

Re: Authentication accross child domains

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-08/msg01201

- *From:* "Sean M. Loftus" <sean(remove me)@loftus.org>
 - *Date:* Tue, 16 Aug 2005 11:50:58 -0400
-

I'll take a look at that guide...

I would say yes we are using the transitive trust mechanism. I've been thinking a shortcut trust may be in order, but I never had this problem before and usually the shortcut trust it to speed up slow logons that have to walk the tree in large forest implementations so I was hesitant to just put one in.

DomainA computers "are" allowed to talk to DomainB DC's, as stated in my previous post all ports to the child domains are open that need to be (I may have neglected to list all ports in the post).

That's why I find it strange, it should do a lookup on the local domain DNS for SRV records and GC for objects to do the authentication, should it not?

DNS should do a DC to DC DNS lookup for SRV records and return them to the client, since the _msdcs zone is in the root I would expect that behavior, but why an LDAP connection?

The client should not be waking the tree, the DC should be referring it to the other child domain.

Sean

"Al Mulnick" <amulnick_No_SPAM@xxxxxxxxxxxx> wrote in message <news:eLgwFFmoFHA.3316@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

- > In looking at your post, it sounds like it's using the transitive trust
- > mechanism to authenticate the domainb client (using domaina computer) to
- > access resources. To do that, I would think a transitive trust would have
- > to be used so that the kerberos authentication could succeed. I'm guessing
- > that your policy doesn't allow the domaina computer to talk to domainb
- > dc's either?
- >
- > Since they're part of the same forest, that would not be a surprise that
- > the client would try and talk to the root in this scenario.
- >
- > Have you already seen the branch office deployment guide? I think that

Re: Authentication accross child domains

> most closely matches your scenario and goals and might offer some tips as
> to how you might control the traffic differently.
>
> Al
>
> "Sean M. Loftus" <sean(remove me)@loftus.org> wrote in message
> news:esRPiEcoFHA.2484@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>> I have a Windows 2003 Forest, in 2003 mode. We have 1 root domain and 2
>> child domains connected to the root as separate trees. All DC are
>> integrated DNS servers and there is 1 GC in each domain (not on infrast
>> mstr). All DC are on the same subnet and behind a firewall. The child
>> domains are allowed to communicate through the firewall for
>> authentication traffic, DNS etc (389, 3268, 53, 88, 445 etc.) and the
>> ROOT is allowed to communicate with all DCs in the forest unrestricted
>> (do to them being on the same subnet) and do internet DNS lookups, but no
>> client is allowed to communicate with them. DNS is also forwarded up
>> through the root to resolve internet queries.
>>
>> I have a computer joined to child DomainA and a "user" from child DomainA
>> using a UPN can logon without any issues. However when a "user" from
>> child DomainB logs onto the same machine in child DomainA using a UPN it
>> makes LDAP 389 and Kerberos 88 call to the ROOT DC's when trying to
>> connect to SMB shares and changing passwords, we have verified this with
>> packet captures. Because we don't allow clients to talk to the root this
>> fails.
>>
>> Can anyone shed some light on what's going on here, I thought the GC and
>> SRV records lookup would tell the child DomainA servers where the child
>> DomainB services are and forward the client calls to there not the root.
>> Is it because the UPN needs to do a top down lookup? Do I need a shortcut
>> trust to prevent this from walking the tree to resolve calls to the other
>> child domain? I've never run into this particular issue before with
>> either version of AD.
>>
>> Thanks in advance for any information helping me understand this issue.
>>
>> --
>> Sean M. Loftus
>> Enterprise Architect
>> Loftus Consulting, Inc.
>> www.LoftusConsulting.com
>> sean(removeme)@loftus.org
>>
>
>

Re: Authentication accross child domains

- ***Follow-Ups:***
 - ◆ ***Re: Authentication accross child domains***
 - ◇ *From: Al Mulnick*

- ***References:***
 - ◆ ***Authentication accross child domains***
 - ◇ *From: Sean M. Loftus*
 - ◆ ***Re: Authentication accross child domains***
 - ◇ *From: Al Mulnick*

- Prev by Date: ***Re: GPMC 1.02***
- Next by Date: ***RE: Setup GPO to map drive without using scripts***
- Previous by thread: ***Re: Authentication accross child domains***
- Next by thread: ***Re: Authentication accross child domains***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***