

RE: How to create trust relationship between Windows 2003 Server (domain controller) and Windows NT 4.0 PDC

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-06/0064.html>

From: S Vijay [MSFT] (svijay_at_online.microsoft.com)

Date: 06/02/04

Date: Wed, 02 Jun 2004 02:14:11 GMT

Hi,

Check whether you have followed the correct steps to establish a trust relationship between Windows NT and Windows 2003 by following the instructions in the article given below:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:325874&Product=winserver2003#4>

or

HOW TO: Establish Trusts with a Windows NT-Based Domain in Windows Server 2003

This article was previously published under Q325874

SUMMARY

How to Create a Trust Relationship

Windows NT Trusts Windows Server 2003
Windows Server 2003 Trusts Windows NT
Create a Two-Way Trust Relationship
Verify a Trust
Troubleshooting

SUMMARY

This step-by-step article describes how to establish a trust relationship between a Microsoft Windows NT 4.0-based domain and a Windows Server 2003-based domain.

The creation of a trust with a Windows NT-based domain uses the Windows NT trust model in a Windows Server 2003-based environment. Windows NT trusts are one-way trusts between a "trusting" domain and a "trusted" domain. For

RE: How to create trust relationship between Windows 2003 Server (domain controller) and Windows NT 4.0 PDC

example, if you have a Windows Server 2003–based domain whose users want to gain access to resources that are stored in a Windows NT–based domain, you must create a trust relationship in which the Windows NT–based domain trusts the users from the Windows Server 2003–based domain. In this case, the Windows NT–based domain is the trusting domain, and the Windows Server 2003–based domain is the trusted domain.

NOTE: You must use NetBIOS name resolution to enable trust between the two domains.

[back to the top](#)

How to Create a Trust Relationship

You can create either of the following one–way trust relationships between a Windows NT–based domain and a Windows Server 2003–based domain:

Windows NT trusts Windows Server 2003

Windows Server 2003 trusts Windows NT

Or you can create a two–way trust where both domains trust each other.

You must be logged on to the domain controllers of both domains with an administrator account to create a trust. When you create a one–way trust, first create the trust on the trusting domain, and then on the trusted domain.

[back to the top](#)

Windows NT Trusts Windows Server 2003

To create a trust relationship in which a Windows NT–based domain trusts a Windows Server 2003–based domain:

On the Windows NT–based primary domain controller (PDC):

Click Start, point to Programs, point to Administrative Tools, and then click User Manager for Domains.

On the Policies menu, click Trust Relationships.

Click the Add button that corresponds to the Trusted Domains box. The Add Trusted Domain dialog box appears.

In the Domain box, type the Windows Server 2003–based domain name without the .com portion of the domain name. For example, if the Windows Server 2003–based domain is Example.com, type Example.

In the Password box, type a password for the trust.

NOTE: You must use the same trust password on both the domain controller from the trusting and the domain controller from the trusted domain.

Click OK. The following message appears, where Windows Server 2003–based domain name is the name of the Windows Server 2003–based domain and where Windows NT–based domain name is the name of the Windows NT domain:

The trust relationship could not be verified at this time. If you find that it was not established, contact the administrator of the Windows Server 2003–based domain name domain and verify that it includes Windows NT–based domain name on its list of trusting domains.

Click OK. Note that the Windows Server 2003–based domain is listed in the Trusted Domains list.

In the Trust Relationships dialog box, click Close.

On the Windows Server 2003–based domain controller:

Click Start, point to Administrative Tools, and then double–click Active Directory Domains and Trusts.

In the Active Directory Domains and Trusts snap–in, right–click the domain that you want, and then click Properties.

Click the Trusts tab, and then click New Trust.

The New Trust Wizard appears. Click Next to continue.

Type the NetBIOS name of the Windows NT domain for this trust. For example, type supplier01–int, and then click Next.

In the Direction of Trust window, click One–way: incoming

Users in this domain can be authenticated in the specified domain, realm, or forest.

Click Next, and then in the Trust password box, type the same trust password that you used on the Windows NT–based domain controller. Type the password again in the Confirm trust password box.

Click Next, review your settings, and then click Next.

A message similar to the following message appears

Trust relationship created successfully.

Specified domain: supplier01–int

Direction:

Incoming: Users in the local domain can authenticate in the specified domain.

Trust type: External

Windows will authenticate users from the specified domain for all resources in the local domain.

Transitive: No

Sides of trust: Created the trust for this domain only.

where supplier01–int is the NetBIOS name of the Windows NT domain for this trust. Click Next, and then click Yes, confirm the incoming trust.

Type the user name and password of an account with administrative privileges for the specified domain, and then click Next. A message similar to the following message appears:

Completing the New Trust Wizard

You have successfully completed the New Trust Wizard.

Status of changes:

The trust relationship was successfully created and confirmed.

Click Finish to close the wizard, and then click OK to close the domain properties dialog box.

Quit Active Directory Domains and Trusts.

The trust is created. The Windows NT–based domain trusts accounts from the Windows Server 2003–based domain. However, this trust is a one–way trust.

The Windows Server 2003–based domain does not trust the Windows NT–based domain accounts.

back to the top

Windows Server 2003 Trusts Windows NT

To create a trust relationship in which a Windows Server 2003–based domain trusts a Windows NT–based domain:

On the Windows Server 2003–based domain controller:

Click Start, point to Administrative Tools, and then double-click Active Directory Domains and Trusts.

In the Active Directory Domains and Trusts snap-in, right-click the domain that you want, and then click Properties.

Click the Trusts tab, and then click New Trust.

The New Trust Wizard appears. Click Next to continue.

Type the NetBIOS name of the Windows NT domain for this trust. For example, type supplier01-int, and then click Next.

In the Direction of Trust window, click One-way: outgoing

Users in the specified domain, realm, or forest can be authenticated in this domain.

Click Next, and then click one of the following to select the scope of authentication for users from the Windows NT domain:

Allow authentication for all resources in the local domain

Windows authenticates users from the specified domain for all resources in the local domain. This option is preferred when both domains belong to the same organization.

Allow authentication only for selected resources in the local domain

Windows does not automatically authenticate users from the specified domain for any resources in the local domain. After you finish this wizard, grant individual access to each server that you want to make available to users in the specified domain. This option is preferred if the domains belong to different organizations.

Click Next, and then type a password for this trust in the Trust password box. You must use the same password when you create this trust relationship in the specified domain. After you create the trust, Active Directory periodically updates the trust password for security purposes. Type the password again in the Confirm trust password box, and then click Next.

Review your settings, and then click Next.

A message similar to the following message appears

Trust relationship created successfully.

Specified domain: supplier01-int

Direction:

Outgoing: Users in the specified domain can authenticate in the local domain.

Trust type: External

Windows will authenticate users from the specified domain for all resources in the local domain.

Transitive: No

Sides of trust: Created the trust for this domain only.

where supplier01-int is the NetBIOS name of the Windows NT domain for this trust. Click Next, and then click Yes, confirm the incoming trust.

Click Finish to close the wizard, and then click OK to close the domain properties dialog box.

Quit Active Directory Domains and Trusts.

On the Windows NT-based PDC:

Click Start, point to Programs, point to Administrative Tools, and then click User Manager for Domains.

On the Policies menu, click Trust Relationships.

Click the Add button that corresponds to the Trusting Domains box. The Add

Trusting Domain dialog box appears.

In the Trusting Domain box, type the Windows Server 2003–based domain name without the .com portion of the domain name. For example, if the Windows Server 2003–based domain is Example.com, type Example.

In the Initial Password box, type the same password that you used for the trust on the Windows Server 2003–based domain controller.

NOTE: You must use the same trust password on both the domain controller from the trusting and the domain controller from the trusted domain.

Type the password again in the Confirm Password box, make sure that you are currently logged on to both the Windows NT–based domain controller and the Windows Server 2003–based domain controller as an administrator, and then click OK. The Windows Server 2003–based domain is listed in the Trusting Domains list.

In the Trust Relationships dialog box, click Close.

The trust is created. The Windows Server 2003–based domain trusts accounts from the Windows NT–based domain.

back to the top

Create a Two–Way Trust Relationship

To create a two–way trust so both domains trust each other:

On the Windows Server 2003–based domain controller:

Click Start, point to Administrative Tools, and then double–click Active Directory Domains and Trusts.

In the Active Directory Domains and Trusts snap–in, right–click the domain that you want, and then click Properties.

Click the Trusts tab, and then click New Trust.

The New Trust Wizard appears. Click Next to continue.

Type the NetBIOS name of the Windows NT domain for this trust. For example, type supplier01–int, and then click Next.

In the Direction of Trust window, click 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.

Click Next, and then click one of the following to select the scope of authentication for users from the Windows NT domain:

Allow authentication for all resources in the local domain

Windows authenticates users from the specified domain for all resources in the local domain. This option is preferred when both domains belong to the same organization.

Allow authentication only for selected resources in the local domain

Windows does not automatically authenticate users from the specified domain for any resources in the local domain. After you finish this wizard, grant individual access to each server that you want to make available to users in the specified domain. This option is preferred if the domains belong to different organizations.

Click Next, and then in the Trust password box, type a password for this trust. You must use the same password when you create this trust relationship in the specified domain. After the trust is created, Active Directory periodically updates the trust password for security purposes.

Type the password again in the Confirm trust password box, and then click

Next.

Review your settings, and then click Next.

A message similar to the following message appears

Trust relationship created successfully.

Specified domain: supplier01-int

Direction:

Two-way: Users in the local domain can authenticate in the specified domain and users in the specified domain can authenticate in the local domain.

Trust type: External

Windows will authenticate users from the specified domain for all resources in the local domain.

Transitive: No

Sides of trust: Created the trust for this domain only.

where supplier01-int is the NetBIOS name of the Windows NT domain for this trust.

Click Next, and then click Yes, confirm the outgoing trust.

Click Next, and then click Yes, confirm the incoming trust.

Click Next, Type the user name and password of an account with administrative privileges for the specified domain, and then click Next. A message similar to the following message appears

Completing the New Trust Wizard

You have successfully completed the New Trust Wizard, but the newly created trust relationship could not be confirmed for the following reasons:

The verification of the incoming trust failed with the following error(s):

The target system supplier01-int does not support NetLogon trust password verification.

A secure channel reset will be attempted.

The secure channel reset failed with error 1355: The specified domain either does not exist or could not be contacted.

The verification of the outgoing trust failed with the following error(s):

The trust password verification failed with error 1787: The security database on the server does not have a computer account for this workstation trust relationship.

A secure channel reset will be attempted.

The secure channel reset failed with error 1787: The security database on the server does not have a computer account for this workstation trust relationship.

Before this trust can function, it must also be created in the other domain. Ensure that the same password is used in both domains.

where supplier01-int is the NetBIOS name of the Windows NT domain for this trust.

Click Finish to close the wizard, and then click OK to close the domain properties dialog box.

Quit Active Directory Domains and Trusts.

On the Windows NT-based PDC:

Click Start, point to Programs, point to Administrative Tools, and then click User Manager for Domains.

On the Policies menu, click Trust Relationships.

Click the Add button that corresponds to the Trusted Domains box. The Add Trusted Domain dialog box appears.

In the Domain box, type the Windows Server 2003–based domain name without the .com portion of the domain name. For example, if the Windows Server 2003–based domain is Example.com, type Example.

In the Password box, type a password for the trust.

NOTE: You must use the same trust password on both the domain controller from the trusting domain and the domain controller from the trusted domain. Click OK. Note that the Windows Server 2003–based domain is listed in the Trusted Domains list.

Click the Add button that corresponds to the Trusting Domains box. The Add Trusting Domain dialog box appears.

In the Trusting Domain box, type the Windows Server 2003–based domain name without the .com portion of the domain name.

In the Password box, type the same password that you used for the trust on the Windows Server 2003–based domain controller, and then click OK. The Windows Server 2003–based domain is listed in the Trusting Domains list.

In the Trust Relationships dialog box, click Close.

The two–way trust is created. The Windows NT–based domain trusts accounts from the Windows Server 2003–based domain, and the Windows Server 2003–based domain trusts the Windows NT–based domain accounts.

[back to the top](#)

[Verify a Trust](#)

To verify that the trust relationship is working, follow these steps on the Windows Server 2003–based domain controller:

Click Start, point to All Programs, point to Administrative Tools, and then click Active Directory Domains and Trusts.

In the console tree, right–click the domain that contains the trust you want to verify, and then click Properties.

Click the Trusts tab, and then under either Domains trusted by this domain (outgoing trusts) or Domains that trust this domain (incoming trusts), click the trust to be verified, and then click Properties.

Click Validate.

[back to the top](#)

[Troubleshooting](#)

When you try to create a trust between domains, you may receive the following error message:

Could not find domain controller for this domain

This error message can occur for the following reasons:

Networking issues

Make sure that both computers are using TCP/IP and that you can connect to the other computer by using a network utility such as Ping.exe.

Name resolution issues

Make sure that the Windows NT–based domain controller can resolve the host name of the Windows Server 2003–based domain controller, and that the

.public.win2000.security: RE: How to create trust relationship between Windows 2003 Server (domain controller) and Windows

Windows Server 2003-based domain controller can resolve the NetBIOS name of the Windows NT-based domain controller. If you cannot resolve the NetBIOS and host names, create an entry in the Lmhosts file on each domain controller that specifies the location of the other controller. For additional information about how to create and modify Lmhosts files, click the article numbers below to view the articles in the Microsoft Knowledge Base:

181171 Secure Channel Manipulation with TCP/IP

102725 Lmhosts File Information and Predefined Keywords

Trust issues

You may have to set the RestrictAnonymous value to 0 to establish the trust. For additional information, click the following article number to view the article in the Microsoft Knowledge Base:

246261 How to Use the RestrictAnonymous Registry Value in Windows 2000

Hope this helps.

S.Vijay

This posting is provided "AS IS" with no warranties, and confers no rights

RE: How to create trust relationship between Windows 2003 Server (domain controller) and Windows NT 4.0