Guía de desarrollo, Anexo 22.06

Acceso a servidores FTP-SFTP

Arquitectura de Sistemas

GERENCIA INFORMÁTICA
JOSEFA VALCÁRCEL, 44
28027-MADRID

Índice General

1 Introducción

Hasta la fecha, la DGT contaba con 2 servidores ftp/sftp desplegados en el entorno de producción para dar servicio a las diferentes aplicaciones y procesos que requerían intercambiar ficheros.

Con el objeto de actualizar y mejorar la seguridad en los accesos, se han desplegado dos nuevos servidores SFTP para sustituir a los actuales. Además, se ha desplegado un servidor adicional para dar servicio a los entornos de preproducción y desarrollo que, hasta estos momentos, estaban utilizando los servidores de producción.

1.1 Objetivo

Este documento tiene la finalidad de describir las funcionalidades, normas de uso y forma de acceso al servicio.

1.2 Audiencia

Este documento está dirigido a los equipos de desarrollo y, en general, a cualquier equipo o departamento que requiera el uso de los servidores SFTP.

1.3 Glosario

Los términos y acrónimos que se utilizan en este documento y en el resto de documentos de la guía se encuentran recogidos por orden alfabético en el Anexo 30. Glosario con el objetivo de facilitar su lectura y comprensión.

1.4 Estructura del documento

Este documento está distribuido en 3 capítulos, con los siguientes contenidos:

- Capítulo 1: Introducción, contiene información relativa al propio documento.
- Capítulo 2: Descripción y características solución implantada.

- Capítulo 3: Contiene formas de acceso, protocolos, usuarios, normas básicas de uso.

2 Características solución implantada

Tal y como se ha indicado en la introducción, siguiendo el modelo de arquitectura ya existente, se han desplegado 3 nuevos servidores, cuyas datos se detallan a continuación.

2.1 Entorno de producción

2.1.1 Servidor Internet

Dará servicio a los procesos que en el intercambio de ficheros intervengan aplicaciones internas y organizaciones externas que requieran el acceso vía internet.

- Nombre máquina virtual: **vmSFTPproinet01**
  - DNS interno: **sftp-inet.trafico.es** (10.50.146.41)
  - DNS público: **interfichero.dgt.es** (212.128.100.159)

2.1.2 Servidor Intranet

Dará servicio a los procesos que en el intercambio de ficheros intervengan aplicaciones internas o accesos desde/hacia red SARA.

- Nombre máquina virtual: **vmSFTPprointr01**
  - DNS interno: **sftp.trafico.es** (10.50.142.48)

2.2 Entorno de preproducción

2.2.1 Servidor Internet/Intranet

Inicialmente se ha desplegado un único servidor, que dará servicio a los procesos y aplicaciones de los entornos de desarrollo y preproducción que requieran el acceso desde la intranet y/o internet.

- Nombre máquina virtual: **vmSFTPpre01**

- DNS: **sftppre.trafico.es** (10.50.106.162)
- DNS Público: **interfichero-pre.dgt.es** (212.128.100.232)

3 Acceso

3.1 Puertos y protocolos

Los servidores se han configurado para escuchar por los siguientes puertos:

- SFTP: 1365/tcp.
- FTP: 21/tcp, 60000-63000/tcp (ftp pasivo).

Con carácter general, las conexiones se establecerán siempre utilizando el protocolo SFTP. El acceso mediante protocolo FTP está habilitado únicamente para ofrecer compatibilidad con los sistemas internos DGT que, por causa técnica justificada, no puedan implementar el protocolo SFTP. (Los servidores están configurados para atender peticiones FTP únicamente a los orígenes que se autoricen).

Con el objeto de mejorar la seguridad en los accesos con protocolo FTP, se ha activado FTPS (FTP sobre TLS. No confundir con SFTP) con una configuración relajada (TLSRequired off) de manera que, si el cliente lo soporta, se establece la conexión utilizando TLS. En caso contrario, se seguirá utilizando el protocolo ftp sin seguridad.

3.2 Reglas de firewall

Acceso FTP. Las reglas necesarias para el acceso desde redes internas DGT ya están solicitadas por lo que, en principio, no sería necesario solicitar reglas adicionales.

Acceso SFTP. Al solicitar las reglas, para evitar apertura de puertos incorrecta, se deberá especificar que se solicita el puerto 1365/tcp.

3.3 Usuarios

3.3.1 Alta nuevos usuarios

En el caso de ser necesario solicitar un nuevo usuario, se deberá abrir el ticket correspondiente indicando, al menos, los siguientes datos:

- Servidor al que accederá:
    - Entornos de desarrollo y preproducción:
        - sftppre.trafico.es / interfichero-pre.dgt.es (intranet/internet).
    - Entorno de producción:
        - sftp.trafico.es (intranet)
        - sftp-inet.trafico.es / interfichero.dgt.es (internet).
        - O ambos, si fuera necesario.
- Aplicación.
- Solicitante, persona o equipo responsable y datos de contacto.
- Propósito del usuario.
- Espacio de almacenamiento estimado (ver punto 3.3.3).

3.3.2 Autenticación usuarios

Además de método tradicional mediante usuario/contraseña, el protocolo SFTP nos permite el acceso sin contraseña mediante claves SSH. Para ello, se deberá proporcionar la clave pública del usuario (en formato RFC4716) al equipo encargado de administrar los servidores, para que sea incluida en el fichero authorized_keys del usuario en cuestión en el servidor SFTP que corresponda.

3.3.3 Espacio de almacenamiento

Cuando se solicite el alta de un nuevo usuario se deberá facilitar una estimación del espacio en disco requerido y su justificación. Si no se informa de dicho dato, la configuración por defecto de los servidores establece una cuota de 100 Mb a cada usuario (una vez alcanzada dicha cuota, el servidor no permitirá subir más ficheros).

Los usuarios, aplicaciones y scripts automatizados que suban/descarguen ficheros en los servidores, una vez que el intercambio de ficheros ha finalizado (Por ej. usuario1 carga fichero1 desde

servidor1 y usuario1 descarga fichero desde servidor2), deberán establecer los mecanismos necesarios para que el contenido ya procesado sea eliminado.

Es importante tener en cuenta que los servidores SFTP no se pueden considerar como un espacio de almacenamiento permanente ni un lugar para guardar copias de seguridad.

3.4 Acceso FTP anónimo a directorios públicos (solo en sftp.trafico.es)

Al igual que en el antiguo servidor, se ha configurado un directorio que permite el acceso público de forma anónima (solo protocolo ftp). Dentro de ese subdirectorio, inicialmente se han configurado 2 subdirectorios diferenciados:

```
├── PUBLICO
└── UTILIDADES-SOFTWARE
```

PUBLICO: Directorio temporal (lectura y escritura) destinado para compartir de forma rápida ficheros entre usuarios dentro de la intranet. **No está pensado como repositorio de software, almacenamiento permanente o backup. Los usuarios deberán eliminar el contenido una vez que el destinatario ha descargado el contenido.**

A la hora de cargar contenido sensible, es importante tener en cuenta que se trata de un directorio público, **al que cualquier usuario dentro de la intranet DGT puede acceder, leer y eliminar contenido.**

El contenido con más de 30 días de antigüedad será eliminado de forma automática.

UTILIDADES-SOFTWARE: Directorio de acceso público que contiene diversas utilidades y aplicaciones (solo lectura).