

Trust between two forests (Using DNS stub zone):

NOTE: Please note that these steps were tried between two forests with root domain in Windows 2012R2 DC and the Forest functional level used is 2012.

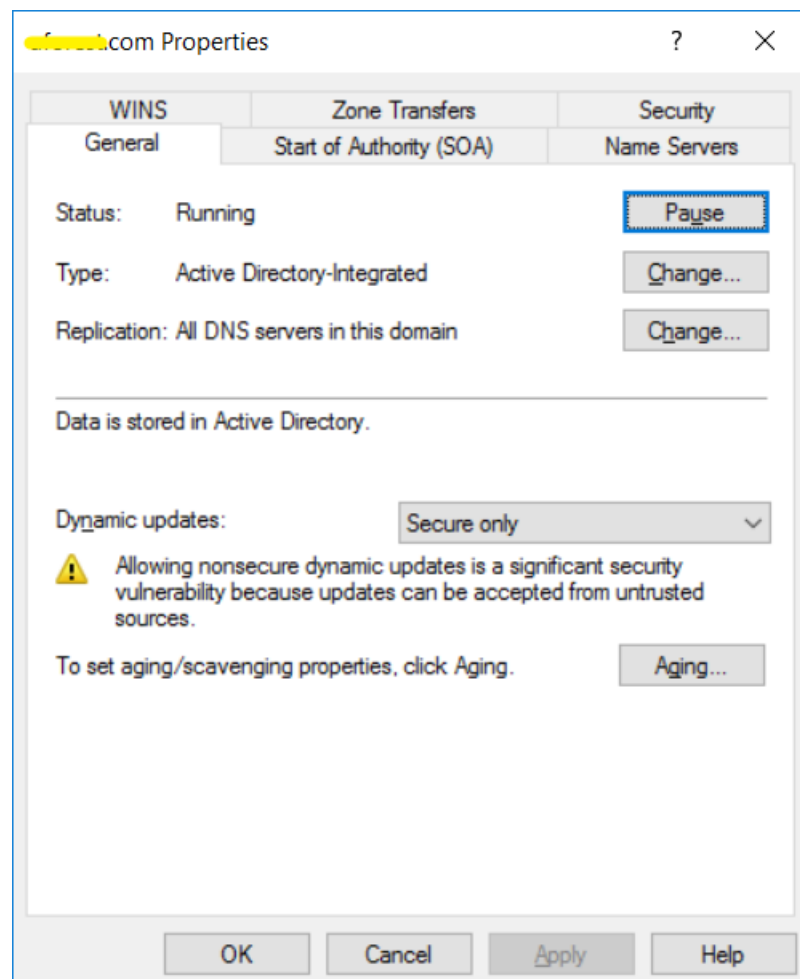
For reference, the forests are named as Forest A and Forest B.

Configure the source DNS server to allow for zone transfers

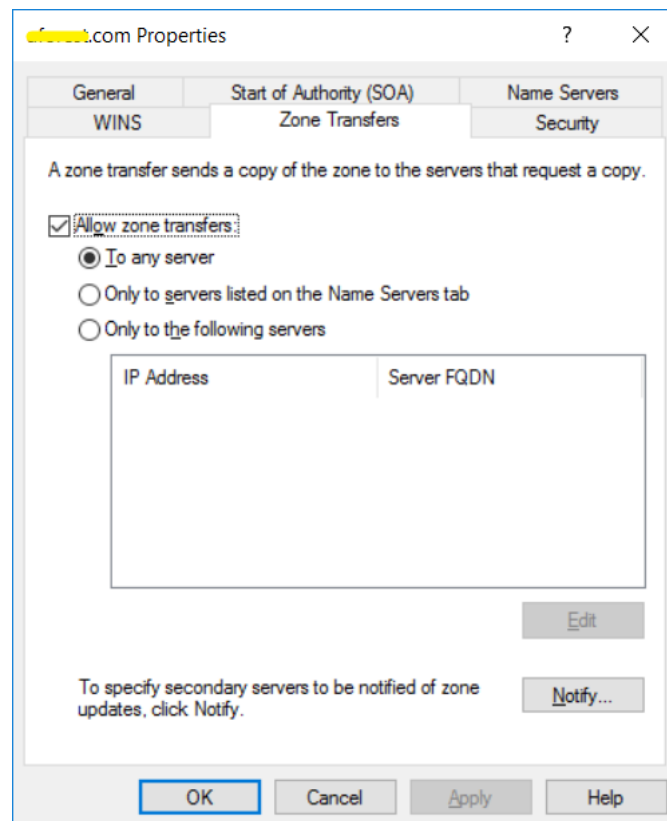
(These steps will be accomplished on both DNS Servers).

To forward lookup zone properties,

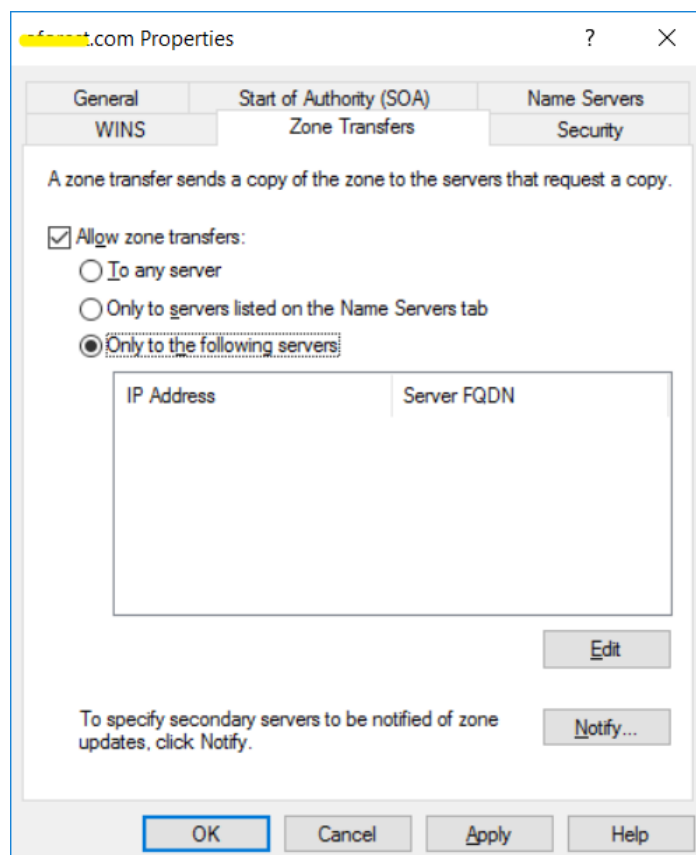
1. Launch the **DNS console**.
2. Click on the **Forward Look Zone** that you desire so configure.
3. Click on **Properties**.



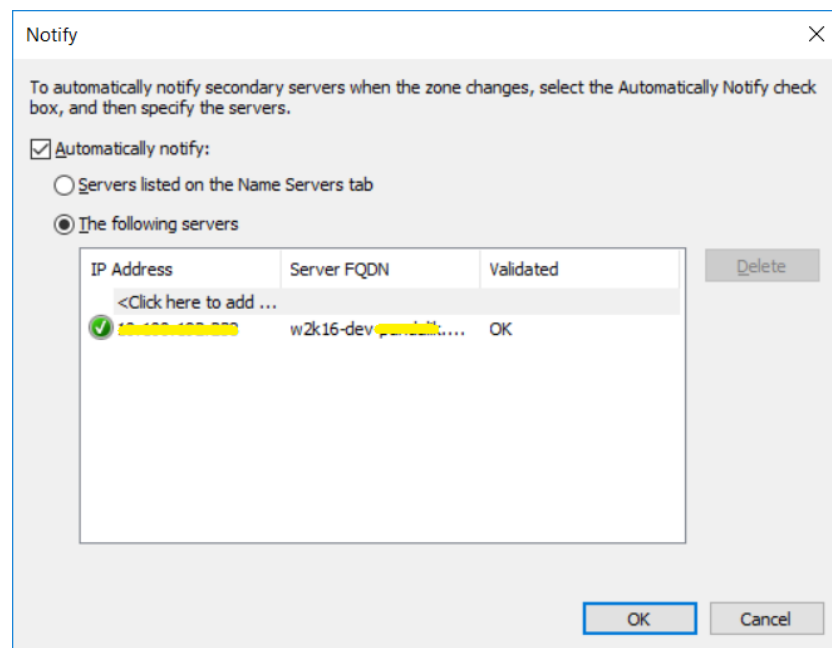
4. Select the **Zone Transfers** tab.



5. Select "**Only to the following servers**".



6. Click on **Automatically notify** and add the IP of the Forest B. Make sure the IP is resolved and the green check mark appears.
7. Click **OK**.



Configure a Stub Zone

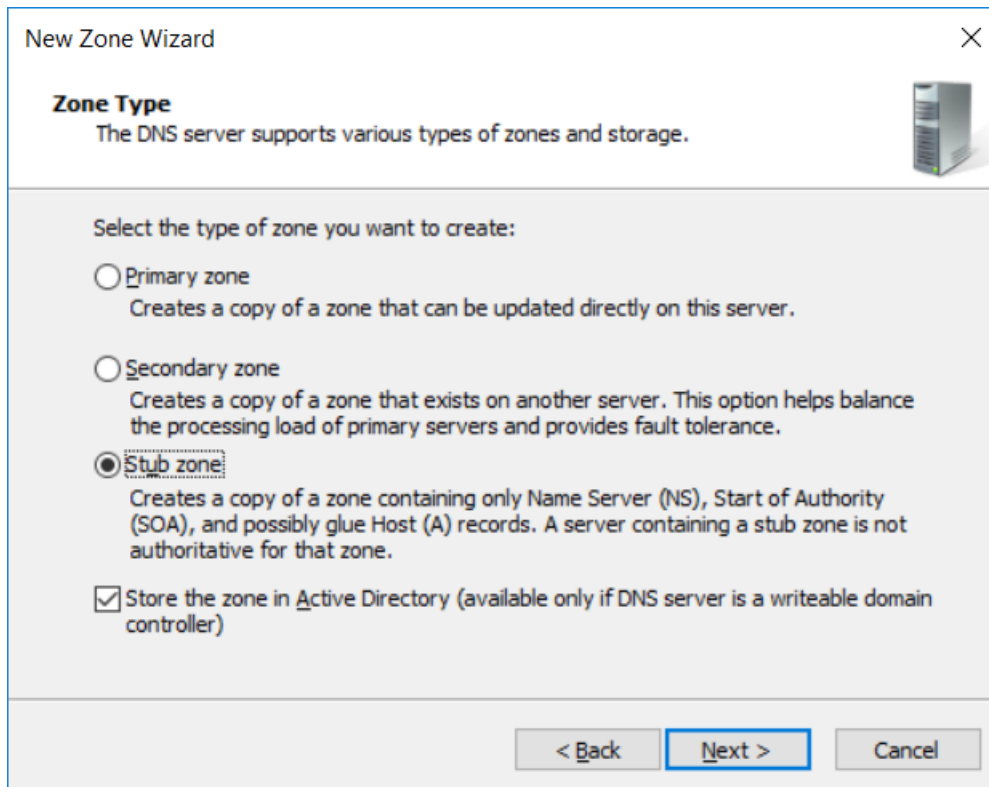
(These steps will be accomplished in both DNS servers).

To create a new forward lookup zone for Forest B in Forest A,

1. Launch the **DNS Console**.
2. Click on **Forward Lookup Zone** and choose **New Zone**.
3. In the **Welcome to the New Zone Wizard**, click **Next**.



- Click on **Next** and select the Zone type.



New Zone Wizard

Zone Type
The DNS server supports various types of zones and storage.

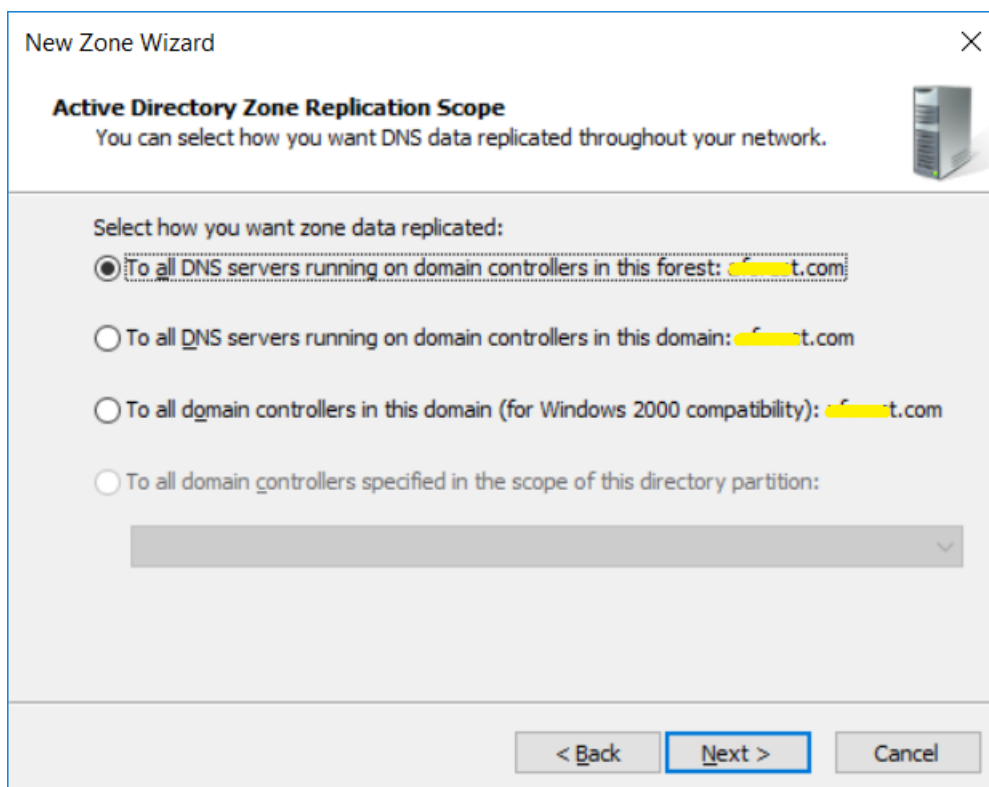
Select the type of zone you want to create:

- Primary zone
Creates a copy of a zone that can be updated directly on this server.
- Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
- Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

< Back Next > Cancel

- In the next step, select "To all DNS servers running on domain controller in this forest".



New Zone Wizard

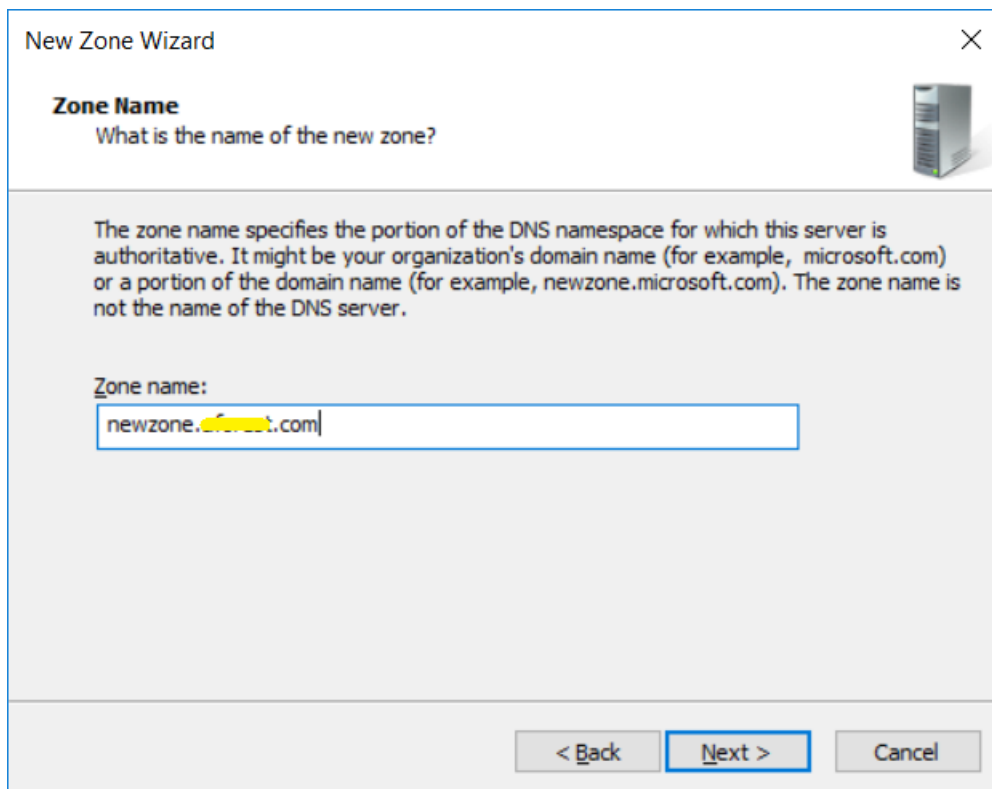
Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

- To all DNS servers running on domain controllers in this forest:
- To all DNS servers running on domain controllers in this domain:
- To all domain controllers in this domain (for Windows 2000 compatibility):
- To all domain controllers specified in the scope of this directory partition:

< Back Next > Cancel

- On the **Zone Name** page, enter the desired zone to transfer from, click **Next**.



New Zone Wizard

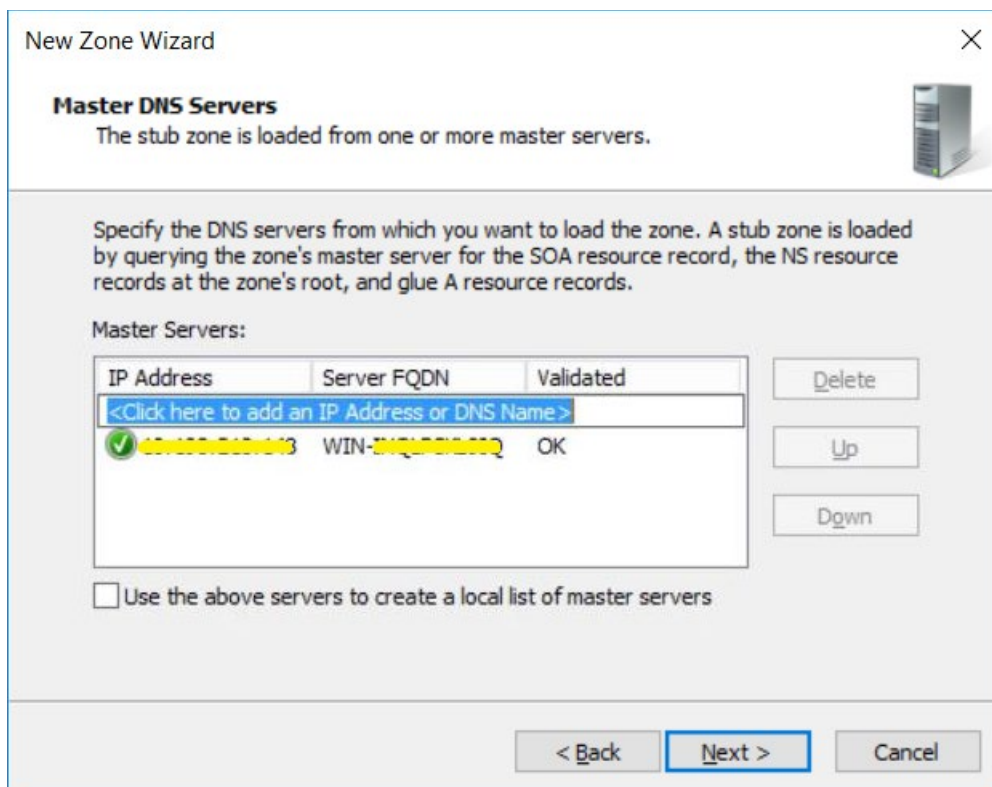
Zone Name
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:
newzone.192.168.1.100.com

< Back Next > Cancel

- Add the IP of Forest B DC and hit **Enter**. Make sure the IP is resolved.



New Zone Wizard

Master DNS Servers
The stub zone is loaded from one or more master servers.

Specify the DNS servers from which you want to load the zone. A stub zone is loaded by querying the zone's master server for the SOA resource record, the NS resource records at the zone's root, and glue A resource records.

Master Servers:

IP Address	Server FQDN	Validated
<Click here to add an IP Address or DNS Name>		
192.168.1.100	WIN-192.168.1.100	OK

Use the above servers to create a local list of master servers

Delete
Up
Down

< Back Next > Cancel

- Click **Finish** and perform the same steps in Forest B DNS for Forest A.

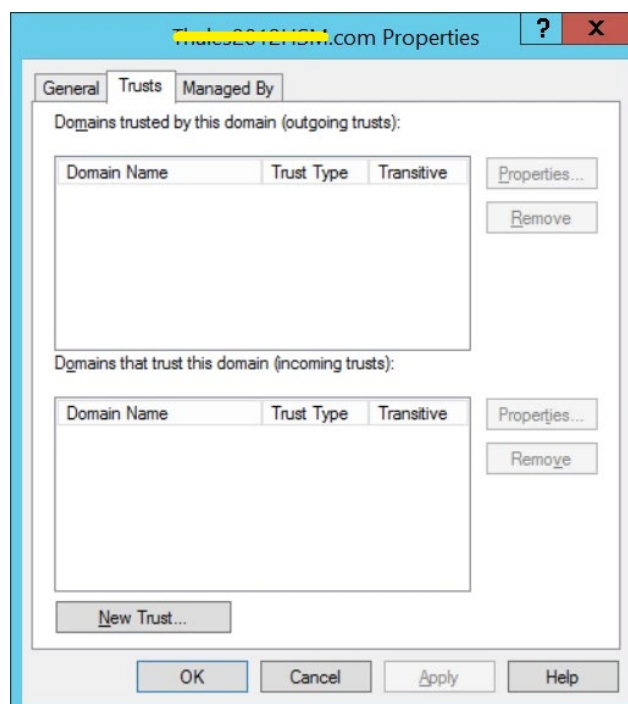


NOTE: nslookup should work from Forest A to Forest B and vice-versa without adding IPs of the domain in Host file.

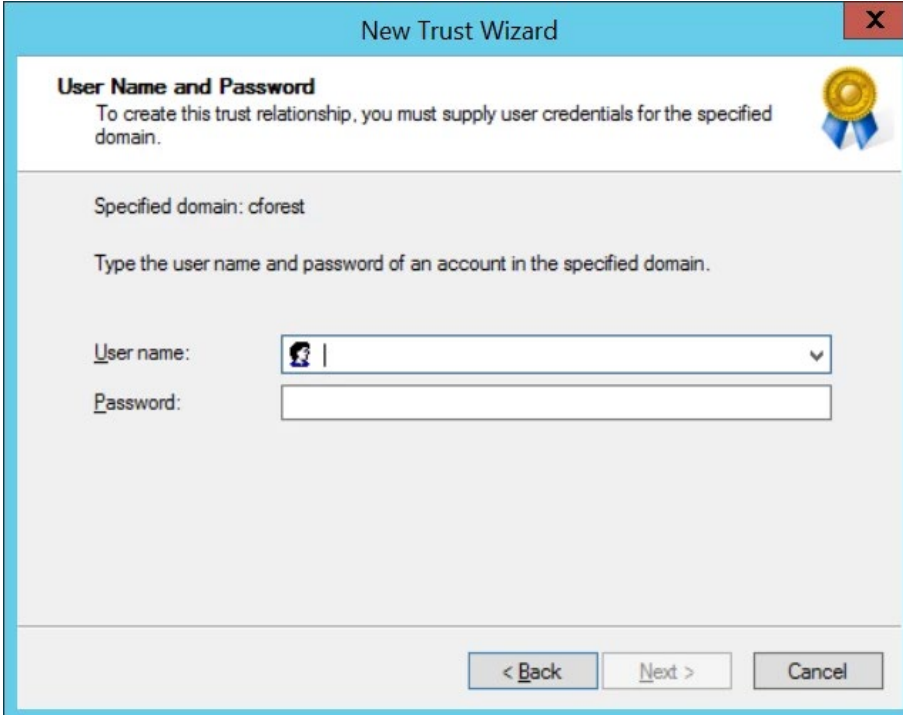
Create a cross-forest trust

For Active directory domains and trust,

- Go to property of root domain in Forest A. Navigate to **Trusts** tab and add a new trust.



2. Enter NetBIOS name of Forest B, on the next screen and enter the admin credentials for Forest B.



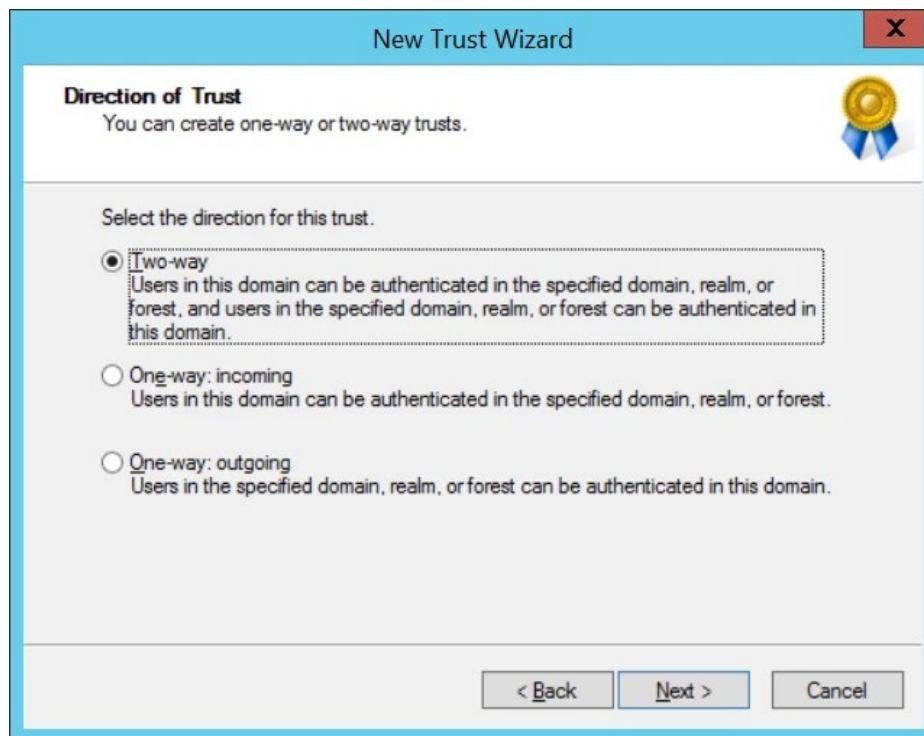
The screenshot shows the 'New Trust Wizard' window, step 2: 'User Name and Password'. The title bar reads 'New Trust Wizard' with a close button (X). The main heading is 'User Name and Password' with a gold medal icon. Below the heading, it says: 'To create this trust relationship, you must supply user credentials for the specified domain.' The 'Specified domain' is 'cforest'. The instruction is: 'Type the user name and password of an account in the specified domain.' There are two input fields: 'User name:' with a dropdown menu showing a user icon and a vertical bar, and 'Password:' with an empty text box. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

3. Select the **Forest trust** for trust type.

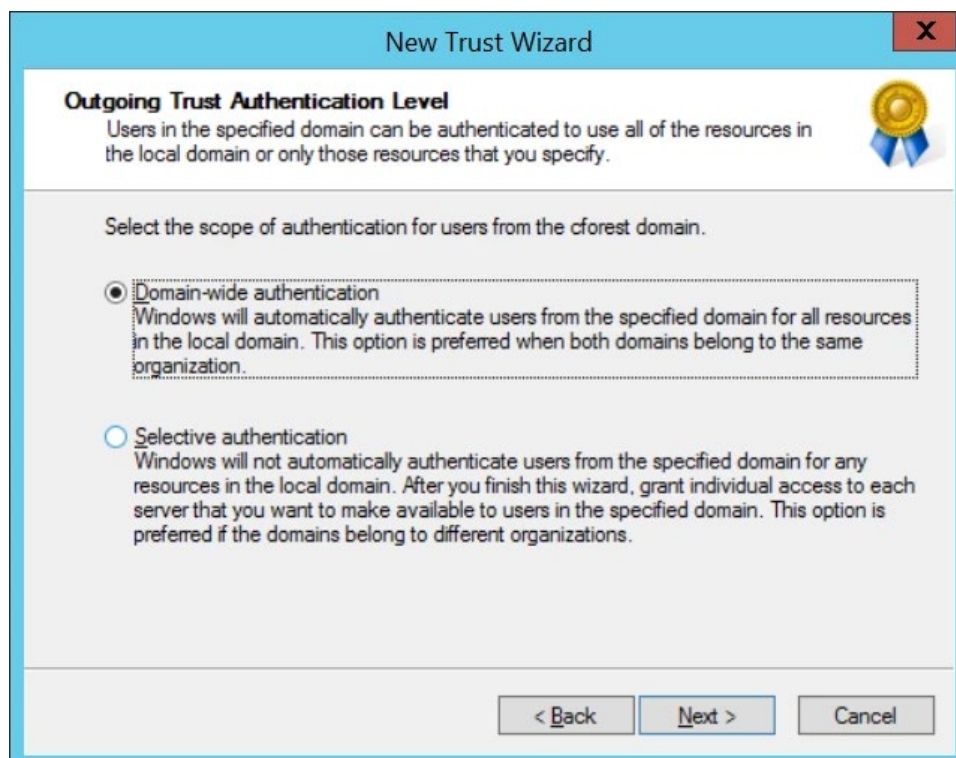


The screenshot shows the 'New Trust Wizard' window, step 3: 'Trust Type'. The title bar reads 'New Trust Wizard' with a close button (X). The main heading is 'Trust Type' with a handshake icon. Below the heading, it says: 'This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.' The instruction is: 'Select the type of trust you want to create.' There are two radio button options: 'External trust' (unselected) and 'Forest trust' (selected). The 'Forest trust' option is enclosed in a dashed box. Below the options, there are three buttons: '< Back', 'Next >', and 'Cancel'.

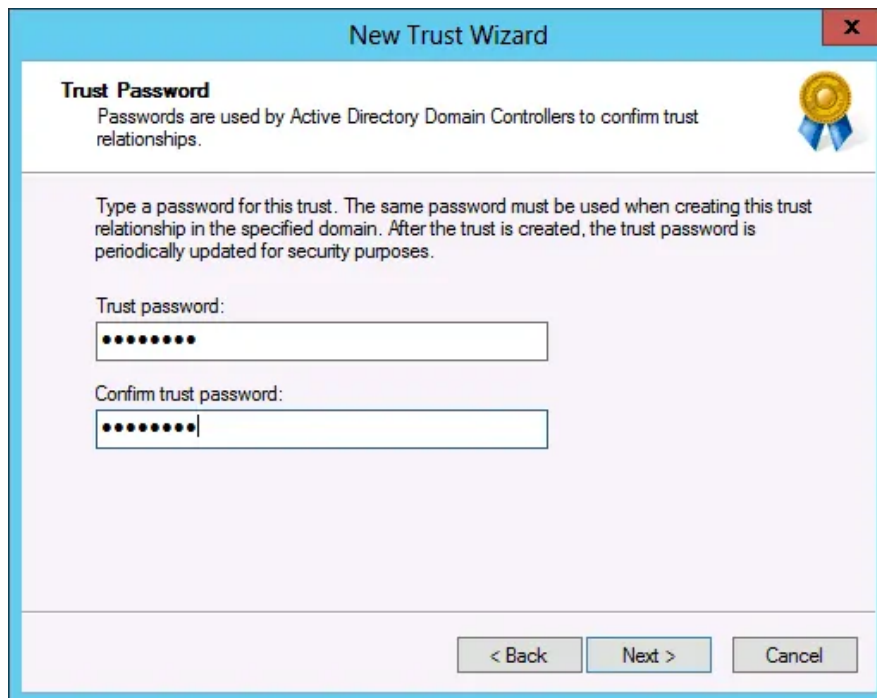
4. Select the **Two-way** direction for this trust.



5. For Outgoing Trust Authentication Level, select **Domain-wide authentication**.



6. Provide a trust password. This is required for creating the trust in Forest B.
7. Proceed with the wizard and complete it.



The screenshot shows a Windows dialog box titled "New Trust Wizard" with a close button (X) in the top right corner. The main heading is "Trust Password" in bold. Below it, a subtitle reads: "Passwords are used by Active Directory Domain Controllers to confirm trust relationships." To the right of this text is a gold medal icon with a blue ribbon. The main instruction text says: "Type a password for this trust. The same password must be used when creating this trust relationship in the specified domain. After the trust is created, the trust password is periodically updated for security purposes." There are two text input fields: the first is labeled "Trust password:" and contains seven black dots; the second is labeled "Confirm trust password:" and contains seven black dots. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".