Who do you trust? Options for setting up forest-to-forest trusts

By **Douglas A. Paddock, SearchWin2000.com contributor**
21 May 2003, **SearchWindowsManageability.com**

One of the important things about trusts in Windows Server 2003 is that it gives you the ability to sp a trust will operate. In this article, the second installment in a two-part series, we look at your optior forest and forest trust in Active Directory. Part one of this series discusses how Microsoft tracks trusts using trusted domain o

You have three options for setting up a trust.

1. Two-way trust. In a two-way trust (remember, we're assuming a forest root-to-forest root trust here), users in both forests can be authenticated in one another's forest. This does not automatically grant rights in each forest; users will still have to be granted rights. You will also want to watch your Guests and the Everyone account, if you're using those rights with any assets in your forest.

2. One-way incoming trust. Users in your domain can be authenticated and access objects or can be granted rights and privileges in the trusting forest. Remember the old rule used when diagramming and establishing trusts: "You point to the person you trust." Users from the other forest cannot do the same in your forest.

3. One-way outgoing trust. This is just the opposite of option two: You are granting others the ability to access objects and/or be granted rights and privileges in your forest.

A note on empty root domains

As you read about establishing just about everything in both Windows 2000 and Windows 2003, you will notice that you must either Domain Admins or Enterprise Admins, or else of some other group, like Incoming Forest Trust Builders Group, in order actions. Remember that a Domain Administrator in the forest root domain can make himself an Enterprise Administrator, a Sc Administrator or a member of some other group, simply because Domain Admins (of which the local Administrator is a memb group memberships.

More than any other domain administrator, the root domain administrator has tremendous power in any organization, which is empty root domain at the top of your forest is frequently desirable. By creating an empty root domain for your forest, you can the root domain's Domain Administrators group. This should not create an undue workload, since the forest root domain has regular tasks that must be accomplished in a domain that is populated with ordinary users and resources.

After you have decided on a direction for the trust, the next question to address is whether you want to allow authentication fc the domain you are trusting or only for selected resources in the local domain.

As the screen explains, Microsoft only recommends authentication for resources for trusts that involve intra-organizational un recommends limited authentication for selected domain resources for domains belonging to different organizations. If you cho authentication, you will need to manually enable rights for users from the other forest for each domain and the individual reso will be accessing. The authentication level can be changed at any time by opening Properties for the root domain in Active Di and Trusts and accessing the Trusts tab.

The rest of the trusts wizard is fairly straightforward. It will prompt you to confirm the outgoing and incoming trusts, for exampl

The ability to set up trusts among different forests can be extremely helpful, but keep in mind that administrators configuring W Server typically created separate forests in the same company to avoid security problems involving domain boundaries (such SIDHistory flaw). The SIDHistory flaw has the potential to allow administrators in a trusted domain unauthorized administrativ the SIDHistory attribute. In Windows Server 2003, SID filtering is enabled by default for forest-to-forest trusts to prevent the S problem from occurring. (Refer to "forest trusts" and "securing external trusts" under Help for more information.)

Even though some security issues have been addressed, administrators will still want to meet with all corporate stakeholders this new capability meets their corporate Active Directory design requirements. Separate companies in the process of mergin may wish to establish forest-to-forest trusts for easy resource access between companies. On the other hand, separate depa same company that need to segregate data (such as legal department, for example) would probably not want to establish suc to avoid the compromise of sensitive information.

In any case, security and the possibility of as-yet undiscovered vulnerabilities should always be primary considerations, espe operating system of this complexity. All such decisions should involve a careful risk/cost benefit analysis and a thorough discu many design and security issues involved.

>>Back to part one

***About the author**: Douglas Paddock is an IT instructor at Louisville Technical Institute in Louisville, Ky. He holds CIW Secur Certified Instructor, MCSE, MCT, MCSA, A+ and N+ certifications.*

FOR MORE INFORMATION

Best Web Links on Active Directory and network management
Click here to ask expert Paul Hinsberg a question.

>> Microsoft to make manageability a forethought (vnunet)