

Kerberos realm referral problem

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-09/msg01589

- *From:* WesE <WesE@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 30 Sep 2008 13:11:03 -0700
-

Hello,

I am troubleshooting what I believe to be a Kerberos realm referral problem. This is all Win 2003 and XP.

The environment looks like this: resource servers are in the peanut.com domain, the users are in the cashew.nut domain. Peanut.com is a single domain forest. Cashew is the child domain of nut. Peanut.com trusts cashew.nut, this is an external trust. Users in cashew.nut access resources in peanut.com There is no DNS forwarding between the domains/forest, all DNS records have been created manually.

Now the question. When user1, in cashew.nut, requests a ticket for RPCSS\server1.peanut.com, the ticket request is sent to the KDC/DC in cashew.nut. I think this shouldn't be a problem since the KDC should respond with a referral to the KDC/DC in the peanut.com domain. However this doesn't happen, instead the KDC/DC responds with KDC_ERR_S_PRINCIPAL_UNKNOWN and thats the end of it, the system proceeds with NTLM authen. Presumably there is some DNS misconfiguration somewhere that is causing the referral to fail however I have been unable to determine exactly what info the KDC uses in making the decision to provide a referral. The best description I can find is here <http://tools.ietf.org/html/draft-ietf-krb-wg-kerberos-referrals-11>

A little guidance on what needs to be in place for the referral to work would be really appreciated.

Thanks,

-Wes