strongSwan - Feature #2853

Add RADIUS Accounting Acct-Session-Id Attribute to Access-Request Messages

09.12.2018 01:18 - James Dogopoulos

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.7.2		
Resolution:	Fixed		

Description

iOS (latest) clients connect ok with the built in ike2. However, it seems like exactly every 10 minutes a checkout occurs and fails, the client stays connected and even though it seems like a new SPI takes over, a new radacct entry is created and the old one is not updated with a stoptime, the radacct acctsessionid is the same but acctuniqueid changes , the outcome of this is even though the connection was recreated, the old entry remains and is not cleared/stopped which builds up stale records in the database and this completely breaks Simultaneous Login checking. No more users can login after the number of stale entries matches and radwho/radutmp also shows additional active logins since radius is handling that file as well.

```
Dec  8 17:57:40 avspam charon: 07[MGR] checkout IKEv2 SA with SPIs 4e1bfa15292707c7_i 6c61008b89d8b3f3_r
Dec  8 17:57:40 avspam charon: 07[MGR] IKE_SA radius-ike2[5] successfully checked out
Dec  8 17:57:40 avspam charon: 07[KNL] querying SAD entry with SPI ccff3954
Dec  8 17:57:40 avspam charon: 07[KNL] querying SAD entry with SPI 04d0ea26
Dec  8 17:57:40 avspam charon: 07[MGR] checkin IKE_SA radius-ike2[5]
Dec  8 17:57:40 avspam charon: 07[MGR] checkin of IKE_SA successful
Dec  8 17:57:40 avspam charon: 04[MGR] checkout IKEv2 SA with SPIs 81b0913f0cdd95ae_i a7fdef192a4389e7_r
Dec  8 17:57:40 avspam charon: 04[MGR] IKE_SA checkout not successful
Dec  8 17:57:40 avspam charon: 07[CFG] RADIUS server 'primary' is candidate: 210
Dec  8 17:57:40 avspam charon: 07[CFG] sending RADIUS Accounting-Request to server 'primary'
Dec  8 17:57:40 avspam charon: 07[CFG] received RADIUS Accounting-Response from server 'primary'
Dec  8 17:57:40 avspam charon: 02[NET] received packet: from y.y.y.y[19211] to x.x.x.x[4500]
Dec  8 17:57:40 avspam charon: 02[NET] waiting for data on sockets
Dec  8 17:57:40 avspam charon: 13[MGR] checkout IKEv2 SA by message with SPIs 4e1bfa15292707c7_i 6c61008b89d8b3f3_r
Dec  8 17:57:40 avspam charon: 13[MGR] IKE_SA radius-ike2[5] successfully checked out
Dec  8 17:57:40 avspam charon: 13[NET] received packet: from y.y.y.y[19211] to x.x.x.x[4500] (80 bytes)
Dec  8 17:57:40 avspam charon: 13[ENC] parsed INFORMATIONAL request 4 [ ]
Dec  8 17:57:40 avspam charon: 13[ENC] generating INFORMATIONAL response 4 [ ]
Dec  8 17:57:40 avspam charon: 13[NET] sending packet: from x.x.x.x[4500] to y.y.y.y[19211] (80 bytes)
Dec  8 17:57:40 avspam charon: 13[MGR] checkin IKE_SA radius-ike2[5]
Dec  8 17:57:40 avspam charon: 13[MGR] checkin of IKE_SA successful
Dec  8 17:57:40 avspam charon: 03[NET] sending packet: from x.x.x.x[4500] to y.y.y.y[19211]
Dec  8 17:57:42 avspam charon: 05[MGR] checkout IKEv2 SA with SPIs 4e1bfa15292707c7_i 6c61008b89d8b3f3_r
Dec  8 17:57:42 avspam charon: 05[MGR] IKE_SA radius-ike2[5] successfully checked out
```

Associated revisions

Revision 533efa91 - 17.12.2018 09:46 - Tobias Brunner

eap-radius: Add RADIUS Accounting session ID to Access-Request messages

This allows e.g. associating database entries for IP leases and
accounting directly from the start.

Fixes #2853.

History

#1 - 10.12.2018 01:23 - James Dogopoulos

I just witnessed something similar happen with a windows 10 client connection. It's much more stable though. This time it was connected for about 6 hours , then dropped for an unknown reason, a new one opened and worked fine but the old session was never cleared so became stale and no session stop time was recorded. I'm not too worried about the occasional hiccup, a script can clean these up, the iphone issue is more severe, I got a couple other models of iphone to test with and will try to get client side logs.

#2 - 10.12.2018 10:25 - Tobias Brunner

- Description updated

- Status changed from New to Feedback

Please use the log settings given on HelpRequests (perhaps with *mgr* set to 1).

#3 - 10.12.2018 21:40 - James Dogopoulos

I will need to further debug this, a script to clear db records that have not received an accounting update in a certain amount of time after the interim accounting interval will keep things working but it does create the risk of some accounting data being lost if that accounting update gets lost due to connection issues/ packet loss.

#4 - 12.12.2018 23:38 - James Dogopoulos

A little more info on this... when the iphone drops from whatever is happening every ten minutes... it looks like the radius server is getting all the correct info in future Interim-Updates, the new login that is created is because of a new acctuniqueid. The data usage is even incremented properly. There is just something changing slightly that is resulting in a new acctuniqueid and the RADIUS server treating it like a new connection which confuses Simultaneous-Use calculations. Will continue tracking it down as time allows.

Aside from the acctuniqueid change, the pool_key in the sqlippool table is changing within FreeRADIUS which makes it no longer update the lease time on the IP address that was in use and eventually another user will get assigned the IP while it is still in use.

I notice Acct-Session-Time is going backwards between Interim-Updates after the iphone sa fails, that is the main difference between the Interim-Updates that I have noticed so far.. https://freeradius.org/rfc/rfc2866.html#Acct-Session-Time -- the RFC says this is only supposed to be sent when Account-Status-Type: Stop happens. Not sure if this is what is causing the new acctuniqueid or not but it is the only thing standing out right now.

radacctid	acctsessionid	acctuniqueid	username	groupname	realm	nasipaddress	nasportid	nasporttype	acctstarttime	acctupdatetime	acctstoptime	acctinterval	acctsessiontime	acctauthentic	connectinfo_start	connectinfo_stop	acctinputoctets	acctoutputoctets	calledstationid	callingstationid	acctterminatecause	servicetype	framedprotocol	framedipaddress
431	1544565821-28	796d3206317c2068d3d523390621cab2	jd			nasip.135	radius-ike2	Virtual	2018-12-12 16:25:37	2018-12-12 17:19:37	NULL	180	3240				13034153	664697393	y.y.y.y=5B4500=5D	x.x.x.x=5B4500=5D		Framed-User		z.z.z.112
432	1544565821-28	4f8b5f32e34103544ae91962abf138dd	jd			nasip.135	radius-ike2	Virtual	2018-12-12 16:25:37	2018-12-12 17:22:37	NULL	NULL	3420				13759413	684740418	y.y.y.y=5B4500=5D	x.x.x.x=5B4500=5D		Framed-User		z.z.z.112

#5 - 13.12.2018 00:18 - James Dogopoulos

I just noticed NAS-Port is also changing along with Acct-Session-Time going backwards in the Interim-Update that follows the sa breakdown. I'm assuming one of these is triggering generation of a new acctuniqueid in FreeRADIUS.

I also just witnessed the Windows 10 client do the same thing after being connected for 8 hours. NAS Port changed , acctuniqueid in FreeNAS changed but this time the Session Time incremented without issue. The client stayed connected just fine however, so some fancy scripting can watch and correct for this but obviously that's a hack of a fix.

#6 - 13.12.2018 02:40 - James Dogopoulos

Here are two potential fixes for this problem: StrongSWAN needs to keep its NAS-Port number whenever possible (which seems to be the ipsec reqid internally), when reauthenticating etc. It seems to change even when nothing else does. Acct-Session-Id needs to also be sent with the initial Access-Request so it can be used as a unique identifier for FreeRADIUS sqlippool. The second one might not be a complete fix as im not sure when/how FreeRADIUS decides to generate a new acctuniqueid and it could still leave the stale login issue behind.

#7 - 13.12.2018 10:29 - Tobias Brunner

> the new login that is created is because of a new acctuniqueid.

What exactly is that referring to? I don't see any RADIUS attribute with such or a similar name. This must be something internal to FreeRADIUS. So the question is when/how it is created/generated.

> There is just something changing slightly that is resulting in a new acctuniqueid and the RADIUS server treating it like a new connection which confuses Simultaneous-Use calculations.

It might be a new connection (depending on what exactly the client does, you haven't provided information on this, i.e. your log leaves too much out to see what's going on).

> Aside from the acctuniqueid change, the pool_key in the sqlippool table is changing within FreeRADIUS which makes it no longer update the lease time on the IP address that was in use and eventually another user will get assigned the IP while it is still in use.

Hm, that seems strange or even like a bug in FreeRADIUS, because the virtual IP is apparently still the same (at least in the table you posted). So why wouldn't it be tracked via the "new" session?

> I notice Acct-Session-Time is going backwards between Interim-Updates after the iphone sa fails

What do you mean with "the iphone sa fails"? And backwards how (the table doesn't show this)?

> https://freeradius.org/rfc/rfc2866.html#Acct-Session-Time -- the RFC says this is only supposed to be sent when Account-Status-Type: Stop happens.

That was clarified in RFC 5080, section 2.3.1.

> I just noticed NAS-Port is also changing along with Acct-Session-Time going backwards in the Interim-Update that follows the sa breakdown.

Hm, that could point to an IKE_SA rekeying, which creates a new IKE_SA with a new unique ID, which results in a new NAS-Port. However, the session ID stays the same over rekeyings (it is based on the unique ID of the original IKE_SA).

> I'm assuming one of these is triggering generation of a new acctuniqueid in FreeRADIUS.

Yeah, probably depends on the information FreeRADIUS uses to generate the acctuniqueid value (if it was only the session ID, this would probably not be an issue, if it also includes the NAS-Port somehow, IKE_SA rekeying could be problematic).

> strongSWAN needs to keep its NAS-Port number whenever possible (which seems to be the ipsec reqid internally)

No, not the reqid, which is used for CHILD_SAs, but the unique ID of the IKE_SA, which changes during rekeyings. While I suppose we could keep this the same, like the session ID, it could possibly also be useful to see if the IKE_SA got rekeyed. Couldn't you just change something in FreeRADIUS so it only uses the session ID to generate acctuniqueid?

> when reauthenticating etc.

That's not possible because reauthentication creates completely unrelated IKE_SAs (also creates a new session ID) and the old IKE_SA will be closed. Depending on the kind of reauthentication that's used, this happens overlapping, so framed IPs probably must be refcounted for this to work, so they are not released when the Stop message for the old IKE_SA arrives while the new IKE_SA still uses the same IP.

> Acct-Session-Id needs to also be sent with the initial Access-Request so it can be used as a unique identifier for FreeRADIUS sqlippool.

Yes, I mentioned that in #2856-1. I guess that could be added somehow, but needs some refactoring.

#8 - 13.12.2018 16:10 - James Dogopoulos

> What do you mean with "the iphone sa fails"? And backwards how (the table doesn't show this)?

Backwards as in one Update it says Session-Time: 3060 seconds and the next it says 1000, even though the octet counters have all gone up and the same session ID is attached.

> Hm, that seems strange or even like a bug in FreeRADIUS, because the virtual IP is apparently still the same (at least in the table you posted). So why wouldn't it be tracked via the "new" session?

> Yes, I mentioned that in #2856-1. I guess that could be added somehow, but needs some refactoring.

The RADIUS server needs a unique identifier to track IPs when the session starts, none are sent. NAS-Port doesn't work because it changes too much and there is no method to notify the RADIUS server of the changed port. Either that or generate a new session ID every time the port changes and treat it as an entirely new session as far as RADIUS goes? I'm not saying something can't be done differently on the RADIUS side but sending a unique identifier right from the start from strongswan seems logical to me.

#9 - 13.12.2018 16:26 - Tobias Brunner

>> What do you mean with "the iphone sa fails"? And backwards how (the table doesn't show this)?
>
> Backwards as in one Update it says Session-Time: 3060 seconds and the next it says 1000, even though the octet counters have all gone up and the same session ID is attached.

Again, that isn't seen in the table you posted above (unless you waited until the time caught up). The time that's sent depends on the time at which the session ID was created. So as long as the same session ID is sent it should not be possible that the time goes backwards (unless your system has issues with the monotonic clock, which is used for this).

>> Hm, that seems strange or even like a bug in FreeRADIUS, because the virtual IP is apparently still the same (at least in the table you posted). So why wouldn't it be tracked via the "new" session?

>> Yes, I mentioned that in #2856-1. I guess that could be added somehow, but needs some refactoring.
>
> The RADIUS server needs a unique identifier to track IPs when the session starts, none are sent.

That can't be done via Accounting-Start? (Since Accounting-Stop is apparently used to clear leases, maybe Accounting-Start could be used to confirm the lease and associate it with a session.)

> Either that or generate a new session ID every time the port changes and treat it as an entirely new session as far as RADIUS goes?

That won't really work because an IKE_SA rekeying (if that's the case here) does not affect the CHILD_SAs at all, so a new session ID would mess up your traffic stats.

#10 - 13.12.2018 18:02 - James Dogopoulos

> That can't be done via Accounting-Start? (Since Accounting-Stop is apparently used to clear leases, maybe Accounting-Start could be used to confirm the lease and associate it with a session.)

Well radius is assigning dynamic IPs in this situation so it would be nice to update its database with a unique ID that ties it directly to the session right from the start. It could wait for the first accounting packet but really authentication should be able to work without accounting and IPs are handed out as part of that process.

I just noticed freeradius is generating its acctuniqueid with an md5 hash that includes the NAS-Port, so when the nas port changes it changes the acctuniqueid and creates a new db record, leaving behind a stale one... I just removed nas-port from it since its plenty unique without it. This seems to have fixed the problem of multiple records in the database but there are still issues with handling things when the NAS Port changes as far as IPs go. Freeradius only allows identifiers to be used to track IPs if they are in both auth and acct packets. So when the NAS Port changes it no longer advances the lease time of the IP for that client and IPs get assigned multiple times. I'll try to find an easy way around this and will report back as I get more info.

Thanks for the fast responses to everything.

#11 - 14.12.2018 09:36 - Tobias Brunner

> I just noticed freeradius is generating its acctuniqueid with an md5 hash that includes the NAS-Port, so when the nas port changes it changes the acctuniqueid and creates a new db record, leaving behind a stale one... I just removed nas-port from it since its plenty unique without it. This seems to have fixed the problem of multiple records in the database

OK, great.

> but there are still issues with handling things when the NAS Port changes as far as IPs go. Freeradius only allows identifiers to be used to track IPs if they are in both auth and acct packets. So when the NAS Port changes it no longer advances the lease time of the IP for that client and IPs get assigned multiple times.

I see. I pushed a patch to the *2853-radius-session-id* branch (based on the branch for #2856), which adds the session ID to Access-Request messages if accounting is enabled.

#12 - 14.12.2018 14:40 - Tobias Brunner

> I pushed a patch to the *2853-radius-session-id* branch (based on the branch for #2856), which adds the session ID to Access-Request messages if accounting is enabled.

Also, is the fix for #2856 actually necessary if the session ID is included in Access-Request? My thinking is that if the IP is associated with the session ID from the start, it could also be cleared if an Accounting-Stop message is received with that session ID, whether it actually includes the IP or not. Or doesn't it work like that with FreeRADIUS?

#13 - 14.12.2018 16:53 - James Dogopoulos

Good question and I'm not sure if it works like that in freeradius, i'll be doing more testing soon. I tend to think handing out a little more information can't hurt anything if it's relevant and not out of whack as far as RFCs go and would improve compatibility overall with other software.   Hopefully it doesn't break any compatibility instead though. :-)

#14 - 15.12.2018 19:15 - James Dogopoulos

This worked, nothing else needed to be done in freeradius.   It looks like the way it is currently coded, the acct-session-id can't be used for the sqlippool module unless it arrives in the Access-Request packet. In which case it gets populated and is usable as an identifier. IPs are handed out as part of the authentication process, so it really should assign an IP right away and tie it to a unique connection ID before accounting is even considered. I do think this is ideal. Thanks!

#15 - 17.12.2018 09:43 - Tobias Brunner

- Tracker changed from Issue to Feature

- Subject changed from iOS issue with EAP user/pass and RADIUS back end. to Add RADIUS Accounting Acct-Session-Id Attribute to Access-Request Messages

- Category set to libcharon

- Assignee set to Tobias Brunner

- Target version set to 5.7.2

- Affected version deleted (5.7.1)

- Resolution set to Fixed

OK, good, I'll push this patch to master today.

I guess you didn't test what happens in regards to #2856, did you? (i.e. if leases are released for clients that don't request a virtual IP with only the session ID patch and without Framed-IP-Address attribute in the Accounting-Stop message).

#16 - 17.12.2018 19:25 - James Dogopoulos

Nothing changed with #2856 , IPs still stayed leased if the connection fails. I think you could be right in thinking freeradius could reset the IPs based on the now sent Acct-Session-Id. Not sure if this would be a cleaner better way or not. The more info sent the better as long as it doesn't break anything else and they seem to think this method is better. In situations where people are using multiple access servers/VPN servers with the same IP pool, if radiusd thinks an IP is free but for some reason it is not cleared on the AS/VPNserver there could potentially be an issue using an IP that is already bound/routed. So strongswan taking care of it is probably safer from that point of view.   At least maybe, I haven't thought about it a whole lot. :-)

Your patch for 2856 seems to work fine and IPs are now being cleared right away after applying the 2856 patch.

#17 - 18.12.2018 10:43 - Tobias Brunner

- Status changed from Feedback to Closed

OK, thanks for the feedback. Both fixes are now in master.