

Re: What is easier: to delegate or to use ACLs?

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-01/1079.html

From: Joe Richards [MVP] (*humorexpress_at_hotmail.com*)

Date: 01/17/05

Date: Mon, 17 Jan 2005 13:12:02 -0500

No problem, hope it helps out. We used to have quite a few people that would contact us and meet with us to see how we did it. Even then I knew we were unusual on how tight the environment was. I am not a FT consultant for a large technology company and see many many environments now and still think that was the tightest best controlled environment I have seen.

Mostly people don't do a lot of this because they don't realize it is possible, hopefully hearing that it is, helps others reach it.

joe

--

Joe Richards Microsoft MVP Windows Server Directory Services
www.joeware.net

Gera wrote:

> Hm... this is probably the biggest reply in this newsgroup ever ;-)
> And really overwhelming amount of information.

> Thanks, Joe.

>

> --

> Gera

>

> "Joe Richards [MVP]" <humorexpress@hotmail.com> wrote in message

> news:%2310xdfm%23EHA.2580@TK2MSFTNGP15.phx.gbl...

>

>>Password resets are handled by the user provisioning system or through an
>>auto system that we purchased from MTEC called PSYNCH. It allows password
>>resets/unlocks/changes to multiple environments based on RSA token, old
>>password, or Q&A profile through a web site. Initially I had a lot of
>>issues with them in how their stuff worked for various things like they
>>couldn't work with an ID that had basic delegated powers
>>(useraccountcontrol, pwdLastSet, set password, lockouttime) but I
>>eventually beat them into shape. :o) Took about 18 additional months for
>>their product to be launched but I refused to allow them to launch without
>>the product working properly.

>>

>>The reason for the delegation model isn't political. It is for safety and
>>change control due to the lack of business rule logic in Active Directory.
>>You can't enforce naming standards or other standards through the
>>directory so you either need to proxy through some provisioning system
>>(which I don't really consider AD delegation) or pass the tickets to some
>>other group who funnels all of the requests and makes sure the rules are
>>being followed. With the scripts the scripts themselves follow the rules

microsoft.public.windows.server.active_directory: Re: What is easier: to delegate or to use ACLs?

>>so the team with the power isn't even really working it out, they are just
>>trusted to always use the scripts. You can't say that if you give them out
>>to lots of people with rights, they may or may not use them. If the group
>>is small and in slapping distance, they will keep doing it. Especially
>>when they know they are ultimately responsible for the stuff being right.
>>When I left I was slowly working towards having a provisioning website
>>built that actually handled all of our requests that the user provisioning
>>system didn't handle. It was going slow because I was yanked into figuring
>>out the implementation of Exchange 2000. Had that not come up, I would
>>have had it completed before I left and the work could have been done by
>>one person most likely and that person would have been responsible for
>>keeping the website running and break/fix of AD.

>>

>>As for the groups, the company uses a lot of shared data that can be
>>accessed by people all over the world and company but not necessarily
>>whole divisions, groups, departments. Role based security doesn't work
>>very well in many companies and ours was one of them as role based
>>security is often admin'ed in an 80/20 rule. If 80% of a group needs
>>access to something, everyone gets that access instead of having more
>>security groups. We had too many financial and other security rules we had
>>to deal with to allow that much freedom to access to data.

>>

>>The project data structure is such that any owner with a top level shared
>>folder under a project share for a server will generally have at least two
>>security groups. One read-only access group and one read/write group. Some
>>folders also had additional permissions such as maybe ADD only access
>>rights and some had groups for subfolders under the top level folders say
>>like you had a shared web structure that you had people update and it got
>>rolled up to a web server from there.... so say you have a project server
>>with say 100 top level folders for various things. Then you have one of
>>them as a web folder which has subfolders for each group who publishes to
>>the web site controlled by that web folder. You would have a read-only
>>group for all web authors to get into the top level web folder and a
>>read-write for the person who manages the whole structure and then a read
>>only and read-write group for each subfolder. A single project share on a
>>single server could easily eat up hundreds or thousands of groups on its
>>own depending on who was using it and how. Another server may have only
>>4-10 groups. There were also groups used for grouping users together for
>>the IM software we used which was called, I think, SameTime.

>>

>>

>>The 3 domain admins were just that domain admins, 2/3 level support
>>completely. Global operation and our pagers would maybe go off after hours
>>once every couple of weeks and that is only for break/fix and usually
>>because someone didn't understand how the system worked or troubleshot it
>>wrong. You could take all of the group requests or subnet requests say for
>>a whole day and do them all in a few minutes with the scripts, that could
>>be 10 groups or a 1000 groups. Didn't really matter, the scripts just ran
>>a wee bit slower. During initial migrations into AD we were
>>creating/importing thousands of groups a day every day while doing our
>>normal workload as well.

>>

>>The help desk itself is huge and spread across the world and is actually
>>handled by another company for them. They have NO rights inside of AD
>>other than normal user rights so they can look at it. Since there aren't
>>people dorking things up all over the place with mistakes, you don't need
>>a bunch of people that can run around making changes to correct the
>>mistakes.

>>

>>The biggest downside to having only 3 people was around coverage when
>>someone was out for some reason. You have a dual pager system, primary and
>>secondary that way if the primary got shot or something, the secondary

microsoft.public.windows.server.active_directory: Re: What is easier: to delegate or to use ACLs?

>>could fill in. It was a pain when someone went on vacation or got sick or
>>injured or as it started occurring more and more before I left getting
>>pulled off to consult for app developers and integrators in the company so
>>they used Active Directory properly. During normal course of things the
>>team regularly went out to lunch together or some of them would go golfing
>>(with the supervisor) during the day. We could work from home or the
>>office pretty much on the schedules we needed. During the blackout (the
>>main headquarters and our site was right in the middle of all of that) we
>>made our way down to the datacenter, checked out our stuff. Anywhere in
>>the world that had power was up and running fine (including our data
>>centers as we have massive generators that sound like locomotives). Any
>>sites that didn't have power we couldn't do anything about and anyway,
>>they couldn't use our stuff anyway. After the power came back, all of the
>>replication kicked back in and everything was back to normal. We didn't
>>miss a single SLA for break/fix nor new requests due to our redundancy and
>>structuring.

>>

>>AD is a great system because it is very flexible. The people get in
>>trouble though when they take that flexibility and run it in an AD HOC
>>way with little or no controls and that simply isn't reasonable to do in a
>>large enterprise. Very tight change control and fixed ways of doing things
>>(strict processes) are required to have a supportable environment. The
>>more out of control things get the more power you have to start giving out
>>to more people and the more out of control it will get from there. The
>>more people with power to make changes, the more people with power to
>>screw things up.

>>

>>My perfect environment would be one where no users nor local admins have
>>any delegated write power in the directory at all and DA's rarely log on
>>with their DA account, usually just with their normal user account.
>>Everything comes through provisioning systems and has full business logic
>>and logging applied to it. It is possible to do with AD, just takes the
>>initial start up work to do it.

>>

>> joe

>>

>>

>>--

>>Joe Richards Microsoft MVP Windows Server Directory Services
>>www.joeware.net

>>

>>

>>Gera wrote:

>>

>>>Well, from all this I see that there are not much rights delegated to
>>>those

>>>"very local" admins.

>>>As far as I understood, probably not because it is difficult or
>>>impossible,

>>>but because of "political" system of sending such tickets to your support
>>>queue,

>>>which consists of Domain Admin with full rights everywhere. It is also a
>>>type of delegation, "delegation up" ;-)

>>>Also ratio of users (and may be +contacts) to number of groups is

>>>interesting. Or was there computer accounts grouped?...

>>>

>>>I liked the idea of scripting delegation process, of course, in medium to
>>>large env's.

>>>

>>>What about passwords resets? Whom this task was delegated (or not) to?

>>>Probably, to the provisioning system, and

>>>I hope helpdesk wasn't those 3 admins.

microsoft.public.windows.server.active_directory: Re: What is easier: to delegate or to use ACLs?

>>>
>
>
>