

Re: Confusing Kerberos Error

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2007-01/msg00575.html>

- *From:* "Sibine" <simon.jessop@xxxxxxxxxx>
 - *Date:* 15 Jan 2007 03:06:59 -0800
-

Hi Brian,

I think I'm with you on the DNS error. I have a new machine with me today onsite and I've plugged it into the network and got myself online without logging onto the domain so i'm not authenticated with the box. As such I note the server event log is again full of the errors.

I'm going to compare the 2 DNS servers and just make sure they are both identical and not mis-configured and then I'll come back to you.

Anything obvious I could be looking for would be appreciated. Times seem to be irrelevant as I've set my machine to exactly the same time as the sever (down to the second haha) and it still occurs.

Many thanks,

Simon

Brian Delaney [MSFT] wrote:

Hi Simon,

This error is typically caused by a DNS error, or incorrect SPN registration. When you request a kerberos ticket the request is made to a KDC with the SPN in the form service/servername. The KDC takes this request and searches the AD DB for any objects with the SPN specified in the request in the serviceprincipalname attribute. The kerberos ticket is then encrypted with the password of the security principal the SPN was found in. The CIFS service is covered by the host/servername SPN.

If this were a DNS problem the situation would progress something like this: A User requests authentication for fileserver1. The host SPN for fileserver1 is located in the fileserver1 computer account and a ticket is provided encrypted with fileserver1's password. DNS however is directing fileserver1's name to the IP address of fileserver2. The error will then be logged as the ticket provided to fileserver2 is encrypted with a password that fileserver2 cannot decrypt.

Re: Confusing Kerberos Error

If this were an SPN registration problem the situation would progress like this:

A user requests authentication for fileserver1. The host SPN for fileserver1 is located on the fileserver2 computer account and a ticket is provided encrypted with fileserver2's password. DNS directs the client to fileserver1 but since the ticket is encrypted with fileserver2's password the error is thrown as it cannot be decrypted.

It would not be common for this error to be thrown by a time skew alone as the ticket can be successfully decrypted as the password is still the same, however the authenticator is too far in the past or future. This would typically throw a different error, KRB_AP_ERR_SKEW.

Hope this helps,

Brian Delaney
Microsoft Canada

--

This posting is provided "AS IS" with no warranties, and confers no rights.

From: "Sibine" <simon.jessop@xxxxxxxxxx>
Newsgroups: microsoft.public.windows.server.general
Subject: Confusing Kerberos Error
Date: 5 Jan 2007 09:04:16 -0800
Organization: <http://groups.google.com>

The main Server at a site which has 3 servers (login, file server, exchange server) has started reporting these errors.

I've had a nose through and I wanted to follow up a previous topic but its now expired.

This is the error: (edited for security)

The kerberos client received a KRB_AP_ERR_MODIFIED error from the server workstation\$. The target name used was cifs/*****.*****.co.uk. This indicates that the password used to encrypt the kerberos service ticket is different than that on the target server. Commonly, this is due to identically named machine accounts in the target realm (*****.*****.com), and the client realm. Please contact your system administrator.

I've seen a few people pointing towards maybe a clock problem on the workstations or maybe checking the DNS for a problem. Can anyone assist in helping pointing me in the right direction? If it is a DNS issue, what am I looking for and where might I find it?

Re: Confusing Kerberos Error

Many thanks,

Simon