NATO Communications and Information Agency
Agence OTAN d'information et de communication

HOW TO ENABLE SSL FOR DIRECT DATABASE REPLICATION

Last updated: 04 April 2022

Applies to: LOGFAS **7.x.x.**

Table of contents

Document change log			
Version	Comments	Date	Author
1.0	Initial version	23-Mar-22	Stanislav HRABOVSKY

HOW TO ENABLE SSL FOR DIRECT DATABASE REPLICATION

1. GENERAL

Database replication component is offering different methods for the set-up of DB replication. Direct method can be configured either using SSL protocol or without SSL (unsecured). In case of more secure way the recommendation is to use SSL option on.

For meeting this requirement the certain mandatory steps need to be executed as a prerequisite.

2. SYMPTOMS

Wrong SSL configuration can end-up with the following error statements:

- [localhost logfas_name] SSL error: sslv3 alert bad certificate
- [localhost logfas_name] Fatal error occured: 28000: no pg_hba.conf entry for host "203.0.113.6", user "admin", database "logfas_name", SSL off
- [localhost logfas_name] Fatal error occured: The remote certificate is invalid according to the validation procedure.

3. CAUSE

Misconfiguration of Replication component and LOGFAS main configuration files or wrongly issued Postgres certificate.

4. RESOLUTION / WORKAROUND

1. Ensure that the correct build number for LOGFAS **7.x.x** Replication is in fact 7.0.0.**36735**.
2. Make sure that there is a similar record in pg_hba.conf file on Primary and Target servers:

```
# Accept Secure Remote Servers
hostssl     all     all     203.0.113.6/32     md5
```

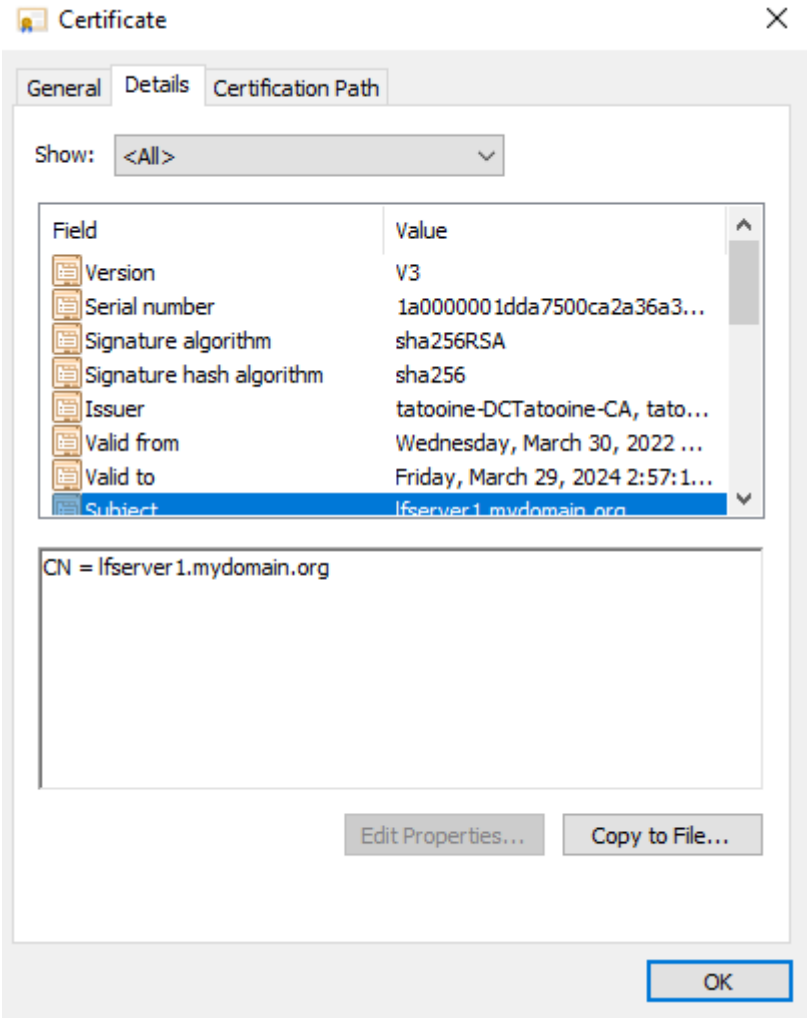
Note: In this example IP address 203.0.113.6 refers to Primary server if this record is inserted on Target server.

3. Verify if postgresql.conf file on Primary and Target servers is configured for accepting ssl option as follows:

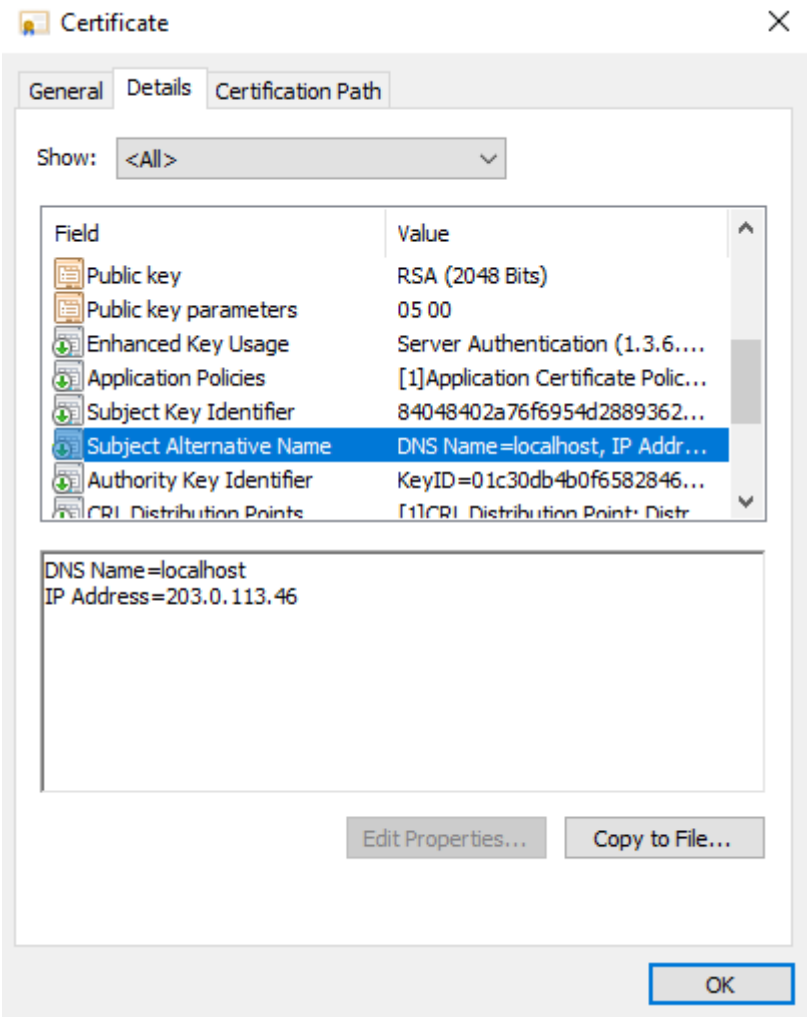
```
ssl = on
ssl_ciphers=
'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-
SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-
SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:DHE-RSA-
AES128-SHA256:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-
SHA256:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK:!EXP:!EDH:!SSLV2:!SSLV
3'
ssl_prefer_server_ciphers = true
password_encryption = md5
```

4. Check if server.crt contains following parameters :

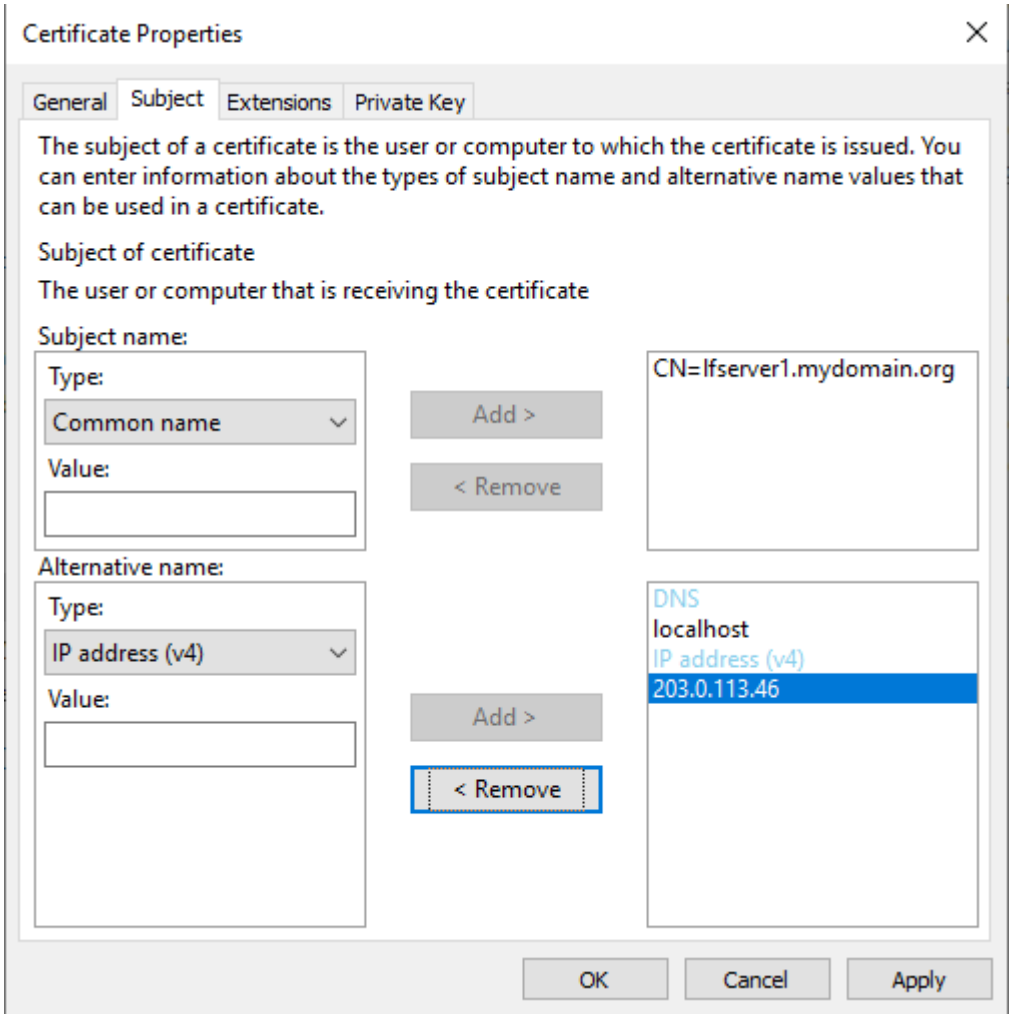
- Version: V3
- Signature algorithm: sha256RSA
- Issuer: Domain Certification Authority
- Valid to: Not expired
- Subject: FQDN



- Public key: RSA 2048 Bits
- Subject Alternative Name: DNS Name=localhost
  IP Address= Target Server IP



Note: If some of the above mentioned parameters are missing recreate the certificate following the LOGFAS Administration Guide, section 2.6.4.2 Get an appropriated PKI certificate from your Certification Authority (CA) . Certificate Properties have to include following parameters while creating CSR.



5. Restart LOGFAS_PostGres service

No further action is required.