

Remove policies, usign registry editor, for WAHA mode.

Para remover políticas en modo WAHA, se puede seguir el siguiente step by step.

1. *Realizar conexión remota a una máquina que se encuentre en red de tp,*
 - en este caso se puede utilizar el comando Windows+R y en la ventana ejecutar, escribir el comando “mstsc” (ver figura 1) este mismo nos permitirá realizar la conexión remota en este caso para la máquina de Teleperformance donde iniciaremos el proceso.

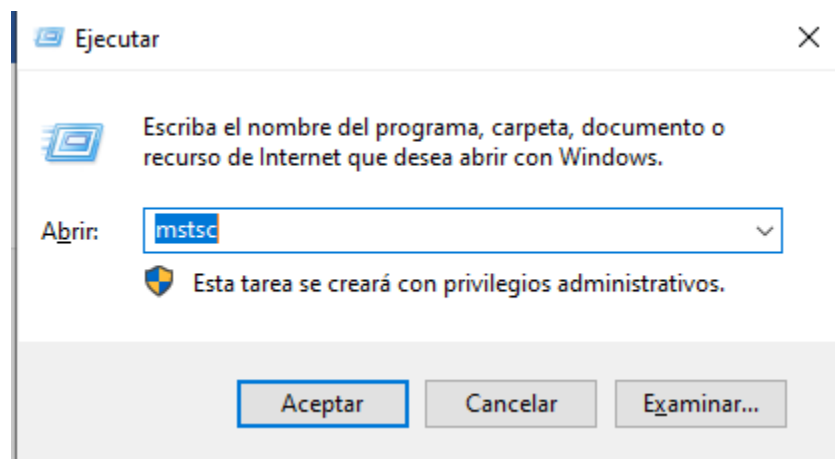


Figura 1

- Luego presionar aceptar, se nos abrirá una ventana donde nos pedirá o la ip de la maquina o el nombre de la misma (ver figura 2), presionamos conectar y colocamos las credenciales de acuerdo al usuario por el ingreso

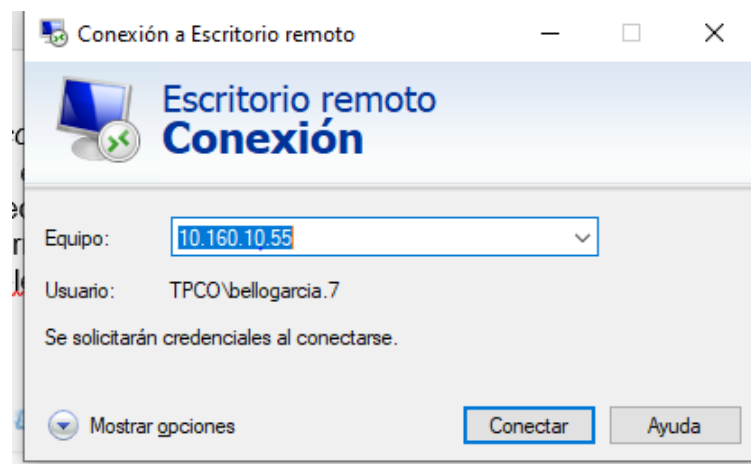


Figura 2

- Una vez estemos dentro de la maquina remota, ejecutamos nuevamente el buscador con Windows+R, y ejecutamos el comando “Regedit”, se nos abrirá una ventana emergente donde se encuentran alojados los registros de la máquina (ver figura 3).

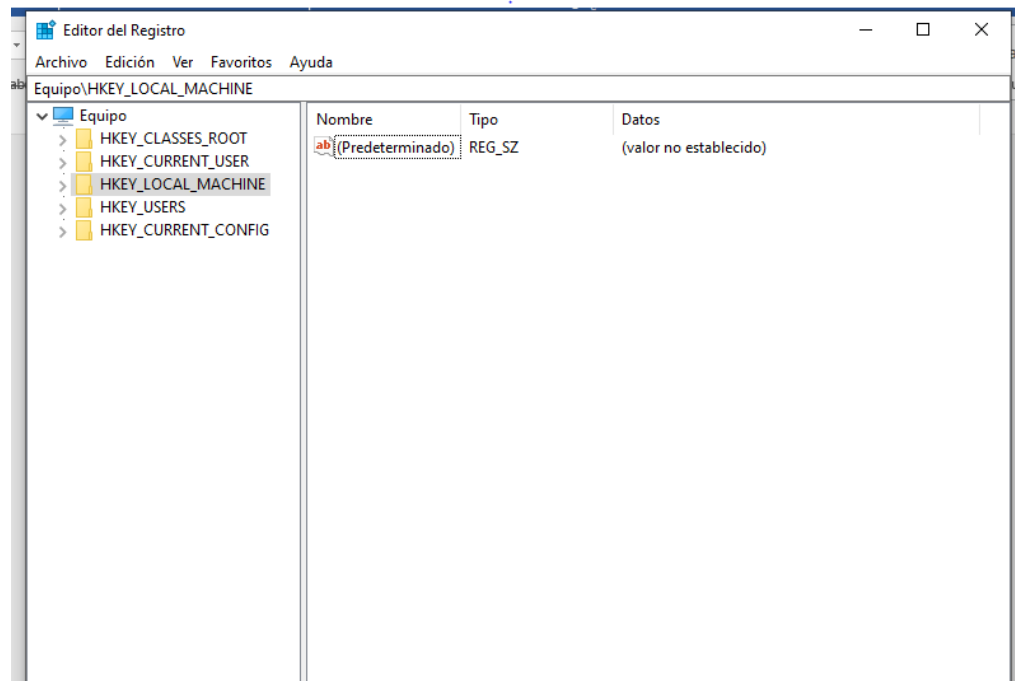


Figura 3

2. Realizar conexión remota al equipo que deseamos eliminar políticas.

- En este proceso básicamente conectaremos la maquina donde estamos remoteados con la que deseamos quitar políticas, siguiendo el siguiente proceso, en la barra de opciones de la ventana indicada, presionar la opción archivo y nos desplazamos a la opción, conectar a registro de red, luego presionamos aceptar, donde nos aparecerá una ventana (ver figura 4). En esta misma se colocará o el nombre de la máquina que deseamos alcanzar o la ip local asignada por la vpn.

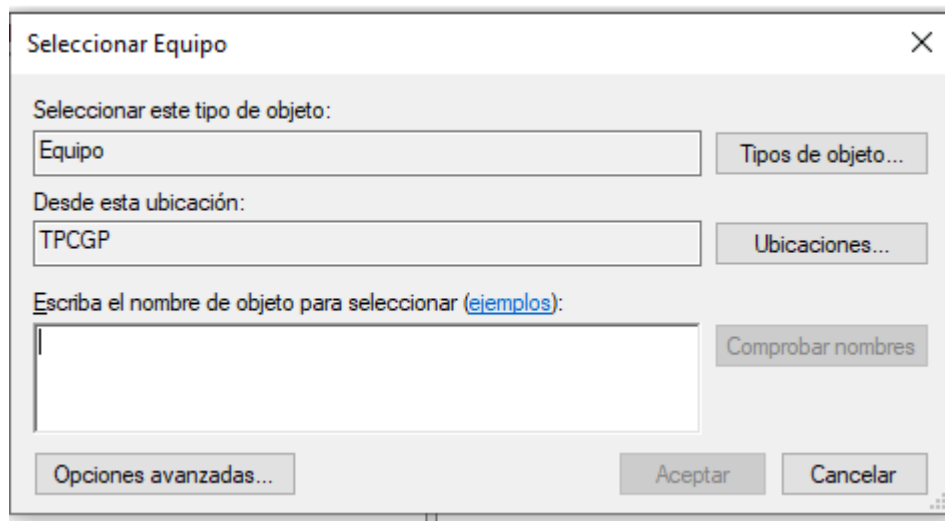


Figura 4

- Una vez colocada la dirección ip correspondiente o el nombre de la máquina, seleccionamos aceptar y básicamente nos cargaran los registros de la máquina a la que deseamos removerle políticas.

3. Ubicar registro de políticas correspondiente de acuerdo al usuario.

- En este paso realizaremos la búsqueda de la ruta específica que nos permitirá encontrar las políticas que tiene la sesión del usuario cargada, atento en este proceso ya que puede ser algo tedioso.
- Es necesario ubicar la siguiente ruta: **Equipo\HKEY_USERS\S-1-5-21-4123172745-1281542410-1921287844-1002\Software\Microsoft\Windows\CurrentVersion\Policies.** (Ejemplo de ruta generado con computador de prueba)
- Atención en este punto, la parte de la ruta mostrada como ejemplo (\S-1-5-21-4123172745-1281542410-1921287844-1002\) es variable de acuerdo al usuario, a su vez la cantidad de carpetas con nombre parecido varía de acuerdo a la cantidad de usuarios logeados en la máquina, sin embargo, esta misma es verificable.
- La carpeta terminada en “CLASSES” no se debe validar ya que esta no nos servirá, solo validar las carpetas que tengan el nombre como en el ejemplo, y para verificar que es la correspondiente al usuario que le vamos a quitar las políticas entramos a la siguiente ruta. Equipo\HKEY_USERS\S-1-5-21-4123172745-1281542410-1921287844-1002\Environment.
- Al entrar en la carpeta environment podemos validar el nombre del usuario y con eso verificar si estamos en el registro correspondiente. (ver figura 5). La prueba se realizó con un equipo donde la sesión del usuario era “DESKTOP-R”

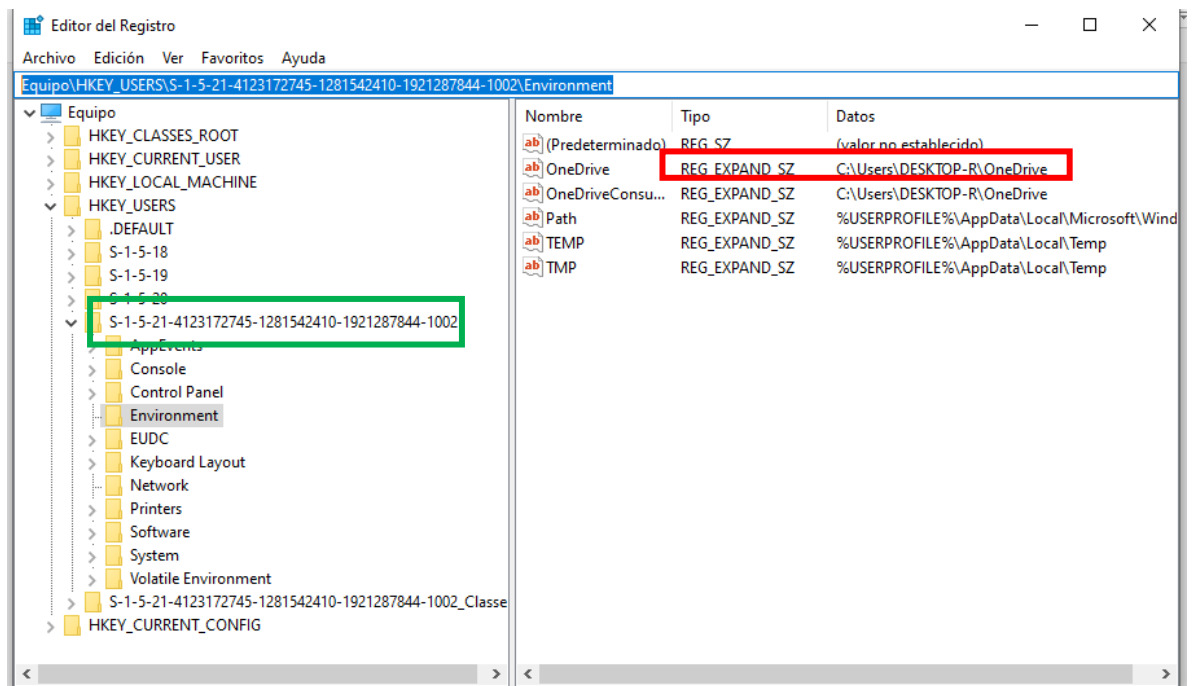


Figura 5

- Una vez validada la ruta del usuario a eliminar políticas, nos devolvemos a la carpeta principal (ejemplo marcado en recuadro verde de la figura 5), y ubicamos en orden descendiente la ruta **\Software\Microsoft\Windows\CurrentVersion\Policies**.
- Una vez nos encontremos en la carpeta de políticas, antes de borrarlas es necesario exportarlas presionando click derecho sobre ella, luego exportar y luego la dirección donde se guardarán las políticas, no es necesaria alguna dirección específica, (ver figura 6), esto con el fin de poder guardarlas e importarlas una vez terminado el proceso. De esta manera nos aseguramos que la sesión del usuario se le reapliquen las políticas eliminadas.
- Al ubicar la carpeta "POLICES" presionar suprimir sobre ella y esto la eliminará

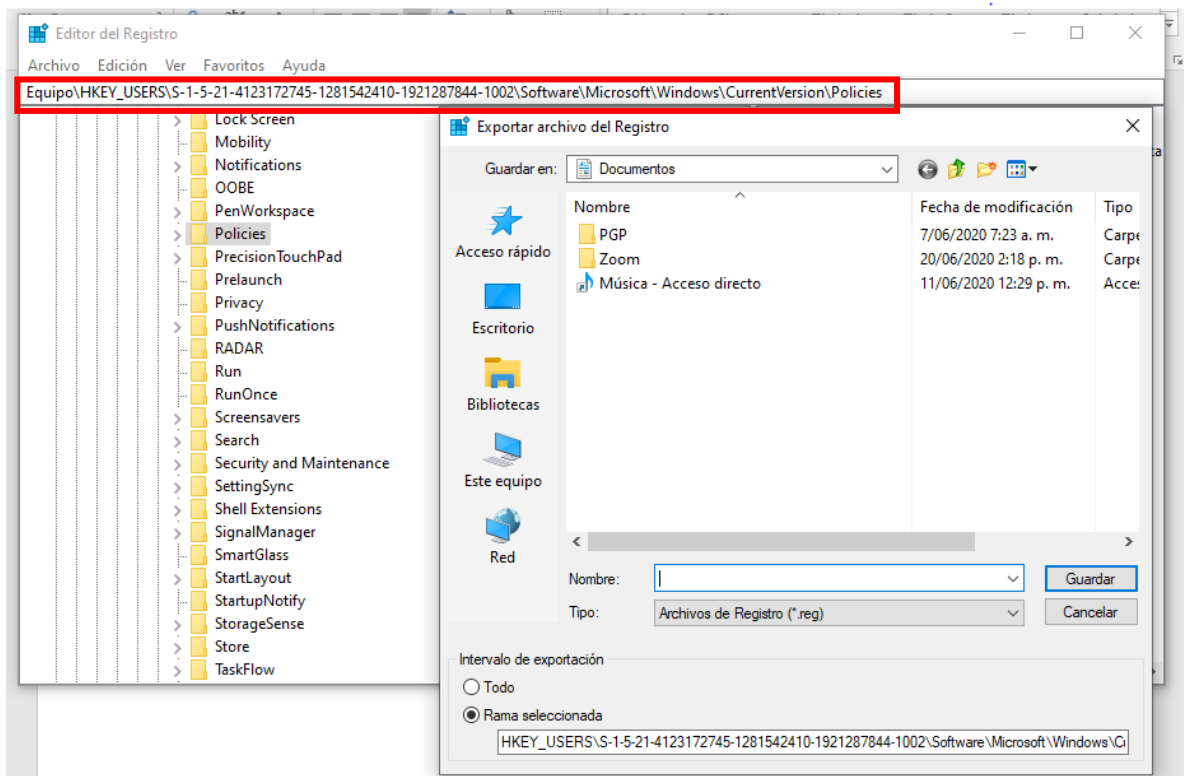


Figura 6

4. *Dejar en el escritorio del usuario los archivos de registro y el .bat de reinicio del explorador de Windows.*
 - Para esto es necesario entrar por debajo a la máquina con el comando **\\(NOMBREDEMAQUINA O IP)\c\$** y en el escritorio del usuario, dejarle el archivo (*.reg) y el (.bat) de reinicio del explorer.exe
 - Al eliminar la carpeta de "POLICES" es necesario correr el archivo .bat de reinicio del explorador de Windows para que queden removidas las políticas, dicho bat se puede ubicar en la siguiente ruta **\\10.160.10.16\Shared\Analistas\Román Bello\bats (RESTART EXPLORER- ESCRITORIO)**.
 - Una vez eliminada la carpeta indicada y ejecutado el (.bat) dicha sesión de usuario quedará libre de políticas para realizar el proceso necesario.

5. *Reestablecer políticas a la sesión del usuario una vez finalizada la actividad.*
 - Para finalizar el proceso y dejar la sesión del usuario con las respectivas políticas es necesario ejecutar el archivo que anteriormente habíamos exportado (*.reg) y ubicado en el escritorio del usuario según el paso 4.1, con esto la máquina volverá a tomar las políticas que habíamos eliminado y no tendremos el riesgo de una máquina sin políticas.