

Le contrat d'accès dans la solution logicielle Vitam

- Le contrat d'accès permet d'octroyer sur un **tenant*** des droits aux utilisateurs applicatifs habilités pour accéder aux unités archivistiques, qu'il s'agisse de les consulter, de modifier unitairement ou en masse leurs métadonnées descriptives et de gestion ou de télécharger ou d'exporter les unités archivistiques avec les objets techniques associés. Il octroie également des droits pour la consultation du registre des fonds.
- Chaque opération d'accès (consultation, modification de métadonnées, accès au registre des fonds) doit préciser dans sa requête le contrat utilisé.
- Diverses configurations du contrat d'accès sont possibles en fonction des restrictions que l'on souhaite apporter aux droits des utilisateurs.

PRÉSENTATION DU CONTRAT D'ACCÈS

Périmètre du contrat d'accès

Un contrat d'accès est propre au **tenant*** sur lequel il a été importé.

- Une application qui serait amenée à effectuer des accès sur plusieurs tenants devrait disposer d'un contrat pour chaque tenant.

Paramétrage des actions autorisées

- Le contrat d'accès permet de ne donner accès aux unités archivistiques qu'en lecture seule, c'est-à-dire sans possibilité de modifier les métadonnées. Il est recommandé de choisir ce paramétrage du contrat d'accès quand une application n'a besoin que de consulter les archives.
- Si le contrat autorise la modification de métadonnées, cette autorisation peut ne porter que sur les métadonnées descriptives ou sur les métadonnées descriptives et les métadonnées de gestion des unités archivistiques (**règles de gestion*** et **profil d'unité archivistique***).
- Les métadonnées de gestion sont en effet considérées comme plus sensibles, car elles conditionnent la mise en œuvre de sorts finaux (élimination, transfert) ou le statut de communicabilité des archives. La modification des métadonnées de gestion doit donc être réservée aux applications qui en ont vraiment besoin.

Paramétrage du périmètre de consultation autorisé

Restriction des services producteurs autorisés

- Un contrat d'accès permet de restreindre la consultation des archives et du registre des fonds au(x) seul(s) producteur(s) qu'il déclare.
- La déclaration des services producteurs autorisés se fait par l'identifiant de ces services dans le **référentiel des services agents***.
- Il est également possible de donner accès à tous les services producteurs.

Restriction des usages autorisés

- Un contrat d'accès permet de limiter la consultation des objets techniques (visualisation et téléchargement) en n'autorisant l'accès qu'à certains usages :
- archives physiques (PhysicalMaster),

- original numérique (BinaryMaster),
- version de diffusion (Dissemination),
- 40 • contenu textuel (TextContent),
- vignettes (Thumbnail).

Restriction de navigation dans l'arborescence

Un contrat d'accès permet de déclarer un **nœud***, dans une arborescence, à partir duquel l'accès aux archives est accordé. Seules les unités archivistiques filles de ce nœud de consultation seront
45 accessibles.

La déclaration de ce nœud se fait sur la base de l'identifiant (GUID) d'une unité archivistique déjà présente dans le système. Le nœud peut être un nœud d'**arbre de positionnement***, un nœud de **plan de classement*** ou un nœud d'unité archivistique **standard***.

Un contrat d'accès permet également de déclarer un **nœud***, dans une arborescence, à partir duquel
50 l'accès aux archives est interdit. Les unités archivistiques filles de ce nœud seront inaccessibles.

La déclaration de ce nœud se fait sur la base de l'identifiant (GUID) d'une unité archivistique déjà présente dans le système. Le nœud peut être un nœud d'**arbre de positionnement***, un nœud de **plan de classement*** ou un nœud d'unité archivistique **standard***.

Paramétrage du niveau de traçabilité attendu

55 Le contrat d'accès permet de préciser si des logs d'accès doivent être générés lors d'un accès à l'objet (fichier numérique), que ce soit par téléchargement de l'objet ou export d'un **DIP***.

Les accès aux métadonnées des unités archivistiques ne sont pas concernés (cf. fiche *Le suivi des accès dans la solution logicielle Vitam*).

Par défaut, cette option n'est pas activée.

60 **CONFIGURATION DU CONTRAT D'ACCÈS**

Constitution du contrat d'accès

Pour constituer un contrat d'accès, l'administrateur fonctionnel recense les droits à accorder en fonction des besoins des utilisateurs.

65 *Les utilisateurs ont-ils besoin d'accéder aux archives et/ou de faire des traitements sur les unités archivistiques ?*

Une application transférant des archives dans la solution logicielle Vitam n'aura pas nécessairement besoin de consulter ces archives, en ce cas il ne sera pas utile de lui attribuer un contrat d'accès.

Cas d'usage : une chaîne de numérisation verse les documents numérisés dans le SAE, mais n'y accède pas ; dans ce cas, l'application doit disposer d'un **contrat d'entrée***, mais pas
70 d'un contrat d'accès.

Si les utilisateurs n'ont besoin que d'accéder aux archives, sans faire de traitement sur les unités archivistiques, il n'est pas utile de leur donner des droits de modification.

Seuls les utilisateurs en ayant vraiment besoin doivent avoir des droits d'écriture sur les métadonnées de gestion.

75 *Si les utilisateurs ont besoin d'accéder aux archives et/ou de faire des traitements sur les unités archivistiques, pourront-ils accéder à toutes les archives ?*

Si l'on souhaite restreindre l'accès des utilisateurs applicatifs aux seules archives dont ils sont les

producteurs, il faudra autant de contrat d'accès que d'utilisateurs applicatifs, chaque contrat ne déclarant que le ou les producteurs autorisés.

- 80 Il est également possible de restreindre les utilisateurs à un périmètre plus fin en limitant les possibilités de navigation dans l'arborescence, en déclarant des **nœuds*** de consultation et des **nœuds*** inaccessibles.

Les droits octroyés dans le contrat d'accès doivent être compatibles avec ceux du **profil de sécurité***.

- 85 Une application ayant des droits d'administration de la solution logicielle Vitam, par exemple un système d'information archivistique (SIA), doit détenir un contrat d'accès lui permettant d'accéder à l'ensemble des fonds conservés dans la solution logicielle Vitam et de modifier les métadonnées descriptives et de gestion.

- 90 Pour une application devant filtrer les accès en fonction de profils utilisateurs, un contrat d'accès unique peut ne pas être suffisant pour gérer les droits des utilisateurs finaux. On pourrait vouloir limiter par exemple certains utilisateurs à une partie de l'arborescence ou à certains usages seulement.

Dans ce cas, l'application accédante peut ajouter des filtres d'accès supplémentaires afin de réduire le périmètre des archives consultables en fonction des profils utilisateurs qu'elle définit.

- 95 Il est également possible d'attribuer plusieurs contrats d'accès à l'application.

Exemple : tous les utilisateurs du SIA ne sont pas autorisés à consulter l'ensemble des usages des archives. Le SIA pourra avoir un contrat d'accès lui permettant de consulter tous les usages, mais des filtres seront installés dans le front-office pour trier les résultats et ne présenter que certains usages aux utilisateurs finaux en fonction de leur profil.

100 Gestion de l'identifiant du contrat d'accès

À l'installation de la plate-forme Vitam, l'administrateur technique peut configurer le tenant pour que les identifiants des contrats d'accès soient générés par Vitam (mode « **maître*** ») ou par le front-office (mode « **esclave*** »).

- 105 Le mode « esclave » permet à un service de conserver la main sur les identifiants des contrats d'accès pour utiliser des identifiants normés au niveau de l'institution et/ou à un niveau national ou international.

Formalisation du contrat d'accès

Un contrat d'accès prend la forme d'un fichier JSON, pouvant contenir 1 à n contrat(s) d'accès.

Un contrat d'accès donné doit **obligatoirement** comporter les informations suivantes :

- 110
- identifiant signifiant. Ce champ est obligatoire seulement s'il est généré par l'application à l'origine de sa création. Si cet identifiant est généré par la solution logicielle Vitam, il n'est pas nécessaire de le renseigner dans le fichier JSON ;

- nom du contrat.

D'autres informations, facultatives, peuvent venir compléter ces informations.

- 115 Le contrat d'accès est composé des éléments suivants :

Éléments obligatoires

<ul style="list-style-type: none"> - identifiant unique donné au contrat, sauf s'il est généré automatiquement par le système - nom du contrat - statut « Actif » ou « Inactif » ; par défaut la valeur est « Inactif » - service(s) producteur(s) associé(s) au contrat pour déterminer les périmètres de consultation. Il peut s'agir de : <ul style="list-style-type: none"> o tous les services producteurs (valeur par défaut : « false » – obligatoire), o une sélection de services producteurs (facultatif) - usage(s) au(x)quel(s) le contrat donne accès. Il peut s'agir de : <ul style="list-style-type: none"> o tous les usages (valeur par défaut : « false » – obligatoire), o une sélection d'usages (facultatif) - droit d'écriture sur les archives (valeur par défaut : « false ») - droit de modification de l'ensemble des métadonnées d'une unité archivistique ou de ses seules métadonnées descriptives (valeur par défaut : « false ») - droit d'enregistrer les accès sur les objets dans un log (valeur par défaut : « INACTIVE ») 	<p><i>Éléments facultatifs</i></p> <ul style="list-style-type: none"> - description du contrat - si le contrat est inactif, date de désactivation du contrat - sélection de services producteurs associés au contrat - sélection d'usages - identifiant du nœud ou des nœuds au(x)quel(x) et à partir des/duquel(s) on souhaite donner accès - identifiant du nœud ou des nœuds à partir de(s)quel(s) on souhaite interdire l'accès
---	---

Il est obligatoire d'indiquer dans un contrat d'accès actif si le service externe, une fois authentifié par la solution logicielle Vitam, a accès

- o à tous les services producteurs ou au moins à l'un d'entre eux,
- o à tous les usages ou à au moins l'un d'entre eux.

- 120 Si aucun de ces éléments n'a été renseigné, même si le contrat d'accès est actif, le service externe ne pourra accéder à aucun service de la solution logicielle Vitam.

Pour plus d'information sur la formalisation des contrats d'accès, consulter le document *Vitam. Modèle de données*.

Activation/désactivation du contrat d'accès

- 125 Un contrat d'accès peut être importé avec un statut inactif ou être désactivé lors d'une mise à jour du contrat.

Cette fonctionnalité est utile quand on souhaite créer un contrat d'accès et l'importer avant d'autoriser des applications à l'utiliser ou lorsqu'on souhaite désactiver temporairement ou définitivement un contrat d'accès.

- 130 Un contrat au statut inactif ne permet pas de réaliser un accès.

MODIFICATION D'UN CONTRAT D'ACCÈS

Les contrats d'accès peuvent être modifiés unitairement pour permettre d'activer ou de désactiver certaines options.

135

Les champs « Identifiant », « Date de création », « Dernière modification » et « Tenant » ne sont pas modifiables.

Il est possible de modifier un contrat d'accès utilisé dans un contexte applicatif particulier. Il est conseillé de suivre les étapes suivantes en fonction du contexte d'utilisation du contrat :

Contexte	Action
Avec un contrat d'accès	Désactivation du contexte ou du seul contrat d'accès, le temps de procéder à la modification
Avec un contrat d'accès et un contrat d'entrée	Désactivation du seul contrat d'accès, le temps de procéder à la modification, de manière à ne pas interrompre les transferts du contrat d'entrées associé au contexte applicatif.
Avec plusieurs contrats d'accès	Désactivation d'un seul contrat d'accès, le temps de procéder à la modification, de manière à ne pas interrompre l'utilisation des autres contrats d'accès associés au contexte applicatif.
Avec un ou plusieurs contrats d'accès	<ul style="list-style-type: none">• Création d'un nouveau contrat d'accès contenant les modifications à apporter.• Association de ce contrat d'accès au contexte applicatif.• Activation de ce contrat d'accès.• Désactivation de l'ancien contrat d'accès.• Suppression du lien entre l'ancien contrat d'accès et le contexte applicatif.

Pour aller plus loin, consulter le document *Vitam. Gestion des habilitations*.