

Re: AD forest layout recommendations

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-01/msg00039

- *From:* R. E. Wendel <REWendel@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 2 Jan 2006 11:33:04 -0800
-

Regardless of AD security, we are implementing separate network level protections in order to directly address security issues. Currently just shutting the two worlds off from one another is growing to be more of a hassle than it is worth. Some measures we are looking at are:

- a) promiscuous port assignments to all clients, except IT
- b) tiered network security on important servers/services (no need for clients to be able to connect directly to Oracle when they go through a middle-tier anyway; same for front-end/back-end exchange). Some of this is done, but not finished.
- c) no secured data would be available on any machine network-ly accessible from student machines. we are going to keep the student machines separated by vlan and acls, so this is still cake.
- d) remote sites would not actually contain secure data at all. links joining major campuses A/B/C will be 10MB metro-ethernet connection, with 3MB dsl connections bringing in sites D/E. D/E only have 1-3 admin/faculty staff on them anyway, so load is not a big deal. students don't get separate logons, as I realize that the replication of thousands of logons would sig. increase load. we are doing sso stuff for students, but everything is web based through a portal, not windows logon based.
- e) trust would be one way (student machines allow admin logon, admin machines reject student logon)

I understand the trusts. My primary question really related around whether I can have a single domain controller (GC) provide authentication for both domains on each of the remote sites.

"Al Mulnick" wrote:

- > Now, my questions:
- > A) GCs will authenticate for any domain in the forest, right?
- > B) Any problems with above?
- >
- > A = Here's a much more in-depth discussion of authentication and security
- > services.
- >
- > <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/e36ceae6-ff36-4a1b-9895-79>
- >

Re: AD forest layout recommendations

> B = Problems? Aside from your expectations of authentication (see A above
> to clarify them and note that it's my impression of your expectation that
> I'm basing that on) I think you should carefully consider the security
> implications. You can have forest trusts if that's needed, but knowing that
> you're a school tells me that you have students. Students are curious
> critters by nature. As such, they *could* decide to load a program that
> tries to gain access to your forest. I suppose they could even try to gain
> access to your forest. Since the domain is not a security boundary, the
> risk is higher and you should carefully consider the tradeoffs you expect.
> If you've already done that, then the placement of your solution would be
> more dependent on your available network bandwidth.

>

> A1

>

>

> "R. E. Wendel" <REWendel@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
> news:0380E022-493C-411D-AA32-74378EA10C87@xxxxxxxxxxxxxxxxxxxx
>> I am looking to do a few things in the very near future concerning our AD
>> layout and would like to ask a few questions, give my design, and see if
>> it
>> floats.

>>

>> We are a school. Currently we have 2 separate domains: one administrative,
>> one student.

>>

>> They do not have trusts because the former network operators did not see
>> the
>> need. I do.

>>

>> So we have 5 sites, currently we only have domain controllers on 3 of them
>> (our full sized campuses, the other two are small single building remote
>> sites). The Main campus is A, the two large campuses are B & C, and the
>> two
>> small sites are D & E.

>>

>> In order to support the current design, obviously we have 2 domain
>> controllers on each campus A, B, & C. Currently we cannot setup trusts
>> between the existing b/c as a school, security is an issue, so we restrict
>> ALL traffic between the sides, save for VNC one way from admin to student
>> for
>> remote management. We will be opening up this, as we are implementing more
>> standard security practices.

>>

>> I would like to move to the following topology:

>>

>> Site A := 2 primary DCs (one admin, one student)

>> Site B & C := 1 DC each site, both being GCs, providing DNS, DHCP, and AD
>> services for both domains

>> Site D & E := same as B & C, with spare servers from B & C redes.

>>

>> Now, my questions:

Re: AD forest layout recommendations

- >> A) GCs will authenticate for any domain in the forest, right?
- >> B) Any problems with above?
- >
- >
- >
- .

• **Follow-Ups:**

- ◆ **Re: AD forest layout recommendations**
◇ From: Al Mulnick

• **References:**

- ◆ **Re: AD forest layout recommendations**
◇ From: Al Mulnick
- Prev by Date: **Re: Administrators Group in Local Users and Groups**
- Next by Date: **Error : No se encuentra el Objeto DSA**
- Previous by thread: **Re: AD forest layout recommendations**
- Next by thread: **Re: AD forest layout recommendations**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**