

Re: Cross Forest Administration

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-04/msg01554

- *From:* Brad <BDS@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 29 Apr 2008 01:31:00 -0700
-

Thanks for the response, maybe I am missing something obvious, but I still don't see a resolution here. Given that EA is a Universal Group it can contain either Global or Universal groups. Neither Global or Universal groups can contain objects from another Forest. The only group type that can contain objects from another forest is Domain Local. However Domain Local can not be a member of a Universal group.

Any ideas?

"Herb Martin" wrote:

"Brad" <BDS@xxxxxxxxxxxxxxxxxxxx> wrote in message
news:4F5DA8E2-F9C3-4943-95CB-B40756131E00@xxxxxxxxxxxxxxxxxxxx

That was my first hope. But it is only possible to add users from another forest to a Domain Local group, and it is not possible to add a Domain Local Group to a Universal group. Enterprise Admins is a Universal group.

Group containment operates in this direction:

Global --> Universal --> (Domain or computer) Local

The one to the right can contain the one(s) to the left.

For granting permission you usually do this on Local groups, so adding UNIVERSAL (or Globals) from a Trusted Domain is the usual method.

As written above, you seem to have the strategy (but not the technical rules) backwards.

"Herb Martin" wrote:

Re: Cross Forest Administration

"Brad" <BDS@xxxxxxxxxxxxxxxxxxxx> wrote in message
news:3B4DFCA4-644E-4356-B369-BDD0533A379E@xxxxxxxxxxxxxxxxxxxx

Hey All,

I have three forests (all with one domain) that are managed by the same AD administration team. Forest A is the main production forest with thousands of users and trusts Forest C. Forest B holds resources used by internal and external users, and trusts Forest A. Forest C holds some specific infrastructure and trusts Forest A. To summarize:

Forest A <----> Forest C (Two way)
Forest B <---- Forest A (Forest B trusts Forest A but not vice versa).

All Forests are managed by the exact same IT staff, and Forest A has a very highly configured delegation model in place. I want to extend the delegation model to the other two forests. I can easily create permisisions (using Ative Roles FWIW) on Forests B and C. What I wanted to also achive was getting users that are members of Enterprise Admin and Domain Admins in Forest A to be members of the same in Forests B and C. What is the easiet way of getting Enterprise Admins and Domain Admins in Forests B and C to match that of Forest A?

Add their accounts to the Enterprise Admins in the other forest?

Re: Cross Forest Administration