

# Re: Grant Administrative Access to a Domain Controller

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-12/msg01640](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-12/msg01640)

---

- *From:* "Joe Richards [MVP]" <[humorexpress@xxxxxxxxxxxx](mailto:humorexpress@xxxxxxxxxxxx)>
  - *Date:* Wed, 27 Dec 2006 23:59:46 -0500
- 

Ah that was probably mean.

It bothers me greatly that a company that produces tools for AD including Security type tools has support people that have such a core misunderstanding of AD security and they take the time to post their misunderstandings in a public forum in a seemingly authoritative way.

Again, it is not possible to give admin rights to a single DC or even a set of DCs and then lock those same people out of AD. AD is a subordinate service on a DC meaning an Admin can muck with it in any way they want whenever they want regardless of the permissioning in the directory that you think can be done to prevent it. The fact that your tests show this to be the case illustrates your short comings and lack of understanding versus any AD Security capability.

This isn't something I am guessing about. This is something I know because I have "broken" into several ADs that were allegedly locked down. This is without any fancy tricks or tools. The fancy tricks and tools just make it take seconds instead of minutes. This is something I know also because I have spoken to many of the best AD folks inside and outside of Microsoft including the Dev team over the last 6 years and this is a known weakness in all circles. Again this will be helped a little with Longhorn server, but it still won't be solved for the general case.

—  
Joe Richards Microsoft MVP Windows Server Directory Services  
Author of O'Reilly Active Directory Third Edition  
[www.joeware.net](http://www.joeware.net)

—O'Reilly Active Directory Third Edition now available—

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

Joe Richards [MVP] wrote:

You know as little about Active Directory and Domain Controllers as your coworker.

Seriously, where are you guys coming from?

Re: Grant Administrative Access to a Domain Controller

—  
Joe Richards Microsoft MVP Windows Server Directory Services  
Author of O'Reilly Active Directory Third Edition  
[www.joeware.net](http://www.joeware.net)

—O'Reilly Active Directory Third Edition now available—

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

mfarr wrote:

Archi one other thing . .

To clarify, this user cannot be a member of the domain admins group, but shouldn't be if they are not managing AD. Use the capability of AD to delegate the appropriate rights.

Matt

mfarr wrote:

Archi,

My colleague Mike is correct in saying you can deny access to Active Directory but still allow logon to the DC's. To do this, delegate read only rights to your restricted administrator to everything within AD then add that user to the list of accounts that can log on locally to the dc within the Domain Controller Security Policy. Within the Domain Controller Security Policy are also options to log on as a service, etc for management functionality.

I recommend checking out Active Administrator from Scriptlogic to handle the delegations of control within AD. With Active Administrator you can easily configure these restricted permission within AD for your admins via permissions templates that even self heal. Good luck.

Matt

Re: Grant Administrative Access to a Domain Controller

Archi wrote:

We have a group Domain Server Operators and we need to give them admin rights to domain controllers to restart services, install software and etc. But they should not have rights to Active directory

"Jorge Silva" wrote:

Hi

Can you explain exactly what do you need to do?

also have a look at :

Step-by-Step Guide to Using the Delegation of Control Wizard

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technolog>

--

I hope that the information above helps you.

Have a Nice day.

Jorge Silva

MCSE

"Archi"

<Archi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

<news:24F63807-E425-4294-AFFD-6A36ACD3DB97@xxxxxxxxxxxxxxxxxxxx>

I need to give admin access to domain controllers for a certain domain group but without accessing Active directory. Any options?

Re: Grant Administrative Access to a Domain Controller