WHM Transfer Tool: error SSH key invalid format en OpenSSH 8.0

WHM Transfer Tool: error SSH key "invalid format" en OpenSSH 8.0

Síntoma

Al configurar WHM Transfer Tool para migrar una cuenta desde un servidor remoto usando autenticación por llave SSH, la conexión falla con:

```
Load key "/root/.ssh/servidor_remoto": invalid format
root@servidor.example.com: Permission denied (publickey,gssapi-keyex,gssapi-with-mic)
```

La llave existe, tiene permisos `600`, y `cat` muestra un contenido aparentemente correcto que empieza con:

```
-----BEGIN OPENSSH PRIVATE KEY-----
```

Causa raíz

La llave fue generada en un servidor con **OpenSSH >= 7.8** (formato nuevo `OPENSSH PRIVATE KEY`), pero el servidor que intenta usarla (donde corre WHM) tiene **OpenSSH 8.0 de CentOS/CloudLinux/AlmaLinux 8**, que **no soporta este formato para autenticación**.

Esto es confuso porque:

- `file ~/.ssh/llave` dice `OpenSSH private key` (parece válido)
- `ssh-keygen -l -f ~/.ssh/llave` muestra el fingerprint correctamente
- Pero `ssh -i ~/.ssh/llave` falla con `invalid format`

El binario `ssh` y `ssh-keygen` son programas distintos y el soporte de formatos no es idéntico en versiones antiguas empaquetadas por Red Hat.

Servidores afectados

Cualquier servidor con:

- **CentOS 8** / **CloudLinux 8** / **AlmaLinux 8** (OpenSSH 8.0p1)
- **CentOS 7** (OpenSSH 7.4) — también afectado
- cPanel no actualiza OpenSSH del sistema, usa la versión del OS

NO afecta a:

- **Ubuntu 22.04+** (OpenSSH 8.9+)
- **AlmaLinux 9** / **Rocky 9** (OpenSSH 8.7+)
- **Debian 12** (OpenSSH 9.2)

Diagnóstico

```
# 1. Verificar versión de OpenSSH en el servidor WHM (destino)
ssh -V
# Si dice OpenSSH_8.0 o inferior → afectado

# 2. Verificar formato de la llave
head -1 ~/.ssh/llave_remota
# Si dice "BEGIN OPENSSH PRIVATE KEY" → formato nuevo (incompatible)
# Si dice "BEGIN RSA PRIVATE KEY" → formato PEM clásico (compatible)

# 3. Confirmar el fallo
ssh -i ~/.ssh/llave_remota -p PUERTO -o BatchMode=yes root@servidor_remoto hostname
# Si dice "Load key: invalid format" → confirmado
```

Solución

Opción A: Generar llave nueva en formato PEM (recomendado)

Desde el servidor WHM (destino), generar una llave directamente en formato compatible:

```
# Generar llave RSA 4096 en formato PEM clásico
ssh-keygen -t rsa -b 4096 -m PEM -f ~/.ssh/servidor_remoto -N "" -C "root@$(hostname)"

# Verificar que tiene el formato correcto
head -1 ~/.ssh/servidor_remoto
# Debe decir: -----BEGIN RSA PRIVATE KEY-----
```

Luego autorizar la pública en el servidor remoto (origen):

```
# Copiar la pubkey al servidor remoto
ssh-copy-id -i ~/.ssh/servidor_remoto.pub -p PUERTO root@servidor_remoto

# O manualmente:
cat ~/.ssh/servidor_remoto.pub | ssh -p PUERTO root@servidor_remoto "cat >>
~/.ssh/authorized_keys"
```

Verificar:

```
ssh -i ~/.ssh/servidor_remoto -p PUERTO root@servidor_remoto hostname
```

Opción B: Convertir llave existente (requiere OpenSSH nuevo)

Si tienes acceso a un servidor con OpenSSH >= 7.8:

```
# Convertir de formato OPENSSH a PEM (en servidor con OpenSSH moderno)
ssh-keygen -p -m PEM -f ~/.ssh/llave -N "" -P ""

# Verificar
head -1 ~/.ssh/llave
# Ahora debe decir: -----BEGIN RSA PRIVATE KEY-----
```

Nota: esto NO funciona desde el propio servidor con OpenSSH 8.0 — el mismo `ssh-keygen` que lee el fingerprint no puede convertir el formato. Hay que hacerlo desde otro servidor con versión más

reciente.

Configuración en WHM Transfer Tool

Una vez resuelta la llave:

1. **WHM → Transfer Tool → Copy an Account**
2. **Remote Server:** `servidor_remoto.example.com`
3. **Port:** el puerto SSH del servidor remoto
4. **Authentication:** SSH Key
5. **Key path:** `/root/.ssh/servidor_remoto`
6. Seleccionar las cuentas a migrar

Aplica también fuera de cPanel

Este problema **no es exclusivo de WHM Transfer Tool**. Afecta a cualquier uso de `ssh -i` en servidores con OpenSSH empaquetado por Red Hat/CentOS/CloudLinux 8 o anterior cuando la llave privada está en formato nuevo.

Ejemplos afectados:

- **rsync con llave:** `rsync -e "ssh -i ~/.ssh/llave" ...`
- **scp con llave:** `scp -i ~/.ssh/llave ...`
- **Scripts de backup** que usan llaves SSH
- **JetBackup** con destinos SSH
- **cPanel Backup Transport** a servidor remoto

Prevención

Al generar llaves SSH que se usarán en servidores con CentOS/CloudLinux 7-8, usar siempre:

```
ssh-keygen -t rsa -b 4096 -m PEM -f ~/.ssh/nombre_llave -N "" -C "comentario"
```

El flag `-m PEM` fuerza el formato clásico compatible con todas las versiones.

Documentado: 2026-03-17 — Incidente real migrando cuenta de servidor20 a central (ambos CloudLinux 8, OpenSSH 8.0)

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de Castris

Si necesitas soporte profesional puedes contratar con Castris soporte profesional.

Revision #2
Created 2026-03-17 03:59:17 UTC by Abkrim
Updated 2026-03-17 04:00:42 UTC by Abkrim