

Re: Restrict Access

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-08/msg01553

- *From:* "Anthony" <anthony.spam@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 8 Aug 2006 16:38:18 +0100
-

Its a pleasure, hope you manage to achieve what you are trying to do,
Anthony
"mark" <mwheat28@xxxxxxxxxxxxxxxx> wrote in message
news:uAi9vHvuGHA.4544@xxxxxxxxxxxxxxxx

Thank you anthony. I appreciate your thoughts and input. You've offered other options that I'd not considered and confirmed others that I had. Have a great week and thank you again for your suggestions.
Mark

"Anthony" <anthony.spam@xxxxxxxxxxxxxxxx> wrote in message
news:Oam3igruGHA.4160@xxxxxxxxxxxxxxxx

Really you have a business policy problem and a logical dilemma
masquerading
as a technical problem. The company wants the DB's to be "off limits" and also wants the Enterprise Admins to run everything. Just give the

Enterprise

Admins a formal notice that accessing the data is a dismissal offence. But I think you already realise this from the things you have looked at. Obviously an Enterprise Admin can take the rights of any user in the
forest,

so you would need to make sure that no user account had the rights to even read the data.
This means that you would need to use a completely separate unconnected security system. You would also need to make sure that the credentials required to access the DBs were not stored in any user account, and were

not

Re: Restrict Access

retained in any cache on any PC uses to access the system. So your

solution

is:

- Separate Forest, no trust of any kind.
 - Access only through something like an SSL VPN, browser cache cleared on logoff
 - Two-factor authentication with one-time token, something like SecureID
- This is not an odd solution. It is exactly the same as if you were trying

to

create a new system with reasonably secure access.

Anthony

"mwheat" <mwheat28@xxxxxxxxxxxxxxxxxxxx> wrote in message
news:uqKTZcnuGHA.5076@xxxxxxxxxxxxxxxxxxxxxxxx

Good afternoon. I'm hoping someone has a suggestion for how to proceed

on

this as it doesn't quite fit any scenarios I've dealt with before.

Can we restrict management and access to servers in Active Directory

from

upper level enterprise admins?

Scenario:

Company A is has multiple database servers that need to be protected due

to proprietary information. Company B has acquired company A and agreed that all DB servers are off limits to company B. They are migrating all users and objects from A into a new OU in company B's Active Directory.

The concern is trying to restrict upper level enterprise admins from having access or changing permissions on those boxes. All users from

Re: Restrict Access

company A will still need access to the DB servers.

Sorry for the somewhat confusing scenario. We've noodled the possibility of creating a separate network space and restricting access by ACLs and rules. Alternatively we could remove these machines from the new domain and create a new one with a non-transitive trust. Then lock it down with group membership. Both seem to have pros and cons.

Any assistance would be greatly appreciated.
MW