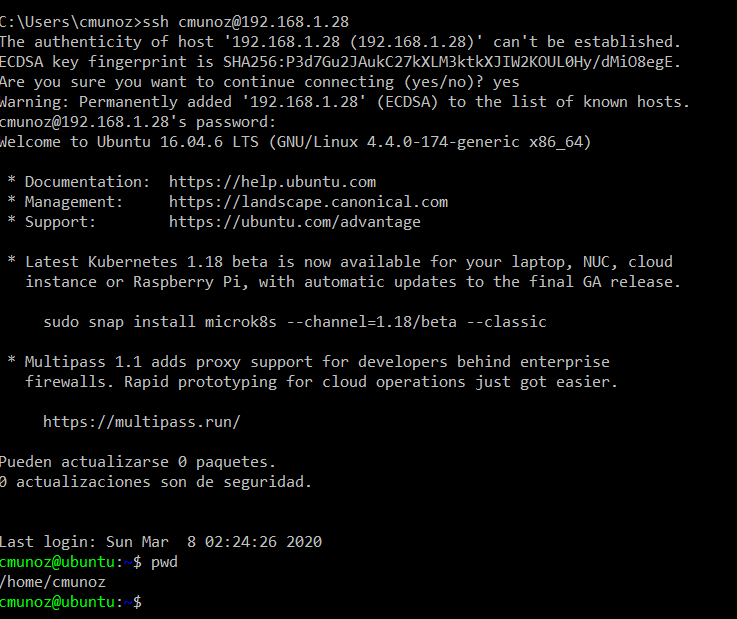
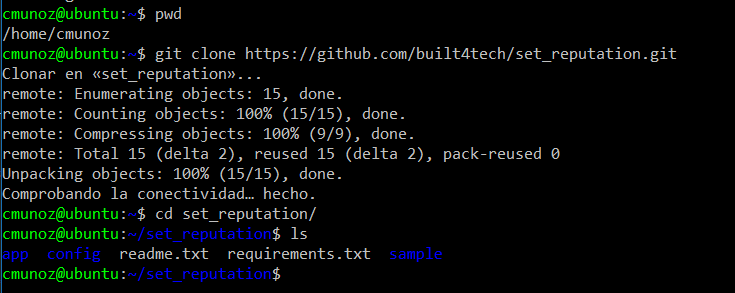
# Procedimiento para montar el entorno

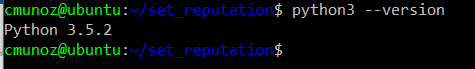
1. SSH al sistema Linux intermedio desde el cual se ejecutará el proceso.



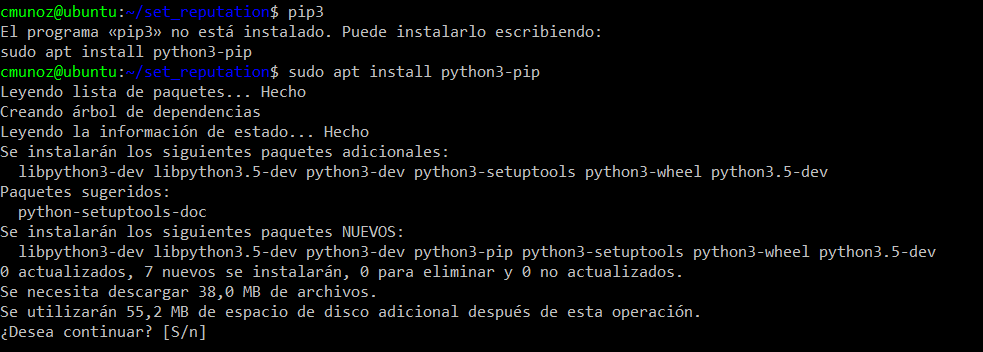
1. Clonamos el repositorio de información



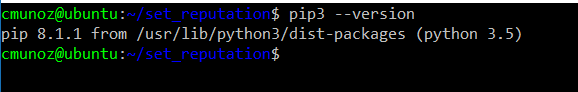
1. Comprobar que Python versión 3 se encuentra instalado



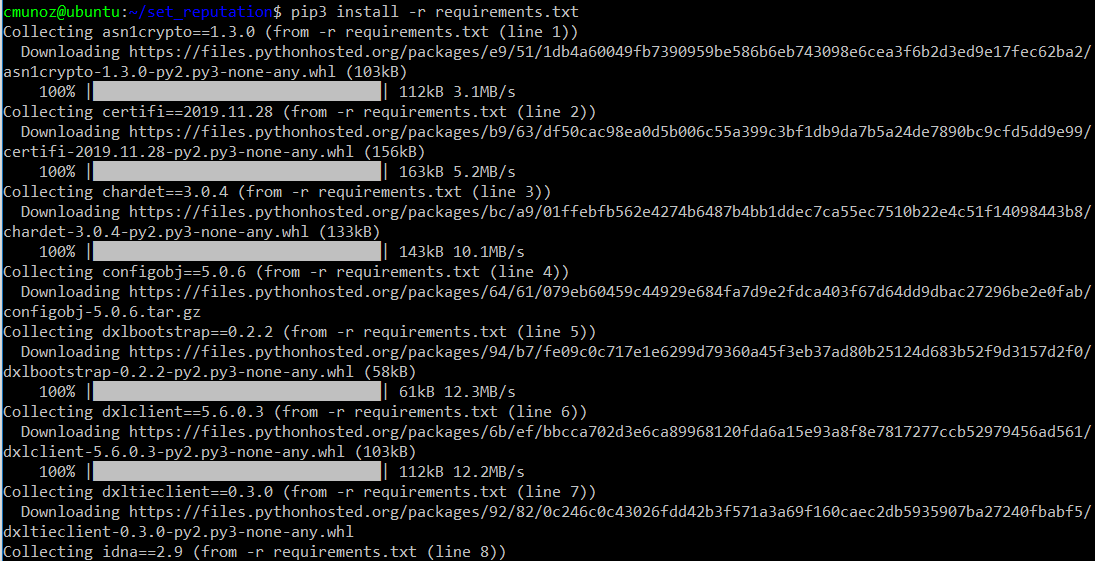
1. Comprobar que el gestor de paquetes pip se encuentra instalado, en caso contrario instarlo.



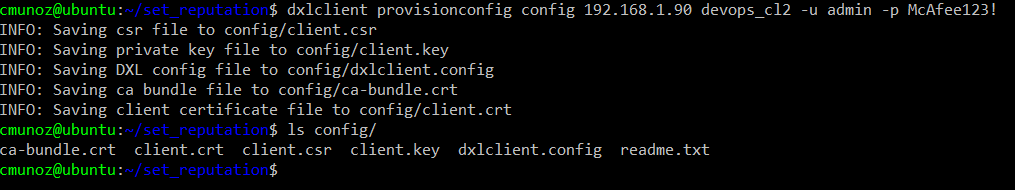
1. Comprobar que el gestor de paquetes se ha instalado correctamente



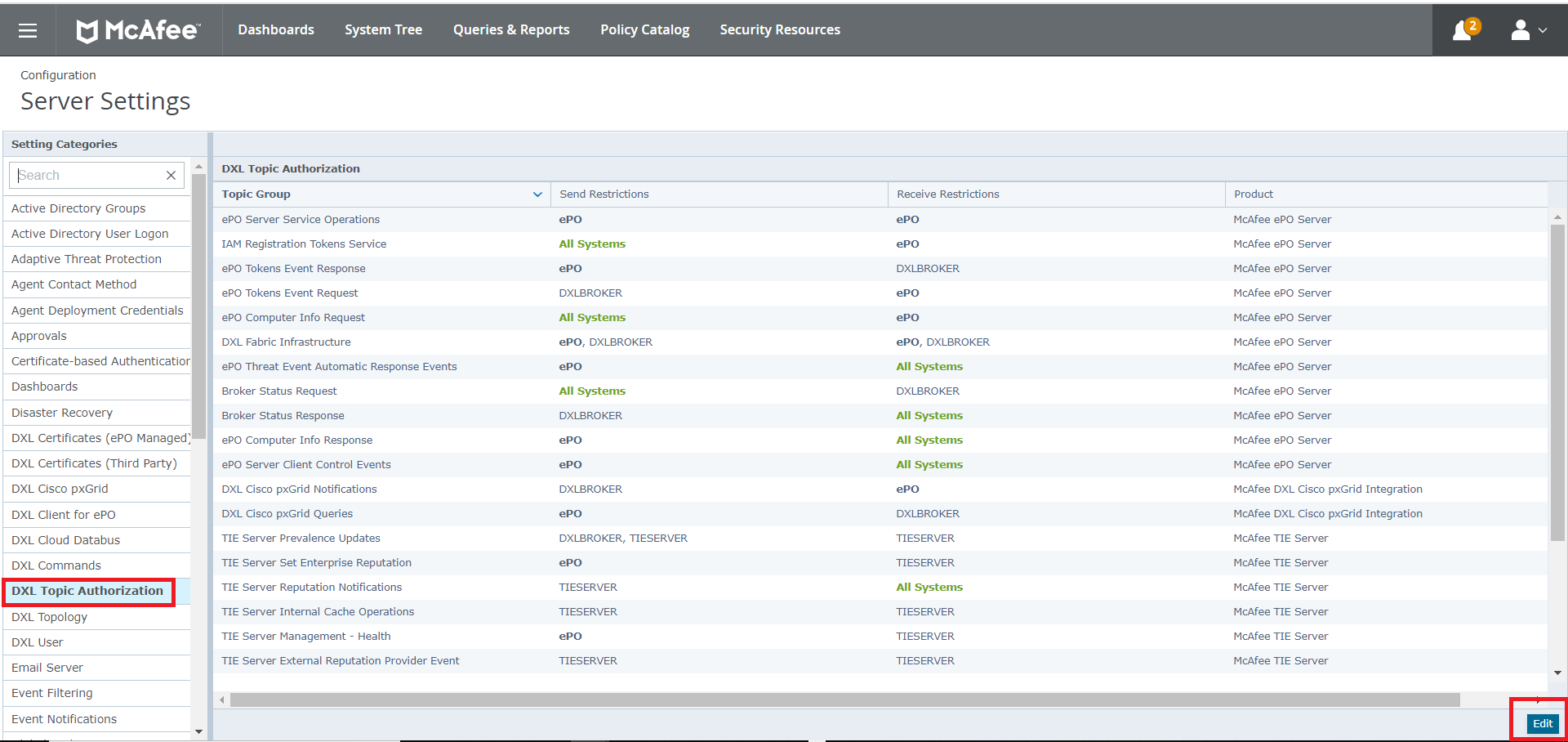
1. Instalar las librerías necesarias

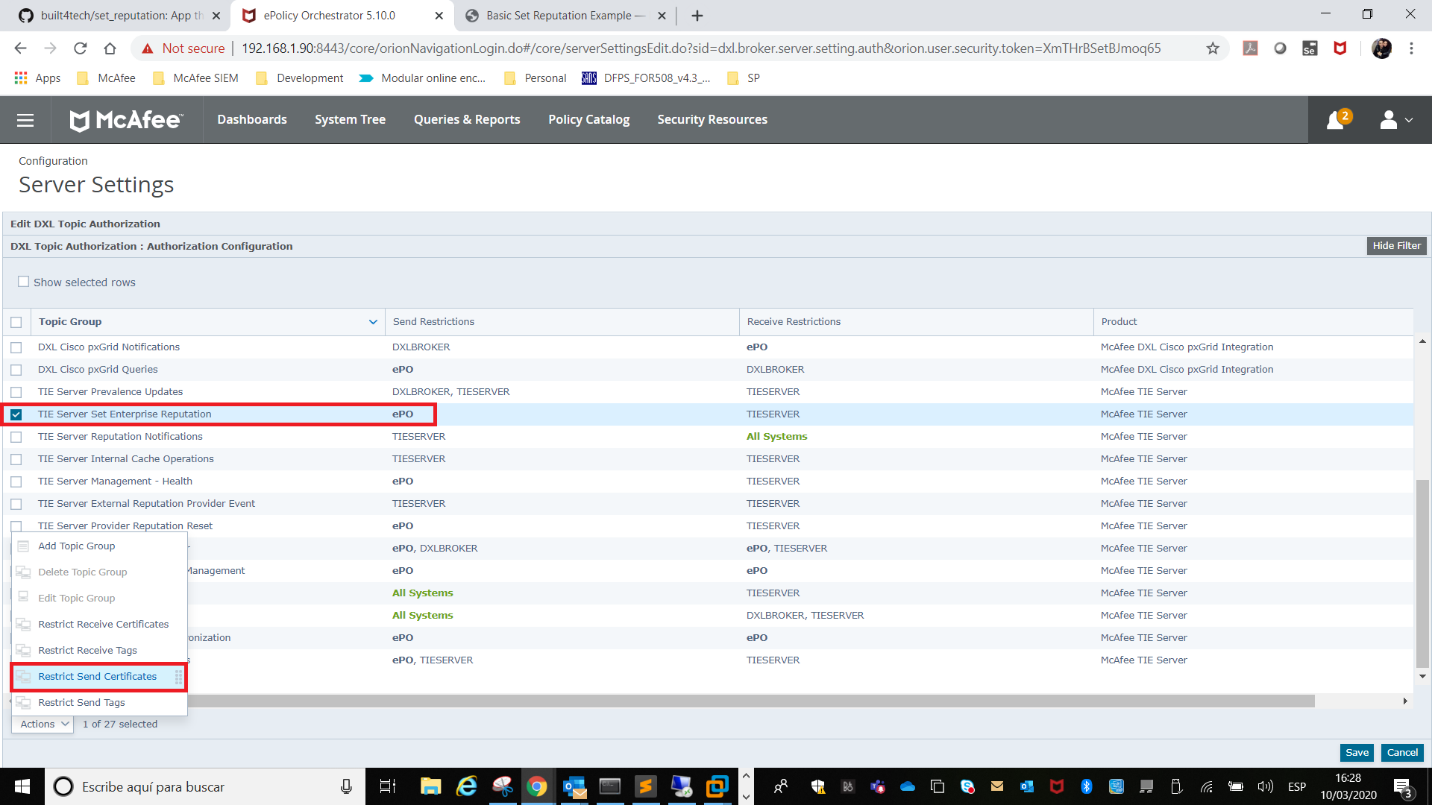


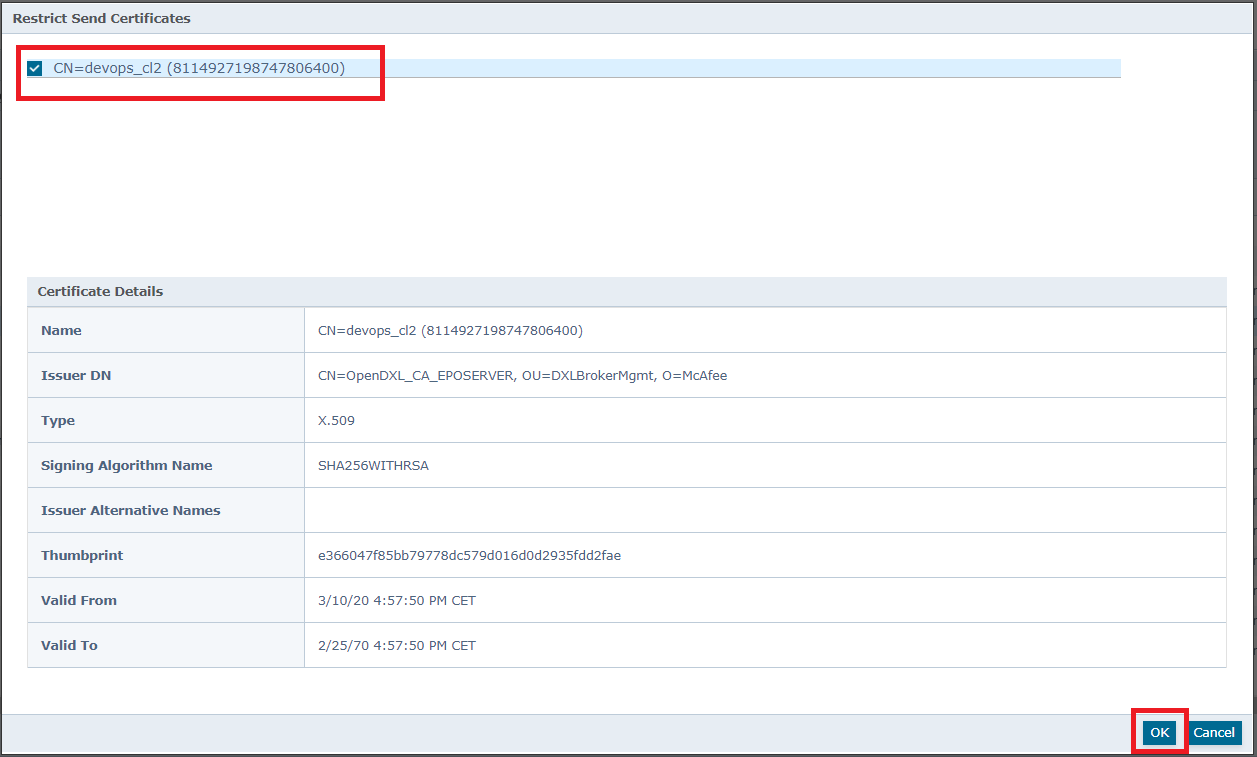
1. Conectar con el servidor ePO con permisos de administración para la generación de los certificados necesarios, comprobar que los certificados se han creado correctamente en la carpeta config.

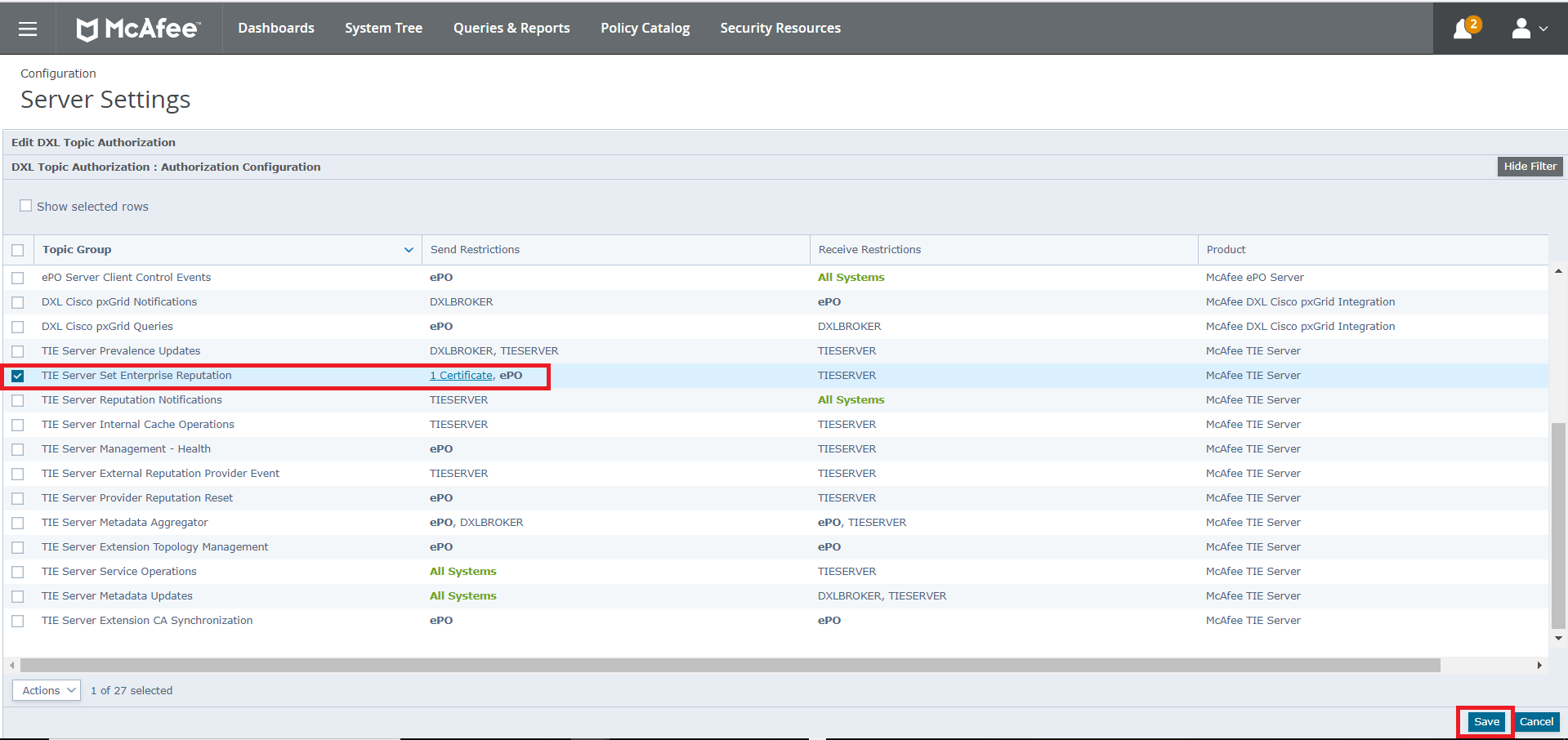


1. Conectar con el servidor ePO y asignar permisos al nuevo certificado (devops\_cl2) para que pueda establecer reputaciones en el servidor de TIE

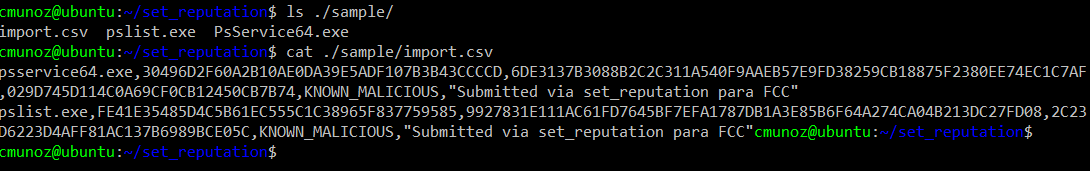




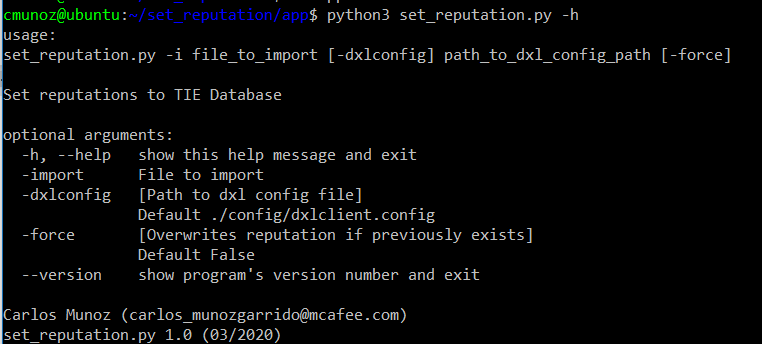


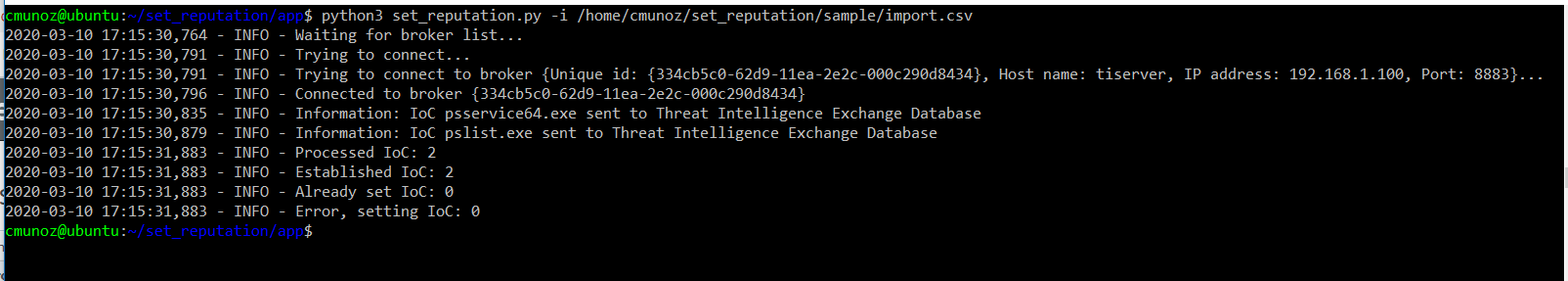


1. Comprobar el fichero csv, para entender que será importado en la BBDD de TIE

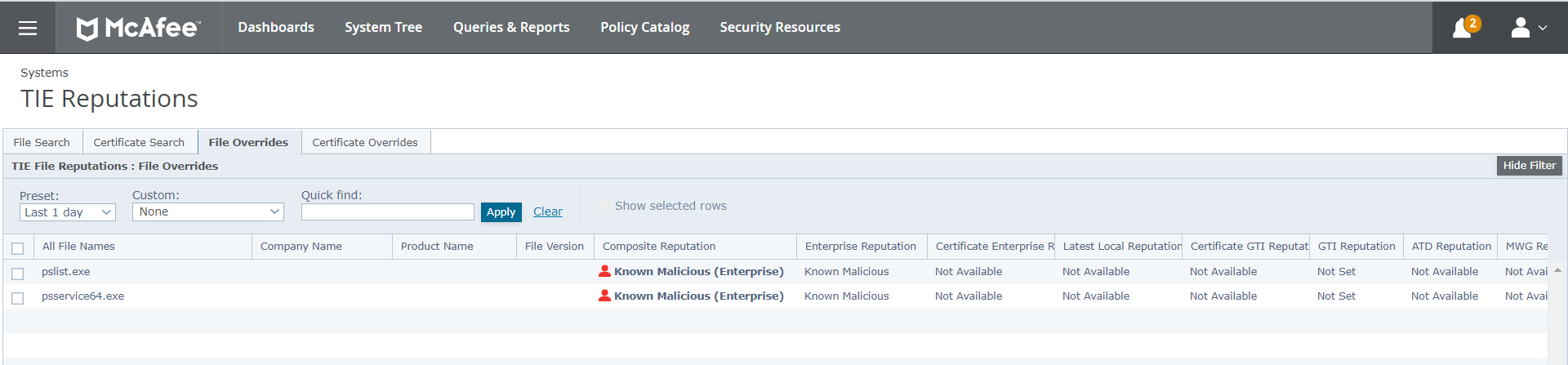


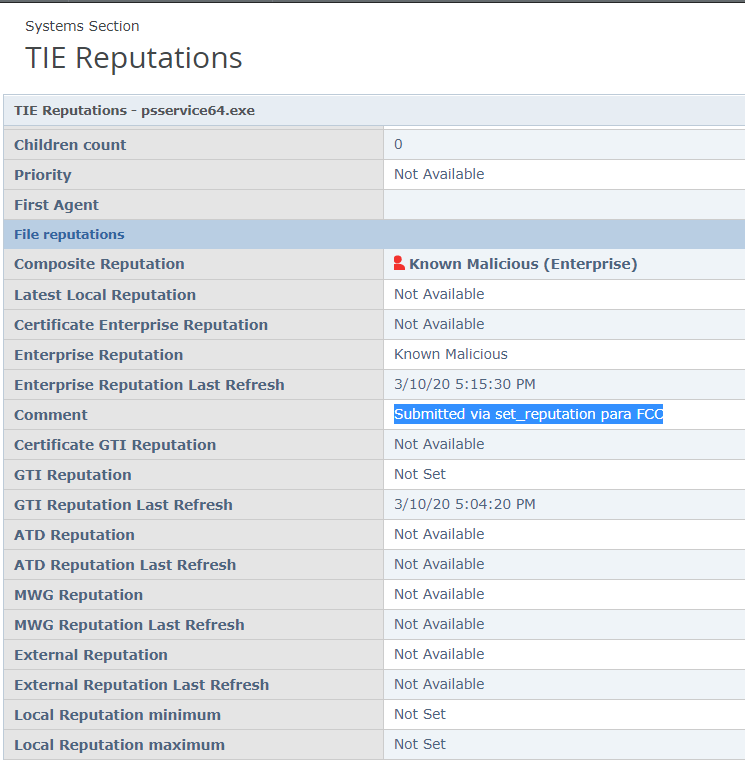
1. Ejecutamos el script, tal y como se indica



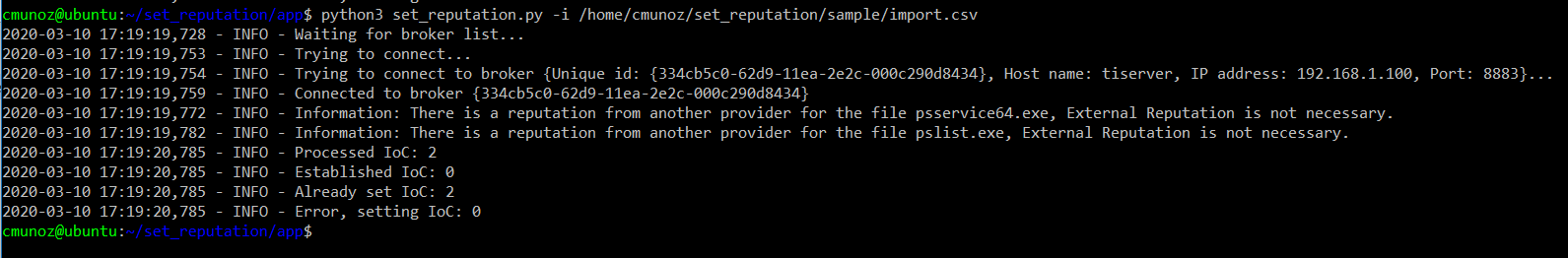


1. Comprobamos la aplicación de la reputación en la BBDD de TIE

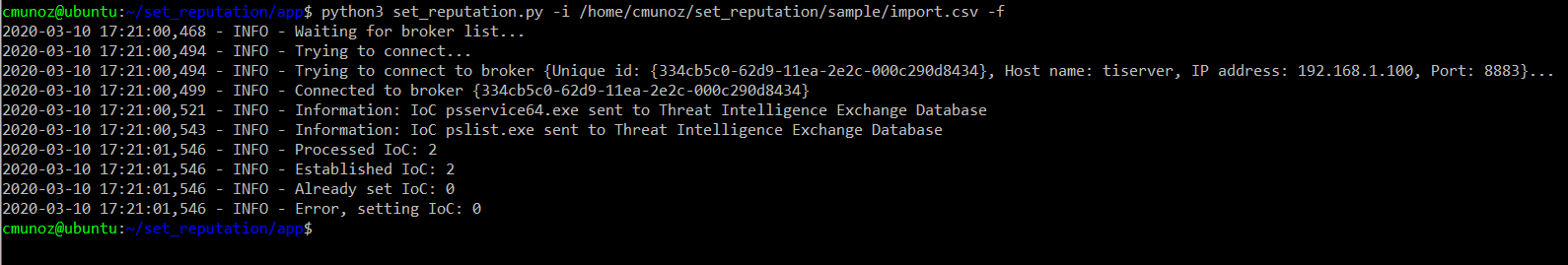




1. Si se intenta ejecutar de nuevo el procedimiento con el mismo conjunto de IoC a importar el script se da cuenta de ello e impide la actualización de la BBDD



1. Se ha creado en cualquier caso el parámetro -force para forzar la aplicación del cambio, con independencia de que exista previamente en la BBDD



1. A partir de este momento, ningún cliente conectado a TIE y con una política que bloquee Known Malicious podrá ejecutar los archivos enviados.