Home » How to configure Forest Level Trust in Windows Server

How to configure Forest Level Trust in Windows Server

Posted on May 6, 2013 by <u>Rick Trader</u> inShare2

Scenario – Two organizations, USSHQ (USSHQ.Local) and Dulce Base (DulceBase.Local) need to be able to share resources. A forest trust relationship between the two organizations Active Directory Domain Services is desired. Before the trust can be created name resolution needs to configured and tested for connectivity between the two domains. Once the trust relationship is configured, resource administrators will be able to configure permissions, privileges and rights to the trusted forest users.

Requirements

- Both Forests need to be in Forest Functional Level 2003 or higher
- Name resolution must be in place. Check out the blogs below for more information on how to create.

Conditional Forwarder - How to configure a Conditional Forwarder in DNS

Stub Zone - How to configure a DNS Stub Zone in Windows Server

Secondary Zone – <u>How to configure a DNS Secondary Zone in Windows Server</u>

• Must be a member of the Enterprise Admins Group or the Domain Admins Group in the forest root or delegated the rights to create trusts.

Terms

- <u>Trusted Domain or Forest</u> is the domain or forest where the users are authenticated.
- <u>Trusting Domain or Forest</u> is the domain or forest where the resources reside.

Note: Trust**TED** / Trust**ING** – *Ted* has the user, *Ing* has the things.

- <u>Transitive</u> User are able to traverse through the Parent Child trust relationship to access resources in the trusting domain.
- <u>Non-transitive</u> User are not to traverse through the Parent Child trust relationship to access resources in the trusting domain.

Verifying Name Resolution

If a computer from Dulce Base attempts to contact a computer in USSHQ it should be able to resolve the name to an IP Address.



If a computer from USSHQ attempts to contact a computer in Dulce Base it should be able to resolve the name to an IP Address.

Administrator: Command Prompt	_ 0	x
Microsoft Windows [Version 6.2.9200] <c> 2012 Microsoft Corporation. All rights reserved.</c>		^
C:\Users\Administrator>ping dbasesrv1.dulcebase.local		
Pinging dbasesrv1.dulcebase.local [172.16.11.20] with 32 bytes of data Reply from 172.16.11.20: bytes=32 time=1ms TTL=127 Reply from 172.16.11.20: bytes=32 time<1ms TTL=127	:	
Ping statistics for 172.16.11.20: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = 1ms, Average = Oms C:\Users\Administrator>		

Configuring the Forest Trust (steps will be accomplished in both Forest root domains).

1. Launch Server Manager, using the Tools drop down menu select Active Directory Domain and Trusts.

b		Server Manager	
	Server M	lanager • Dashboard	• 3
			Д Д
Dashboard		WELCOME TO SERVER MANAGER	A
Local Server			A
All Servers		1 Configure this local conv	A

2. In Active Directory Domains and Trusts, Secondary click on the domain and Click on Properties.

	Active Dir	ectory Domains and Trusts	
File Action View	Help		
Active Directory Dom	Manage	Type domainDNS	Actio
	Raise Domain Functional Level Properties		
	Help		

3. On the Domain Properties sheet, click on the Trusts tab.

4. Click New Trust, on the Welcome to the New Trust Wizard click Next.

5. On the Trust Name page, enter the name of the forest you want to establish the trust with, click Next.

New Trust Wizard
Trust Name You can create a trust by using a NetBIOS or DNS name.
Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.
Example NetBIOS name: supplier01-int Example DNS name: supplier01-internal.microsoft.com
Name:
USSHQ.Local
< Back Next > Cancel

6. On the Trust Type page click on Forest trust, click Next.

New Trust Wizard
Trust Type This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.
Select the type of trust you want to create. External trust An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.
Forest trust A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.
< Back Next > Cancel

Note: If one of the forest were not at Forest Functional Level 2003 or higher, an external trust relationship would be the default and the above screen would not have appeared.

7. On the Direction of Trust page choose the direction of the trust, click Next.

New Trust Wizard	x
Direction of Trust You can create one-way or two-way trusts.	
Select the direction for this trust.	
Two-way Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.	
 One-way: incoming Users in this domain can be authenticated in the specified domain, realm, or forest. 	
 One-way: outgoing Users in the specified domain, realm, or forest can be authenticated in this domain. 	
< Back Next > Cance	el

8. On the Sides of Trust page, in order to set the trust up for both domains you will need the administrative privileges or know the administrator account and password for both domains. In this demo I will choose **This Domain Only**, click Next.

New Trust Wizard
Sides of Trust If you have appropriate permissions in both domains, you can create both sides of the trust relationship.
To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.
Create the trust for the following:
 This domain only This option creates the trust relationship in the local domain.
 Both this domain and the specified domain This option creates trust relationships in both the local and the specified domains. You must have trust creation privileges in the specified domain.
< Back Next > Cancel

9. On the Outgoing Trust Authentication Level page, choose the appropriate authentication level, click Next.

Forest-wide will allow any authenticated user from the trusted forest to access any resource in the trusting forest that they have the permissions, privileges or rights. They will also be able to log onto computers in the trusting forest.

Selective will allow the administrator in the trusting forest to specify which resources and domain the users from the trusted forest.

New Trust Wizard
Outgoing Trust Authentication Level Users in the specified forest can be authenticated to use all of the resources in the local forest or only those resources that you specify.
Select the scope of authentication for users from the USSHQ.Local forest.
Forest-wide authentication Windows will automatically authenticate users from the specified forest for all resources in the local forest. This option is preferred when both forests belong to the same organization.
Selective authentication Windows will not automatically authenticate users from the specified forest for any resources in the local forest. After you finish this wizard, grant individual access to each domain and server that you want to make available to users in the specified forest. This option is preferred if the forests belong to different organizations.
< Back Next > Cancel

10. On the Trust Password page, enter a password that the administrators from both forests have agreed upon as the trust password, click Next.

New Trust Wizard
Trust Password Passwords are used by Active Directory Domain Controllers to confirm trust relationships.
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.
Trust password:
•••••
Confirm trust password:
••••••
< Back Next > Cancel

- 11. On the Trust Selections Complete page click Next.
- 12. On the Trust Creation Complete page click Next.
- 13. On the Confirm Outgoing Trust page and the Confirm Incoming Trust page click Next.
- 14. On the Completing the New Trust Wizard page click Finish
- 15. On the Domain Properties page, click Apply.

	Base.Local F	Properties	? X
General Trusts Manager	d By		
Domains trusted by this do	main (outgoing tr	usts):	
Domain Name	Trust Type	Transitive	Properties
USSHQ.Local	Forest	Yes	Remove
Domains that trust this dom	nain (incoming tru	ists):	
Densis News	T	T	D
Domain Name	Trust Type Forest	Transitive	Properties
Domain Name USSHQ.Local	Trust Type Forest	Transitive Yes	Properties Remove
Domain Name USSHQ.Local	Trust Type Forest	Transitive Yes	Properties Remove
Domain Name USSHQ.Local	Trust Type Forest	Transitive Yes	Properties Remove
Domain Name USSHQ.Local	Trust Type Forest	Transitive Yes	Properties Remove
Domain Name USSHQ.Local	Trust Type Forest	Transitive Yes	Properties Remove
Domain Name USSHQ.Local New Trust	Trust Type Forest	Transitive Yes	Properties Remove

Once the Forest Trust has been created in the other forest the two-way trust will be completed. User will then be able to access resources across the transitive trust between the forests. Use the Sharing and Security tabs to give the appropriate permissions to folders and/or files.