Distribution EOLE - Tâche #35616

Scénario # 35563 (Terminé (Sprint)): Étude : possibilité de générer des données statistiques à l'aide des logs générés via full_audit

Étude

09/10/2023 12:14 - Benjamin Bohard

Statut:	Fermé	**Début:**	01/10/2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Bohard	**% réalisé:**	100%
Version cible:	Livraison Cadoles 31/10/2023	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Historique

#1 - 09/10/2023 12:14 - Benjamin Bohard

- Statut changé de Nouveau à En cours

#2 - 09/10/2023 12:35 - Benjamin Bohard

La documentation du logiciel cité dans le document joint au scénario semble tirer partie des informations brutes suivantes :
- événement de connexion avec utilisateur et machine
- évènement de déconnexion avec utilisateur et machine.

Côté samba, ces événements précis ne sont pas journalisés. On dispose des événements d'authentification via les journaux auth_audit ou auth_json_audit, et des événements de connexion, déconnexion aux ressources réseaux via les journaux vfs_full_audit.

Exemple pour la connexion avec auth_audit et auth_json_audit

```
oct. 09 12:22:41 addc samba[6008]:   Auth: [Kerberos KDC,ENC-TS Pre-authentication] user [(null)]\[prenom.elev
e22@DOMPEDAGO] at [Mon, 09 Oct 2023 12:22:41.904863 CEST] with [aes256-cts-hmac-sha1-96] status [NT_STATUS_OK]
 workstation [(null)] remote host [ipv4:10.1.2.50:57221] became [DOMPEDAGO]\[prenom.eleve22] [S-1-5-21-2532775
984-2743565765-2173024361-1199]. local host [NULL]
oct. 09 12:22:41 addc samba[6008]:   {"timestamp": "2023-10-09T12:22:41.905133+0200", "type": "Authentication"
, "Authentication": {"version": {"major": 1, "minor": 2}, "eventId": 4624, "logonId": "7ccaf8b372cf9650", "log
onType": 3, "status": "NT_STATUS_OK", "localAddress": null, "remoteAddress": "ipv4:10.1.2.50:57221", "serviceD
escription": "Kerberos KDC", "authDescription": "ENC-TS Pre-authentication", "clientDomain": null, "clientAcco
unt": "prenom.eleve22@DOMPEDAGO", "workstation": null, "becameAccount": "prenom.eleve22", "becameDomain": "DOM
PEDAGO", "becameSid": "S-1-5-21-2532775984-2743565765-2173024361-1199", "mappedAccount": "prenom.eleve22", "ma
ppedDomain": "DOMPEDAGO", "netlogonComputer": null, "netlogonTrustAccount": null, "netlogonNegotiateFlags": "0
x00000000", "netlogonSecureChannelType": 0, "netlogonTrustAccountSid": null, "passwordType": "aes256-cts-hmac-
sha1-96", "duration": 2701}}
```

Et de déconnexion

```
oct. 09 12:24:25 addc samba[6008]:   Auth: [Kerberos KDC,ENC-TS Pre-authentication] user [(null)]\[prenom.elev
e22@DOMPEDAGO.ETB1.LAN] at [Mon, 09 Oct 2023 12:24:25.372460 CEST] with [aes256-cts-hmac-sha1-96] status [NT_S
TATUS_OK] workstation [(null)] remote host [ipv4:10.1.2.50:57253] became [DOMPEDAGO]\[prenom.eleve22] [S-1-5-2
1-2532775984-2743565765-2173024361-1199]. local host [NULL]
oct. 09 12:24:25 addc samba[6008]:   {"timestamp": "2023-10-09T12:24:25.372627+0200", "type": "Authentication"
, "Authentication": {"version": {"major": 1, "minor": 2}, "eventId": 4624, "logonId": "403efe62893f5fdf", "log
onType": 3, "status": "NT_STATUS_OK", "localAddress": null, "remoteAddress": "ipv4:10.1.2.50:57253", "serviceD
escription": "Kerberos KDC", "authDescription": "ENC-TS Pre-authentication", "clientDomain": null, "clientAcco
unt": "prenom.eleve22@DOMPEDAGO.ETB1.LAN", "workstation": null, "becameAccount": "prenom.eleve22", "becameDoma
in": "DOMPEDAGO", "becameSid": "S-1-5-21-2532775984-2743565765-2173024361-1199", "mappedAccount": "prenom.elev
e22", "mappedDomain": "DOMPEDAGO", "netlogonComputer": null, "netlogonTrustAccount": null, "netlogonNegotiateF
lags": "0x00000000", "netlogonSecureChannelType": 0, "netlogonTrustAccountSid": null, "passwordType": "aes256-
cts-hmac-sha1-96", "duration": 2538}}
oct. 09 12:24:25 addc samba[6029]:   Auth: [LDAP,simple bind/TLS] user [DOMPEDAGO]\[cn=eole-workstation-reader
,cn=Users,dc=dompedago,dc=etb1,dc=lan] at [Mon, 09 Oct 2023 12:24:25.798948 CEST] with [Plaintext] status [NT_
STATUS_OK] workstation [ADDC] remote host [ipv4:10.1.2.50:57256] became [DOMPEDAGO]\[eole-workstation-reader]
```

```
[S-1-5-21-2532775984-2743565765-2173024361-1112]. local host [ipv4:10.1.3.11:389]
oct. 09 12:24:25 addc samba[6029]:   {"timestamp": "2023-10-09T12:24:25.799944+0200", "type": "Authentication"
, "Authentication": {"version": {"major": 1, "minor": 2}, "eventId": 4624, "logonId": "0", "logonType": 8, "st
atus": "NT_STATUS_OK", "localAddress": "ipv4:10.1.3.11:389", "remoteAddress": "ipv4:10.1.2.50:57256", "service
Description": "LDAP", "authDescription": "simple bind/TLS", "clientDomain": "DOMPEDAGO", "clientAccount": "cn=
eole-workstation-reader,cn=Users,dc=dompedago,dc=etb1,dc=lan", "workstation": "ADDC", "becameAccount": "eole-w
orkstation-reader", "becameDomain": "DOMPEDAGO", "becameSid": "S-1-5-21-2532775984-2743565765-2173024361-1112"
, "mappedAccount": "eole-workstation-reader", "mappedDomain": "DOMPEDAGO", "netlogonComputer": null, "netlogon
TrustAccount": null, "netlogonNegotiateFlags": "0x00000000", "netlogonSecureChannelType": 0, "netlogonTrustAcc
ountSid": null, "passwordType": "Plaintext", "duration": 3950}}
oct. 09 12:24:28 addc samba[6029]:   Auth: [LDAP,simple bind/TLS] user [DOMPEDAGO]\[cn=eole-workstation-reader
,cn=Users,dc=dompedago,dc=etb1,dc=lan] at [Mon, 09 Oct 2023 12:24:28.591729 CEST] with [Plaintext] status [NT_
STATUS_OK] workstation [ADDC] remote host [ipv4:10.1.2.50:57261] became [DOMPEDAGO]\[eole-workstation-reader]
[S-1-5-21-2532775984-2743565765-2173024361-1112]. local host [ipv4:10.1.3.11:389]
oct. 09 12:24:28 addc samba[6029]:   {"timestamp": "2023-10-09T12:24:28.592453+0200", "type": "Authentication"
, "Authentication": {"version": {"major": 1, "minor": 2}, "eventId": 4624, "logonId": "0", "logonType": 8, "st
atus": "NT_STATUS_OK", "localAddress": "ipv4:10.1.3.11:389", "remoteAddress": "ipv4:10.1.2.50:57261", "service
Description": "LDAP", "authDescription": "simple bind/TLS", "clientDomain": "DOMPEDAGO", "clientAccount": "cn=
eole-workstation-reader,cn=Users,dc=dompedago,dc=etb1,dc=lan", "workstation": "ADDC", "becameAccount": "eole-w
orkstation-reader", "becameDomain": "DOMPEDAGO", "becameSid": "S-1-5-21-2532775984-2743565765-2173024361-1112"
, "mappedAccount": "eole-workstation-reader", "mappedDomain": "DOMPEDAGO", "netlogonComputer": null, "netlogon
TrustAccount": null, "netlogonNegotiateFlags": "0x00000000", "netlogonSecureChannelType": 0, "netlogonTrustAcc
ountSid": null, "passwordType": "Plaintext", "duration": 2769}}
```

On voit qu'en plus de l'authentification de l'utilisateur, on a l'authentification de eole-workstation-reader

Côté vfs_full_audit, on a, pour la seule connexion

```
oct. 09 12:29:21 addc smbd_audit[6118]: 2023/10/09 12:29:21|DOMPEDAGO/SCRIBE_|addc|scribe_|192.0.2.1|connect|o
k|IPC$
oct. 09 12:29:22 addc smbd_audit[6120]: 2023/10/09 12:29:22|DOMPEDAGO/prenom.eleve22|addc|prenom.eleve22|10.1.
2.50|connect|ok|sysvol
oct. 09 12:29:22 addc smbd_audit[6120]: 2023/10/09 12:29:22|DOMPEDAGO/PC-1122685_|addc|pc-1122685_|10.1.2.50|c
onnect|ok|sysvol
oct. 09 12:29:30 addc smbd_audit[6126]: 2023/10/09 12:29:30|DOMPEDAGO/prenom.eleve22|addc|prenom.eleve22|10.1.
2.50|connect|ok|IPC$
oct. 09 12:29:30 addc smbd_audit[6126]: 2023/10/09 12:29:30|DOMPEDAGO/prenom.eleve22|addc|prenom.eleve22|10.1.
2.50|connect|ok|sysvol
oct. 09 12:29:33 addc smbd_audit[6126]: 2023/10/09 12:29:33|DOMPEDAGO/prenom.eleve22|addc|prenom.eleve22|10.1.
2.50|connect|ok|netlogon
oct. 09 12:29:36 addc smbd_audit[6126]: 2023/10/09 12:29:36|DOMPEDAGO/PC-1122685_|addc|pc-1122685_|10.1.2.50|c
onnect|ok|netlogon
oct. 09 12:29:36 addc smbd_audit[6120]: 2023/10/09 12:29:36|DOMPEDAGO/PC-1122685_|addc|pc-1122685_|10.1.2.50|d
isconnect|ok|sysvol
```

et pour la déconnexion

```
oct. 09 12:32:01 addc smbd_audit[6203]: 2023/10/09 12:32:01|DOMPEDAGO/prenom.eleve22|addc|prenom.eleve22|10.1.
2.50|connect|ok|IPC$
oct. 09 12:32:15 addc smbd_audit[6203]: 2023/10/09 12:32:15|DOMPEDAGO/prenom.eleve22|addc|prenom.eleve22|10.1.
2.50|disconnect|ok|IPC$
```

On a bien un événement de connexion et de connexion à la ressource IPC$ mais immédiatement suivie de l'événement de déconnexion. Aucun contexte de leur émission (ouverture ou clôture de session).

Il est peut-être nécessaire d'envisager des scripts de logon et logoff pour tracer les événements nécessaires à la génération des statistiques souhaitées.

#3 - 05/02/2024 11:34 - Benjamin Bohard

- Statut changé de En cours à À valider

#4 - 19/02/2024 09:28 - Laurent Gourvenec

- Statut changé de À valider à Résolu

#5 - 07/03/2024 14:20 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- % réalisé changé de 0 à 100

- Restant à faire (heures) mis à 0.0