

# Re: AD design question

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2007-05/msg00314](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-05/msg00314)

---

- *From:* "Jeremy" <[jeremy@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:jeremy@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sat, 5 May 2007 10:38:55 +1000
- 

I am in complete agreement with Allan. The cases where you put in a root domain for the purposes of enterprise administration are very rare and specialised.

I've been putting in ADs for 7 years and have never put in multiple Domains let alone multiple forests. Usually because the administration model of the organisation has been centralised.

"Allan Jacobs" <[allanjnyc@xxxxxxxxxxxx](mailto:allanjnyc@xxxxxxxxxxxx)> wrote in message  
[news:40291832-0CA7-46F2-B71F-32779DEE6744@xxxxxxxxxxxxxxxxxxxx](mailto:news:40291832-0CA7-46F2-B71F-32779DEE6744@xxxxxxxxxxxxxxxxxxxx)

Hi Phil,

I may be in the minority, but I have never seen the value of the empty root domain, except to solve political issues (which division should "own" the root) or for VARs and consultants to sell more hardware and server licenses. In order to solve most security concerns a well constructed delegation model should be created. Keep membership in the domain admins group very small. Carefully construct an OU structure. Intelligently create shares. If you don't design for security, two extra DCs in an empty root will do little good.

Allan Jacobs  
<[phil2627@xxxxxxxxxxxx](mailto:phil2627@xxxxxxxxxxxx)> wrote in message  
[news:1178312811.523579.14990@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:1178312811.523579.14990@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

We are in a school district with 500 staff and 4000 non staff. We are still undecided on the model, but know the following

- only real secure model is separate forest, where staff could be in one and non staff in the other and setup trusts to have certain staff access resources in other forest
- One forest, domain model is simple, and the suggested way to go unless there are political or admin delegation reasons
- empty domain model would not "secure" the enterprise admin accounts. But, can Domain admins in a child domain access the enterprise admin group without physical access to the servers ?

We would like to go with the single domain as, if we secure the administrator account, no user should be able to gain access to the domain admin or enterprise admin group.

## Re: AD design question

With the Empty Root model the enterprise account is in its own domain which somewhat secures it, but this model requires more ha