

Re: Re: Re: Re: Gradually migrate from Win2000 to Win2003 AD

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2005-01/0044.html

From: Herb Martin (*news_at_LearnQuick.com*)

Date: 01/01/05

Date: Fri, 31 Dec 2004 19:01:11 -0600

- > *Thanks for the info. Windows 2003 is quite new to me so I will have to explore it further.*
- >
- > *You wouldn't happend to know the registry key to change to make all new shares Everyone=Full Control instead of Everyone=Read would you?*
- > *It is the One most annoying thing about Windows 2003 that I haven't figured out how to change.*

No, I don't but were I to know that I might not tell <grin> since it is such a bad idea.

Really, I try to get people to REMOVE all of the Everyone references and substitute (at worst) Authenticated Users, or better the specific groups who should have access.

- > *Who uses Share permissions in W2003, I don't know. Why bother when NTFS is far more effective and adding share permissions only complicates things.*

They both have their value. For one, if you know that a group will never need more than read, you set the share to READ for that group so that you cannot accidentally grant to much through NTFS.

Defense in depth.

You can also use CHANGE on the share to prevent people from changing permissions on their own files or to secure files on FAT, FAT32, etc.

- > *I have never had non-NT clients so I have never seen the need to use share permissions.*

You may not need them in your situation, but those

that make blanket statements to never use them are
not thinking it through.

--

Herb Martin

"lforbes" <UseLinkToEmail@WindowsForumz.com> wrote in message
news:41d5dlb8\$1_4@alt.athenaneews.com...

> "Herb Martin" wrote:

> > > Thanks. I understand the different modes in Windows 2000 and
> > the
> > > benefit of going to native mode in W2k. For me it was the
> > RRAS access
> > > in Group Policy.

> >
> > Yes. I was pretty sure you knew about Win2000 Server
> > mode but it is much easy to discuss the other modes and
> > FFL if you start with those changes and build it
> > incrementally.

> >
> > Most people make the mistake of trying to understand this
> > stuff en masse.

> >
> > > I didn't know you had to be in the Windows 2003 Server mode
> > to rename
> > > a dc.

> >
> > It is greyed out in all Win2000 modes.

> >
> > > Also I didn't know you could rename a domain in 2003. That
> > is
> > > a definite improvement I have been pushing for.

> >
> > There are some limitations so before you depend on it
> > you need to investigate more deeply.

> >
> > > Now if only they would
> > > allow you to merge to pre-existing Forest/Tree/Domains into
> > one
> > > Forest. That is the next step. They should have done this
> > with 2003 in
> > > my opinion. There are too many cases where two companies
> > merge and
> > > don't want to have to dissolve one domain.

> >
> > This is approximated by Forest level trusts. While
> > there is still no true "prune and graft" of domains or
> > Forests, the Forest level trust allows for a single
> > trust between the two forests to be transitive to all
> > domains within those forests (one-way or two-way
> > as an option.)

> >
> > Although the documentation says that Forest trusts
> > are transitive, they are in fact only SEMI-transitive,
> > i.e., a single trust creates an effective trust between
> > all domains in two forests but if a third forest is
> > involved the transitivity does not propagate across
> > FORESTS -- to the next forest.

> >
> > --

> > Herb Martin

> > "lforbes" <UseLinkToEmail@WindowsForumz.com> wrote in message
> > news:41d4bbf7\$1_3@alt.athenaneews.com...

```
> > > "Herb Martin" wrote:
> > &nbsp;&nbsp;&nbsp;> > > However, as I have only played with 2003
> > for a few months I
> > &nbsp;&nbsp;&nbsp;> > wasn't
> > &nbsp;&nbsp;&nbsp;> > aware of the Windows 2003 server mode? What
> > is the advantage
> > &nbsp;&nbsp;&nbsp;> > of this?
> > &nbsp;&nbsp;&nbsp;> > I have all Windows 2003 DC's now and was
> > running in native
> > &nbsp;&nbsp;&nbsp;> > mode before
> > &nbsp;&nbsp;&nbsp;> > the upgrade.
> > &nbsp;&nbsp;&nbsp;> >
> > &nbsp;&nbsp;&nbsp;> > There were only two modes for Domains (and none
> > &nbsp;&nbsp;&nbsp;> > for Forests) in Win2000.
> > &nbsp;&nbsp;&nbsp;> >
> > &nbsp;&nbsp;&nbsp;> > Win2003 adds several; there are now 4 modes for
> > &nbsp;&nbsp;&nbsp;> > domains and 3 "functional levels" for forests --
> > many
> > &nbsp;&nbsp;&nbsp;> > people use the term "functional mode" for both
> > forests
> > &nbsp;&nbsp;&nbsp;> > and domains but I prefer to keep the distinct terms
> > for
> > &nbsp;&nbsp;&nbsp;> > clarity.
> > &nbsp;&nbsp;&nbsp;> >
> > &nbsp;&nbsp;&nbsp;> > Domain modes:
> > &nbsp;&nbsp;&nbsp;> > 1) Mixed mode -- the default (available in
> > Win2000)
> > &nbsp;&nbsp;&nbsp;> > 2) Native mode -requires all Win2000+ DCs,
> > i.e., no BDCs
> > &nbsp;&nbsp;&nbsp;> > (available in Win2000
> > &nbsp;&nbsp;&nbsp;> > 3) Interrim (new to Win2003) allows BDCs but no
> > Win2000
> > &nbsp;&nbsp;&nbsp;> > 4) Win2003 Server mode (Win2003 DCs ONLY)
> > &nbsp;&nbsp;&nbsp;> > (this has also been called Win2003
> > Native mode at
> > &nbsp;&nbsp;&nbsp;> > times)
> > &nbsp;&nbsp;&nbsp;> >
> > &nbsp;&nbsp;&nbsp;> > Forest functional levels:
> > &nbsp;&nbsp;&nbsp;> >
> > &nbsp;&nbsp;&nbsp;> > 1) Windows 2000 FFL (roughly equivalent to
> > Mixed
> > &nbsp;&nbsp;&nbsp;> > mode at the domain level)
> > &nbsp;&nbsp;&nbsp;> > 2) Win2003 Interrim FFL (mostly improves
> > replication
> > &nbsp;&nbsp;&nbsp;> > behavior since no Win2000 DCs are/can
> > be involved.
> > &nbsp;&nbsp;&nbsp;> > 3) Windows 2003 -- enables things like Forest
> > level trusts
> > &nbsp;&nbsp;&nbsp;> > and domain rename (since the entire forest
> > is now
> > &nbsp;&nbsp;&nbsp;> > Win2003
> > &nbsp;&nbsp;&nbsp;> > DC and will not be confused by such
> > changes.)
> > &nbsp;&nbsp;&nbsp;> > Also "Defunteing" (yes, it's a verb) of
> > Schema object
> > &nbsp;&nbsp;&nbsp;> > additions
> > &nbsp;&nbsp;&nbsp;> >
> > &nbsp;&nbsp;&nbsp;> > There are various improvements but the simplest way
> > &nbsp;&nbsp;&nbsp;> > to understand the difference between Native and
> > Mixed
> > &nbsp;&nbsp;&nbsp;> > (available even in Win2000) is that anything that
> > would
```

microsoft.public.win2000.active_directory: Re: Re: Re: Re: Gradually migrate from Win2000 to Win2003 AD

> > > > confuse an NT-BDC is not allowed.
> > > >
> > > > Note that Native mode is practically a DC issue and
> > has
> > > > NO direct effect on legacy clients. Some
> > improvements
> > > > include (not a full list): Group nesting and
> > Universal
> > > > groups, improved support for migrating users INTO
> > the
> > > > domain, dropping of the SAM (and any practically
> > limits
> > > > on domain size) by the PDC-emulator (which is STILL
> > > > needed), improvements to RRAS for users (Policy
> > grant
> > > > and deny of access, IP assignment etc.), most group
> > type
> > > > conversions,
> > > >
> > > > The main improvements for Win2003 Server DOMAIN
> > mode
> > > > are Domain controller rename, InetOrgPerson
> > password
> > > > (can be used in place of User account object), and
> > the
> > > > updating of the last logon time -- really though
> > for most
> > > > people, the real reason for Win2003 mode at the
> > domain
> > > > is that all domains must be here to reach Win2003
> > FFL
> > > > on the Forest.
> > > >
> > > >
> > > > <
> > > >
> >

<http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default>

> > > > > >
> > > >
> > > > --
> > > > Herb Martin
> > > >
> > > >
> > > > "lforbes" <UseLinkToEmail@WindowsForumz.com>
> > wrote in message
> > > > news:41d44fe3\$1_1@alt.athenaneews.com...
> > > > > > Hi,
> > > > > >
> > > > >> > You cannot raise a Domain level to
> > "Win2003 Server
> > > > mode"
> > > > >> > until ALL DCs in domain run
> > Win2003.
> > > > >> >
> > > > >> > You cannot raise the Forest level
> > to "Win2003
> > > > Forest Functional
> > > > >> > Level" until ALL DOMAINS are at
> > "Win2003 Server
> > > > Mode",
> > > > >> > and thus until all DCs in Forest

microsoft.public.win2000.active_directory: Re: Re: Re: Re: Gradually migrate from Win2000 to Win2003 AD

> > are running
> > > > Win2003.
> > > > >> >
> > > > > >
> > > > > > I just returned from a year off on
> > Maternity leave. My
> > > > replacement
> > > > > > upgraded both my domains from windows 2000
> > to windows 2003
> > > > in one day
> > > > > > basically running the install off the CD.
> > Things went really
> > > > smootly
> > > > > > and there were no issues. I felt no need to
> > do a completely
> > > > new
> > > > > > install of 2003 because of how similar it
> > was to 2000
> > > > (unlike with
> > > > > > NT).
> > > > > >
> > > > > > However, as I have only played with 2003
> > for a few months I
> > > > wasn't
> > > > > > aware of the Windows 2003 server mode? What
> > is the advantage
> > > > of this?
> > > > > > I have all Windows 2003 DC's now and was
> > running in native
> > > > mode before
> > > > > > the upgrade.
> > > > > >
> > > > > > Cheers,
> > > > > >
> > > > > > Lara
> > > > > >
> > > > > > --
> > > > > > <http://www.WindowsForumz.com/> This article
> > was posted by author's
> > request
> > > > > > Articles individually checked for
> > conformance to usenet
> > > > standards
> > > > > > Topic URL:
> > > >
> >

<http://www.WindowsForumz.com/Active-Directory-Gradually-migrate-Win2000-Win2003-AD-ftopic242271>.

> > > > > > Visit Topic URL to contact author (reg.
> > req'd). Report
> > > > abuse:
> > > > <http://www.WindowsForumz.com/eform.php?p=740977>
> > >
> > > Hi,
> > >
> > > Thanks. I understand the different modes in Windows 2000 and
> > the
> > > benefit of going to native mode in W2k. For me it was the
> > RRAS access
> > > in Group Policy.
> > >
> > > I didn't know you had to be in the Windows 2003 Server mode
> > to rename

microsoft.public.win2000.active_directory: Re: Re: Re: Re: Gradually migrate from Win2000 to Win2003 AD

> > > a dc. Also I didn't know you could rename a domain in 2003.
> > That is
> > > a definite improvement I have been pushing for. Now if only
> > they would
> > > allow you to merge to pre-existing Forest/Tree/Domains into
> > one
> > > Forest. That is the next step. They should have done this
> > with 2003 in
> > > my opinion. There are too many cases where two companies
> > merge and
> > > don't want to have to dissolve one domain.
> > >
> > > Cheers,
> > >
> > > Lara
>
> Hi,
>
> Thanks for the info. Windows 2003 is quite new to me so I will have to
> explore it further.
>
> You wouldn't happen to know the registry key to change to make all
> new shares Everyone=Full Control instead of Everyone=Read would you?
> It is the One most annoying thing about Windows 2003 that I haven't
> figured out how to change.
>
> Who uses Share permissions in W2003, I don't know. Why bother when
> NTFS is far more effective and adding share permissions only
> complicates things. I have never had non-NT clients so I have never
> seen the need to use share permissions.
>
> Cheers,
>
> Lara
>
> --
> <http://www.WindowsForumz.com/> This article was posted by author's request
> Articles individually checked for conformance to usenet standards
> Topic URL:
> <http://www.WindowsForumz.com/Active-Directory-Gradually-migrate-Win2000-Win2003-AD-ftopic242271>.
> Visit Topic URL to contact author (reg. req'd). Report abuse:
> <http://www.WindowsForumz.com/eform.php?p=743379>