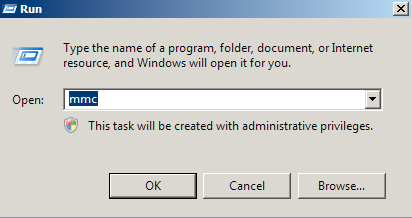
Guideline - Activate HTTPS (Draft)

TODO: organizar as informações usando como fonte os endereços abaixo:

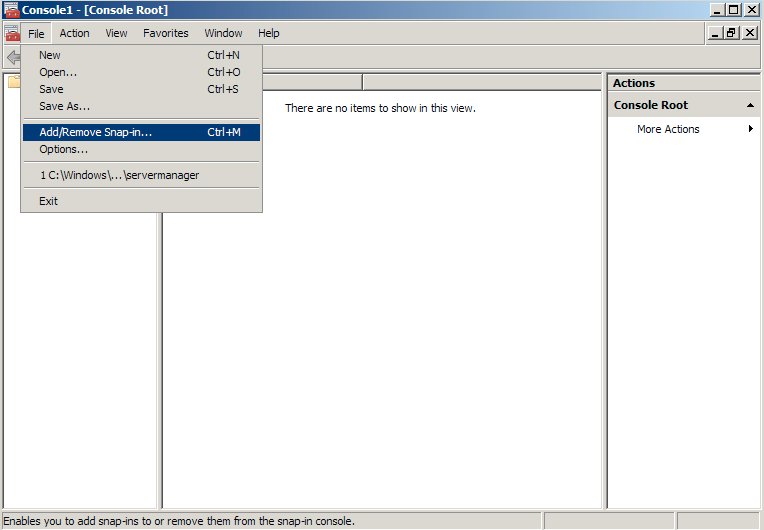
**Como exportar um certificado para utilizar no Apache.**

O primeiro passo é exportar o certificado para .pfx .

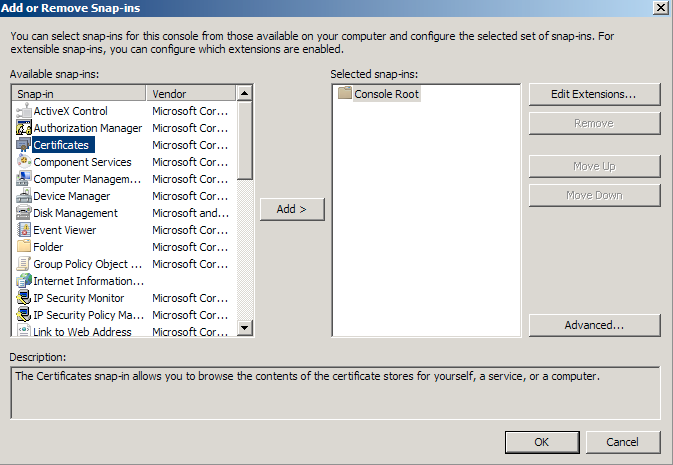
No Windows, digite :



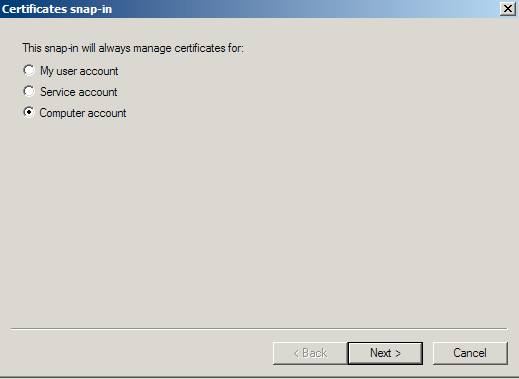
Em seguida Add/Remove Snap-in :

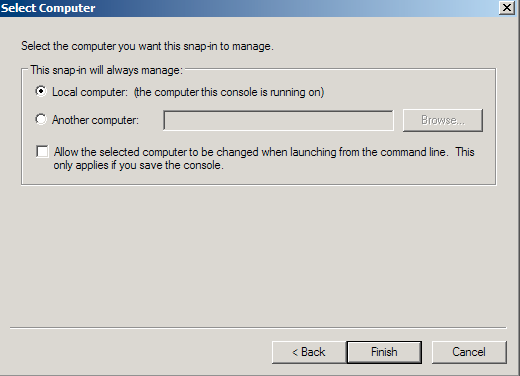


Clique duas vezes no certificado.

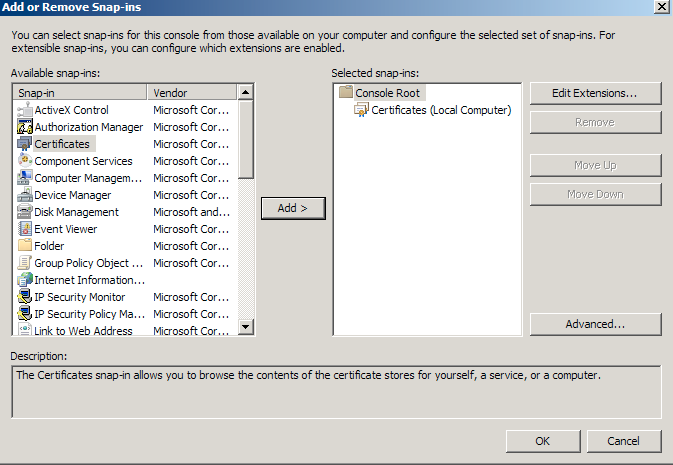


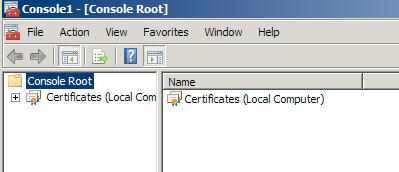
Siga os passos abaixo.

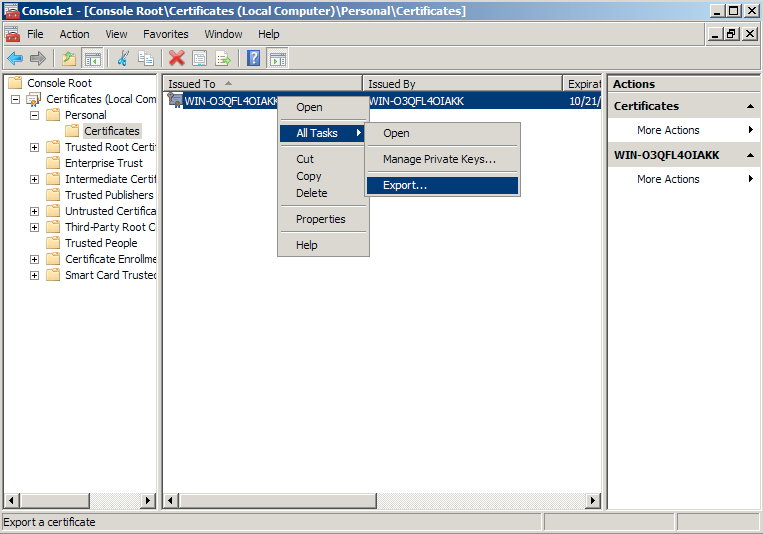




Clique em ok após finalizar.

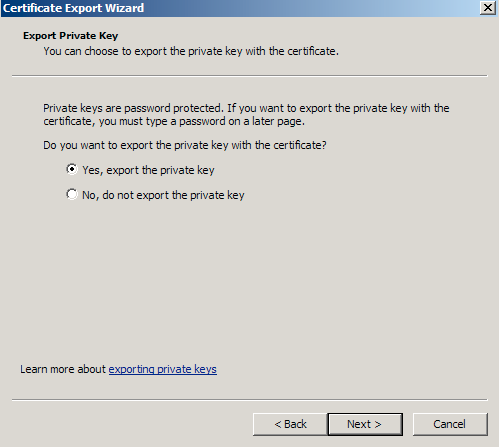




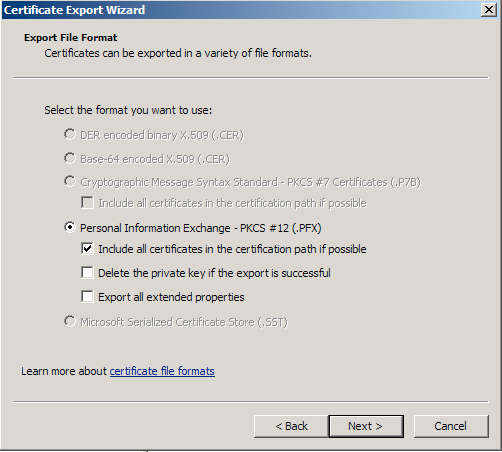




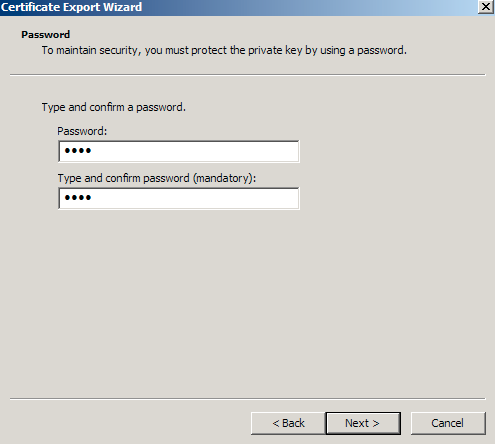
Exporte também a chave privada.



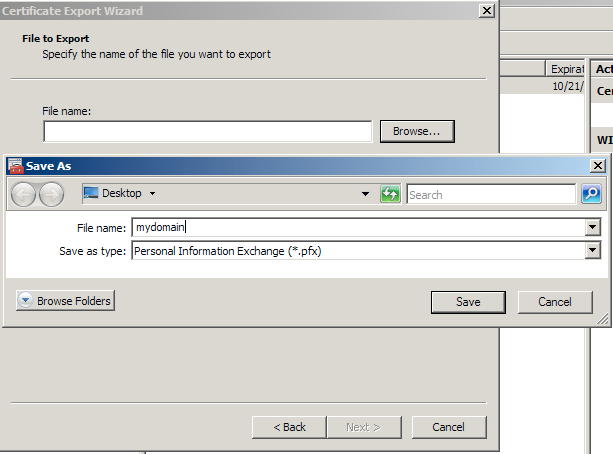
Inclua todos os certificados.

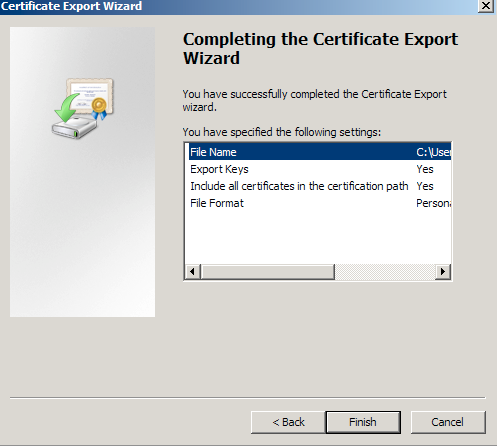


Insira uma senha.



Salve o arquivo .**pfx**

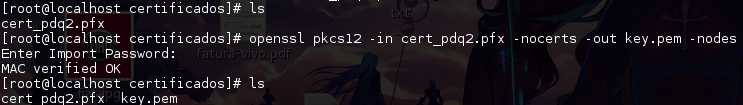




Agora que temos o .pfx, precisamos extrair as informações do certificado.

Extraindo a have privada :

|  |
| --- |
| openssl pkcs12 -**in** cert\_pdq2.pfx -nocerts -out key.pem -nodes |



Removendo a senha da chave privada :

|  |
| --- |
| openssl rsa -**in** key.pem -out server.key |

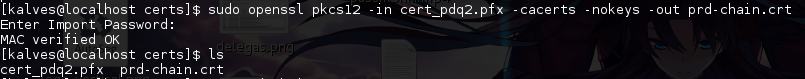


Edite o arquivo server.key , mantenha somente o que está entre

*“ -----BEGIN RSA PRIVATE KEY-----”* e *“-----END RSA PRIVATE KEY-----”*

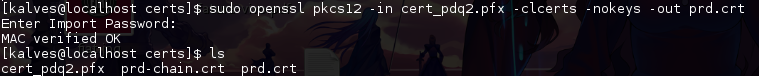
Agora, extraia a cadeia do certificado :

|  |
| --- |
| openssl pkcs12 -**in** cert\_pdq2.pfx -cacerts -nokeys -out prd-chain.crt |



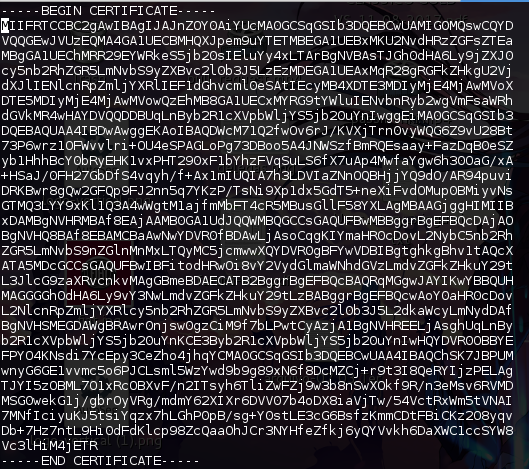
Agora, basta extrair o certificado

|  |
| --- |
| openssl pkcs12 -**in** cert\_pdq2.pfx -clcerts -nokeys -out prd.crt |



Abra os arquivos prd.crt e prd-chain.crt e mantenha somente o que tem entre “*-----BEGIN CERTIFICATE-----”* e “*-----END CERTIFICATE-----* “

Segue um exemplo:

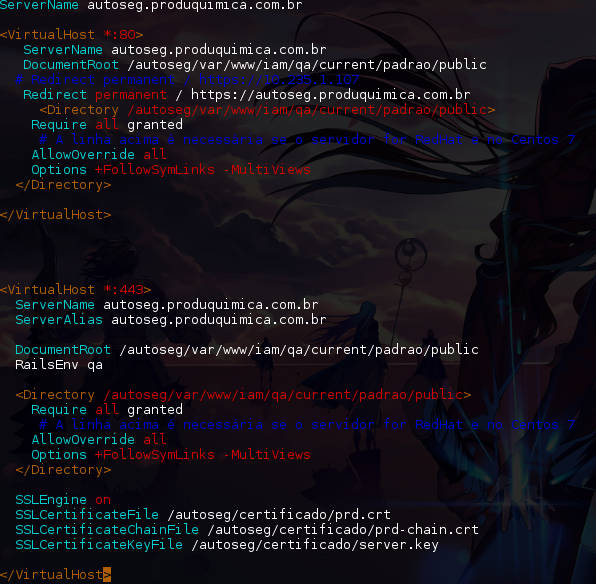


Agora que temos os arquivos, precisamos configurar o apache para que ele encontre-os. Adicione as linhas abaixo na configuração referenciando os certificados.

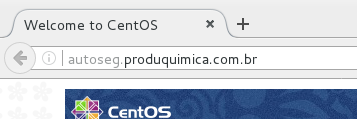
|  |
| --- |
| SSLEngine on  SSLCertificateFile /autoseg/certificado/prd.crt  SSLCertificateChainFile /autoseg/certificado/prd-chain.crt  SSLCertificateKeyFile /autoseg/certificado/server.key |

Para fazer o redirecionamento das portas, use as configurações abaixo.

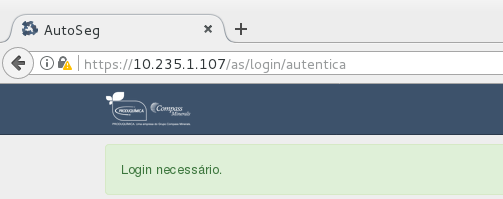
|  |
| --- |
| <VirtualHost \*:80>  ServerName autoseg.produquimica.com.br  DocumentRoot /autoseg/var/www/iam/qa/current/padrao/public  # Redirect permanent / https://10.235.1.107  Redirect permanent / https://autoseg.produquimica.com.br  <Directory /autoseg/var/www/iam/qa/current/padrao/public>  Require all granted  # A linha acima é necessária se o servidor for RedHat e no Centos 7  AllowOverride all  Options +FollowSymLinks -MultiViews  </Directory>  </VirtualHost>  <VirtualHost \*:443>  ServerName autoseg.produquimica.com.br  ServerAlias autoseg.produquimica.com.br  DocumentRoot /autoseg/var/www/iam/qa/current/padrao/public  RailsEnv qa  <Directory /autoseg/var/www/iam/qa/current/padrao/public>  Require all granted  # A linha acima é necessária se o servidor for RedHat e no Centos 7  AllowOverride all  Options +FollowSymLinks -MultiViews  </Directory>  SSLEngine on  SSLCertificateFile /autoseg/certificado/prd.crt  SSLCertificateChainFile /autoseg/certificado/prd-chain.crt  SSLCertificateKeyFile /autoseg/certificado/server.key </VirtualHost> |



Salve o arquivo e reinicie o apache, ao acessar o aplicação na porta 80, ela deve te redirecionar automaticamente para a 443.



Resultado :



**Referencias:**

Criar certificado do Windows para Apache

https://www.sslshopper.com/move-or-copy-an-ssl-certificate-from-a-windows-server-to-an-apache-server.html

Extrair o certificado, chave e certificado do CA do arquivo PFX

https://wiki.cac.washington.edu/display/infra/Extracting+Certificate+and+Private+Key+Files+from+a+.pfx+File

Instalar certificado

https://support.godaddy.com/help/article/5238/como-instalar-um-certificado-ssl-no-apache?locale=pt-BR&countrysite=br

https://www.sslshopper.com/apache-server-ssl-installation-instructions.html

Redirect

https://wiki.apache.org/httpd/RedirectSSL

https://www.sslshopper.com/apache-redirect-http-to-https.html

<http://serverfault.com/questions/570288/is-it-bad-to-redirect-http-to-https>

Extensões dos arquivos:

certificados: .pem ou .crt

chaves: .keys

Formato PKCS #12 - contém todos os componentes (certificado, chave e certificado do CA root ou intermediário)