Puppet LDAP - Bug #32066

le profile ldap devrait conserver "systemd" dans nsswitch.conf

2019-12-23 05:09 PM - Gabriel Filion

Status:	Closed	**Start date:**	2019-12-23
Priority:	Normal	**Due date:**	
Assignee:	John B	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
RT ticket:		**Points:**	1
Affected versions:			

Description

quand on enable le profile ldap, on a ça comme changement:

```
Notice: /Stage[main]/Profile::Ldap/File[/etc/nsswitch.conf]/content:
--- /etc/nsswitch.conf    2019-12-19 19:09:26.532226134 -0500
+++ /tmp/puppet-file20191223-15484-1p439aa    2019-12-23 16:57:57.251642856 -0500
@@ -6,8 +6,8 @@
 # If you have the `glibc-doc-reference' and `info' packages installed, try:
 # `info libc "Name Service Switch"' for information about this file.

-passwd:         files ldap systemd
-group:          files ldap systemd
+passwd:         files ldap
+group:          files ldap
 shadow:         files ldap

 #possible config
```

selon cette doc là, le lookup systemd sert pour les services qui utilisent `DynamicUser=` pour utiliser un user non privilégié mais qui a pas besoin d'un user système.

http://man7.org/linux/man-pages/man8/nss-systemd.8.html

Donc on devrait probablement ramener le lookup `systemd` même si on configure ldap.

faudrait voir si c'est un changement qu'on doit faire pour seulement stretch+ ou bien si jessie aussi a systemd là par défaut.

History

#1 - 2019-12-23 05:49 PM - Gabriel Filion

- Status changed from New to In progress

- Assignee set to Gabriel Filion

jessie a pas `systemd` dans nsswitch.conf par défaut.

stretch non plus.

buster oui.

donc seulement buster+

#2 - 2020-01-06 10:48 AM - Kienan Stewart

- Parent task set to #32104

#3 - 2020-01-20 10:28 AM - Kienan Stewart

- Parent task changed from #32104 to #32250

#4 - 2020-02-04 06:05 PM - Gabriel Filion

- Parent task changed from #32250 to #32445

#5 - 2020-03-02 03:53 PM - Kienan Stewart

- Parent task changed from #32445 to #32714

#6 - 2020-06-26 01:28 PM - Gabriel Filion

- Parent task changed from #32714 to #33845

#7 - 2020-08-14 04:39 PM - Kienan Stewart

- Parent task changed from #33845 to #34262

#8 - 2020-10-01 04:05 PM - Kienan Stewart

- Parent task changed from #34262 to #34595

#9 - 2020-11-20 02:32 PM - Gabriel Filion

- Parent task changed from #34595 to #35035

#10 - 2021-01-18 11:43 AM - John B

- Assignee changed from Gabriel Filion to John B

#11 - 2021-02-03 03:24 PM - John B

- Status changed from In progress to Needs deployment

Bon, le changement était minime (littéralement rajouter "systemd" dans `site/profile/files/ldap/etc/nsswitch.conf`).
Par contre, c'est la partie **test** qui représente le gros du travail (en plus de tout le travail qu'il m'a fallu pour me remettre dans Puppet, voir comment LDAP est sétupé, comment NSS marche, pourquoi mes VMs m'ont demandé des mdp pour root etc).

Simplement:

- il faut déployer LDAP sur `pc_buster` et s'assurer qu'un service utilisant `DynamicUser` démarre toujours

Cependant:

- je ne suis pas vraiment certain d'avoir déployé LDAP correctement en local, j'ai utilisé `basic_instance` pour `pc_buster` mais il se plaignait tout le temps de `nss_ldap: could not connect to any LDAP server as (null)` pour `ldap://ldap0.office.koumbit.net` - est-ce que je suis sensé déployer tout un serveur LDAP en local pour mes tests?
- à aucun moment en déployant `basic_instance` le contenu de `/etc/nsswitch.conf` changeait pour enlever `systemd`, ça a l'air que ça reste dans le fichier une fois que ça y est
- j'ai déployé `basic_instance` avec et sans `systemd` dans `/etc/nsswitch.conf` et dans les deux cas mon service avec `DynamicUser=yes` marchait donc soit mes tests n'était pas complets soit la config n'est pas vitale ?

#12 - 2021-02-03 03:24 PM - John B

- Status changed from Needs deployment to Needs testing

#13 - 2021-02-22 10:44 AM - John B

- Status changed from Needs testing to Needs deployment

Merge ticket: https://redmine.koumbit.net/issues/35815

#14 - 2021-02-22 11:48 AM - John B

- Status changed from Needs deployment to In progress

#15 - 2021-02-24 04:01 PM - Kienan Stewart

Pour nsswitch.conf, de ce que je comprends est que ce n'est pas embêtant de lister un module qui n'est pas présent. Pour chaque module listé sous une base de données particulière, un objet partagé est loadé puis libc échoue de manière graceful s'il n'existe pas. Ref: https://www.gnu.org/software/libc/manual/html_node/Services-in-the-NSS-configuration.html

La librarie systemd est normalement fourni dans le package libnss-systemd. Celà est installé par défaut sur Debian buster, disponible mais ne pas installé par défaut sur Debian stretch et finalement ce n'est pas disponible sur Debian jessie.

Voici ce qui arrive sur Stretch si ce n'est pas installé et que systemd est placé avant files:

```
root@pc-stretch:/etc# strace -o /home/vagrant/output getent passwd vagrant
```

```
vagrant:x:942:942:vagrant,,,:/home/vagrant:/bin/bash
```

Puis dans le strace, on voit que systemd a été essayé mais la lib n'existe pas, donc ça a passé au prochain:

```
execve("/usr/bin/getent", ["getent", "passwd", "vagrant"], [/* 22 vars */]) = 0
brk(NULL)                               = 0x2350000
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=31603, ...}) = 0
mmap(NULL, 31603, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f58ddd24000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\0\4\2\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=1689360, ...}) = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f58ddd22000
mmap(NULL, 3795296, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f58dd76a000
mprotect(0x7f58dd8ff000, 2097152, PROT_NONE) = 0
mmap(0x7f58ddaff000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x195000) = 0x7f58dd
aff000
mmap(0x7f58ddb05000, 14688, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x7f58ddb05000
close(3)                                = 0
arch_prctl(ARCH_SET_FS, 0x7f58ddd23440) = 0
mprotect(0x7f58ddaff000, 16384, PROT_READ) = 0
mprotect(0x604000, 4096, PROT_READ)     = 0
mprotect(0x7f58ddd2c000, 4096, PROT_READ) = 0
munmap(0x7f58ddd24000, 31603)           = 0
brk(NULL)                               = 0x2350000
brk(0x2371000)                          = 0x2371000
open("/usr/lib/locale/locale-archive", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=2932240, ...}) = 0
mmap(NULL, 2932240, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f58dd49e000
close(3)                                = 0
socket(AF_UNIX, SOCK_STREAM|SOCK_CLOEXEC|SOCK_NONBLOCK, 0) = 3
connect(3, {sa_family=AF_UNIX, sun_path="/var/run/nscd/socket"}, 110) = -1 ENOENT (No such file or directory)
close(3)                                = 0
socket(AF_UNIX, SOCK_STREAM|SOCK_CLOEXEC|SOCK_NONBLOCK, 0) = 3
connect(3, {sa_family=AF_UNIX, sun_path="/var/run/nscd/socket"}, 110) = -1 ENOENT (No such file or directory)
close(3)                                = 0
open("/etc/nsswitch.conf", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=505, ...}) = 0
read(3, "# /etc/nsswitch.conf\n#\n# Example"..., 4096) = 505
read(3, "", 4096)                       = 0
close(3)                                = 0
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=31603, ...}) = 0
mmap(NULL, 31603, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f58ddd24000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/tls/x86_64/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or
directory)
stat("/lib/x86_64-linux-gnu/tls/x86_64", 0x7fff92df43c0) = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/tls/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directo
ry)
stat("/lib/x86_64-linux-gnu/tls", 0x7fff92df43c0) = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/x86_64/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or dire
ctory)
stat("/lib/x86_64-linux-gnu/x86_64", 0x7fff92df43c0) = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)
stat("/lib/x86_64-linux-gnu", {st_mode=S_IFDIR|0755, st_size=12288, ...}) = 0
open("/usr/lib/x86_64-linux-gnu/tls/x86_64/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file
 or directory)
stat("/usr/lib/x86_64-linux-gnu/tls/x86_64", 0x7fff92df43c0) = -1 ENOENT (No such file or directory)
open("/usr/lib/x86_64-linux-gnu/tls/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or dir
ectory)
stat("/usr/lib/x86_64-linux-gnu/tls", 0x7fff92df43c0) = -1 ENOENT (No such file or directory)
open("/usr/lib/x86_64-linux-gnu/x86_64/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or
directory)
stat("/usr/lib/x86_64-linux-gnu/x86_64", 0x7fff92df43c0) = -1 ENOENT (No such file or directory)
open("/usr/lib/x86_64-linux-gnu/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directo
ry)
stat("/usr/lib/x86_64-linux-gnu", {st_mode=S_IFDIR|0755, st_size=20480, ...}) = 0
open("/lib/tls/x86_64/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)
stat("/lib/tls/x86_64", 0x7fff92df43c0) = -1 ENOENT (No such file or directory)
```

```
open("/lib/tls/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)
stat("/lib/tls", 0x7fff92df43c0)        = -1 ENOENT (No such file or directory)
open("/lib/x86_64/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)
stat("/lib/x86_64", 0x7fff92df43c0)     = -1 ENOENT (No such file or directory)
open("/lib/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)
stat("/lib", {st_mode=S_IFDIR|0755, st_size=4096, ...}) = 0
open("/usr/lib/tls/x86_64/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)
stat("/usr/lib/tls/x86_64", 0x7fff92df43c0) = -1 ENOENT (No such file or directory)
open("/usr/lib/tls/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)
stat("/usr/lib/tls", 0x7fff92df43c0)    = -1 ENOENT (No such file or directory)
open("/usr/lib/x86_64/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)
stat("/usr/lib/x86_64", 0x7fff92df43c0) = -1 ENOENT (No such file or directory)
open("/usr/lib/libnss_systemd.so.2", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)
stat("/usr/lib", {st_mode=S_IFDIR|0755, st_size=4096, ...}) = 0
munmap(0x7f58ddd24000, 31603)           = 0
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=31603, ...}) = 0
mmap(NULL, 31603, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f58ddd24000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/libnss_compat.so.2", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260\22\0\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0644, st_size=31616, ...}) = 0
mmap(NULL, 2126944, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f58dd296000
mprotect(0x7f58dd29d000, 2093056, PROT_NONE) = 0
mmap(0x7f58dd49c000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x6000) = 0x7f58dd49c
000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/libnsl.so.1", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\320?\0\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0644, st_size=89064, ...}) = 0
mmap(NULL, 2194008, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f58dd07e000
mprotect(0x7f58dd092000, 2097152, PROT_NONE) = 0
mmap(0x7f58dd292000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x14000) = 0x7f58dd29
2000
mmap(0x7f58dd294000, 6744, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x7f58dd294000
close(3)                                = 0
mprotect(0x7f58dd292000, 4096, PROT_READ) = 0
mprotect(0x7f58dd49c000, 4096, PROT_READ) = 0
munmap(0x7f58ddd24000, 31603)           = 0
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=31603, ...}) = 0
mmap(NULL, 31603, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f58ddd24000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/libnss_nis.so.2", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\340 \0\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0644, st_size=47688, ...}) = 0
mmap(NULL, 2143656, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f58dce72000
mprotect(0x7f58dce7d000, 2093056, PROT_NONE) = 0
mmap(0x7f58dd07c000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0xa000) = 0x7f58dd07c
000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/libnss_files.so.2", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\320!\0\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0644, st_size=47632, ...}) = 0
mmap(NULL, 2168600, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f58dcc60000
mprotect(0x7f58dcc6a000, 2097152, PROT_NONE) = 0
mmap(0x7f58dce6a000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0xa000) = 0x7f58dce6a
000
mmap(0x7f58dce6c000, 22296, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x7f58dce6c000
close(3)                                = 0
mprotect(0x7f58dce6a000, 4096, PROT_READ) = 0
mprotect(0x7f58dd07c000, 4096, PROT_READ) = 0
munmap(0x7f58ddd24000, 31603)           = 0
open("/etc/passwd", O_RDONLY|O_CLOEXEC) = 3
lseek(3, 0, SEEK_CUR)                   = 0
fstat(3, {st_mode=S_IFREG|0644, st_size=3621, ...}) = 0
mmap(NULL, 3621, PROT_READ, MAP_SHARED, 3, 0) = 0x7f58ddd2b000
lseek(3, 3621, SEEK_SET)                = 3621
munmap(0x7f58ddd2b000, 3621)            = 0
close(3)                                = 0
fstat(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
```

```
write(1, "vagrant:x:942:942:vagrant,,,:/ho"..., 53) = 53
exit_group(0)                           = ?
+++ exited with 0 +++
```

Tout celà pour dire que même si la librarie n'existe pas sur jessie ni stretch, je pense pas que ça pose un problème. La pénalité est un peu de perte de performance sur des loads d'objet partagé qui échouera tjrs.

#16 - 2021-02-24 04:04 PM - Kienan Stewart

- Status changed from In progress to Closed