

Re: How does authentication work?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2007-11/msg00695.html>

- *From:* "The_Nite_Owl" <the_nite_owl@xxxxxxxxxxx>
 - *Date:* Fri, 16 Nov 2007 12:59:41 -0500
-

I can only guess as to the authentication. I would think that Kerberos is used but I do not know if the SAN configuration changes or adds to the authentication process. I have no idea how the SAN shares are setup and do not have access to them to investigate.

The connection does not drop every day and it is hard to tell when it occurs as it usually happens during the evening and early morning hours when nobody is here. We do not find out until a job tries to process and fails on our application server and someone has to investigate. So we have no idea how long before that job tried to run the connection might have dropped.

Our application server has 10 drive mappings. 6 of those mappings go to three different servers using the same domain account and have no problems with their connections. 4 mappings go to different folders on the SAN server and they fail intermittently.

My own XP device (and my team mates as well) have the same mappings to the SAN shares using the domain account credentials and we never have these issues.

I believe it is a combination of Win Server 2003 not caching (XP does cache) and some timeout on the SAN server. The non 2003 servers we map to do not fail and mappings to the SAN server from non-2003 devices do not fail.

"Joseph T Corey" <jcorey@xxxxxxxxxxxxxxxx> wrote in message <news:FC6E1526-82C8-44E9-8018-58610C7BCDB8@xxxxxxxxxxxxxxxx>

Assuming that these two machines are authenticating via Kerberos, the maximum lifetime of a service ticket (by default) is 600 minutes (10 hours). This is configurable via Group Policy (Computer Configuration\Windows Settings\Security Settings\Kerberos Policy\Maximum Lifetime for a Service Ticket). The downside to increasing this amount is that a user may continue to access a resource long after their account is disabled, or some other threshold (like logon hours) is met.

I'm not a Kerberos expert so that's where my advice will stop.

--

Re: How does authentication work?

Joseph T. Corey MCSE, Security+
Systems Administrator
jcorey@xxxxxxx

"The_Nite_Owl" <the_nite_owl@xxxxxxxxxxxx> wrote in message
<news:%23Ira%23sEKIHA.4688@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

When a device attempts to connect to a shared drive on another server it is the remote server that requests the credentials to authenticate the connection right?

What determines how long the connection can remain before the remote server requests authentication again?

We have a Win 2003 server that maps drives to SAN sharespace through another Win 2003 server.

The drive mappings are made using a different set of credentials than the current logged on account.

Win 2003 server after SP1 no longer caches credentials for connections using a different account than the logon account.

When we boot our server the mappings are established but the drives do not connect until you click on one of them in Windows Explorer which pops up an ID/Password prompt (because it will not store the credentials). Once the credentials are entered the connection works. If the connection is unused for 15 minutes the remote server auto-disconnects the connection as it should but when the connection is accessed again it is re-established. This works as expected but in something less than 48 hours the connection dies and clicking on the drive in Explorer pulls back an error. The mappings have to be deleted and re-added which forces a new authentication prompt and then the connection works again.

I believe that when the remote server receives valid authentication credentials that it sets the connection to be allowed from that remote device for a specified time after which it requires re-authentication which our server cannot provide because it does not cache credentials for connections using a different logon id/password.

What could be governing the time the connection can remain before needing re-authentication?

Our Network Engineering team just shrug their shoulders and say it is not on their end.