

Re: Two Server Setup Question.

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.setup/2006-07/msg00080.html>

- *From:* "Purtech" <mikek(remove)@hlit.net>
 - *Date:* Fri, 14 Jul 2006 11:52:20 -0500
-

It will be a couple weeks but I will let you know how it goes.

Thanks!

"Dennis Chung [MVP]" <dennis@xxxxxxx> wrote in message
news:uM9CENvpGHA.756@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi Purtech,

i'm really glad you find it helping.

First of all, the term "external" only refers to something domain outside your current domain. It doesn't mean coming from the internet and back. The 2 domain controllers from the 2 domains, could be sitting next to each other, connected to the same switch. That external trust factor thing only means that the domains don't trust each other by default in any directions.

So taking the scenario that we've been talking about and putting in the external trust thingy. We can derive at this design.

First of all, get your admin domain up first.

You install this normally like you would for a normal domain. I assume you know how, if you don't, pop over to support.microsoft.com and search for how to setup a domain controller. Say this domain is school.org. After your dcpromo the computer to a dc, this dc is said to be a single forest, single domain.

Second, your other lab domain, lets call this lab.school.org. Don't be concern by the name, the name doesn't mean its a child domain. Whether its a child domain or a seperate forest depends on how you install it. For this machine, you would do a dcpromo on the computer and proceed to install as if you are installing school.org. **DO NOT ADD THIS AS A CHILD DOMAIN OF AN EXISTING DOMAIN.** After you're done, you'll end up with 2 seperate domains in 2 seperate forest.

What you need to do now is to establish an external trust from school.org to lab.school.org. Its better for your to learn more about which direction you should create. If you have access to a book, get MS

Re: Two Server Setup Question.

Press (Active Directory for Windows Server 2003 – Technical Reference) and find out more about trust. Your job here is to establish trust between the 2 domains in a SINGLE direction. Naturally the direction is for teachers in school.org to enter lab.school.org and not the other way round.

If you don't have the book, doesn't matter. I believe think link will get you all you need to know about the external trusts. :-) Have fun and let us know if you're successful in your setup.

<http://technet2.microsoft.com/WindowsServer/en/Library/261d6ecf-b4bc-4188-8805-d31fb49954d81033.ms>

--
Best Regards,
Dennis Chung

MCP, MCSA (2k3/Security), MCSE (2000/2003)
MCDBA, MCTS (SQL 2005), MCITP (SQL 2005 – DBA)
Microsoft Certified Trainer, Microsoft MVP – Windows

Microsoft Windows & SQL Server Advisory Panel Member
MS IT Academy – Mentor (APAC)
MS Vista & Office12 Influencer Lead (APAC)
Founder: Singapore Windows User Group (<http://sgWindowsGroup.org>)

"Purtech" <mikek(remove)@hlit.net> wrote in message
<news:uaKysjqpGHA.3936@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Wow.

Sounds like the outgoing external trust thing is the best way. (I googled that term and found our discussion!)

How...do I set that up or please point me to a resource to help. I don't want students or teachers from lab.school.org being able log on to admin machines.

Gareth brought up a point...should just I just subnet the two domains, put a router between them...then how do I configure and external trust? (Or does a VLAN do something better.)

Or when you say external are you talking out on the Internet and back?

Thanks so much! This is really helping.

"Dennis Chung [MVP]" <dennis@xxxxxxx> wrote in message
<news:e4BQP0ipGHA.3584@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Hi Purtech,

Dave has a point. Both designs will work for you.

Re: Two Server Setup Question.

What I don't understand is how a child domain works – particularly with Authentication. Actually...now that I think about it... so teacher@xxxxxxxxx who is a admin/account operator of lab.school.org does not have admin privileges in the school.org domain, right?

But administrator in the school.org domain does, have admin right to lab.school.org, right?

Yes, administrator@xxxxxxxxx has admin rights over lab.school.org because the first administrator is also an enterprise admin. And enterprise admin is the king.

Well, its going to take very long to tell you how a child domain works. But we create child domain normally to separate/setup security boundaries in the domain. There are several concerns though and as usual, pros and cons to every design. Yes, teacher@xxxxxxxxx will be able to login to lab.school.org and be able to control accounts related things. However, because within the same forest, the domains trusts each other, anyone in lab.school.org can logon to any workstation within the school.org forest provided they have rights which by default yes.

Another way of doing this is what Dave suggested, which tend to be better in terms of security if you are talking about setting up school.org and perhaps maybe lab.org. In this case, it gets a little more complicated because each one holds 1 forest 1 domain. No trust relationship exists. Having said that, teacher@xxxxxxxxx has no control over lab.org. You need to establish an external trust from school.org to lab.org (outgoing external trust–single direction). This means teacher@xxxxxxxxx can go to lab.org, but students within lab.org cannot

Re: Two Server Setup Question.

go to school.org because there no trust established in that direction.

After this, you add teacher@xxxxxxxxx to lab.org and make teache the account operator or lab.org. There.. you're done... Alternatively, don't do trust. Get your teachers to remember two ids and passwords. 1 for each domain. ;-)

Dave – in the other post – said he would just create to separate domains. school.org and school2.org I suppose. Is this more secure?

To help Dave answer, yes it is.

--
Best Regards,
Dennis Chung

MCP, MCSA (2k3/Security), MCSE (2000/2003)
MCDBA, MCTS (SQL 2005), MCITP (SQL 2005 – DBA)
Microsoft Certified Trainer, Microsoft MVP – Windows

Microsoft Windows & SQL Server Advisory Panel Member
MS IT Academy – Mentor (APAC)
MS Vista & Office12 Influencer Lead (APAC)
Founder: Singapore Windows User Group
(<http://sgWindowsGroup.org>)

"Purtech" <mikek(remove)@hlit.net> wrote in message
news:ecBoaobpGHA.2400@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Excellent Dennis.

What I don't understand is how a child domain works – particularly with Authentication. Actually...now that I think about it... so teacher@xxxxxxxxx who is a admin/account operator of lab.school.org does not have admin privileges in the school.org domain, right?

But administrator in the school.org domain

Re: Two Server Setup Question.

does, have admin right to
lab.school.org, right?

Also:

There are about 20 computers in the lab and
about 10–15 in admin. I
have two switches. Would two separate
VLAN's or two subnets be
appropriate. I don't think broadcast traffic is
a big issue with this
setup and these switches.

Dave – in the other post – said he would just
create to separate
domains. school.org and school2.org I
suppose. Is this more secure?

Thanks!

"Dennis Chung [MVP]"

<dennis@xxxxxxxx> wrote in message

news:eK9HVZVpGHA.2256@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

There are several scenarios
you can create from there.
Assuming these followings;
Teacher has an account in
school.org. But here, the
teacher is a
normal user. Limited rights,
just normal user. This can
also be
administration.

After that domain is up and
the teacher has a normal
account, say
teacher@xxxxxxxx
You go on to build another
child domain, lab.school.org
Put the
teacher@xxxxxxxx as a
domain admin / account
operator in
lab.school.org.

Of course domain design
wise will be like that.

But observing that you

Re: Two Server Setup Question.

mention the new server will be school.org, and your old server be lab.school.org. You have a few stage here to deal with.

Stage 1. Assuming your current old server is housing school.org. You need to put your new server as school.org. You need to make the new server a dc. Before you can add a w2k3 dc into a w2k domain, you need to perform adprep. Go to support.microsoft.com and search for the adprep command to extend the schema. Then you dcpromo to make the w2k3 box a DC. Subsequent, leave it for about 30 mins.

Stage 2. You need to remove the old server and make it the DC for lab.school.org. DCpromo your old server to remove it as a domain controller. Remember to deal with your DNS/DHCP to reflect the new DC else your clients will not be able to find the w2k3 DC. After dcpromo, it'll be a normal member server of the domain.

Stage 3. Now you can put your old server as the dc for lab.school.org as a DC by doing dcpromo.

Stage 4. In lab.school.org, you specify that TEacher@xxxxxxxxxxx is a member of lab.school.org\domain admin or account operators

Re: Two Server Setup Question.

group.

Then i guess you're more or less done. :-)

--

Best Regards,
Dennis Chung

MCP, MCSA
(2k3/Security), MCSE
(2000/2003)
MCDBA, MCTS (SQL
2005), MCITP (SQL 2005 –
DBA)
Microsoft Certified Trainer,
Microsoft MVP – Windows

Microsoft Windows & SQL
Server Advisory Panel
Member
MS IT Academy – Mentor
(APAC)
MS Vista & Office12
Influencer Lead (APAC)
Founder: Singapore
Windows User Group
(<http://sgWindowsGroup.org>)

"Purtech"
<mikek(remove)@hlit.net>
wrote in message
news:%23avhV%23RpGHA.1440@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

A school
currently
has one
2000 server.
Single
domain.
Lets says
school.org.

They want
to add a
second
server and
upgrade
both to
Windows
2003

Re: Two Server Setup Question.

Re: Two Server Setup Question.

Standard.

They want
the newer
second
server to be
in
administration,
and the
older server
to be in a
computer
lab.

They want
administration
and lab to
have
separate log
in controls.
The teacher
in charge of
the lab
server can
add and
removed
student
log ins.
However,
he will have
limited
access to
the
administration
server.

First:
should I
create two
separate
domains?
administration.school.org
and
lab.school.org.
Or just
create a
lab.school.org
under
school.org?

They will

Re: Two Server Setup Question.

not grow
past this for
years.

Thanks for
you help.