

Re: ADAM Bind to alias pointing local server fails

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-02/msg01831

- *From:* "Lee Flight" <lef@xxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 21 Feb 2006 23:48:20 -0000
-

Hi

you do not want duplicate SPNs that will break the Kerberos auth. I do not think you can set up failover for kerberos logons without some sort of middle tier. You can use NLB for LDAP/LDAPS connections but I am not sure that would work for kerberos SASL bind. Eric from Microsoft is the expert in this area maybe he will spot this thread.

Connecting to the alias from another machine I cannot explain are you sure that it was a kerberos auth and not NTLM? I do not think you can avoid this by messing with DNS e.g. using a CNAME rather than an additional A record, in short I would expect the SPN to be required. If you confirm that is not the case I'd be interested to hear.

Thanks

Lee Flight

"Craig Gilmour" <CraigGilmour@xxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:91DCA21E-EBE6-42DC-BB64-7C186A747D9E@xxxxxxxxxxxxxxxxxx>

Lee,
thanks very much for this pointer. It fixed the problem. I plan to have an ADAM replica that I will failover to if necessary. Should I simply add the SPN to the other server's AD entry as well or will having the same entries against two different servers cause a problem?

Also, what I a little confused about though is why I could connect to this DNS alias from another machine without a problem. In fact at other deployments I have never added the SPN's - I always accessed the ADAM instance from another server. Does Windows do the DNS translation back to the actual host name prior to presenting the query?

In case anyone else is interested, the following are the SPN's I wrote:

c:\windows\adam\repadmin.exe /writespn mydc.mydomain.com ADD

Re: ADAM Bind to alias pointing local server fails

```
"CN=ADAMSERVER,CN=Computers,DC=corp,DC=riotinto,DC=org"  
ldap/adam.mydomain.com  
c:\windows\adam\repadmin.exe /writespn mydc.mydomain.com ADD  
"CN=ADAMSERVER,CN=Computers,DC=corp,DC=riotinto,DC=org"  
ldap/adam.mydomain.com:389  
c:\windows\adam\repadmin.exe /writespn mydc.mydomain.com ADD  
"CN=ADAMSERVER,CN=Computers,DC=corp,DC=riotinto,DC=org"  
ldaps/adam.mydomain.com:636  
c:\windows\adam\repadmin.exe /writespn mydc.mydomain.com ADD  
"CN=ADAMSERVER,CN=Computers,DC=corp,DC=riotinto,DC=org" ldap/adam  
c:\windows\adam\repadmin.exe /writespn mydc.mydomain.com ADD  
"CN=ADAMSERVER,CN=Computers,DC=corp,DC=riotinto,DC=org" ldap/adam:389  
c:\windows\adam\repadmin.exe /writespn mydc.mydomain.com ADD  
"CN=ADAMSERVER,CN=Computers,DC=corp,DC=riotinto,DC=org" ldaps/adam:636
```

"Lee Flight" wrote:

Hi

in negotiated authentication you will need to update the
servicePrincipalName
attribute of the computer account that hosts the ADAM instance to add
access
for LDAP against the DNS alias in order for Kerberos access to work. You
can do this from the command line using setspn.exe.

```
setspn <netbiosname of ADAM machine>
```

to list the current SPNs you should see that a subset of these agree with
the ADAM SPNs specified in the ADAM Help file

ADAM Help
Administering ADAM
Administering ADAM service principal names

You can add an SPN for LDAP on a DNS alias name e.g.

```
setspn -A ldap/adam.mydomain.com:<adam port number> < netbiosname of  
ADAM  
machine>
```

looking at the list of existing SPNs for the computer account should give
you
the idea.

Notes:

You will probably need to be a domain admin to update the SPNs.

You can also use repadmin /writespn as per the ADAM Help instead of

Re: ADAM Bind to alias pointing local server fails

setspn

Apart from LDAP\dnshostname:port, you will see SPNs for

E3514235-4B06-11D1-AB04-00C04FC2DCD2-ADAM\ntbiosname:port

that are used for replication, I do not believe that you will need to add

to

that

as you should probably only be using the primary host name when setting

up

replication (IMO).

Lee Flight

"Craig Gilmour" <CraigGilmour@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message

news:A6438DAF-CDE6-436E-9787-37BEA53BEA12@xxxxxxxxxxxxxxxxxxxx

All,

I have a weird one that I would appreciate some help on. I

have

attempted

this on three separate Virtual Server instances as well as two

production

servers, so it is not a specific server problem.

Scenario:

The Domain is running Windows 2000

Windows2003 Member Server Server called:

myserver.mydomain.com IP

192.168.0.5

DNS Alias called: adam.mydomain.com referencing

myserver.mydomain.com

The Windows user I am logged on has full admin rights over

the server,

domain admin rights over the domain and full rights over

ADAM.

What I can do:

1.0 run LDP on any other host other than myservers and

connect and bind

to

the ADAM instance using Windows Credentials (currently

logged on user)

using

the actual hostname, IP Address or DNS Alias.

Re: ADAM Bind to alias pointing local server fails

2.0 Run ldp on myserver and connect / bind as the currently logged on user using the actual host name, localhost, the IP Address.

What I can't do is:

3.0 Run ldp on myserver and connect / bind as the currently logged on user using the DNS Alias (adam.mydomain.com). I get a bind failure – invalid credentials

I have tried setting a host file entry instead, all to no avail. Does anyone have any ideas?

Following is the output from LDP (I have only included the tail end of the connection output)

```
1> highestCommittedUSN: 17316;
4> supportedSASLMechanisms: GSSAPI; GSS-SPNEGO;
EXTERNAL; DIGEST-MD5;
1> dnsHostName: sqlserv.corp.riotinto.org;
1> serverName:
CN=MYSERVER$MYINSTANCE,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=
3> supportedCapabilities: 1.2.840.113556.1.4.1851 = (
LDAP_CAP_ACTIVE_DIRECTORY_ADAM_OID );
1.2.840.113556.1.4.1791 = (
LDAP_CAP_ACTIVE_DIRECTORY_LDAP_INTEG_OID
); 1.2.840.113556.1.4.1880 = (
LDAP_CAP_ACTIVE_DIRECTORY_ADAM_DIGEST );
1> isSynchronized: TRUE;
1> forestFunctionality: 2 = ( DS_BEHAVIOR_WIN2003 );
1> domainControllerFunctionality: 2 = (
DS_BEHAVIOR_WIN2003 );
-----
0 = ldap_set_option(ld, LDAP_OPT_ENCRYPT, 0)
res = ldap_bind_s(ld, NULL, &NtAuthIdentity,
NEGOTIATE (1158)); // v.3
{NtAuthIdentity: User='NULL'; Pwd= <unavailable>;
domain = 'NULL'.}
Error <49>: ldap_bind_s() failed: Invalid Credentials.
Server error: 8009030C: LdapErr: DSID-0C090441,
comment:
AcceptSecurityContext error, data 52e, vece
Error 0x8009030C The logon attempt failed
```

Re: ADAM Bind to alias pointing local server fails