

Traveling Users Unable to Authenticate to AD

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-03/0606.html

From: Scott (*Scott_at_discussions.microsoft.com*)

Date: 03/06/05

Date: Sun, 6 Mar 2005 09:31:01 -0800

Statement of Problem:

Laptop users from MYCO traveling to OTHERCO (Novell NDS location with no AD) are unable to authenticate to MYCO.US.GRPLEG.COM Active Directory.

Required Result:

To enable laptop users from MYCO traveling to OTHERCO to authenticate to MYCO.US.GRPLEG.COM Active Directory, get their mapped drives, access to file shares, etc.

Background Information:

Overseas parent company does not allow delegation/forwarding from/to their UNIX BIND 9.2 DNS servers to W2k3 Active Directory DNS;

Parent company (not on Active Directory) is authoritative for DNS root zone: PARENT.COM. Neither name server records nor SOA records are allowed to be populated in any of the parent company-hosted DNS zones;

Parent company is also authoritative 1st level DNS zone: US.PARENT.COM (this zone is hosted overseas);

Our company's dual-authoritative AD-integrated and UNIX DNS zone: MYCO.US.PARENT.COM (from parent company perspective the UNIX servers are authoritative, from our company's internal client/server systems W2k3 DNS is authoritative);

The W2k3 Active Directory DNS servers conditionally forward queries for PARENT.COM and all child domains of PARENT.COM other than MYCO.US.PARENT.COM to MYCO's UNIX BIND DNS servers. This has worked fine.

Affiliated, WAN-connected US company with Novell DNS zone OTHERCO.US.GRPLEG.COM (unable to conditionally forward and not in budget to perform necessary upgrade to OS to enable this feature);

microsoft.public.windows.server.active_directory: Traveling Users Unable to Authenticate to AD

Within a year, both the parent company and otherco will be migrated to a globally-unified Active Directory implementation in a completely different namespace so that this will cease to be a problem.

Discussion:

I believe the reason that laptop users from MYCO traveling to OTHERCO are unable to authenticate to MYCO.US.GRPLEG.COM Active Directory is that the OTHERCO DNS server sends packets to the US.PARENT.COM zone which looks to the UNIX BIND servers of MYCO.US.PARENT.COM for resolution—the UNIX BIND servers have the A records for the W2k3 DC DNS servers don't have the SRV and LDAP records necessary to enable authentication to the MYCO DCs running DNS.

Without spending a lot of \$\$ and without having to deploy an additional MYCO DC/DNS server at otherco, we need a temporary workaround so that the traveling users can authenticate.