



Presentación

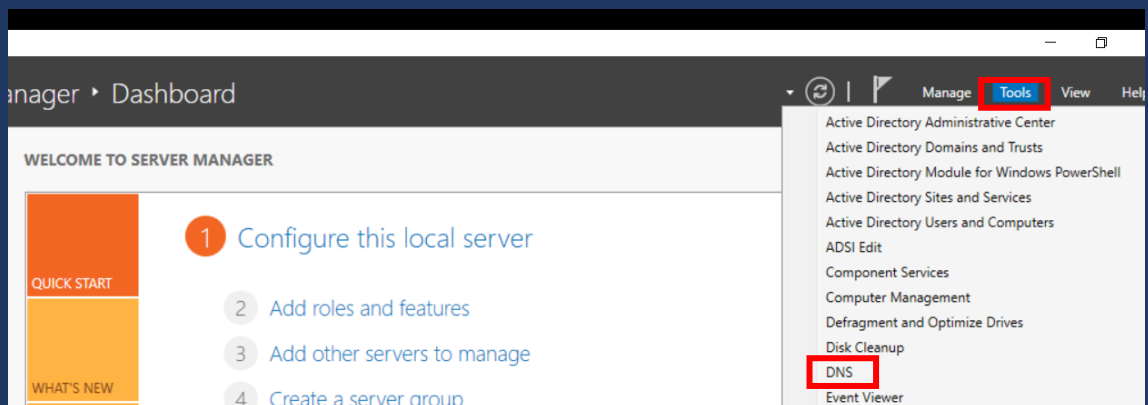
- **Nombre del estudiante:** Jamiel Santana.
- **Matricula:** 2019-8095.
- **Nombre del profesor:** Geancarlos Sosa.
- **Mat:** Seguridad de SO.
- **Tema:** DNSSEC.
- **Centro Educativo:** Instituto tecnológico de las Américas.

➤ **DNSSEC:**

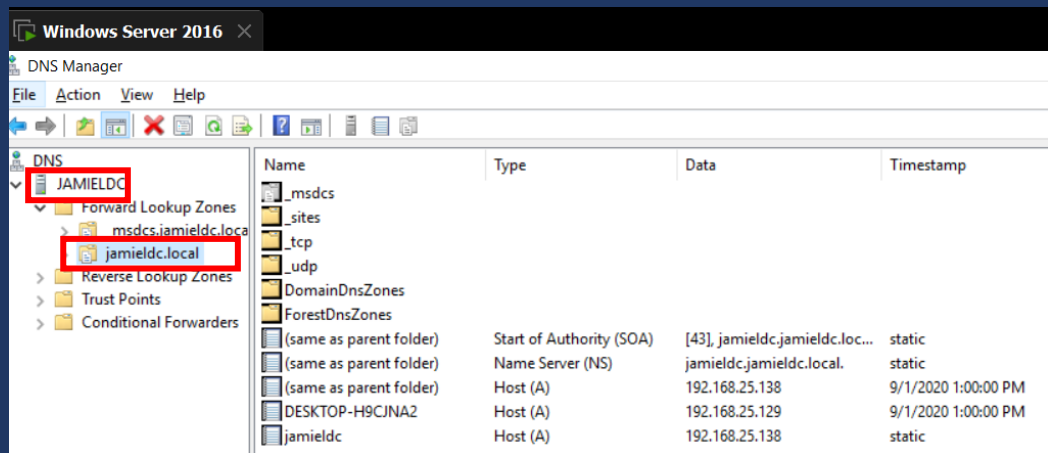
- Las extensiones de seguridad del sistema de nombres de dominio (DNSSEC) son una extensión del protocolo DNS, definido por el Grupo de trabajo de ingeniería de Internet (IETF, del cual Microsoft es miembro), que utiliza criptografía de clave pública para proporcionar integridad y autenticación a la zona DNS registro.
- Al utilizar DNSSEC se añaden firmas digitales en cada una de las partes implicadas: dominio, servidor DNS y Registry.
- Las DNSSEC agregan dos funciones importantes al protocolo del DNS:
 - La autenticación del origen de los datos permite a un resolutor verificar criptográficamente que los datos que recibe provienen de la zona donde considera que los datos se originaron.
 - La protección de la integridad de los datos permite que el resolutor sepa que los datos no han sido modificados en tránsito desde que fueron firmados originalmente por el propietario de la zona con la clave privada de la zona.

➤ **Habilitar DNSSEC:**

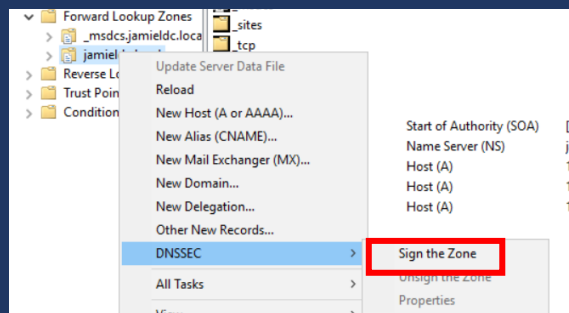
1. Como primer paso tendremos que dirigirnos a nuestro DNS manager que lo podemos visualizar en nuestro **server manager > Tools > DNS**.



2. Ya en nuestro server manager vamos a (Nombre DNS) > Forward lookup zone > (Nombre de nuestro dominio), nos dirigimos hasta aquí para realizar el DNSSEC justo sobre nuestro dominio y sobre los registros que este contiene.

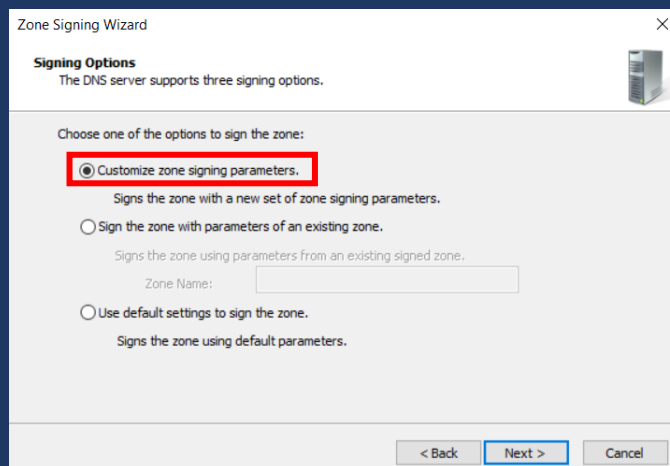


3. Ya encontrado nuestro dominio damos **click** derecho sobre el y elegimos la opción de **DNSSEC**.

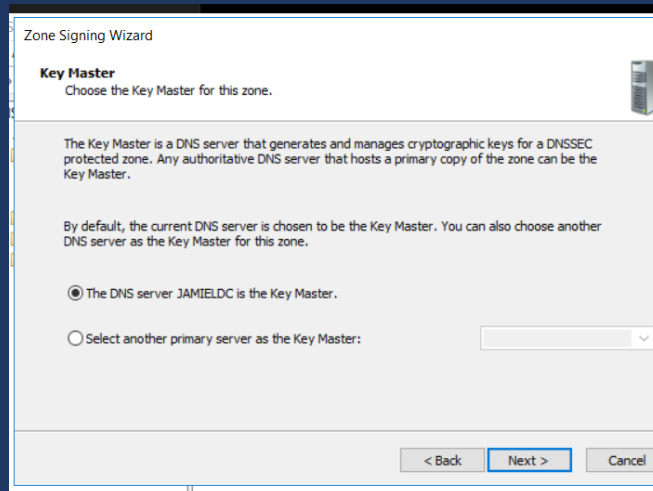


4. Ya hecho click en **DNSSEC** se nos abre el asiste para realizar la configuración de **DNSSEC**, la primera ventana emergente solo nos explica un poco de DNSSEC por lo tanto inmediatamente le damos click en **next**.
5. Ya en el siguiente paso el wizard nos muestra que existen 3 opciones de configuración el **DNSSEC**.
 - a. Configurar el dominio con nuevos signing parameters.
 - b. Configurar dominio seleccionado con los parámetros de otro dominio existente.
 - c. Utilizar los valores predeterminados del wizard.

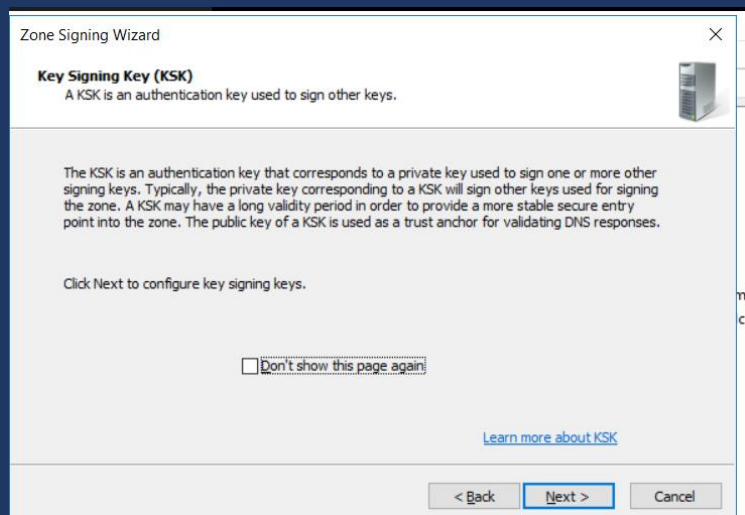
Nosotros haremos uso de la primera opción para configurar los parámetros desde 0 nosotros mismos.



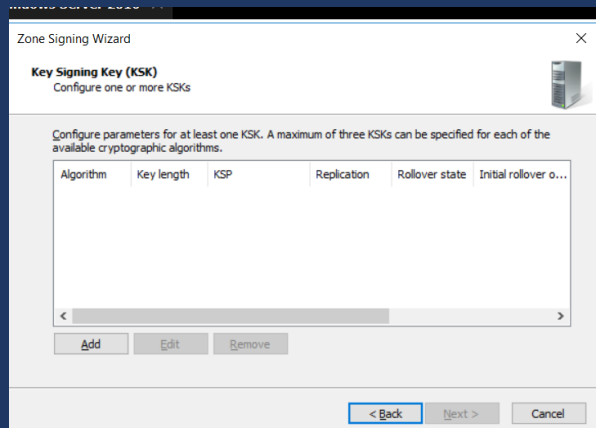
6. En el siguiente paso vamos a seleccionar el dominio para el cual se le van a generar las key masters.



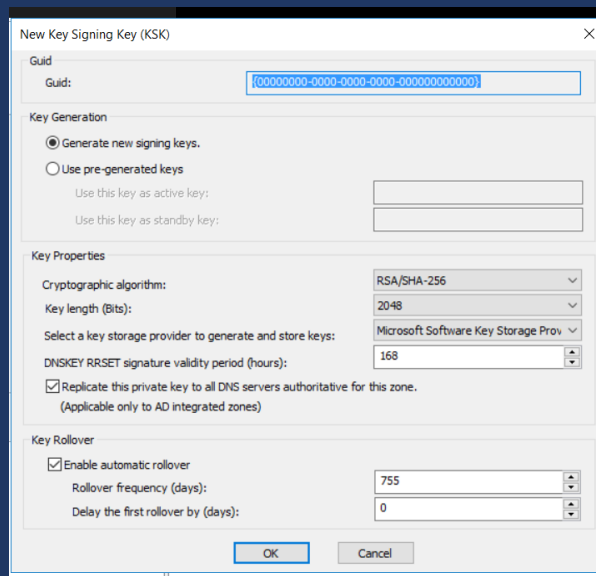
7. Ya en el siguiente paso vamos a muestra de que trata un poco las claves KSK y para que sirven, damos click en next.



8. Ya vienen los pasos importantes como la configuración de las claves ya en este paso hacemos click en ADD para configurar los parámetros de la clave ksk, dado click en add se nos abrirá una ventana para configurar las claves con las opciones mostradas en la imagen.

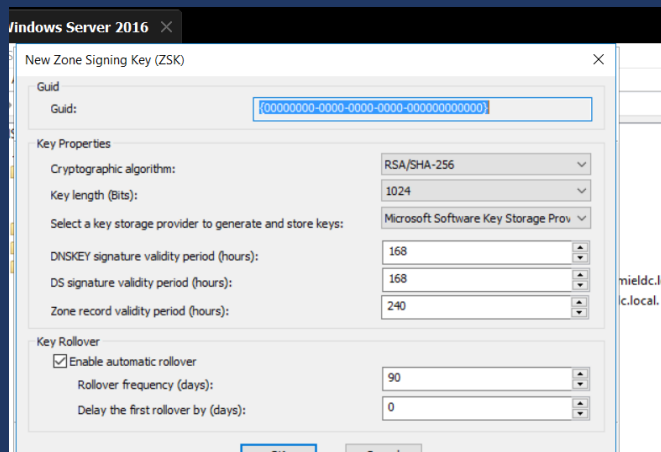


Por motivos prácticos dejaremos los valores predeterminados de la clave de cifrado,

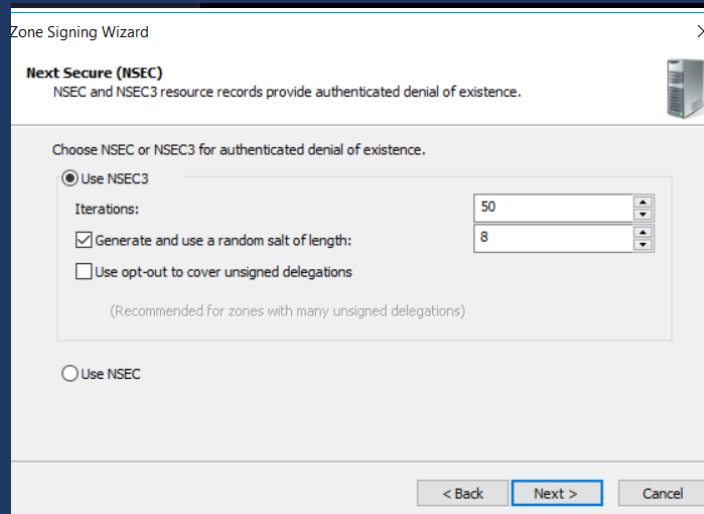


Ya en el paso exterior damos click en ok y posteriormente a next para realizar el siguiente paso.

9. Ahora vamos a configurar el cifrado de las claves ZSK son unas claves privadas uy hacen la función de llaves de autenticación, volvemos a dar click en add, vamos a dejar los valores predeterminados igual en zks

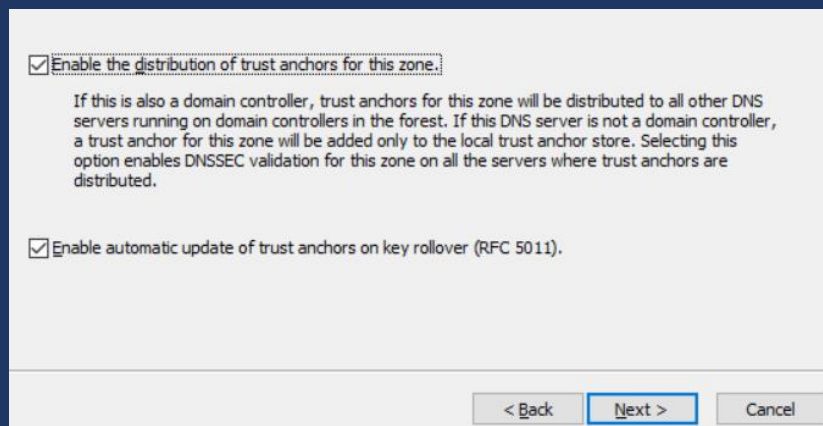


10. Ahora en el siguiente paso vamos a habilitar quien será el proporcionados de nuestro denegador de existencia autentificada, dejaremos la primera opción seleccionada.



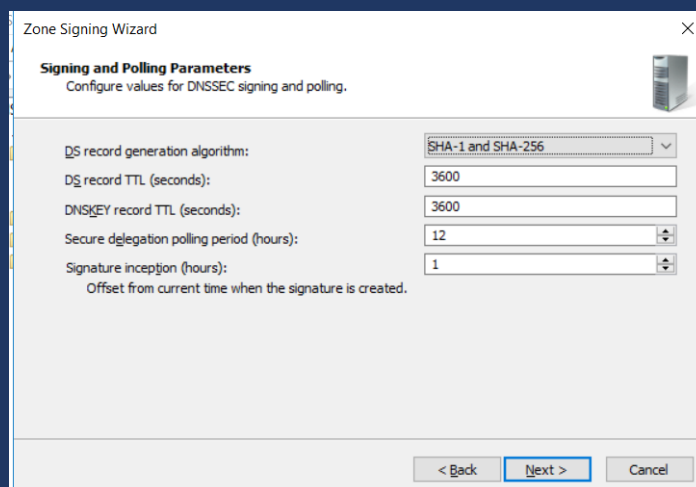
The screenshot shows the 'Zone Signing Wizard' window, specifically the 'Next Secure (NSEC)' step. The title bar says 'Zone Signing Wizard'. Below the title, it says 'Next Secure (NSEC)' and 'NSEC and NSEC3 resource records provide authenticated denial of existence.' The main instruction is 'Choose NSEC or NSEC3 for authenticated denial of existence.' There are two radio buttons: 'Use NSEC3' (which is selected) and 'Use NSEC'. Under 'Use NSEC3', there are three options: 'Iterations:' with a value of 50, 'Generate and use a random salt of length:' with a value of 8, and 'Use opt-out to cover unsigned delegations' (which is unchecked). A note below says '(Recommended for zones with many unsigned delegations)'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

11. Ya en este último paso vamos a seleccionar la primera casilla para habilitar la zona completa.



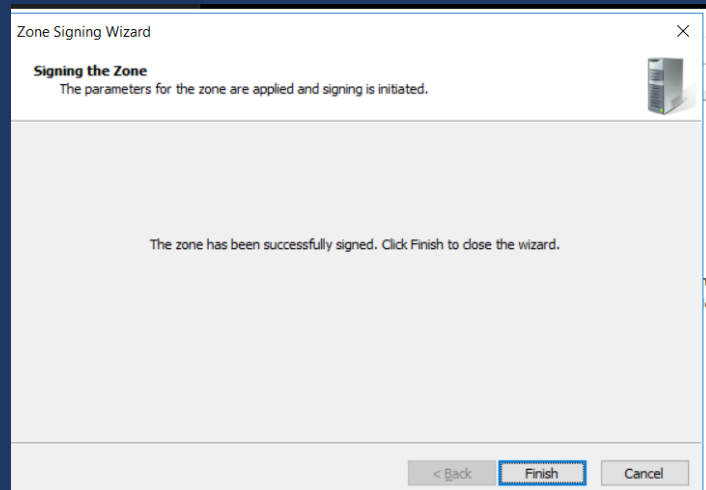
The screenshot shows the 'Zone Signing Wizard' window, specifically the 'Trust Anchors' step. The title bar says 'Zone Signing Wizard'. Below the title, it says 'Trust Anchors' and 'Trust anchors are used to validate the authenticity of the zone's data.' The main instruction is 'Select the trust anchors for this zone.' There are two checkboxes: 'Enable the distribution of trust anchors for this zone.' (which is checked) and 'Enable automatic update of trust anchors on key rollover (RFC 5011).' (which is also checked). A text block explains: 'If this is also a domain controller, trust anchors for this zone will be distributed to all other DNS servers running on domain controllers in the forest. If this DNS server is not a domain controller, a trust anchor for this zone will be added only to the local trust anchor store. Selecting this option enables DNSSEC validation for this zone on all the servers where trust anchors are distributed.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

12. Hacemos click en nexts para comenzar continuar el siguiente paso, que seria configurar el algoritmo de cifrado, por motivos prácticos y no reales dejaremos todo como predeterminado.



The screenshot shows the 'Zone Signing Wizard' window, specifically the 'Signing and Polling Parameters' step. The title bar says 'Zone Signing Wizard'. Below the title, it says 'Signing and Polling Parameters' and 'Configure values for DNSSEC signing and polling.' The main instruction is 'Configure values for DNSSEC signing and polling.' There are five settings: 'DS record generation algorithm:' (set to 'SHA-1 and SHA-256'), 'DS record TTL (seconds):' (set to 3600), 'DNSKEY record TTL (seconds):' (set to 3600), 'Secure delegation polling period (hours):' (set to 12), and 'Signature inception (hours):' (set to 1). A note below says 'Offset from current time when the signature is created.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- Ya nos muestra un resumen de todo lo que hemos configurado y hecho click en next solo es esperar unos segundos a que se configure.

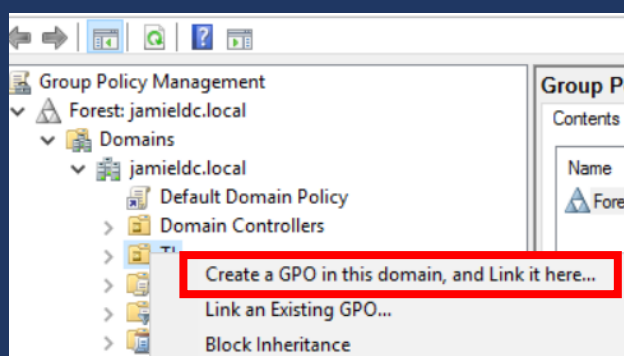


- Terminamos de configurar esto y lo primero que hacemos reiniciar el servidor para que se cumplan los cambios realizados a nuestro DNS, una vez reiniciado nuestro servidor nos dirigimos nuevamente a nuestro DNS manager. Si nos fijamos nuestra zona obtiene un candadito indicando que nuestro DNSSEC está perfectamente configurado.

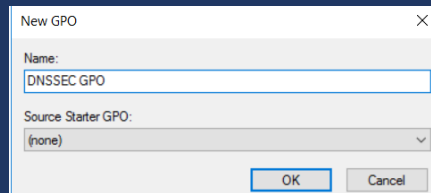
Name	Type	Status	DNSSEC Status	Key Master
_msdcs.jamieidc.local	Active Directory-Integrated Pr...	Running	Not Signed	
jamieidc.local	Active Directory-Integrated Pr...	Running	Signed	jamieidc.jam...

➤ Propagar la configuración de DNSSEC a los clientes mediante GPO:

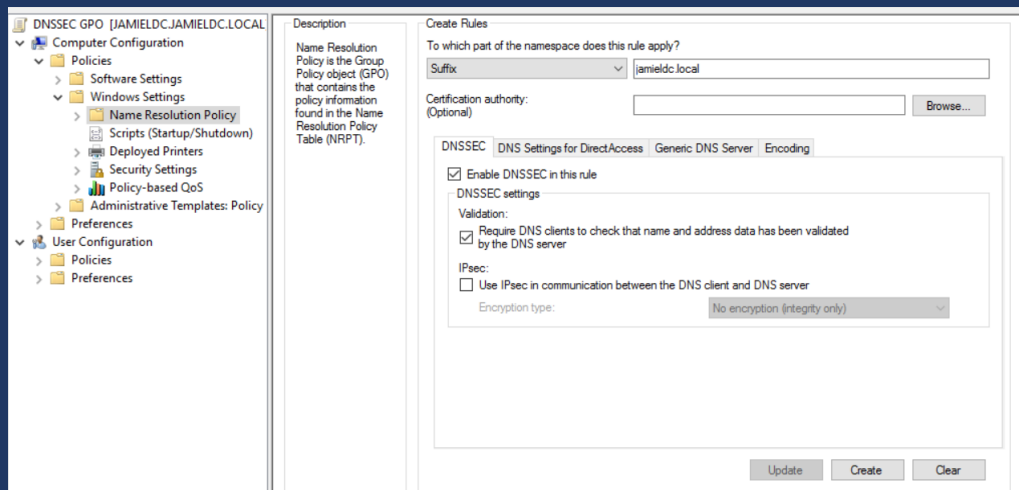
- Dentro de nuestro servidor tenemos una OU llamada TI que es a la cual le vamos a aplicar la GPO.
- Dicho lo anterior nos vamos a dirigir a nuestro **Group policy management**, y procederemos a crear una GPO para dicha OU donde desplegaremos DNSSEC.



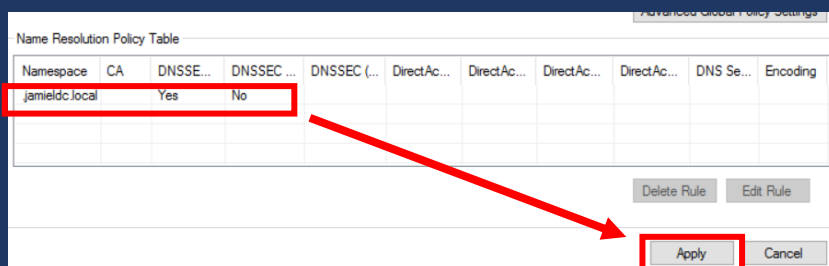
- Donde le pondremos un nombre respectivo a lo que trabajaremos dentro de ella (DNSSEC GPO).



- Ya dentro de la administración de la GPO que acabamos de crear nos dirigimos a **Computer Configuration > Políticas > Window Settings > Name Resolution Policy**. Dentro de esta configuración rellenaremos las siguientes casillas **después de 'Suffix' ingrese su nombre de dominio, Marque 'Habilitar DNSSEC en esta regla, Marque Requerir que los clientes DNS marquen y crear**.



- Vemos como se ha agregado nuestra configuración a nuestra tabla de **políticas de resolución de nombres y damos click en aplicar**



- Asegúrese de que los clientes tienen la tabla de directivas de resolución de nombres correcta, con el siguiente comando de PowerShell: **Get-DnsClientNrptPolicy**


```

PS C:\Windows\system32> Get-DnsClientNrptPolicy

Namespace                : .jamielc.local
QueryPolicy               :
SecureNameQueryFallback  :
DirectAccessIPsecCARestriction :
DirectAccessProxyName    :
DirectAccessDnsServers    :
DirectAccessEnabled       :
DirectAccessProxyType     : NoProxy
DirectAccessQueryIPsecEncryption :
DirectAccessQueryIPsecRequired : False
NameServers               :
DnsSecIPsecCARestriction  :
DnsSecQueryIPsecEncryption :
DnsSecQueryIPsecRequired  : False
DnsSecValidationRequired  : True
NameEncoding              : Utf8WithoutMapping

PS C:\Windows\system32>

```

- Para comprobar los "Anclas de confianza" y "Puntos de confianza".

Get-DnsServerTrustAnchor -Name (Nombre del dominio)

Get-DnsServerTrustPoint

```

Administrator: Windows PowerShell
PS C:\Windows\system32> Get-DnsServerTrustAnchor -Name jamielc.local

TrustAnchorName      TrustAnchorType      TrustAnchorState      TrustAnchorData
-----
jamielc.local        DNSKEY               Valid                 [47911][DnsSec][RsaSha256][AwEAAZOU...
jamielc.local        DNSKEY               Valid                 [61894][DnsSec][RsaSha256][AwEAAeSw...

PS C:\Windows\system32> Get-DnsServerTrustPoint

TrustPointName      TrustPointState      LastActiveRefreshTime      NextActiveRefreshTime
-----
jamielc.local        Active               10/16/2020 2:13:15 AM      10/16/2020 3:13:15 AM

```

- Y para asegurarse de que los registros se están firmando, utilice la sintaxis siguiente.

Resolve-DnsName -Name lan-host -Type A -Server lan-dc-2016 -DnsSecOK

```

Administrator: Windows PowerShell
PS C:\Windows\system32> Resolve-DnsName -Name jamielc -Type A -Server jamielc -DnsSecOK

Name      Type  TTL  Section  IPAddress
-----
jamielc.jamielc.local  A     1200  Answer   192.168.25.138

Name      : jamielc.jamielc.local
QueryType : RRSIG
TTL       : 1200
Section   : Answer
TypeCovered : A
Algorithm : 8
LabelCount : 3
OriginalTtl : 1200
Expiration : 26/10/2020 6:57:43
Signed     : 16/10/2020 5:57:43
Signer     : jamielc.local
Signature  : {167, 22, 140, 246...}

Name      : .
QueryType : OPT
TTL       : 32768
Section   : Additional
Data      : {}

```