Catégorie : gestion des droits

La gestion des droits et permissions des utilisateurs applicatifs dans la solution logicielle Vitam

La solution logicielle Vitam, comme toute application, dispose d'utilisateurs qui ont des droits plus ou moins avancés. Ses utilisateurs ne sont cependant pas des individus, mais d'autres applications informatiques qui vont utiliser ses services, comme un service d'archives qui n'aurait pour utilisateurs que des administrations, des entreprises ou des universités, sans savoir plus précisément quels sont les droits des différents personnes relevant de ces entités.
L'accès à la solution logicielle Vitam et les droits accordés sont paramétrables.

ARTICULATION DES DIFFÉRENTES HABILITATIONS

La gestion des droits et permission d'un utilisateur applicatif dans la solution logicielle Vitam s'opère de la manière suivante :

- il faut d'abord définir la liste des services qu'il pourra utiliser en lui octroyant un profil de sécurité ;
- il faut ensuite enregistrer l'utilisateur en lui créant un contexte applicatif ;
- il faut ensuite lui attribuer un moyen d'authentification et de connexion (l'équivalent de l'identifiant et du mot de passe pour un utilisateur individuel) en lui attribuant un certificat ;
- il faut enfin lui définir un périmètre d'intervention en termes de contenus en définissant les tenants dans lesquels il va pouvoir effectuer ses opérations.

Les services utilisés et le périmètre d'intervention autorisé peuvent être affinés, pour les opérations d'entrées, au moyen de **contrats d'entrée*** et, pour les autres opérations (recherche, consultations d'archives, modifications, élimination, audit, préservation), au moyen de **contrats d'accès***.

Liste des services utilisables par les utilisateurs applicatifs

Pour un **contexte applicatif*** donné, le **profil de sécurité*** formalise les privilèges, c'est-à-dire les droits octroyés à une application externe par la solution logicielle Vitam, et par conséquent les points d'accès par lesquels cette application, une fois authentifiée, pourra transmettre des requêtes à la solution logicielle Vitam.
Cela revient à définir pour un utilisateur applicatif les fonctionnalités de la solution logicielle Vitam qu'il pourra utiliser.

Exemples de services : récupérer le bordereau de transfert pour une opération d'entrée donnée, envoyer un SIP à Vitam afin qu'il en réalise l'entrée, récupérer le journal de cycle de vie d'une unité archivistique, télécharger un objet, importer un référentiel des scénarios de préservation…
Pour connaître les autres services, consulter l'annexe 3 du document *Vitam. Gestion des habilitations*.

Le profil de sécurité applicatif détermine les droits suivants :

- soit un accès à tous les services proposés par la solution logicielle Vitam ;
- soit une liste de services définis auxquels le service de sécurité donne accès ; pour chaque service, cette liste précise le type de service concerné et les droits associés (lecture, écriture, suppression).

Catégorie : gestion des droits

La création d'un profil de sécurité et l'attribution des privilèges qui lui sont associés relèvent d'une opération d'administration technique.

Un service externe souhaitant utiliser les services de la solution logicielle Vitam doit disposer d'un **profil de sécurité***. Ce profil doit être associé à un **contexte*** dès la création de ce dernier, sans quoi l'application cherchant à s'authentifier à la solution logicielle Vitam ne pourra accéder à aucun de ses services.

Enregistrement des utilisateurs applicatifs

Le **contexte applicatif*** est une description de l'utilisateur applicatif qui rassemble l'ensemble des informations sur celui-ci. Il formalise les interactions entre un service externe et la solution logicielle Vitam. Il permet notamment d'authentifier une application et de lui affecter des droits.
Pour qu'une application externe puisse utiliser les services fournis par la solution logicielle Vitam, son contexte applicatif doit être associé à :

- 1 ou plusieurs **tenants***,
- 1 ou plusieurs **contrats d'entrée*** si l'application doit réaliser des entrées,
- 1 ou plusieurs **contrats d'accès*** si l'application doit réaliser des accès,
- 1 **profil de sécurité***.

Le contrôle sur les tenants et les contrats peut être désactivé : le contexte applicatif permet alors à l'application externe d'accéder à l'ensemble des services mis à disposition par la solution logicielle Vitam.
Le contexte doit ensuite être associé à un **certificat*** pour que l'application puisse se connecter.

Outils d'authentification et de connexion des utilisateurs applicatifs

Dès qu'on souhaite connecter une application à la solution logicielle Vitam, il faut avant toute chose, l'authentifier au moyen d'un **certificat applicatif*** qui détermine un contexte applicatif, avant de lui associer un **profil de sécurité*** et des **contrats***, préexistants ou créés à cette occasion.

Un service externe souhaitant utiliser les services de la solution logicielle Vitam doit avoir déclaré son **certificat applicatif*** dans la solution logicielle Vitam. Ce certificat doit être associé à un **contexte*** dès la création de celui-ci, sans quoi l'application cherchant à s'authentifier à la solution logicielle Vitam ne pourra accéder à aucun de ses services.

Certificat applicatif et certificat personnel

Le **certificat applicatif*** permet d'identifier et d'authentifier une application souhaitant accéder aux services de la solution logicielle Vitam.
Il doit être associé obligatoirement à au moins un **contexte applicatif***.
Le **certificat personnel*** correspond à un certificat propre à une personne physique utilisatrice en particulier de l'application souhaitant accéder aux services de la solution logicielle Vitam. Le certificat personnel ne se substitue pas au certificat applicatif qui authentifie une application, et il sert uniquement à identifier et non à authentifier une personne qui se connecte derrière une application.
Son utilisation répond à un besoin de sécurité supplémentaire, associé aux fonctions d'administration avancée ou considérées comme sensibles.

La création d'un **certificat personnel*** et l'attribution des privilèges qui lui sont associés relèvent

d'une opération d'administration technique.
Il est recommandé de n'utiliser ce type de certificat que pour des utilisateurs en nombre restreint, par exemple pour les administrateurs de la solution logicielle Vitam ayant vocation à accéder à l'ensemble des services mis à disposition.

Périmètre d'action des utilisateurs applicatifs
Le contexte applicatif doit être associé à un ou plusieurs **tenants*** auxquels l'application aura le droit d'accéder.

Pour assurer une étanchéité entre les tenants*, il est préconisé d'associer un seul tenant par **contexte***. De cette manière, le mécanisme d'authentification d'une application externe à un tenant ne permet de verser et d'accéder qu'à ce seul tenant. Le mécanisme de multi-tenant pour le contexte applicatif est mis en place pour le cas d'un système d'information archivistique (SIA) qui devrait pouvoir accéder à plusieurs tenants.

Affinage des droits et périmètres d'intervention des utilisateurs applicatifs
Si l'utilisateur applicatif doit réaliser des entrées, son contexte applicatif doit également être associé à un ou plusieurs **contrats d'entrée***.
De même, pour réaliser des accès, son contexte applicatif doit être associé à un ou plusieurs **contrats d'accès***.
Les contrats d'entrée et d'accès permettent de paramétrer finement les droits des utilisateurs applicatifs : par exemple, une application externe qui a le droit de télécharger un objet pourra dans son contrat d'accès être limitée aux archives de certains producteurs et à certains **usages*** des objets.
Pour en savoir plus, consulter les fiches *Le contrat d'entrée dans la solution logicielle Vitam* et *Le contrat d'accès dans la solution logicielle Vitam*.

PRÉSENTATION DES RÉFÉRENTIELS DES HABILITATIONS

Périmètre des habilitations
La solution logicielle Vitam intègre un référentiel pour chaque type d'habilitation, administrable par l'administrateur fonctionnel ou technique.
Les référentiels des **certificats applicatifs***, des **certificats personnels***, des **contextes applicatifs*** et des **profils de sécurité*** sont multi-**tenants***. Ils sont administrables et journalisés depuis le **tenant*** d'administration.
Les référentiels des **contrats d'entrée*** et des **contrats d'accès*** sont propres à chaque **tenant*** de la solution logicielle Vitam.

Contrôles réalisés par la solution logicielle Vitam au moyen des habilitations
Un service externe doit toujours s'authentifier à la solution logicielle Vitam au moyen de son **certificat applicatif*** qui détermine un **contexte applicatif***.
Lorsqu'il adresse une requête à la solution logicielle Vitam celle-ci vérifie que :

- elle connaît cet utilisateur (le contexte applicatif déclaré existe bien dans le référentiel des contextes applicatifs et est actif) ;

- l'utilisateur utilise un certificat valide (non expiré) ;
- l'utilisateur dispose des droits lui permettant d'adresser cette requête (par exemple, il a accès au service permettant de télécharger un objet) ;
- l'utilisateur dispose des droits lui permettant d'adresser cette requête pour le tenant sur auquel il veut accéder ;
- l'utilisateur dispose d'un contrat cohérent avec sa requête (par exemple, un contrat d'accès qui l'autorise à accéder aux archives du producteur souhaité et à l'usage voulu).

L'authentification est une étape préalable à toute opération d'entrée ou d'accès.
Si un élément fait défaut, le service externe ne pourra pas accéder aux services de la solution logicielle Vitam.

CONFIGURATION DES HABILITATIONS

La configuration des habilitations est une opération d'administration technique.
Toutefois, l'administrateur fonctionnel intervient dans la définition des droits à accorder à chaque application en fonction de ses besoins d'interaction avec la plate-forme d'archivage.
Pour en savoir plus sur la formalisation des habilitations, consulter le document *Vitam. Modèle des données.*

Gestion d'une nouvelle application

Pour connecter une nouvelle application à la solution logicielle Vitam, il est recommandé de suivre les étapes suivantes :

Qui ?	Quoi ?	Via l'IHM démo Vitam ?	Commentaires
Administrateur fonctionnel/ technique	- Définition des privilèges à octroyer à une application et à associer ultérieurement à un profil de sécurité, - Définition des profils utilisateurs à mettre en place dans le Front Office et définition de leur mode de connexion (LDAP, certificat personnel, authentification gérée par le Front Office).	Non	
Administrateur technique	Création d'un profil de sécurité	Non	Préalable à la création d'un contexte
Administrateur fonctionnel/ technique	Création d'un contexte : - sans permission - avec un profil de sécurité - statut « Inactif »	Oui	Préalable à la création d'un certificat
Administrateur	Création d'un certificat applicatif	Non	Déclare le contexte

technique			précédemment créé
Administrateur technique	Création de certificat(s) personnel(s)	Non	Étape facultative.
Administrateur fonctionnel	Création et paramétrages des contrats d'entrée et/ou d'accès	Oui	
Administrateur fonctionnel	Association des contrats d'entrée et/ou d'accès au contexte applicatif	Oui	
Administrateur fonctionnel	Activation du contexte	Oui	À la date souhaitée pour commencer les interactions entre l'application versante et/ou accédante et la solution logicielle Vitam
Administrateur technique / fonctionnel	Test avant utilisation courante	Oui	

Gestion des identifiants des habilitations

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

Le mode « esclave » est intéressant si les habilitations sont générées dans le front office qui leur donne un identifiant que l'on souhaite pouvoir suivre.

Activation et désactivation des éléments des habilitations

La solution logicielle Vitam permet de rendre actif ou de désactiver un **contexte applicatif***, un **contrat d'entrée*** ou un **contrat d'accès***.

En fonction du statut du contexte applicatif et de celui du contrat d'entrée associé, un transfert de **SIP*** sera autorisé ou non :

	Contexte applicatif	**Contrat d'entrée**	**Résultat**
CAS 1	ACTIF	ACTIF	Transfert de SIP dans le système autorisé.
CAS 2	ACTIF	INACTIF	Transfert de SIP dans le système non autorisé.
CAS 3	INACTIF	ACTIF	Transfert de SIP dans le système non autorisé.
CAS 4	INACTIF	INACTIF	Transfert de SIP dans le système non autorisé.

En fonction du statut du contexte applicatif et de celui du contrat d'accès associé, un accès au système sera autorisé ou non :

	Contexte applicatif	Contrat d'accès	Résultat
CAS 1	ACTIF	ACTIF	Accès au système autorisé.
CAS 2	ACTIF	INACTIF	Accès au système non autorisé.
CAS 3	INACTIF	ACTIF	Accès au système non autorisé.
CAS 4	INACTIF	INACTIF	Accès au système non autorisé.

IMPORT, MODIFICATION ET SUPPRESSION DES HABILITATIONS

Import

Dans la solution logicielle Vitam, il est possible d'importer :

- 1 à n contexte(s) applicatif(s),
- 1 à n contrat(s) d'entrée,
- 1 à n contrat(s) d'accès.

Il s'agit d'une opération d'administration, tracée dans le journal des opérations de la solution logicielle Vitam.

Pour chaque catégorie d'habilitation à importer dans la solution logicielle Vitam (contexte applicatif, contrat d'entrée, contrat d'accès), il est possible d'importer un référentiel complet, comprenant plusieurs items, en une seule fois. La solution logicielle Vitam ne comptabilisera qu'une seule opération, et ne prend pas en compte dans le journal des opérations la création unitaire des différents items compris dans le référentiel importé.
Afin d'optimiser la traçabilité de la création des différents référentiels d'habilitations, il est donc recommandé de créer ces derniers un par un.

L'ajout d'un certificat applicatif, la déclaration d'un certificat personnel ou encore la création d'un profil de sécurité relèvent d'opérations d'administration technique, tracées dans les logs.
Il est possible de générer ainsi :

- 1 à n certificat(s) applicatif(s),
- 0 à n certificat(s) personnel(s),
- 1 à n profil(s) de sécurité.

Modification

Cette action provoque la création d'une nouvelle version du **contexte***, **contrat d'entrée***, **contrat d'accès*** ou **profil de sécurité*** modifié.
Elle fait l'objet d'une journalisation dans le journal des opérations.

Suppression

La solution logicielle permet de supprimer unitairement certaines habilitations : **certificat applicatif***, **certificat personnel***, **profil de sécurité*** et **contexte applicatif***.
Cette suppression peut avoir un impact sur les interactions entre l'application versante et/ou accédante et la solution logicielle Vitam. Cette opération relève d'une opération d'administration technique.
Elle fait l'objet d'une journalisation dans le journal des opérations.

Pour en savoir plus, consulter le document *Vitam. Gestion des habilitations*.