

By Rick Vanover

Domain trusts can be complicated to administer, and it's important to implement changes correctly the first time. Here are some key points to keep in mind to help ensure that your trusts are configured effectively with a minimum of headaches.

Table of contents

Determine what kind of trust you should use.....	2
Get familiar with the Active Directory Domains And Trusts Console	2
Know the tools.....	2
Set up a test environment	3
Review privileges	3
Map out the trusts	3
Document trust relationships.....	3
Avoid making trust relationships too deep.....	3
Manage different versions of Windows.....	4
Remove expired or overlapping trusts.....	4

1 Determine what kind of trust you should use

Before deploying a domain trust, you should ensure that the type(s) used are correct for the tasks at hand. Consider the following dimensions of a trust:

- **Type:** Identifies the types of domains involved in trust(s).
- **Transitivity:** Determines whether one trust can let a trusted domain pass through to a third domain.
- **Direction:** Identifies the direction of access and trust (trusted accounts and trusting resources).

Type	Transitivity	Direction
Parent and Child	Transitive	2-way
Tree-root	Transitive	2-way
External	Nontransitive	1-way OR 2-way
Realm	Transitive or Nontransitive	1-way OR 2-way
Forest	Transitive	1-way OR 2-way
Shortcut	Transitive	1-way OR 2-way

2 Get familiar with the Active Directory Domains And Trusts Console

Trust relationships are managed via the Active Directory Domains And Trusts Console. It lets you perform these basic tasks:

- Raise domain functional level
- Raise forest functional level
- Add UPN suffixes
- Manage domain trust
- Manage forest trust

For details on using this tool, see "[TechRepublic Guided Tour: Active Directory Domains And Trusts Console](#)." (Note: A TechProGuild membership is required to access the article.)

3 Know the tools

As with most other elements of the Windows Server family, command-line tools can be used to script repetitive tasks or to ensure consistency in the case of trust creation. Some of the top tools include:

NETDOM: Used to establish or break trust types.

NETDIAG: The output of this tool can give basic status on trust relationships.

NLTEST: Can be used to verify a trust relationship.

You can also use Windows Explorer to view membership to shared resources as they are assigned from trusted domains and/or forests. Active Directory Users And Computers can also provide membership details of Active Directory Objects that have members from trusted domains and/or forests.

4 Set up a test environment

Depending on your environment and usage requirements, a simple mishap in the creation of domain trusts can have enterprise-wide repercussions. But it's difficult to set up a completely similar test environment to replicate multi-domain and forest issues. Having similar domain scenarios is easier to facilitate, as a means to reinforce the principles and test basic functionality. Consider also template Active Directory objects to test on the live domain relationships to ensure that the desired functionality is obtained but not exceeded before using live groups, accounts, and other objects.

5 Review privileges

When trusts are created, it's important to ensure that the desired functionality is achieved. But be sure to review the configured trust to verify that the direction of access is correct. For example, if domain A needs to access only a limited amount of resources on domain B; a two-way trust would suffice. However, an administrator from domain B may be able to assign access to resources on domain A. Ensuring the desired direction, type, and transitivity of trusts is critical.

6 Map out the trusts

Create a map of trusts with simple arrows and boxes illustrating which domains will be trusting and trusted and which trusts will be 1-way and 2-way. Then, with the simple picture(s) in place, map out which domains will trust which—and determine the transitivity as well. This simple chart will make more sense of the greater task at hand and allow you to determine which domains need direction of access and in which direction. Some domains will simply act as a gateway for transitive access to other domains.

7 Document trust relationships

As organizations marry (and divorce) in today's business world, it's important to have clear documentation of the trust inventory—and to make sure it's accessible without the trust or domain. For example, if you're in Domain B and your headquarters in Domain A sells your division and breaks your trust, your concise documentation saved on a server in Domain A does you little good. Document the type of trust, transitivity, direction, business need for the trust, anticipated duration of the trust, credentials, domain/forest principal information (name, DNS, IP addresses, locations, computer names, etc.), and contact person(s) for the corresponding domains.

8 Avoid making trust relationships too deep

In the interest of everyone's time, don't nest membership more than one deep when using trusts in multiple domains and forests. Nesting membership can consolidate the number of manageable Active Directory objects, but determining actual membership administration is greatly increased.

9 Know how to manage different versions of Windows

When running in Windows 2000 and Windows Server 2003 native mode for Active Directory, full functionality is maintained for member domains and forests. If any NT domains or member systems are present in the enterprise, their trust entry functionality is limited by the inability to recognize the Active Directory objects. A frequent strategy in this scenario is to have “domain islands” of those that don't connect to the more common enterprise infrastructure.

10 Remove expired or overlapping trusts

Changes in business organization may have left unused trusts in place on your domain. Clear out any trusts that are not actively being used. You should also ensure that the trusts you have are set up correctly for the required access and usage patterns. An audit of your trust inventory can be a strong supplement to your well-rounded security policy.



Rick Vanover works for Siemens Logistics and Assembly Systems in Grand Rapids, MI, where he's part of a team of IT professionals that deploy custom software solutions to the material handling industry using a mix of current hardware and software products. Previously, he lived in Columbus, OH, and focused on client-server administration and support, project management, negotiating vendor agreements, and Internet connectivity and VPN. You can reach Rick at b4real@usa.net.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) [XML](#)
- Sign up for our [Downloads Weekly Update](#) newsletter
- Sign up for our [Network Administration NetNote](#)
- Check out all of TechRepublic's [free newsletters](#)
- ["Trust Types"](#) (Microsoft TechNet)
- ["Understanding Win2K Domain Trusts"](#) (TechRepublic article)
- ["Create Trust Relationships"](#) (TechProGuild)
- ["Comprehend Windows Server 2003 trust relationships and functional levels"](#) (TechRepublic article)
- ["Establishing Trusts in Windows 2000"](#) (TechProGuild)

Version history

Version: 1.0

Published: October 26, 2005

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team