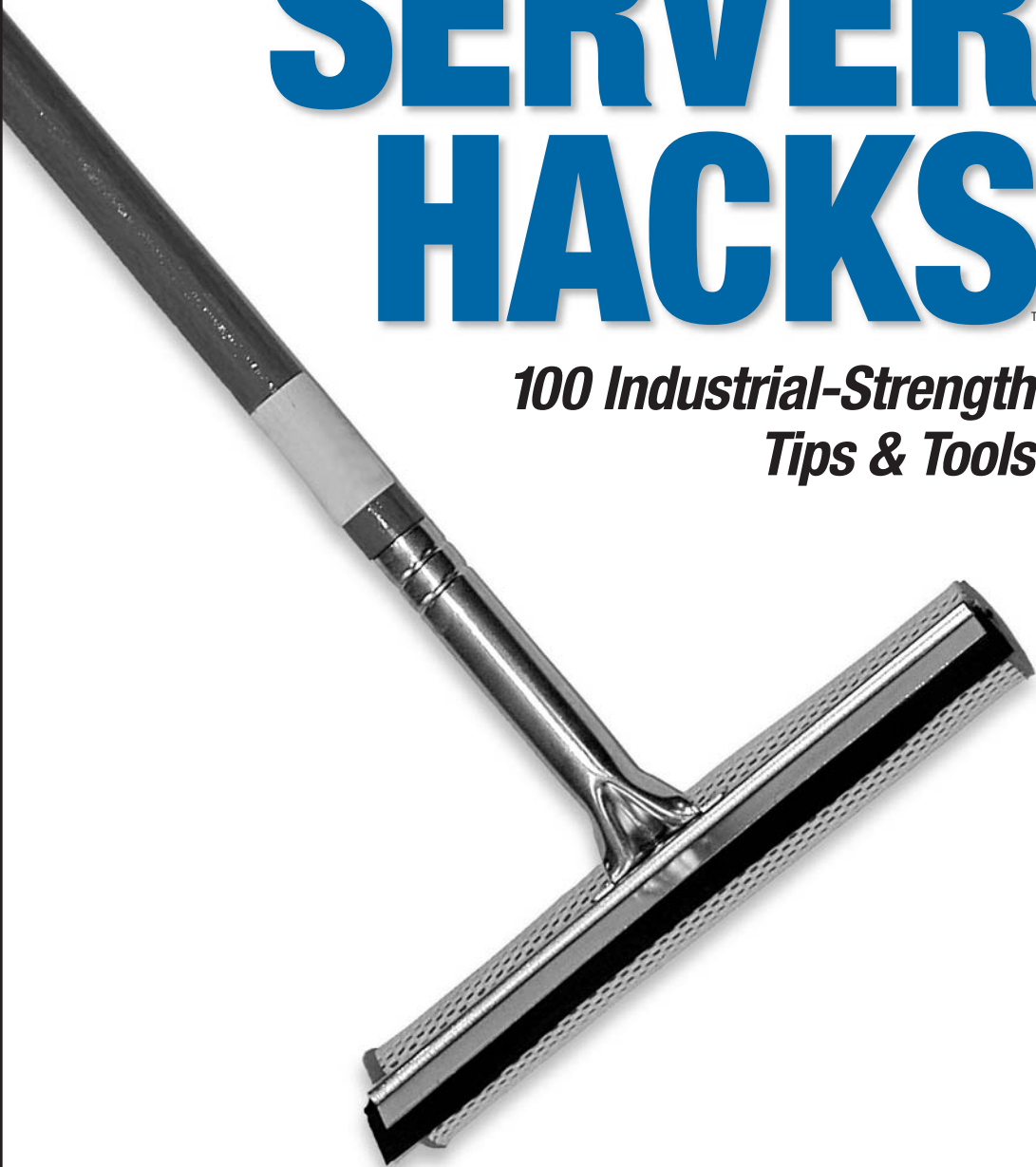


WINDOWS SERVER HACKS™

*100 Industrial-Strength
Tips & Tools*



O'REILLY®

Mitch Tulloch

HACK
#74

Grant Administrative Access to a Domain Controller

Here's a hack that will help you secure any domain controllers you have running at a remote site.

Active Directory has introduced many new levels of complexity to server and security management. For example, if you would like to grant a remote site administrator the rights to install software or services on a domain controller, that person would have to be a domain administrator. Granting that person domain administrator rights introduces the possibility of that user creating new accounts with administrative rights. Obviously, this is not an ideal situation.

The following steps show how to grant a user the same level of rights as an administrator of a member server or a workstation on a domain controller, while preventing that user from having rights to Active Directory.



Please note that this hack does not eliminate all possible security risks, and the users who are granted these rights need to be highly trusted

1. Log onto a domain controller with full domain administrator rights. Make sure your Active Directory domain is in native mode.
2. Inside of Active Directory Users and Computers, create a global security group called DCAdmins. Add all users/groups that will need administrative access to the domain controllers to this group.
3. Create another global security group called DenyDCAdmins.
4. Add the DCAdmins group to the DenyDCAdmins group.
5. Inside of Active Directory Users and Computers, right-click on the domain name and choose Properties. Click on the Security tab (if the Security tab is not available, go to the View menu and choose Advanced).
6. Click on Add and choose the DenyDCAdmins group. Once the group has been selected, click on the Deny checkbox next to Full Control in the Permissions area, as shown in [Figure 8-4](#).

Now, all users or groups that are members of the DCAdmins group have full administrative access to all domain controllers but do not have any access to Active Directory.

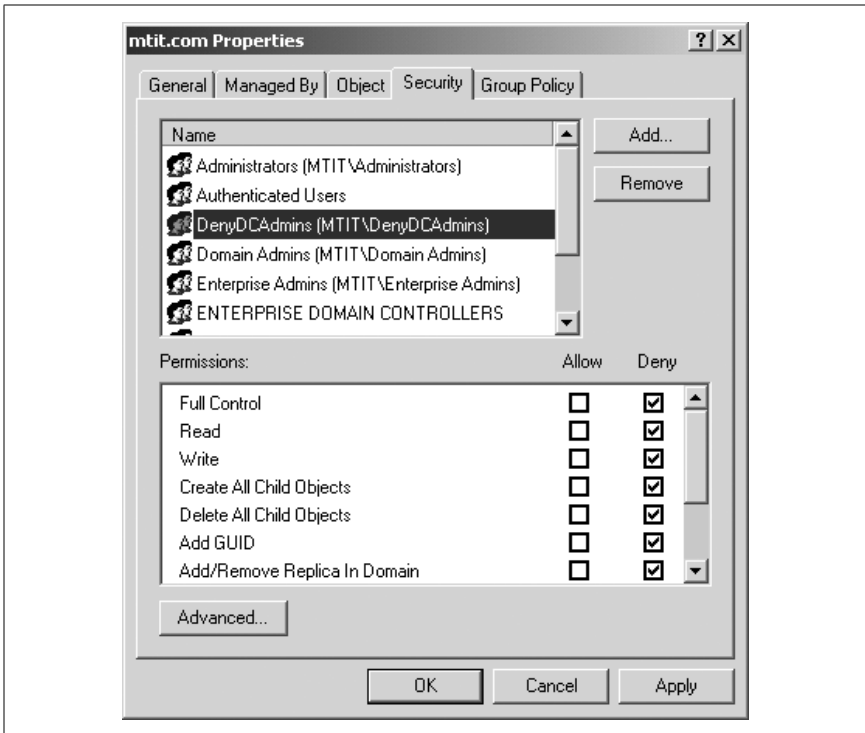


Figure 8-4. Denying Full Control permission for the DenyDCAdmins global group



These users won't even be able to browse Active Directory to apply permissions on shares or files. It is generally a best practice for these users to have two accounts: one for administering the domain controllers and another for day-to-day use.

Overall, this is a great approach to limit security for remote administrators and operations teams that need to be able to make changes on domain controllers. I highly recommend trying this approach before blanketing your Active Directory environment with unnecessary domain administrators.

—Tim Mintner