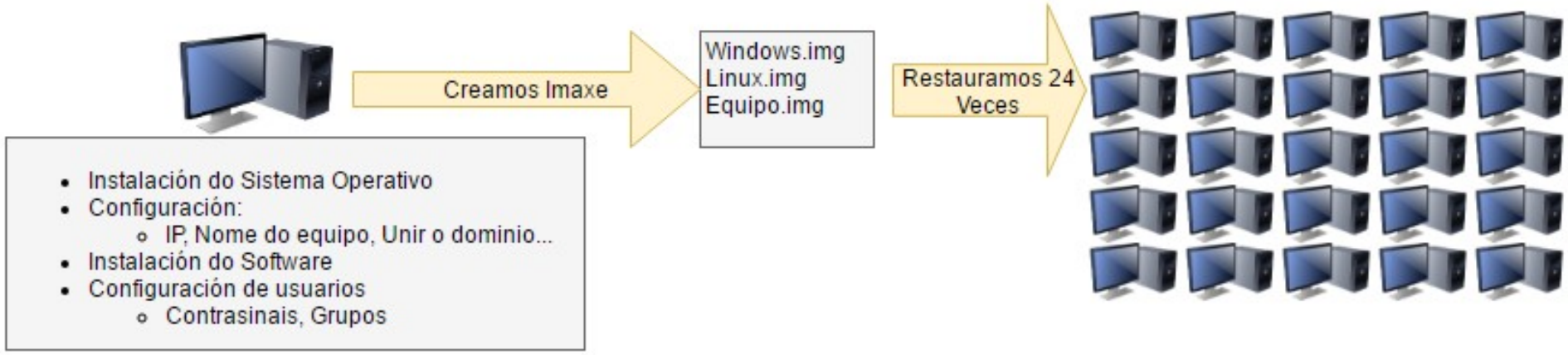
Clonación Windows

Problemática de partida

- Temos que instalar unha aula con 25 equipos
- Queremos instalar neles Windows e GNU/Linux
- Iso implica facer 50 veces:
  - Instalación do Sistema Operativo
  - Configuración
    - Configuración IP, Nome de equipo, Unir o dominio...
  - Instalación do Software
  - Configuración de usuarios
    - Contrasinais, Grupos

Clonación

- O noso **obxectivo** é facer unha imaxe universal de Windows, que poidamos restaurar en calquera equipo
- Permítenos aforrar moitísimo traballo
  - Instalamos e configuramos todo 1 vez
  - Creamos os arquivos de Imaxe



Tempo Instalación/Configuración 1 Equipo : 4 horas

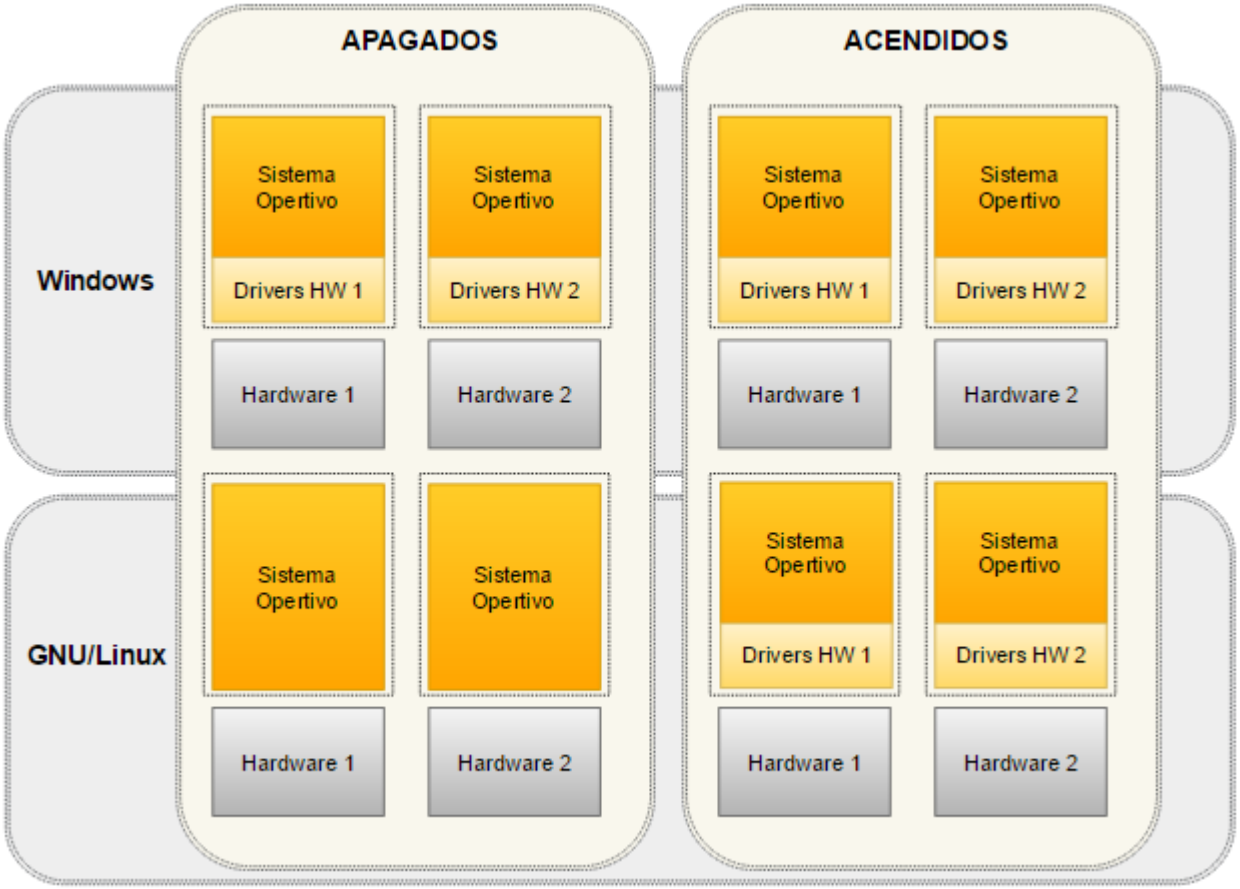
Tempo restauración 1 Equipo : 20 minutos

Problemas á hora de clonar

- Os sistemas Operativos Windows presentan varios problemas a hora de ser clonados
  - DRIVERS
  - SID

Drivers en Windows

- Cando instalamos un Windows, os drivers para ese equipo quedan configurados
- Se cambiamos o HD a outro HW non arrancará
- No caso de GNU/Linux o HW é detectado en cada arranque



Exemplo:

MV Windows, se cambiamos controladora IDE a SATA temos un BSOD.

Drivers en Windows (2)

- Isto é un problema a hora de facer clonacións
- Temos que ter unha imaxe distinta por cada hardware

SID

- Windows non utiliza o nome de usuario para identificar unha conta de usuario senón un código interno chamado **SID (Security ID, IDentificador de Seguridade)**
- Se eliminamos unha conta de usuario e logo a volvemos a crear, aínda que usemos o mesmo nome, a conta será totalmente distinta a anterior, por que o sistema lle asigna un SID distinto
- Os SID non se reempregan, sempre se crean novos

SID for PC1:
S-1-5-21-299502267-492894223-1708537768 ➔ Equipo
SID for PC1\administrador:
S-1-5-21-299502267-492894223-1708537768-500 ➔ Administrador
SID for PC1\ana:
S-1-5-21-299502267-492894223-1708537768-1006 ➔ Usuario Limitado

SID (2)

- Problema:
  - Se clonamos o Windows todos os equipos terían o mesmo sysprep
  - Que nunha mesma rede teñamos dous equipos co mesmo SID podería ser problemático
  - Aínda que hai controversia sobre o tema

```
C:\Windows\system32>whoami /user

INFORMACIÓN DE USUARIO
----------------------

Nombre de usuario              SID
============================== ============================================
desktop-njo7ouk\administrador S-1-5-21-137993792-604642658-3203137243-500
```

Solución

- Instalaremos e configuraremos un equipo que será o noso equipo de referencia
- Para solucionar os problemas de Windows empregaremos **Sysprep**
  - Xerará un novo SID para o equipo restaurado
  - Eliminará os drivers incorporados na instalación, e recoñecerá o HW no equipo onde se restaure

Situación Inicial

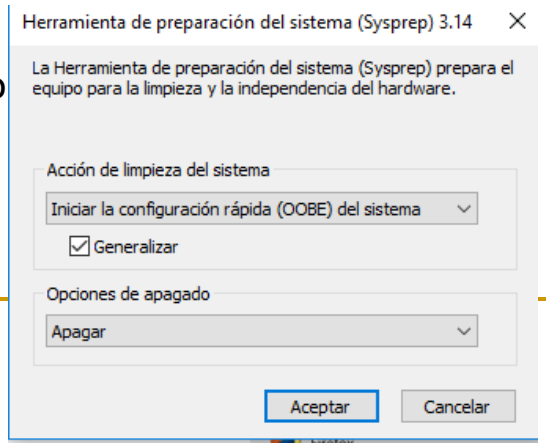
- Importamos **Win 10Base.ova** e creamos unha MV con VirtualBox
- Características da MV
  - Windows 10 instalado
  - Ten o usuario creado durante a instalación
    - Usuario: Usuario Limitado
  - Configuración da rede: Rede Interna
- Instalamos o seguinte SW
  - Notepad++, VLC, Firefox
- Personalizacións
    - Creamos unha carpeta no escritorio de usuario
    - Carpeta en C:\D1
    - Non ocultar extensións arquivos coñecidos
    - Notepad++ En español

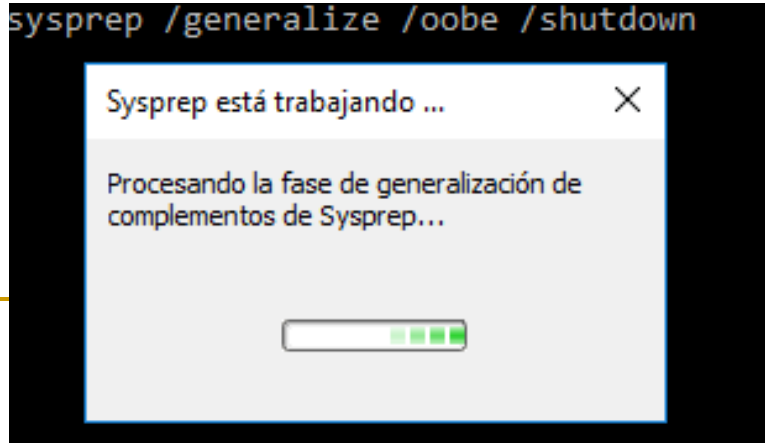
Preparando o equipo para crear a imaxe

Comprendendo Sysprep

Intento 1: Sysprep

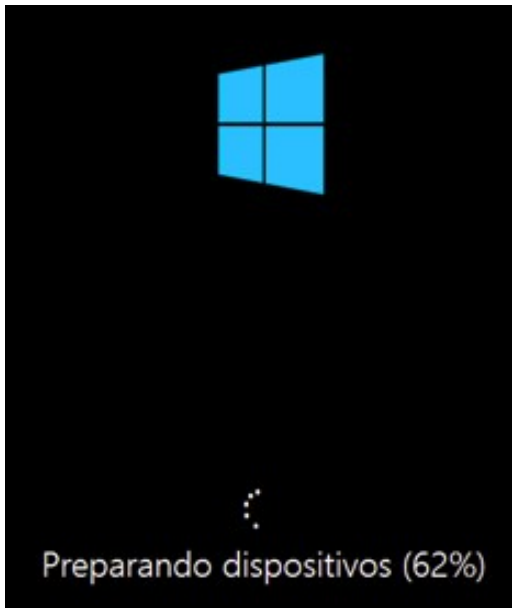
- **Importante: Facemos instantánea**
- Podémolo executar dende entorno gráfico ou liña de comandos
  - *cd C:\Windows\System32\sysprep*
  - *Sysprep.exe /generalize /oobe /shutdown*
- Opcións
  - /generalize:
    - Prepara a instalación de Windows para facer unha imaxe del e poder logo clonala. Resetéase o SID creado na instalación.
  - /oobe:
    - Restaura o equipo ao Modo de Benvida. Neste Modo o usuario final pode configurar ao seu antoxo o sistema operativo, así pode crear usuarios, cambiarlle de nome ao equipo e outras configuracións.
  - /shutdown
    - Apaga o equipo

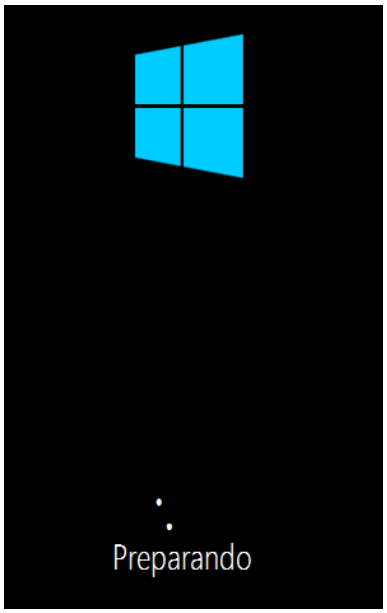


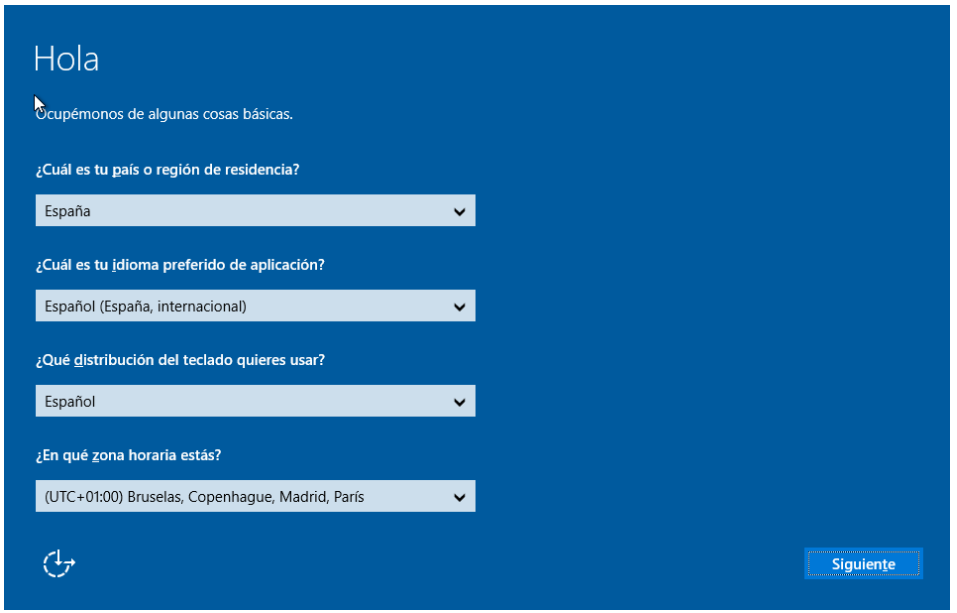


Intento 1 (2)

- O proceso é o seguinte







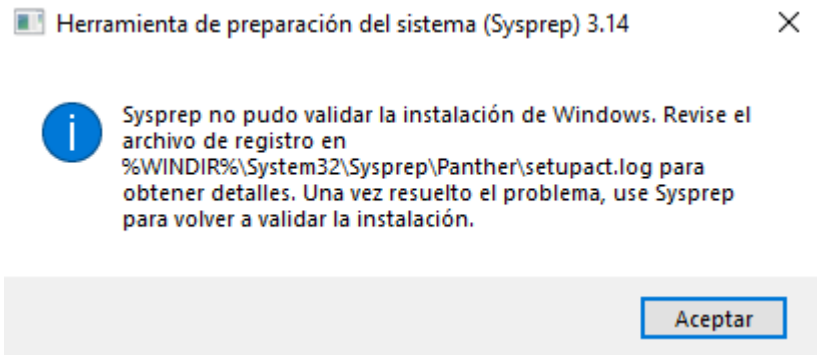
Recoñecendo o Hardware

Aparece o oobe

- **PROBLEMA:**
  - Teríamos que introducir outra vez a información requirida na **oobe**
    - Crear usuarios
    - Zona horaria
    - ....

Intento 1: Sysprep Posibles Erros

- Podería ocorrer que o lanzar o sysprep tivésemos unha mensaxe de erro



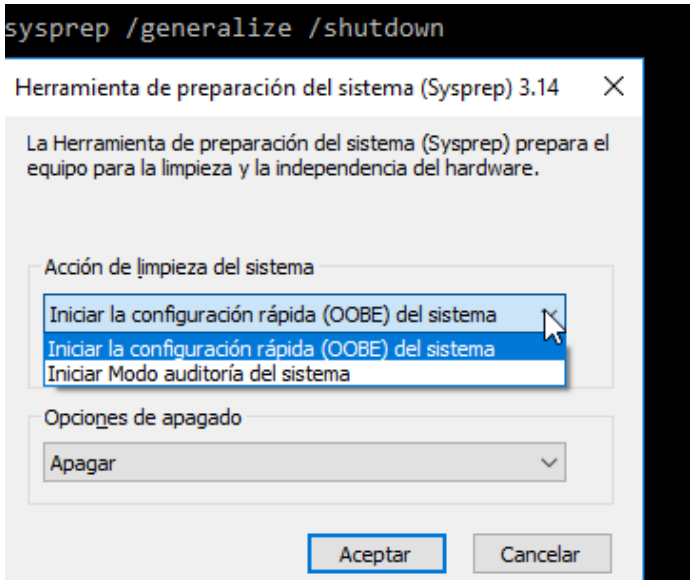
- Para saber o motivo temos que examinar os arquivos de log

```
C:\Windows\System32\Sysprep>sysprep.exe /generalize /oobe /shutdown

C:\Windows\System32\Sysprep>more Panther\setuperr.log
2019-11-12 12:14:50, Error      [0x0f00b0] SYSPRP spopk.dll:: There are one or more Windows updates that require a re
boot. To run Sysprep, reboot the computer and restart the application.[gle=0x000036b7]
2019-11-12 12:14:50, Error      [0x0f0082] SYSPRP ActionPlatform::LaunchModule: Failure occurred while executing 'Syspre
p_Clean_Validate_Opk' from C:\Windows\System32\spopk.dll; dwRet = 0x139f[gle=0x000036b7]
```

- Neste caso o problema era debido a que tíñamos unha actualización pendente.
- Reinicamos, deixamos que finalice a actualización e probamos novamente.

Intento 2: Sysprep sen oobe

- **Recuperamos a Instantánea**
- Queremos que non apareza a pantalla oobe
  - *Sysprep.exe /generalize /shutdown*



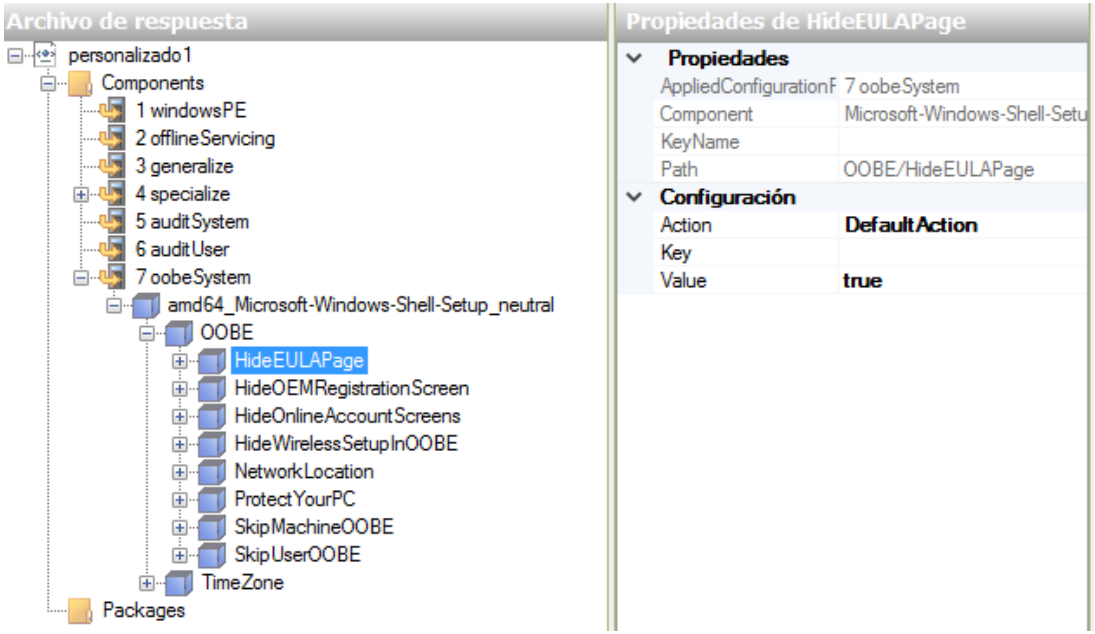
- Non é posible. Temos que escoller entre:
  - Audit
  - Configuración OOBE

Intento 3: Sysprep con arquivo de respostas

- Temos que crear un arquivo para automatizar as respostas ó oobe
- Os arquivos de respostas pódense empregar para:
  - Facer unha instalación de Windows desatendida
    - Crear particións, usuarios, ...
    - **unattend.xml** no raíz do Medio de instalación
  - Que non pregunte nada cando estamos preparando unha imaxe para a súa clonación
    - Fase OOBE, Personalizacións...
- No noso caso empregarémolo para o segundo. Queremos:
  - Que o reinicio sexa totalmente automatizado, é dicir non pregunte nada na fase OOBE
  - Existan os dous usuarios (Usuario, Administrador), e conservern as personalizacións que fagamos no seu perfil.

Intento 3: Sysprep con arquivo de respostas (2)

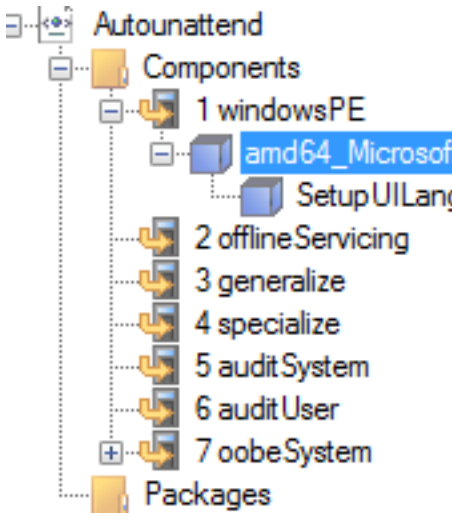
- O proceso de creación do arquivo de respostas saése do obxecto desta presentación
- Para crear o arquivo de respostas, Microsoft proporcionanos a ferramenta **Windows ADK** (Assessment and Deployment Kit)



- Con ela podemos escoller de xeito gráfico as respostas que lle damos a cada unha das fases de instalación do Windows

Intento 3: Sysprep con arquivo de respostas (3)

- A instalación de Windows pode pasar polas seguintes fases:
  - **WindowsPE:**
    - Opcións básicas da instalación: Número de serie, configuración de disco
  - **Offline Servicing**
    - Actualizacións, paquetes de idioma, drivers para realizar a instalación
  - **Specialize**
    - Axustes de rede, hora, idioma, dominio.
  - **Generalize**
    - Só se executa co comando sysprep
  - **oobeSystem**
    - Configuración de Windows antes da pantalla de benvida.
- Teremos que introducir a información necesaria para instalación sexa totalmente desatendida



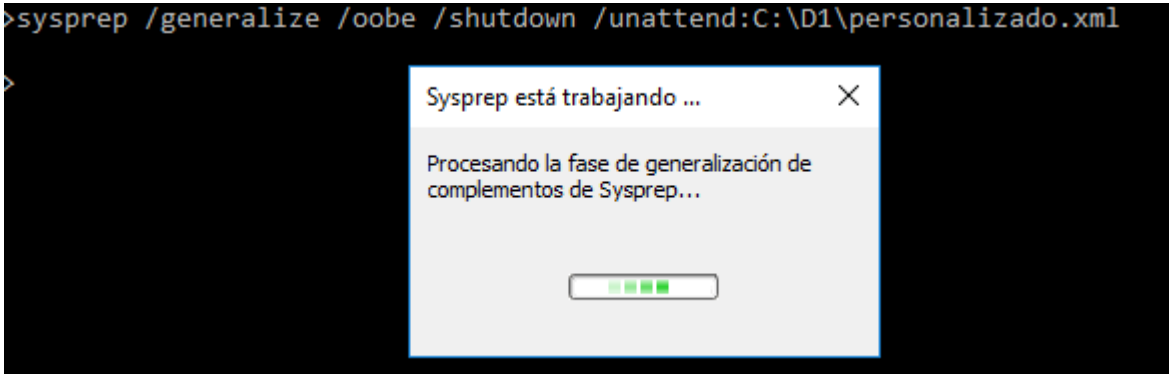
```
<!--*****************************************************
Windows 10 Arquivo de respostas
Útil para crear imaxes co sysprep
*****************************************************-->

<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="specialize">
        <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
            <!-- Zona Horaria -->
            <TimeZone>Romance Standard Time</TimeZone>
            <!-- Nome do Equipo -->
            <ComputerName>XW10-01</ComputerName>
        </component>
    </settings>
    <settings pass="oobeSystem">
        <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
            <!-- Para que non pregunte nada -->
            <OOBE>
                <!-- Non amosa o contrato de licencia -->
                <HideEULAPage>true</HideEULAPage>
                <HideOEMRegistrationScreen>true</HideOEMRegistrationScreen>
                <!-- Non nos pide crear contas de usuario online -->
                <HideOnlineAccountScreens>true</HideOnlineAccountScreens>
                <!-- Non nos amosa o asistente para conectarnos á Wifi -->
                <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
                <!-- Na configuración da rede local escollemos como ubicación Traballo -->
                <NetworkLocation>Work</NetworkLocation>
                <!-- Non nos pregunta para crear un usuario -->
                <SkipUserOOBE>true</SkipUserOOBE>
                <!-- Non nos pregunta un nome parao o equipo -->
                <SkipMachineOOBE>true</SkipMachineOOBE>
                <!-- Escollemos a configuración de protección do equipo por defecto  -->
                <ProtectYourPC>3</ProtectYourPC>
            </OOBE>

        </component>
    </settings>

</unattend>
```

Intento 3: Sysprep con arquivo de respostas (4)

- Comentarios o arquivo
  - Na fase specialize
    - Nome de equipo
    - Zona horaria
  - Na fase OOBE
    - Non amose o contrato de licenza
    - Non amose a pantalla para crear usuario
    - Escollemos configuración de rede no traballo

Intento 3: Sysprep con arquivo de respostas (5)

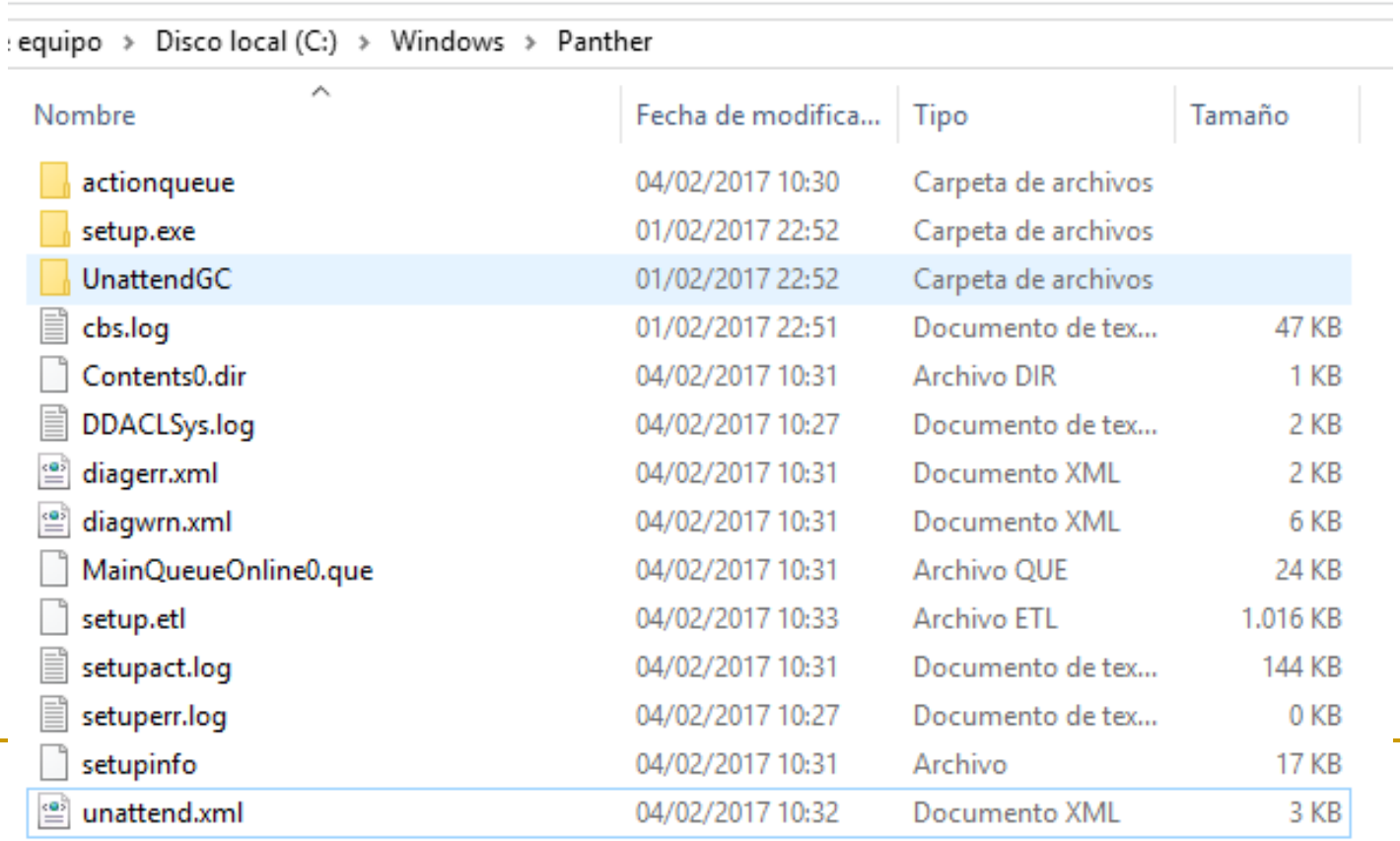
- Para executalo
  - *Sysprep /generalize /oobe /shutdown /unattend:personalizado.xml*



- **Problema**
  - Non habilita o usuario administrador
  - Só existe usuario como administrador

Intento 3: Sysprep con arquivo de respostas (6)

- O finalizar, na carpeta C:\Windows\Panther atopamos:
  - Un arquivo de log
  - O arquivo de respostas.
    - Unattend.xml
    - Pode ser interesante borralo pois pode conter contrasinais.



Intento 4: Sysprep Habilitando o Administrador

- **Importante: Non o imos a facer, só para saber que existe.**
- Podemos modificar o arquivo de repostas para que habilite o usuario administrador
- Temos varios xeitos. Faremos que execute un comando durante a instalación
- Incluímos na fase specialize o seguinte código:

```
<component name="Microsoft-Windows-Deployment" 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">
            <RunSynchronous>
               <RunSynchronousCommand wcm:action="add">
                   <Path>net user administrador /active:yes</Path>
                   <Order>1</Order>
               </RunSynchronousCommand>
           </RunSynchronous>
       </component>
```

Intento 4: Sysprep Habilitando o Administrador (2)

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="specialize">
        <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64" pu
            <TimeZone>Romance Standard Time</TimeZone>
            <ComputerName>IF4-XX</ComputerName>
            <CopyProfile>true</CopyProfile>
        </component>
        <component name="Microsoft-Windows-Deployment" processorArchitecture="amd64" pub
          <RunSynchronous>
            <RunSynchronousCommand wcm:action="add">
              <Path>net user administrador /active:yes</Path>
              <Order>1</Order>
            </RunSynchronousCommand>
          </RunSynchronous>
        </component>
    </settings>
    <settings pass="oobeSystem">
        <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64" pu
            <OOBE>
              <HideEULAPage>true</HideEULAPage>
              <HideOEMRegistrationScreen>true</HideOEMRegistrationScreen>
              <HideOnlineAccountScreens>true</HideOnlineAccountScreens>
              <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
              <NetworkLocation>Work</NetworkLocation>
              <SkipUserOOBE>true</SkipUserOOBE>
              <SkipMachineOOBE>true</SkipMachineOOBE>
              <ProtectYourPC>3</ProtectYourPC>
            </OOBE>
        <TimeZone>Romance Standard Time</TimeZone>
        </component>
    </settings>

</unattend>
```

Intento 4: Sysprep executando un bat

- **Importante: Non o imos a facer, só para saber que existe.**
- Do mesmo xeito que executamos un comando podemos executar un bat
- Na fase specialize introducimos o seguinte código

```
<component name="Microsoft-Windows-Deployment" 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">
            <RunSynchronous>
               <RunSynchronousCommand wcm:action="add">
                   <Path>C:\D1\custom.bat</Path>
                   <Order>1</Order>
               </RunSynchronousCommand>
           </RunSynchronous>
       </component>
```

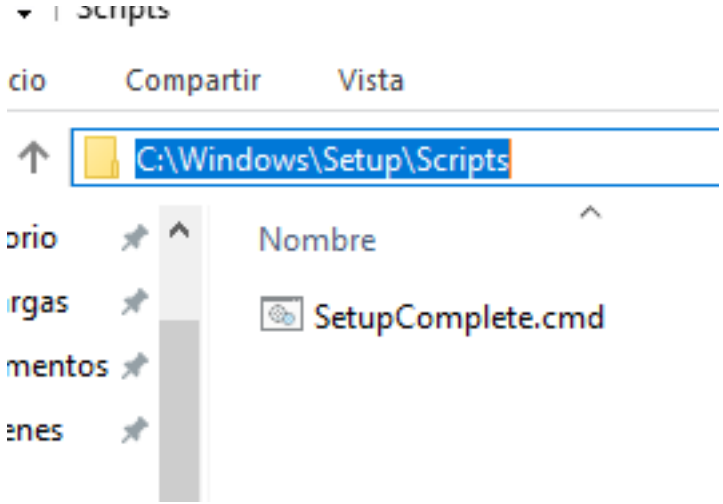
Intento 4: Sysprep executando un bat (2)

- No bat podemos facer o que queramos
  - Habilitamos usuario administrador
  - Poñémoslle de contrasinal abc123.
  - Engadimos a usuario ó grupo Usuarios
  - Quitamos a usuario do grupo de administradores

```
@echo off

REM Habilito Usuario Administrador
net user administrador /active:yes
net user administrador abc123.

REM Cambiamos o grupo de Usuario
net localgroup Usuarios usuario /add
net localgroup Administradores usuario /del
```

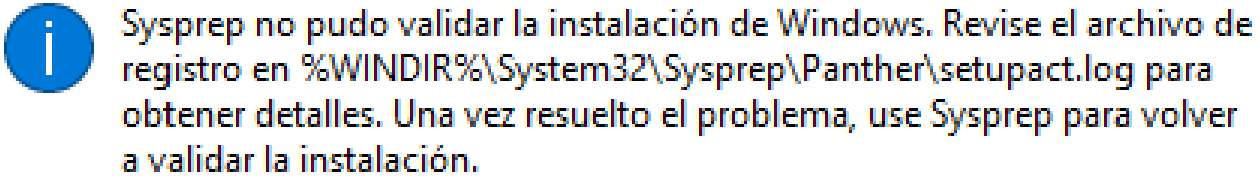
Intento 5: Outro xeito de executar un bat

- **Importante: Restauramos a instantánea**
- En **C:\Windows\Setup\Scripts**
- O arquivo **SetupComplete.cmd** execútase con permisos do usuario **System** antes de finalizar a instalación
- Quitamos o código para executar o .bat do **personalizado.xml**
- Poñemos as nosas instrucións nese .bat



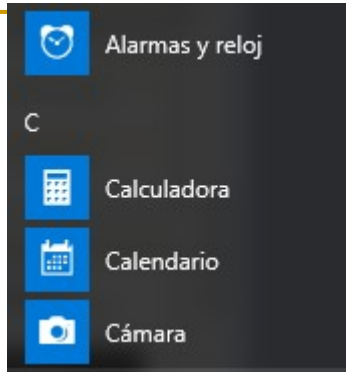
Posibles Problemas

Podemos atopar o seguinte erro o facer o Sysprep



- Se vemos o arquivo de log
  - C:\Windows\System32\Sysprep\Panther\setupact.log

```
2017-03-07 11:58:39, Error SYSPRP Package Microsoft.MicrosoftSolitaireCollection_3.9.5100.0_x64__8wekyb3d8bbwe was installed for a user, but not provisioned for all users. This package will not function properly in the sysprep image.
```



- O problema está en que creamos dous usuarios
  - Administrador
  - Usuario
- E iniciamos sesión con ambos
- Windows 10 provisiona certas apps da interface Modern
- As apps provisionadas son as que se instalan cada vez que iniciamos sesión con un novo usuario
- Despois de instalar os novos programas e actualizar o equipos, pode que algunha desas apps de problemas e non permita facer o sysprep
- A solución de desinstalála de cada usuario
- Podemos facelo de dous xeitos:
  - Powershell
  - ccleaner

Aplicacións instaladas para todos os usuarios

- `get-appxPackage -allusers | where publisherid -eq 8wekyb3d8bbwe | Format-list -property PackageFullName,PackageUserInformation`

```
PS C:\Windows\system32> get-appxPackage -allusers | where publisherid -eq 8wekyb3d8bbwe | Format-list -property PackageFullName,PackageUserInformation


PackageFullName        : Microsoft.VCLibs.120.00_12.0.21005.1_x86__8wekyb3d8bbwe
PackageUserInformation : {S-1-5-18 [S-1-5-18]: Staged}

PackageFullName        : Microsoft.VCLibs.120.00_12.0.21005.1_x64__8wekyb3d8bbwe
PackageUserInformation : {S-1-5-18 [S-1-5-18]: Staged}

PackageFullName        : Microsoft.NET.Native.Runtime.1.0_1.0.22929.0_x86__8wekyb3d8bbwe
PackageUserInformation : {S-1-5-21-632668091-650027800-445224884-1001 [usuario]: Installed,
                         S-1-5-21-632668091-650027800-445224884-500 [Administrador]: Installed}

PackageFullName        : Microsoft.NET.Native.Runtime.1.0_1.0.22929.0_x64__8wekyb3d8bbwe
PackageUserInformation : {S-1-5-21-632668091-650027800-445224884-1001 [usuario]: Installed,
                         S-1-5-21-632668091-650027800-445224884-500 [Administrador]: Installed}

PackageFullName        : Microsoft.NET.Native.Framework.1.0_1.0.22929.0_x86__8wekyb3d8bbwe
PackageUserInformation : {S-1-5-21-632668091-650027800-445224884-1001 [usuario]: Installed,
                         S-1-5-21-632668091-650027800-445224884-500 [Administrador]: Installed}
```

- Pode que teñamos aplicacións instaladas para só un usuario

```
Microsoft.BingNews_4.3.193.0_x86__8wekyb3d8bbwe
{S-1-5-21-632668091-650027800-445224884-500 [Administrador]: Installed}

Microsoft.BingSports_4.3.193.0_x86__8wekyb3d8bbwe
{S-1-5-21-632668091-650027800-445224884-1001 [usuario]: Installed}
```

- A solución máis sinxela é:
  - Borrar o usuario usuario
    - Témolo que facer dende o panel de control e indicando que queremos eliminar todos os seus arquivos
    - (Dende o administrador de usuarios non funcionaría)
  - Modificamos o script para que recree ó usuario
    - Net user usuario /add
  - Executar novamente o sysprep
    - Se aparece o erro outra vez, vemos no arquivo de log que app da o problema
    - Desinstalámola con powershell
      - get-appxpackage *3dbuilder* | remove-appxpackage

Creación da imaxe

Creación da imaxe

- Engadimos un 2º HD
- Iniciamos có System Rescue CD
- Preparamos o 2º HD para escribir nel
  - *cfdisk /dev/sdb*
  - *mkfs -t ext4 /dev/sdb1*
  - *mount /dev/sdb1 /mnt*
- Facemos unha copia da táboa de particións
  - *sfdisk -d /dev/sda > /mnt/tp.bak*
- Facemos unha copia do arranque
  - *dd if=/dev/sda of=/mnt/bootLoader.bak bs=512 count=63*

Creación da imaxe (2)

- Agora mesmo o fsarchiver non permite clonar particións ntfs correctamente

- Así que empregamos parclone.ntfs
  - *partclone.ntfs -c -s /dev/sda1 -o /mnt/win10.img*

```
root@sysresccd /root % partclone.ntfs -c -s /dev/sda1 -o /mnt/win10.img
Partclone v0.2.73 http://partclone.org
Starting to clone device (/dev/sda1) to image (/mnt/win10.img)
Reading Super Block
Elapsed: 00:00:02, Remaining: 00:00:00, Completed: 100.00%
Total Time: 00:00:02, 100.00% completed!
done!
File system:  NTFS
Device size:   34.4 GB = 8388095 Blocks
Space in use:   9.0 GB = 2200595 Blocks
Free Space:    25.3 GB = 6187500 Blocks
Block size:   4096 Byte
Elapsed: 00:06:59, Remaining: 00:00:00, Completed: 100.00%, Rate:   1.29GB/min,
current block:    2655426, total block:    8388095, Complete: 100.00%
Total Time: 00:06:59, Ave. Rate:    1.3GB/min, 100.00% completed!
Syncing... OK!
Partclone successfully cloned the device (/dev/sda1) to the image (/mnt/win10.im
g)
Cloned successfully.
```

Restauración da imaxe

Restauración da imaxe

- Restauramos a táboa de particións
- Restauramos o sistema con **partclone.ntfs**
  - *partclone.ntfs -r -s /mnt/win10.img -o /dev/sda1*

```
root@sysresccd /mnt % partclone.ntfs -r -s win10.img -o /dev/sda1
Partclone v0.2.73 http://partclone.org
Starting to restore image (win10.img) to device (/dev/sda1)
Calculating bitmap... Please wait... done!
File system:  NTFS
Device size:   34.4 GB = 8388095 Blocks
Space in use:   9.0 GB = 2200595 Blocks
Free Space:    25.3 GB = 6187500 Blocks
Block size:   4096 Byte
Elapsed: 00:05:27, Remaining: 00:00:00, Completed: 100.00%, Rate:   1.65GB/min,
current block:    2655426, total block:    8388095, Complete: 100.00%
Total Time: 00:05:27, Ave. Rate:    1.7GB/min, 100.00% completed!
Syncing... OK!
Partclone successfully restored the image (win10.img) to the device (/dev/sda1)
Cloned successfully.
```

Restauración do arranque

- Poderíamos restaurar o arranque coa copia que fixemos antes:
  - `dd if=/dev/sda of=/mnt/bootLoader.bak bs=512 count=63`
  - **Problema:**
    - Sería pouco flexible, xa que restauraríamos tamén a táboa de particións
    - Non poderíamos restaurar a particións máis grandes
- **Solución:**
  - Reparamos o MBR
    - `ms-sys -7 /dev/sda`
  - Reparamos o arranque de Windows
    - `partclone.ntfsfixboot -w /dev/sda1`

Imaxe Restaurada

- O equipo arranca e recoñece o novo hardware
- Os SID do equipo orixinal e o restaurado son diferentes

Orixinal

```
C:\Windows\system32>whoami /user

INFORMACIÓN DE USUARIO
----------------------

Nombre de usuario              SID
============================== ============================================
desktop-njo7ouk\administrador S-1-5-21-137993792-604642658-3203137243-500
```

Restaurado

```
C:\Users\Administrador>whoami /user

INFORMACIÓN DE USUARIO
----------------------

Nombre de usuario    SID
==================== ============================================
if4-xx\administrador S-1-5-21-1473910781-3603349826-2185459480-500
```