

Re: Moving DC's From Default OU ?

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-08/msg02745

- *From:* "Joe Richards [MVP]" <humorexpress@xxxxxxxxxxx>
 - *Date:* Thu, 24 Aug 2006 11:45:27 -0400
-

LOL. Excellent example of what I said. Complete misunderstanding on how Domain Security works.

Once the outsourcing company has rights to make admin changes on a single DC they own your entire forest. You cannot protect against this in any way you dream up because it just cannot be done with Active Directory.

You might as well make them Domain and Enterprise Admins, at least you will be honest with yourself them on what rights they have.

Again, I don't care who told you otherwise, you cannot protect the AD from someone you give admin level rights or in fact even server operator rights or even less.

--

Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

Jim B. wrote:

Joe,

I've got one for you. My company is moving the production systems to a utility computing environment that is hosted at a 3rd party data center. The 3rd party will be managing the O/S and hardware for us. One of their requirements is that we establish a trust to their management domain and grant their management group access as members of the Built-in Administrators group on the DCs that they will be hosting for the production domains and forest. While setting up a resource domain would be the preferred method, it is out of scope for this project.

In an effort to secure the AD, we want to move these DCs and all other computer objects in to another tree structure so that we can apply a DENY for all permissions.

Re: Moving DC's From Default OU ?

Make Sense? Hope so.

Jim

"Joe Richards [MVP]" wrote:

It can be done safely but the more important question is why? I have yet in 6 years of hundreds of people in lots of companies trying to convince me of this to have heard a single good reason for it.

In almost every case it the thought to do this is based on some misunderstanding on how Domain Security works or some stupid plan to have a pretty hierarchy.

joe

--

Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

Chris wrote:

Is there any known issues from moving our DC's from the default domain controller OU?