

Distribution EOLE - Demande #33109

Seth 2.7.2 - Erreur démarrage DNS (service bind)

09/07/2021 03:17 PM - Borgne Stephane

Status:	Fermé	Start date:	09/07/2021
Priority:	Normal	Due date:	
Assigned To:		% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:		Spent time:	0.00 hour
Description (en pièce jointe, le .tar.gz du dossier /etc/bind) <p>Les lignes suivantes du statut du service bind semblent être "un reste" après essai de configuration de zones reverse DNS puis retour arrière (configuration et retour faites avec gen_config)</p> <pre>sept. 06 01:12:34 tst-seth-1 named[17687]: zone 173.10.in-addr.arpa\010CNF:d435cfe6-f8a7-4e3d-b454-2f43f2f2032f/NONE: has 0 SOA records sept. 06 01:12:34 tst-seth-1 named[17687]: zone 173.10.in-addr.arpa\010CNF:d435cfe6-f8a7-4e3d-b454-2f43f2f2032f/NONE: has no NS records</pre> <p>Les actions effectuées :</p> <ul style="list-style-type: none">- Tentative de configuration de résolution inverse DNS par gen_config- reconfigure => échec démarrage du service bind- suppression de la configuration reverse DNS par gen_config- reconfigure => toujours échec de démarrage du service bind <p>Le statut du service bind :</p> <pre>root@tst-seth-1:~# systemctl status bind9.service ❑ bind9.service - BIND Domain Name Server Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled) Active: failed (Result: exit-code) since Mon 2021-09-06 01:12:34 CEST; 1 day 13h ago Docs: man:named(8) Process: 17687 ExecStart=/usr/sbin/named -f \$OPTIONS (code=exited, status=1/FAILURE) Main PID: 17687 (code=exited, status=1/FAILURE) sept. 06 01:12:34 tst-seth-1 named[17687]: samba_dlz: configured writeable zone 'tstsavoie.fr' sept. 06 01:12:34 tst-seth-1 named[17687]: samba_dlz: configured writeable zone '173.10.in-addr.arpa' sept. 06 01:12:34 tst-seth-1 named[17687]: samba_dlz: configured writeable zone '0.173.10.in-addr.arpa' sept. 06 01:12:34 tst-seth-1 named[17687]: zone 173.10.in-addr.arpa\010CNF:d435cfe6-f8a7-4e3d-b454-2f43f2f2032f/NONE: has 0 SOA records sept. 06 01:12:34 tst-seth-1 named[17687]: zone 173.10.in-addr.arpa\010CNF:d435cfe6-f8a7-4e3d-b454-2f43f2f2032f/NONE: has no NS records sept. 06 01:12:34 tst-seth-1 named[17687]: samba_dlz: Failed to configure zone '173.10.in-addr.arpa CNF:d435cfe6-f8a7-4e3d-b454-2f43f2f2032f' sept. 06 01:12:34 tst-seth-1 named[17687]: loading configuration: bad zone sept. 06 01:12:34 tst-seth-1 named[17687]: exiting (due to fatal error) sept. 06 01:12:34 tst-seth-1 systemd[1]: bind9.service: Main process exited, code=exited, status=1/FAILURE sept. 06 01:12:34 tst-seth-1 systemd[1]: bind9.service: Failed with result 'exit-code'.</pre> <p>D'après la documentation samba https://wiki.samba.org/index.php/BIND9_DLZ_DNS_Back_End#New_DNS_Entries_Are_Not_Resolvable La commande "samba_upgradedns --dns-backend=BIND9_DLZ" devrait rétablir les "hard links" des fichiers dans les répertoires /var/lib/samba/private/sam.ldb.d/ et /var/lib/samba/private/dns/sam.ldb.d/ Ce qui n'est pas le cas sur notre serveur de test :</p> <pre>root@tst-seth-1:~# samba_upgradedns --dns-backend=BIND9_DLZ Reading domain information DNS accounts already exist No zone file /var/lib/samba/bind-dns/dns/TST-COLLEGES.FR.zone DNS records will be automatically created DNS partitions already exist</pre>			

dns-tst-seth-1 account already exists
See /var/lib/samba/bind-dns/named.conf for an example configuration include file for BIND
and /var/lib/samba/bind-dns/named.txt for further documentation required for secure DNS updates
Finished upgrading DNS

Ci-dessous, le listing des fichiers samba et des fichiers bind non "hard linké" :

```
root@tst-seth-1:~# ls -lai /var/lib/samba/private/sam.ldb.d/
total 93116
263285 drwx----- 2 root root 4096 sept. 7 14:59 .
263945 drwxr-xr-x 8 root root 4096 sept. 7 14:59 ..
263290 -rw----- 1 root root 20406272 sept. 7 15:03 CN%3DCONFIGURATION%2CDC%3DTST-COLLEGES%2CDC%3DFR.ldb
263297 -rw----- 1 root root 44859392 sept. 7 15:02
CN%3DSHEMA%2CCN%3DCONFIGURATION%2CDC%3DTST-COLLEGES%2CDC%3DFR.ldb
263303 -rw-rw---- 2 root bind 4247552 sept. 7 15:02
DC%3DDOMAINDNSZONES%2CDC%3DTST-COLLEGES%2CDC%3DFR.ldb
263304 -rw-rw---- 2 root bind 4247552 sept. 7 15:03
DC%3DFORESTDNSZONES%2CDC%3DTST-COLLEGES%2CDC%3DFR.ldb
263288 -rw----- 1 root root 21139456 sept. 7 15:03 DC%3DTST-COLLEGES%2CDC%3DFR.ldb
263286 -rw-rw---- 2 root bind 421888 sept. 6 01:13 metadata.tdb
root@tst-seth-1:~# ls -lai /var/lib/samba/bind-dns/dns/sam.ldb.d/
total 26024
262331 drwxrwx--- 2 root bind 4096 sept. 7 14:59 .
262208 drwxrwx--- 3 root bind 4096 sept. 7 14:59 ..
262385 -rw-rw---- 1 root bind 8200192 sept. 7 14:59 CN%3DCONFIGURATION%2CDC%3DTST-COLLEGES%2CDC%3DFR.ldb
262506 -rw-rw---- 1 root bind 8220672 sept. 7 14:59
CN%3DSHEMA%2CCN%3DCONFIGURATION%2CDC%3DTST-COLLEGES%2CDC%3DFR.ldb
263303 -rw-rw---- 2 root bind 4247552 sept. 7 15:02 DC%3DDOMAINDNSZONES%2CDC%3DTST-COLLEGES%2CDC%3DFR.ldb
263304 -rw-rw---- 2 root bind 4247552 sept. 7 15:03 DC%3DFORESTDNSZONES%2CDC%3DTST-COLLEGES%2CDC%3DFR.ldb
262332 -rw-rw---- 1 root bind 1286144 sept. 7 14:59 DC%3DTST-COLLEGES%2CDC%3DFR.ldb
263286 -rw-rw---- 2 root bind 421888 sept. 6 01:13 metadata.tdb
```

Related issues:		
Related to Distribution EOLE - Tâche #32957: Suivi du contact utilisateur pou...	Fermé	07/21/2021

History

#1 - 09/09/2021 11:41 AM - Joël Cuissinat

- Related to Tâche #32957: Suivi du contact utilisateur pour son problème de DNS added

#2 - 09/09/2021 11:59 AM - Gilles Grandgérard

Le pb est visible sur l'infra de test.

<https://dev-eole.ac-dijon.fr/jenkins/job/2.7.2/job/test-seth-001-2.7.2-amd64/475/console>
<https://dev-eole.ac-dijon.fr/jenkins/job/2.8.1/job/test-seth-001-2.8.1-amd64/185/consoleFull>
chercher "test New DNS Entries Are Not Resolvable"

les inodes sont différents.

C'est un bug.

#3 - 09/09/2021 03:34 PM - Gilles Grandgérard

Il ne faut pas trop regarder les 'hard links' dans [https://wiki.samba.org/index.php/BIND9_DLZ_DNS_Back_End#New_DNS_Entries_Are_Not_Resolvable] ...
Dans le code [<https://github.com/samba-team/samba/blob/master/python/samba/provision/sambadns.py>], ce sont des tdb_copy qui sont exécutées...
et dans [https://github.com/samba-team/samba/blob/master/python/samba/tdb_util.py] il n'y a pas d'os.link, mais l'utilisation de tdbbackup (qui explique aussi la différence de taille des fichiers) ... Donc, certains fichiers sont des liens physiques, les autres non !

Le contournement serait de basculer en mode non Bind, puis re-passer en mode Bind.

```
systemctl stop samba-ad-dc.service
systemctl stop bind9.service

ls -lai /var/lib/samba/private/sam.ldb.d/
samba_upgradedns --dns-backend=SAMBA_INTERNAL
ls -lai /var/lib/samba/bind-dns/dns/ (==> vide !)
samba_upgradedns --dns-backend=BIND9_DLZ
ls -lai /var/lib/samba/bind-dns/dns/sam.ldb.d/

systemctl start bind9.service
systemctl status bind9.service --no-pager
systemctl start samba-ad-dc.service
systemctl status samba-ad-dc.service --no-pager

journalctl -xe -u bind9.service --no-pager
journalctl -xe -u samba-ad-dc.service --no-pager
```

#4 - 09/09/2021 04:57 PM - Borgne Stephane

Pas de changement après avoir exécuté le switch BIND_DLZ/SAMBA_INTERNAL/BIND_DLZ, le service bind échoue au démarrage avec les mêmes erreurs.

```
root@tst-seth-1:~# systemctl status bind9.service
[] bind9.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
Active: failed (Result: exit-code) since Thu 2021-09-09 16:53:23 CEST; 6s ago
Docs: man:named(8)
Process: 26513 ExecStart=/usr/sbin/named -f $OPTIONS (code=exited, status=1/FAILURE)
Main PID: 26513 (code=exited, status=1/FAILURE)

sept. 09 16:53:23 tst-seth-1 named26513: samba_dlz: configured writeable zone 'tstsavoie.fr'
sept. 09 16:53:23 tst-seth-1 named26513: samba_dlz: configured writeable zone '173.10.in-addr.arpa'
sept. 09 16:53:23 tst-seth-1 named26513: samba_dlz: configured writeable zone '0.173.10.in-addr.arpa'
sept. 09 16:53:23 tst-seth-1 named26513: zone 173.10.in-addr.arpa\010CNF:d435cfe6-f8a7-4e3d-b454-2f43f2f2032f/NONE: has 0 SOA records
sept. 09 16:53:23 tst-seth-1 named26513: zone 173.10.in-addr.arpa\010CNF:d435cfe6-f8a7-4e3d-b454-2f43f2f2032f/NONE: has no NS records
sept. 09 16:53:23 tst-seth-1 named26513: samba_dlz: Failed to configure zone '173.10.in-addr.arpa
CNF:d435cfe6-f8a7-4e3d-b454-2f43f2f2032f'
sept. 09 16:53:23 tst-seth-1 named26513: loading configuration: bad zone
sept. 09 16:53:23 tst-seth-1 named26513: exiting (due to fatal error)
sept. 09 16:53:23 tst-seth-1 systemd1: bind9.service: Main process exited, code=exited, status=1/FAILURE
sept. 09 16:53:23 tst-seth-1 systemd1: bind9.service: Failed with result 'exit-code'.
```

#5 - 09/20/2021 04:35 PM - Gilles Grandg rard

OK. C'est dans l'annuaire AD que la donn e n'est pas correcte.
Il faut utiliser RSAT avec DNS Servers et identifier la zone incorrecte. Puis la supprimer.

#6 - 10/06/2021 04:52 PM - Borgne Stephane

L'utilisation de RSAT n' tait pas possible car le service bind refusait de d marrer.

Les commandes suivantes ont permis de supprimer de l'AD les zones incoh rents par rapport aux fichiers bind.

```
samba-tool dns zonedelete 173.10.in-addr.arpa -P
samba-tool dns zonedelete localhost 173.10.in-addr.arpa -P
samba-tool dns zonelist localhost -P
samba-tool dns zonedelete localhost "173.10.in-addr.arpa" -P
samba-tool dns zonedelete localhost "173.10.in-addr.arpa CNF:d435cfe6-f8a7-4e3d-b454-2f43f2f2032f" -P
samba-tool dns zonedelete localhost "173.10.in-addr.arpa" -P
samba-tool dns zonelist localhost -P
samba-tool dns zonelist localhost -P
samba-tool dns zonedelete localhost "0.173.10.in-addr.arpa" -P
samba-tool dns zonelist localhost -P
samba-tool dns zonelist localhost -P
samba-tool dns zonelist localhost -P
samba-tool dns zonedelete localhost "173.10.in-addr.arpa" -P
samba-tool dns zonelist localhost -P
samba-tool dns zonedelete localhost "CNF:d435cfe6-f8a7-4e3d-b454-2f43f2f2032f" -P
samba-tool dns zonedelete localhost "173.10.in-addr.arpa CNF:d435cfe6-f8a7-4e3d-b454-2f43f2f2032f" -P
samba-tool dns zonelist localhost -P
```

Je pense que c'est la d claration d'une zone 173.10 dans l'EAD qui est   l'origine du blocage.

Depuis la remise en service, la cr ation et la suppression des zones inverses via RSAT fonctionnent tr s bien.

La cr ation de zones inverses via l'EAD fonctionne elle aussi, avec l'inscription automatique des 2 seths.

Par contre, la suppression des zones inverses n'est pas effective lorsqu'on passe l'option de cr ation   "non" dans l'EAD, on se trouve alors avec une "incoh rence" entre config et fonctionnement effectif.

Apr s avoir mont  les "seth" de test en version 2.8.1, je vais effectuer de nouveaux tests.

  suivre...

#7 - 11/18/2021 10:52 AM - Borgne Stephane

Tests OK en 2.8.1 depuis l'outil RSAT de gestion des DNS sur notre infra de test.

Tests à faire pour définir les zones dans gen_config

#8 - 12/10/2021 12:15 PM - Gilles Grandgérard

Est-ce que l'on peut clore ?

#9 - 12/10/2021 12:15 PM - Gilles Grandgérard

- *Status changed from Nouveau to En attente d'informations*

#10 - 12/11/2021 10:20 AM - Joël Cuissinat

- *Status changed from En attente d'informations to Fermé*

Mail de Stéphane :

Oui, vous pouvez fermer ce ticket.

Files

bind.tar.gz	4.1 KB	09/07/2021	Borgne Stephane
-------------	--------	------------	-----------------