**Arquitectura y Soporte TI**

**Guía para generar**

**llave pública/privada de**

**autenticación GAW**

**Preparado por**

**Andy Castro Amaiquema**

**Arquitectura y Soporte IT**

Banco Bolivariano

2022

# **Resumen Ejecutivo**

El presente instructivo permite configurar un mecanismo adicional de autenticación BBO-Cliente, utilizando un esquema de seguridad asimétrico generando un par de llaves pública y privada.

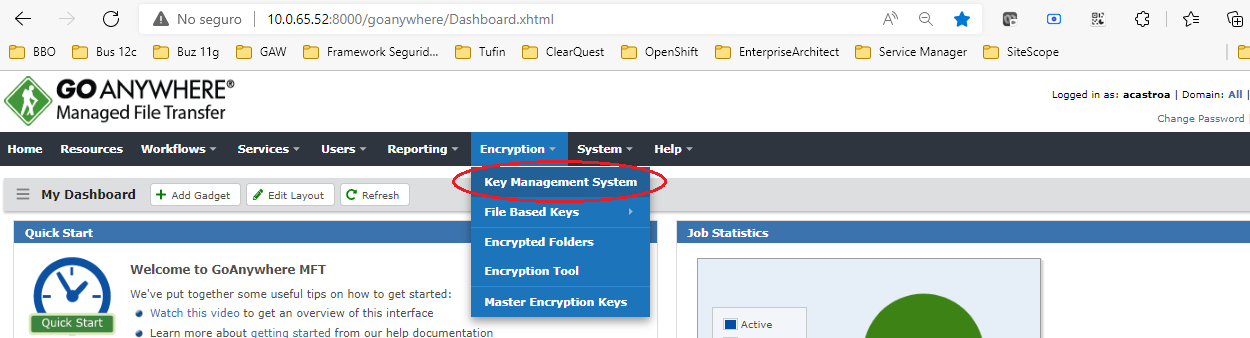
El objetivo es dar a cliente únicamente la llave pública, mientras BBO mantenga llave privada para robustecer la conectividad y seguridad en ambos lados.

# **Configuración.**

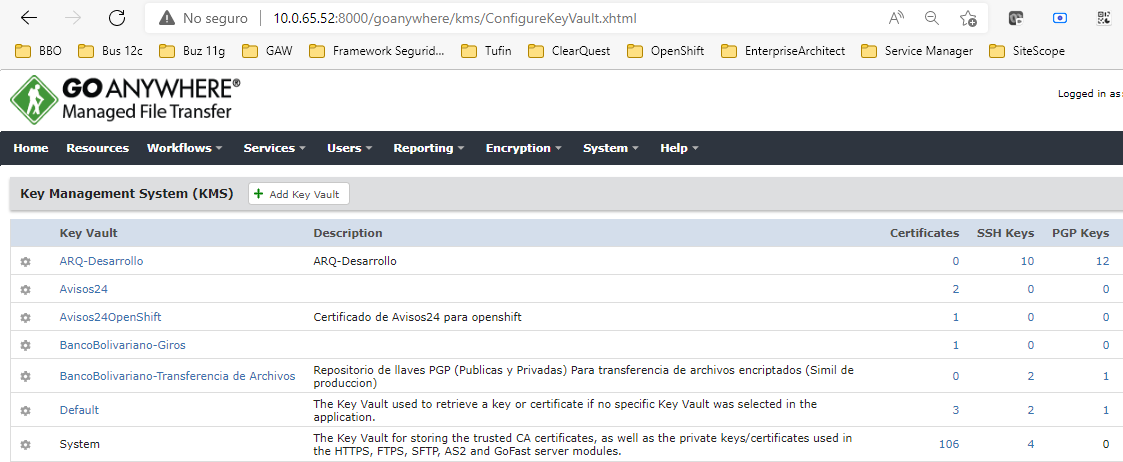
Se tiene presente que la custodia y gestión de esta información únicamente debe ser atendida por personal de Seguridad de la Información. Por aquello se realiza esta guía que les permitirá gestionarlo:

# **Creación de llaves**

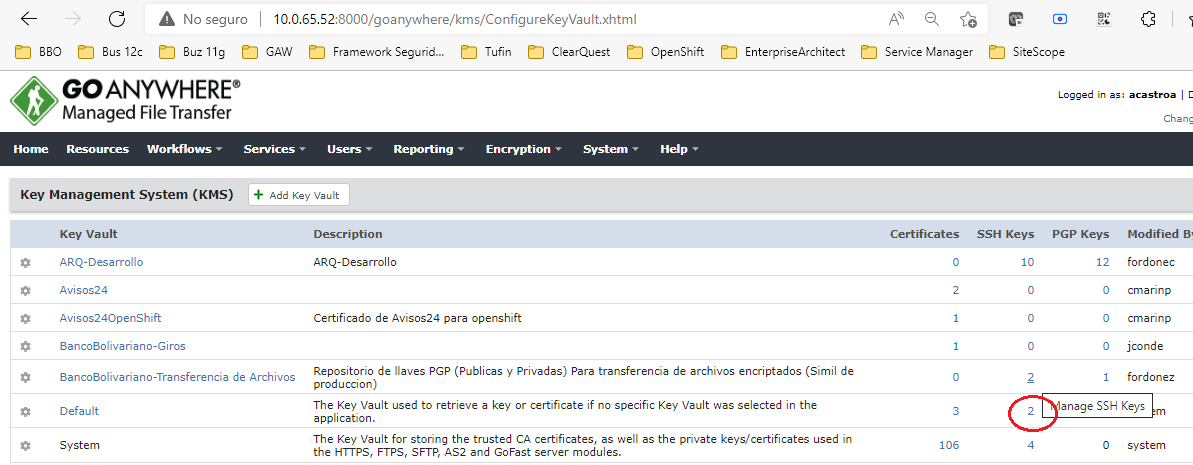
Para crear llaves de seguridad, el usuario debe tener permisos administrativos o poder visualizar la siguiente opción del menú **Encryption**:



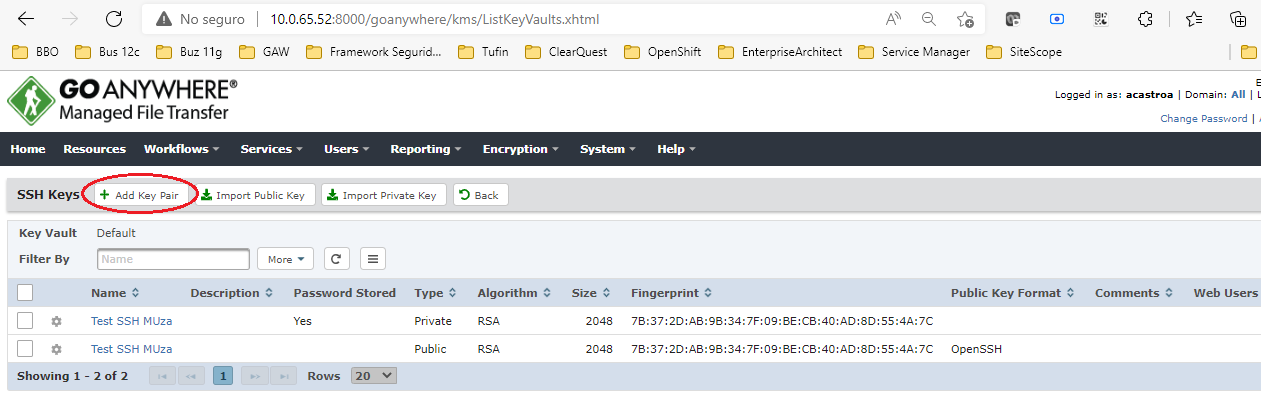
Una vez seleccionada la opción del menú, se visualiza la siguiente pantalla. Aquí S.I. deberá contemplar que KMS debería utilizar para determinada conectividad/cliente:



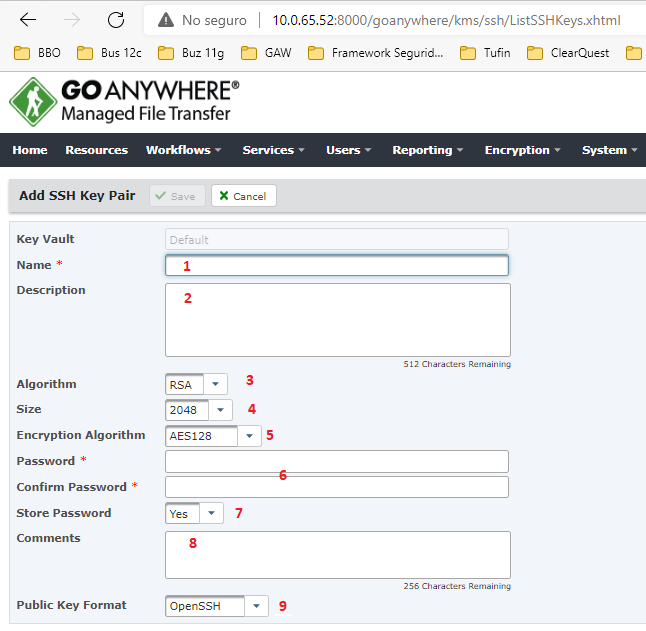
Teniendo ubicado cual **Key Management System** (KMS) a utilizar, se debe hacer clic en el número que está ubicado en dirección de la columna SSH Key, tal cual se observa en la imagen. Para el caso de la imagen, el KMS seleccionado fue **Default**, el número 2 que está encerado indica 2 llaves configuradas:



Desde punto anterior, se accede a la siguiente pantalla en donde permite crear un par de llaves, tal cual se lo señala en la imagen:

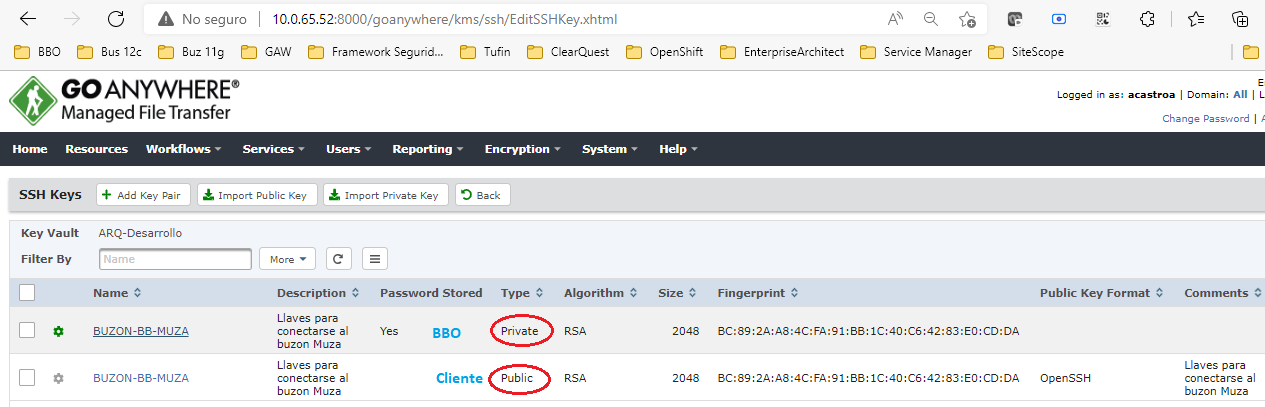


Para el caso de agregar un nuevo par de llaves, se visualizará el siguiente formulario, que debe ser llenado a criterio de la conectividad que sea desea realizar:



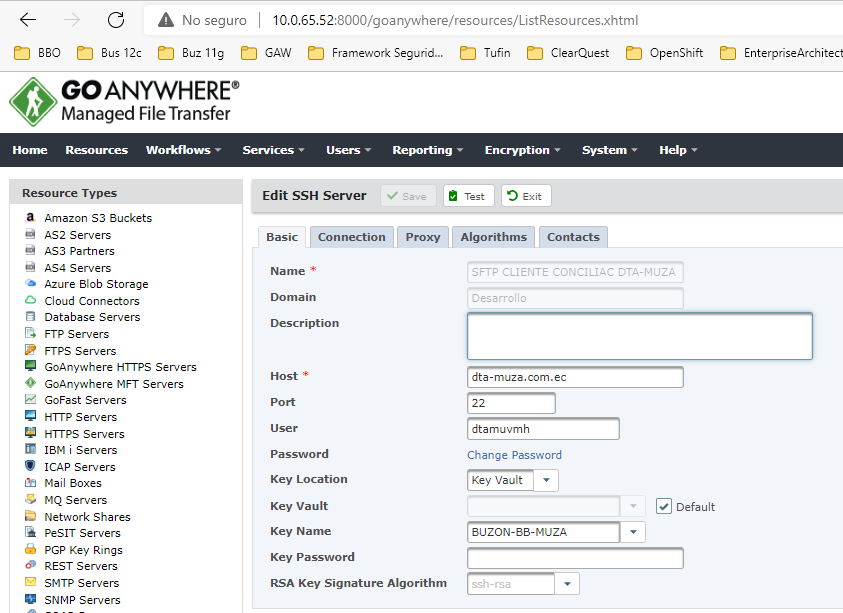
|  |  |
| --- | --- |
| **1** | Nombre representativo del par de claves a crear |
| **2** | Breve descripción del par de llaves |
| **3** | Tipo de algoritmo asimétrico a utilizar |
| **4** | Tamaño de la llave a utilizar con el algoritmo simétrico |
| **5** | Tipo de encriptación |
| **6** | Contraseña empleada en la configuración, como segundo factor de seguridad |
| **7** | Opción para almacenar contraseña |
| **8** | Comentarios adicionales de ser el caso |
| **9** | Formato de la clave pública a utilizar. OpenSSH en caso del ejemplo MUZA |

Una vez agregada la información en el formulario haciendo clic en “Save”, se procede a crear el par de llaves. Regresando a la pantalla principal de SSH Key, se observará el par de llaves creadas. Para el registro realizado, deberán existir **2 filas** que corresponde a una fila por la llave pública y otra fila por la llave privada.

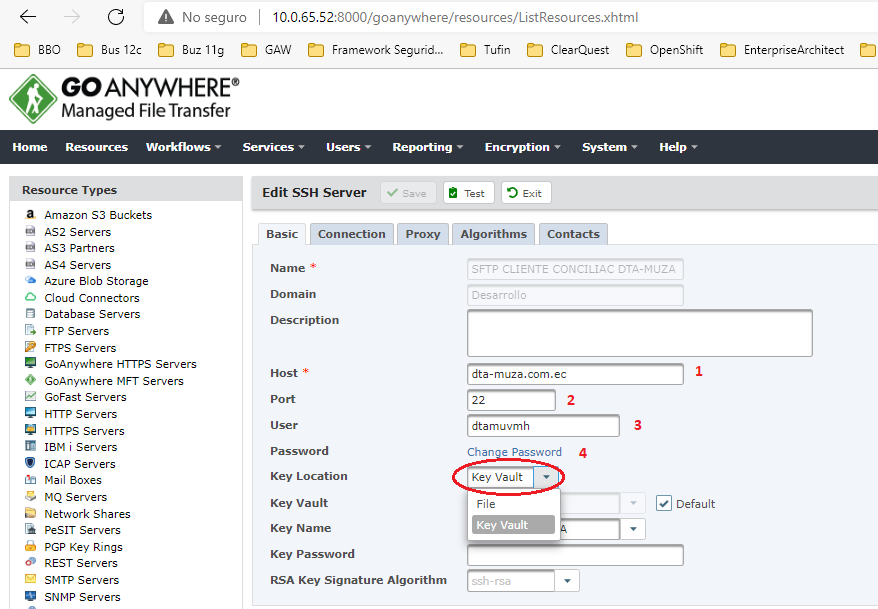


# **Pruebas.**

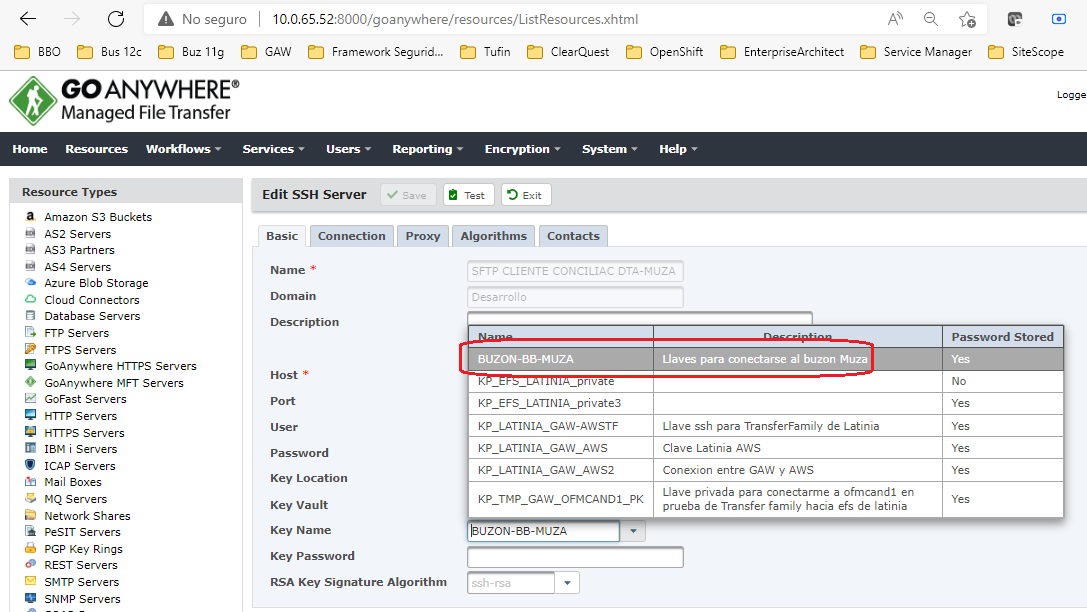
Para las respectivas pruebas del par de llaves, se deberá utilizar un componente que permita anexar y utilizar el par de llaves creado. Se expone unas pruebas realizadas con un componente especificado creado para el cliente MUZA:



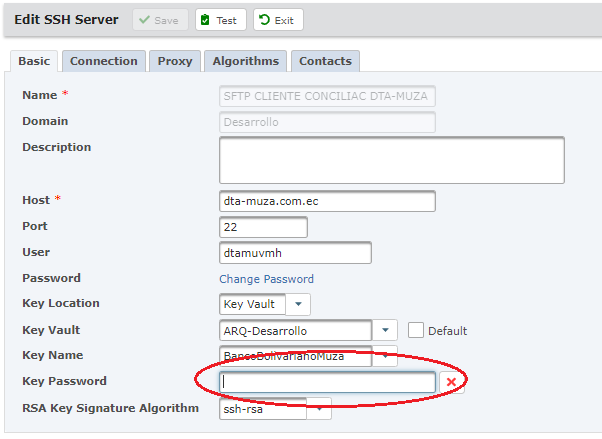
En el componente se indica el host **1**, puerto **2**, usuario **3** y clave **4** creada para la conectividad. La clave (Campo **Password**) es enviada por el cliente. En la información de **Key Location** se debe seleccionar **key Valult**, según imagen:



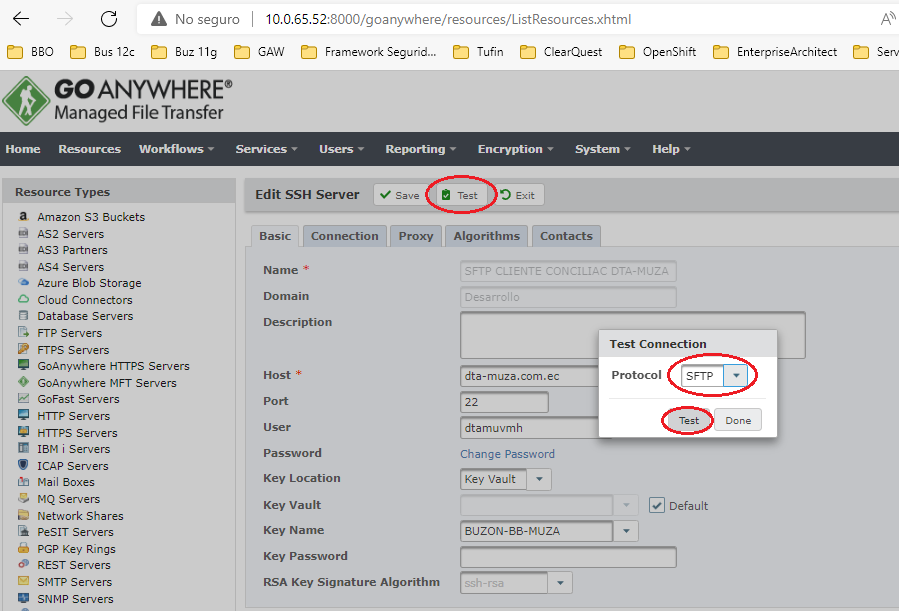
En la información de **Key Name** se debe seleccionar la llave que fue creada según guía del actual documento. En el cuadro presentado en la imagen, se presentan todas las llaves que han sido creadas.



De igual manera se debe colocar el **Key Password**; esta clave es la misma clave colocada en el campo **Password** del formulario; Se indica nuevamente que esta clave es la que genera y envía el cliente.



Una vez colada toda la información y seleccionada la llave, estaríamos listos para realizar una prueba de conectividad para validar la configuración del recurso actual. Guiar según imagen.



Una prueba exitosa de conectividad mostraría la siguiente pantalla:

