Catégorie : gestion des droits, utilisation d'une fonctionnalité Vitam

Le suivi des accès dans la solution logicielle Vitam

Pour répondre aux besoins d'enquête en cas de divulgation d'informations, la solution logicielle Vitam permet de tracer dans un log d'accès, si le contrat d'accès le spécifie :

- l'accès aux **objets techniques***, qu'il s'agisse de visualisation ou de téléchargement ;
- l'export de **DIP***, dès lors que ceux-ci contiennent des objets.

Les accès aux métadonnées des archives (**unités archivistiques*** comme **groupes d'objets techniques***) ne sont pas concernés.

PRÉSENTATION DES LOGS D'ACCÈS

Structure des logs

Information	**Nom du champ correspondant**	**Exemple de valeur**
Date et heure de l'opération d'accès au format AAAA-MM-JJTHH:MM:SS:[3 digits de millisecondes]	eventDateTime	2019-01-11T12:50:53.344
Identifiant de l'opération d'accès pour la solution logicielle Vitam	xRequestId	aeeaaaaaachfmo4dabyw6aliht3q74aaaaaq
Identifiant de l'opération d'accès pour l'application demandeuse	ApplicationId	MyApplicationId-ChangeIt
Identifiant de l'objet auquel l'application demandeuse a accédé	objectIdentifier	aeaaaaaaaahk2vrsabz26alhywthyoaaaaba
Taille en octets de l'objet auquel l'application demandeuse a accédé	Size	11
Usage de l'objet auquel l'application demandeuse a accédé	qualifier	BinaryMaster
Version de l'usage de l'objet auquel l'application demandeuse a accédé	Version	1
Identifiant du contexte utilisé pour l'accès	ContextId	CT-000001
Identifiant du contrat d'accès utilisé pour l'accès	ContractId	ContratTNR
Identifiant de l'unité archivistique dont dépend le groupe d'objets contenant l'objet auquel l'application demandeuse a accédé	archivesId	aeaqaaaaaahk2vrsabz26alhywthzbaaaaea

Nombre de logs générés

Le nombre de logs généré va dépendre du nombre d'objets concernés par l'opération :

- accès à 1 objet : 1 log ;
- export d'un DIP de sept unités archivistiques dont quatre seulement avaient un GOT contenant un objet : 4 logs ;
- export d'une unité archivistique ayant un GOT comprenant trois objets : 3 logs ;
- export d'une unité archivistique ayant un GOT comprenant trois objets, mais avec un contrat d'accès n'autorisant que l'accès à une seule catégorie d'usage : 1 log.

ACTIVATION DE LA GÉNÉRATION DES LOGS D'ACCÈS

Le **contrat d'accès*** permet de préciser si des logs d'accès doivent être générés. Par défaut, cette option n'est pas activée.
Il est utile de générer des logs d'accès lorsque l'on craint un risque de compromission sur des informations non librement communicables et que l'on veut pouvoir connaître l'application qui a eu accès à ces fichiers.

CONSULTATION DES LOGS D'ACCÈS

Les logs de l'heure en cours peuvent être consultés sur les machines hébergeant le composant **storage** sous l'arborescence « /vitam/log/storage/access-log/ ». Chaque fichier de log est nommé « <tenant>_<date>_<id opération>.log ».

Toutes les heures, les logs sont archivés et sont alors accessibles dans des `containers` nommés ``<environnement>_<tenant>_storageaccesslog``.