Distribution EOLE - Tâche #25331

Scénario # 26377 (Terminé (Sprint)): Évolution de la configuration de Samba

Specifier le paramètrage des logs

10/02/2018 08:33 AM - Emmanuel IHRY

Status:	Fermé	**Start date:**	09/17/2018
Priority:	Normal	**Due date:**	
Assigned To:	Benjamin Bohard	**% Done:**	0%
Target version:	sprint 2019 2-4 Equipe MENSR	**Estimated time:**	0.00 hour
		Spent time:	0.00 hour

Description

La version samba 4.9 améliore la journalisation des événements et leur complétude. Les développements faits permettent la journalisation de toutes les modifications LDAP (mise en œuvre de log génériques pour tracer le changement de tout attribut dans le LDAP sur l'ensemble des partitions). Des développements ont été faits également pour logger les changements sur les membres d'un groupe.

Le format de sortie est JSON

Objectifs des travaux :
- étudier les options de paramétrage possibles pour les logs dans samba
- eoliser une partie de ces options
- voir s'il est possible d'avoir plusieurs fichiers journaux en sortie, spécialisés dans des types événements.

Exemple d'ajout d'un compte user : **Rajout de l'entrée utilisateur (eventid 4720)

log level = 0 dsdb_json_audit:9

JSON dsdbChange: {"timestamp": "2018-07-16T15:55:58.800653+0200", "type": "dsdbChange", "dsdbChange": {"version": {"major": 1, "minor": 0}, "statusCode": 0, "status": "Success", "operation": "Add", "remoteAddress": null, "performedAsSystem": false, "userSid": "S-1-5-18", "dn": "CN=toto,CN=Users,DC=kg", "transactionId": "4ba5a14e-76d8-4425-b781-70a5e942ce96", "sessionId": "be5e90c9-66ac-4dd4-a4a0-cb509c062ee6", "attributes": {"objectClass": {"actions": [{"action": "add", "values": [{"value": "user"}]}]}, "sAMAccountName": {"actions": [{"action": "add", "values": [{"value": "dcardon"}]}]}, "userPrincipalName": {"actions": [{"action": "add", "values": [{"value": "toto@kg.test"}]}]}}}}

Related issues:

Related to Documentations - Tâche #26609: Documenter les nouvelles options de...	**Fermé**	**02/10/2020**	**02/10/2020**
Related to eole-genconfig - Scénario #29588: Impossible de déclarer une "Caté...	**Terminé (Sprint)**	**02/07/2020**	**03/20/2020**

Associated revisions

Revision f478b38b - 01/10/2019 09:07 AM - Benjamin Bohard

Donner la possibilité de configurer le niveau de log de samba.

Ref #25331

Revision f8519dbb - 01/14/2019 03:55 PM - Benjamin Bohard

Suppression de certaines classes de journaux.

Ref #25331

Revision 8c9f43af - 01/22/2019 11:28 AM - Benjamin Bohard

Donner la possibilité de configurer le niveau de log de samba.

Ref #25331

Revision 8a5b651c - 01/22/2019 11:28 AM - Benjamin Bohard

Suppression de certaines classes de journaux.

Ref #25331

History

#1 - 10/02/2018 09:27 AM - Emmanuel IHRY

- Assigned To set to Remi BAPTISTE

#2 - 01/08/2019 08:28 AM - Emmanuel IHRY

- Assigned To deleted (Remi BAPTISTE)

Voir description du fonctionnement des logs dans le scénario associé #24597

Le besoin précis en terme d'éolisation du paramétrage des log sera spécifié par le MTES pour le 11/01 au + tard

#3 - 01/08/2019 09:37 AM - Benjamin Bohard

- Parent task changed from #24597 to #26377

#4 - 01/08/2019 09:38 AM - Benjamin Bohard

- Description updated

#5 - 01/09/2019 10:06 AM - Benjamin Bohard

- Project changed from EOLE AD DC to Distribution EOLE

- Status changed from Nouveau to En cours

#6 - 01/09/2019 10:27 AM - Benjamin Bohard

La liste des éléments à surveiller est assez conséquente :

- all
- tdb
- printdrivers
- lanman
- smb
- smb2
- mb2_credits
- rpc_parse
- rpc_srv
- rpc_cli
- passdb
- sam
- auth
- winbind
- vfs
- idmap
- quota
- acls
- locking
- msdfs
- dmapi
- registry
- scavenger
- dns
- ldb
- tevent
- auth_audit
- auth_json_audit
- kerberos
- dsdb_audit

- dsdb_json_audit
- dsdb_password_audit
- dsdb_password_json_audit
- dsdb_transaction_audit
- dsdb_transaction_json_audit

Est-ce qu'on propose tous ces éléments dans la configuration ou simplement un sous-ensemble ?

#7 - 01/09/2019 10:47 AM - Benjamin Bohard

Pour le changement à la volée du niveau de journalisation, la commande smbcontrol est toujours disponible :

```
root@dc1:~# smbcontrol smbd debuglevel
PID 860: all:0 tdb:0 printdrivers:0 lanman:0 smb:0 rpc_parse:0 rpc_srv:0 rpc_cli:0 passdb:0 sam:0 auth:0 winbi
nd:0 vfs:0 idmap:0 quota:0 acls:0 locking:0 msdfs:0 dmapi:0 registry:0 scavenger:0 dns:0 ldb:0 tevent:0 auth_a
udit:0 auth_json_audit:0 kerberos:0 drs_repl:0 smb2:0 smb2_credits:0 dsdb_audit:0 dsdb_json_audit:0 dsdb_passw
ord_audit:0 dsdb_password_json_audit:0 dsdb_transaction_audit:0 dsdb_transaction_json_audit:0 dsdb_group_audit
:0 dsdb_group_json_audit:0
root@dc1:~# smbcontrol smbd debug "3 kerberos:4"
root@dc1:~# smbcontrol smbd debuglevel
PID 860: all:3 tdb:3 printdrivers:3 lanman:3 smb:3 rpc_parse:3 rpc_srv:3 rpc_cli:3 passdb:3 sam:3 auth:3 winbi
nd:3 vfs:3 idmap:3 quota:3 acls:3 locking:3 msdfs:3 dmapi:3 registry:3 scavenger:3 dns:3 ldb:3 tevent:3 auth_a
udit:3 auth_json_audit:3 kerberos:4 drs_repl:3 smb2:3 smb2_credits:3 dsdb_audit:3 dsdb_json_audit:3 dsdb_passw
ord_audit:3 dsdb_password_json_audit:3 dsdb_transaction_audit:3 dsdb_transaction_json_audit:3 dsdb_group_audit
:3 dsdb_group_json_audit:3
```

On peut donc envisager un paramétrage normal effectué dans gen_config et un moyen de modifier temporairement ce niveau (prévoir une facilité pour le retour au niveau normal).

#8 - 01/09/2019 04:25 PM - Benjamin Bohard

- Description updated

- Assigned To set to Benjamin Bohard

#9 - 01/10/2019 04:48 PM - Emmanuel IHRY

*Vu le premier commit réalisé f478b38b, ça me parait une bonne solution ! * : çaa permet de configurer des niveaux de log à la carte et générer une syntaxe dans le smb.conf du type : log level = 1 auth_audit:3 auth_json_audit:9 dsdb_json_audit:9

QQ remarques ou questions :

1) Faut il ajouter un paramètre EOLE pour choisir la destination des logs (log file =)... ou bien sont ils dirigés naturellement dans rsyslog ?

2) Est-ce que c'est gênant dans le fichier de log d'avoir deux type de logs : json et pas json (voir ci après) ? Notamment si un jour on les exploite via outil spécifique.

Tout peut-il être au format Json ? Ou bien peut-on séparer dans deux fichiers les log json et les autres ?

```
[2019/01/10 16:23:11.226708,  0] ../source3/winbindd/winbindd_cache.c:3160(initialize_winbindd_cache)
  initialize_winbindd_cache: clearing cache and re-creating with version number 2
[2019/01/10 16:23:11.236819,  0] ../lib/util/become_daemon.c:138(daemon_ready)
  daemon_ready: STATUS=daemon 'winbindd' finished starting up and ready to serve connections
[2019/01/10 16:23:30.434487,  0] ../source4/dsdb/dns/dns_update.c:330(dnsupdate_nameupdate_done)
  ../source4/dsdb/dns/dns_update.c:330: Failed DNS update - with error code 110
[2019/01/10 16:23:51.357189,  5] ../lib/audit_logging/audit_logging.c:141(audit_log_json)
  JSON dsdbChange: {"timestamp": "2019-01-10T16:23:51.357081+0100", "type": "dsdbChange", "dsdbChange": {"vers
ion": {"major": 1, "minor": 0}, "statusCode": 0, "status": "Success", "operation": "Modify", "remoteAddress":
"ipv4:192.168.227.169:49515", "performedAsSystem": false, "userSid": "S-1-5-21-2039604760-904587110-1313591226
-500", "dn": "CN=p11.nfr", "transactionId": "7ac4b7f0-9a7f-4632-9a53-12b6fa5c970c", "sessionId": "52b4f932-7b9
e-4963-bd38-87f036d773c8", "attributes": {"description": {"actions": [{"action": "replace", "values": [{"value
": "rrrrrr"}]}]}}}}
```

3) Ca ne me gène pas qu'on laisse toutes ces valeurs dans la liste déroulante plutôt que de les rechercher en cas de besoin. Ce serait bien d'avoir une grande bulle d'aide qui explique ce qui se cache derrière chaque valeur mais je n'ai pas non plus la réponse !

<param>['all','tdb','printdrivers','lanman','smb','smb2','mb2_credits','rpc_parse','rpc_srv','rpc_cli','passdb','sam','auth','winbind','vfs','idmap','quota','acls','locking','msdfs','dmapi','registry','scavenger','dns','ldb','tevent','auth_audit','auth_json_audit','kerberos','dsdb_audit','dsdb_json_audit','dsdb_password_audit','dsdb_password_json_audit','dsdb_transaction_audit','dsdb_transaction_json_audit']</param>

#10 - 01/11/2019 05:04 PM - Emmanuel IHRY

Complément suite à lecture de https://www.samba.org/samba/history/samba-4.9.0.html

Supprimer ces valeurs dans la liste des valeurs possibles :

dsdb_audit
dsdb_password_audit
dsdb_group_audit

#11 - 01/14/2019 03:57 PM - Benjamin Bohard

La classe dsdb_group_audit n'était pas présente… Est-ce qu'il faut en ajouter d'autres qui seraient absentes ?

#12 - 01/22/2019 02:10 PM - Benjamin Bohard

Le passage des logs de Samba se fait toujours avec le même nom de programme et ne suffit pas à répartir en différents fichiers.
Il reste à tester le traitement des journaux au format json et l'utilisation du contenu du message pour répartir dans différents fichiers.

#13 - 01/24/2019 09:34 AM - Scrum Master

- Status changed from En cours to Résolu

#14 - 01/28/2019 11:41 AM - Joël Cuissinat

- Related to Tâche #26609: Documenter les nouvelles options de journalisation Samba added

#15 - 01/28/2019 11:44 AM - Joël Cuissinat

- Status changed from Résolu to Fermé

- Remaining (hours) set to 0.0

#16 - 02/07/2020 12:14 PM - Joël Cuissinat

- Related to Scénario #29588: Impossible de déclarer une "Catégorie d'événements à journaliser" avec Firefox 72/73 added