

How To Force LDAP Queries Through One Domain?

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-12/msg00994

- *From:* "Will" <westes-usc@xxxxxxxxxxxxxxxx>
 - *Date:* Sat, 17 Dec 2005 20:28:11 -0800
-

When you login to a domain on a computer that is a member server in the domain, and then create an ACL against a file that refers to entities in other domains in the same forest, it appears that the LDAP query is placed directly to the domain controllers for each domain you reference in the ACL. I can see this in the firewall log pretty clearly (there is a firewall between the clients and the domain controllers). Is there any way to configure a client or its member domain's DC so that the LDAP queries for entities in other domains go through the member server's domain as a proxy for the other domains? I want to avoid the direct contact between the computer that is a member server of a domain and the DCs of any other domain.

Would this behavior be any different if the domains were in different forests with a trust between them? In the case of a trust, where a user on a member server logged into its domain creates an ACL on a file that references a trusted domain, will the LDAP queries go directly to the trusted domain's DC? Is there any way to stop that behavior?

--
Will

-
- *Follow-Ups:*
 - ◆ **[Re: How To Force LDAP Queries Through One Domain?](#)**
 - ◇ *From:* Todd J Heron
 - Prev by Date: **[Re: DCPromo failing on a W2k3 R2 server](#)**
 - Next by Date: **[Re: How to distribute a certificate to many trusted publisher stores](#)**
 - Previous by thread: **[Re: DCPromo failing on a W2k3 R2 server](#)**
 - Next by thread: **[Re: How To Force LDAP Queries Through One Domain?](#)**
 - Index(es):
 - ◆ **[Date](#)**

How To Force LDAP Queries Through One Domain?

◆ *Thread*