ScriptDotS

We are all in a void. A pointer to something that doesn't exist…

ACTIVE DIRECTORY PENTESTING | BLOGS | WINDOWS PENTESTING

Winsaaf Man

October 29, 2018 · 2 Comments

Active Directory Penetration Dojo- Creation of Forest Trust: Part 3

Hi everyone,

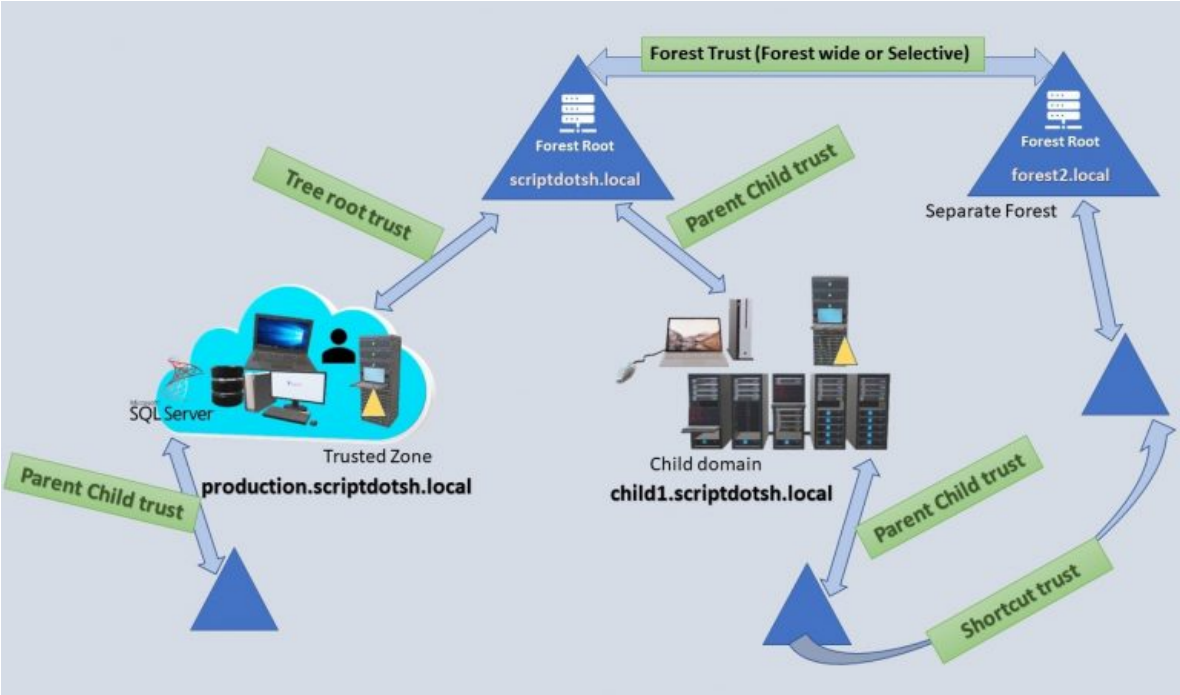
Welcome to the third part of the setup series on Pentesting lab in AD environment. I apologize for the delay. Reason being I was busy in few family issues and couldn't get time to write. Anyways, let's take a look at the current post.

In the previous posts, we learnt about the Active Directory basics and the different servers in AD environment. Now you know basic operations like how to create a domain controller, member servers in AD environment, how to add users & computers in the domains.

Now, let's have a look at current post. I've decided to explain Active Directory trusts at this stage because it's important to understand it as we're gonna abuse the trusts later.

Active Directory Trusts:-

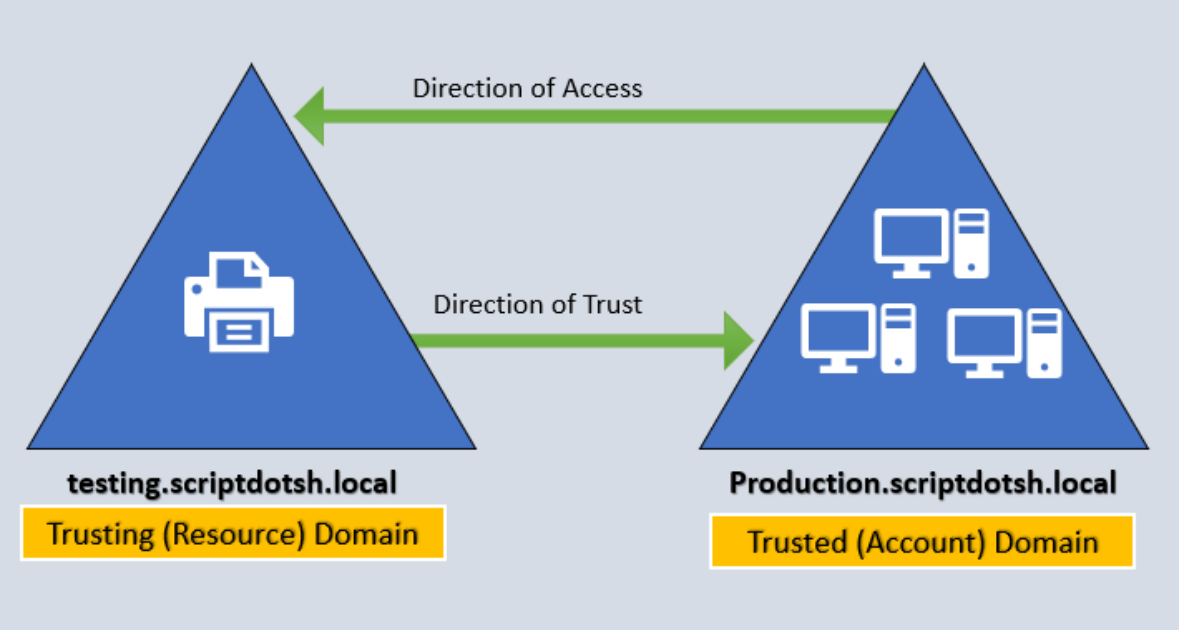
Diagram showing few trust types:-



In Active Directory environment, trust enables you to grant access to resources to users, groups and computers across entities by linking up the authentication systems of two domains and allows authentication traffic to flow between them through a system of referrals. It's a two-step process. First step is to establish the trust. Second step is to assign the permissions.

> Trust direction (One-way or two way)

Trusts can be one-way or two-way. In two-way trust, the domain on either side can access the other side. And in one-way trust "Domain A trusts domain B." which means that domain A is the trusting domain and domain B will be the trusted domain. For a user in a certain domain to access a resource in another domain, the user needs to be in the trusted domain. Have a look at below diagram to understand one way trust:



If it still looks confusing i.e. which direction does the trust point?, let me explain it using an analogy using my friends as an example. Let's say if Paranoid Ninja were to give his KTM Motorcycle to Slaer to allow him to use it, he is establishing a trust between him and Slaer. In this case, Paranoid Ninja is the trusting domain, and Slaer is the trusted domain. Once the Motorcycle is provided, then the next step is to allow access to use Motorcycle (Motorcycle Key). So, this trust is only in one direction i.e. Paranoid Ninja trusts Slaer.

Types of AD trusts:

There are various trust types. Trusts can be transitive or non-transitive. Below table explains some types of trusts:

Trust Type	Property	Trust Direction	Auth.	Details
Tree-Root	Transitive	Two-way	Kerberos V5 or NTLM	Created automatically when a new Tree is added to a forest.
Parent-Child	Transitive	Two-way	Kerberos V5 or NTLM	Created automatically when a child domain is added.
Shortcut	Transitive	One-way or Two-way	Kerberos V5 or NTLM	Created Manually. Used in a forest to shorten the trust path to improve authentication times.
Forest	Transitive	One-way or	Kerberos V5 or NTLM	Created Manually. Used to share resources between AD

		Two-way		DS forests.

Transitive Trust in a forest:-

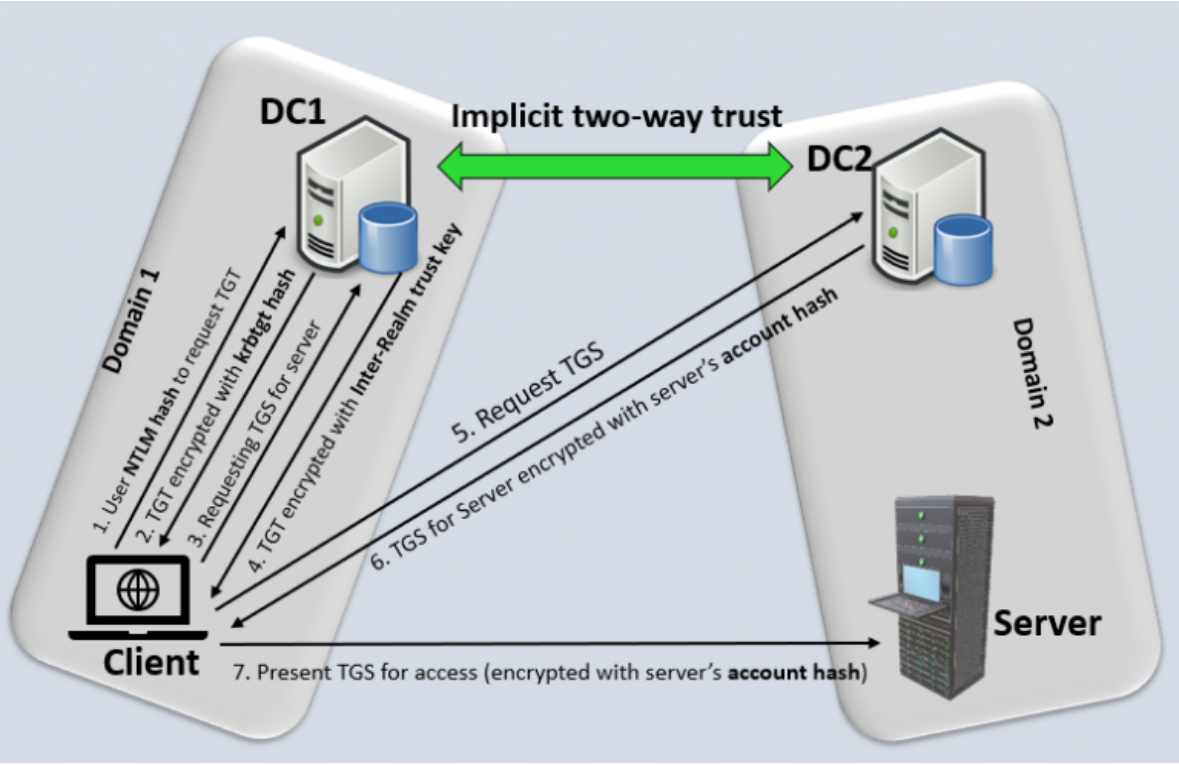
A trust that extends to any other trusted domain in the forest. For example:- If A *trusts* B, and B *trusts* C. Therefore, A *trusts* C.

Automatic Trusts in forest:-

By default, two-way, transitive trusts are created automatically when a child domain is added or when a domain tree is added. The two default trust types are parent-child trusts and tree-root trusts.

> Trust Flow in Parent-Child domains:-

Below is a picture to visualize the Kerberos process across trust boundaries:



TGT–>TGT stands for “Ticket Granting Ticket”. A ticket-granting ticket (TGT) is a special ticket that permits the client to obtain additional Kerberos tickets within the same Kerberos realm. When a client sends a request for a ticket to the Key Distribution Center (KDC), the KDC creates a ticket-granting ticket (TGT) for the client, (encrypts it using the client’s password as

the key) and sends the encrypted TGT back to the client. The client then attempts to decrypt the TGT, using its password. If the client successfully decrypts the TGT (i.e., if the client gave the correct password), it keeps the decrypted TGT, which indicates proof of the client's identity.

TGT permits the client to obtain additional tickets (like TGS) which gives permission for specific services.

TGS–> TGS stands for "Ticket granting service". TGS is a KDC component that issues a service ticket when a client requests connection to a Kerberos service. Client needs to have a valid TGT, only then the TGS will be issued to it.

Inter-Realm TGT –> In case of authentication in inter-forest trusts, instead of encrypting with Domain1's **krbtgt** account, a ticket is encrypted/signed with the inter-realm trust key that the domains previously exchanged, which is called as an "Inter-realm ticket-granting-ticket/TGT." Then Domain2 verifies the TGT included in the referral, decrypts it with the previously negotiated inter-realm trust key and proceeds further. An inter-realm TGT can be forged. We'll do that in coming posts.

I'll explain the Kerberos process in detail in the next posts when performing kerberoasting.

Anyways, Coming back to the above diagram, let me explain what's happening in it. A client from Domain 1 wants to access the server located in Domain 2. Here is how it happens:
1. A client from Domain1 requests a TGT from the DC1.
2. DC1 responds back with the TGT (encrypted with krbtgt hash)
3. Client shows the TGT and requests a TGS for accessing the server in Domain2.

As DC1 doesn't find the server in current domain and realizes that the TGS needs to be issued by the DC2 (of Domain2) because the server is located in the Domain2. So it responds back to client with the Inter-realm TGT.

4. Client shows the TGT encrypted with Inter-Realm trust key to DC2 in the Domain2 and requests TGS to access the server.
5. DC2 sends back the TGS for Server encrypted with server's account hash
6. Client presents the TGS (encrypted with server's account hash) to the server for access.

Scope of Authentication when establishing Trusts:

When creating trust, it asks for the scope. In this environment, we'll use "*Selective Authentication*" and there will be a jump server that would have access to the server from

other forest. Let me explain the two types of Authentication scopes:-

Forest-wide authentication:- If we use forest-wide authentication, users from the outside forest have the same level of access to resources in the local forest as users who belong to the local forest.

Selective authentication**:-** In case of Selective authentication, you need to manually assign permissions on each computer in the domain as well as the resources to which you want users in the second forest to have access.

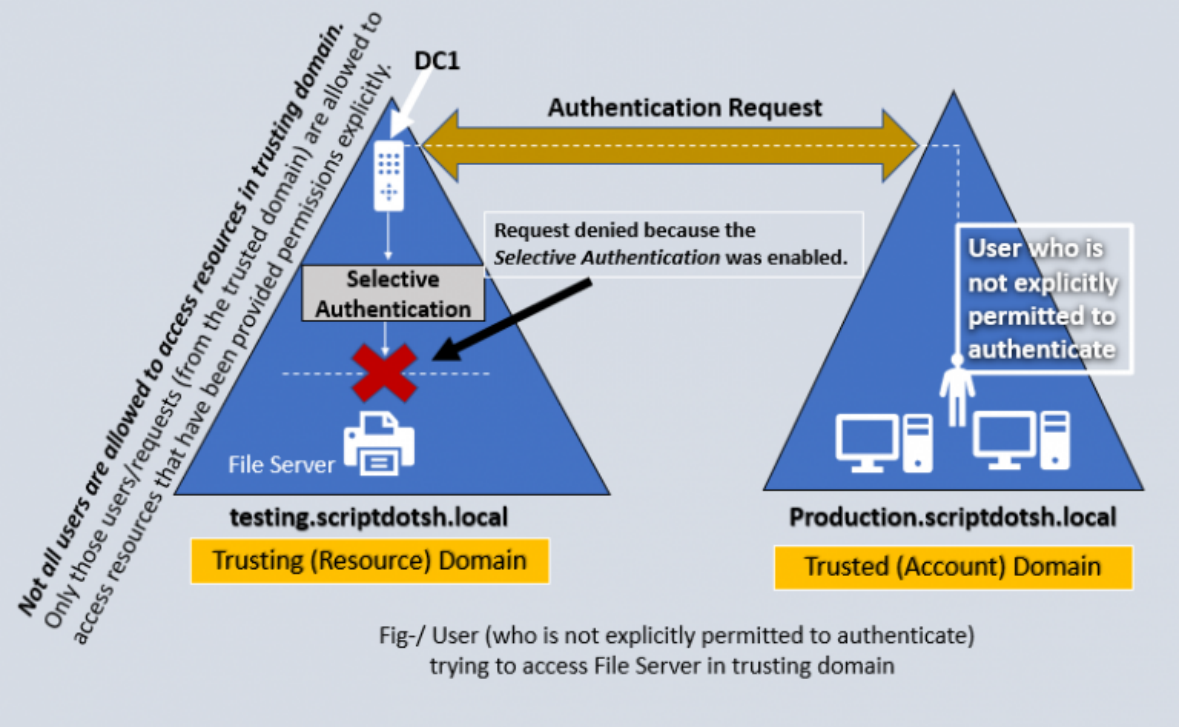
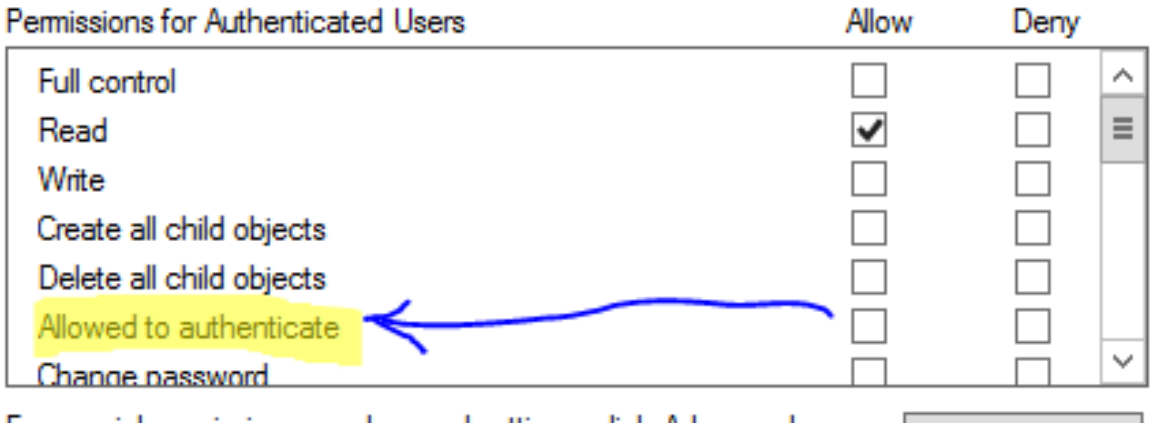


Fig-/ User (who is not explicitly permitted to authenticate) trying to access File Server in trusting domain

To explicitly allow a user to authenticate in this scenario of Selective Authentication, you need to edit an ACE (Access control entry) shown below:



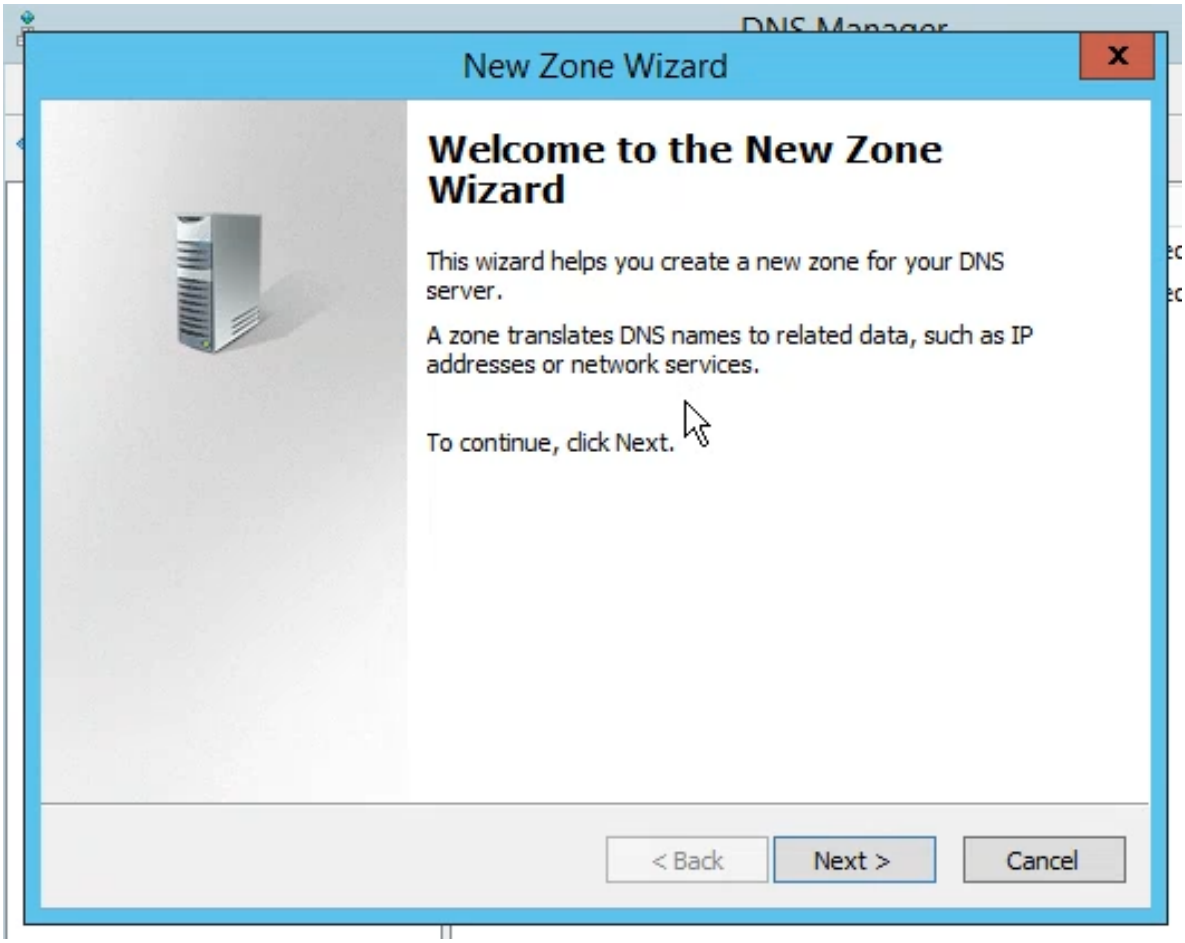
Demonstration

Now we will setup trust between two domains. Let's say we have a domain *"production.scriptdotsh.local"* and an external domain from other forest "*solar.local".*

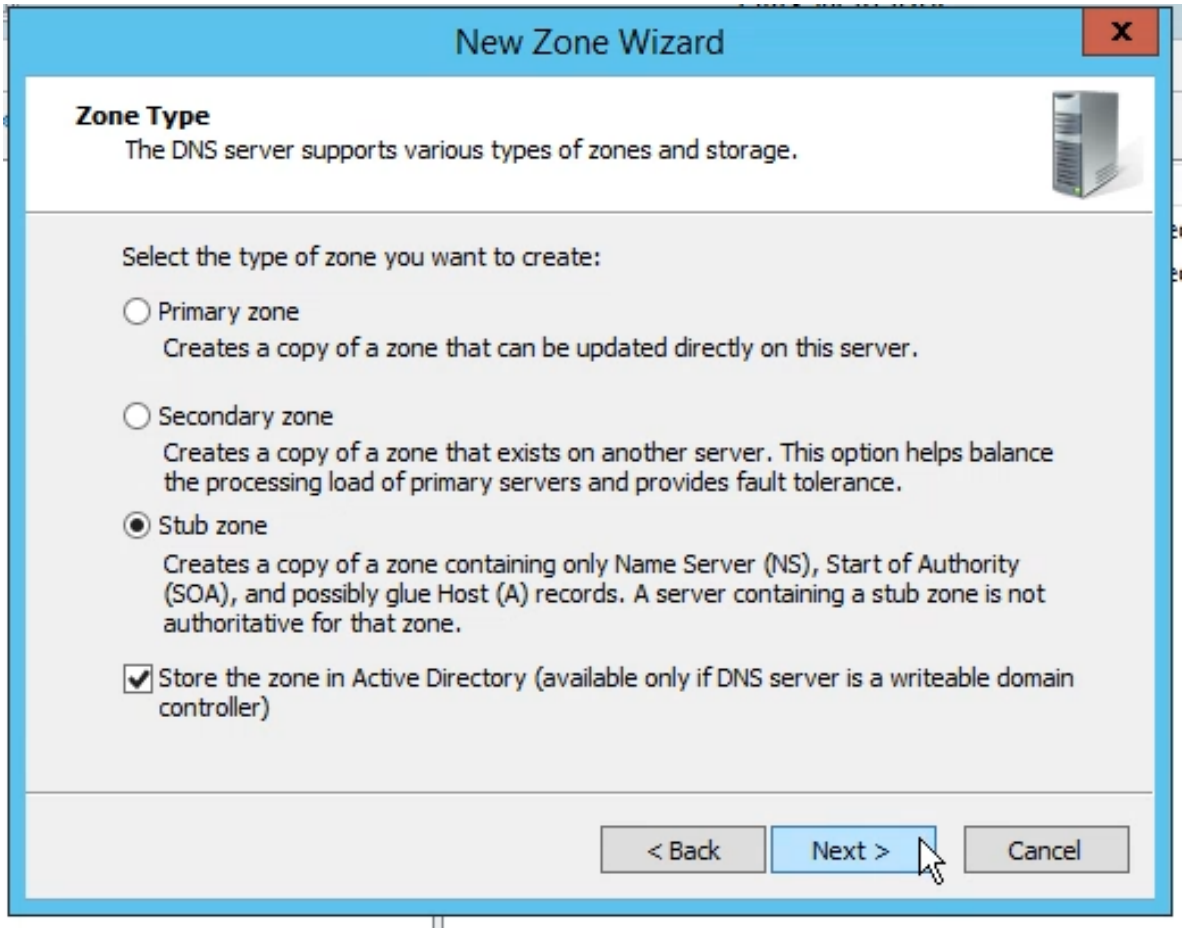
Before creating a cross-forest trust, we need to ensure that we have enough privileges i.e. domain admins at both side. DNS should be configured properly on both sides. Each forest must be able to resolve the DNS name and SRV records contained in the other forest through the use of DNS zones i.e. stub zones, or conditional forwarding (otherwise the trust wizard will fail). Let's do this.

- **Add DNS Stub zone:-**

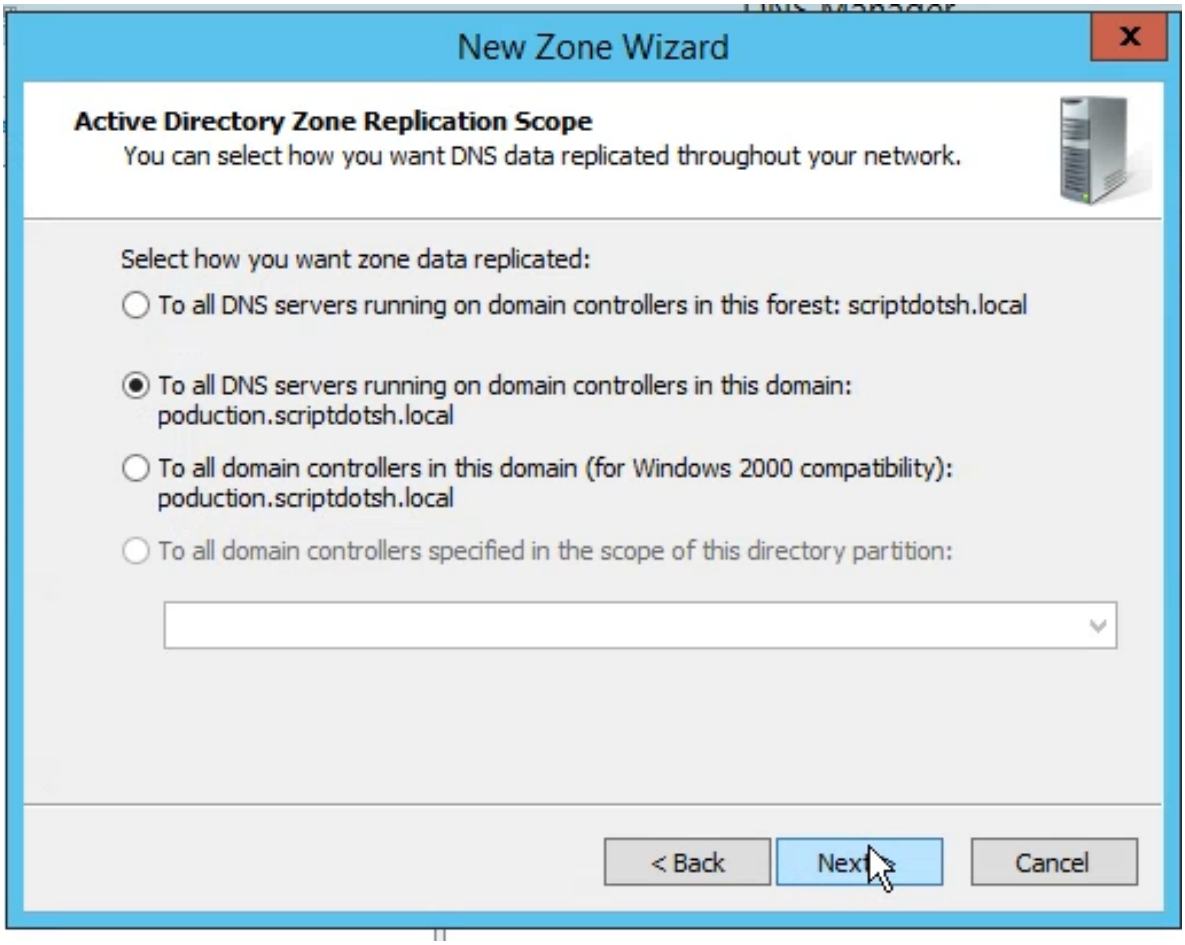
Let's add DNS stub zone. We'll start with the primary site *(production.scriptdotsh.local)* Login into the domain controller and open the *DNS Manager* console. Right-click the *Forward Lookup Zones* folder and choose "*New Zone*".



In the **Zone Type** page select the **Stub zone** radio button then click **Next**.

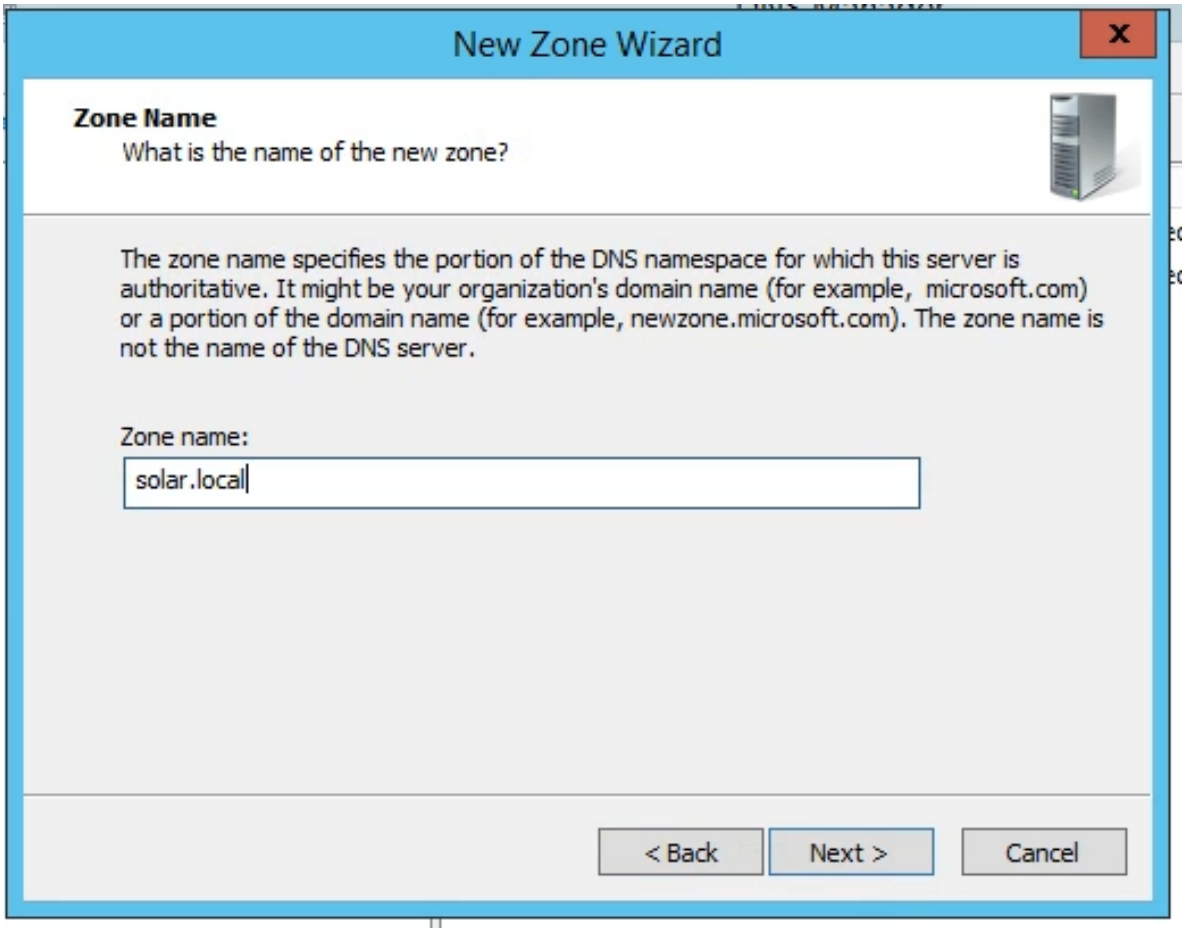


Leave the defaults here and continue the wizard.

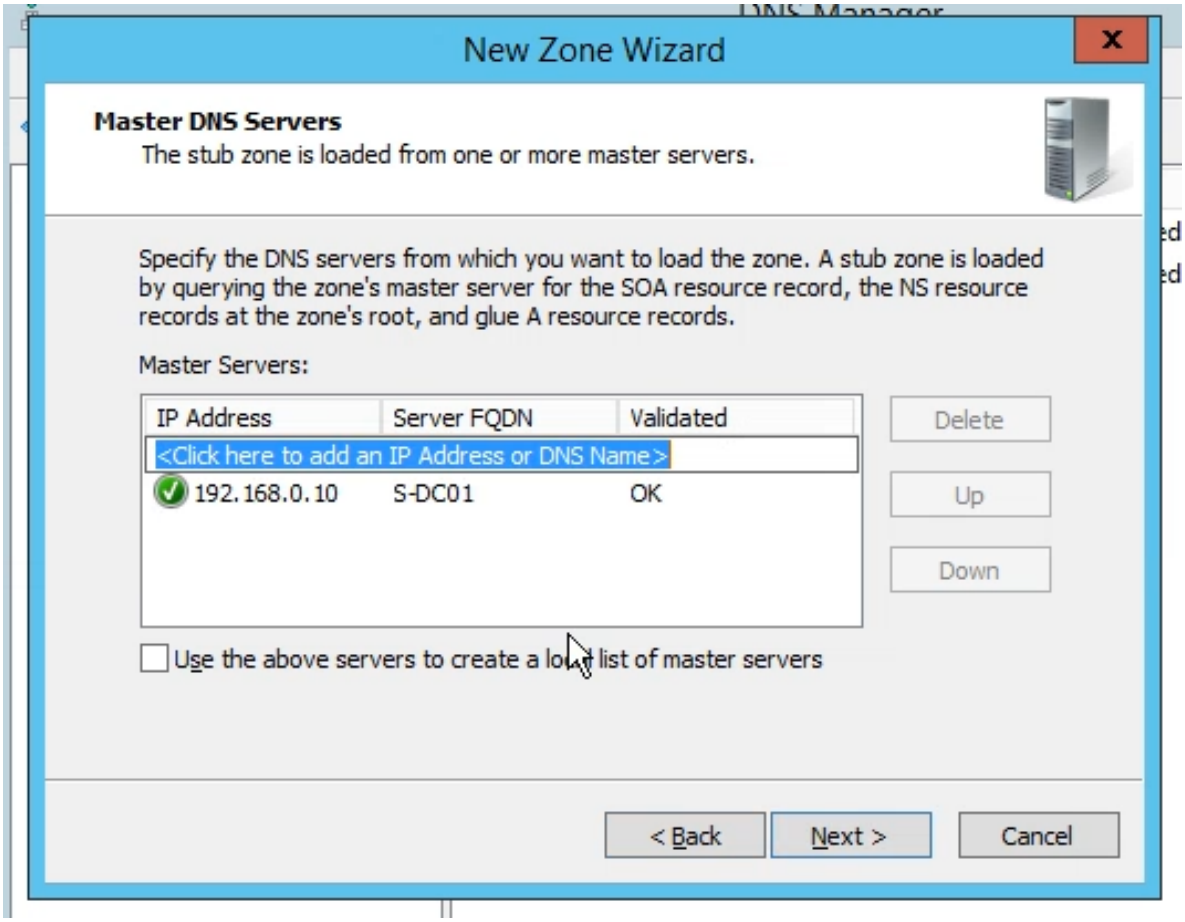


The zone name that we need to type in this box needs to match the name of the forest in the other site. In our case, it is **solar.local**.

Type it in then continue the wizard.

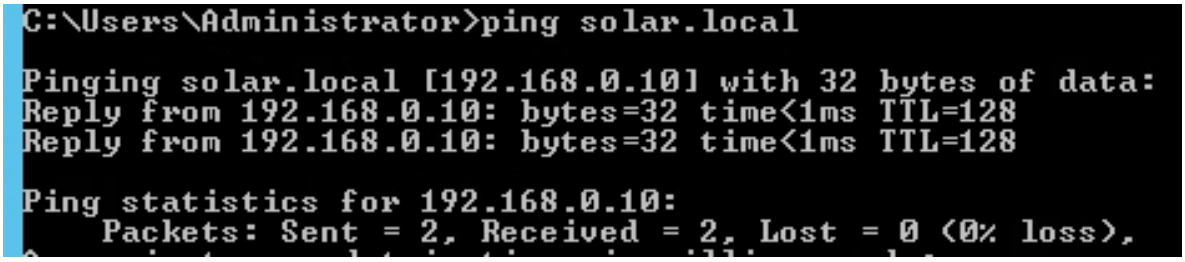


In this section, provide the IP address of that DNS server or domain controller of the other domain. Click **Next** when you're done.



Click **Finish** to create the zone.

In the **solar.local** site, follow the same process in its DNS server to add the stub zone for scriptdotsh. After adding it, the connection should work fine.

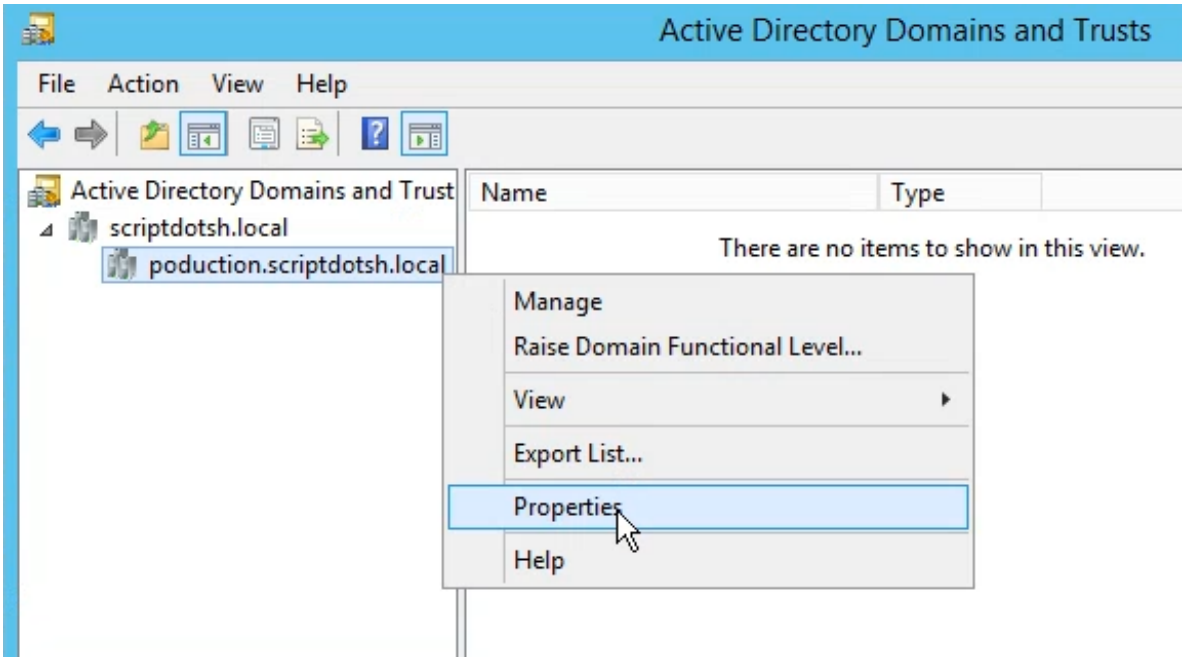


Now, we're done with the DNS settings, the next step will be to create the trust between the two forests.

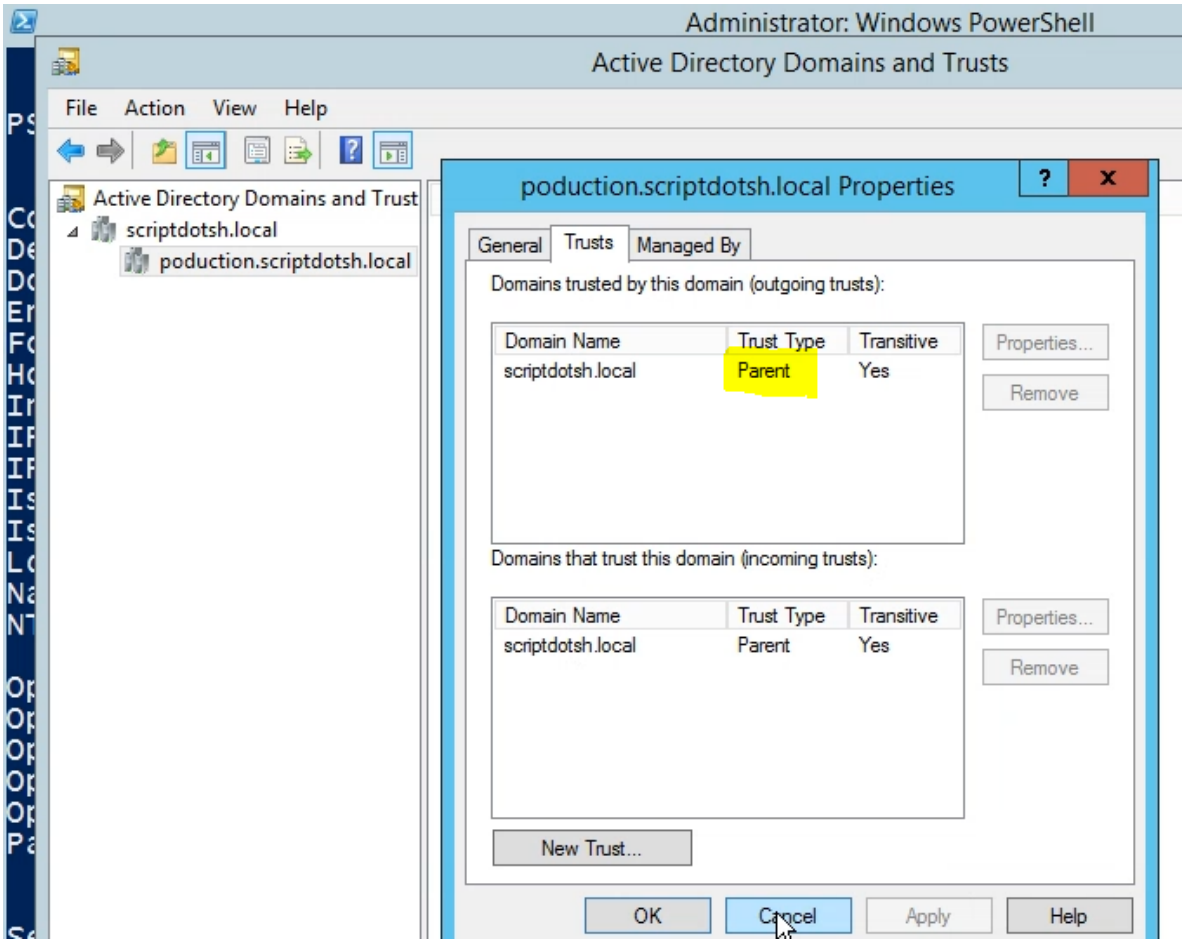
Creation of Trust:-

To create trusts in Active Directory, open Active Directory Domain and Trusts from administrative tools.

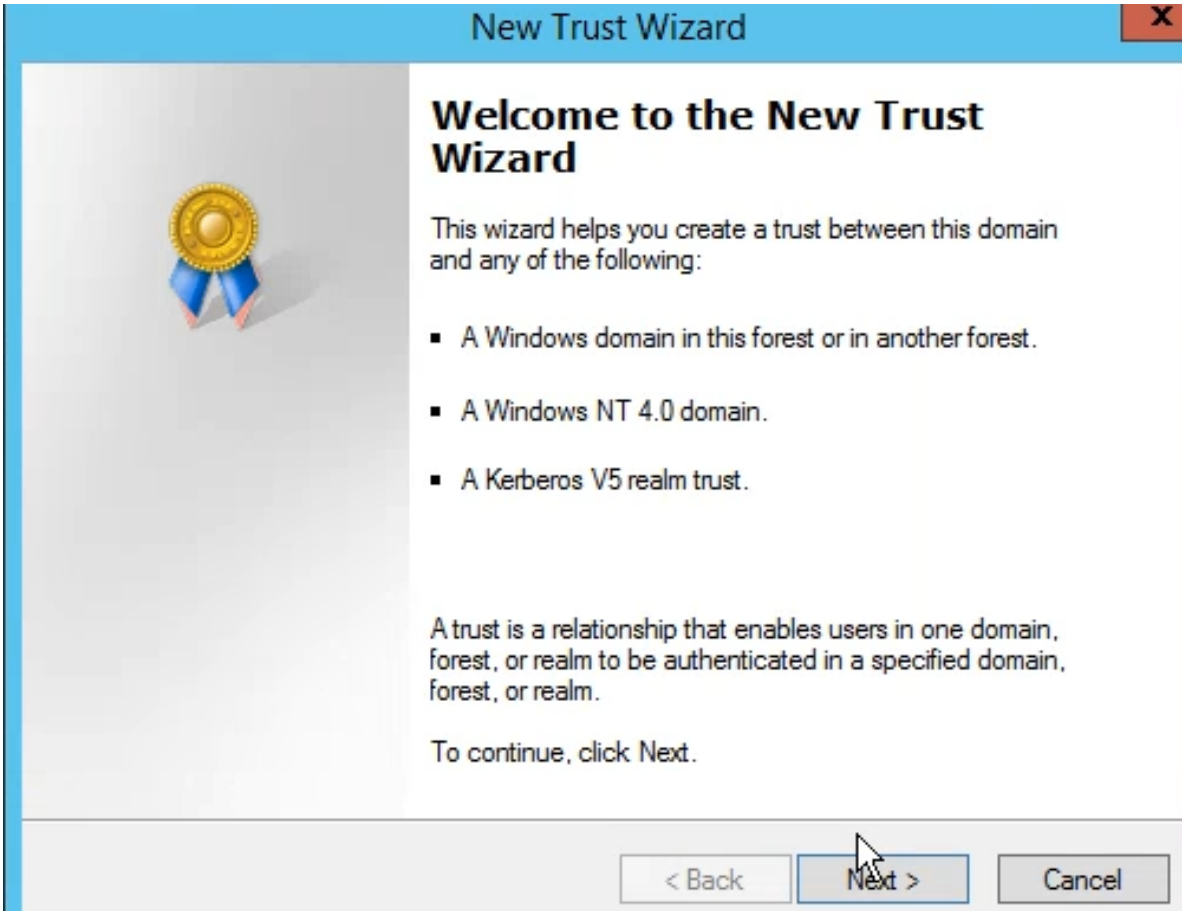
Right click the domain name and choose **properties**



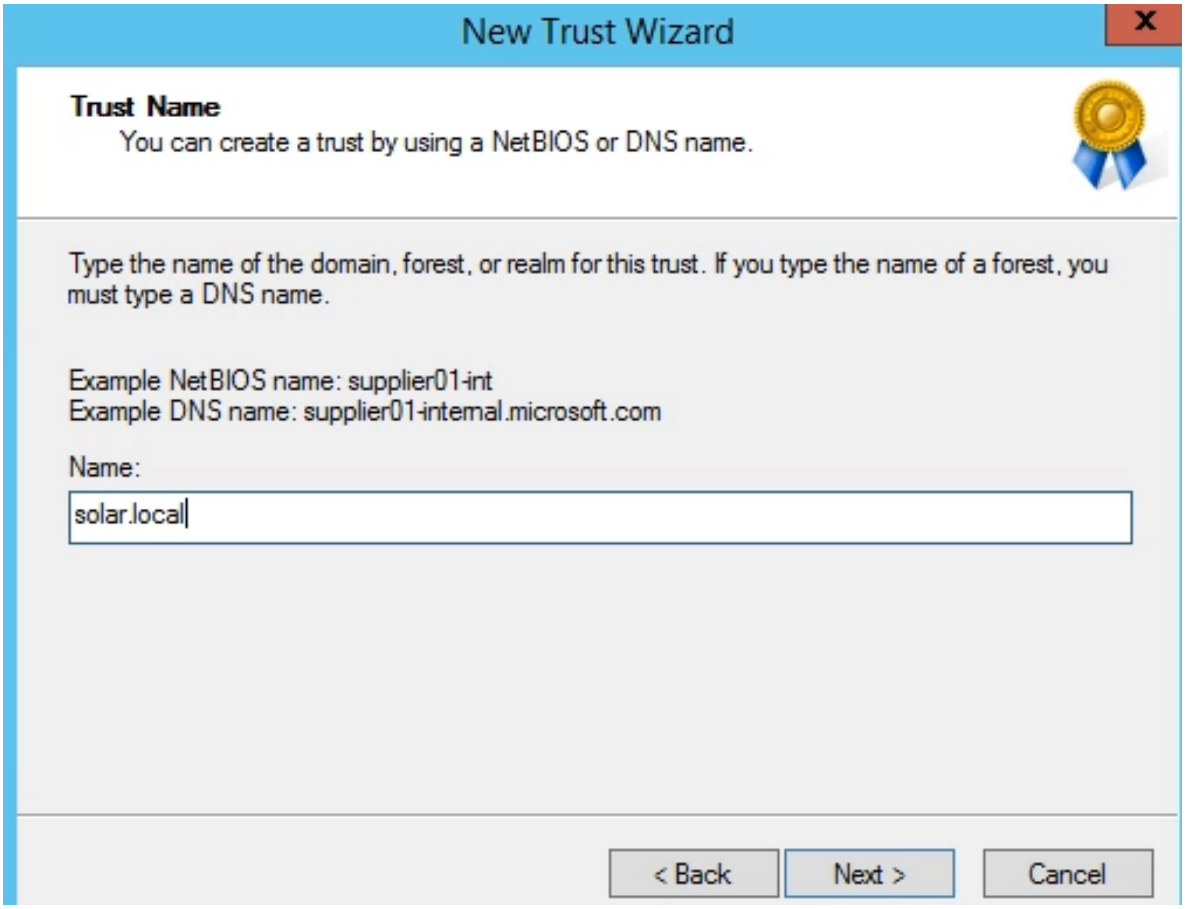
Go to Trusts tab. This shows a list of all domains with the trust types. As you can see, I already have a trust displaying here. There is a parent-child trust between scriptdotsh.local and its child production.scriptdotsh.local. This trust was automatically created when I added the domain (production.scriptdotsh.local) as a child domain into the forest.



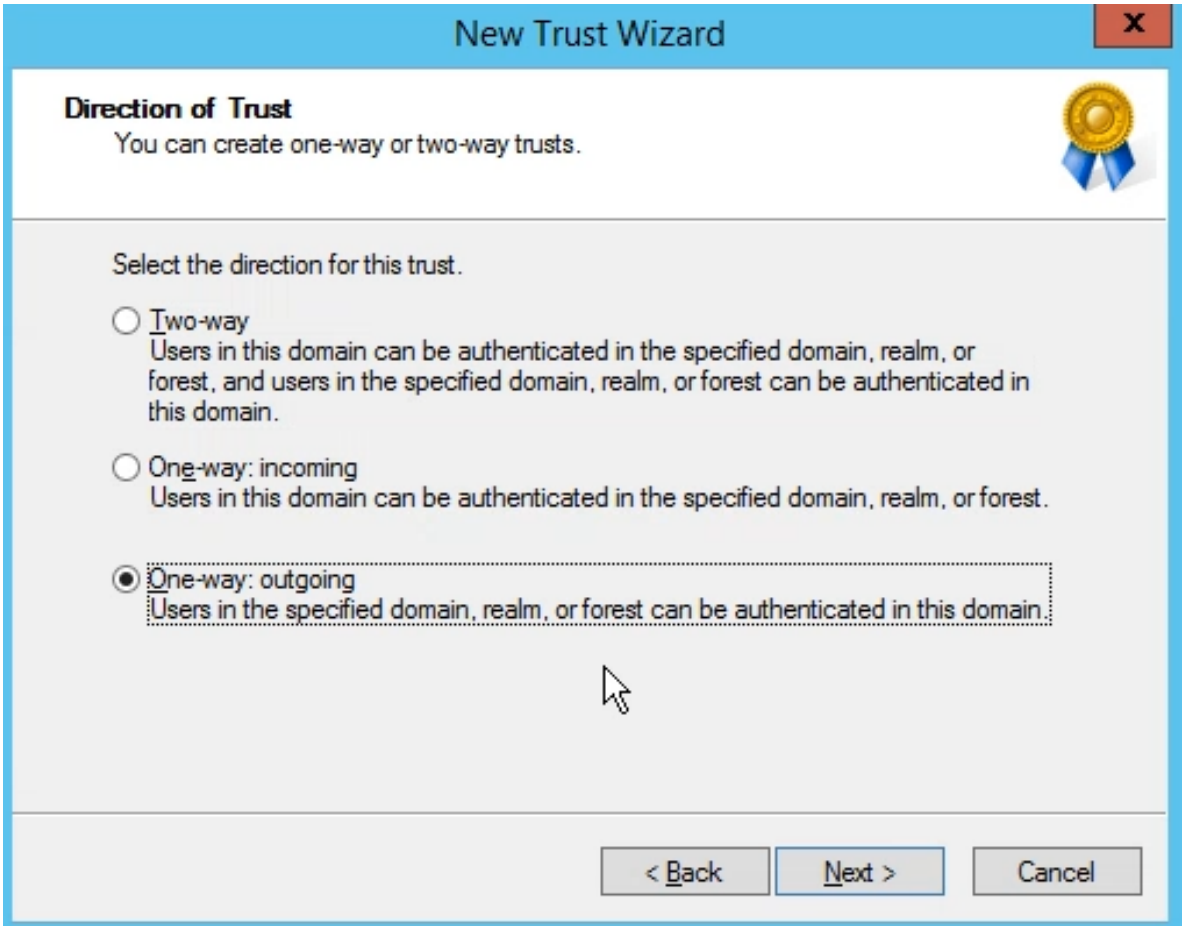
To create a new trust, click at the bottom of the trust tab select the option, “new trust,” to launch the trust wizard. Click next to skip the welcome screen.



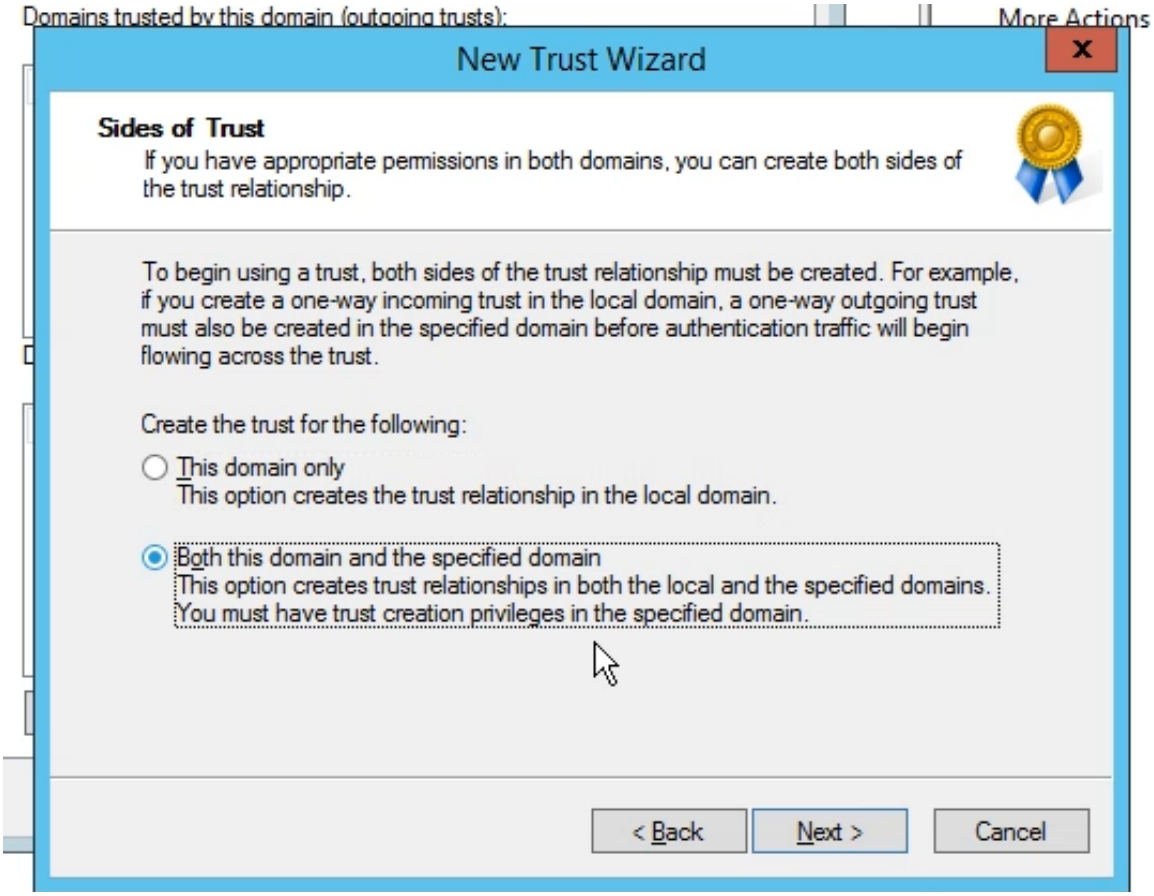
Here we need to type the domain name or forest name with which we need to create the trust. The name must match the DNS stub zone name created earlier, which in our case is **solar.local**.



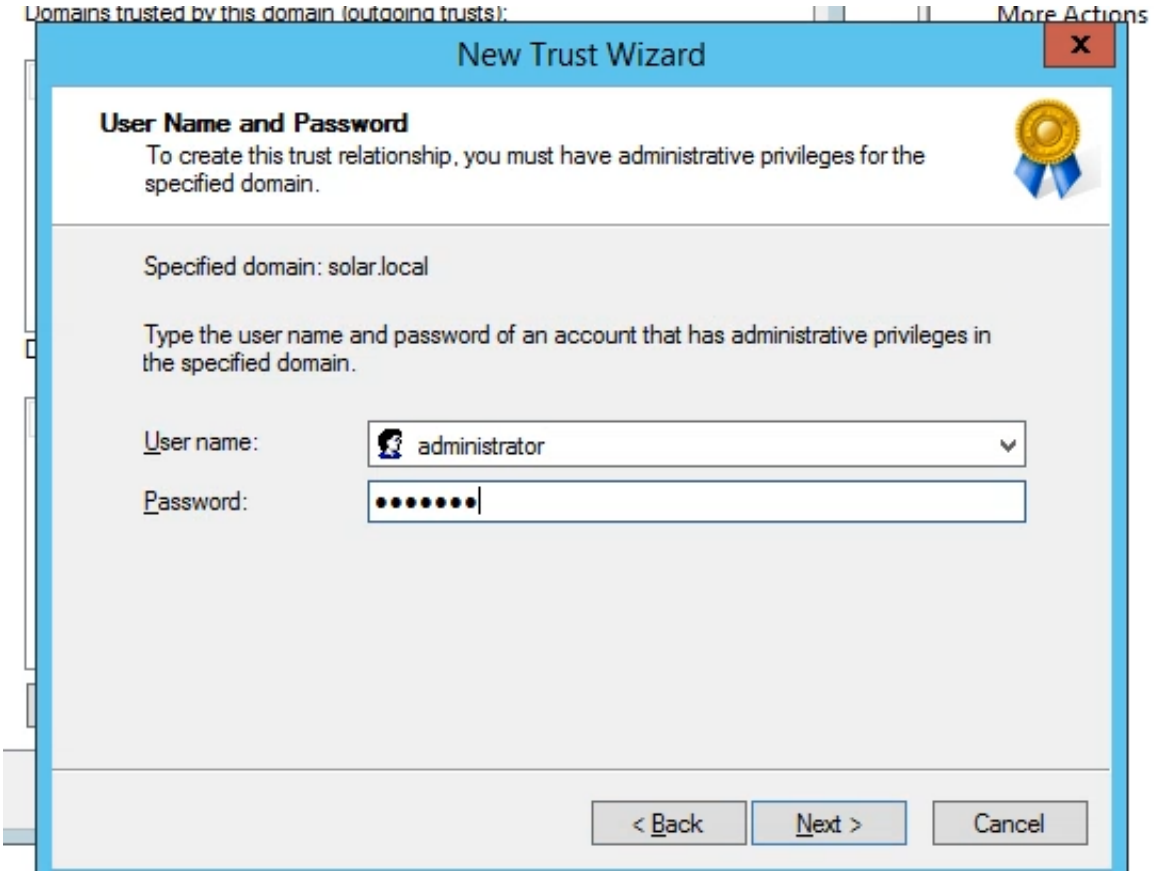
Select the one way outgoing trust and click next



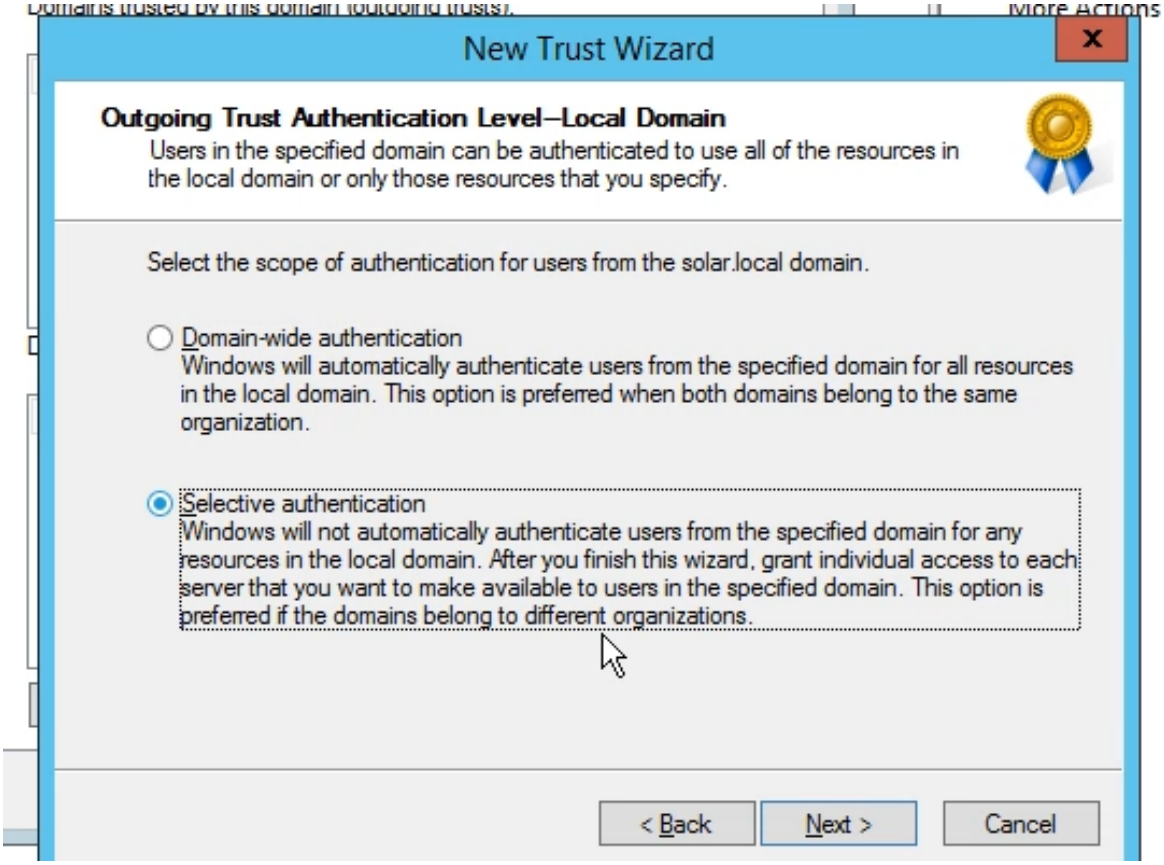
Now, choose to create trust on both sides.



Enter credentials that has rights to create trust in the specified domain (admin of solar.local):



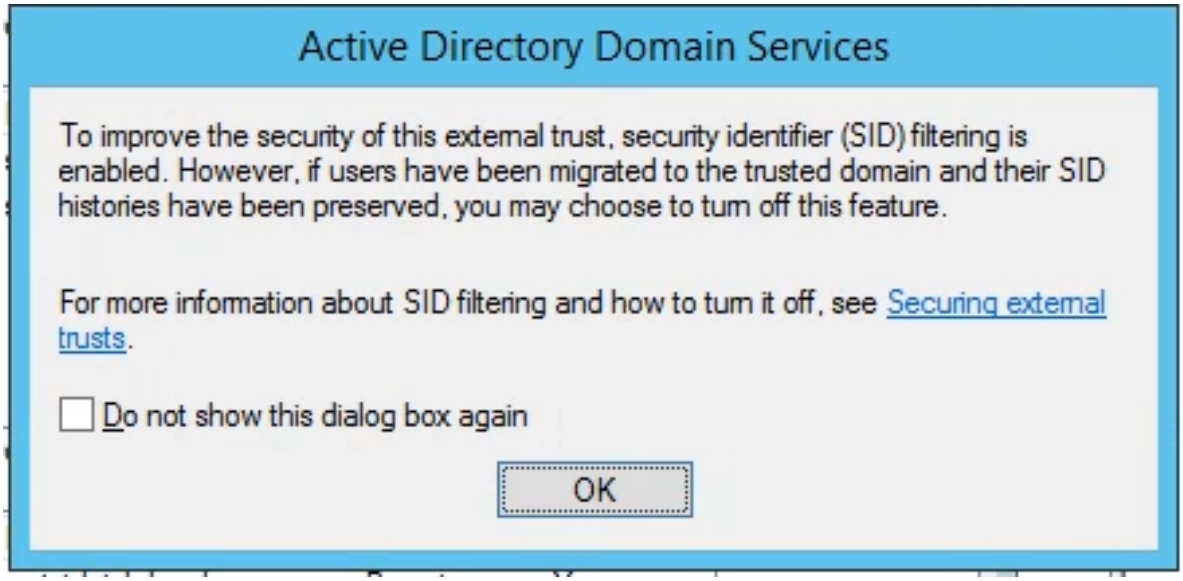
Click Next and select the authentication type. Choose **“Selective Authentication”**



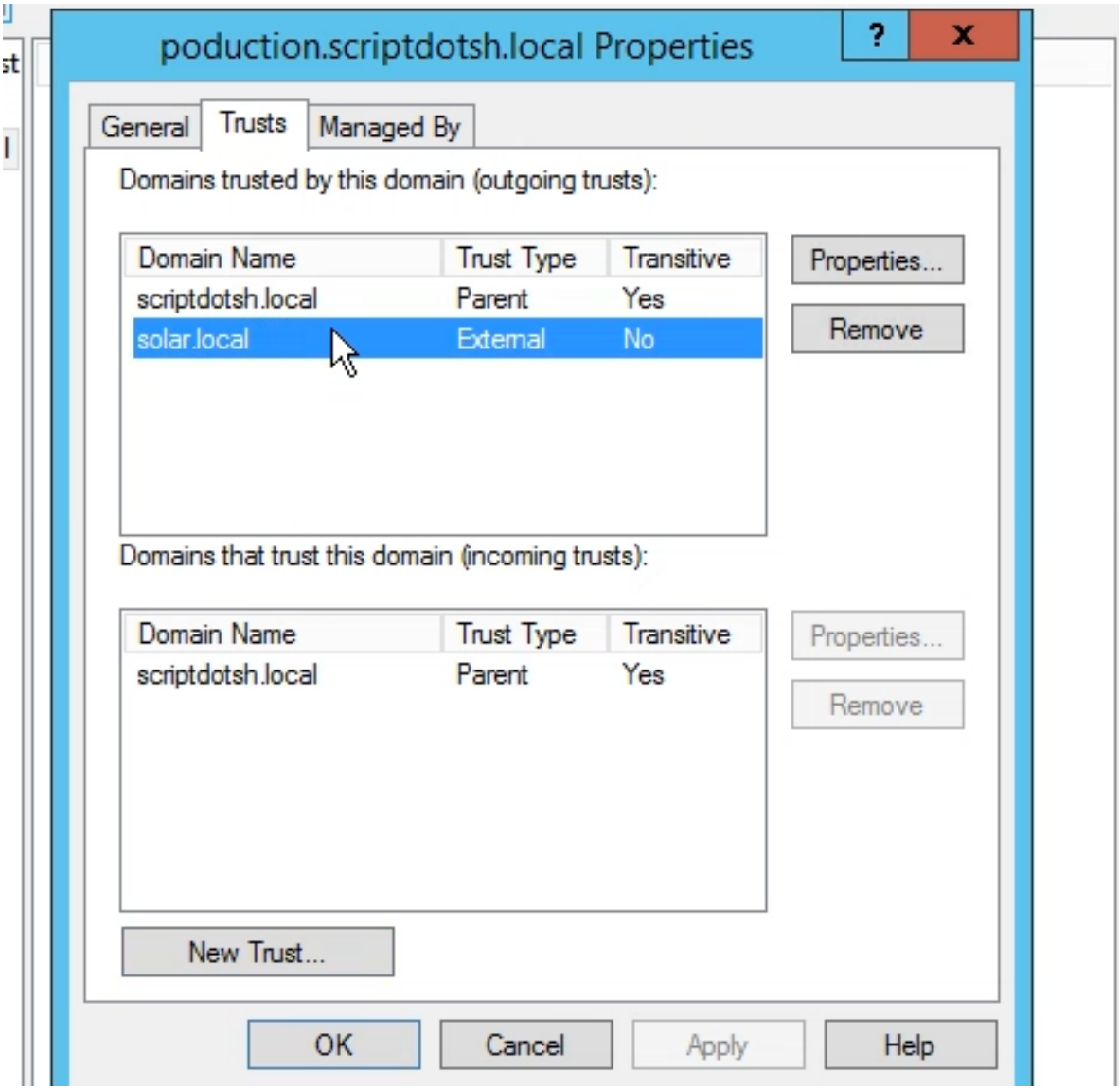
Now, it will not automatically authenticate the users. You need to specify the access manually. Click next and confirm the trust to finish the process.

You’ll get the dialog box saying that SID filtering is enabled. Click OK.

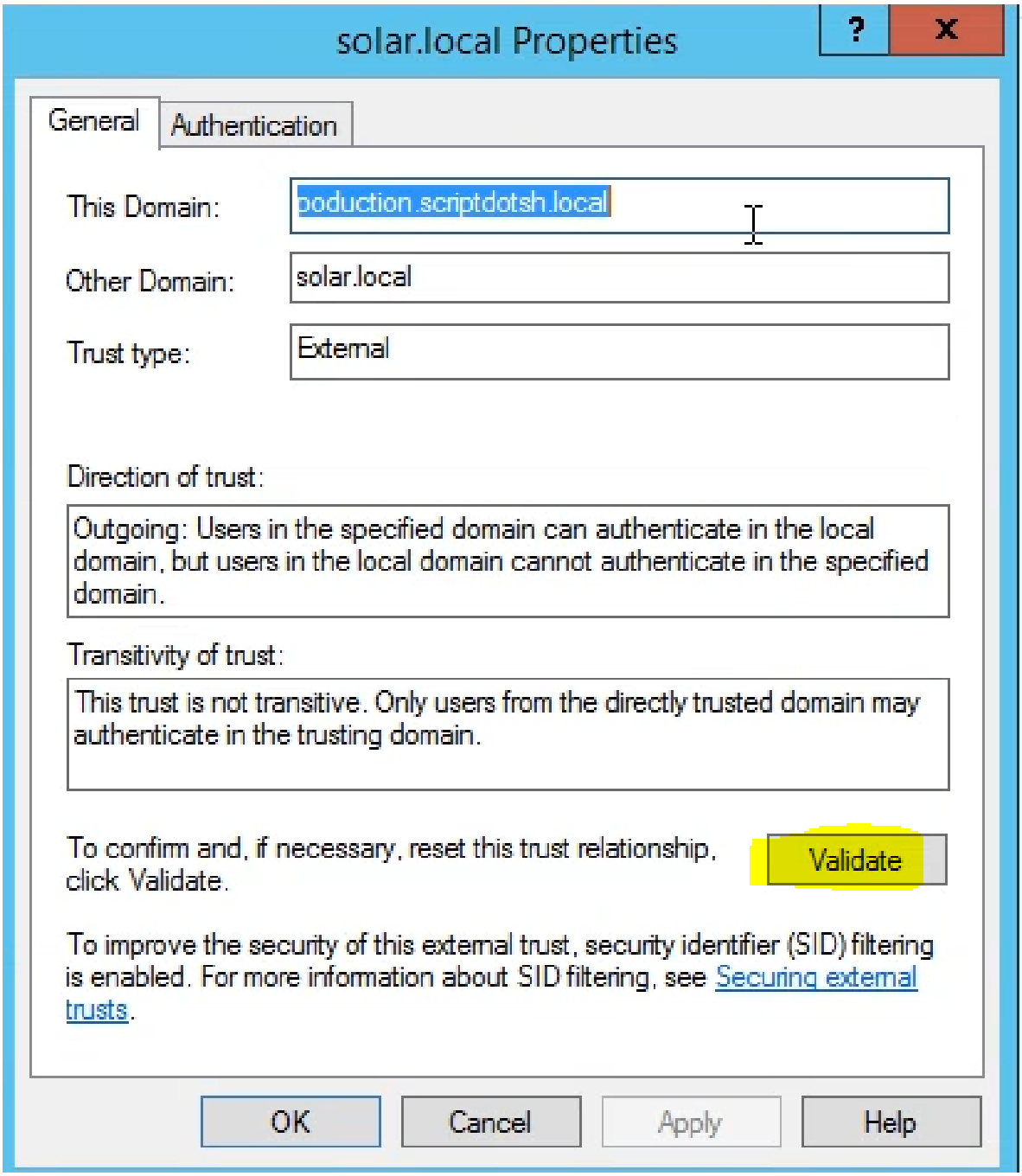
Note:- **SID filtering is enabled by default on all inter-forest trusts.** Microsoft considers security boundary as Forest and not the domain. We can abuse SID history attribute to do the child to root domain privilege escalation i.e. Domain admin to Enterprise Admin on forest root.



Now if you see, an external trust has been created.



Click properties of this trust and choose validate option to verify the trust.



I hope you've learnt how to create trusts in Active Directory. You can try to create trusts by yourself and ask me anything regarding this post or any other issues.

In the coming posts that I'm writing right now, I'll start with the domain enumeration techniques in the environment with demonstration, lateral movement and privilege escalation techniques at the domain level, enumerate and exploit trust relationships, forge the inter-realm trust key and retrieve the **krbtgt** hash of that domain etc. Stay tuned for upcoming blogs :)

Winsaaf Man

Security Engineer | Security Analytics using #ELK | #Pentesting AD | #ActiveDirectory Attacks | Blogger | Twitter ID is @WinsaafMan

Tags: Active Directory, Pentesting Active Directory, Windows AD

Written by

Winsaaf Man

Security Engineer | Security Analytics using #ELK | #Pentesting AD | #ActiveDirectory Attacks | Blogger | Twitter ID is @WinsaafMan

View all posts by Winsaaf Man

2 COMMENTS

NotImportant

February 21, 2019 *at* 8:10 *pm*

Hi,

Thanks for your guide. I do however find this part very confusing. Suddenly you write “Let’s say we have a domain “production.scriptdotsh.local” and an external domain from other forest “solar.local”.”. When did you create the first one and on which machine? On which machine did you create the second one? Which machine is the DHCP? Which machine is the DNS server? How many machines have you added so far? I have only one DC/DNS/DHCP and one client since that is how I understood your guide. But that does not seem to fit your steps in this part of the guide…

Winsaaf Man

February 24, 2019 at 4:33 pm

Hi mate, I just showed how to setup a domain controller. You could create another one in the similar manner. This post was to make the readers familiar with the trust and how to setup trust. If you want to learn in detail about the setup part of the domain controllers and adding additional DCs, please visit here.

bitcoin

We don't get paid for writing these blogs. If you enjoy reading our blogposts and would like to support our work, you can buy us a coffee by donating here:
14mN2S5JYmy98KDFWkxC33Urhmu8NvHP3X
Or scan the **QR Code** here

RECENT POSTS

May 13, 2019

Understanding Windows OS Architecture – Theory

May 4, 2019

WinDBG Configuration