

OFICINA DE TECNOLOGÍAS DE INFORMACIÓN DEL CONCYTEC

Software DSPACE-v6.3

Habilitar https

Historial de Versiones

Fecha	Versión	Descripción	Autor
28/09/2021	1.1	Elaboración del Documento	Vilialdo Mancisidor

Revisado y Aprobado por:

Nombre	Rol	Firma
Juan Manuel Rojas	Jefe OTI	
Mirtha Quipas	Coordinador de desarrollo	

Contenido

1. INTRODUCCIÓN	4
2. OBJETIVO	4
3. ALCANCE	4
4. PROCEDIMIENTO	4
4.1. Características técnicas	5
4.2. Pasos para configuración y personalización	5

PROCEDIMIENTO DE CONFIGURACION Y PERSONALIZACION DE REPOSITORIO INSTITUCIONAL

1. INTRODUCCIÓN

DSPACE, que es una aplicación informática de código abierto, utilizado como estándar por CONCYTEC para la implementación de repositorios digitales en las instituciones peruanas, los cuales formaran parte de la red de repositorios del país a través de la Plataforma de código abierto ALICIA.

2. OBJETIVO

Por el presente documento, se comparten los lineamientos necesarios para realizar la configuración y personalización del Dspace.

3. ALCANCE

El procedimiento es de alcance del SINACYT.

4. PROCEDIMIENTO

Antes de iniciar los trabajos de configuración y personalización del repositorio, asegúrese de implementar un servidor con las características mínimas de hardware indicados a continuación, esto con la finalidad de que no se presenten problemas y/o conflictos durante la ejecución de los pasos.

Una vez se cuente con el hardware solicitado, se deberán de ejecutar los pasos en el orden indicado en la presente guía.

4.1. Características técnicas

Características mínimas de hardware

Memoria	3-4 GB.
CPU	Cualquiera, pc o servidor
Almacenamiento	20 GB

Software usado para la elaboración de la guía

SO	Ubuntu 20.04.2 LTS
Base de datos	PostgreSQL 12.7
Java	openjdk version 1.8.0_292
Maven	Apache Maven 3.6.3
Ant	Apache Ant(TM) version 1.10.7

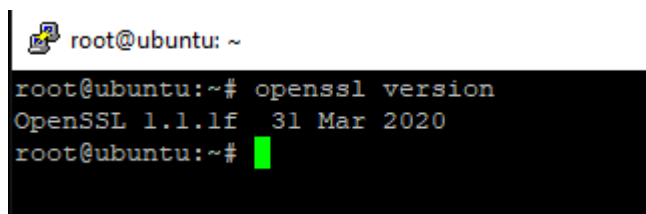
4.2. Pasos para configuración y personalización

Habilitar https

1. Verificar que la librería openssl está instalada. (Por defecto viene pre instalada en Ubuntu)

Comando

openssl versión



```

root@ubuntu: ~
root@ubuntu:~# openssl version
OpenSSL 1.1.1f 31 Mar 2020
root@ubuntu:~#
  
```

2. Crear una carpeta para almacenar todos los archivos de los certificados (Llave privada, csr, crt)

Comando

mkdir /etc/encryption

3. Crear:

- ✓ Una llave privada (private key)
- ✓ Una solicitud de firma de certificado (CSR: Certificate Signing Request)

Comando

sudo openssl req -new -newkey rsa:2048 -nodes -keyout /etc/encryption/server.key -out /etc/encryption/server.csr

Al ejecutar el comando anterior se nos van a realizar las siguientes preguntas:

- ✓ Country Name (2 letter code) [AU]:PE
Abreviación de dos letras para el país

- ✓ State or Province Name (full name) [Some-State]:Lima
Nombre completo del departamento
- ✓ Locality Name (eg, city) []:Lima
Nombre de la ciudad
- ✓ Organization Name (eg, company) [Internet Widgits Pty Ltd]:Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica
Nombre de la entidad
- ✓ Organizational Unit Name (eg, section) []:Oficina de Tecnologías de la Información
Nombre de la unidad organizativa
- ✓ Common Name (e.g. server FQDN or YOUR name) []:dev-dspace.concytec.gob.pe
Nombre del dominio o subdominio de la entidad
- ✓ Email Address []:vmancisidor@concytec.gob.pe
Correo electrónico de contacto

Preguntas adicionales:

- ✓ A challenge password []:
Dejar en blanco y presionar enter
- ✓ An optional company name []:
Dejar en blanco y presionar enter

```

root@ubuntu: ~
root@ubuntu:~# sudo openssl req -new -newkey rsa:2048 -nodes -keyout /etc/encryption/server.key -out /etc/encryption/
server.csr
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/encryption/server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PE
State or Province Name (full name) [Some-State]:Lima
Locality Name (eg, city) []:Lima
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Consejo Nacional de Ciencia, Tecnología e Innovación Tecno
logica
Organizational Unit Name (eg, section) []:Oficina de Tecnologías de la Información
Common Name (e.g. server FQDN or YOUR name) []:concytec.gob.pe
Email Address []:vmancisidor@concytec.gob.pe

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@ubuntu:~#
  
```

4. Verificar la creación de la llave privada y de la solicitud de firma de certificado (CSR)

/etc/encryption/	
Nombre	Tamaño
 server.csr	2 KB
 server.key	2 KB

Comando

nano /etc/encryption/server.csr

```

root@ubuntu: ~
GNU nano 4.8 /etc/encryption/server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDNTCCAhoCAQAwge8xCzAJBgNVBAYTA1BFMQ0wCwYDVQQIDARMaWlhMQ0wCwYD
VQOHDARMaWlhMUKwRwYDVQQKDEBDb25zZWpveIE5hY2l2bmFsIGR1IENpZW5jaWES
IFRlY25vbG9naWEgZSBjb250dFjaW9uIFRlY25vbG9naWNhMTEwLWYDVQQLDChP
ZmljaW5hIGR1IFRlY25vbG9naWFzIGR1IGxhIEluZm9ybWJjaW9uMRgwFgYDVQQD
DA9jb25jeXRlYy5nb2IucGUxKjAoBgkqhkiG9w0BCQEWG3ZtYW5jaXNpZG9yQGNv
bmN5dGVjLmdvYi5wZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKtD
Ti8mW14P5pZDOO0LbQwcj4Eb4ic+p0ieKdc3pZmolBAsKou+lO5IqbJgqbHDW343
+Payt3bB3mFWnsggaB04DYjhNcQVZ3iAuTgJChzuz/F+PKRRray6WaTP1TVqX29Z
DtNyfbY1wLXU+VFUNIC9MEUGCs9BY9Xpoz0039bRLKXivUL9+0RbBP/dMEliIrIc
6Z12mbrdmLF8bebr6+BCUU+Vlr8fl/15J+O65JyvfohLpuKyMlr0Nj7q+5z2UBc4
qnK7ytUtLLGYukch4J7juPDxnwG89V0QKh3JiNH7EsH5rw6P5Q9/pI+OFBd4HRqh
RwQqg/ZZxPZn8Ga+0hcCAwEAAaAAMA0GCSqGSIb3DQEBGwUAA4IBAQA45sImIb7z
br/P36G10SIiuAHXnA0vs6f4rSMax6jNC8aTPp/OSCG3ZqakcohVkJi8SQVOX
fWHPj3WHXplfQpCqj2J0Cv9yxAhmDP0W1f42TMuj2v4Pz7DGEYmdXGJjxRHFpauA
DiXsrMavuLhc0EIMiScFbCn+wWC9jBIZDJY3dWyhA/+0CzVtVzGNFRRN3+/oTn0
WPvDnmeyHm7/vofW7OmZ0g56eZnlwXlNQ5DRF1OuRjKGAwU5IHygv+2UpNzkZwCy
9AjChI+nYaJQLnAH44L8YlyT4DMXOWGHTwduXlpAQClkm7ffuo034FuBnWX2s+Qe
jzuBV22QdR2A
-----END CERTIFICATE REQUEST-----

```

Comando

nano /etc/encryption/server.key

```

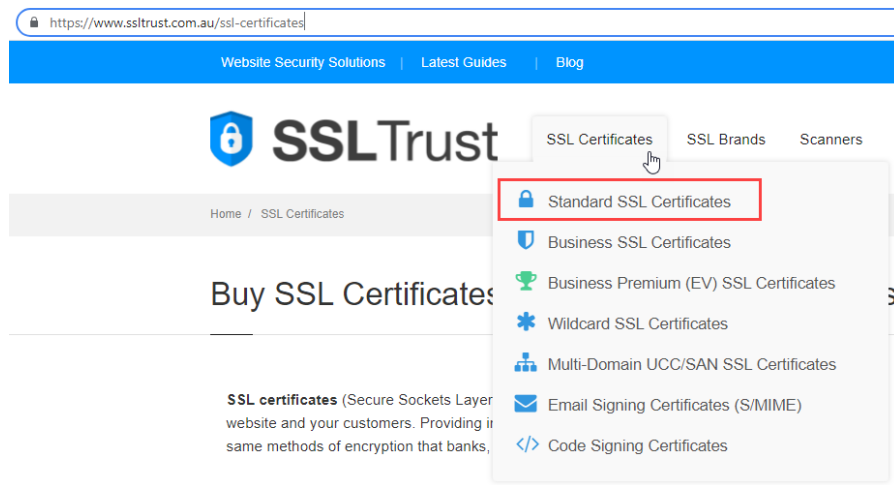
root@ubuntu: ~
GNU nano 4.8 /etc/encryption/server.key
-----BEGIN PRIVATE KEY-----
MIIEFwIBADANBgkqhkiG9w0BAQEFAASCBAkkgwGSlAgEAAoIBAQCq004vJlpeD+aW
QzjtC20MHI+BG+InPqdIninXN6WZqNQQLCqLvpTuSKmyYKmxwlt+N/j2srd2wd5n
lp7IKmgd0A2I4TXEFWd4gLk4CQoc7s/xfjykUa2sulmkz5Ula19vWQ7Tcn22JcMC
1lPlX1DSaVtBFBgrPQWPV6aM6Dt/W0S5F4r1C/ftEWwT/3TBNYqyHOMZdpm63Zix
fG3m6+vgQlFP12a/H5f5eSfjuuScr36IS6bisjJa9DY+6vuc91AXOKpyu8rVLS5R
mLpHieCe47jw8Z8BvPVdECodyYjR+XLB+a80j+UPf6SPjhQXEB0a0UcEKYP2WcRW
YfBmvtIXAgMBAECCggEAcuy6Yif9sxxrQekwYilASledjQfs2thpuAXn+BdMiBlC
VKRjWITEQ4Wq0i0vwj76rkekuug0Lav1OtX8IfWHA06u2AfmJBcyzAhQarhZ5Szh
SVNyH4BtWebG8KzdrAZIYUpWypeWmttAW1lgOmFrw26o/cFwAGxA9DjKu6KSlnf
sGuv/SzaQIRDY1lwHRCvpXDKmGCwINByVUOW8AY/Ls8XpA76kbQu6dtkoGaD03cC
z3JOX1L0uKk6hsEaW3UorxYmfj3uzDeTkurDYl+5ptq9u4XgUChBhhSx0sU9zewk
ziFm6Y8z7EwFwPal/LaHk75QE3ydlapVe5B1jBgd8QKBgQDeN+E3IAmGNOcDJMQI
AetQ8JVIzmpCC23h7n2kpPLVa6cbYcQTEgBfDPnm+JtlZSIqTrVRw5eVQwvWw1lo
yFoZNCf92F0Ho7N2HjDXuumsUWHPWgwzootoIzWlruftkxpmWB4iRYBCFvjzPo7
wsl67/muhBbM1IlelNP0ypwHwKBgQDFTGI/6SGSPepI1NJOen9S2XGjJGaxXsZ2
/hRReExde0zFzJwsqGgwYkKFYjSpsBiXFjycV77sYzOQ6uo2X7fdOhsd5B6/B1BW
dLFAF9gFsGhCemT2mPo7U9nn/Tlk3dIHmKWywewC1Rx3yLjA7u2DjJXRG7Zs2M2Q
NnXCDwA/CQKBgQCMr037S2IcQFPczqL4+tYS2S15t7Uf+QJpHkcXPIKskUorsY8a
qzPm+V0hWfV7fjqfFCA41aOXfM21XUuBnPcLv/hH2DOXFPiWm/LtH7//88oMJJf
CU2700BHMx7/3zcDR+ImjYuLvdIHJ5dozEywv0sQrHmOli2mW1GSUc+OOWKBgQCN
b417LV/wmOwJTg5ZTflaECMXpa+sdTmm8cuU/70Wwp4tqdSeWneeP8JaJiWEg4WN
QdaFaVon2BGOUKkn44RGJjJsQi08WYVcBP1P7gfhRC3pgh4r0zuHLjwmz2PGiDHZ
WjdmrNPwof4vbIfXxqLVEvOAtn+O4Qm2nOeccb3KQKBgQC6ke/xH4Se9L1hqnGt
2lmQt+6IDv6iYWBzBuAslbSvf7ro1UQZ0Wdh2BZWiiM25aIWksU93AxytWDmLYga
AQG81LWhecl4PtV8+w2w2+9/1PbSoLCmZ2tQKHxQjHe2EBbMdVJGUY6+RRZAJB+a9
gWSYrZMiJHHT1sOi815tOrezsA==
-----END PRIVATE KEY-----

```

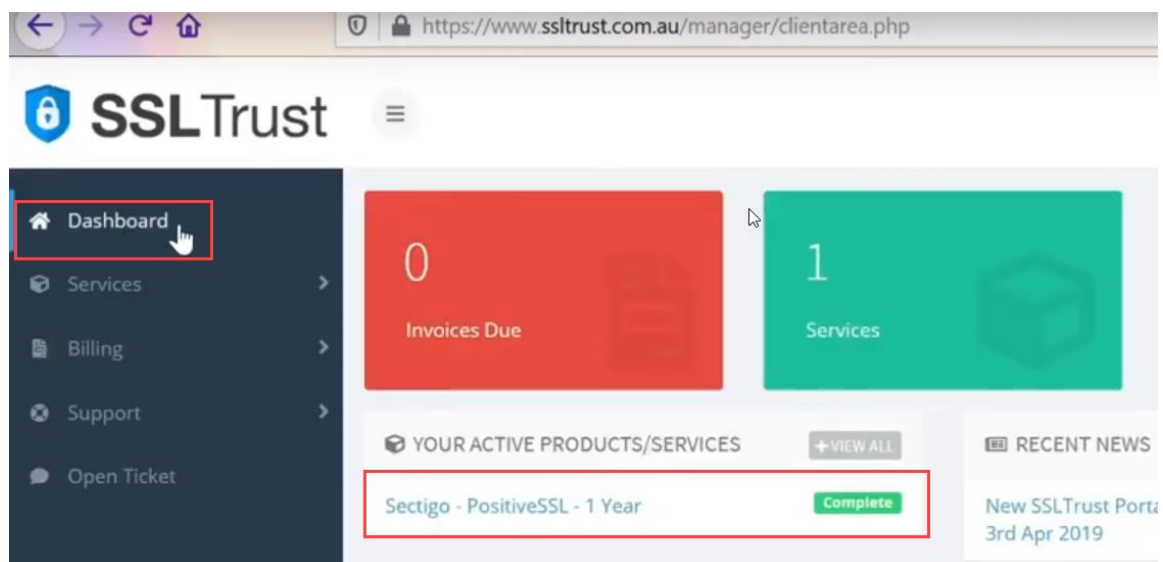
5. Comprar un certificado SSL. Por ejemplo, puede revisar la página del siguiente proveedor de Certificados:

<https://www.ssltrust.com.au/ssl-certificates>

Existen varios tipos de certificados, para este ejemplo vamos a usar el Certificado Estándar



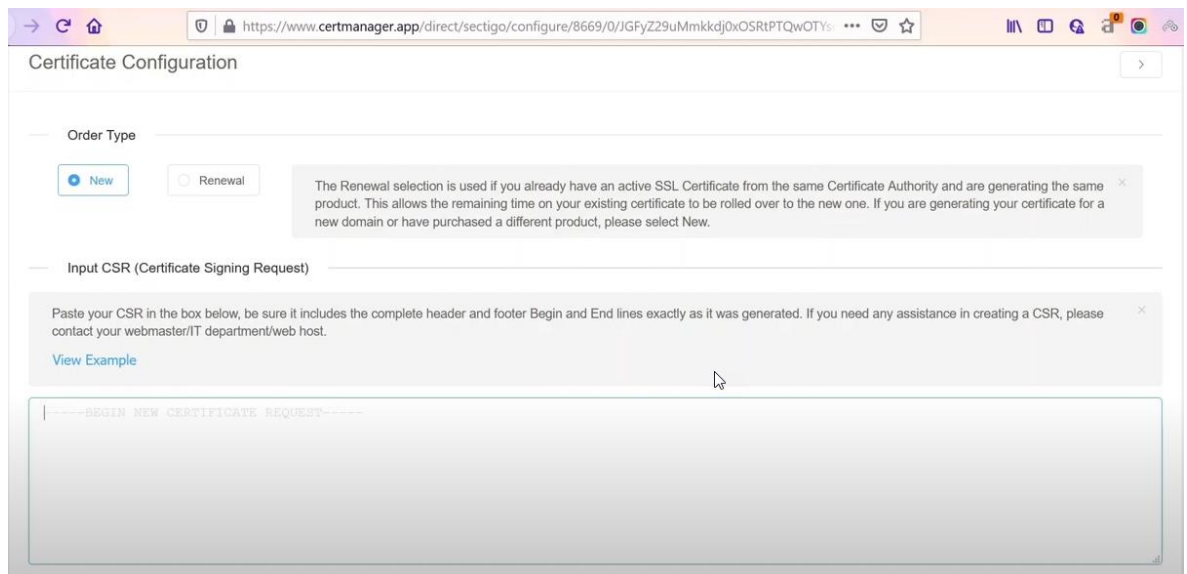
Una vez haya realizado el pago del certificado, el proveedor que eligió le habilitará un acceso a su página web para que realice la configuración del certificado.



- En el panel de control que su proveedor de certificados le habilitó, tendrá que realizar las siguientes actividades para que su certificado este habilitado.

✓ **Registrar la configuración del certificado.**

Esto se realiza registrando el contenido del archivo **server.csr** creado en el punto 3.



→ ↻ 🏠 <https://www.certmanager.app/direct/sectigo/configure/8669/0/JGFyZ29uMmkkdj0xOSRtPTQwOTYs> ... 📄 ⚙️ 🔍

Certificate Configuration

Order Type

☒ New ☐ Renewal

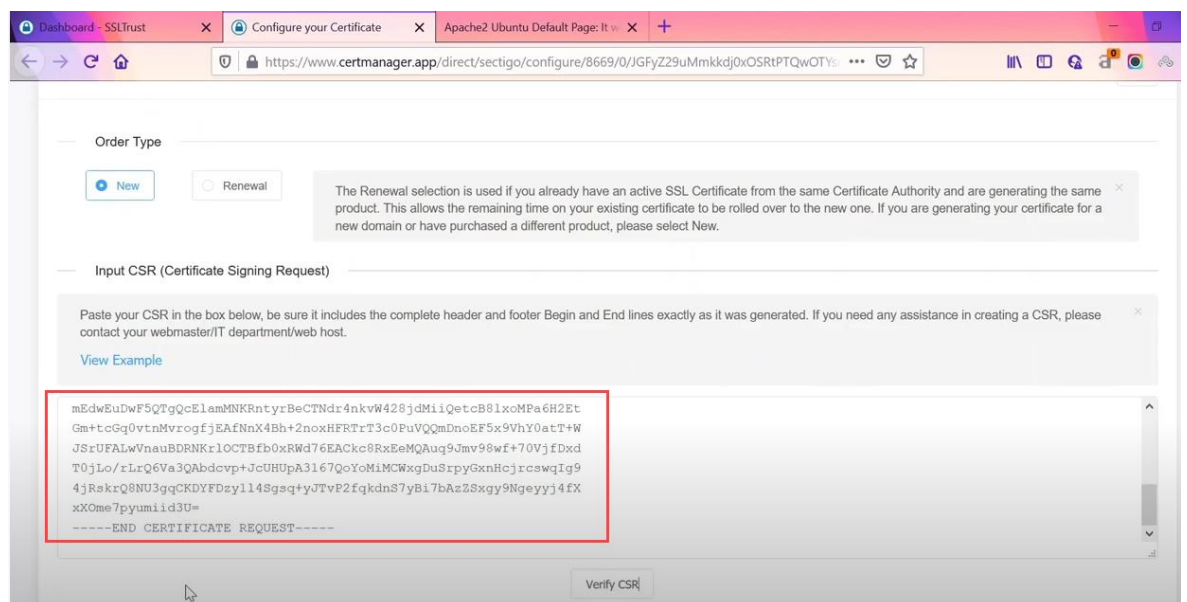
The Renewal selection is used if you already have an active SSL Certificate from the same Certificate Authority and are generating the same product. This allows the remaining time on your existing certificate to be rolled over to the new one. If you are generating your certificate for a new domain or have purchased a different product, please select New.

Input CSR (Certificate Signing Request)

Paste your CSR in the box below, be sure it includes the complete header and footer Begin and End lines exactly as it was generated. If you need any assistance in creating a CSR, please contact your webmaster/IT department/web host.

[View Example](#)

```
-----BEGIN NEW CERTIFICATE REQUEST-----
```



Dashboard - SSLTrust | Configure your Certificate | Apache2 Ubuntu Default Page: It v... | +

→ ↻ 🏠 <https://www.certmanager.app/direct/sectigo/configure/8669/0/JGFyZ29uMmkkdj0xOSRtPTQwOTYs> ... 📄 ⚙️ 🔍

Certificate Configuration

Order Type

☒ New ☐ Renewal

The Renewal selection is used if you already have an active SSL Certificate from the same Certificate Authority and are generating the same product. This allows the remaining time on your existing certificate to be rolled over to the new one. If you are generating your certificate for a new domain or have purchased a different product, please select New.

Input CSR (Certificate Signing Request)

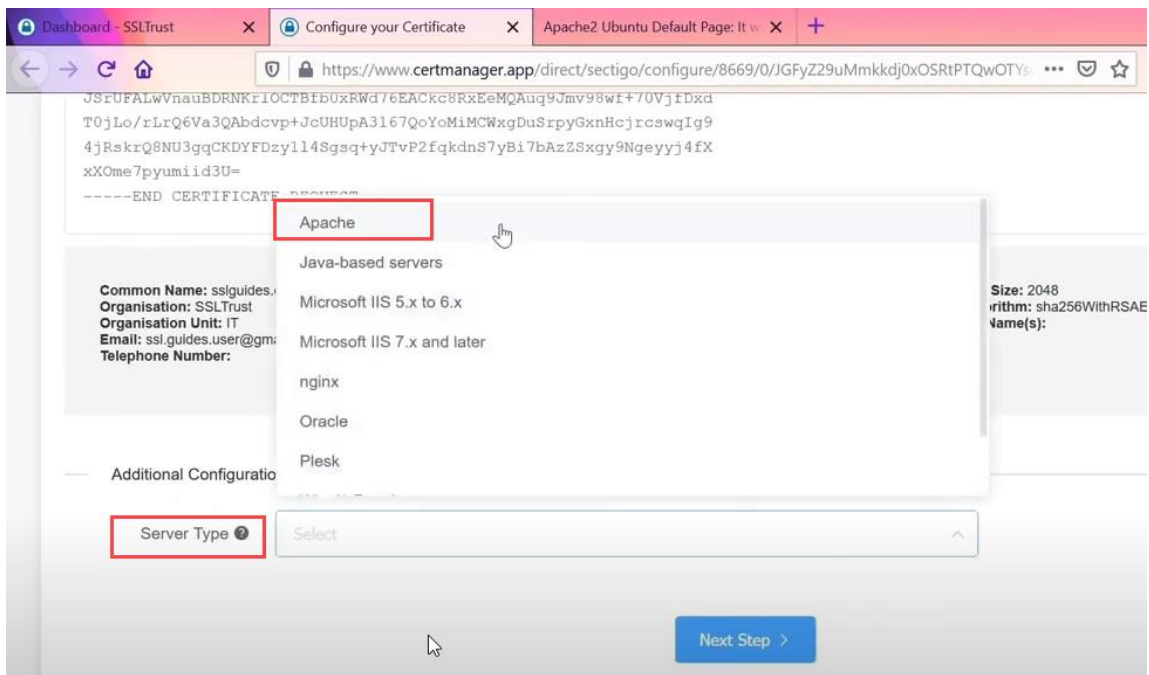
Paste your CSR in the box below, be sure it includes the complete header and footer Begin and End lines exactly as it was generated. If you need any assistance in creating a CSR, please contact your webmaster/IT department/web host.

[View Example](#)

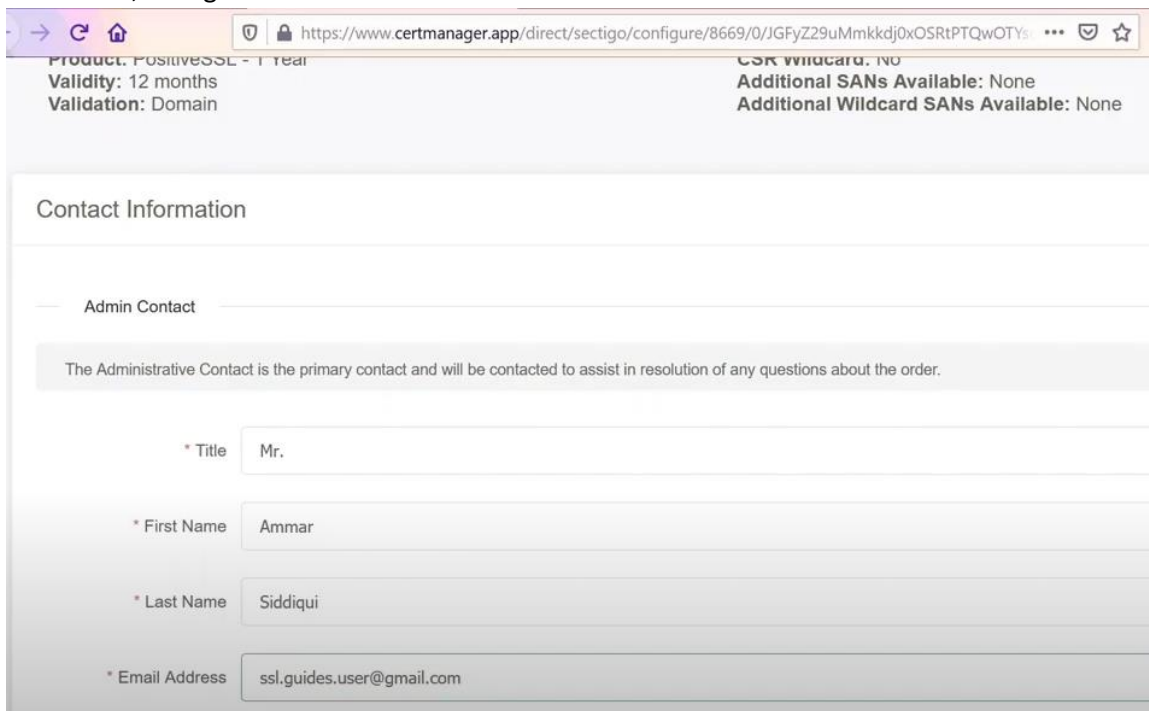
```
mEdwEuDwF5QTgQcElamMnKRntyrBeCTNdr4nkVW428jdMiiQetC881xoMPa6H2Et
Gm+tcGq0vtnMvroGfjEafNnX4Bh+2noxHfRTTrT3c0PuVQmDnoEF5x9VhY0atT+W
JSrUFALwVnauBDRNKR1OCTBfb0xRWd76EACkC8RxEeMQAug9Jmv98wf+70VjFDxd
T0jLo/rLrQ6Va3QAbdcvp+JcUHUpA3167QoYoMiMCWxgDuSryGxnHcjrCawqIg9
4jRskrQ8NU3gqCKDYFDzy1148gsq+yJTvP2fqkdnS7yBi7bAzZSxgy9Ngeyyj4fX
xXOme7pyumiid3U=
-----END CERTIFICATE REQUEST-----
```

Verify CSR

Se selecciona el tipo de servidor en donde será usado el certificado, en este caso será Apache.

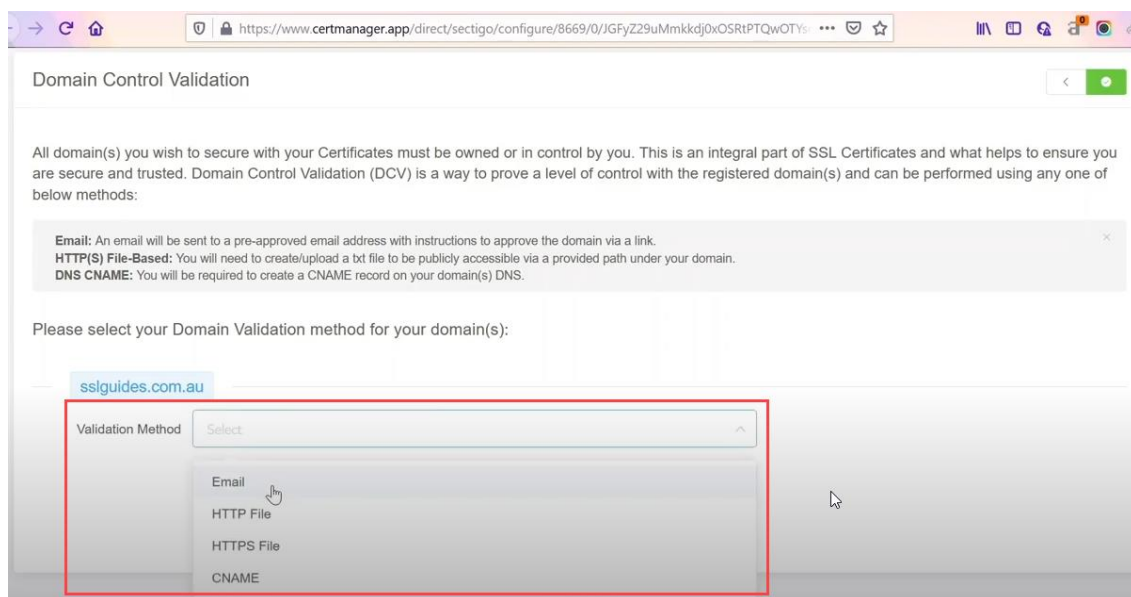


Por último, se registran los datos del administrador del certificado.



- ✓ **Validar que usted es el dueño o administrador del dominio que se quiere asociar al certificado**

Existen 4 métodos para realizar la validación, el más sencillo es Email



Domain Control Validation

All domain(s) you wish to secure with your Certificates must be owned or in control by you. This is an integral part of SSL Certificates and what helps to ensure you are secure and trusted. Domain Control Validation (DCV) is a way to prove a level of control with the registered domain(s) and can be performed using any one of below methods:

Email: An email will be sent to a pre-approved email address with instructions to approve the domain via a link.
HTTP(S) File-Based: You will need to create/upload a txt file to be publicly accessible via a provided path under your domain.
DNS CNAME: You will be required to create a CNAME record on your domain(s) DNS.

Please select your Domain Validation method for your domain(s):

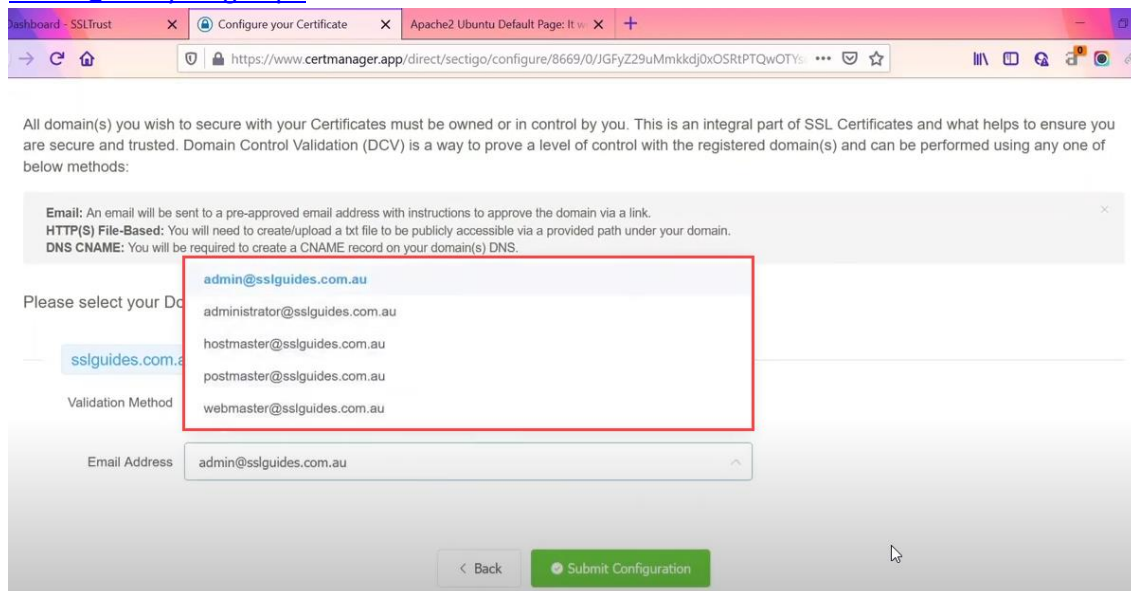
sslguides.com.au

Validation Method: Select

- Email
- HTTP File
- HTTPS File
- CNAME

Se debe seleccionar del listado el correo del administrador de su dominio. Por ejemplo:

admin@concytec.gob.pe



All domain(s) you wish to secure with your Certificates must be owned or in control by you. This is an integral part of SSL Certificates and what helps to ensure you are secure and trusted. Domain Control Validation (DCV) is a way to prove a level of control with the registered domain(s) and can be performed using any one of below methods:

Email: An email will be sent to a pre-approved email address with instructions to approve the domain via a link.
HTTP(S) File-Based: You will need to create/upload a txt file to be publicly accessible via a provided path under your domain.
DNS CNAME: You will be required to create a CNAME record on your domain(s) DNS.

Please select your Domain Validation method for your domain(s):

sslguides.com.au

Validation Method: Select

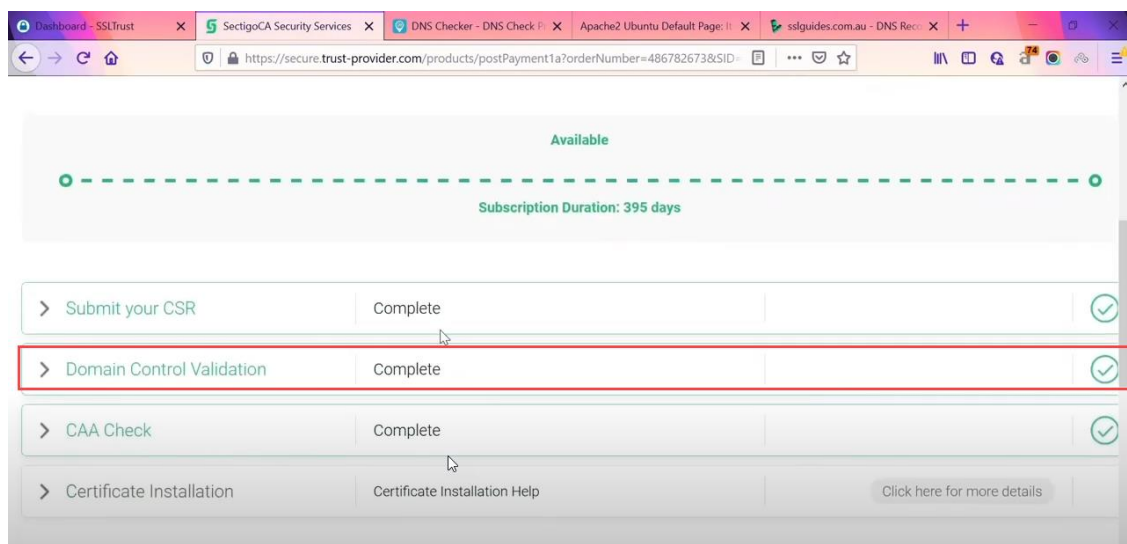
- admin@sslguides.com.au
- administrator@sslguides.com.au
- hostmaster@sslguides.com.au
- postmaster@sslguides.com.au
- webmaster@sslguides.com.au

Email Address: admin@sslguides.com.au

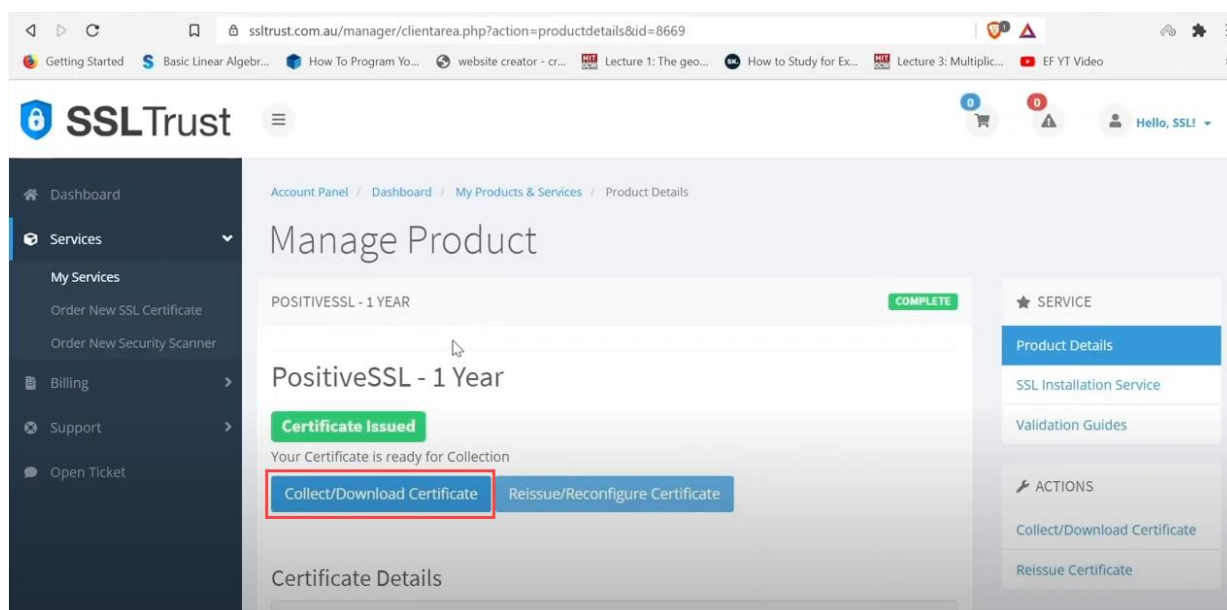
< Back Submit Configuration

Después de confirmar que usará el método de validación por email, la cuenta de correo de su administrador de dominio recibirá un enlace enviado por la Autoridad emisora de certificados. Mediante este enlace usted podrá probar que es el dueño o administrador del dominio para el cual se le desea generar un certificado.

Una vez realizada la validación de la propiedad del dominio, esta no se reflejará inmediatamente como concluida en el panel de administración del certificado, pudiendo tomar unos minutos en actualizarse el estado.



7. Una vez el certificado este habilitado debido a las 2 actividades realizadas en el paso anterior, se procederá a descargar los certificados desde el panel de control.



```
GNU nano 2.9.3 /etc/encryption/certificate.crt
-----BEGIN CERTIFICATE-----
MIIGPzCCBSegAwIBAgIQ7FxFx4ivNucOzfSEn/rzBgjANBgkqhkiG9w0BAQsFADCB
jZELMAkGA1UEBhMCRCR0IXgZA2BgNVBAGTEkdYXZlIHRyZWVudmVydVYENB
A1UEBMXMHU2FsZm9yZDEVMYGA1UEChMPU2VjdGlnbWJmaW1pdGVKMTCwNQYDQDQD
EySTZWN0awdvIFJfTQS8EB21haw4gvMFsawRhDG1vb1BTZN1clcmUgu2VydmVYIENB
MB4XD0t1XMdXUwNTAwMDAwMFOxdTIYMdyXNDIZntK10vowGZEZMBcGA1UEAxMQC3Ns
Z3VpZGVzLmNvbS5hdHkTCCASIDYQJKoZIhvcNAQEBBQggEPADCCAQcggEBAmtL
q9lwbDjq6qOf6Lt4F8Lmk9GaJlrvxC5eFls+uDiy+FACHgwcn/Khf01QEek/i6hdJC
8p40AL7MvaqwckCJApeAvF5vmuf4Z25BVBarjkhiARmeOQ3qv0GHGLSrge4CoXlpz
SyZIR7jjccLoonqrINF+EvdqXC9RW7mBJPhpvewlw1jacAZXlgsABYFv7ar5ZwvhA
zIz6kJPzxUNjinIU/Lb2AtH3S38j/ejuNYg7qq5WB4mlvb/C0JaJ8ECGq2+T2QEE4
IvwaxRIEPPQQKUDDD9FFeGkbzbDzonWm9144monN2zvG2va2XPnb2vlqZ2wl/jtswr
Ebvgg8/r07UgfGafSIKMcAWeAAAOCAwgwgMEMB8GA1udIwQYMBAAFI2MXSRURYrh
d+mb+zsF4bgBJWHMMBOGA1udDgQWBBQznFoBQTXXje/1xNqChemegRG9N9DAOBgnV
HQ8BAF8EBAMCBAAwDAYDVROTAQH/BAIwADAAdBgNVHSUEFjAUBgggrBgEFBQCDAQYI
KWYBBQUHAWIwsQYDVR0gBEIiwQDA0BggsrBgEEAbIxAQICBzAlMCMGCCSGAQUFBwIB
FHgdHRRwczoVL3NlY3RpZ28uY29tL0NQZUAIBGZngQwBAGEWgyQGCGCSGAQUFBwEB
BHwdjPBGRgcBgEFBQCwIAZDdhRHOCDOvL2Nydc5ZZWN0awdvLmNvbS59TZWN0awdv
U1NBGR9tYWluVmFsaWRhDG1vb1NlY3VyZVN1cnZlcKNBLmNydDAJBgggrBgEFBQCw
AYYYXAHR0cDovL29jc3Auc2VjdGlnby5jb2wmcQYDVRORBCOWKIiQc3NsZ3VpZGVz
LmNvbS5hdYU2Id3dlNNzbGdLawRLcy5jb20uYXUwggGF+BgorBgEEAdZ5AACQBIIb
bgSCAwBoBAAB2AEAlvet1+pEGMLWIwn0830RLF0vv1JuIwr8yxw/m1HAABew7t
m5oAAAQAACecwRQtAI6Qvz+wC3LyeCwcTj2j93sz56+Bg5ANKimgIMEI/uHNAiAp
Xmr148L3SQLLYvoq/crBI04zeCe5z6rx9CyFDVw0XAB2AEHIyrHfIkZKEMahog1c
hl15OMysba+vrS8do8Jbltg5F2AAABew7tm50AAAQAACecwRQIRMZCFJZub/nCRX3
MIODDKiyYZTKwgmKOutoBFSDORDUCIQmx4JMhzOvDnepbAhad4jkdPlPh6ZsgsvDI
TZRTHO+KcwB2AC15vvceOTkh8FZZn2Ol+d+W+V32CYAr4+Uldjlw1XceEAABew7t
M3sAAQAACecwRigabzg56MOX/yEqhmAf6fg1DeLbw4kfr6Z7quVBf92UkwCIQC
vsYAF70+I5Zs3NQSG6P6tyvyrWN3943ITztFrupXb6DZANBgkqhkiG9w0BAQsFAAOC
AEQAWPCGS1zX6SkIEyky11VRXLj+K8edyMxBUMYjc3E+jlr09ZF03WNoLOu6fJ0YG
OYJU9Z8guy7zP2jdzdtOS63awoot9E8xw+155eyLmOX32ywy8jpZbmP42igs0iWVg
3IucdGLFx6zuIdrlFvLiIRluFfgksA8BoP3c3RoBji8W6HEbwfsL16ME4a80/FZ3
1t26n7TiwhljLIdukCsHiRbeFLKV6oy+v+XTXuLwxhu7tGMzmY79WjveXynbFcH
MkMmm+UbwpvjSHHjgLSvwt9JouT8U5/o9fBuHhq1IuFdPLWg8AzEnyJ+tp7OEQV7X
tDnvAnV7izrlkas99knJfBn5Mg==
-----END CERTIFICATE-----
```


[Copiar y pegar las directivas]

```

GNU nano 2.9.3 /etc/apache2/conf-available/ssl-params.conf
SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder On
# Disable preloading HSTS for now. You can use the commented out header line that includes
# the "preload" directive if you understand the implications.
# Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff
# Requires Apache >= 2.4
SSLCompression off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"
# Requires Apache >= 2.4.11
SSLSessionTickets off

```

10. Habilitar SSL en Apache2

Comando

a2enmod ssl

```

root@ubuntu: ~
root@ubuntu:~# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@ubuntu:~# systemctl restart apache2
root@ubuntu:~#

```

11. Habilitar los headers y los parámetros para el SSL en Apache2

Comando

a2enmod headers

a2enconf ssl-params

```

root@ubuntu: ~
root@ubuntu:~# a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@ubuntu:~# a2enconf ssl-params
Enabling conf ssl-params.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@ubuntu:~#

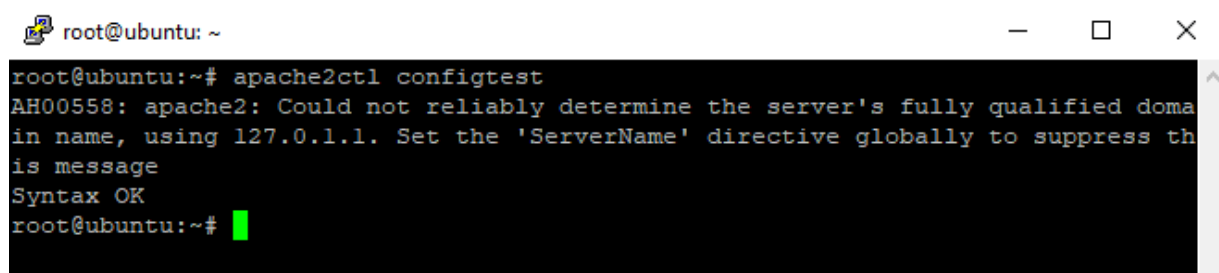
```

12. Probar la configuración del Apache2

Comando

apache2ctl configtest

Si se muestra el mensaje "Syntax OK", la configuración es correcta. Omitir el mensaje de error sobre ServerName Global Directive.



```

root@ubuntu: ~
root@ubuntu:~# apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
root@ubuntu:~#
  
```

13. Editar el archivo:

/etc/apache2/sites-available/[nombre del subdominio]

Por ejemplo:

/etc/apache2/sites-available/dev-dspace.concytec.gob.pe.conf

Nota: Revisar el manual técnico "009 Cambiar el puerto 8080 al 80" en el cual se describen los pasos para asociar un subdominio al Dspace usando Apache2.

Realizar los siguientes cambios:

- ✓ Crear otro VirtualHost para el puerto 443, para esto copiar y pegar el VirtualHost del puerto 80.
- ✓ En el VirtualHost del puerto 443, agregar las líneas:

```

SSLEngine on
SSLCertificateFile [Ruta del certificado]
SSLCertificateKeyFile [Ruta de la llave privada]
SSLCertificateChainFile [Rtua del certificado intermedio]
  
```

Ejemplo:

```

SSLEngine on
SSLCertificateFile /etc/encryption/certificate.crt
SSLCertificateKeyFile /etc/encryption/server.key
SSLCertificateChainFile /etc/encryption/intermediate.crt
  
```

- ✓ Modificar el log para que se genere un log independiente para el puerto 443

Ejemplo:

```
ErrorLog ${APACHE_LOG_DIR}/dev-dspace-ssl.error.log
```

CustomLog \${APACHE_LOG_DIR}/dev-dspace-ssl.access.log combined

- ✓ En el VirtualHost del puerto 80, comentar las líneas:

```
#ProxyPass / ajp://localhost:8009/
#ProxyPassReverse / ajp://localhost:8009/
```

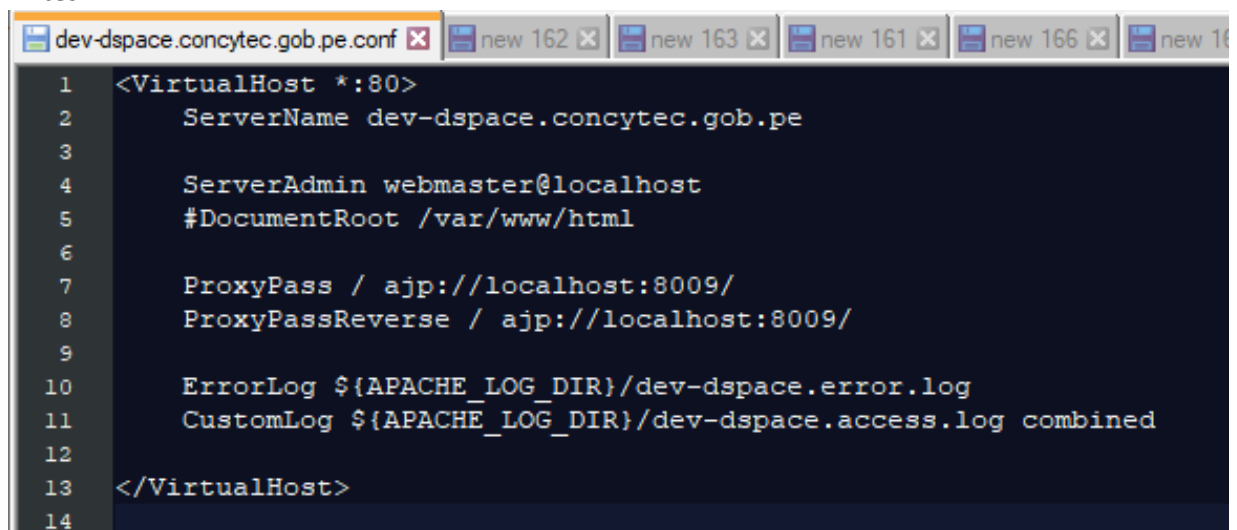
Y agregar la línea:

Redirect permanent / [https://\[tu-dominio\]/](https://[tu-dominio]/)

Ejemplo:

Redirect permanent / https://dev-dspace.concytec.gob.pe/

Antes



```

1  <VirtualHost *:80>
2      ServerName dev-dspace.concytec.gob.pe
3
4      ServerAdmin webmaster@localhost
5      #DocumentRoot /var/www/html
6
7      ProxyPass / ajp://localhost:8009/
8      ProxyPassReverse / ajp://localhost:8009/
9
10     ErrorLog ${APACHE_LOG_DIR}/dev-dspace.error.log
11     CustomLog ${APACHE_LOG_DIR}/dev-dspace.access.log combined
12
13 </VirtualHost>
14

```

Después

```

dev-dspace.concytec.gob.pe.conf x new 151 x new 153 x new 152 x new 154 x new 155 x new 156 x new 1
1 <VirtualHost *:80>
2     ServerName dev-dspace.concytec.gob.pe
3
4     ServerAdmin webmaster@localhost
5     #DocumentRoot /var/www/html
6
7     #ProxyPass / ajp://localhost:8009/
8     #ProxyPassReverse / ajp://localhost:8009/
9     Redirect permanent / https://dev-dspace.concytec.gob.pe/
10
11     ErrorLog ${APACHE_LOG_DIR}/dev-dspace.error.log
12     CustomLog ${APACHE_LOG_DIR}/dev-dspace.access.log combined
13
14 </VirtualHost>
15
16 <VirtualHost *:443>
17     ServerName dev-dspace.concytec.gob.pe
18
19     ServerAdmin webmaster@localhost
20     #DocumentRoot /var/www/html
21
22     ProxyPass / ajp://localhost:8009/
23     ProxyPassReverse / ajp://localhost:8009/
24
25     SSLEngine on
26     SSLCertificateFile /etc/encryption/certificate.crt
27     SSLCertificateKeyFile /etc/encryption/server.key
28     SSLCertificateChainFile /etc/encryption/intermediate.crt
29
30     ErrorLog ${APACHE_LOG_DIR}/dev-dspace-ssl.error.log
31     CustomLog ${APACHE_LOG_DIR}/dev-dspace-ssl.access.log combined
32
33 </VirtualHost>
  
```

Así debe quedar

```

<VirtualHost *:80>
    ServerName dev-dspace.concytec.gob.pe

    ServerAdmin webmaster@localhost
    #DocumentRoot /var/www/html

    #ProxyPass / ajp://localhost:8009/
    #ProxyPassReverse / ajp://localhost:8009/
    Redirect permanent / https://dev-dspace.concytec.gob.pe/

    ErrorLog ${APACHE_LOG_DIR}/dev-dspace.error.log
    CustomLog ${APACHE_LOG_DIR}/dev-dspace.access.log combined

</VirtualHost>

<VirtualHost *:443>
  
```

ServerName dev-dspace.concytec.gob.pe

ServerAdmin webmaster@localhost

#DocumentRoot /var/www/html

ProxyPass / ajp://localhost:8009/

ProxyPassReverse / ajp://localhost:8009/

SSLEngine on

SSLCertificateFile /etc/encryption/certificate.crt

SSLCertificateKeyFile /etc/encryption/server.key

SSLCertificateChainFile /etc/encryption/intermediate.crt

ErrorLog \${APACHE_LOG_DIR}/dev-dspace-ssl.error.log

CustomLog \${APACHE_LOG_DIR}/dev-dspace-ssl.access.log combined

</VirtualHost>

14. Reiniciar Apache2

```
systemctl restart apache2
```

15. Si el Apache2 no inicia, realizar lo siguiente:

- ✓ Revisar el log:

Comando

```
tail /var/log/apache2/error.log
```

- ✓ Si se muestra un mensaje genérico como:

AH00016: Configuration Failed

Instalar y ejecutar el siguiente comando para obtener el detalle de inicialización del Apache2

Comandos

```
sudo apt-get update
```

```
sudo apt-get install strace
```

```
sudo strace -f apache2ctl start
```

16. Verificar el estado de la configuración del servicio SSL.

Ir a la página:

<https://www.ssllabs.com/ssltest/>

← → ↻ ssllabs.com/sslttest/ 

 **Qualys. SSL Labs** Home Projects Qualys Free Trial Contact

You are here: [Home](#) > [Projects](#) > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname:

☐ Do not show the results on the boards

17. Referencias

<https://www.youtube.com/watch?v=zgUshTJa4sc>

<https://www.ssltrust.com.au/help/setup-guides/apache-ubuntu-ssl-install-guide>