strongSwan - Issue #3418

exporting log/monitoring swantcl messages to external scripts

20.04.2020 20:29 - Tuarego Silva

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	swanctl		
Affected version:	5.8.4	**Resolution:**	No change required

Description

Hi guys,
First of all I tried to find some info about this I am looking for but I didn't find anything on this subject. Also I am not a programmer so this is why I am asking for help.
I am running Strongswan with support for IKEv2 and IPSec/L2TP sessions and I would like to built some kind of system that could store and manage client VPN sessions. I tried to run Strongswan with mysql plugin and then fetch session info from mysql databases but it seems that when I activate this plugin I need to configure Strongswan from mysql databases and all my configuration it's on text files. I would like to run mysql plugins only for logs and sessions monitoring, is this possible? I couldn't manage to do it.
Because I didn't find how to use mysql plugin only for logs I tried to change swanctl log option and I am able to parse any message from swantcl log and call an external batch script to send desired data to mysql databases. However it seems better to use swantcl sas monitor option (--monitor-sa) to track changes to sas. This option uses vici_dump function to send messages to stdout and I am not been able to redirect this messages to an external batch script because vici_dump requires a FILE stream output and not a variable where I can store the message to send to an external batch script as argument! So my question it's, is there an easy way to redirect a monitoring event message to an external batch script and pass event message as a batch script argument? I can do this with log function because I can use vici_find_str(msg, NULL, "msg") and export the result however in monitoring events I cannot do the same because sections keys are dynamic and I am not able to use wildcards inside vici_find_str function.
I hope one can understand my english and my message.

History

#1 - 21.04.2020 10:10 - Tobias Brunner

- Status changed from New to Feedback

> I would like to built some kind of system that could store and manage client VPN sessions.

You can use RADIUS Accounting for this (authentication does not have to be done via RADIUS).

> I would like to run mysql plugins only for logs and sessions monitoring, is this possible?

The sql plugin does the actual logging (if enabled via *charon.plugins.sql.loglevel*), but it does not store any session data.

> I tried to change swanctl log option and I am able to parse any message from swantcl log and call an external batch script to send desired data to mysql databases. However it seems better to use swantcl sas monitor option (--monitor-sa) to track changes to sas.

Actually, it would be even better to use the vici events directly (e.g. via Python or Ruby script).

> So my question it's, is there an easy way to redirect a monitoring event message to an external batch script and pass event message as a batch script argument?

You can surely pipe the output to a custom script. But again, using vici directly is probably way easier.

> I can do this with log function because I can use vici_find_str(msg, NULL, "msg") and export the result however in monitoring events I cannot do the same because sections keys are dynamic and I am not able to use wildcards inside vici_find_str function.

Read the vici protocol documentation. There will be only one section per event, which you can parse with vici_parse_cb().

#2 - 21.04.2020 16:56 - Tuarego Silva

Hi Tobias, many thanks for your reply...

I am using already Radius accounting and Radius exec module to save some data from VPN sessions, but sometimes clients may have their public ip changed without stopping or loosing their VPN sessions and I loose track from VPN sessions! This is why I want to create a new way of get sessions info and track sessions changes.
So by now I think the best way it is to use monitor-sa events data to track changes to each SA. I have not been able to use vici_dump because it streams to stdout. I cannot really use vici_find_str for keys inside sections because section name it is dynamic. As example,
I can fetch initiator-spi because this section name it's static:
printf("initiator-spi: %s\n", vici_find_str(res, "not found", "ikev1conn.initiator-spi"));
I cannot do the same with spi-in in Child-sas section because Child name depends from Child uniqueid:
printf("spi-in: %s\n", vici_find_str(res, "not found", "ikev1conn.child-sas.ikev1conn-???.spi-out"));
I will try to learn more about vici_parse_cb and try fetch events data in order to pass them to external script.
best.

#3 - 21.04.2020 17:12 - Tobias Brunner

> I am using already Radius accounting and Radius exec module to save some data from VPN sessions, but sometimes clients may have their public ip changed without stopping or loosing their VPN sessions and I loose track from VPN sessions!

Why do you think that gets better if you use vici events? (The *eap-radius* plugin uses the same events to notify the RADIUS server.)

> So by now I think the best way it is to use monitor-sa events data to track changes to each SA.

Just use the vici events directly, not --monitor-sa.

> I have not been able to use vici_dump because it streams to stdout.

Why modify the code? You could probably just use the output of the command if you don't want to write your own script.

> I will try to learn more about vici_parse_cb and try fetch events data in order to pass them to external script.

Why not use a custom script in the first place? Why modify the swanctl code?

#4 - 22.04.2020 00:07 - Tuarego Silva

Does eap-radius plugin tell radius when a vpn client change it's ip address or source port (not vpn ip address)? I thought not but not sure about that...
what I am trying to do about "--monitor-sa" it's duplicate this function and use a new one to trigger an external script and use events messages as arguments of external script. This way I do not have to query swanctl about vpn session changes!
I could use swanctl (--log) log messages to trigger the external script because I can use vici_find_str with log messages but log messages do not have the same detailed information about SAS as "--monitor-sa" events. If I go with log messages after receive this messages I will have to run swanctl -l -I to fetch the desired info.
So create a copy of --monitor-sa and change it in order to do something like:
args = vici_dump(res, buf, *format & COMMAND_FORMAT_PRETTY, stdout);
system("external_script args");
with vici_dump in RAW format seems to be the easiest and best way!!
Please remember I am not a programmer and I know zero about C!!

#5 - 22.04.2020 00:15 - Tuarego Silva

another question, can vici_parse_cb return string values in a message? It seems not, right?

#6 - 22.04.2020 09:09 - Tobias Brunner

> Does eap-radius plugin tell radius when a vpn client change it's ip address or source port (not vpn ip address)?

Not directly, but the IP address/port will be different in any RADIUS-Accounting messages after such a change (i.e. in interim updates or the eventual stop message). See the table on EapRadius for details on what attributes are sent.

> what I am trying to do about "--monitor-sa" it's duplicate this function and use a new one to trigger an external script and use events messages as arguments of external script.

You can't, because there is currently no such event via vici either. Only plugins can receive the ike_update() events that are triggered if the endpoint of an IKE_SA changes. Also, the --monitor-sa command only subscribes to the updown events, not even the rekeying events, so tracking SAs would be quite difficult that way.

> another question, can vici_parse_cb return string values in a message? It seems not, right?

What do you mean?

#7 - 22.04.2020 12:54 - Tuarego Silva

ok, there is something that I should have mentioned from the beginnig... The reason why I am doing this it's because my vpn server has a management webpage, built on Observium (great tool!) as a adapted webpage where the splash page contains a list of vpn sessions. So when someone access this webpage this webpage needs to fetch current vpn sessions info on the fly.
For example to count sessions traffic I managed to use swanctl --log function to intercept messages with Closing CHILD_SA and extract Child SA counters. These values are then added to the last one and to instantaneous counters from current child SA. This is made individually for each vpn session.
I believe that swantcl --monitor-sa will display messages when child changes occurs. I just need to update SA entries on a mysql database.
My problem it's because I am not a programmer I do not know how to "deal" with blobs and so I do not know how to extract strings from CALLBACK function responses. I can use vici_find_str and extract values when I know the name of the key. So what I am doing I am inside CALLBACK function and fetching data with vici_find_str, example: printf("local-host: s\n", vici_find_str(res, "not found", "ikev1conn.local-host"));
So what I really want to do it's inside this CALLBACK function catch the entire response in string format to be able to send it as argument for external script:
args = vici_dump(res, buf, *format x%x COMMAND_FORMAT_PRETTY, stdout);
system("external_script args");
I know that "args = vici_dump..." does not make any sense!! this is just a kind of illustration because I do not know how to do it!!
maybe something like: args = vici_find_str(res, "not found", <all keys and all values>) explains it better... I just want to catch the entire message in string format, not blob.
Maybe this sounds crazy to you, but again I know zero about C.
Many thanks for your patience.

#8 - 22.04.2020 13:26 - Tobias Brunner

> For example to count sessions traffic I managed to use swanctl --log function to intercept messages with Closing CHILD_SA and extract Child SA counters.

RADIUS Accounting provides such counters.

> I believe that swantcl --monitor-sa will display messages when child changes occurs.

Again, not when they are rekeyed.

> My problem it's because I am not a programmer I do not know how to "deal" with blobs and so I do not know how to extract strings from CALLBACK function responses.

Then hire somebody (but again, doing this via events directly would be way better than trying to parse output of another tool).

> Maybe this sounds crazy to you, but again I know zero about C.

Then use a different language that's easier for beginners (see vici for a list of bindings).

#9 - 25.09.2020 11:26 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required