strongSwan - Issue #3584

Separate ipsec.conf file per conn and separate ipsec.secrets file per conn

30.09.2020 11:49 - Andy Marliyev

Status:	Feedback		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.7.2	**Resolution:**	

Description

Hello,

We have too many conns in ipsec.conf and ipsec.secrets files. We want to include separate conn file per customer. means in ipsec.conf file include directory where located conns for each customer and secrets. How we can achieve this?

History

#1 - 30.09.2020 12:43 - Tobias Brunner

- Status changed from New to Feedback

> means in ipsec.conf file include directory where located conns for each customer and secrets. How we can achieve this?

You basically answered this question yourself, see the include statement in the man page for ipsec.conf (works the same for ipsec.secrets). swanctl.conf supports it too.

#2 - 30.09.2020 13:18 - Andy Marliyev

Tobias Brunner wrote:

> > means in ipsec.conf file include directory where located conns for each customer and secrets. How we can achieve this?
>
> You basically answered this question yourself, see the include statement in the man page for ipsec.conf (works the same for ipsec.secrets). swanctl.conf supports it too.

yes, we tried but no connection available when pointed to other .conf file.

#3 - 30.09.2020 15:50 - Andy Marliyev

Tobias Brunner wrote:

> > means in ipsec.conf file include directory where located conns for each customer and secrets. How we can achieve this?
>
> You basically answered this question yourself, see the include statement in the man page for ipsec.conf (works the same for ipsec.secrets). swanctl.conf supports it too.

ipsec.conf -> include /etc/ipsec.d/customers/*
ipsec.secrets -> include /etc/ipsec.d/customers_secrets/*

ipsec restart
Starting strongSwan 5.8.2 IPsec [starter]...
/etc/ipsec.d/customers_secrets/aws.secrets:2: syntax error, unexpected STRING [x.x.x.x]
invalid config file '/etc/ipsec.conf'
unable to start strongSwan -- fatal errors in config

#4 - 30.09.2020 15:53 - Tobias Brunner

> /etc/ipsec.d/customers_secrets/aws.secrets:2: syntax error, unexpected STRING [x.x.x.x]
> invalid config file '/etc/ipsec.conf'

> unable to start strongSwan -- fatal errors in config

Seems pretty clear, no?

#5 - 30.09.2020 16:01 - Andy Marliyev

Tobias Brunner wrote:

> > /etc/ipsec.d/customers_secrets/aws.secrets:2: syntax error, unexpected STRING [x.x.x.x]
> > invalid config file '/etc/ipsec.conf'
> > unable to start strongSwan -- fatal errors in config
>
> Seems pretty clear, no?

hmm, no. am configured secrets as same as in original file but not loading.

#6 - 30.09.2020 16:14 - Andy Marliyev

Tobias Brunner wrote:

> > /etc/ipsec.d/customers_secrets/aws.secrets:2: syntax error, unexpected STRING [x.x.x.x]
> > invalid config file '/etc/ipsec.conf'
> > unable to start strongSwan -- fatal errors in config
>
> Seems pretty clear, no?

yes :) got it working. ipsec up not detected conn name automatically, so am entered manually and changed secrets file location.

#7 - 30.09.2020 16:25 - Tobias Brunner

> ipsec up not detected conn name automatically

What do you mean? Detected automatically how?

> so am entered manually and changed secrets file location.

What does that mean?

#8 - 30.09.2020 16:31 - Andy Marliyev

Tobias Brunner wrote:

> > ipsec up not detected conn name automatically
>
> What do you mean? Detected automatically how?
>
> > so am entered manually and changed secrets file location.
>
> What does that mean?

when am typing ipsec up "twice TAB" no conn name is appearing. i am entered name manually to connect, now i am getting this but not connectiong:

Security Associations (0 up, 1 connecting):
testing[1]: CONNECTING, x.x.x.x[%any]...x.x.x.x[%any]

#9 - 30.09.2020 16:32 - Tobias Brunner

> when am typing ipsec up "twice TAB" no conn name is appearing.

Possibly a limitation of the bash completion script.

> now i am getting this but not connectiong:

Read the log.

#10 - 30.09.2020 16:35 - Andy Marliyev

Tobias Brunner wrote:

> > when am typing ipsec up "twice TAB" no conn name is appearing.
>
> Possibly a limitation of the bash completion script.
>
> > now i am getting this but not connectiong:
>
> Read the log.

dont think its bash completion cause when conn name is in ipsec.conf file, twice tab giving me all conns available in file, in this situation ipsec.conf is empty and all conns in other folder. in ipsec.conf file only this string -> include /etc/ipsec.d/customers/*

#11 - 30.09.2020 16:37 - Tobias Brunner

> dont think its bash completion cause when conn name is in ipsec.conf file, twice tab giving me all conns available in file

That functionality is provided by a script that's part of bash completion, it might not support include.

#12 - 30.09.2020 16:59 - Andy Marliyev

Tobias Brunner wrote:

> > dont think its bash completion cause when conn name is in ipsec.conf file, twice tab giving me all conns available in file
>
> That functionality is provided by a script that's part of bash completion, it might not support include.

file location that am mentioned in ipsec.conf via include, not functional, conn is not getting up, even tcpdump is empty on other side, not receiving any packet. configured logging in strongswan, no logs available, empty. Is there any suggestion about how to get multiple conn files outside of ipsec.conf?

#13 - 30.09.2020 17:05 - Tobias Brunner

> Is there any suggestion about how to get multiple conn files outside of ipsec.conf?

What do you mean? That has already been answered. If you don't get it to work, you did it incorrectly.

#14 - 30.09.2020 17:06 - Andy Marliyev

Tobias Brunner wrote:

> > Is there any suggestion about how to get multiple conn files outside of ipsec.conf?
>
> What do you mean? That has already been answered. If you don't get it to work, you did it incorrectly.

great, thank you.