

# Re: kerberos SQL service accounts

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2009-02/msg01538](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2009-02/msg01538)

---

- *From:* "skip" <[shofmann@xxxxxxx](mailto:shofmann@xxxxxxx)>
  - *Date:* Wed, 25 Feb 2009 13:09:19 -0800
- 

That makes perfect sense. Thank You!

"Joe Kaplan" <[joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:uRf5ft3IJHA.5028@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uRf5ft3IJHA.5028@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

It goes like this:

Given service with host name "SQL1" configured to run under account SERVICEACC1 needs to make a remote call to another SQL box with host name "SQL2" with SQL running under domain account SERVICEACC2 using delegation (on behalf of an impersonated caller):

On the account SERVICEACC1 (which should have an SPN like MSSqlSvc/SQL1:1433 and possibly an FQDN version as well), it should have "Trusted for delegation" "to specific services" with MSSqlSvc/SQL2:1433 as the target. It will look basically like that in ADUC. Note that ADUC only shows the delegation tab for accounts that have a the servicePrincipalName attribute set.

In LDP, you'll see that that SERVICEACC1 has:  
servicePrincipalName: MSSqlSvc/SQL1:1433  
userAccountControl includes flag "UF\_TRUSTED\_FOR\_DELEGATION"  
msds-AllowedToDelegateTo has "MSSqlSvc/SQL2:1433"

SERVICEACC1 will just have:  
servicePrincipalName: MSSqlSvc/SQL2:1433

Since it is not delegating to anything, it does not need to be trusted for delegation or have an "allowed to delegate to" attribute.

Make sure that only one account in the entire forest has servicePrincipalName equal to either of those SPNs or you will have Kerb errors.

HTH!

--

Joe Kaplan-MS MVP Directory Services Programming  
Co-author of "The .NET Developer's Guide to Directory Services Programming"  
<http://www.directoryprogramming.net>  
"skip" <[shofmann@xxxxxxx](mailto:shofmann@xxxxxxx)> wrote in message

Re: kerberos SQL service accounts

news:Oxbkpm3IJHA.4252@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

thank you very much for the explanation it was most helpful. I have question regarding constrained delegation. We do have SQL servers that need to make a remote call to another SQL server, both SQL servers in question are running there services as a domain user account. If i want to use constrained delegation, i know i set it up on the service account, but what account do i point the service account to use for constrained delegation? is it the other service account that is on running on other seperate SQL server?  
"Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:uuZVOT3IJHA.2064@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Also, on the delegation question, you only need to enable delegation on the SQL service account if SQL will be making a call to a remote system on behalf of a remote user it is impersonating.

It is much more common to have a web front end require delegation rights to allow it to query SQL on a user's behalf, but it is certainly possible that SQL itself might make such a remote call to another backend.

I suggest you make sure they tell you what they need to delegate to. You can enforce this in your own policy by using constrained delegation exclusively (you are 2003 native, so this is available). Constrained delegation says that a service can only delegate to other specific services (based on the SPN of the target). It is much more secure than unconstrained delegation (the only method available in Win2K) and is also self-documenting in that once you have configured it, you are certain to know exactly what services are delegating to what other services and are certain that they cannot delegate to anything but those services.

In some cases, unconstrained may really be necessary, but in most cases constrained should be possible. Make them figure what they need to delegate to.

--

Joe Kaplan-MS MVP Directory Services Programming  
Co-author of "The .NET Developer's Guide to Directory Services Programming"

<http://www.directoryprogramming.net>

"skip" <shofmann@xxxxxxx> wrote in message

news:9F3952AB-EBD1-400D-AD16-F378D0BA364D@xxxxxxxxxxxxxxxxxxxx

Hello all

The AD forest and domain are at windows 2003 native mode. The SQL DBA's are being asked to change all SQL service

## Re: kerberos SQL service accounts

accounts from local system to a domain user account. My question is and if this is not the correct forum for this please politely let me know. Once the SQL service account is changed from local system to a domain user account does SQL start using kerberos authentication? Does the spn for the domain account get registered in AD automatically? If i have a SQL cluster that has several SQL instance or virtual servers that are running on one of the pyhsical node's in the cluster, what spn gets registered in AD? I would think i would need to regsiter a SPN for the service account that is running on the SQL virtual server or instance and not the physical node?

Example physical node name is irv-idx-ms11 SQL virtual server running on physical node is irv-idx-vs11. Service account name is sqladmin. If i did a query on the service account name (sqladmin) using setspn then if this is correct the output from the command should look like

```
"MSSQLSvc/irv-idx-vs11"
```

Last question Delegation. If the SPN's are registered correctly for the service account why must i enable delegation on the service account in AD?

Many thanks for any guidance on this