

Re: the "." zone

Source: <http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.dns/2004-03/0053.html>

From: the confused (*anonymous_at_discussions.microsoft.com*)

Date: 03/01/04

Date: Mon, 1 Mar 2004 07:07:37 -0800

What I meant is to set up the internal and external namespace, for obvious security reasons, there are needs to set up "." zones for the internal name spaces. In this case, yes, proxy is used.

Did anyone mentioned that deleting "." zone can be a security measure? I haven't follow all the threads closely.

>-----Original Message-----

>I wouldn't say that's a requirement unless you want to block Internet access

>or you are using Proxy or ISA.

>

>Just deleting the Root zone is NOT a security measure on it's own.

>

>--

>Regards,

>Ace

>

>Please direct all replies to the newsgroup so all can benefit.

>This posting is provided "AS IS" with no warranties.

>

>Ace Fekay, MCSE 2000, MCSE+I, MCSA, MCT, MVP

>Microsoft Windows MVP – Active Directory

>--

>=====

>

>"the confused" <anonymous@discussions.microsoft.com> wrote in message

>news:44c301c3ff44\$9a592ba0\$a501280a@phx.gbl...

>

>For security reasons, more and more companies want their internal and external name space to be separated, so

>there are real needs to set up "." zones for the internal
>spaces.
>
>
>>-----Original Message-----
>>It was a "mistake" :) MS assumed that we all want to use
>our DNS server in a
>>fortress (or an Island), so they automatically configure
>a Win2K server to be
>>a root server. In the root mode, the server believes
>that it is the "end of
>>the world" and any record it does not currently have
>does not exist. So, in
>>this mode, when the server receives a query for
>www.sendasalami.com, it
>>looks at itself (ONLY) and goes, "hmmmm.. nothing here.
>Sorry. Don't exist".
>>It never attempts to ask the people who would really
>know about salamis and
>>other food stuffs (in this case, the REAL Root servers).
>>
>>MS heard about this from many sources and they realized
>that there aren't
>>that not that many people have their own Island, so they
>fixed it in Win2K3.
>>
>>So, the long and short of the story: In Win2K DNS, you
>will see a "." zone.
>>Unless you really run this network in isolation from the
>rest of the world
>>and you, therefore, have no need to resolve external
>records, ALWAYS delete
>>this "." zone and move on.
>>--
>>Sincerely,
>>
>>Dèjì Akómöláfé, MCSE MCSA MCP+I
>>www.akomolafe.com
>>www.iyaburo.com
>>Do you now realize that Today is the Tomorrow you were
>worried about
>>Yesterday? -anon
>>"the confused" <anonymous@discussions.microsoft.com>
>wrote in message
>>news:186101c3fed9\$893c13c0\$a601280a@phx.gbl...
>>>
>>> In 291382, the following is listed as one of the
common
>>> mistakes that is made when administrators set up DNS
on
>>> network that contains a single Windows 2000 or Windows

>>> *Server 2003 domain controller:*
>>>
>>> *The "." zone exists under forward lookup zones in DNS.*
>>>
>>> *What does this mean? I thought this "." zone is set up*
>*in*
>>> *the forward lookup zones by default, when needing a*
>>> *separate name space.*
>>>
>>> *Or, the "." zone was set up by default there,*
>*regardless*
>>> *whether you need a separate space or not, in a early*
MS
>>> *DNS (heard this' a before 2003 feature)?*
>>>
>>> *In addition, if it should be there by default for a*
>>> *saparate name space, I would think it should be a*
level
>>> *up, i.e., both of the foward and reverse zones should*
>*be*
>>> *under the "." domain, not that the "." zone being*
under
>>> *forward zones, and including both forward*
domains/zones
>>> *and reverse domains. I think this way would make more*
>>> *sense, if MS wants to list separately the forward and*
>>> *reverse zones.*
>>>
>>> *Anyone can shed some light on this? Thanks!*
>>>
>>>
>>
>>
>>
>>
>>
>>
>>
>
>
>
>
>