Re: AD account − limiting access to a single server

Source:
http://www.tech−archive.net/Archive/Windows/microsoft.public.windows.group_policy/2007−08/msg00398.html

- *From*: "Florian Frommherz [MVP]" <florian@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
- *Date*: Tue, 28 Aug 2007 13:22:33 +0200

Howdie!

RadioLontrA schrieb:

> What about creating a gpo for the whole domain, excluding that single computer, saying "deny access to this computer from the network" for that user?

Good point, you could to that − but "injecting" every single machine and server in your domain just to lock out one single user. I don't feel like this is a good approach for such a thing. If you feel the effort is worth it and you're not afraid to create new policy at domain level and affect every client with it, you can give it a try, that should work.

Be sure to only add the particular user to that since you could easily lock yourself and all users out.

> if he has local admin privileges he shouldnt be able to change domain policies..

If you configure an Administrative Template which is nothing more than a registry entry in the client's registry, "Bob the bad guy" could, using his local administrative rights, change the corresponding registry entry's key and "unlock" whatever you set by (domain) policy. At least he could until the background refresh of Group Policy takes place and your settings get applied again. Then he would have to re−do his "reghacks"...

cheers,

Florian
−−
Microsoft MVP − Windows Server − Group Policy.
eMail: prename [at] frickelsoft [dot] net.
blog: http://www.frickelsoft.net/blog.
.