eole-common - Tâche #35153

Scénario # 34941 (Terminé (Sprint)): [EOLE 2.9] Impossibilité d'instancier DC2 si un service podman est installé sur le DC1 avant instance

Vérifier le cas AmonEcole

15/12/2022 10:57 - Joël Cuissinat

Statut:	Fermé	**Début:**	15/12/2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Philippe Caseiro	**% réalisé:**	100%
Version cible:	Livraison Cadoles 31/03/2023	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Je n'ai pas forcément constaté de dysfonctionnement, mais cela m'interroge :

```
root@amonecole:~# CreoleRun "grep interfaces /etc/samba/smb.conf" all
Exécution de la commande [grep interfaces /etc/samba/smb.conf] dans le conteneur internet

  interfaces = 10.3.2.2

Exécution de la commande [grep interfaces /etc/samba/smb.conf] dans le conteneur bdd

grep: /etc/samba/smb.conf: Aucun fichier ou dossier de ce type

Exécution de la commande [grep interfaces /etc/samba/smb.conf] dans le conteneur reseau

  interfaces = 192.168.0.33

Exécution de la commande [grep interfaces /etc/samba/smb.conf] dans le conteneur partage

  interfaces = 192.168.0.33/255.255.255.0 10.3.2.1/255.255.255.0

Exécution de la commande [grep interfaces /etc/samba/smb.conf] dans le conteneur addc

  interfaces = 192.168.0.33/255.255.255.0 10.3.2.1/255.255.255.0
```

Révisions associées

Révision 86bc04c7 - 15/02/2023 12:30 - Joël Cuissinat

AmonEcole : remove deprecated "encrypt passwords" parameter

Ref: #35153

Révision 9ddaec6d - 15/02/2023 12:42 - Joël Cuissinat

AmonEcole : remove unnecessary "password server" parameter

Ref: #35153

Révision cfdd8a2a - 16/02/2023 14:14 - Joël Cuissinat

Proxy : remove deprecated "encrypt passwords" parameter

Ref: #35153

Révision 3b89cfb0 - 17/02/2023 15:47 - Joël Cuissinat

Revert "AmonEcole : remove unnecessary "password server" parameter"

This reverts commit 9ddaec6decc6210f9b3ad793de855c79d0da0d88.

Ref: #35153

Historique

#1 - 15/12/2022 11:11 - Joël Cuissinat

Dans le conteneur **addc**, on dirait que samba écrase les valeurs ???

```
root@addc:~# grep interfaces /etc/samba/smb.conf
  interfaces = 192.168.0.33/255.255.255.0 10.3.2.1/255.255.255.0
root@addc:~# testparm -vs 2>&1| grep "interfaces ="
    interfaces = 10.3.2.5
```

#2 - 15/12/2022 11:27 - Gilles Grandgérard

root@amonecole:~# CreoleRun "testparm -s" all
Exécution de la commande [testparm -s] dans le conteneur internet

Load smb config files from /etc/samba/smb.conf
lpcfg_do_global_parameter: WARNING: The "encrypt passwords" option is deprecated
Loaded services file OK.
Weak crypto is allowed

WARNING: The setting 'security=ads' should NOT be combined with the 'password server' parameter.
(by default Samba will discover the correct DC to contact automatically).

Server role: ROLE_DOMAIN_MEMBER

1. Global parameters
   [global]
   domain master = No
   idmap gid = 10000-20000
   idmap uid = 10000-20000
   interfaces = 10.3.2.2
   local master = No
   os level = 0
   password server = addc.etb3.lan
   preferred master = No
   realm = ETB3.LAN
   security = ADS
   server string = %h server (Samba %v)
   winbind separator = /
   winbind use default domain = Yes
   workgroup = ETB3
   idmap config * : range = 10000-20000
   idmap config * : backend = tdb

Exécution de la commande [testparm -s] dans le conteneur bdd

bash: ligne 1: testparm : commande introuvable

Exécution de la commande [testparm -s] dans le conteneur reseau

bash: ligne 1: testparm : commande introuvable

Exécution de la commande [testparm -s] dans le conteneur partage

Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_DOMAIN_MEMBER

1. Global parameters
   [global]
   cups server = /var/run/cups/cups.sock:631
   deadtime = 15
   disable netbios = Yes
   interfaces = 10.3.2.3
   netbios name = SCRIBE
   realm = ETB3.LAN
   restrict anonymous = 2
   security = ADS
   smb ports = 445
   template homedir = /home/adhomes/%U
   unix extensions = No
   usershare max shares = 0
   winbind enum groups = Yes
   winbind enum users = Yes
   winbind max clients = 400
   winbind refresh tickets = Yes
   winbind request timeout = 30
   winbind separator = /
   winbind use default domain = Yes
   workgroup = ETB3
   full_audit:priority = NOTICE
   full_audit:failure = none
   full_audit:success = connect
   full_audit:prefix = %T|%u|%h|%U|%I
   idmap config etb3:range = 1000000-1999999
   idmap config etb3:backend = rid
   idmap config *:range = 2000-999999
   idmap config * : backend = tdb
   acl allow execute always = Yes
   admin users = "@Domain Admins"
   hide files = /desktop.ini/
   include = /etc/samba/conf.d/interface.global
   level2 oplocks = No
   map acl inherit = Yes
   oplocks = No
   vfs objects = full_audit acl_xattr
   wide links = Yes

[printers]
browseable = No
comment = All Printers
path = /var/spool/samba
printable = Yes

[print$]
create mask = 0664
directory mask = 0775
force group = "Print Operators"
path = /var/lib/samba/printers
valid users = "@Print Operators" "@Domain Users"
vfs objects =
write list = "@Print Operators"

[homes]
browseable = No
comment = Home Directories
include = /etc/samba/conf.d/nextcloud.conf
path = "/home/adhomes/%U"
read only = No
root preexec = /usr/share/eole/sbin/create_adhome.sh "%U" "/home/adhomes"

[nextcloud]
comment = disque groupes
create mask = 0664
directory mask = 0775
include = /etc/samba/conf.d/wpkg.conf
inherit acls = Yes

```
inherit permissions = Yes
 invalid users = nobody guest
path = %H/.ftp
read only = No
valid users = %U
write list = %U

[wpkg]
browseable = No
guest ok = Yes
include = /etc/samba/conf.d/eole.conf
inherit acls = Yes
inherit permissions = Yes
path = /home/wpkg
read only = No

[opt1]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/opt1
read only = No
valid users = @opt1 "@Domain Admins"
write list = @opt1

[profs-5a]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-5a
read only = No
valid users = @profs-5a "@Domain Admins"
write list = @profs-5a

[profs-cycle3]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-cycle3
read only = No
valid users = @profs-cycle3 "@Domain Admins"
write list = @profs-cycle3

[c43]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/c43
read only = No
valid users = @c43 "@Domain Admins"
write list = @c43

[profs-opt1]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-opt1
read only = No
valid users = @profs-opt1 "@Domain Admins"
write list = @profs-opt1

[3a]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/3a
read only = No
valid users = @3a "@Domain Admins"
write list = @3a

[profs-3a]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-3a
```

```
read only = No
valid users = @profs-3a "@Domain Admins"
write list = @profs-3a

[3b]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/3b
read only = No
valid users = @3b "@Domain Admins"
write list = @3b

[5b]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/5b
read only = No
valid users = @5b "@Domain Admins"
write list = @5b

[profs-c33]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-c33
read only = No
valid users = @profs-c33 "@Domain Admins"
write list = @profs-c33

[opt2]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/opt2
read only = No
valid users = @opt2 "@Domain Admins"
write list = @opt2

[profs-5b]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-5b
read only = No
valid users = @profs-5b "@Domain Admins"
write list = @profs-5b

[profs-6a]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-6a
read only = No
valid users = @profs-6a "@Domain Admins"
write list = @profs-6a

[6a]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/6a
read only = No
valid users = @6a "@Domain Admins"
write list = @6a

[profs-c41]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-c41
read only = No
valid users = @profs-c41 "@Domain Admins"
write list = @profs-c41
```

```
[c32]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/c32
read only = No
valid users = @c32 "@Domain Admins"
write list = @c32

[profs-3b]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-3b
read only = No
valid users = @profs-3b "@Domain Admins"
write list = @profs-3b

[cycle3]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/cycle3
read only = No
valid users = @cycle3 "@Domain Admins"
write list = @cycle3

[c41]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/c41
read only = No
valid users = @c41 "@Domain Admins"
write list = @c41

[profs-mmeleveque]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-mmeleveque
read only = No
valid users = @profs-mmeleveque "@Domain Admins"
write list = @profs-mmeleveque

[profs-c32]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-c32
read only = No
valid users = @profs-c32 "@Domain Admins"
write list = @profs-c32

[commun]
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/commun
read only = No

[profs-4a]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-4a
read only = No
valid users = @profs-4a "@Domain Admins"
write list = @profs-4a

[6b]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/6b
read only = No
```

```
valid users = @6b "@Domain Admins"
write list = @6b

[4b]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/4b
read only = No
valid users = @4b "@Domain Admins"
write list = @4b

[c31]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/c31
read only = No
valid users = @c31 "@Domain Admins"
write list = @c31

[c42]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/c42
read only = No
valid users = @c42 "@Domain Admins"
write list = @c42

[profs-c31]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-c31
read only = No
valid users = @profs-c31 "@Domain Admins"
write list = @profs-c31

[groupes]
create mask = 0664
directory mask = 0775
inherit acls = Yes
inherit permissions = Yes
path = %H/groupes
read only = No
valid users = %U
write list = %U

[profs-4b]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-4b
read only = No
valid users = @profs-4b "@Domain Admins"
write list = @profs-4b

[profs-opt2]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-opt2
read only = No
valid users = @profs-opt2 "@Domain Admins"
write list = @profs-opt2

[4a]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/4a
read only = No
valid users = @4a "@Domain Admins"
write list = @4a
```

```
[profs-c42]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-c42
read only = No
valid users = @profs-c42 "@Domain Admins"
write list = @profs-c42

[profs-6b]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-6b
read only = No
valid users = @profs-6b "@Domain Admins"
write list = @profs-6b

[c33]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/c33
read only = No
valid users = @c33 "@Domain Admins"
write list = @c33

[5a]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/5a
read only = No
valid users = @5a "@Domain Admins"
write list = @5a

[professeurs]
browseable = No
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/professeurs
read only = No
valid users = @professeurs "@Domain Admins"
write list = @professeurs

[mmeleveque]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/mmeleveque
read only = No
valid users = @mmeleveque "@Domain Admins"
write list = @mmeleveque

[icones$]
browseable = No
path = /home/netlogon/icones
read only = No

[profs-c43]
create mask = 0644
inherit acls = Yes
inherit permissions = Yes
path = /home/workgroups/profs-c43
read only = No
valid users = @profs-c43 "@Domain Admins"
write list = @profs-c43

[devoirs]
browseable = No
create mask = 0664
directory mask = 0775
inherit acls = Yes
inherit permissions = Yes
```

path = %H/devoirs
read only = No
valid users = %U
write list = %U

Exécution de la commande [testparm -s] dans le conteneur addc

Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_ACTIVE_DIRECTORY_DC

1. Global parameters
   [global]
   cups server = /var/run/cups/cups.sock:631
   deadtime = 15
   disable netbios = Yes
   interfaces = 10.3.2.5
   passdb backend = samba_dsdb
   realm = ETB3.LAN
   restrict anonymous = 2
   server role = active directory domain controller
   server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl, winbindd, ntp_signd, kcc, dnsupdate
   smb ports = 445
   template homedir = /home/adhomes/%U
   tls cafile =
   tls certfile = /var/lib/samba/private/tls/certs/addc.crt
   tls keyfile = /var/lib/samba/private/tls/private/addc.key
   unix extensions = No
   usershare max shares = 0
   winbind enum groups = Yes
   winbind enum users = Yes
   winbind max clients = 400
   winbind refresh tickets = Yes
   winbind request timeout = 30
   winbind separator = /
   winbind use default domain = Yes
   workgroup = ETB3
   rpc_server:tcpip = no
   rpc_daemon:spoolssd = embedded
   rpc_server:spoolss = embedded
   rpc_server:winreg = embedded
   rpc_server:ntsvcs = embedded
   rpc_server:eventlog = embedded
   rpc_server:srvsvc = embedded
   rpc_server:svcctl = embedded
   rpc_server:default = external
   winbindd:use external pipes = true
   full_audit:priority = NOTICE
   full_audit:failure = none
   full_audit:success = connect
   full_audit:prefix = %T|%u|%h|%U|%I
   idmap config * : backend = tdb
   acl allow execute always = Yes
   admin users = "@Domain Admins"
   hide files = /desktop.ini/
   include = /etc/samba/conf.d/interface.global
   level2 oplocks = No
   map acl inherit = Yes
   map archive = No
   oplocks = No
   vfs objects = acl_xattr dfs_samba4 full_audit
   wide links = Yes

[printers]
browseable = No
comment = All Printers
path = /var/spool/samba
printable = Yes

[print$]
create mask = 0664
directory mask = 0775
force group = "Print Operators"

path = /var/lib/samba/printers
valid users = "@Print Operators" "@Domain Users"
vfs objects =
write list = "@Print Operators"

[netlogon]
comment = Network Logon Service
guest ok = Yes
path = /home/sysvol/etb3.lan/scripts
read only = No
vfs objects = dfs_samba4 acl_xattr

[sysvol]
comment = Sysvol Service
guest ok = Yes
path = /home/sysvol
read only = No
vfs objects = dfs_samba4 acl_xattr

#3 - 15/12/2022 16:10 - Benjamin Bohard

La bonne commande pour savoir ce qui est configuré est celle-ci :

```
root@amonecole:~#  CreoleRun "[ -d /etc/samba/ ] && grep -RI interfaces /etc/samba/" all
Exécution de la commande [[ -d /etc/samba/ ] && grep -RI interfaces /etc/samba/] dans le conteneur internet

/etc/samba/smb.conf:  interfaces = 10.3.2.2

Exécution de la commande [[ -d /etc/samba/ ] && grep -RI interfaces /etc/samba/] dans le conteneur bdd

Exécution de la commande [[ -d /etc/samba/ ] && grep -RI interfaces /etc/samba/] dans le conteneur reseau

/etc/samba/smb.conf:  interfaces = 192.168.0.33

Exécution de la commande [[ -d /etc/samba/ ] && grep -RI interfaces /etc/samba/] dans le conteneur partage

/etc/samba/smb.conf:  interfaces = 192.168.0.33/255.255.255.0 10.3.2.1/255.255.255.0
/etc/samba/conf.d/interface.global:interfaces = 10.3.2.3

Exécution de la commande [[ -d /etc/samba/ ] && grep -RI interfaces /etc/samba/] dans le conteneur addc

/etc/samba/smb.conf:  interfaces = 192.168.0.33/255.255.255.0 10.3.2.1/255.255.255.0
/etc/samba/conf.d/interface.global:interfaces = 10.3.2.5
```

Comme on le voit toutes les valeurs sont soit bonne, soit écrasé par une inclusion avec la bonne valeur.

Seul le conteneur réseau (en fait web) n'est pas bon, mais on ne s'en sert que pour configurer le client samba :
https://dev-eole.ac-dijon.fr/issues/32071

Les observations effectuées ne semblent pas problématiques.

#4 - 27/12/2022 09:58 - Benjamin Bohard

- Statut changé de Nouveau à À valider

#5 - 02/02/2023 14:47 - Laurent Gourvenec

- Statut changé de À valider à Résolu

- Assigné à mis à Philippe Caseiro

- % réalisé changé de 0 à 100

#6 - 15/02/2023 12:10 - Joël Cuissinat

https://www.samba.org/samba/history/samba-4.11.0.html

```
The "lanman auth" and "encrypt passwords" parameters are deprecated
with this release as both are only applicable to SMB1 and are quite
insecure.  NTLM, NTLMv2 and Kerberos authentication are unaffected, as
"encrypt passwords = yes" has been the default since Samba 3.0.0.
```

```
root@amonecole:~# rgrep "encrypt passwords"  /usr/share/eole/creole/distrib/
/usr/share/eole/creole/distrib/smb-proxy_auth.conf:  encrypt passwords = true
/usr/share/eole/creole/distrib/smb-ad-master.conf:  encrypt passwords = true
```

Cf. #30773 (idem AmonEcole 2.8.1)

Je propose de supprimer ce paramètre en 2.9 ;)

#7 - 15/02/2023 12:40 - Joël Cuissinat

Concernant "password server" ça fait longtemps qu'il a été supprimé sur ScribeAD/HorusAD :
https://dev-eole.ac-dijon.fr/projects/eole-ad/repository/revisions/17d21ed0d247a4c0730626f8b22a3115c55ffbce/diff

On peut tenter de l'enlever sur AmonEcole 2.9 voir ce que ça donne ;)

#8 - 16/02/2023 14:16 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0

#9 - 17/02/2023 15:47 - Joël Cuissinat

- Temps estimé mis à 0.00 h

Finalement, on dirait que **password server** est nécessaire dans le cas où l'on souhaite uniquement la résolution winbind comme sur le conteneur "root" d'AmonEcole :

```
root@amonecole:~# id admin
id: «admin» : utilisateur inexistant
root@amonecole:~# echo "  password server = addc.etb3.lan" >> /etc/samba/smb.conf
root@amonecole:~# systemctl restart winbind.service
root@amonecole:~# id admin
uid=1001116(admin) gid=1000513(domain users) groupes=1000513(domain users),1001116(admin),1001108(professeurs)
,1000512(domain admins),1000572(denied rodc password replication group)
```