strongSwan - Issue #3495

Connection problem work vpn

25.06.2020 14:25 - Florian Ortner

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	networkmanager (charon-nm)		
Affected version:	5.8.2	**Resolution:**	No feedback

Description

I try to connect to my work vpn and have this issue with Ubuntu 20.04.
It's an IKEv2/EAP-mschapv2 server and I can't connect. Any idea why it's failing?

```
Jun 25 14:24:36 ODIN2 NetworkManager[1190]: <info>  [1593087876.9915] audit: op="connection-activa
te" uuid="89ea04e0-b3a4-45b2-83f0-a3cdfe607bf0" name="INHECO VPN" pid=6936 uid=1000 result="succes
s"
Jun 25 14:24:36 ODIN2 gnome-shell[1623]: JS ERROR: TypeError: item is undefined#012setActiveConnec
tions/<@resource:///org/gnome/shell/ui/status/network.js:1523:17#012setActiveConnections@resource:
///org/gnome/shell/ui/status/network.js:1520:24#012_syncVpnConnections@resource:///org/gnome/shell
/ui/status/network.js:1867:26
Jun 25 14:24:36 ODIN2 NetworkManager[1190]: <info>  [1593087876.9929] vpn-connection[0x55f94822453
0,89ea04e0-b3a4-45b2-83f0-a3cdfe607bf0,"INHECO VPN",0]: Saw the service appear; activating connect
ion
Jun 25 14:24:37 ODIN2 NetworkManager[1190]: <info>  [1593087877.1054] vpn-connection[0x55f94822453
0,89ea04e0-b3a4-45b2-83f0-a3cdfe607bf0,"INHECO VPN",0]: VPN connection: (ConnectInteractive) reply
 received
Jun 25 14:24:37 ODIN2 charon-nm: 05[CFG] received initiate for NetworkManager connection INHECO VP
N
Jun 25 14:24:37 ODIN2 charon-nm: 05[CFG] using CA certificate, gateway identity '217.6.192.10'
Jun 25 14:24:37 ODIN2 charon-nm: 05[IKE] initiating IKE_SA INHECO VPN[14] to 217.6.192.10
Jun 25 14:24:37 ODIN2 charon-nm: 05[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Jun 25 14:24:37 ODIN2 charon-nm: 05[NET] sending packet: from 192.168.0.124[39926] to 217.6.192.10
[500] (1128 bytes)
Jun 25 14:24:37 ODIN2 NetworkManager[1190]: <info>  [1593087877.1077] vpn-connection[0x55f94822453
0,89ea04e0-b3a4-45b2-83f0-a3cdfe607bf0,"INHECO VPN",0]: VPN plugin: state changed: starting (3)
Jun 25 14:24:37 ODIN2 charon-nm: 14[NET] received packet: from 217.6.192.10[500] to 192.168.0.124[
39926] (38 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 14[ENC] parsed IKE_SA_INIT response 0 [ N(INVAL_KE) ]
Jun 25 14:24:37 ODIN2 charon-nm: 14[IKE] peer didn't accept DH group ECP_256, it requested MODP_20
48
Jun 25 14:24:37 ODIN2 charon-nm: 14[IKE] initiating IKE_SA INHECO VPN[14] to 217.6.192.10
Jun 25 14:24:37 ODIN2 charon-nm: 14[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Jun 25 14:24:37 ODIN2 charon-nm: 14[NET] sending packet: from 192.168.0.124[39926] to 217.6.192.10
[500] (1320 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 07[NET] received packet: from 217.6.192.10[500] to 192.168.0.124[
39926] (472 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 07[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(N
ATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
Jun 25 14:24:37 ODIN2 charon-nm: 07[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_
HMAC_SHA2_256/MODP_2048
Jun 25 14:24:37 ODIN2 charon-nm: 07[IKE] local host is behind NAT, sending keep alives
Jun 25 14:24:37 ODIN2 charon-nm: 07[IKE] sending cert request for "CN=INHECO GmbH CA"
Jun 25 14:24:37 ODIN2 charon-nm: 07[IKE] establishing CHILD_SA INHECO VPN{14}
Jun 25 14:24:37 ODIN2 charon-nm: 07[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTR
EQ SA TSi TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP)
 ]
Jun 25 14:24:37 ODIN2 charon-nm: 07[NET] sending packet: from 192.168.0.124[38151] to 217.6.192.10
[4500] (368 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 16[NET] received packet: from 217.6.192.10[4500] to 192.168.0.124
[38151] (1236 bytes)
```

```
Jun 25 14:24:37 ODIN2 charon-nm: 16[ENC] parsed IKE_AUTH response 1 [ EF(1/2) ]
Jun 25 14:24:37 ODIN2 charon-nm: 16[ENC] received fragment #1 of 2, waiting for complete IKE messa
ge
Jun 25 14:24:37 ODIN2 charon-nm: 15[NET] received packet: from 217.6.192.10[4500] to 192.168.0.124
[38151] (868 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 15[ENC] parsed IKE_AUTH response 1 [ EF(2/2) ]
Jun 25 14:24:37 ODIN2 charon-nm: 15[ENC] received fragment #2 of 2, reassembled fragmented IKE mes
sage (2032 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 15[ENC] parsed IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/ID ]
Jun 25 14:24:37 ODIN2 charon-nm: 15[IKE] received end entity cert "C=DE, ST=Bayern, L=Martinsried,
 O=INHECO GmbH, OU=IT, CN=muc-fw3.inheco.com"
Jun 25 14:24:37 ODIN2 charon-nm: 15[CFG]   using certificate "C=DE, ST=Bayern, L=Martinsried, O=IN
HECO GmbH, OU=IT, CN=muc-fw3.inheco.com"
Jun 25 14:24:37 ODIN2 charon-nm: 15[CFG]   using trusted ca certificate "CN=INHECO GmbH CA"
Jun 25 14:24:37 ODIN2 charon-nm: 15[CFG] checking certificate status of "C=DE, ST=Bayern, L=Martin
sried, O=INHECO GmbH, OU=IT, CN=muc-fw3.inheco.com"
Jun 25 14:24:37 ODIN2 charon-nm: 15[CFG]   fetching crl from 'ldap:///CN=INHECO%20GmbH%20CA,CN=phi
lotes,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=inheco,DC=com?certificateR
evocationList?base?objectClass=cRLDistributionPoint' ...
Jun 25 14:24:37 ODIN2 charon-nm: 15[LIB] LDAP bind to 'ldap:///CN=INHECO%20GmbH%20CA,CN=philotes,C
N=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=inheco,DC=com?certificateRevocati
onList?base?objectClass=cRLDistributionPoint' failed: Can't contact LDAP server
Jun 25 14:24:37 ODIN2 charon-nm: 15[CFG] crl fetching failed
Jun 25 14:24:37 ODIN2 charon-nm: 15[CFG] certificate status is not available
Jun 25 14:24:37 ODIN2 charon-nm: 15[CFG]   reached self-signed root ca with a path length of 0
Jun 25 14:24:37 ODIN2 charon-nm: 15[IKE] authentication of 'muc-fw3.inheco.com' with RSA_EMSA_PKCS
1_SHA2_256 successful
Jun 25 14:24:37 ODIN2 charon-nm: 15[IKE] server requested EAP_IDENTITY (id 0x00), sending 'inheco\
FOrtner'
Jun 25 14:24:37 ODIN2 charon-nm: 15[ENC] generating IKE_AUTH request 2 [ EAP/RES/ID ]
Jun 25 14:24:37 ODIN2 charon-nm: 15[NET] sending packet: from 192.168.0.124[38151] to 217.6.192.10
[4500] (96 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 09[NET] received packet: from 217.6.192.10[4500] to 192.168.0.124
[38151] (80 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 09[ENC] parsed IKE_AUTH response 2 [ EAP/REQ/PEAP ]
Jun 25 14:24:37 ODIN2 charon-nm: 09[IKE] server requested EAP_PEAP authentication (id 0x01)
Jun 25 14:24:37 ODIN2 charon-nm: 09[TLS] EAP_PEAP version is v0
Jun 25 14:24:37 ODIN2 charon-nm: 09[ENC] generating IKE_AUTH request 3 [ EAP/RES/PEAP ]
Jun 25 14:24:37 ODIN2 charon-nm: 09[NET] sending packet: from 192.168.0.124[38151] to 217.6.192.10
[4500] (272 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 08[NET] received packet: from 217.6.192.10[4500] to 192.168.0.124
[38151] (1236 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 08[ENC] parsed IKE_AUTH response 3 [ EF(1/2) ]
Jun 25 14:24:37 ODIN2 charon-nm: 08[ENC] received fragment #1 of 2, waiting for complete IKE messa
ge
Jun 25 14:24:37 ODIN2 charon-nm: 10[NET] received packet: from 217.6.192.10[4500] to 192.168.0.124
[38151] (404 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 10[ENC] parsed IKE_AUTH response 3 [ EF(2/2) ]
Jun 25 14:24:37 ODIN2 charon-nm: 10[ENC] received fragment #2 of 2, reassembled fragmented IKE mes
sage (1568 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 10[ENC] parsed IKE_AUTH response 3 [ EAP/REQ/PEAP ]
Jun 25 14:24:37 ODIN2 charon-nm: 10[ENC] generating IKE_AUTH request 4 [ EAP/RES/PEAP ]
Jun 25 14:24:37 ODIN2 charon-nm: 10[NET] sending packet: from 192.168.0.124[38151] to 217.6.192.10
[4500] (80 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 11[NET] received packet: from 217.6.192.10[4500] to 192.168.0.124
[38151] (576 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 11[ENC] parsed IKE_AUTH response 4 [ EAP/REQ/PEAP ]
Jun 25 14:24:37 ODIN2 charon-nm: 11[TLS] negotiated TLS 1.0 using suite TLS_ECDHE_RSA_WITH_AES_256
_CBC_SHA
Jun 25 14:24:37 ODIN2 charon-nm: 11[TLS] server certificate does not match to 'muc-fw3.inheco.com'
Jun 25 14:24:37 ODIN2 charon-nm: 11[TLS] sending fatal TLS alert 'access denied'
Jun 25 14:24:37 ODIN2 charon-nm: 11[ENC] generating IKE_AUTH request 5 [ EAP/RES/PEAP ]
Jun 25 14:24:37 ODIN2 charon-nm: 11[NET] sending packet: from 192.168.0.124[38151] to 217.6.192.10
[4500] (96 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 13[NET] received packet: from 217.6.192.10[4500] to 192.168.0.124
[38151] (80 bytes)
Jun 25 14:24:37 ODIN2 charon-nm: 13[ENC] parsed IKE_AUTH response 5 [ EAP/FAIL ]
```

```
Jun 25 14:24:37 ODIN2 charon-nm: 13[IKE] received EAP_FAILURE, EAP authentication failed
Jun 25 14:24:37 ODIN2 charon-nm: 13[ENC] generating INFORMATIONAL request 6 [ N(AUTH_FAILED) ]
Jun 25 14:24:37 ODIN2 charon-nm: 13[NET] sending packet: from 192.168.0.124[38151] to 217.6.192.10
[4500] (80 bytes)
Jun 25 14:24:37 ODIN2 NetworkManager[1190]: <warn>  [1593087877.2086] vpn-connection[0x55f94822453
0,89ea04e0-b3a4-45b2-83f0-a3cdfe607bf0,"INHECO VPN",0]: VPN plugin: failed: connect-failed (1)
Jun 25 14:24:37 ODIN2 NetworkManager[1190]: <warn>  [1593087877.2087] vpn-connection[0x55f94822453
0,89ea04e0-b3a4-45b2-83f0-a3cdfe607bf0,"INHECO VPN",0]: VPN plugin: failed: connect-failed (1)
Jun 25 14:24:37 ODIN2 NetworkManager[1190]: <info>  [1593087877.2087] vpn-connection[0x55f94822453
0,89ea04e0-b3a4-45b2-83f0-a3cdfe607bf0,"INHECO VPN",0]: VPN plugin: state changed: stopping (5)
Jun 25 14:24:37 ODIN2 NetworkManager[1190]: <info>  [1593087877.2088] vpn-connection[0x55f94822453
0,89ea04e0-b3a4-45b2-83f0-a3cdfe607bf0,"INHECO VPN",0]: VPN plugin: state changed: stopped (6)
```

History

#1 - 25.06.2020 18:03 - Tobias Brunner

- Description updated

- Category set to networkmanager (charon-nm)

- Status changed from New to Feedback

- Affected version changed from 5.8.4 to 5.8.2

```
Jun 25 14:24:37 ODIN2 charon-nm: 11[TLS] server certificate does not match to 'muc-fw3.inheco.com'
Jun 25 14:24:37 ODIN2 charon-nm: 11[TLS] sending fatal TLS alert 'access denied'
```

In versions before 5.8.3, the NM backend does not configure an AAA identity (later versions set it to %any). So it defaults to the IKE identity, which is apparently not what the RADIUS server uses. There is currently also no option to configure the AAA identity manually. So unless you can upgrade to a newer version or change the server config, the only other option with charon-nm is to disable the *eap-peap* plugin and hope the server also accept other EAP methods (you could also switch from the NM plugin to the command line, where you could configure the AAA identity as needed).

#2 - 30.09.2020 14:06 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No feedback