones indican que el firmware es capaz de manejar PXE. Los servidores DHCP estándar (no habilitados para PXE) podrán responder con un DHCPOFFER regular que contenga información de red (es decir, dirección IP) pero no los parámetros específicos de PXE. Un cliente PXE no podrá arrancar si sólo recibe una respuesta de un servidor DHCP no habilitado para PXE.

En la fase de arranque, el cliente PXE (firmware de la BIOS) trata de encontrar un servicio de redirección/proxy PXE en la red para recabar información sobre los servidores de arranque PXE disponibles. Tras analizar la respuesta, el firmware solicitará, al servidor de arranque correspondiente, la ruta de un *network bootstrap program* (NBP), programa de arranque inicial, lo cargará en la memoria RAM, mediante una descarga TFTP, y lo ejecutará. Los NBPs son sólo el primer eslabón en el proceso de la cadena de arranque y generalmente solicitan a través de TFTP un pequeño conjunto de archivos complementarios para poder cargar un ejecutable de sistema operativo minimalista (es decir, WindowsPE, o un kernel+initrd básico de Linux). En este punto, las instrucciones restantes necesarias para arrancar o instalar un sistema operativo completo no se proporcionan a través de TFTP, sino utilizando un protocolo de transferencia robusto (como HTTP, CIFS o NFS).
[1],[2],[3],[4]



2.3. Configuración del entorno de arranque

La herramienta elegida para realizar esta función es Microsoft Windows Deployment Server (en adelante WDS), en primer lugar por la facilidad de uso gracias a su interfaz gráfica e integración con el sistema operativo Windows y en segundo lugar por encontrar dificultades con las integraciones en otras soluciones para el despliegue del S.O. Windows.

En primer lugar para comenzar con la configuración del servicio es necesario un servidor con Microsoft Windows Server, en nuestro caso partimos de una máquina virtual con Windows Server 2019. Los requisitos de la misma son modestos ya que será la única función que realizará:

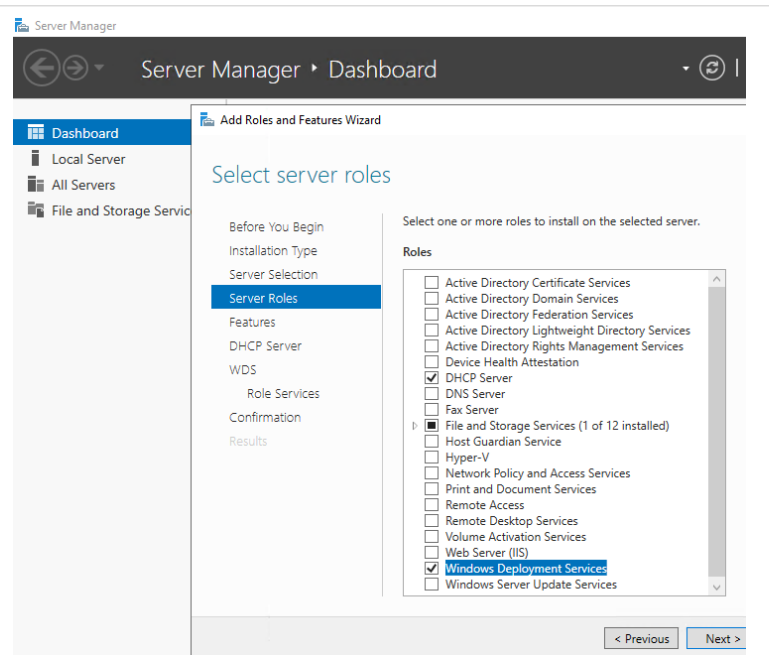
- Disco Duro: 60-80 GB
- Memoria Ram: 4GB
- CPU: 2 o más cores
- Red: 1 interfaz, con IP fija

Desde la versión Server 2016, el servidor de WDS puede estar, o no, en dominio, no obstante para la configuración del servicio es irrelevante dicho parámetro, por lo que no se entra en detalle.

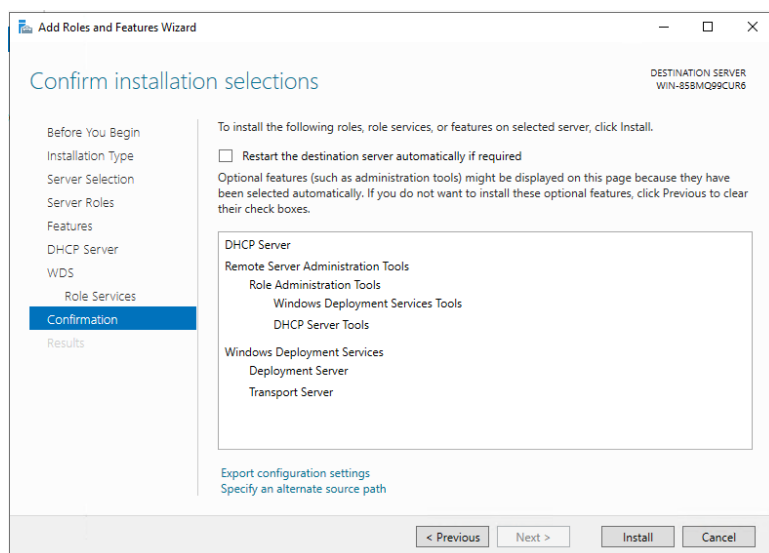
2.3.1 Instalación de los servicios necesarios

A continuación se describen los pasos necesarios para la configuración del servicio WDS en un servidor Windows.

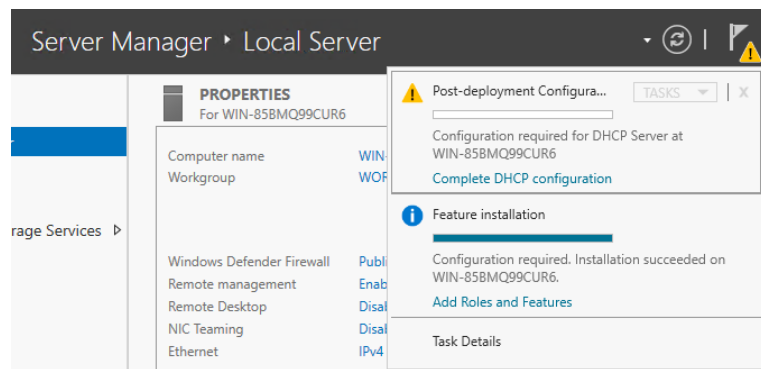
Procedemos a instalar el servicio DHCP y Windows Deployment Services, bien desde powershell o bien desde el administrador del servidor: "Server Manager" --> "Add Roles and Features", donde deberemos marcar en la sección "Server Roles" ambos servicios.



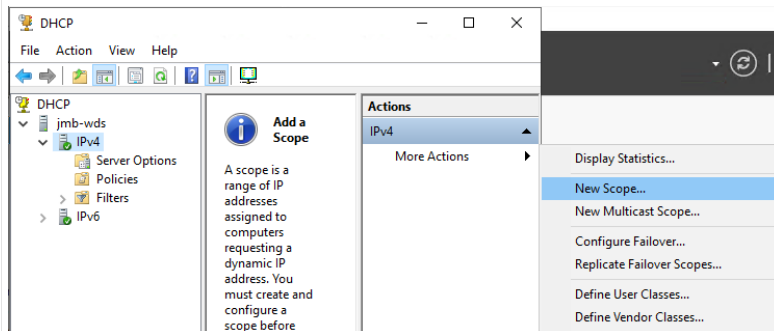
Al finalizar, será necesario completar la configuración del servicio DHCP, desde el mismo administrador del servidor.



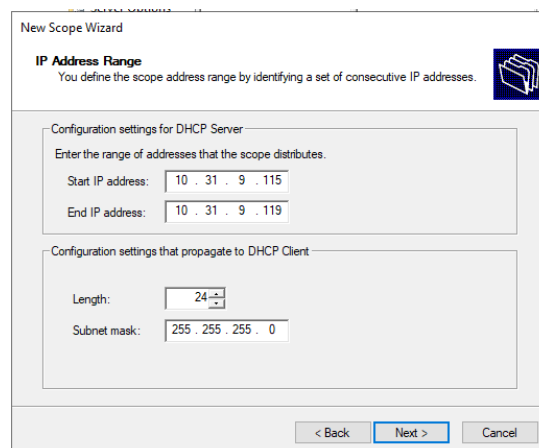
El proceso de configuración es trivial, procediendo a confirmar la configuración sugerida automáticamente en el siguiente paso (*Complete DHCP configuration*).



El siguiente paso es, desde el administrador del servicio DHCP, crear un *scope* ajustado nuestra subred (ej. 10.x.x.x/24), definiendo el rango de direcciones IPs y el gateway.



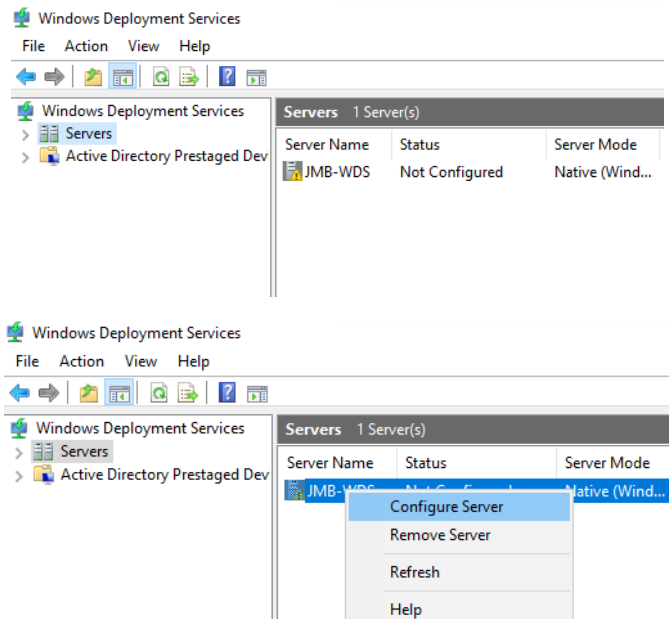
Al finalizar, dependiendo de si el servidor se ha unido al dominio, se deberá autorizar el servicio DHCP, desde el menú, mediante la cuenta de administrador de dominio.



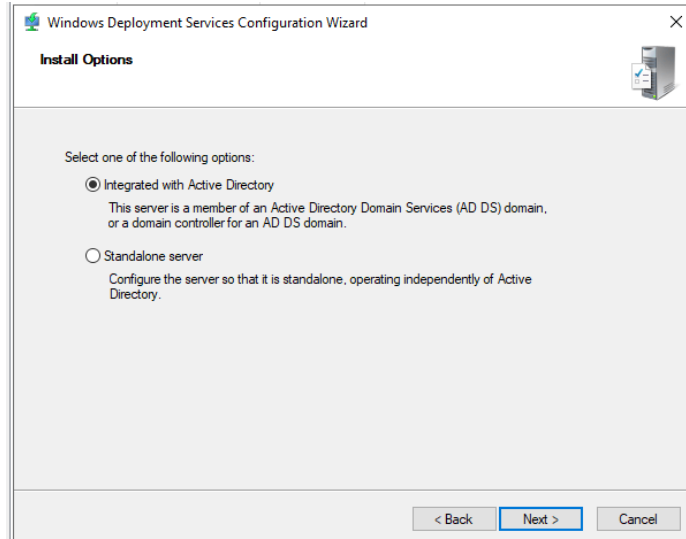
Una vez creado el scope, se configura el servicio WDS.

Desde su consola nos indica que el servidor no está configurado, y mediante las opciones del botón derecho lanzamos el asistente de configuración.

Durante el asistente se configuran las siguientes opciones:



- Si operará con el directorio activo (en caso de estar el servidor a dominio se puede utilizar la opción integrada).



- La ruta de los ficheros del servicio.

- La configuración del servicio DHCP (deben activarse ambas opciones de la imagen).

Proxy DHCP Server

If Dynamic Host Configuration Protocol (DHCP) is running on this server, check both of the following check boxes and use DHCP tools to add appropriate PXE options to all DHCP and DHCPv6 scopes.

If a non-Microsoft DHCP server is running on this server, then check the first box and manually configure DHCP option 60 and DHCPv6 Vendor Class for Proxy DHCP.

The Windows Deployment Services Configuration Wizard detected Microsoft DHCP service running on the server. Please select from the following options:

- Do not listen on DHCP and DHCPv6 ports
- Configure DHCP options for Proxy DHCP

-El comportamiento en las respuestas (debe habilitarse la opción de responder a todas las peticiones de cliente, necesario para una fase posterior).

Select one of the following options:

- Do not respond to any client computers
- Respond only to known client computers
- Respond to all client computers (known and unknown)

Require administrator approval for unknown computers. When you select this option, you must approve the computers using the Pending Devices node in the snap-in. Approved computers will be added to the list of prestaged clients.

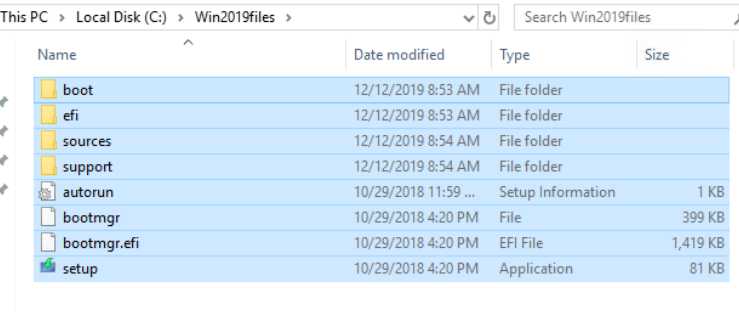
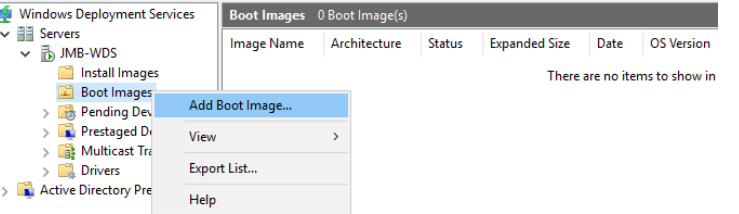
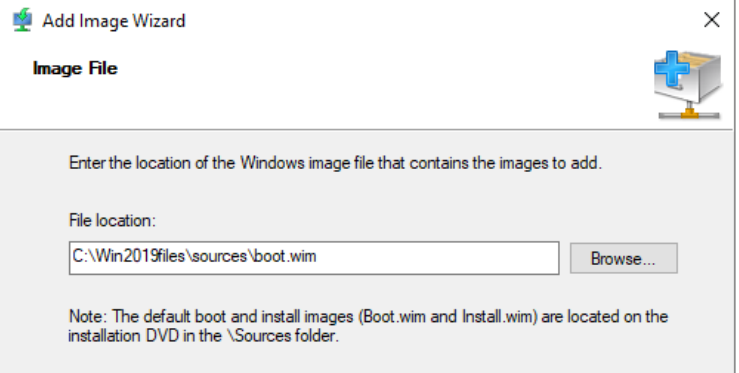
To configure this server, click Next.

A pesar de que al finalizar el asistente indique un error, de no haber podido arrancar correctamente, se puede proceder al arranque manual desde el administrador.

The image shows two screenshots related to Windows Deployment Services (WDS). The top screenshot is a configuration dialog box titled "Configuring Windows Deployment Services...". It displays "Starting Windows Deployment Services" with a green progress bar. Below the progress bar, a message states: "The service did not respond to the start or control request in a timely fashion." The bottom screenshot shows the "Windows Deployment Services" console in the Windows Server environment. The "Servers" folder is expanded, showing a server named "JMB-WDS". A context menu is open over the server, with the "All Tasks" option selected, which has opened a sub-menu containing "Start", "Stop", and "Restart".

2.3.2 Configuración del servicio WDS para imágenes Windows

El siguiente paso es probar el correcto funcionamiento y el arranque. Desde el administrador de WDS se importan las imágenes de arranque e instalación. Éstos son archivos ".wim" localizados en el DVD de instalación, por lo que se puede montar la ISO si se trata de una máquina virtual o descomprimirla en una carpeta del disco duro. En una fase posterior serán necesarios dichos archivos por lo que será mejor realizar la extracción de ficheros.

<p>En primer lugar se copian los ficheros del DVD al disco duro.</p>	 <table border="1"><thead><tr><th>Name</th><th>Date modified</th><th>Type</th><th>Size</th></tr></thead><tbody><tr><td>boot</td><td>12/12/2019 8:53 AM</td><td>File folder</td><td></td></tr><tr><td>efi</td><td>12/12/2019 8:53 AM</td><td>File folder</td><td></td></tr><tr><td>sources</td><td>12/12/2019 8:54 AM</td><td>File folder</td><td></td></tr><tr><td>support</td><td>12/12/2019 8:54 AM</td><td>File folder</td><td></td></tr><tr><td>autorun</td><td>10/29/2018 11:59 ...</td><td>Setup Information</td><td>1 KB</td></tr><tr><td>bootmgr</td><td>10/29/2018 4:20 PM</td><td>File</td><td>399 KB</td></tr><tr><td>bootmgr.efi</td><td>10/29/2018 4:20 PM</td><td>EFI File</td><td>1,419 KB</td></tr><tr><td>setup</td><td>10/29/2018 4:20 PM</td><td>Application</td><td>81 KB</td></tr></tbody></table>	Name	Date modified	Type	Size	boot	12/12/2019 8:53 AM	File folder		efi	12/12/2019 8:53 AM	File folder		sources	12/12/2019 8:54 AM	File folder		support	12/12/2019 8:54 AM	File folder		autorun	10/29/2018 11:59 ...	Setup Information	1 KB	bootmgr	10/29/2018 4:20 PM	File	399 KB	bootmgr.efi	10/29/2018 4:20 PM	EFI File	1,419 KB	setup	10/29/2018 4:20 PM	Application	81 KB
Name	Date modified	Type	Size																																		
boot	12/12/2019 8:53 AM	File folder																																			
efi	12/12/2019 8:53 AM	File folder																																			
sources	12/12/2019 8:54 AM	File folder																																			
support	12/12/2019 8:54 AM	File folder																																			
autorun	10/29/2018 11:59 ...	Setup Information	1 KB																																		
bootmgr	10/29/2018 4:20 PM	File	399 KB																																		
bootmgr.efi	10/29/2018 4:20 PM	EFI File	1,419 KB																																		
setup	10/29/2018 4:20 PM	Application	81 KB																																		
<p>Tras la copia , se añade al WDS la imagen de arranque.</p>																																					
<p>Ha de seleccionarse el fichero boot.wim.</p>	 <p>Enter the location of the Windows image file that contains the images to add.</p> <p>File location: <input type="text" value="C:\Win2019files\sources\boot.wim"/> <input data-bbox="1173 1568 1276 1601" type="button" value="Browse..."/></p> <p>Note: The default boot and install images (Boot.wim and Install.wim) are located on the installation DVD in the \Sources folder.</p>																																				

Proporcionar un nombre, revisar la arquitectura importada y confirmar el proceso para su finalización.

Enter a name and description for the following image:
'Microsoft Windows Setup (x64)'

Image name:

Image description:

Image architecture:
x64

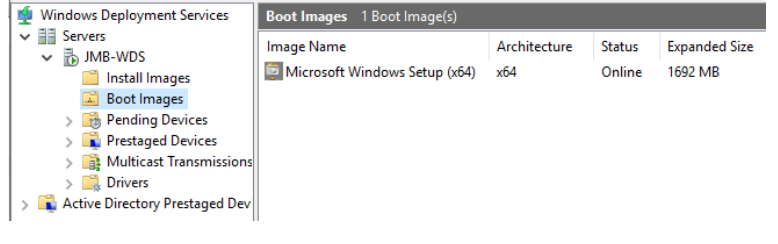


Image Name	Architecture	Status	Expanded Size
Microsoft Windows Setup (x64)	x64	Online	1692 MB

Una vez finalizada la importación, se añade la imagen o imágenes de instalación del sistema operativo de manera parecida al anterior paso.

El asistente requiere crear un grupo para dichas imágenes.

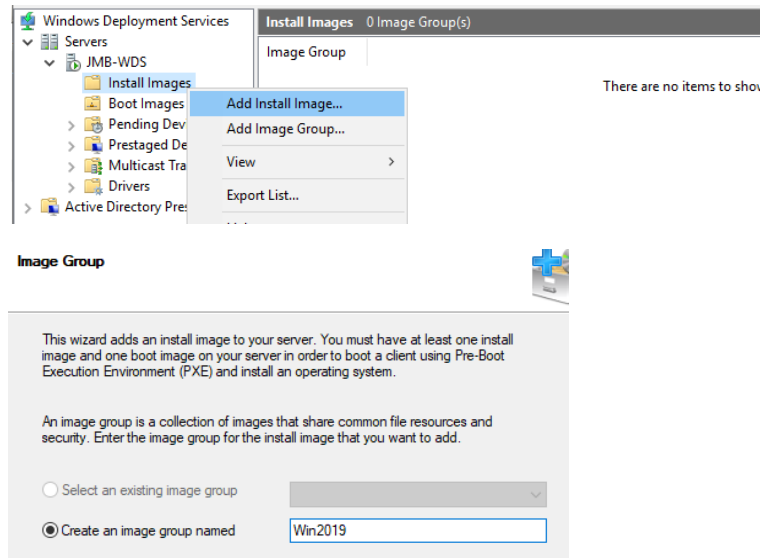


Image Group

This wizard adds an install image to your server. You must have at least one install image and one boot image on your server in order to boot a client using Pre-Boot Execution Environment (PXE) and install an operating system.

An image group is a collection of images that share common file resources and security. Enter the image group for the install image that you want to add.

Select an existing image group

Create an image group named

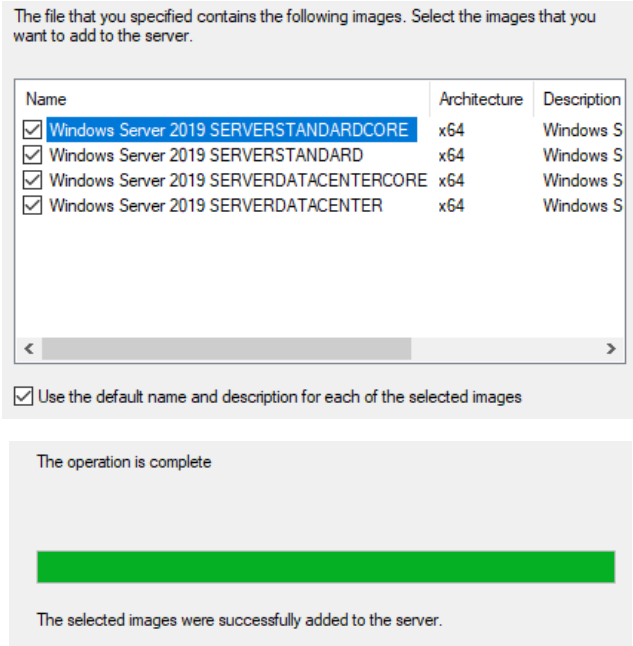
Tras darle un nombre al grupo se localiza y abre el fichero install.wim para su importación.

Enter the location of the Windows image file that contains the images to add.

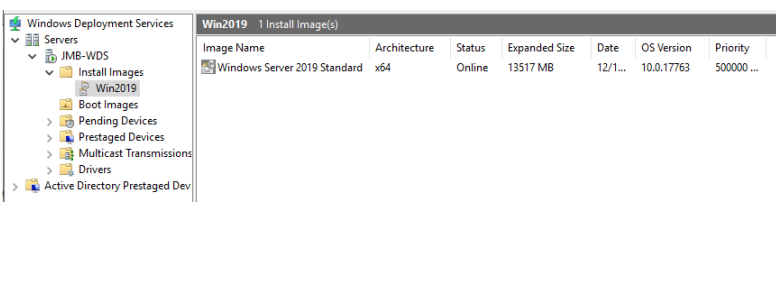
File location:

Note: The default boot and install images (Boot.wim and Install.wim) are located on the installation DVD in the \Sources folder.

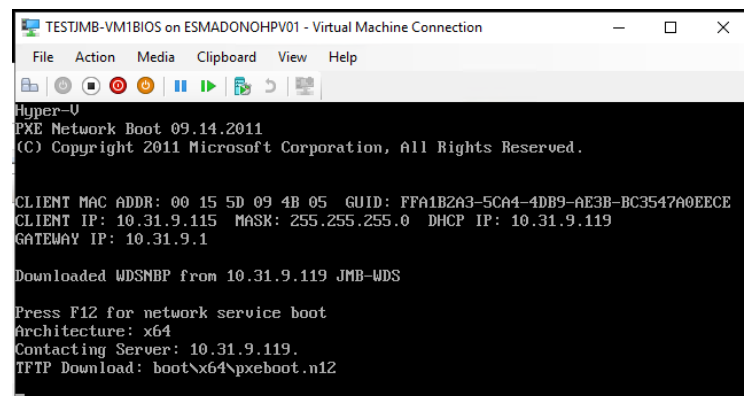
El siguiente paso permite elegir las versiones y arquitecturas a importar. En el presente caso se utilizará únicamente la versión SERVERSTANDARD que corresponde a la version Standard de Windows Server 2019, con la interfaz. En caso de desmarcar la casilla "Use the default name..." ofrece un paso más de renombrar la imagen.



A partir de la configuración actual ya es posible arrancar desde la red tanto con una máquina con arranque BIOS como UEFI, ambas en arquitectura x64.



En una máquina virtual de prueba, tras configurar el arranque por red como primera opción, durante el arranque, la máquina virtual hace la petición DHCP inicial, a la cual el servidor DHCP le responde adecuadamente para encontrar el servidor WDS y descargarse la imagen de arranque.



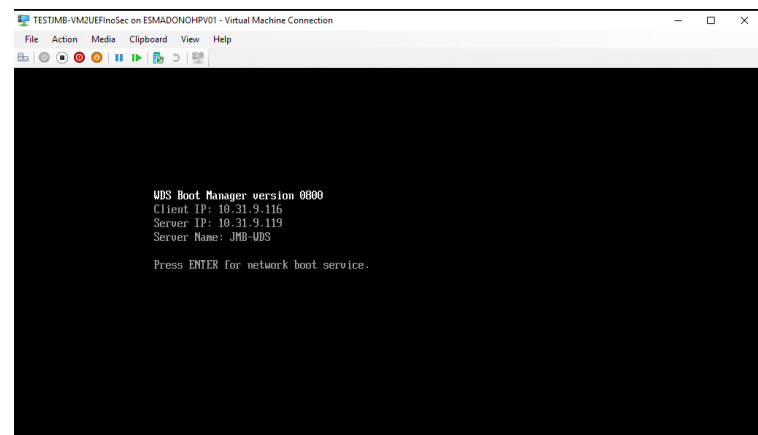
En la captura de paquetes se pueden apreciar los detalles del proceso de arranque PXE, indicados en 2.2 y 2.3, mediante las opciones adicionales del protocolo DHCP, en la respuesta.

No.	Time	Source	sMAC	dMAC	Destination	Protoc	Length	Info
1	0.000	0.0.0.0	Microsoft_09:4b:05	Broadcast	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x5e094b05
2	3.955	0.0.0.0	Microsoft_09:4b:05	Broadcast	255.255.255.255	DHCP	590	DHCP Request - Transaction ID 0x5e094b05
3	3.955	Microsoft_09:4b:05	Microsoft_09:4b:05	Broadcast	Broadcast	ARP	60	Who has 10.31.9.119? Tell 10.31.9.115
4	3.955	Microsoft_09:4b:05	Microsoft_09:4b:05	Microsoft_09:4b:05	Microsoft_09:4b:05	ARP	42	10.31.9.119 is at 00:15:5d:09:4b:0b
5	3.956	10.31.9.115	Microsoft_09:4b:05	Microsoft_09:4b:05	10.31.9.119	DHCP	590	proxyDHCP Request - Transaction ID 0x5e094b05
6	3.957	10.31.9.119	Microsoft_09:4b:05	Microsoft_09:4b:05	10.31.9.115	DHCP	387	proxyDHCP ACK - Transaction ID 0x5e094b05
7	3.977	10.31.9.115	Microsoft_09:4b:05	Microsoft_09:4b:05	10.31.9.119	TFTP	78	Read Request, File: boot\x86\wdsnbp.com, Tran...
8	3.978	10.31.9.119	Microsoft_09:4b:05	Microsoft_09:4b:05	10.31.9.115	TFTP	56	Option Acknowledgement, tsize=30832

```

> Bootp flags: 0x0000 (Unicast)
Client IP address: 10.31.9.115
Your (client) IP address: 0.0.0.0
Next server IP address: 10.31.9.119
Relay agent IP address: 0.0.0.0
Client MAC address: Microsoft_09:4b:05 (00:15:5d:09:4b:05)
Client hardware address padding: 00000000000000000000
Server host name: JMB-WDS
Boot file name: boot\x86\wdsnbp.com
Magic cookie: DHCP
> Option: (54) DHCP Server Identifier (10.31.9.119)
> Option: (97) UUID/GUID-based Client Identifier
  > Option: (60) Vendor class identifier
    Length: 0
    Vendor class identifier: PXEClient
  > Option: (93) Client System Architecture
    Length: 2
    Client System Architecture: IA x86 PC (0)
  
```

En el caso de la máquina virtual con arranque UEFI se puede observar que el fichero que descarga por TFTP es distinto (terminado en .efi) y la arquitectura es distinta, tipo 7 (en el caso de BIOS es 0).

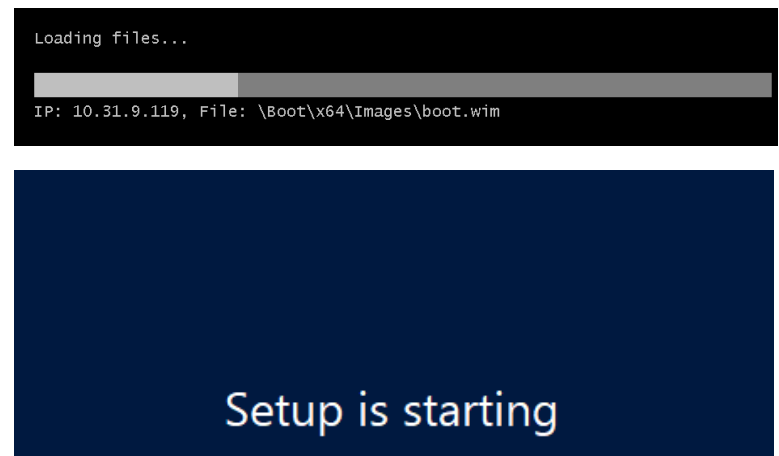


No.	Time	Source	sMAC	dMAC	Destination	Protoc	Length	Info
1	0.000	0.0.0.0	Microsoft_09:4b:07	Broadcast	255.255.255.255	DHCP	389	DHCP Discover - Transaction ID 0xa5e46742
2	0.054	::	Microsoft_09:4b:07	IPv6mcast_ff:09::	ff02::1:ff09:4b07	ICML	86	Multicast Listener Report
3	0.354	::	Microsoft_09:4b:07	IPv6mcast_ff:09::	ff02::1:ff09:4b07	ICML	78	Neighbor Solicitation for fe80::215:daff:fe99::
4	3.974	0.0.0.0	Microsoft_09:4b:07	Broadcast	255.255.255.255	DHCP	401	DHCP Request - Transaction ID 0xa5e46742
5	3.977	Microsoft_09:4b:07	Microsoft_09:4b:07	Broadcast	Broadcast	ARP	42	Who has 10.31.9.119? Tell 10.31.9.116
6	3.977	Microsoft_09:4b:07	Microsoft_09:4b:07	Microsoft_09:4b:07	Microsoft_09:4b:07	ARP	42	10.31.9.119 is at 00:15:5d:09:4b:0b
7	3.977	10.31.9.116	Microsoft_09:4b:07	Microsoft_09:4b:07	10.31.9.119	DHCP	389	proxyDHCP Request - Transaction ID 0xb416daaa
8	3.979	10.31.9.119	Microsoft_09:4b:07	Microsoft_09:4b:07	10.31.9.116	DHCP	391	proxyDHCP ACK - Transaction ID 0xb416daaa
9	4.974	10.31.9.116	Microsoft_09:4b:07	Microsoft_09:4b:07	10.31.9.119	TFTP	92	Read Request, File: boot\x64\wdsnbp.efi, Tra...
10	5.051	10.31.9.119	Microsoft_09:4b:07	Microsoft_09:4b:07	10.31.9.116	TFTP	71	Option Acknowledgement, blksize=1482, tsize=...
11	5.051	10.31.9.116	Microsoft_09:4b:07	Microsoft_09:4b:07	10.31.9.119	TFTP	72	Error Code, Code: Option negotiation failed, ...
12	5.052	10.31.9.116	Microsoft_09:4b:07	Microsoft_09:4b:07	10.31.9.119	TFTP	84	Read Request, File: boot\x64\wdsnbp.efi, Tra...
13	5.052	10.31.9.119	Microsoft_09:4b:07	Microsoft_09:4b:07	10.31.9.116	TFTP	57	Option Acknowledgement, blksize=1482
14	5.052	10.31.9.116	Microsoft_09:4b:07	Microsoft_09:4b:07	10.31.9.119	TFTP	46	Acknowledgement, block: 0

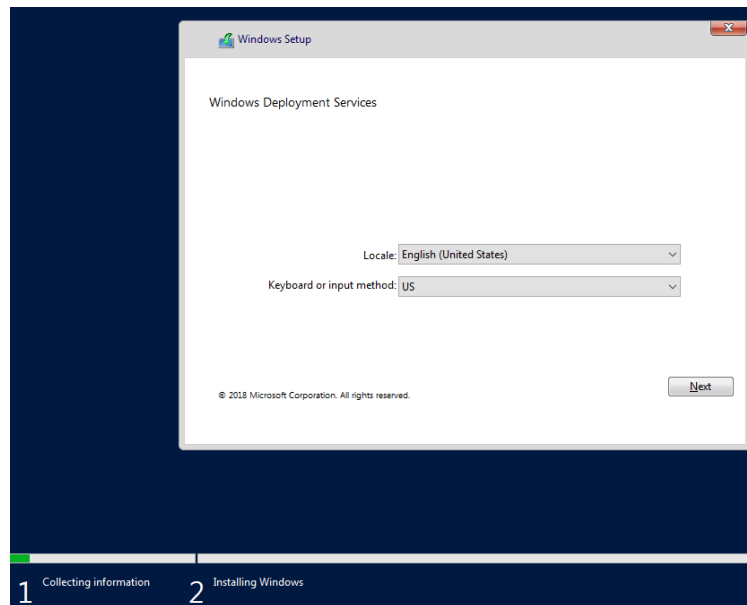
```

> Option: (97) UUID/GUID-based Client Identifier
> Option: (94) Client Network Device Interface
> Option: (93) Client System Architecture
  Length: 2
  Client System Architecture: EFI x64 (7)
> Option: (60) Vendor class identifier
  Length: 32
  Vendor class identifier: PXEClient:Arch:00007:UNDI:003000
> Option: (255) End
  
```

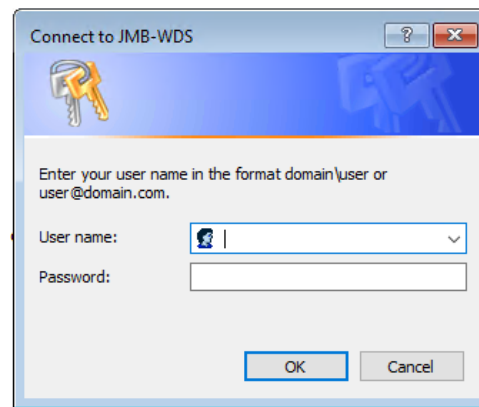
Los pasos que preceden al anterior, en ambos casos, es el proceso de instalación de Windows.



En la siguiente pantalla de instalación que aparece, tras la introducción del idioma y configuración del teclado, solicita las credenciales de acceso al recurso compartido donde se encuentran los datos de la imagen de instalación (que no ha descargado por TFTP).



Los ficheros de los siguientes pasos de la instalación se descargan mediante netbios, lo que permite un mejor rendimiento en la transferencia. Por tanto, **es necesario crear un usuario** (puede ser local del servidor WDS o del dominio, sin privilegios de administrador) para acceder a los ficheros restantes y continuar con la instalación.



2.3.3 Automatización de la instalación de Windows

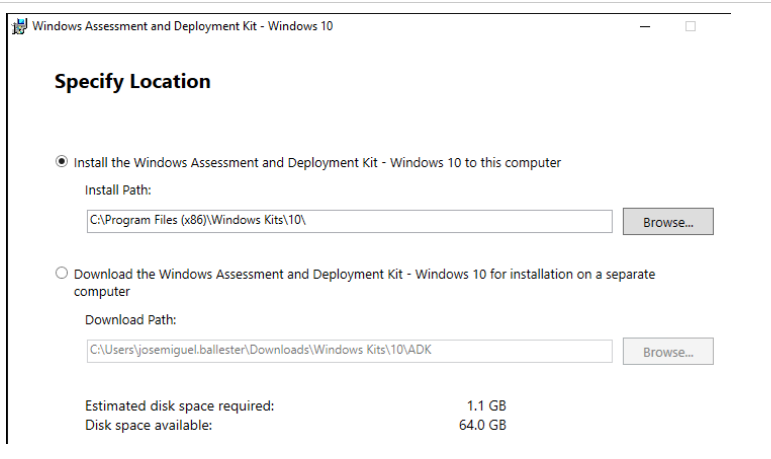
Para la automatización del proceso de instalación y determinadas configuraciones (tipo Sysprep) Microsoft utiliza un fichero XML, llamado answer file [5]. Este fichero puede encontrarse en diferentes ubicaciones según como se lleve a cabo la integración entre el proceso y el fichero.

Las ubicaciones más habituales son: %WINDIR%\Panther, %WINDIR%\System32\Sysprep, o en la carpeta \Sources de un medio de instalación.

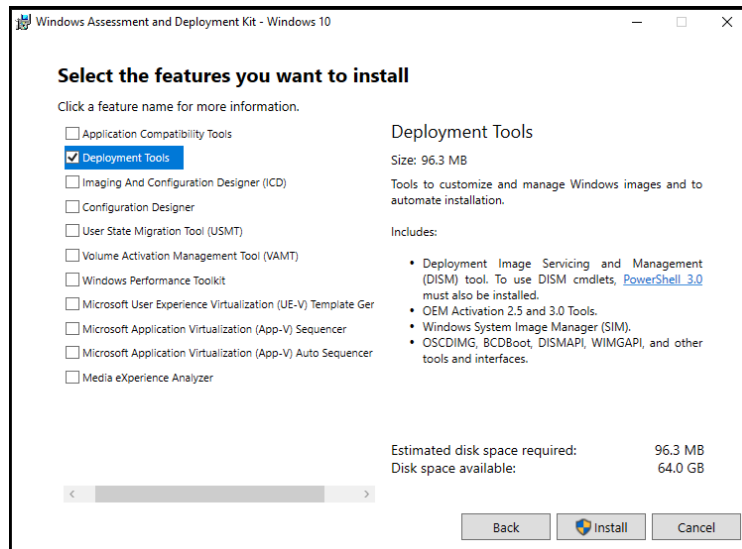
Para la creación de dicho fichero se utilizará la herramienta propia de Microsoft: Windows ADK [6] (Windows Assessment and Deployment Kit). Tras la instalación y configuración inicial, se crearán dos ficheros, el primero con las credenciales de acceso al servidor de WDS, y el segundo para personalizar cada una de las imágenes de instalación que dispongamos.

Existe un bug en el funcionamiento de la última versión 1903 en arquitectura de 64 bits, y el procedimiento correcto de instalación pasa por instalar la versión 1809, generar el fichero de configuración (creando automáticamente el catálogo de la imagen de instalación), desinstalar completamente la versión, reiniciar, instalar la versión 1903 e instalar el parche que ofrece Microsoft junto con la descarga. De esta manera la aplicación carga correctamente el fichero de configuración y no falla a generar el catálogo.

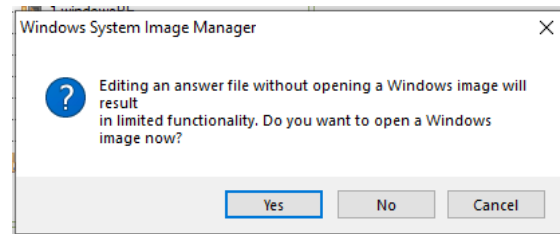
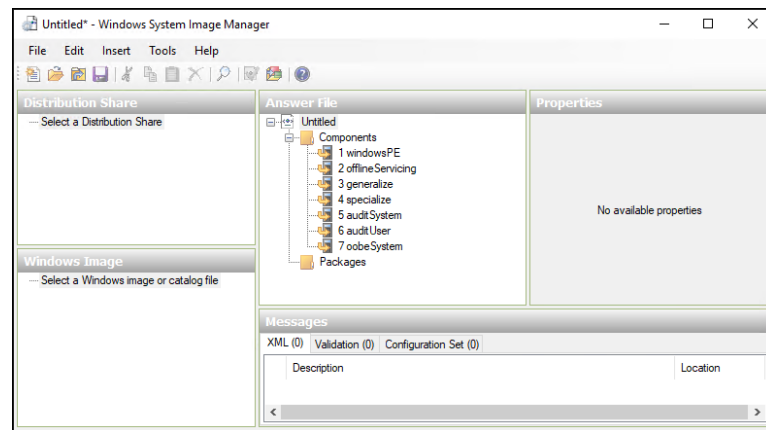
La instalación del software Windows ADK es trivial.



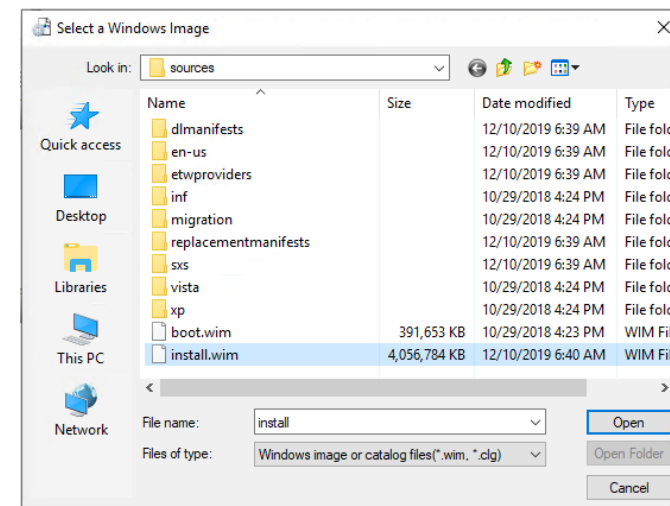
El único software necesario del listado que se ofrece preseleccionado, es **Deployment Tools**.



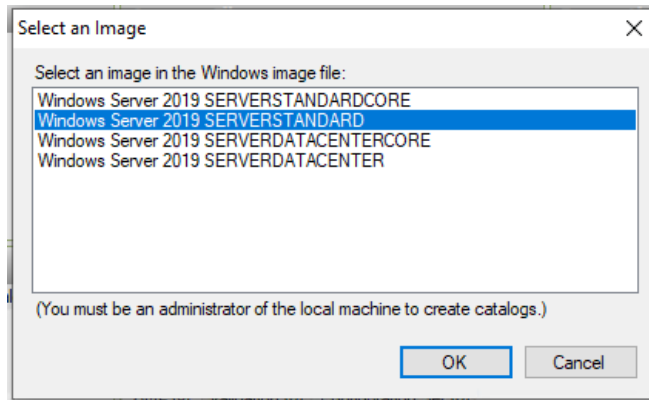
Una vez instalado, desde el programa principal, en la ventana inicial, al crear un nuevo fichero de respuestas, sugiere la apertura de una imagen de Windows.



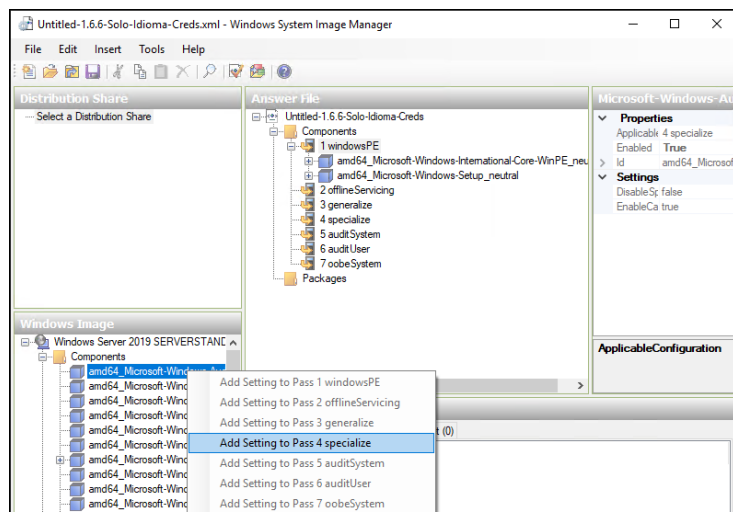
Seleccionar el archivo **install.wim** del DVD/ISO copiado.



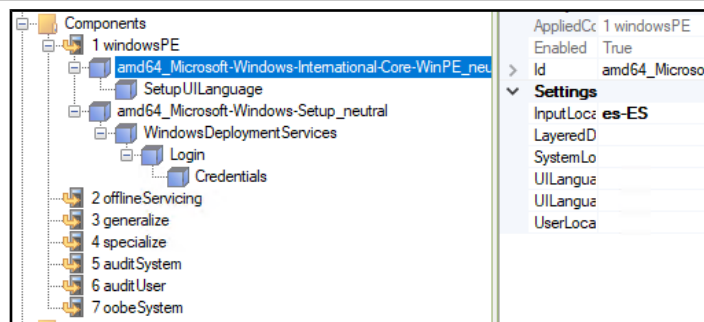
Y posteriormente seleccionar la imagen de instalación (versión de Windows) que se desea importar y se creará automáticamente el catálogo de ésta.



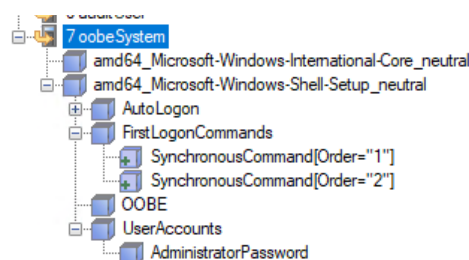
Para añadir configuraciones al fichero, se realiza desde la región inferior izquierda, del listado que corresponde a diferentes apartados de la configuración del sistema operativo. Dependiendo del tipo de configuración, el menú contextual, permitirá añadirlo en unas fases de la instalación u otras.



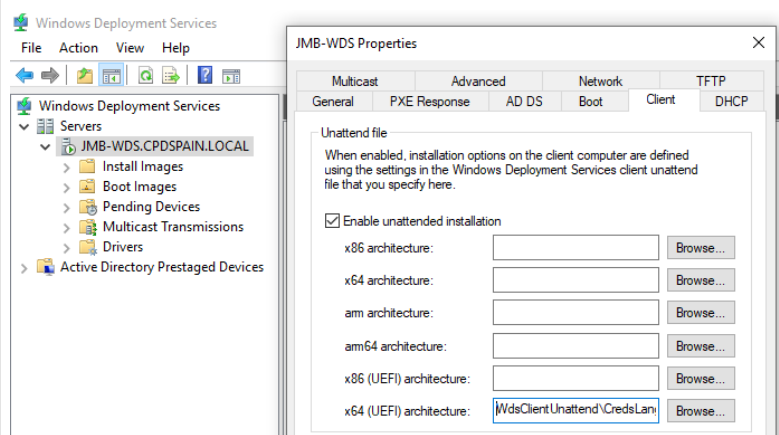
Para el arranque sin solicitud de credenciales, será suficiente añadir en un fichero WDS/Login y SetupUILanguage en la fase 1, adecuándolo a nuestra configuración.



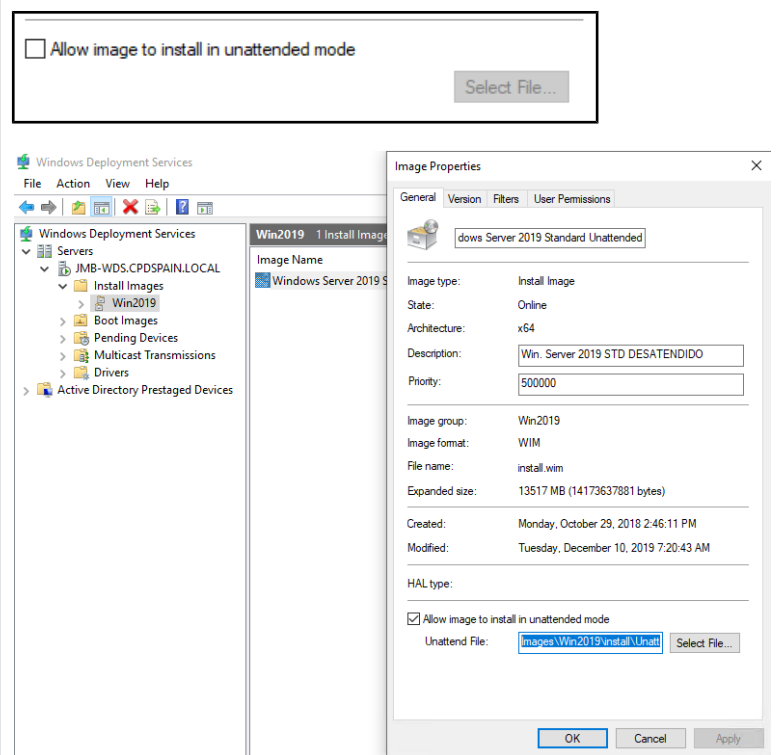
En otro fichero de configuración se insertarán, en el apartado 7 -cuando el sistema arranca tras la instalación-, las configuraciones y comando que se llevarán a cabo. Por ejemplo: idioma del sistema operativo, contraseña del administrador, etc.



Para aplicar dichos ficheros de configuración al servidor WDS, se pueden efectuar los siguientes pasos. Se copia el primero de ellos a la carpeta del servicio WDS (C:\RemoteInstall\Wds ClientUnattend) y en las propiedades del servidor, pestaña Client, se asigna para la/s arquitectura/s deseada/s.



Para el segundo fichero, el de instalación, se asigna a una imagen de instalación desde las propiedades de la misma, tras activar la opción que lo permite. Por tanto, para disponer de diferentes configuraciones de instalación es necesario añadir tantas imágenes de instalación como configuraciones.



2.3.4 Configuración y arranque del menú iPXE

Tras verificar que la configuración anterior funciona para las arquitecturas deseadas, el siguiente paso es implementar la posibilidad de instalación de sistemas operativos Linux sobre un software (WDS) que a priori no dispone de las opciones para ello.

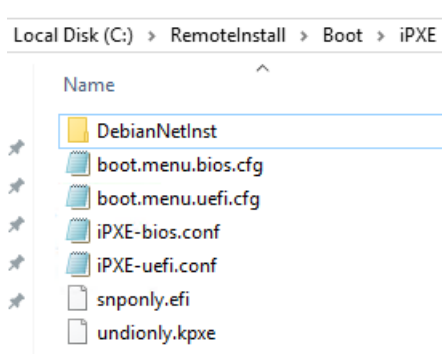
Esta fase ha sido la más conflictiva y en la que más tiempo se ha invertido por motivos de incompatibilidad entre arquitecturas, software existente/disponible y configuraciones posibles. Como bien se ha indicado anteriormente, existen diferentes programas que funcionan correctamente en determinados escenarios, pero no a una escala global, por lo que ha sido necesario invertir tiempo en pruebas y búsqueda de nuevas soluciones tras descartar aquellas que no cumplían con los requisitos, entre las que se incluyen syslinux (no funciona correctamente en UEFI y no carga otros bootloaders) y grub (no ha sido posible hacer que descargue el fichero de configuración grub.cfg a través de TFTP).

Finalmente, mediante los binarios de iPXE es posible cubrir todos los escenarios de los requisitos iniciales del trabajo. [7] iPXE es una implementación de código abierto del firmware y cargador de arranque PXE, creado en 2010, como una bifurcación de gPXE. Puede utilizarse para permitir que los ordenadores sin soporte PXE arranquen desde la red, o para ampliar una implementación de cliente PXE existente de modo que admita protocolos adicionales. Mientras que los clientes PXE estandarizados utilizan TFTP para transferir datos, el firmware de cliente iPXE no estandarizado añade la capacidad de descargar datos a través de otros protocolos, como HTTP, iSCSI, ATA sobre Ethernet (AoE) y Fibre Channel sobre Ethernet (FCoE). Además, en hardware soportado, el firmware de iPXE puede llegar a conectarse mediante un enlace Wi-Fi.

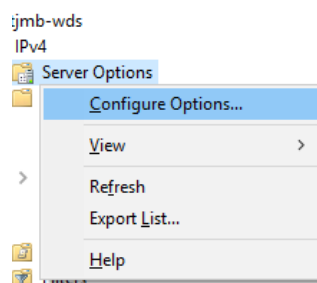
Para utilizar iPXE en el servidor WDS es necesario descargar los ficheros *snponly.efi* y *undionly.kpxe* desde <http://boot.ipxe.org/> o desde la propia ISO de iPXE. El primero será ejecutado en el arranque UEFI y el segundo en arranque BIOS(PC).

Adicionalmente, para la instalación de Debian, se utiliza la imagen de instalación por red, por lo que tras descargar la ISO y extraerla, deben copiarse los ficheros *initrd.gz* y *linux* (o *vmlinuz*) de la carpeta `\install.amd` a una subcarpeta, como se indica con más detalle en el apartado 2.3.6. Por otro lado, también debe modificarse el servidor DHCP de forma manual, como se muestra a continuación, para apuntar el arranque PXE a los nuevos ficheros.

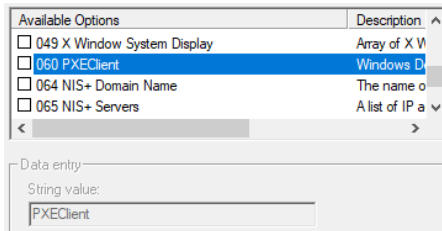
Se debe crear una carpeta en el directorio de instalación del servicio WDS, por ejemplo C:\RemoteInstall\Boot\iPXE, donde se copiarán ambos ficheros y se crearán nuevos ficheros para la configuración. El contenido de los mismos se detalla en el anexo 6.1, al final de la memoria.



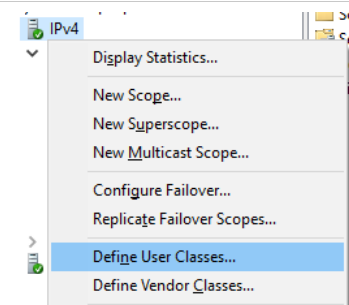
La configuración del servicio DHCP comienza desactivando el parámetro propio de WDS (060 = PXEClient) en las opciones del servicio.



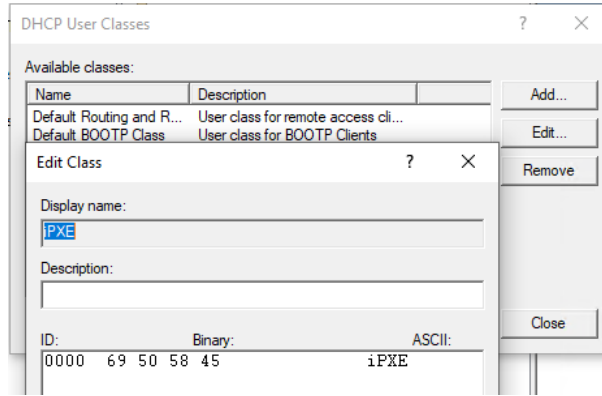
Esto es, para que WDS no tome el control en el arranque PXE.



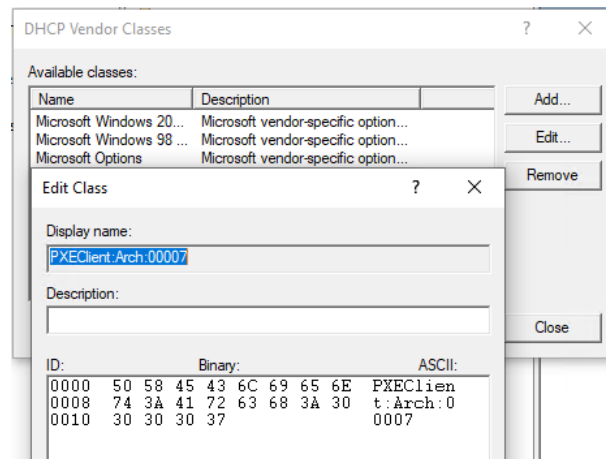
Posteriormente, en el menú contextual de IPv4, debe definirse una nueva clase de usuario.



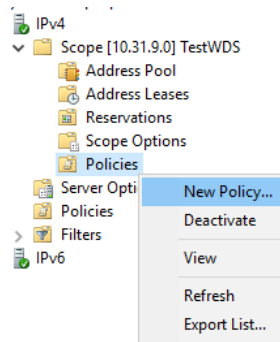
Pulsando en añadir, se le da un nombre y debe escribirse iPXE en el cuadro ASCII.



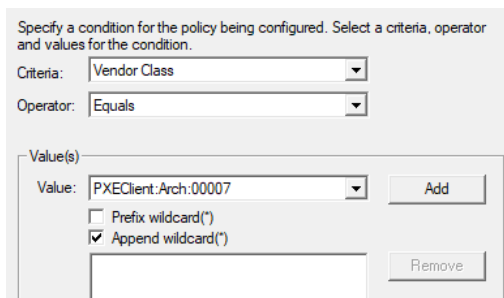
Repetir los pasos para el código de distribuidor (Vendor) y añadir dos clases: una que contenga "PXEClient:Arch:00007" y otra con "PXEClient:Arch:00000", para cubrir ambas arquitecturas (UEFI / BIOS).



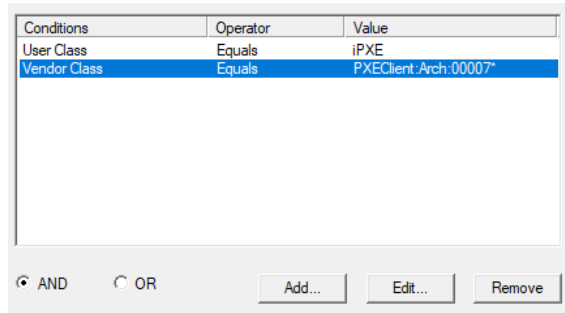
Posteriormente, en Políticas (a nivel de scope, o de IPv4, es indiferente cuando hay solo un scope) han de añadirse varias políticas:



La primera tendrá como nombre "iPXE config for UEFI" y han de añadirse dos condiciones separadas, User Class iPXE y Vendor Class PXEClient:Arch:00007 activando la casilla de append wildcard.



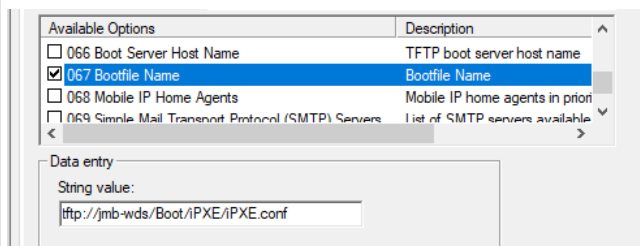
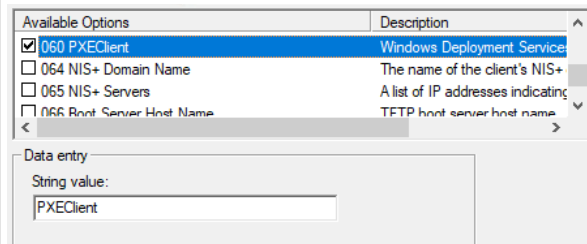
Adicionalmente hay que activar el radio button AND para que se cumplan ambos requisitos.



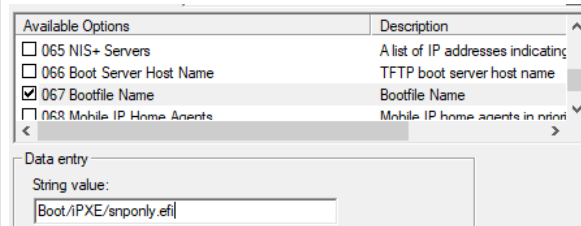
El siguiente paso es activar las opciones 060 y 067, donde se define el archivo que ha de descargar. La opción 060 debe ser PXEClient y el valor que debe tener 067 es el path relativo del servidor TFTP, por ejemplo:

tftp://hostname/Boot/iPXE/iPXE-uefi.conf
La opción 060 es para la compatibilidad al ejecutar el binario de WDS.

Esta condición solo aplicará una vez haya arrancado el binario de iPXE que se definirá en la siguiente regla.



Una vez finalizada la creación de la primera regla, la segunda, llamada "Deliver iPXE UEFI", se crea con la condición menos restrictiva: Vendor Class
PXEClient:Arch:00007, (incluyendo el wildcard al final) y con la opción 067 = "Boot/iPXE/snponly.efi" para indicarle el fichero de arranque.



Han de repetirse ambos pasos para el arranque tipo BIOS (Arch:00000) cambiando respectivamente los nombres de ficheros: *tftp://hostname/Boot/iPXE/iPXE-bios.conf* y *Boot/iPXE/undionly.kpxe*. De forma que en el primer arranque (sin iPXE cumpla las condiciones para la regla del fichero ejecutable, y una vez ejecute iPXE obtenga la configuración del menú.

Policy Name	Processin...	Level
PXE config for UEFI	1	Server
Deliver iPXE UEFI	2	Server
PXE Config for BIOS	3	Server
Deliver iPXE for BIOS	4	Server

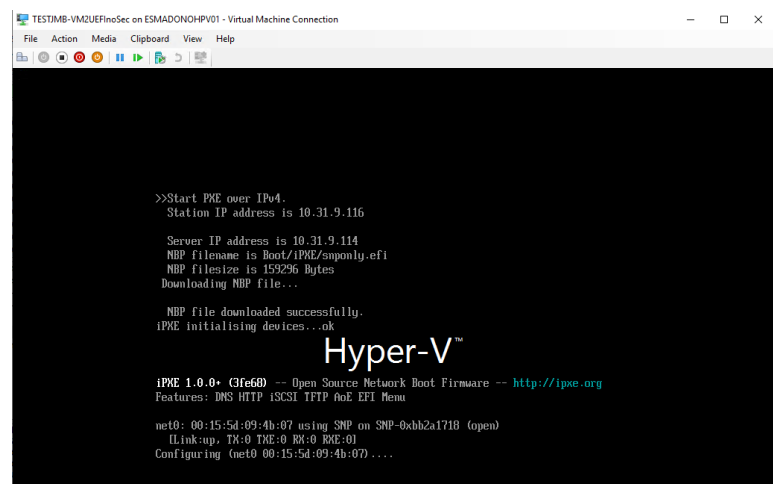
El siguiente paso es configurar que el servicio TFTP de WDS permita peticiones con las barras de las rutas tipo uri o linux (/ en lugar de \). Para ello desde el registro se modifica el siguiente filtro:

HKLM\SYSTEM\CurrentControlSet\Services\WDS\Server\Providers\WDSTFTP\ReadFilter, añadiendo "/boot/* boot/*". Finalmente ha de reiniciarse el servicio WDS para que aplique la configuración.

Name	Type	Data
(Default)	REG_SZ	(value not set)
DataPortPoolSize	REG_DWORD	0x00000010 (16)
DeadCacheSize...	REG_DWORD	0x0000015e (350)
DeadCacheTime...	REG_DWORD	0x000004b0 (1200)
EnableBufferSha...	REG_DWORD	0x00000001 (1)
EnablePortShari...	REG_DWORD	0x00000001 (1)
EnableVariableW...	REG_DWORD	0x00000001 (1)
InitRoutine	REG_SZ	WdsProviderInitialize
IsCritical	REG_DWORD	0x00000001 (1)
ProviderDll	REG_EXPAND_SZ	%systemroot%\system32\wdstftp.dll
ReadFilter	REG_MULTI_SZ	\boot*\tmp* boot*\tmp* /boot* boot*
RootFolder	REG_SZ	C:\Remotelstall
TraceDisabled	REG_DWORD	0x00000000 (0)

Value name:	Value data:
ReadFilter	\boot*\tmp* boot*\tmp* /boot* boot*

Finalmente, añadir el resto de los ficheros de configuración del menú personalizado, adjuntos en el anexo 6.1, en la ubicación correcta. Será necesario -también- configurar la máquina virtual para que arranque sin secure boot (en caso de UEFI)



```
TESTJMB-VM2UEFIoSec on ESMADONHPV01 - Virtual Machine Connection
File Action Media Clipboard View Help

>>Start PXE over IPv4.
  Station IP address is 10.31.9.116

  Server IP address is 10.31.9.114
  NBP filename is Boot/iPXE/snponly.efi
  NBP filesize is 159296 Bytes
  Downloading NBP file...

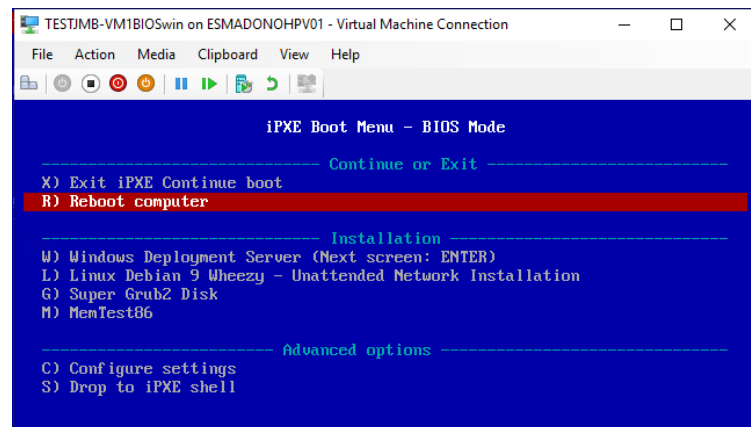
  NBP file downloaded successfully.
  iPXE initialising devices...ok

Hyper-V™

iPXE 1.0.0- (3fe60) -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS HTTP iSCSI TFTP AoE EFI Menu

net0: 00:15:5d:09:4b:07 using SNP on SNP-0xb2a1718 (open)
Link-up, TX:0 TXE:0 RX:0 RXE:0
Configuring (net0 00:15:5d:09:4b:07)....
```

El siguiente paso es probar el arranque y comprobar que aparece el menú de iPXE. En el caso de UEFI, si aparece la descarga del NBP pero no carga el menú, es debido a que el *secure boot* del arranque ha de deshabilitarse.



```
TESTJMB-VM1BIOSwin on ESMADONHPV01 - Virtual Machine Connection
File Action Media Clipboard View Help

iPXE Boot Menu - BIOS Mode

----- Continue or Exit -----
X) Exit iPXE Continue boot
R) Reboot computer

----- Installation -----
W) Windows Deployment Server (Next screen: ENTER)
L) Linux Debian 9 Wheezy - Unattended Network Installation
G) Super Grub2 Disk
M) Memtest86

----- Advanced options -----
C) Configure settings
S) Drop to iPXE shell
```

Como se muestra en el anexo 6.1, para facilitar su configuración y edición, iPXE se ha dividido múltiples ficheros que se importan -para su ejecución- en el momento necesario.

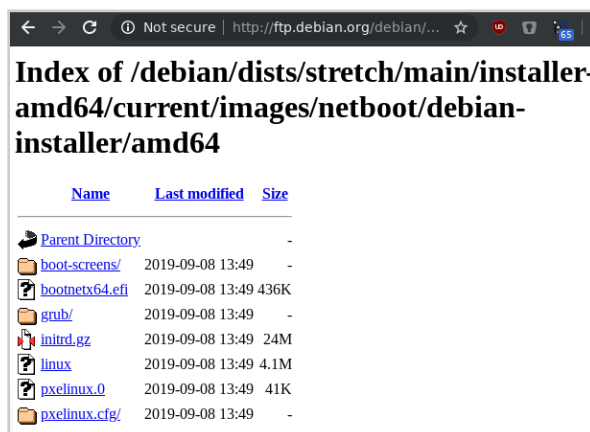
2.3.6 Arranque del kernel Linux y automatización de la instalación de Debian

Así como la instalación de Windows dispone de un fichero de respuestas generalmente llamado *unattend.xml*[9], en linux existen sistemas equivalentes, dependiendo de la distribución; por ejemplo dicho sistema en RedHat / CentOS se llama Kickstart y en Debian/Ubuntu se denomina *Preseed* [10]. El siguiente apartado muestra como iniciar el kernel de instalación de Debian, mediante iPXE, e indicarle al instalador las opciones de configuración con el fichero Preseed.

De igual forma que cuando se arranca desde DVD, para iniciar la instalación del sistema operativo Debian son necesarios dos ficheros:

- *initrd.gz*: Initrd proporciona la capacidad de cargar un RAM disk por el gestor de arranque. Este disco RAM puede ser montado como el sistema de ficheros raíz y los programas pueden ser ejecutados desde él. Después, se puede montar un nuevo sistema de ficheros raíz desde un dispositivo diferente reemplazando y desmontando el anterior. Initrd está diseñado para permitir que el arranque del sistema se produzca en dos fases, donde el kernel se carga con un conjunto mínimo de controladores compilados, y posteriormente permitir la carga de módulos adicionales desde *initrd*.
- *vmlinuz*: es un archivo ejecutable enlazado estáticamente y que contiene el núcleo Linux en uno de los formatos ejecutables soportados por Linux, normalmente tipo ELF.

Estos ficheros pueden extraerse de una ISO tipo net-install, otro DVD de instalación de Debian -situados en la carpeta netboot- o desde la url del repositorio de paquetes Debian [11]:



Una vez obtenidos se copian en la estructura de carpetas del servidor TFTP, por ejemplo `C:\RemoteInstall\Boot\iPXE\DebianNetInstall`, para que sean accesibles desde el menú mediante el protocolo TFTP.

El paso de parámetro preseed se realiza mediante la siguiente opción en la línea de comandos del cargador de arranque, que habitualmente -en grub- es: "auto preseed/url=http://webserver/path/preseed.cfg"

Las líneas para iPXE que permiten indicar el fichero initrd.gz y la configuración de preseed, entre otras posibles combinaciones, son las siguientes:

```
initrd DebianNetInst/initrd.gz
kernel DebianNetInst/vmlinuz initrd=initrd.gz auto=true priority=critical
preseed/url=tftp://JMB-WDS/Boot/iPXE/DebianNetInst/debian-wheezy-preseed.cfg
boot
```

De forma que sería posible realizar diferentes archivos de configuración de respuestas para poder aplicar diferentes plantillas de instalación, seleccionables desde distintas opciones del menú de arranque. En el apartado 2.4.2 se detalla el contenido del fichero preseed.cfg utilizado.

2.4. Instalación desatendida y post-instalación

En ambos tipos de instalación, se aplica un fichero de configuración para la instalación y se enlaza desde éste a otros comandos para aplicar scripts y configuraciones adicionales. En cada uno de los apartados se detallan los puntos clave y configuraciones utilizadas. Las configuraciones mostradas a continuación son mínimas por dos motivos; la extensión del trabajo, y debido a que el objetivo del presente trabajo es configurar los servidores para una posterior especialización, que puede llevarse a cabo remotamente, presencialmente o en el mismo script final.

2.4.1 Configuración Windows Server 2019

El fichero en formato XML creado en el apartado 2.3.3 posee las directivas y configuraciones que se aplicarán durante el proceso de instalación. En el anexo 6.2 se adjuntan los ficheros de configuración, no obstante a continuación se detallan las configuraciones más importantes y el método utilizado para enlazar con la ejecución de los scripts post-instalación.

El fichero asociado al arranque y conexión de WDS contiene la contraseña de conexión al recurso compartido, el idioma del teclado y el idioma de la UI (instalación), dentro de la sección "windowsPE", que es la fase de arranque (número 1):

```
<settings pass="windowsPE">
  <WindowsDeploymentServices>
    <Login>
      <Credentials>
        <Domain>Dominio</Domain>
        <Password>Contraseña</Password>
        <Username>UsuarioDescargaWds</Username>
      </Credentials>
      <WillShowUI>OnError</WillShowUI>
    </Login>
  </WindowsDeploymentServices>

  <SetupUILanguage>
    <UILanguage>en-US</UILanguage>
  </SetupUILanguage>
  <InputLocale>es-ES</InputLocale>
</settings>
```

En el fichero propio del proceso de instalación se incorporan más configuraciones personalizadas:

En la fase de finalización de la configuración "oobeSystem", fase número 7, se llevan a cabo las configuraciones finales de la instalación. Por ejemplo:

Establecer la contraseña de administrador local:

```
<settings pass="oobeSystem">
  <UserAccounts>
    <AdministratorPassword>
      <Value>ContraseñaAdministrador</Value>
      <PlainText>>true</PlainText>
    </AdministratorPassword>
  </UserAccounts>
```

Definición de la zona horaria:

```
<TimeZone>Romance Standard Time</TimeZone>
```

Inicio de sesión automático, número de veces y credenciales, para poder ejecución los comandos posteriores:

```
<AutoLogon>
  <Password>
    <Value>ContraseñaAdministrador</Value>
    <PlainText>>true</PlainText>
  </Password>
  <Domain>.</Domain>
  <Enabled>>true</Enabled>
  <LogonCount>1</LogonCount>
  <Username>Administrator</Username>
</AutoLogon>
```

Idioma del sistema operativo e idioma del teclado:

```
<InputLocale>es-ES</InputLocale>
<SystemLocale>en-US</SystemLocale>
```

Lanzamiento de scripts personalizados:

```
<FirstLogonCommands>
  <SynchronousCommand wcm:action="add">
    <Order>1</Order>
    <CommandLine>C:\Windows\System32\WindowsPowerShell\v
1.0\powershell.exe -executionpolicy unrestricted -C &quot;mkdir
c:\NewServers\; copy-item -recurse \\JMB-WDS\NewServers\*
c:\NewServers&quot;</CommandLine>
  </SynchronousCommand>
  <SynchronousCommand wcm:action="add">
    <Order>2</Order>
    <CommandLine>C:\Windows\System32\WindowsPowerShell\v
1.0\powershell.exe -executionpolicy unrestricted -file
c:\NewServers\StartPoint.ps1</CommandLine>
  </SynchronousCommand>
</FirstLogonCommands>
</settings>
```

Los comandos anteriores han sido codificados automáticamente por el editor de configuración para su interpretación por Windows, no obstante son unas sencillas instrucciones de Powershell:

```
powershell.exe -executionpolicy unrestricted -C "mkdir
c:\NewServers\; copy-item -recurse \\JMB-WDS\NewServers\*
c:\NewServers"

powershell.exe -executionpolicy unrestricted -file
c:\NewServers\StartPoint.ps1
```

Dichas instrucciones crean una carpeta en el nuevo servidor, copian el contenido de la carpeta origen del servidor WDS (compartida previamente para el usuario Administrador), y ejecutan el script StartPoint.ps1.

El script contiene las siguientes instrucciones para llevar a cabo una configuración básica inicial:

Lectura e descifrado de credenciales previamente almacenadas [14]:

```
$pathCreds = "\\JMB-WDS\NewServers"
$username = "CPDSPAIN\UserScripts"
$loadpass1=Get-Content "$pathCreds\credpassword.txt"
$loadaes1=Get-Content "$pathCreds\key.txt"
$securePassword = $loadpass1 | ConvertTo-SecureString -Key
$loadaes1
$domCredentials = New-Object
System.Management.Automation.PSCredential ($username,
$securePassword)
```

Desactivar cortafuegos y permitir la conexión remota:

```
netsh advfirewall set allprofiles state off
Set-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC" -RemoteAddress Any
```

Permitir la ejecución remota de comandos Powershell:

```
Enable-PSRemoting -Force -Confirm:$false
Set-Item wsman:\localhost\client\trustedhosts -Value * -Force -Confirm:$false
Restart-Service WinRM -Confirm:$false
```

Unirse a dominio utilizando las credenciales cargadas:

```
$OUPath="OU=New_Computers,DC=CPDSPAIN,DC=LOCAL"
Add-Computer -DomainName CPDSPAIN.LOCAL -Credential $domCredentials -OUPath
$OUPath -passthru
```

Instalar software de inventario (OCS) y realizar un primer inventariado:

```
cmd.exe /c "c:\NewServers\OCS\OCS-NG-Windows-Agent-Setup.exe /S
/SERVER=http://ocs/ocsinventory /TAG=CPDSPAIN /NOW"
```

2.4.2 Configuración Debian

En este apartado se describen los aspectos relacionados el contenido del fichero preseed. Para crear el fichero se ha partido del modelo que ofrece Debian en su web (example-preseed.txt) [15], para la versión stretch, adaptando las respuestas y configuraciones a los requisitos.

El fichero resultante, debian-wheezy-preseed.cfg, se ubica en la ruta C:\RemoteInstall\Boot\iPXE\DebianNetInst\ y contiene las siguientes directivas configuradas, siendo la mayoría de ellas autodescriptivas, por lo que -disponiendo del fichero completo en el anexo 6.3- no se describen todas ellas a continuación:

Configuración de idioma y teclado:

```
d-i debian-installer/locale string en_US
d-i debian-installer/locale string en_US.UTF-8
d-i console-keymaps-at/keymap select es
d-i keyboard-configuration/xkb-keymap select es
```

Configuración nombre de equipo y sufijo DNS:

```
d-i netcfg/get_hostname string unassigned-hostname
d-i netcfg/get_hostname seen false
d-i netcfg/get_domain string cpdspain.local
```

Configuración del origen de paquetes:

```
d-i mirror/country string manual
d-i mirror/http/hostname string deb.debian.org
```

Configuración del usuario root:

```
d-i passwd/root-password password ROOTPASSWD.
d-i passwd/root-password-again password ROOTPASSWD.
```

Configuración del usuario adicional:

```
d-i passwd/user-fullname string AdminUser
d-i passwd/username string adminuser
d-i passwd/user-password password USERPASSWD.
d-i passwd/user-password-again password USERPASSWD.
```

Zona horaria:

```
d-i time/zone string Europe/Madrid
```

Particionado del disco e instalación del gestor de arranque grub:

```
d-i partman-auto/method string lvm
d-i partman-lvm/device_remove_lvm boolean true
d-i partman-lvm/confirm boolean true
d-i partman-lvm/confirm_nooverwrite boolean true
d-i partman-auto/choose_recipe select multi
d-i partman-partitioning/confirm_write_new_label boolean true
d-i partman/choose_partition select finish
d-i partman-efi/non_efi_system boolean true
```

Instalación de paquetes adicionales:

```
d-i apt-setup/non-free boolean true
d-i apt-setup/contrib boolean true
tasksel tasksel/first multiselect standard, ssh-server
d-i pkgsel/include string build-essential sudo
popularity-contest popularity-contest/participate boolean false
```

Comandos post-instalación:

```
d-i preseed/late_command string apt-install git ansible; in-target ansible-pull
-U http://gitlab/pub/ansible-pull.git -i hosts
```

En el caso de la fase post-instalación en linux, se realiza mediante la instalación y ejecución de ansible. Partiendo de la modalidad que dispone ansible para realizar una ejecución desde repositorio, se llama al ejecutable ansible-pull con el parámetro URL apuntando a la dirección del repositorio donde se encuentran los ficheros de ansible. El segundo parámetro -i es para indicarle el fichero de inventario que figura en el repositorio.

El repositorio indicado es una instalación del software gratuito Gitlab, con un playbook (conjunto de ficheros de ansible) diseñado para añadir determinadas claves SSH como autorizadas para la conexión remota y la instalación del cliente de inventario OCS. El lenguaje en el que se crean los ficheros playbook de Ansible es Yaml (Yet Another Markup Language), parecido a JSON.

A continuación el contenido del fichero principal local.yml que se ejecuta mediante ansible, tras la instalación:

```
---
- hosts: all
  tasks:
  - name: Add ssh authorized keys for root user
    become: true
    authorized_key:
      user: root
      state: present
      key: '{{ item }}'
    with_file:
      - public_keys/monitoring.pub
      - public_keys/josemiguel.ballester.pub

  roles:
  - service-ocs
```

La directiva roles ejecuta los ficheros YAML se incluyen en una subcarpeta por cada tipo de rol, habitualmente son un conjunto de ficheros con múltiples referencias entre ellos, por lo que no se incluyen por motivos de longitud y simplicidad.

3. Conclusiones

Conclusiones y lecciones aprendidas del trabajo:

- A pesar de las horas invertidas y los intentos, el arranque de la instalación de Linux en la arquitectura x64 UEFI no ha sido posible mediante syslinux a través de PXE.
- Gracias a las pruebas de las diferentes aplicaciones, ha sido posible realizar una toma de contacto con nuevas herramientas, como The Foreman, y descubrir que puede cubrir un hueco de cara la automatización, pero no es óptima para el uso que se era necesario darle este proyecto, ya que -además- tiene una curva de aprendizaje más pronunciada que WDS y una configuración más compleja.
- Como ya se ha comentado anteriormente, algunos cálculos de rentabilidad de implementación del proyecto toman como referencia una estimación de tiempo al alza que no es completamente realista, ya que partiendo de una configuración como la que provee la presente memoria, en un día es posible disponer del servicio funcionando, mejorando notablemente la rentabilidad, los tiempos de instalación y configuración de nuevos servidores.

Cumplimiento de objetivos:

- Se han logrado alcanzar plenamente los objetivos principales propuestos al principio de la memoria. Si bien es cierto que la idea original del software complementario post-instalación abarcaba más funcionalidades mediante *scripting*, en el momento de plasmar los scripts en la memoria su explicación se volvería engorrosa y desvirtuaría el objetivo del trabajo. Razón por la cual se ha optado a desarrollar un modelo de script inicial, con las configuraciones básicas, a partir del cual se pueda hacer extensible la configuración y administración del sistema operativo.

Seguimiento de la planificación y metodología:

- La estimación general de la planificación ha sido acertada, no obstante, algunas fases del trabajo han supuesto una mayor dedicación (ej.: integración del arranque Linux en WDS, debido al rechazo del cargador syslinux en favor de iPXE) y otros una menor dedicación (ej.: desarrollo de los scripts).
- La disposición personal de tiempo no ha permitido seguir una dedicación constante al trabajo, por lo que las horas dedicadas se han concentrado en menor número de días, sin impedir ello el seguimiento del calendario.
- Como se indica en un párrafo anterior, la extensión y complejidad de los scripts ha tenido que ser truncada en aras de una mejor presentación y legibilidad de la sección de scripts

Líneas futuras y posibilidades de mejora:

- De igual forma que se han probado e incluido opciones adicionales en el menú para el arranque de las herramientas Memtest86 y SuperGrub2Disk, iPXE es perfectamente extensible al arranque de otras imágenes como Clonezilla, prueba de ello son los siguientes links, donde [16] indica el procedimiento y los ficheros que han de copiarse, y [17] provee las instrucciones exactas para el menú.
- Actualmente existe la limitación de arranque UEFI sin secure boot activo, ya que snponly.efi no está firmado digitalmente, aunque a futuro puede cambiar la limitación o bien que sea posible realizar una firma válida para su arranque. Existe una sección en el apartado de documentación de iPXE [18] donde se muestran herramientas e intentos para realizar una firma del ejecutable, aunque sin éxito.
- La pila de aplicaciones configuradas es aplicable tanto a servidores físicos como virtuales, siempre que dispongan de arranque por red (PXE), el cual no es el caso de algunos servidores en cloud (IaaS) a cuyos servidores no es posible conectarse hasta que ha arrancado el sistema operativo. Dichos proveedores facilitan la máquina virtual con la imagen del sistema operativo preinstalada, y disponen de otros sistemas de automatización de la instalación y configuración, por lo que no tendría sentido implementar el servicio WDS en la nube.
- Un apartado donde es posible incluir multitud de mejoras, es el script post-instalación. Dicho script podría incluir la posibilidad de asignar y configurar direcciones IP estáticas, establecer un nombre de equipo, instalar un conjunto de software concreto, llevar a cabo actualizaciones del sistema operativo, etc. Las posibilidades son ilimitadas, dependiendo de la complejidad de la configuración que sea necesaria.
- Una posible -y muy recomendable- mejora es realizar una plantilla a partir del fichero de respuestas, actualizando dinámicamente algunos valores, como por ejemplo la contraseña del administrador, para mayor seguridad.

4. Glosario

Agregación de interfaces de red: Unión lógica de más de una interfaz de red o conexión para aumentar la redundancia o velocidad. Según el protocolo, sistema operativo o configuración tiene diferentes nombres: Nic teaming, Bonding o LACP.

Answer file: Fichero en formato XML de configuraciones para el sistema operativo Windows. Normalmente nombrado como unattended.xml.

Bash: Lenguaje informático de comandos para sistemas Linux

BIOS: Firmware (o código ejecutable integrado) de la arquitectura PC que se ocupa de las primeras fases del arranque.

Bootloader: Fase del protocolo de arranque que permite cargar y ejecutar el código de arranque del sistema operativo.

Caché: Memoria de almacenamiento temporal de mayor velocidad.

Centos: Distribución Linux creada en 2004 a partir del código de RedHat.

CIFS/NETBIOS: Protocolo de acceso a recursos compartidos por red. Utilizado habitualmente en sistemas Windows.

Debian: Distribución Linux creada en 1993, precursora de otras distribuciones como Ubuntu.

DHCP: Protocolo y servicio que permite la configuración automática de direcciones IP

Discos SSD: Disco duro de estado sólido, formado mediante chips de memoria, tipo NAND o similar, que posee velocidades superiores a los discos mecánicos.

gPXE: Implementación open source de PXE, derivada de Etherboot.

GRUB: (GNU GRand Unified Bootloader) Gestor de arranque por defecto de los sistemas Linux. Es el software que es llamado por el Firmware del ordenador y posteriormente carga el kernel y el disco en memoria.

Hardware: Componentes o partes físicas de los equipos informáticos.

HTTP: (Hypertext Transfer Protocol) Protocolo de transferencia de texto utilizado para la navegación web.

Initrd.gz: Imagen inicial de disco para poder ser cargado en memoria y ejecutar la primera fase de la carga del sistema operativo.

iPXE: Implementación open source de PXE, derivada de gPXE.

Kernel: Habitualmente referido al núcleo del sistema operativo Linux.

Kickstart: Directiva mediante la cual se indica el fichero de respuestas al proceso de instalación. Aplica a distribuciones basadas en RedHat.

NFS: (Network File System) Protocolo de acceso a recursos compartidos por red. Utilizado habitualmente en sistemas Linux.

Online: Relacionado con -o que ocurre a través de- Internet.

Powershell: Lenguaje informático de comandos para sistemas Microsoft

Preseed: Directiva mediante la cual se indica el fichero de respuestas al proceso de instalación. Aplica a distribuciones basadas en Debian.

PXE: Conjunto de protocolos para arrancar y/o instalar el sistema operativo en computadoras a través de la red

Python: Lenguaje de programación orientado a objetos, creado en 1991, con el propósito de que fuera legible y comprensible a simple vista.

Raid: (Redundant array of inexpensive disks) Agrupación de discos de forma lógica para proteger el volumen de datos de una falla.

SaaS: (Software as a service) Modelo de distribución de software que ofrece las aplicaciones sobre la plataforma web, abstrayendo de las capas inferiores al cliente.

Script: Conjunto de instrucciones de del sistema operativo para llevar a cabo una o múltiples tareas

Secure boot: Sistema de seguridad en firmwares UEFI que permite impedir la carga de ficheros de arranque si éstos no están firmados digitalmente.

Syslinux: Proyecto que abarca un conjunto de gestores de arranque ligeros, para arrancar ordenadores con en el sistema operativo Linux.

Sysprep: Aplicación de Microsoft incorporada en los sistemas operativos con el fin de generar nuevos identificadores de la propia máquina. Usada habitualmente tras un clonado del sistema operativo.

TFTP: (Trivial File Transfer Protocol) Protocolo de transferencia simple de ficheros. A pesar de la similitud de su nombre al FTP, TFTP no permite listar el contenido de los directorios remotos.

UEFI: Firmware (o código ejecutable integrado) de la arquitectura PC que se ocupa de las primeras fases del arranque. Es el sucesor de BIOS.

Vmlinuz: Fichero ejecutable que contiene el núcleo Linux

WDS: (Windows Deployment Services) Servicio para la distribución y despliegue de imágenes de sistema operativo Windows.

WSUS: (Windows Server Update Services) Servicio de distribución de paquetes de actualización de sistemas operativos Windows.

XML: (Extensible Markup Language) Lenguaje estructurado de etiquetas anidadas.

5. Bibliografía y enlaces

- Web [1: https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface] Consulta 1 Noviembre 2019.
- Web [2: https://es.wikipedia.org/wiki/Extensible_Firmware_Interface] Consulta 1 Noviembre 2019.
- Web [3: https://es.wikipedia.org/wiki/Preboot_Execution_Environment] Consulta 1 Noviembre 2019.
- Web: [4: <http://www.raspberry-pi-geek.de/Magazin/2014/02/Raspberry-Pi-als-PXE-Server>] Consulta 1 Noviembre 2019. Imagen: arranque PXE.
- Web: [5: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-setup-automation-overview>] Consulta 12 Noviembre 2019
- Web: [6: <https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install>] Consulta 12 Noviembre 2019
- Web: [7: <https://en.wikipedia.org/wiki/IPXE>] Consulta 12 Noviembre 2019
- Web: [8: <https://gist.github.com/mintsoft/e4bf8391cdc3a9d9014-b185897cef41c>] Consulta 13 Noviembre 2019
- Web: [9: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/update-windows-settings-and-scripts-create-your-own-answer-file-sxs>] Consulta 30 Diciembre 2019
- Web: [10: <https://wiki.debian.org/DebianInstaller/Preseed>] Consulta 30 Diciembre 2019
- Web: [11: <http://ftp.debian.org/debian/dists/stretch/main/installer-amd64/current/images/netboot/debian-installer/amd64/>] Consulta 30 Diciembre 2019
- Web: [12: <https://wiki.debian.org/Initrd>] Consulta 30 Diciembre 2019
- Web: [13: <https://es.wikipedia.org/wiki/Vmlinux>] Consulta 30 Diciembre 2019
- Web: [14: <https://stackoverflow.com/questions/7109958/saving-credentials-for-reuse-by-powershell-and-error-convertto-securestring-ke>] Consulta 30 Diciembre 2019
- Web: [15: <https://www.debian.org/releases/stretch/example-preseed.txt>] Consulta 30 Diciembre 2019
- Web: [16: <https://clonezilla.org/livepxe.php>] Consulta 30 Diciembre 2019
- Web: [17: https://sourceforge.net/p/clonezilla/discussion/Clonezilla_live/thread/5ca9f0f103/] Consulta 30 Diciembre 2019
- Web: [18: <https://ipxe.org/appnote/etoken>] Consulta 30 Diciembre 2019

6. Anexos

6.1 Ficheros de configuración de iPXE

C:\RemoteInstall\Boot\iPXE\iPXE-bios.conf

```
#!ipxe
chain --autofree /Boot/iPXE/boot.menu.bios.cfg
```

C:\RemoteInstall\Boot\iPXE\iPXE-uefi.conf

```
#!ipxe
chain --autofree /Boot/iPXE/boot.menu.uefi.cfg
```

C:\RemoteInstall\Boot\iPXE\boot.menu.uefi.cfg

```
#!ipxe

# Figure out if client is 64-bit capable
cpuid --ext 29 && set arch x64 || set arch x86
cpuid --ext 29 && set archl amd64 || set archl i386

##### MAIN MENU #####
:start
menu iPXE Boot Menu - UEFI Mode
item --gap -- ----- Continue or Exit
-----
item --key x exit      X) Exit iPXE Continue boot
item --key r reboot   R) Reboot computer
item
item --gap -- ----- Installation
-----
item --key w wds       W) Windows Deployment Server (Next screen: ENTER)
item --key l linux     L) Linux Debian 9 Wheezy - Unattended Network
Installation
item --key g sg2d      G) Super Grub2 Disk
item
item --gap -- ----- Advanced options
-----
item --key c config    C) Configure settings
item --key s shell     S) Drop to iPXE shell
item
choose --timeout 10000 --default exit selected || goto cancel
set menu-timeout 0
goto ${selected}

:back
set submenu-timeout 0
clear submenu-default
goto start

:exit
exit 1

:reboot
reboot
exit 1

:config
config
goto start

:cancel
echo You cancelled the menu, dropping you to a shell
```

```

:shell
echo Type 'exit' to get the back to the menu
shell
set menu-timeout 0
set submenu-timeout 0
goto start

:failed
echo Booting failed, dropping to shell
goto shell

##### MAIN MENU ITEMS #####

:wds
chain ../x64/wdsmgfw.efi || goto failed
goto start

:linux
chain --autofree /Boot/iPXE/boot.option.linux-debian.cfg
goto start

:sg2d
chain Isos/sg2d.efi || goto failed
boot
goto start

```

C:\RemoteInstall\Boot\iPXE\boot.menu.bios.cfg

```

#!ipxe

# Figure out if client is 64-bit capable
cpuid --ext 29 && set arch x64 || set arch x86
cpuid --ext 29 && set arch1 amd64 || set arch1 i386

##### MAIN MENU #####
:start
menu iPXE Boot Menu - BIOS Mode
item --gap -- ----- Continue or Exit
-----
item --key x exit      X) Exit iPXE Continue boot
item --key r reboot    R) Reboot computer
item
item --gap -- ----- Installation
-----
item --key w wds       W) Windows Deployment Server (Next screen: ENTER)
item --key l linux     L) Linux Debian 9 Wheezy - Unattended Network
Installation
item --key g sg2d      G) Super Grub2 Disk
item --key m mem       M) MemTest86
item
item --gap -- ----- Advanced options
-----
item --key c config    C) Configure settings
item --key s shell     S) Drop to iPXE shell
item
choose --timeout 10000 --default exit selected || goto cancel
set menu-timeout 0
goto ${selected}

:back
set submenu-timeout 0
clear submenu-default
goto start

:exit
exit 1

:reboot
reboot
exit 1

:config

```

```

config
goto start

:cancel
echo You cancelled the menu, dropping you to a shell

:shell
echo Type 'exit' to get the back to the menu
shell
set menu-timeout 0
set submenu-timeout 0
goto start

:failed
echo Booting failed, dropping to shell
goto shell

##### MAIN MENU ITEMS #####

:wds
chain ../x86/wdsntp.com || goto failed
goto start

:linux
chain --autofree /Boot/iPXE/boot.option.linux-debian.cfg
goto start

:sg2d
kernel memdisk/memdisk iso raw || read void
initrd Isos/sg2d.iso || read void
imgargs memdisk iso raw
boot
goto start

:mem
kernel memdisk/memdisk iso raw || read void
initrd Isos/mem.iso || read void
imgargs memdisk iso raw
boot
goto start

```

C:\RemoteInstall\Boot\iPXE\boot.option.linux-debian.cfg

```

#!ipxe
initrd DebianNetInst/initrd.gz
kernel DebianNetInst/vmlinuz initrd=initrd.gz auto=true priority=critical
preseed/url=tftp://10.x.y.z/Boot/iPXE/DebianNetInst/debian-wheezy-preseed.cfg
boot

```

6.2 Fichero de configuración de preseed.cfg

C:\RemoteInstall\Boot\iPXE\DebianNetInst\debian-wheezy-preseed.cfg

```
d-i debian-installer/locale string en_US
d-i debian-installer/locale string en_US.UTF-8
d-i console-keymaps-at/keymap select es
d-i keyboard-configuration/xkb-keymap select es
d-i netcfg/choose_interface select auto
d-i netcfg/get_hostname string unassigned-hostname
d-i netcfg/get_hostname seen false
d-i netcfg/get_domain string cpdspain.local
d-i netcfg/wireless_wep string
d-i hw-detect/load_firmware boolean true
d-i mirror/country string manual
d-i mirror/http/hostname string deb.debian.org
d-i mirror/http/directory string /debian
d-i mirror/http/proxy string
d-i passwd/root-password password ROOTPASSWD.
d-i passwd/root-password-again password ROOTPASSWD.
d-i passwd/user-fullname string AdminUser
d-i passwd/username string adminuser
d-i passwd/user-password password USERPASSWD.
d-i passwd/user-password-again password USERPASSWD.
d-i clock-setup/utc boolean true
d-i time/zone string Europe/Madrid
d-i clock-setup/ntp boolean true
d-i clock-setup/ntp-server string 10.x.y.z
d-i partman-auto/method string lvm
d-i partman-lvm/device_remove_lvm boolean true
d-i partman-md/device_remove_md boolean true
d-i partman-lvm/confirm boolean true
d-i partman-lvm/confirm_nooverwrite boolean true
d-i partman-auto/choose_recipe select multi
d-i partman-partitioning/confirm_write_new_label boolean true
d-i partman/choose_partition select finish
d-i partman/confirm boolean true
d-i partman/confirm_nooverwrite boolean true
d-i partman-md/confirm boolean true
d-i partman-partitioning/confirm_write_new_label boolean true
d-i partman/choose_partition select finish
d-i partman/confirm boolean true
d-i partman/confirm_nooverwrite boolean true
d-i partman-efi/non_efi_system boolean true
d-i apt-setup/non-free boolean true
d-i apt-setup/contrib boolean true
tasksel tasksel/first multiselect standard, ssh-server
d-i pkgsel/include string build-essential sudo
popularity-contest popularity-contest/participate boolean false
d-i grub-installer/bootdev string /dev/sda
d-i finish-install/reboot_in_progress note
d-i preseed/late_command string apt-install git ansible; in-target ansible-pull
-U http://gitlab/pub/ansible-pull.git -i hosts
```

6.3 Ficheros de configuración WDS (Unattended.xml)

C:\RemoteInstall\WdsClientUnattend\Idioma-creds.xml

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="windowsPE">
    <component name="Microsoft-Windows-Setup" processorArchitecture="amd64"
      publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
      xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <WindowsDeploymentServices>
        <Login>
          <Credentials>
            <Domain>SERVIDORWDS</Domain>
            <Password>USUARIOWDS</Password>
            <Username>PASSWORDWDS</Username>
          </Credentials>
          <WillShowUI>OnError</WillShowUI>
        </Login>
      </WindowsDeploymentServices>
    </component>
    <component name="Microsoft-Windows-International-Core-WinPE"
      processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
      language="neutral" versionScope="nonSxS"
      xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <SetupUILanguage>
        <UILanguage>en-US</UILanguage>
      </SetupUILanguage>
      <InputLocale>es-ES</InputLocale>
    </component>
  </settings>
  <cpu:offlineImage cpi:source="wim:c:/w19iso/sources/install.wim#Windows
  Server 2019 SERVERSTANDARD" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
</unattend>
```

C:\RemoteInstall\Images\Win2019\install\Unattend\ImageUnattend.xml

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="oobeSystem">
    <component name="Microsoft-Windows-Shell-Setup"
      processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
      language="neutral" versionScope="nonSxS"
      xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <OOBE>
        <HideEULAPage>true</HideEULAPage>
        <SkipMachineOOBE>true</SkipMachineOOBE>
        <SkipUserOOBE>true</SkipUserOOBE>
      </OOBE>
      <UserAccounts>
        <AdministratorPassword>
          <Value>PASSWORDLOCALADMIN</Value>
          <PlainText>true</PlainText>
        </AdministratorPassword>
      </UserAccounts>
      <RegisteredOrganization>Empresa SL</RegisteredOrganization>
      <ShowPowerButtonOnStartScreen>true</ShowPowerButtonOnStartScreen>
      <TimeZone>Romance Standard Time</TimeZone>
      <AutoLogon>
        <Password>
          <Value>PASSWORDLOCALADMIN</Value>
          <PlainText>true</PlainText>
        </Password>
        <Domain>.</Domain>
        <Enabled>true</Enabled>
      </AutoLogon>
    </component>
  </settings>
</unattend>
```



```

        <LogonCount>1</LogonCount>
        <Username>Administrator</Username>
    </AutoLogon>
    <FirstLogonCommands>
        <SynchronousCommand wcm:action="add">
            <Order>1</Order>
            <CommandLine>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -executionpolicy unrestricted -C &quot;mkdir c:\NewServers\; copy-item -recurse \\JMB-WDS\NewServers\* c:\NewServers&quot;</CommandLine>
        </SynchronousCommand>
        <SynchronousCommand wcm:action="add">
            <Order>2</Order>
            <CommandLine>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -executionpolicy unrestricted -file c:\NewServers\StartPoint.ps1</CommandLine>
        </SynchronousCommand>
    </FirstLogonCommands>
</component>
    <component name="Microsoft-Windows-International-Core"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMICConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <InputLocale>es-ES</InputLocale>
        <SystemLocale>en-US</SystemLocale>
    </component>
</settings>
    <cpu:offlineImage cpu:source="wim:c:/w19iso/sources/install.wim#Windows Server 2019 SERVERSTANDARD" xmlns:cpu="urn:schemas-microsoft-com:cpu" />
</unattend>

```

6.4 Fichero de configuración post-instalación Windows

C:\Shares\NewServers\StartPoint.ps1

```
$pathCreds = "\\JMB-WDS\NewServers"
$username = "CPDSPAIN\UserScripts"
$loadpass1=Get-Content "$pathCreds\credpassword.txt"
$loadaes1=Get-Content "$pathCreds\key.txt"
$securePassword = $loadpass1 | ConvertTo-SecureString -Key $loadaes1
$domCredentials = New-Object System.Management.Automation.PSCredential
($username, $securePassword)

netsh advfirewall set allprofiles state off
Set-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC" -RemoteAddress Any

Enable-PSRemoting -Force -Confirm:$false
Set-Item wsman:\localhost\client\trustedhosts -Value * -Force -Confirm:$false
Restart-Service WinRM -Confirm:$false

$OUPath="OU=Expired_Computers,DC=CPDSPAIN,DC=LOCAL"
Add-Computer -DomainName CPDSPAIN.LOCAL -Credential $domCredentials -OUPath
$OUPath -passthru

cmd.exe /c "c:\NewServers\OCS\OCS-NG-Windows-Agent-Setup.exe /S
/SERVER=http://ocs/ocsinventory /TAG=CPDSPAIN /NOW"
```

6.5 Fichero de configuración post-instalación Linux

(Ubicado en Gitlab interno: <http://gitlab/pub/ansible-pull.git>)

/local.yml

```
---
- hosts: all
  tasks:
    - name: Add ssh authorized keys for root user
      become: true
      authorized_key:
        user: root
        state: present
        key: '{{ item }}'
      with_file:
        - public_keys/monitoring.pub
        - public_keys/josemiguel.ballester.pub

  roles:
    - service-ocs
```

6.6 Resumen de ficheros utilizados en la configuración

```
C:\Shares
\--- NewServers
|   credpassword.txt
|   key.txt
|   StartPoint.ps1
|
\---OCS
    OCS-NG-Windows-Agent-Setup.exe

C:\RemoteInstall
+---Boot
| |
| +---iPXE
| |   boot.menu.bios.cfg
| |   boot.menu.uefi.cfg
| |   boot.option.linux-debian.cfg
| |   iPXE-bios.conf
| |   iPXE-uefi.conf
| |   snponly.efi
| |   undionly.kpxe
| |
| +---DebianNetInst
| |   debian-wheezy-preseed.cfg
| |   initrd.gz
| |   vmlinuz
| |
| +---Isos
| |   mem.iso
| |   memtest86+-5.01.iso
| |   sg2d.efi
| |   sg2d.iso
| |   super_grub2_disk_i386_pc_2.02s10.iso
| |
| +---memdisk
| |   memdisk
+---Images
| \---Win2019
| |   \---install
| | |   \---Unattend
| | | |   ImageUnattend.xml
| |
| \---WdsClientUnattend
| |   Idioma-Creds.xml
```