strongSwan - Feature #842

ipsec purgecerts are not purging CA certs

05.02.2015 04:51 - Pavan Maganti

Status:	Closed	**Start date:**	05.02.2015
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.0		
Resolution:	Fixed		

Description

Hi,

Currently i have an issue with CA certs which is as follows.
My requirement is to add/remove additional root CA cert with out restarting IPSEC.

When the CA cert is added under /etc/ipsec.d/cacerts/ folder and executing "ipsec rereadcacerts" command reflects the certificate under "ipsec listcacerts". However, when i delete the CA cert from /etc/ipsec.d/cacerts/ folder and run the command "ipsec purgecerts" is still showing under the ipsec cache.

Do i need to use any other command to remove the deleted CA cert from cache?
Is this a known limitation in strongswan?

Regards,
Pavan

Associated revisions

Revision 1fd70254 - 03.03.2015 13:52 - Martin Willi

Merge branch 'stroke-purge-on-reread'

Remove all previously loaded certificates during "ipsec reread", finally
allowing the removal of CA certificates from a running daemon.

Fixes #842, #700, #305.

Revision 60d4c1cc - 20.08.2015 19:38 - Tobias Brunner

Merge branch 'stroke-ca-sections'

This resolves the duplicate CERTREQ issue when certificates in
ipsec.d/cacerts were referenced in ca sections. It also ensures CA
certificates are reloaded atomically, so there is never a time when
an unchanged CA certificate is not available.

References #842.

History

#1 - 06.02.2015 11:23 - Emeric Poupon

It would be nice to correct this issue!

I noticed several people are keeping reporting this issue on mailing lists.

#2 - 06.02.2015 13:02 - Martin Willi

- Status changed from New to Resolved

- Assignee set to Martin Willi

#3 - 06.02.2015 13:03 - Martin Willi

- Status changed from Resolved to Assigned

#4 - 06.02.2015 14:38 - Martin Willi

- Tracker changed from Bug to Issue

- Status changed from Assigned to Feedback

> It would be nice to correct this issue!
> I noticed several people are keeping reporting this issue on mailing lists.

While I agree and think this issue is important, unfortunately we have limited resources only. The required changes are not that trivial. Anyway, see below...

> when i delete the CA cert from /etc/ipsec.d/cacerts/ folder and run the command "ipsec purgecerts" is still showing under the ipsec cache.

ipsec purgecerts only affects the global certificate cache, not the credentials provided by starter/stroke. *ipsec reread*, on the other hand, only adds new certificates, but as you mentioned, currently does not remove previously loaded certificates.

Removing previously loaded certificates requires some changes, as we currently use a single pool of certificates, and can't differentiate from which directory they have been loaded.

I've tried to change the behavior with the last six patches from the stroke-purge-on-reread branch. It separates the credential types, and now removes any prevously loaded CA/AA certificate. Please note that CA certificates loaded through the *ipsec.conf ca* section keyword don't get updated, but the section must be reloaded using *ipsec update*.

Regards
Martin

#5 - 06.02.2015 15:05 - Emeric Poupon

This sounds promising!

I suppose it will not affect any established connection? This is maybe a more general issue, already being discussed in the dev mailing list.

Again, thanks for your support. I do agree such a project is very resource consuming.

#6 - 06.02.2015 17:03 - Martin Willi

> I suppose it will not affect any established connection?

No, unless reauthentication is enabled and fails due to a missing trust anchor.

Regards
Martin

#7 - 03.03.2015 14:33 - Martin Willi

- Tracker changed from Issue to Feature

- Category set to libcharon

- Priority changed from High to Normal

- Target version set to 5.3.0

- Resolution set to Fixed

The reference commit merges the previously discussed branch, where "ipsec reread" removes any previously loaded CA certificates before reloading them from disk.

Regards
Martin

#8 - 11.03.2015 15:09 - Martin Willi

- Status changed from Feedback to Closed

#9 - 13.08.2015 16:20 - Emeric Poupon

> The reference commit merges the previously discussed branch, where "ipsec reread" removes any previously loaded CA certificates before

> reloading them from disk.

I guess that if I use ca sections in the ipsec.conf file, the deleted CA are not actually deleted from the cache?
Would it be an acceptable workaround to perform an "ipsec reread" command after reloading the starter's configuration?

Regards,
Emeric

#10 - 13.08.2015 18:36 - Tobias Brunner

> I guess that if I use ca sections in the ipsec.conf file, the deleted CA are not actually deleted from the cache?

The certificate cache is flushed after a CA section is deleted.

But if you store your CA certificate in ipsec.d/cacerts it is actually stored in two credential sets now. The one in stroke_cred_t where such certificates are added when the *stroke* plugin (re-)reads all certificates in that directory, and the one that stroke_ca_t implements by enumerating all CA sections. Looks like the latter was added to handle the case where a certificate referenced in a CA section is *not* stored in ipsec.d/cacerts, so it shouldn't be affected by a flush of the first set.

But this also means that such certificates are now enumerated twice (even though it is the same certificate object as the CA section keeps a reference to the automatically loaded cert) this will e.g. result in duplicate certificate requests for the same CA (this can actually be seen in our examples that use *ca* sections, e.g. ipv6/host2host-ikev2).

So when you delete a CA section the certificate only disappears from the second set. To remove it from the first one you have to call ipsec rereadcacerts. Alternatively, avoid storing CA certs referenced in CA sections in ipsec.d/cacerts.

Resolving this properly seems kinda tricky, it might work by moving the CA certificate store to stroke_ca_t and keep track of which certs were loaded automatically and which are referenced by CA sections.

#11 - 20.08.2015 19:40 - Tobias Brunner

> Resolving this properly seems kinda tricky, it might work by moving the CA certificate store to stroke_ca_t and keep track of which certs were loaded automatically and which are referenced by CA sections.

Merged to master with the referenced commit.