

strongSwan - Issue #3395

Vici command list-sas hangs when invoked from updown script

05.04.2020 19:50 - Jakob Ahlin

Status:	Closed	Resolution:	No change required
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	vici		
Affected version:	5.8.0		

Description

I have the need to call vici commands from an updown script. My problem is that when I issue a **list-sas** command using the vici interface in an updown script, the call hangs. Both for up-client and down-client events. When using vici with tcp I get a timeout after some time, and with a unix socket it seems to hang for an indefinite time.

The updown script is defined on a child in a strongswan/swanctl configuration file:

```
updown = /etc/swanctl/updown/test-test1.updown.sh
```

I've tried both with the Python vici module and for testing purposes also using the swanctl command and the behavior is the same. This is the output from "strace swanctl -l" in an updown script.

```
[CHD] updown: futex(0x56343b6fc278, FUTEX_WAKE_PRIVATE, 1) = 1
[CHD] updown: socket(AF_UNIX, SOCK_STREAM, 0) = 7
[CHD] updown: connect(7, {sa_family=AF_UNIX, sun_path="/var/run/charon.vici"}, 22) = 0
[CHD] updown: futex(0x56343b6f3408, FUTEX_WAKE_PRIVATE, 1) = 1
[CHD] updown: futex(0x56343b6fc278, FUTEX_WAKE_PRIVATE, 1) = 1
[CHD] updown: futex(0x56343b6f8438, FUTEX_WAKE_PRIVATE, 1) = 1
[CHD] updown: sendto(7, "\0\0\0\t", 4, 0, NULL, 0) = 4
[CHD] updown: sendto(7, "\3", 1, 0, NULL, 0) = 1
[CHD] updown: sendto(7, "\7", 1, 0, NULL, 0) = 1
[CHD] updown: sendto(7, "list-sa", 7, 0, NULL, 0) = 7
[CHD] updown: futex(0x56343b72b3c8, FUTEX_WAIT_PRIVATE, 0, NULL) = 0
[CHD] updown: futex(0x56343b6f4478, FUTEX_WAKE_PRIVATE, 1) = 0
[CHD] updown: futex(0x56343b6f3408, FUTEX_WAKE_PRIVATE, 1) = 1
[CHD] updown: futex(0x56343b6fc278, FUTEX_WAKE_PRIVATE, 1) = 1
[CHD] updown: sendto(7, "\0\0\0\n", 4, 0, NULL, 0) = 4
[CHD] updown: sendto(7, "\0", 1, 0, NULL, 0) = 1
[CHD] updown: sendto(7, "\10", 1, 0, NULL, 0) = 1
[CHD] updown: sendto(7, "list-sas", 8, 0, NULL, 0) = 8
(here it hangs)
```

I have tried this with Strongswan 5.8.0 and 5.7.4, with the same behaviour. The problem does however not appear when I make the same call from an external script that triggers on vici updown events (using vici listen function on session with python).

History

#1 - 06.04.2020 09:42 - Tobias Brunner

- Status changed from New to Feedback

My problem is that when I issue a **list-sas** command using the vici interface in an updown script, the call hangs.

That's because the IKE_SA for which the updown script is run is locked and blocks enumeration of IKE_SAs. That is, unless you allow the command to skip locked SAs (via *noblock* option). But you might not see all SAs in that case, as it skips all blocked IKE_SAs not only the one for which the updown script is executed.

What exactly are you trying to do anyway?

#2 - 07.04.2020 17:11 - Jakob Ahlin

Tobias Brunner wrote:

My problem is that when I issue a **list-sas** command using the vici interface in an updown script, the call hangs.

That's because the IKE_SA for which the updown script is run is locked and blocks enumeration of IKE_SAs. That is, unless you allow the command to skip locked SAs (via *noblock* option). But you might not see all SAs in that case, as it skips all blocked IKE_SAs not only the one for which the updown script is executed.

Thanks a lot for your quick response and for the explanation!

What exactly are you trying to do anyway?

When terminating a child, we are trying determine if this is the last child SA active for the connection, and if not perform a number of actions like removing the vti interface shared by the child SAs of the connection. Is there another (obvious) way to get this information?

#3 - 07.04.2020 17:34 - Tobias Brunner

Is there another (obvious) way to get this information?

Yes, use [vici's ike-updown](#) event instead (there is an example in the [route-based/net2net-xfrmi-ike](#) scenario, see [source:testing/tests/route-based/net2net-xfrmi-ike/hosts/sun/etc/updown.py](#)).

#4 - 25.09.2020 10:42 - Tobias Brunner

- Status changed from *Feedback* to *Closed*
- Assignee set to *Tobias Brunner*
- Resolution set to *No change required*