Systancia

the human face of the workplace

Cyberelements IDENTITY 7.0
Conduite des changements de configuration

#Cybersecurity #Virtualization #AI

www.systancia.com

Ref. :	FR_TECH_Systancia_Identity_Conduite des changements de configuration_7.0_rev.1.0.docx
Version :	1.00
Produit :	Systancia Identity
Date :	2024-10-24

Objet :

Ce document décrit les changements de configuration à réaliser lors d'une montée de version d'une version Systancia Identity 6.2 vers Cyberelements Identity 7.0

TABLE DES MATIERES

1. Installation

Vous pouvez télécharger le produit Systancia Identity V7.0 sur le SEP Systancia ou en cliquant sur le lien.

La documentation en ligne pourra vous accompagner pour vos projets d'installations.

Ce produit peut être installé directement dans le cadre d'une primo installation ou à partir d'une **version Identity 6.2** fonctionnelle dans le cadre d'une montée de version.

1.1 Avertissement

En cas de mise à jour de la solution avec Cyberelements Identity V7.0 (à partir d'une version 6.2 avec ou sans SP), les fonctions et procédures stockées hors produit (non développées par Systancia) peuvent générer des erreurs lors de l'installation de la solution. Par prévention, nous recommandons de sauvegarder les procédures et fonctions hors produit, puis de les supprimer avant d'installer Cyberelements Identity 7.0. Les procédures et fonctions hors produit nécessaires à l'utilisation de la solution devront ensuite être réintégrées avec les sauvegardes réalisées au préalable.

Si cette procédure n'a pas été appliquée et qu'une erreur a été rencontrée pendant de l'installation, il est nécessaire de refaire l'installation complètement (repartir du backup de la BDD avant mise à jour).

A partir de la version Cyberelements Identity 7.0, l'usage de procédures et fonctions spécifiques est déprécié par Systancia. Systancia ne peut être tenu responsable d'un dysfonctionnement de la solution s'il est lié à des procédures ou des fonctions hors produit.

2. Détails des configurations à opérer / faire évoluer

2.1 Nouvelle application web

Consulter la documentation d'installation pour connaître la procédure d'installation.

2.2 Architecture

En version 7.0, il est nécessaire d'exécuter les différents services avec des comptes de services distincts. Un minimum de 3 comptes de service est donc désormais nécessaire. Pour des raisons de sécurité, chaque service et applications Web sont installés avec le protocole HTTPS par défaut.

Consulter la documentation de prérequis techniques pour connaître les architectures supportées et les prérequis obligatoires avant d'installer la solution Cyberlements Identity 7.0.

2.3 Evolutions des applications Web Identity (SID)

2.3.1 Connexion à l'application Web nouvelle génération 7.0

Concernant le mode d'authentification, on a des différences entre les 3 consoles web :

- La nouvelle console Web, génération 7.0, est une application fédérée. Elle nécessite donc obligatoirement une authentification via un IDP. Systancia fournit son IDP, Cyberelements Federation, si nécessaire. L'IDP Cyberelements Federation ne gère que le protocole OIDC et les modes d'authentification possible sont :
    - Authentification Windows
    - Fournisseur d'identités : Cyberelements Identity
    - Fournisseur d'identités : Annuaire
- Les 2 anciennes consoles Web, génération 6.2, gardent les modes d'authentification présents historiquement :
    - AD
    - Authentification Windows
    - Fédération (SAMLV2)

Donc, selon les modes d'authentification choisi, il se peut qu'une réauthentification soit nécessaire lors d'une bascule d'une console vers une autre.

Afin d'éviter cette double authentification, les modes de connexion à privilégier sont les suivants quand cela est possible :

- Authentification Windows : dans ce cas, aucune saisie de login / mot de passe n'est nécessaire.
- Authentification fédérée : possible si le client possède une IDP gérant à la fois le protocole OIDC et SAMLV2.

En cas de primo installation, lors de l'installation de Cyberlements Identity 7.0, pour accéder à la nouvelle console Web, si le mode d'authentification choisit est Cyberelements Federation,

il est nécessaire d'utiliser le login admin. Un mot de passe par défaut est créé, il devra être obligatoirement changé à la première connexion.

En cas de montée de version vers Cyberlements Identity 7.0, pour accéder à la nouvelle console Web, si le mode d'authentification choisit est Cyberelements Federation, tous les comptes Identity existants auront le mot de passe de réinitialisé avec le mot de passe par défaut.

Vous pouvez vous procurer le mot de passe par défaut au près du support Systancia.

2.3.2 Ajout des rôles (profils métiers) / multicomptes

Avant de procéder à une montée de version de Systancia Identity 6.2 vers Cyberelements Identity 7.0, procéder aux vérifications suivantes :

- Présence d'un seul type de compte par Référentiel. En cas de présence d'un référentiel avec plusieurs types de comptes, essayez de revenir à un seul type de compte sur la version actuelle
    - Piste à envisagée : sauvegarder les logins des comptes dans un attributs de personnes, supprimer tous les comptes liés aux types de comptes secondaires
- Pour réaliser des nouveaux connecteurs de provisioning nous préconisons d'utiliser le nouveau type de connecteur ACCOUNT, qu'il y ait une gestion multicompte ou non.
    - Créer les attributs de comptes et les lier aux types de comptes du référentiel à provisionner.
    - Utiliser l'export de type ACCOUNT pour exporter les comptes Identity et les attributs. Cet export, exporte également les rôles et habilitations liés.

  Note : les connecteurs de type USER+ACCESS est déprécié à partir de la version 7.0. Pensez à basculer tous vos anciens connecteurs dès que cela est possible.

Les modules de workflow et de campagne de certification ne sont pas compatibles avec le multicompte dans la version 7.0. Ils le seront dans la version suivante, lors de leur intégration dans la nouvelle application. Pour assurer l'attribution de droits via des demandes workflows ou la création de campagne de certification, il sera nécessaire de spécifier le rôle par défaut sur chaque référentiel applicatif. Ainsi les habilitations seront liées aux identités et sur le rôle par défaut.

2.3.3 Bibliothèque de connecteurs

Suite à l'intégration de la bibliothèque de connecteurs dans la nouvelle application Web, la configuration des référentiels du moteur de provisioning a été intégrée dans la configuration des référentiels côté Identity.

Dans le cadre d'une montée de version, hormis le référentiel Identity qui est automatiquement créé, il n'est pas possible de reprendre de manière automatique les référentiels SIP et de faire la liaison avec les référentiels côté Identity. Ainsi, il est obligatoire de recréer manuellement tous les référentiels en cas de montée de version, que ce soit des référentiels source (donc aucune gestion de modèle de droits) ou des référentiels cible.

Dans un souci de sécurité, le mot de passe des comptes utilisés pour les connecteurs ne peut être déchiffré par la console Web. Ainsi, pour toute modification à réaliser sur la configuration SIP d'un référentiel, la saisie du mot de passe du compte associé sera obligatoire.

Le code du référentiel Identity évolue pour être unique : Ref-Identity. Il doit être modifié dans les différents connecteurs (exports, sync ou import) si jamais c'était un code différent.

Consulter le chapitre « Configuration d'un connecteur automatique (via SIP) » de la documentation produit pour connaître la procédure pour créer les référentiels.

2.3.4 Nouvelle interface pour gérer les jobs et séquences de provisioning

Afin de mettre à disposition une liste de jobs de provisioning à lancer manuellement, il est nécessaire de créer les jobs et séquences dans la nouvelle application Web.

Consulter le chapitre « Gestion des jobs et séquences de provisioning » de la documentation produit pour plus de détails.

Afin d'assurer un suivi des jobs de provisioning dans la nouvelle application Web, il est obligatoire d'exécuter les jobs via les Webservices SIP. Consulter le chapitre « Exécution des séquences de provisioning via les webservices SIP » de la documentation produit pour plus de détails.

Néanmoins, il reste possible d'exécuter des séquences de provisioning via HppRunCli.exe.

2.3.5 Tableau de bord

Le tableau de bord sert à mettre en avant des indicateurs.

La liste des indicateurs visibles est paramétrable dans les rôles Identity. Le choix des indicateurs se fait à partir d'une liste prédéfinie. Si vous souhaitez des indicateurs complémentaires, il faut réaliser une demande auprès de Systancia.

Consulter le chapitre « Tableau de bord » de la documentation produit pour plus de détails.

2.3.6 Nouveau module de SoD

Dans le cadre d'une montée de version, toutes les règles de SoD sont reprises automatiquement dans le nouveau format. Un contrôle des règles est néanmoins recommandé pour assurer la conformité des données après mise à jour.

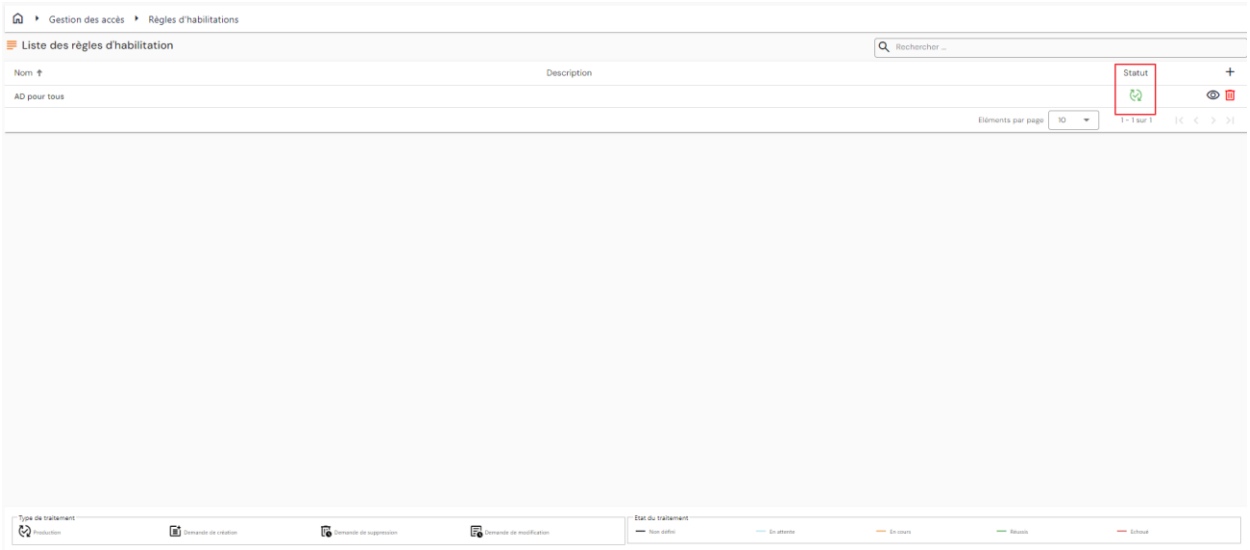
Consulter le chapitre « Gestion des règles de séparation de droits (SoD)» de la documentation produit pour plus de détails sur cette fonctionnalité.

2.3.7 Accès au module Hangfire

L'accès au module Hangfire est soumis aux permissions Identity. Si l'accès est donné, alors toutes les actions dans ce module sont accessibles. Ce module étant un module externe, il ne peut pas y avoir de gestion des permissions plus fines.

Les tâches liées aux traitements réalisés nativement en asynchrone sur les calculs de règles d'habilitations ou de SoD sont identifiées par des liens dans les interfaces des différents menus.

Exemple :



L'icône indique à la fois le statut de la règle mais on peut cliquer dessus pour voir la tâche Hangfire concernée.

Consulter le chapitre « Module Hangfire » de la documentation produit pour plus de détails sur cette fonctionnalité.

2.3.8 Evolutions sur les attributs

2.3.8.1 Conformité entre les objets

En version 7.0, les codes des attributs doivent être uniques tout objet confondu.

En mode montée de version, si des doublons existent, les attributs en double seront préfixés automatiquement. Ceci peut avoir pour conséquences des modifications de connecteurs à réaliser notamment sur l'alimentation amont des structures et des dotations.

2.3.8.2 Gestion des dotations

Dans le cadre d'une montée de version, toutes les données sur les ressources sont reprises et transformées dans le format de destination de manière automatique.

Néanmoins, il est nécessaire de modifier les connecteurs d'alimentation amont qui créent les liens entre une identité et des dotations ou entre des structures et des dotations. En effet, l'attribut « HPPUsers » n'existe plus dans SIP pour réaliser ce lien. Les ressources étant gérés avec les attributs, il convient d'utiliser des opérations mapping classique pour alimenter les attributs de ressources dans les connecteurs d'alimentation amont pour les personnes et structures. C'est le code de la ressource qui doit être renseigné dans les connecteurs.

Cette évolution invalide la fonctionnalité de pouvoir réaliser des demandes de ressources via les workflows telle que c'était implémenté jusqu'en version 6.2. Consulter le menu « Réaliser une demande de dotation (ressource) » dans la documentation produit pour trouver la meilleure méthode à implémenter selon votre cas d'usage.

2.3.8.3 Attributs sur les comptes

Pour les formules des attributs calculés, le mot-clé §ATTRIBUT§ peut être utilisé. Il récupère différentes informations sur les attributs du compte en cours d'évaluation.

Pour récupérer des informations liées aux identités liées au comptes, il faut utiliser les nouveaux mots-clés §OWNER§, §SECONDARY§ ou §IDENTITIES§.

Consulter le chapitre « Configurer une formule de calcul d'un attribut » de la documentation produit pour plus de détails sur cette fonctionnalité.

Note importante : en version 7.0, les dépendances entre attributs calculés sont calculés par type d'objet uniquement. Si des attributs de comptes dépendent d'attributs de personnes, les valeurs d'attributs seront calculées à la création du compte mais une mise à jour d'un attribut de personne ne recalculera pas un attribut de compte de manière automatique. Ces recalculs sont à prévoir manuellement pour le moment. Le produit évoluera pour gérer ces calculs de manière automatique.

2.3.9 Rôles Identity (Profils d'administration)

Pour les accès aux anciennes consoles Web, la reprise des permissions est réalisée à l'identique. Cependant, pour les accès à la nouvelle application Web, celle-ci s'étant enrichie en cumulant la partie exploitation et configuration, les permissions dans Identity ne sont pas exactement les mêmes qu'en version 6.2 même pour les fonctionnalités déjà présentes.

En mode montée de version depuis une 6.2 vers une 7.0, les profils d'administrations existants seront remplacés automatiquement par des rôles avec les droits correspondants mais il convient donc de reprendre chaque rôle Identity pour vérifier que les permissions par défaut sont correctes et qu'il n'en manque pas.

Concernant le rôle « Utilisateur Standard », il sera repris en mode montée de version mais pas créé en mode primo installation.

En mode montée de version, Les liens existants entre les identités et le rôle Utilisateur Standard seront repris mais à partir de la version 7.0, ce rôle ne sera plus automatiquement lié aux nouvelles identités.

Si vous souhaitez conserver ou mettre en place cette fonctionnalité, il faudra créer une règle d'habilitations pour affecter ce rôle à toutes les identités.

2.3.10 Les groupes de droits remplacés par les rôles

En mode montée de version d'une 6.2 vers une 7.0, les groupes de droits sont automatiquement transformés en rôles :

- Autant de rôle seront créés qu'il y a de groupes de droits existants
- Le nom du rôle portera le nom du groupe de droits
- Les référentiels et le type de compte associé liés au rôle seront déterminés via les droits composants le groupe de droits,
    - Note : si plusieurs types de compte sont définis pour un référentiel, le premier sera utilisé par défaut dans la reprise de données, il faudra contrôler manuellement les données.

Avertissement : si les groupes de droits contenaient des habilitations sur le référentiel Identity, ces habilitations ne seront pas importées dans le rôle créé pour remplacer le groupe de droits. En effet, la version 7.0 ne permet pas de créer des liens entre plusieurs rôles donc il n'est pas possible de gérer des groupes de rôles (cf. paragraphe ci-dessus).

2.3.11 Evolution du modèle de base de données

La montée de version d'une 6.2 vers une 7.0 gère automatiquement les évolutions de la base de données et de la reprise de données.

Néanmoins, certaines données ne peuvent être complètement reprises ou nécessite un contrôle plus approfondit :

- Les formules d'attributs sur les attributs de structure et dotation sont à reprendre à la main.
- Les attributs calculés ne doivent pas avoir de valeur par défaut renseignée. Cela rend la formule dysfonctionnelle. Ces modifications sont à faire manuellement après la montée de version.
- Les habilitations Identity contenues dans un groupe de droit seront exclues des rôles (cf. paragraphe ci-dessus). En effet, les habilitations Identity sont désormais transformées en rôle et il n'est pas possible de lier des rôles entre eux.

De manière générale, après une montée de version, nous conseillons de bien vérifier que les données sont conformes après la mise à jour.

2.3.12 Evolutions sur les mots-clés

2.3.12.1 Gestion du type de personnes

Pour les formules dans les attributs calculés, il convient d'utiliser la syntaxe §personne_type_id.code§ pour récupérer le code du type de personne d'une identité. En montée de version, §personneTypeEnum.code§ a été automatiquement remplacé. Cependant, toutes les formules utilisant encore la fonction pour récupérer le type de personne ne peux pas être reprise de manière automatique. Cette fonction n'existe plus dans 7.0, donc il est nécessaire de modifier les formules qui les utilisent.

2.3.12.2 Mot-clé MASTER

§MASTER§ est donc remplacé par §ATTRIBUT§parent_id.[code_attribut]§

Pour les montées de version le remplacement sera automatiquement réalisé.

Attention : contrairement au mot-clé MASTER, si une identité n'a aucune identité parente, alors §ATTRIBUT§parent_id§ est vide. Il peut donc être nécessaire de modifier certaines de vos formules malgré la mise à jour automatique lors de la montée de version.

2.3.12.3 Récupération de l'ID d'un objet avec mot-clé ATTRIBUT n'est plus fonctionnel

En mode montée de version, aucune reprise automatique n'est possible pour remplacer l'usage des ID dans les formules d'attributs calculés. Tous ces changements sont à réaliser manuellement.

Si des formules de calcul appellent des fonctions spécifiques en utilisant l'ID, il est également nécessaire de faire évoluer les fonctions pour gérer avec les codes et uid.

Pour les workflows, pour récupérer les identités dans les manager de workflows ou acteur d'actions ou tâches, il faut utiliser par exemple cette requête – requête qui récupère toutes les identités ayant pour rôle (profil d'administration) ADMIN :

§PERSONNE§ATTRIBUT§uid§ IN (select distinct PERSONNE.personne_uid from ADMIN_LIEN_PERSONNE_PROFIL, PERSONNE where admin_profil_id = 1 AND PERSONNE.personne_id = ADMIN_LIEN_PERSONNE_PROFIL.personne_id)

2.3.12.4 Génération d'un mot de passe aléatoire

Un nouveau mot-clé a été créé pour générer un mot de passe aléatoire. Afin de respecter la fonctionnalité existante, la syntaxe du mot-clé §PASSWORD§ est la suivante :

§PASSWORD§[booléen_chiffre]§[booléen_minuscule]§[booléen_majuscule]§[booléen_caracc tères_spreciaux]§[Liste_caractères_spéciaux]§[nb_caractères]§

La liste des caractères spéciaux autorisés évolue en version 7.0. Elle ne contient que les caractères suivants :

!#$%&()*+,./:;<>?@[]^_|~

Les fonctions fctGeneratePasswordEx et fctGeneratePassword ne sont plus existantes en version 7.0.

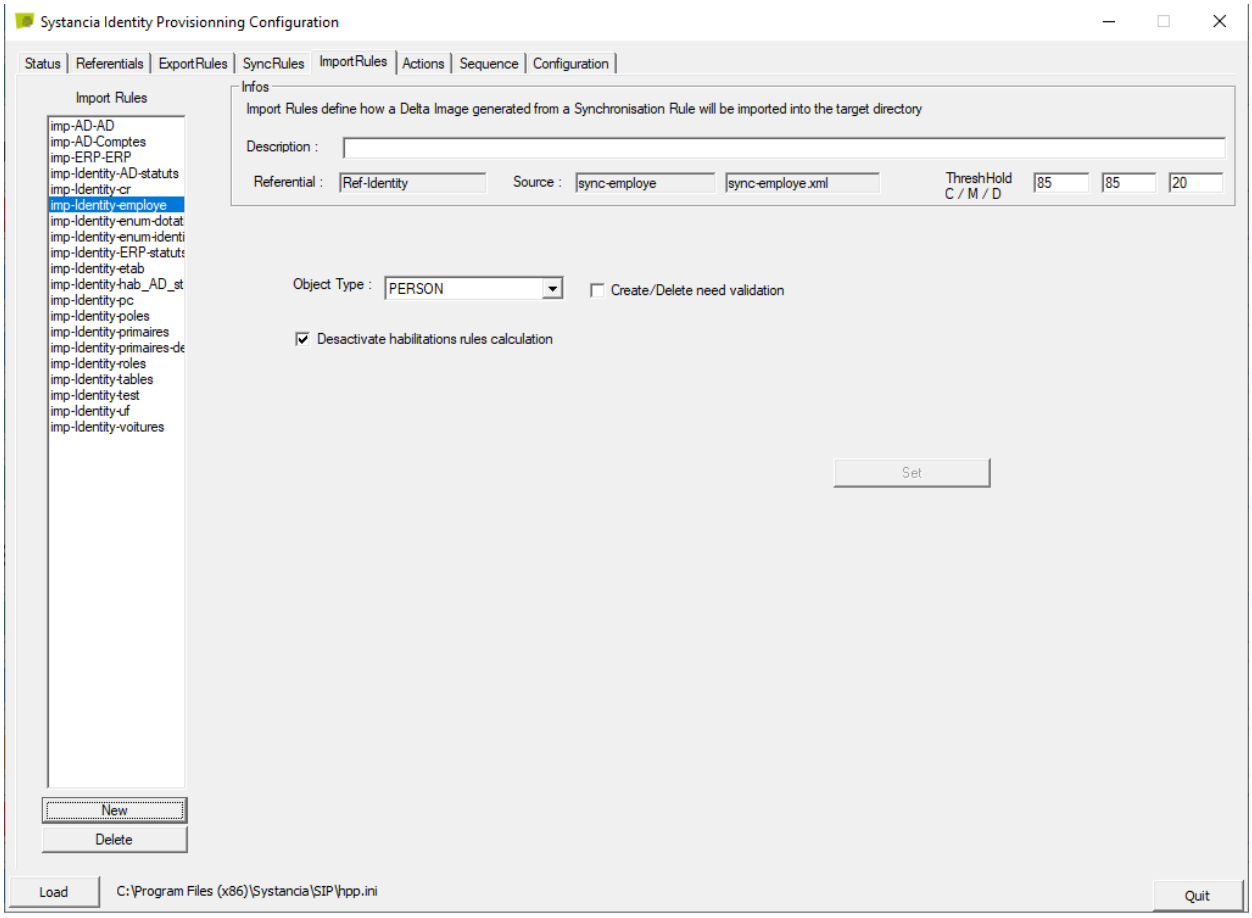
En montée de version, la reprise des formules de mot de passe utilisant les fonctions fctGeneratePasswordEx et fctGeneratePassword doivent être reprises manuellement.

2.3.13 Changements fonctionnels dans la solution

2.3.13.1 Evolutions dans les règles d'habilitations

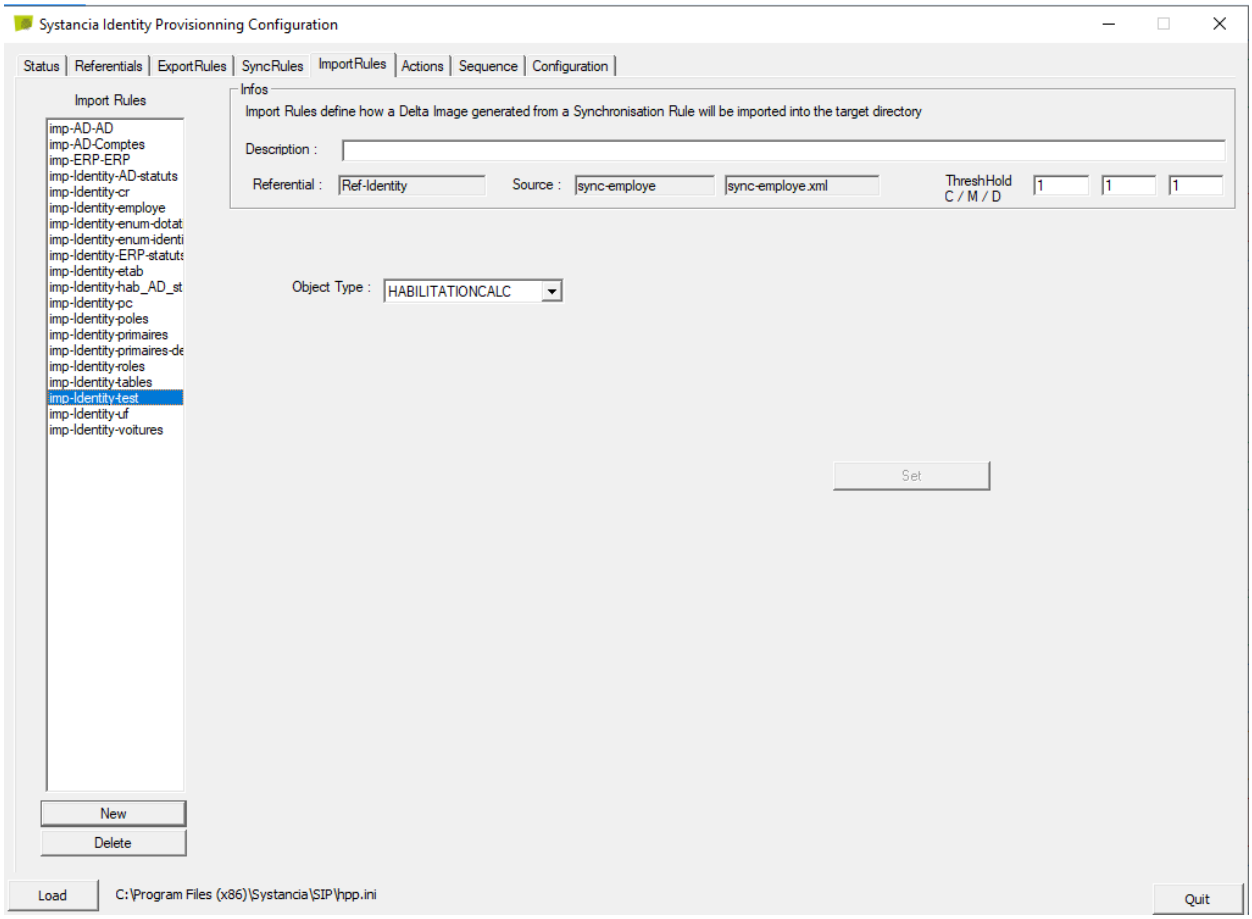
Le booléen COMPUTED_CALC, qui permet d'activer ou de désactiver le calcul des règles d'habilitations et de SoD à la volée, est supprimé en version 7.0.

La fonctionnalité a été intégrée dans SIP via des options dans les imports. En effet, l'option 'Desactivate habilitations rules calculation' a été ajoutée dans les imports du référentiel Identity et de type PERSON, STRUCTURE, DOTATION.



Afin de créer / modifier ces objets sans recalculer de manière unitaire les règles d'habilitations, il est nécessaire de la cocher.

Un nouveau type d'import a été créé pour lancer le calcul des règles via SIP. Il est nécessaire de l'appeler dans une séquence à la fin de l'alimentation amont si vous avez coché la case ci-dessus dans les séquences d'alimentation amont.



Pour les imports réalisés via les webservices, une option est à passer pour les réaliser sans effectuer les recalculs. Consulter la documentation swagger de l'API : https://[URL_Serveur_SID]:44345/swagger/

2.3.13.2 Réconciliation des identités

Consulter le chapitre « Gérer les réconciliations d'identités » de la documentation produit pour plus de détails sur cette fonctionnalité.

2.3.13.3 Evolution de la page de délégation

Consulter le chapitre « Déléguer des habilitations » de la documentation produit pour plus de détails sur cette fonctionnalité.

2.3.13.4 Gestion des états des identités

Un nouveau mot-clé a été créé pour affecter un code état :

§PERSON_STATE§[code_etat]§

Exemple :

Avec cette liste de codes états :

Nous pouvons construire cette formule :

```
CASE WHEN '§ATTRIBUT§personne_active§' = '0'
        THEN §PERSON_STATE§0§
        ELSE CASE WHEN ('§ATTRIBUT§date_debut§' <>'' AND §ATTRIBUT§date_debut§ >GETDATE())
                                OR ('§ATTRIBUT§date_fin§' <> '' AND §ATTRIBUT§date_fin§ < GETDATE())
                THEN §PERSON_STATE§10§
                ELSE §PERSON_STATE§1111§
        END
END
```

Dans le cas d'une monté de version, seuls les états utilisés sont repris dans la base de données. Pour un souci de rétrocompatibilité des formules existantes de l'attribut personne_état, les IDs des codes états repris sont égaux à leur code.

Cependant, tout ajout de code état dans la liste engendre une modification de formule pour affecter le code état en utilisant le mot-clé ci-dessus.

2.3.13.5 Gestion des arbres organisationnels

Fonctionnellement, il n'y a aucun changement dans la gestion des arbres organisationnels. Mais techniquement à partir de la version 7.0, il n'existe plus d'objet de type arbre organisationnel mais uniquement des objets de type structure.

Le premier niveau de structure est un niveau 0 qui remplace l'objet arbre organisationnel.

Par conséquent, ce niveau 0 de structure ne peut pas être alimenté (ne contient pas d'instances de structures).

En mode montée de version, les arbres organisationnels sont automatiquement modifiés en structure de niveau 0.

Consulter le chapitre « Créer / modifier / supprimer un type de structure dans un arbre organisationnel » de la documentation produit pour plus de détails sur cette fonctionnalité.

2.3.13.6 Communication entre SIP et la base de données Identity

En cas de montée de version, le lien odbc vers la BDD Identity créé pour les versions antérieures doit être supprimée.

2.4 Evolutions du moteur de provisioning (SIP)

2.4.1 Nouveaux Webservices

A partir de la version Cyberelements Identity 7.0, les appels aux séquences via le service HplianceSynchronisation doivent évoluer pour appeler les nouveaux WebServices SIP.

Consulter le chapitre « Exécution des séquences de provisioning via les webservices SIP » de la documentation produit pour plus de détails sur cette fonctionnalité.

2.4.2 Nouvelles fonctionnalités

2.4.2.1 Ajouts de mots-clés

Consulter le chapitre « Liste des mots-clés disponibles dans les opérations » de la documentation produit pour plus de détails sur cette fonctionnalité.

2.4.2.2 Nouveaux connecteurs du référentiel Identity

- Connecteur ACCOUNT : Exporte les comptes d'un référentiel indiqué dans la configuration ainsi que ses rôles et habilitations et ses attributs de compte. Peut être utilisé en import également, mais uniquement pour réaliser des mises à jour d'attributs sur les comptes. La création / suppression des comptes sont gérés uniquement par Identity suivant les règles de calculs configurées.
- Connecteur ROLE : Exporte et importe les rôles liés à un référentiel indiqué (paramètre facultatif). Permet de réaliser un connecteur pour créer/modifier/supprimer les rôles dans le référentiel Identity.
- Connecteur RIGHT : Exporte et importe les habilitations liées à un référentiel indiqué (paramètre facultatif). Permet de réaliser un connecteur pour créer/modifier/supprimer les habilitations dans le référentiel Identity.
- Connecteur HABILITATIONCALC : disponible uniquement en import, permet de lancer le recalcul des règles d'habilitations.
- Enumérations : les énumérations sont gérées par type d'objet. Les attributs de structures ayant été séparés des identités et les attributs de comptes ayant été créés, il y a donc désormais 4 types d'export différents :
    - ENUM_PERSON (existait, a été renommé, reprise automatique).
    - ENUM_RESOURCE (existait, a été renommé, reprise automatique).
    - ENUM_STRUCTURE (nouveau).
    - ENUM_ACCOUNT (nouveau).

2.4.2.3 Changements dans les connecteurs du référentiel Identity

- Connecteur de type PERSON, RESOURCE, STRUCTURE : dans les opérations d'import sur ces objets, une nouvelle option est disponible pour désactiver le calcul à la volée des règles d'habilitations lors de la création ou mise à jour des objets. En effet, pour avoir les meilleures performances, il est fortement recommandé de cocher cette option pour les séquences d'alimentation amont puis d'exécuter une séquence avec l'import de calcul des règles à la fin de l'alimentation amont. Ces opérations remplacent l'utilisation du booléen COMPUTED_KAD_ENABLED qui n'existe plus à partir de la version 7.0.
- PERSONACCESS : (anciennement USER+ACCESS) l'export évolue pour exporter uniquement les personnes qui possèdent un compte du référentiel indiqué dans la configuration. En cas de fusion de compte, c'est l'identité primaire qui est exportée. Non compatible avec le multicompte. Ce connecteur est maintenu en version 7.0 pour un souci de rétrocompatibilité en cas de montée de version mais il est déprécié à compter de la version 7.0.

  Pour l'export unitaire des référentiels Identity de type PERSONACCESS, il est obligatoire d'utiliser l'attribut account_id.

- Dans tous les connecteurs d'alimentation amont, dans les opérations Compares Rules dans les règles de Matching, il obligatoire d'avoir l'option Full cochée. En effet, il est obligatoire de renvoyer la valeur complète des attributs. L'option est donc cochée par défaut quand le référentiel de destination est Identity.

  Ce changement a pour conséquences qu'il ne sera plus possible de voir les valeurs avant et les valeurs après dans les rapports de synchronisation en cas de levée de seuil (uniquement pour les rapports d'alimentation amont).

- Pour alimenter des attributs de type énuméré, structure, personne ou dotation dans les connecteurs de personnes, structures, dotations ou comptes, il convient de mettre uniquement le code de l'attribut pour passer la valeur du code. Pour alimenter un attribut de type énuméré, bien que ce ne soit pas recommandé d'un point de vue performances, il est possible de l'alimenter via le libellé en mettant un « @ » devant le code.

- Pour les connecteurs de personnes, structures, dotations ou comptes, pour la matching des attributs dans les opérations On Create et Compare Rules, il est nécessaire d'utiliser les codes des attributs même pour les attributs systèmes. Exemple pour l'attribut « Nom » pour un identité : ne plus utiliser « user_name » mais bien « nom ». Attentions, les noms des attributs systèmes pour les structures et ressources ont évolué.

- Pour les connecteurs de personnes, structures, dotations ou comptes, dans les opérations On Modify, il est nécessaire de passer les attributs « ID » et « Type » issus de l'export de destination.

- Pour les connecteurs de personnes, structures, dotations ou comptes, dans les opérations On Delete, il est nécessaire de passer l'attribut « ID » issus de l'export de destination.

- Pour les connecteurs de remontée des états de provisioning, les changements de code des attributs systèmes doivent être reportés dans les connecteurs existants : utiliser account_login à la place de account.id dans les opérations, On Matching et On Create. Dans l'opération On Create, il est obligatoire de préciser un type de compte en plus du login. Cette configuration est nécessaire dans le cas où des comptes orphelins doivent être créés.

Consulter le chapitre « Les règles de Matching obligatoires dans les connecteurs d'alimentation amont » de la documentation produit pour plus de détails sur cette fonctionnalité.

SYSTANCIA

Actipolis 3, Bât C11

3, rue Paul Henri Spaak

68 390 SAUSHEIM

France

Téléphone : 03 89 33 58 20

Fax : 03 89 33 58 21

site web : https://www.systancia.com