

Re: User authentication and access to "sister" domain resources

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2005-01/0112.html

From: Ryan Hanisco (*rhanisco_at_flagshipis.com*)

Date: 01/03/05

Date: Mon, 3 Jan 2005 15:53:04 -0600

Gera,

Why is it that you want different domains at every site? It seems to make a lot more sense to keep everything in one domain and define sites, delegating administration. You really haven't given any really reason to segregate domains -- political need, reflecting an NT4 structure from legacy (not too valid a reason), need for boundaries in your Domain Security Policy.

What you are listing is exactly what I would do in an NT4 scenario, but this doesn't seem like the way to go with AD. Make sure your site links are set up correctly and your DNS is AD Integrated and you should be able to do everything you need with OUs and Groups.

As to SUS... I have never tried doing updates from outside the domain, but I don't see why it wouldn't work as long as the host can resolve the server name and the SUS policy is set in the local domain.

--

Ryan Hanisco

MCSE, MCDBA

Flagship Integration Services

"Gera" <Gera@discussions.microsoft.com> wrote in message
news:4E3742D4-47E7-4BD6-837E-D0159C5EAEBC@microsoft.com...

> [this is a long question, and difficult too]

>

> I am in process of designing brand new AD structure for our customer.

> A geographic placement is: 3 locations, let's say site A, site B and site C,

> connected with 2 mbit links.

>

> I propose a design with root domain and three child domains all with Windows

> 2003 Servers - pretty classic design (let's say, sites coincide with domains).

> Every location (site) with 2 DCs for every child domain and one rootDC1 in

> siteA and another rootDC2 in siteB.

> All DCs are Global Catalogs.

>

> A customer has some traveling users (notebooks with DHCP in use probably),

> which should have possibility to login in any site and have access to

microsoft.public.win2000.active_directory: Re: User authentication and access to "sister" domain resources

```
local
> (domain B) printers and files.
>
> Situation in question is:
> - group membership is by AGLP rule
> - user_from_domainA arrives in siteB
> - user_from_domainA gets IP address from siteB DHCP server
> - user_from_domainA is trying to make logon in his remote DC in siteA
while
> sitting in siteB
> - link to all DCs from domain A is suddenly broken, user_from_domainA PC
can
> log in using cached credentials
> - links to nearest rootDC and domainB DCs are ok
> - user_from_domainA still needs to print (or share files) to domainB
printers
> - user_from_domainA doesn't have any accounts in domainB
>
> What will happen in this situation? I can't test t
```