CloudLinux CageFS: Resolución de Problemas SSL/OpenSSL

Problema

En servidores CloudLinux con CageFS habilitado, las aplicaciones PHP (como Laravel, WordPress, etc.) pueden experimentar errores SSL al intentar realizar conexiones HTTPS externas:

```
error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed
```

Servicios típicamente afectados:

- Google reCAPTCHA
- Servicios SMTP (envío de emails)
- APIs externas HTTPS
- cURL/file_get_contents() con SSL

Causa Raíz

CageFS aísla a cada usuario en su propio entorno virtualizado, impidiendo el acceso a recursos del sistema como los certificados CA ubicados en `/etc/ssl/certs/` y `/usr/share/ca-certificates/`.

Verificación del Problema

```
# Como root - funciona correctamente
openssl s_client -connect www.google.com:443 -verify_return_error
# Resultado: Verify return code: 0 (ok)

# Como usuario enjaulado - falla
sudo -u usuario php -r "
\$context = stream_context_create(['ssl' => ['verify_peer' => true]]);
\$result = file_get_contents('https://www.google.com', false, \$context);
```

```
echo \$result ? 'SSL OK' : 'SSL FAILED';
"
# Resultado: SSL FAILED
```

Solución Definitiva

La solución correcta es **agregar el paquete `ca-certificates` completo al esqueleto de CageFS**:

```
# 1. Agregar el paquete ca-certificates al esqueleto de CageFS
cagefsctl --addrpm ca-certificates

# 2. Forzar actualización completa del esqueleto
cagefsctl --force-update

# 3. Montar/remontar el esqueleto
cagefsctl -M
```

Ejemplo de Salida del Proceso

Durante `cagefsctl --force-update`, verás output similar a:

```
Copying /usr/sbin/update-ca-certificates to /usr/share/cagefs-skeleton/usr/sbin/update-ca-certificates
Copying /usr/share/ca-certificates/mozilla/ACCVRAIZ1.crt to /usr/share/cagefs-skeleton/usr/share/ca-certificates/mozilla/ACCVRAIZ1.crt
Copying /usr/share/ca-certificates/mozilla/AC_RAIZ_FNMT-RCM.crt to /usr/share/cagefs-skeleton/usr/share/ca-certificates/mozilla/AC_RAIZ_FNMT-RCM.crt
Copying /usr/share/ca-certificates/mozilla/AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.crt to /usr/share/cagefs-skeleton/usr/share/ca-certificates/mozilla/AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.crt
Copying /usr/share/ca-certificates/mozilla/ANF_Secure_Server_Root_CA.crt to /usr/share/cagefs-skeleton/usr/share/ca-certificates/mozilla/ANF_Secure_Server_Root_CA.crt
Copying /usr/share/ca-certificates/mozilla/Actalis_Authentication_Root_CA.crt to /usr/share/cagefs-skeleton/usr/share/ca-certificates/mozilla/Actalis_Authentication_Root_CA.crt
Copying /usr/share/ca-certificates/mozilla/AffirmTrust_Commercial.crt to /usr/share/cagefs-skeleton/usr/share/ca-certificates/mozilla/AffirmTrust_Commercial.crt
```

```
Copying /usr/share/ca-certificates/mozilla/AffirmTrust_Networking.crt to /usr/share/cagefs-skeleton/usr/share/ca-certificates/mozilla/AffirmTrust_Networking.crt
Copying /usr/share/ca-certificates/mozilla/AffirmTrust_Premium.crt to /usr/share/cagefs-skeleton/usr/share/ca-certificates/mozilla/AffirmTrust_Premium.crt
[... continúa copiando todos los certificados CA ...]
```

Verificación Post-Solución

```
# Test desde usuario enjaulado
su - ilustrex
-bash-5.1$ openssl s_client -connect www.google.com:443 -verify_return_error
CONNECTED(00000003)
depth=2 C = US, O = Google Trust Services LLC, CN = GTS Root R1
verify return:1
depth=1 C = US, O = Google Trust Services, CN = WR2
verify return:1
depth=0 CN = www.google.com
verify return:1
---
...
# Resultado esperado: SSL OK en CageFS
```

Ventajas de esta Solución

- **Oficial**: Usa funcionalidad nativa de CageFS
- **Completa**: Incluye todo el ecosistema de certificados CA
- **Mantenible**: Se actualiza automáticamente con el sistema
- **Segura**: No compromete la integridad del sandbox
- **Universal**: Funciona para todas las aplicaciones PHP/OpenSSL

Logs útiles:

- Laravel: `storage/logs/laravel.log`
- PHP-FPM: `/var/log/php-fpm/error.log`
- Apache: `/var/log/httpd/error_log`

Notas Técnicas

- **CageFS Skeleton**: Directorio compartido `/usr/share/cagefs-skeleton` que contiene archivos seguros para todos los usuarios
- **Comando cagefsctl --addrpm**: Agrega paquetes RPM completos al esqueleto, no solo archivos individuales
- **Persistencia**: La solución se mantiene entre reinicios y actualizaciones del sistema

Documentación Relacionada

- CloudLinux CageFS Documentation
- CageFS Command Line Tools

Fecha de actualización: Agosto 2025
Versiones probadas: Ubuntu 24.04, CageFS 6.x+
Estado: Solución verificada y recomendada

Revision #1
Created 2025-08-04 12:34:21 UTC by Abkrim
Updated 2025-08-04 12:37:04 UTC by Abkrim