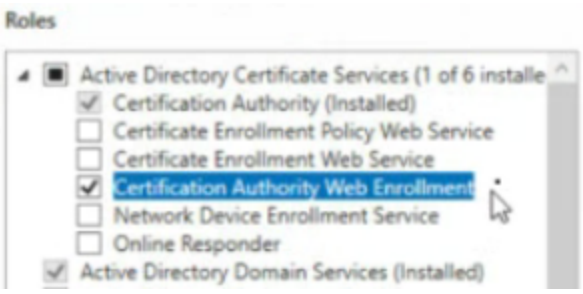
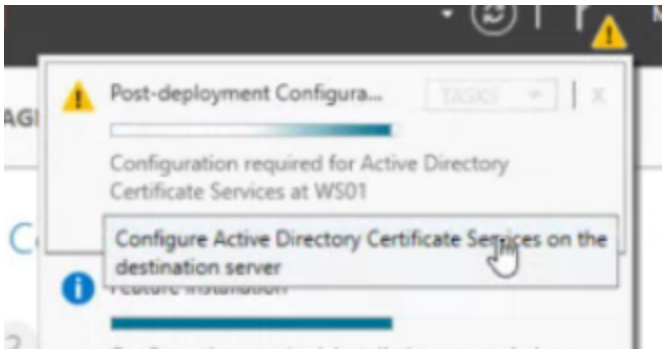
CA (Certificate Autorization)

No Windows

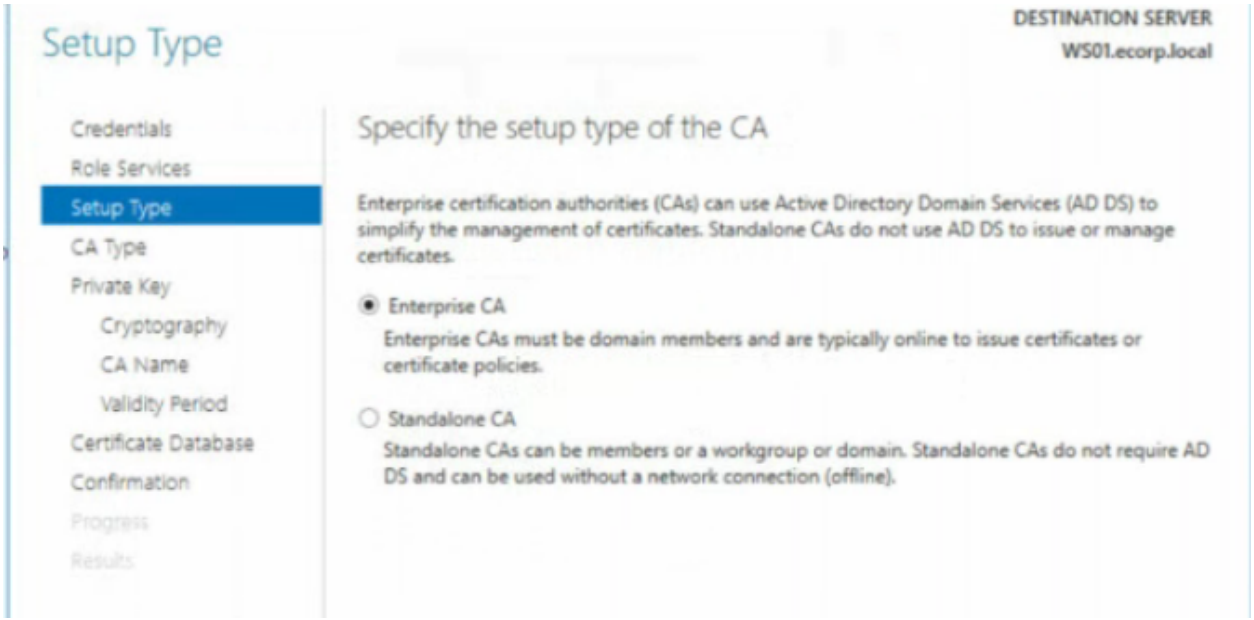
Instalar Certificate Authority Web Enrollment e Certification Authority

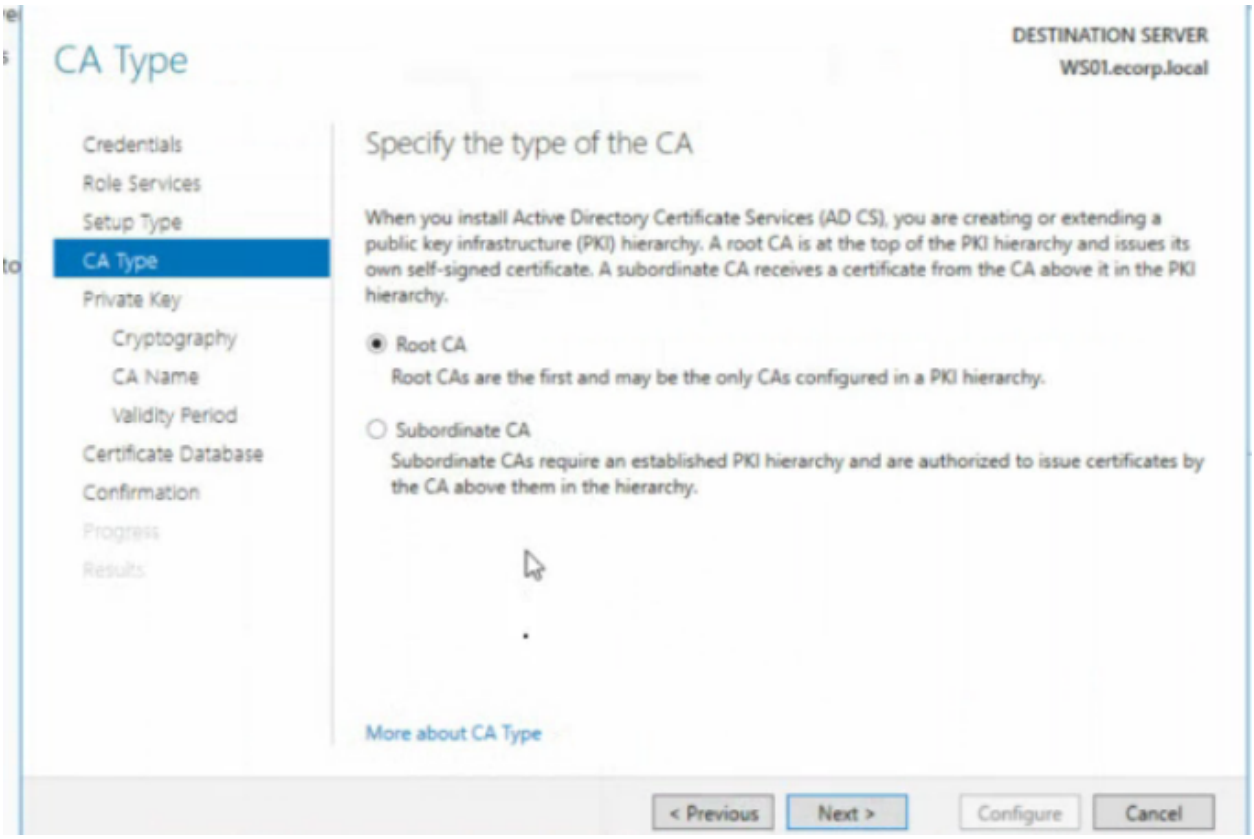


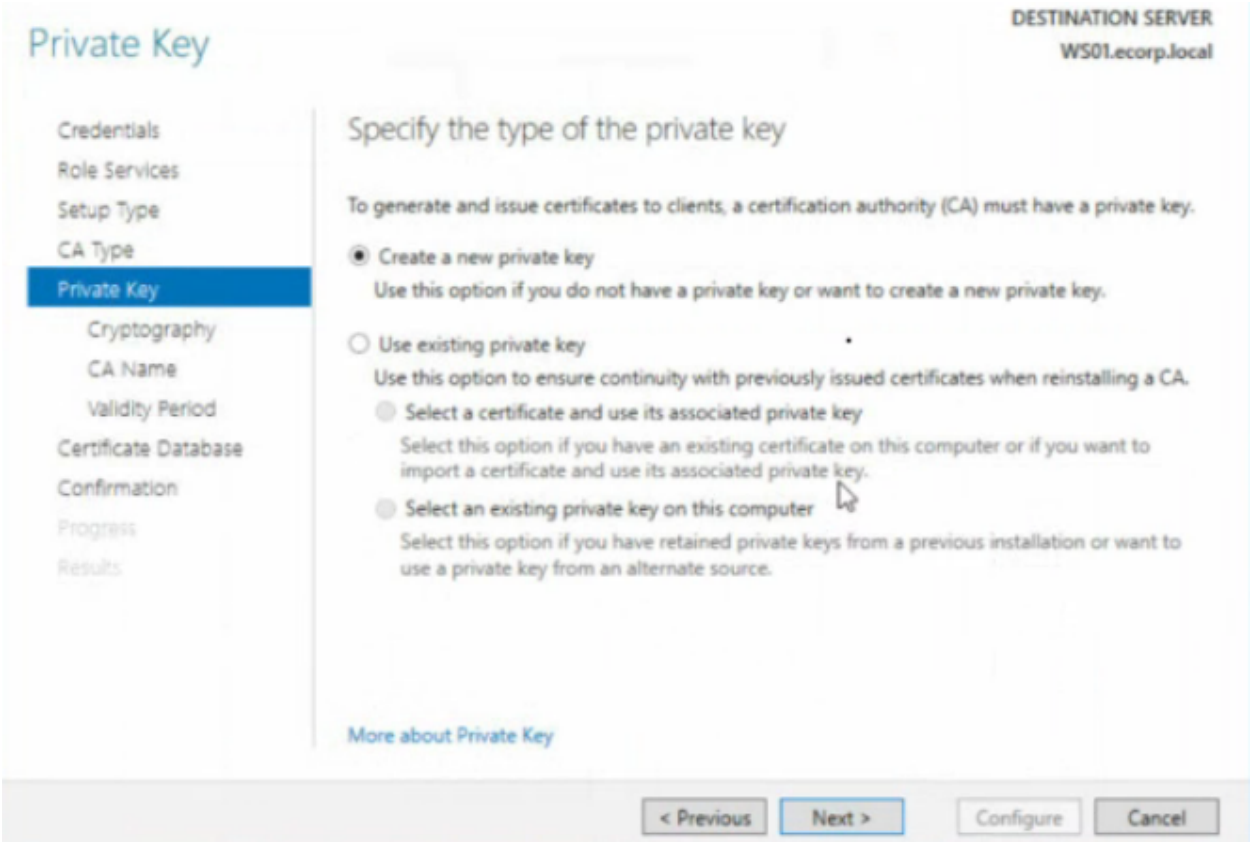
Configurando a CA

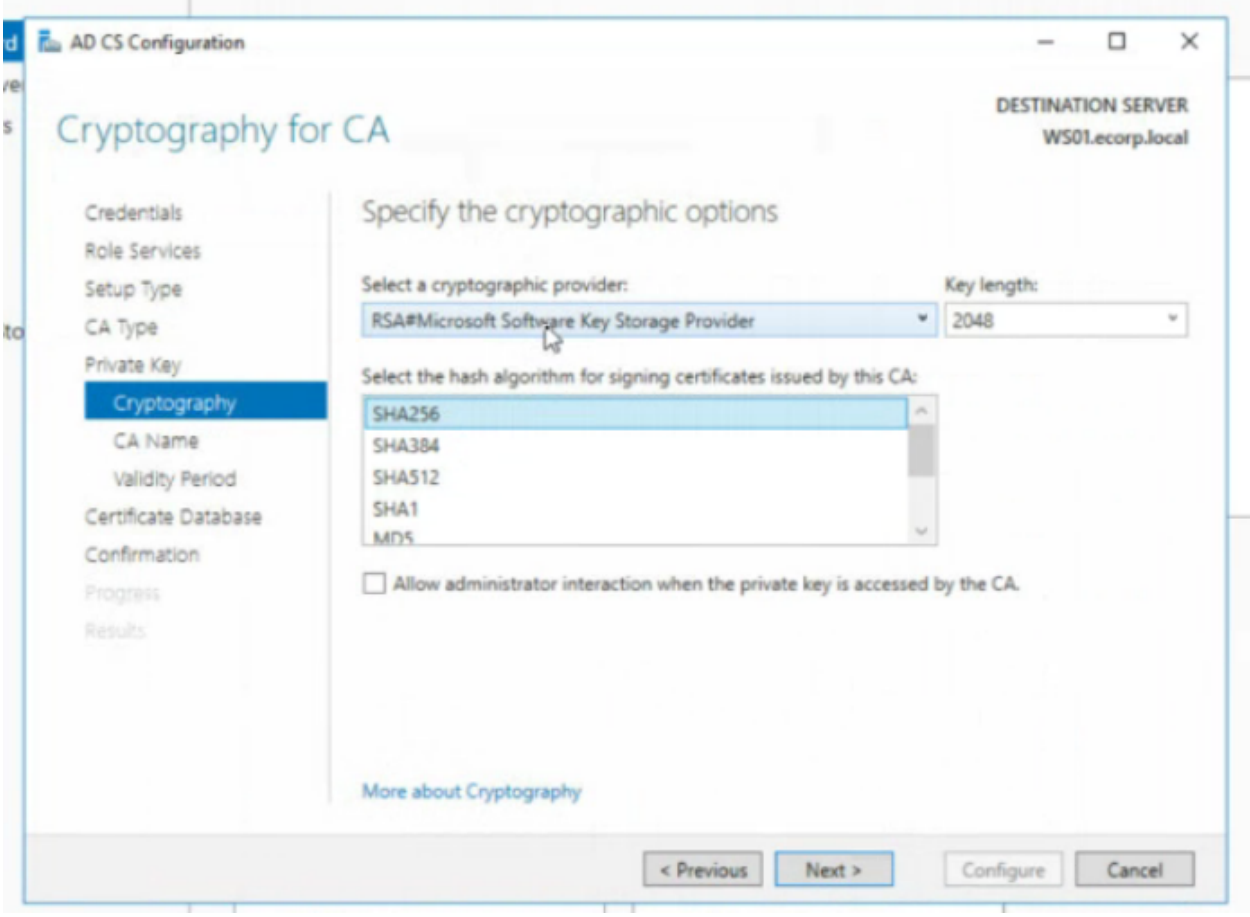


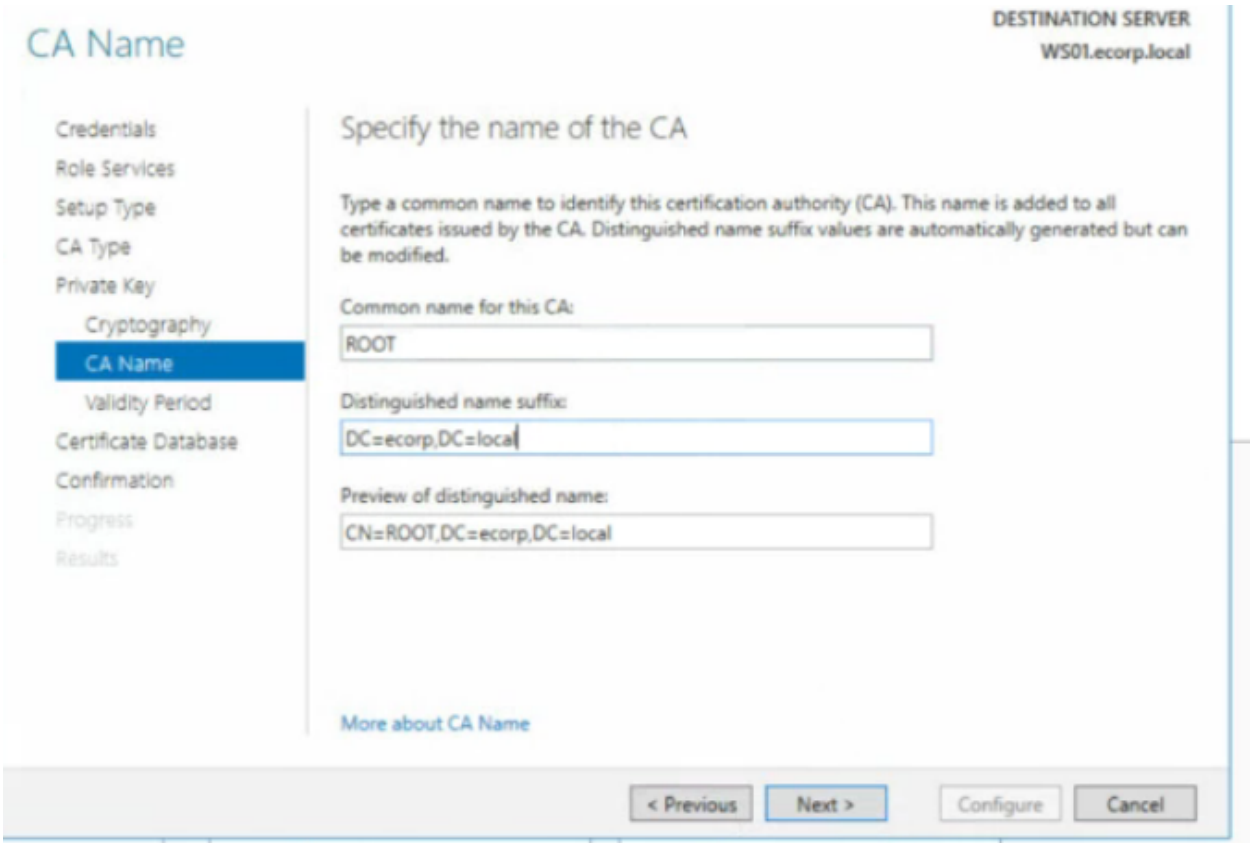

Select Role Services to configure
Certification Authority
Certification Authority Web Enrollment
Online Responder
Network Device Enrollment Service
Certificate Enrollment Web Service
Certificate Enrollment Policy Web Service


Setup Type
DESTINATION SERVER
WS01.ecorp.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the setup type of the CA
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.
Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.
Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

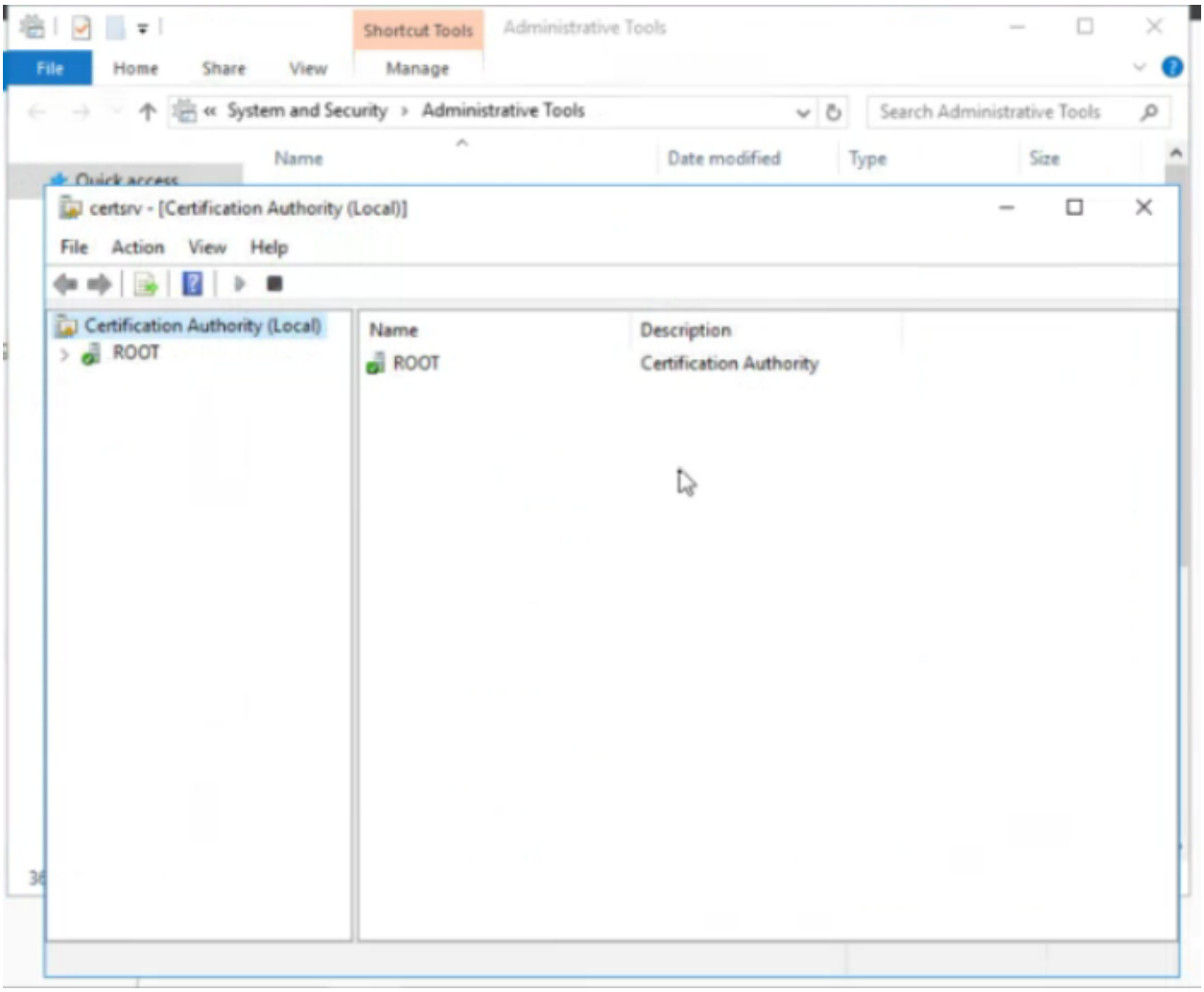

CA Type
DESTINATION SERVER
WS01.ecorp.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the CA
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.
Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.
More about CA Type
< Previous
Next >
Configure
Cancel


Private Key
DESTINATION SERVER
WS01.ecorp.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the private key
To generate and issue certificates to clients, a certification authority (CA) must have a private key.
Create a new private key
Use this option if you do not have a private key or want to create a new private key.
Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
More about Private Key
< Previous
Next >
Configure
Cancel

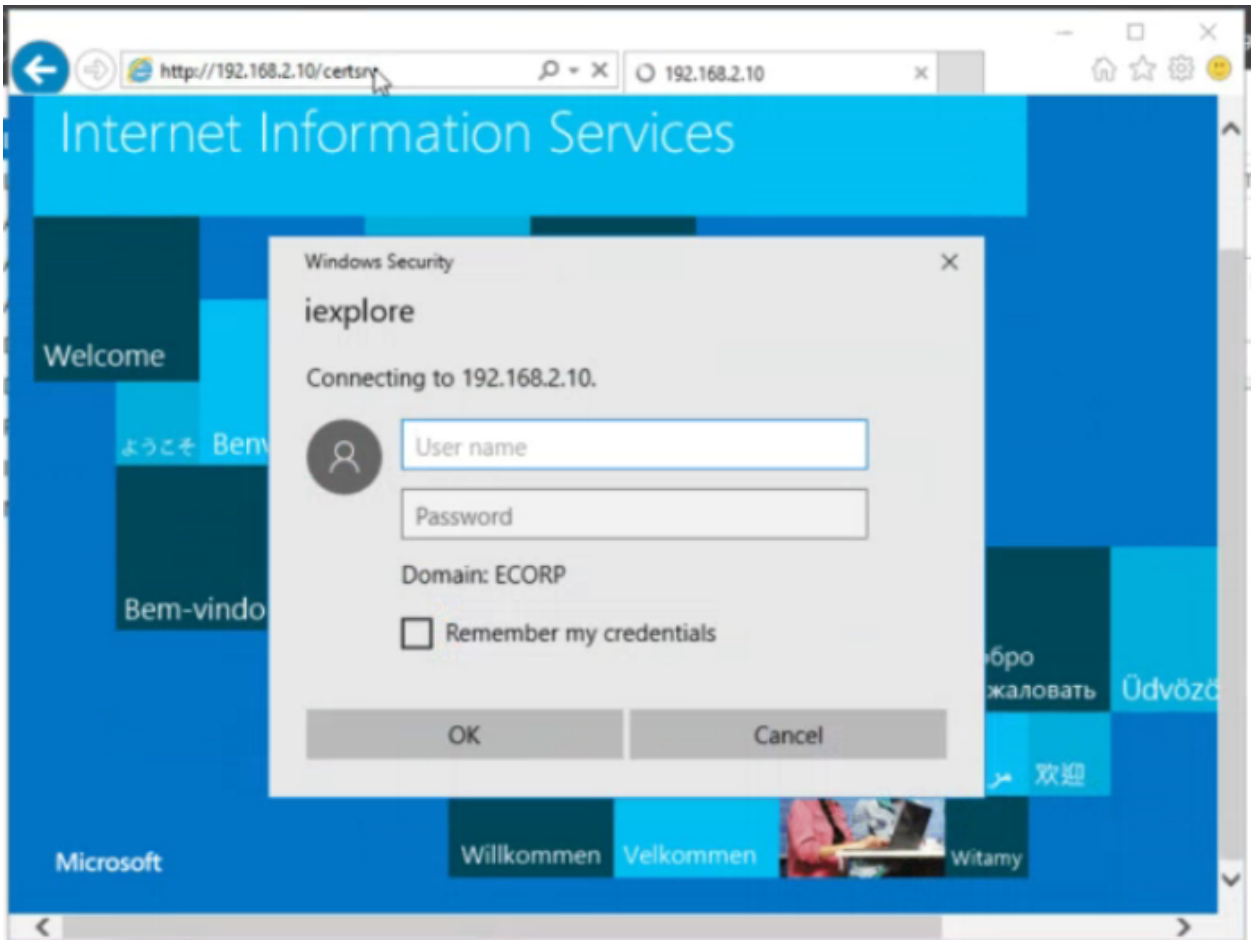

AD CS Configuration
Cryptography for CA
DESTINATION SERVER
WS01.ecorp.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the cryptographic options
Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider
Key length:
2048
Select the hash algorithm for signing certificates issued by this CA:
SHA256
SHA384
SHA512
SHA1
MD5
Allow administrator interaction when the private key is accessed by the CA.
More about Cryptography
< Previous
Next >
Configure
Cancel

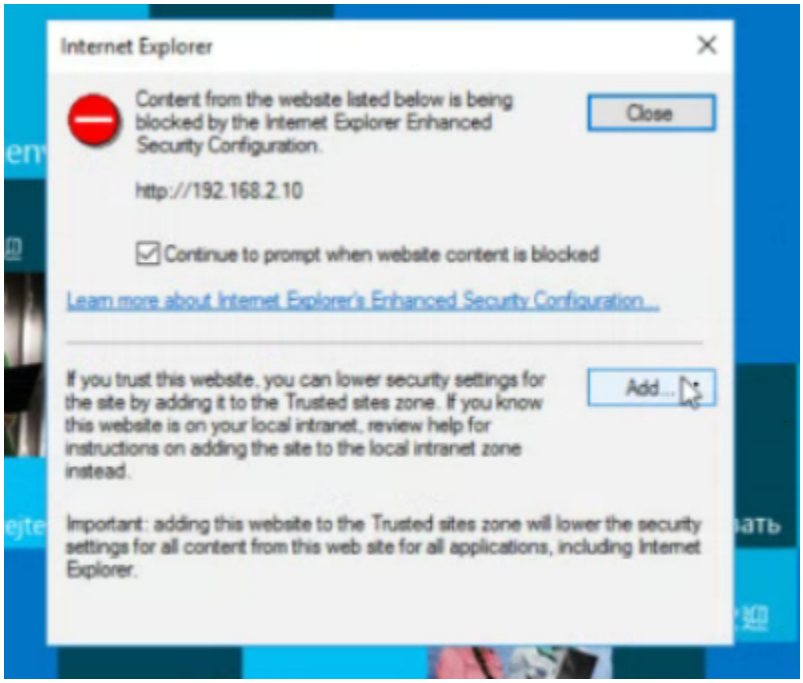


e depois de dar o ok e o configure, reinicia seu windows



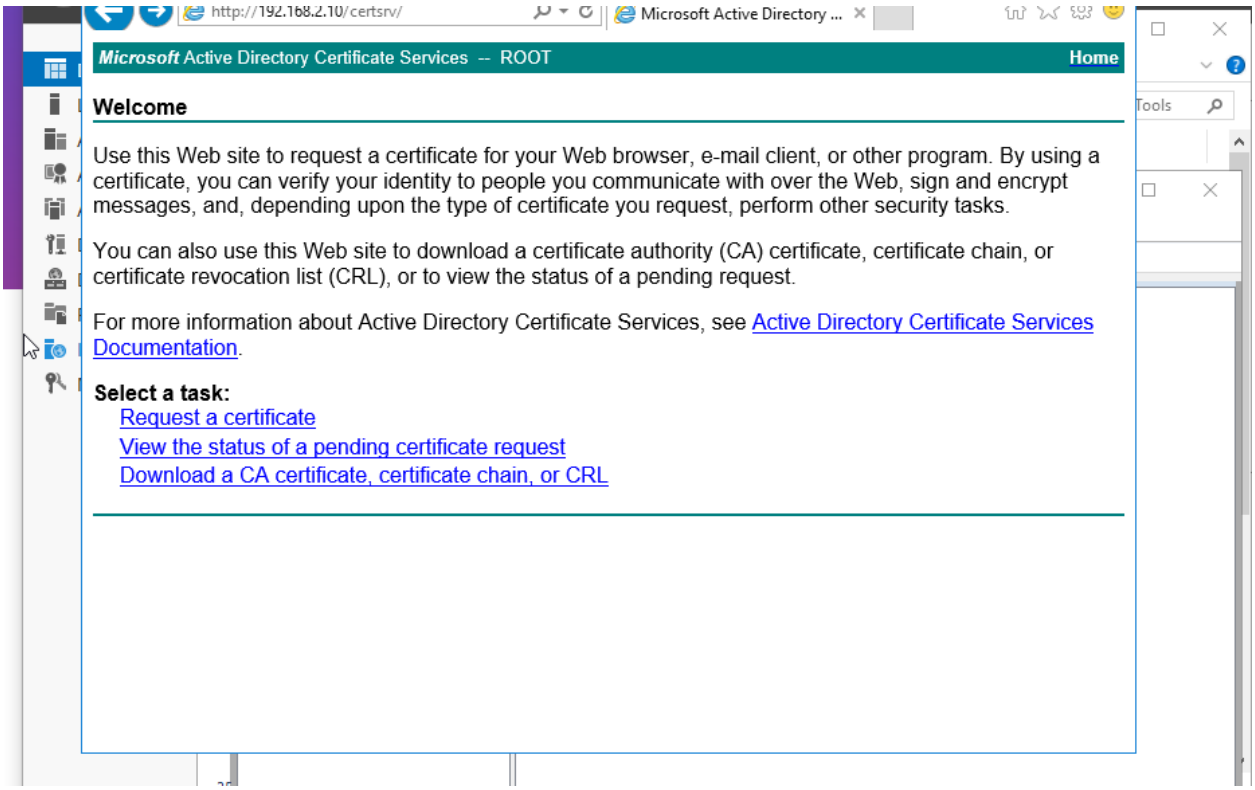
Testar o certificado {IP}/certsrv


http://192.168.2.10/certsrv
192.168.2.10
Internet Information Services
Windows Security
iexplore
Connecting to 192.168.2.10.
User name
Password
Domain: ECORP
Remember my credentials
OK
Cancel
Welcome
Bem-vindo
Willkommen
Velkommen
Witamy
Microsoft

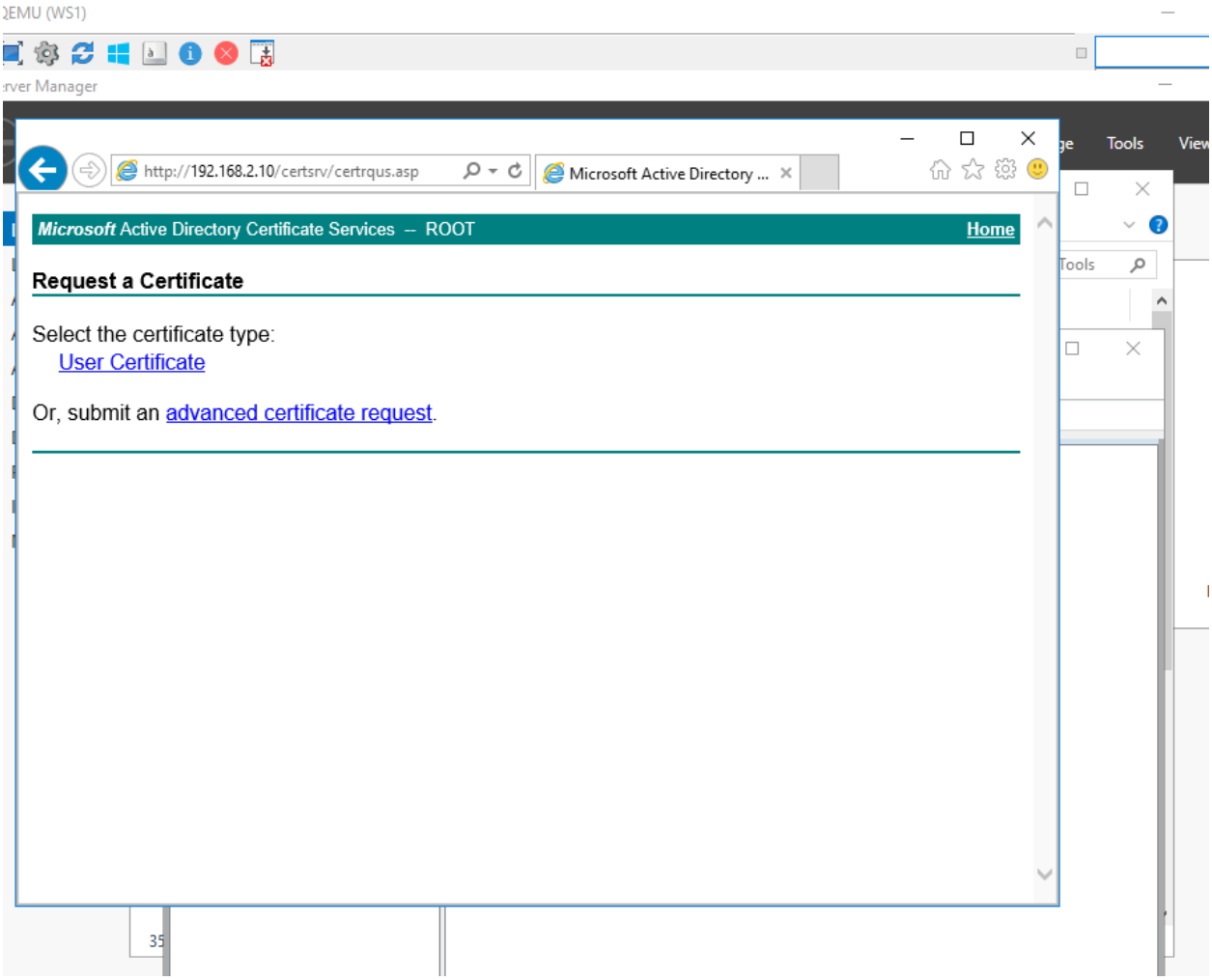

Internet Explorer
Content from the website listed below is being blocked by the Internet Explorer Enhanced Security Configuration.
Close
http://192.168.2.10
Continue to prompt when website content is blocked
Learn more about Internet Explorer's Enhanced Security Configuration...
If you trust this website, you can lower security settings for the site by adding it to the Trusted sites zone. If you know this website is on your local intranet, review help for instructions on adding the site to the local intranet zone instead.
Add...
Important: adding this website to the Trusted sites zone will lower the security settings for all content from this web site for all applications, including Internet Explorer.

Caso apresente erros, adicione ele nos trust websites

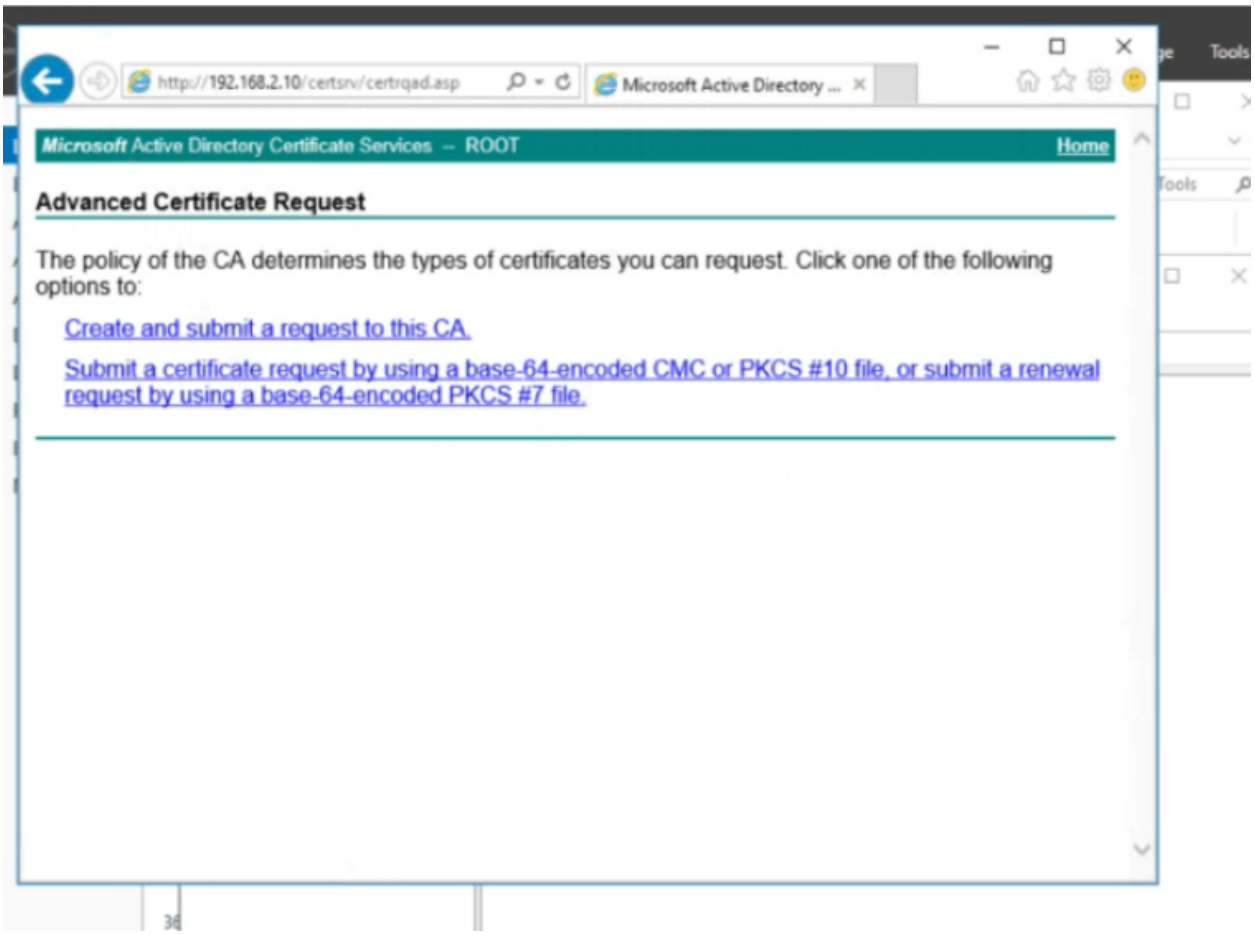
Clique em request a certificate



Depois em advanced certificate request

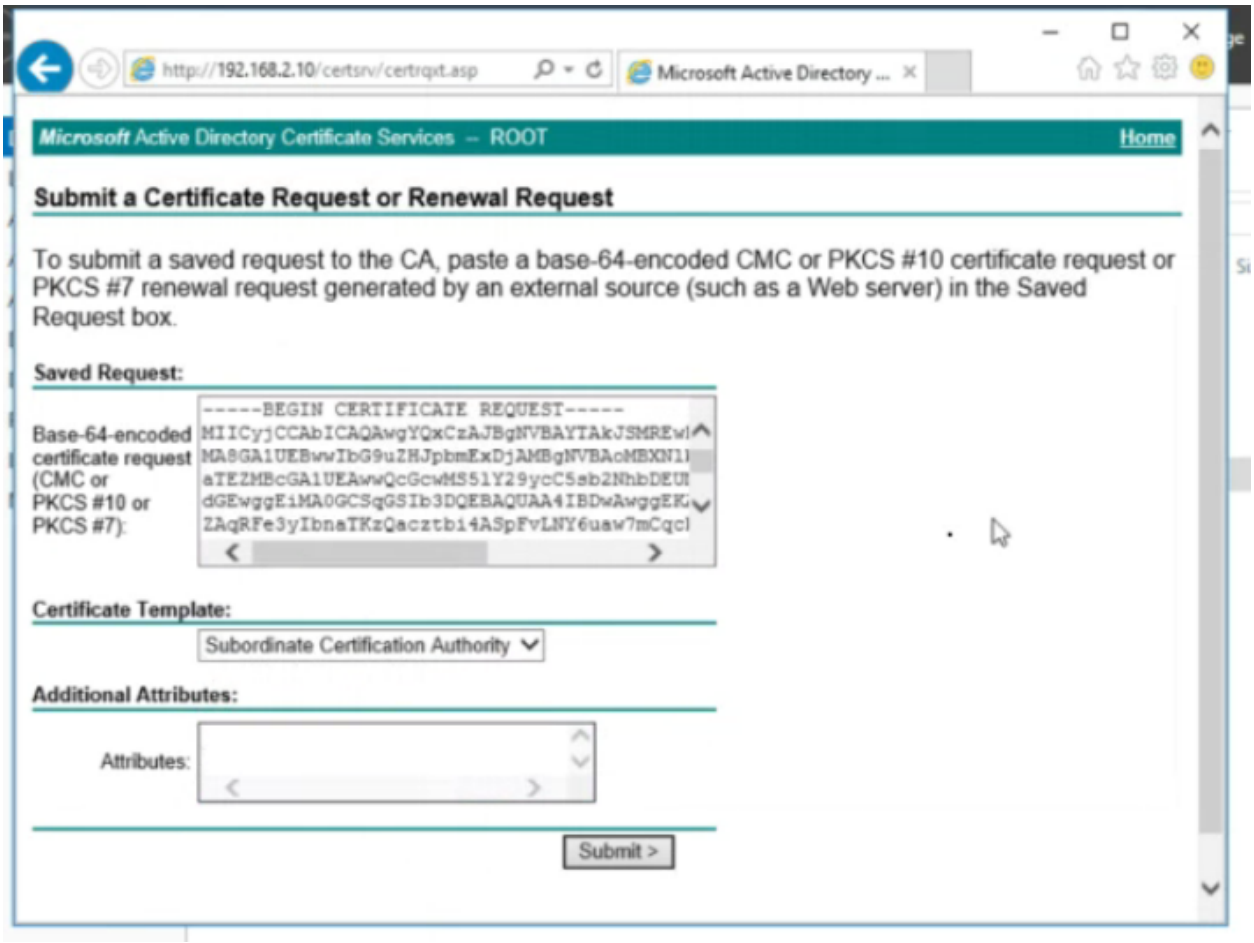


opcao Submit a certificate



Abre o arquivo de req que trouxemos da maquina LINUX

e cola no encoded do base64



Baixa em base64

e agora, vamos enviar ele para a maquina Linux, novamente