Unica Platform 12.1.1 - Guide d'administration

Table des matières

Chapitre 1. Guide de l'Administrateur

Fonctions de Unica Platform

Unica Platform fournit des fonctions de sécurité, de configuration, de notification et de tableau de bord pour les produits Unica.

Unica Platform offre une interface utilisateur commune pour les produits Unica, ainsi que l'infrastructure des fonctions suivantes :

- Prise en charge de la génération de rapports dans de nombreux produits dans Unica.
- Prise en charge de la sécurité dans les applications , notamment l'authentification et l'autorisation.
- Gestion de la configuration, notamment la configuration des préférences de paramètres généraux et une interface qui permet d'éditer les propriétés de configuration de certaines applications d'Unica.
- Planificateur qui vous permet de configurer l'exécution d'un processus à des intervalles définis par vos soins.
- Pages de tableau de bord que vous pouvez configurer pour inclure des informations utiles pour les groupes d'utilisateurs qui rempliront différents rôles dans votre entreprise.
- Prise en charge et interface utilisateur pour les alertes et les notifications.
- Rapports d'audit de sécurité.

A propos des fonctionnalités de sécurité d'Unica Platform

Les fonctions de sécurité dans Unica Platform sont constituées d'un référentiel central et d'une interface Web où les utilisateurs internes Unica sont définis et affectés de divers niveaux d'accès aux fonctions dans les applications Unica.

Les applications Unica utilisent les fonctionnalités de sécurité de Unica Platform pour authentifier les utilisateurs, vérifier les droits d'accès des utilisateurs aux applications et enregistrer les données d'identification de base de données et d'autres données d'identification.

Technologies de sécurité utilisées dans Unica Platform

Unica Platform utilise des méthodes de cryptage standard pour exécuter l'authentification et appliquer la sécurité dans toutes les applications Unica. Les mots de passe utilisateur et de base de données sont protégés par diverses technologies de chiffrement.

Gestion des droits d'accès via les rôles

Unica Platform définit l'accès de base de l'utilisateur aux fonctions de la plupart des applications Unica. En outre, pour Unica Campaign et Unica Platform, vous pouvez contrôler l'accès de l'utilisateur aux fonctions et aux objets dans l'application.

Vous pouvez affecter différents droits d'accès aux rôles. Vous pouvez ensuite gérer les droits d'accès des utilisateurs de l'une des manières suivantes :

- Affectation de rôles aux utilisateurs
- Affectation de rôles aux groupes, puis définition de ces utilisateurs comme membres de ce groupe

A propos des partitions de Unica Campaign

Unica Platform prend en charge les partitions dans la famille de produits Unica Campaign. Les partitions permettent de sécuriser les données associées à différents groupes d'utilisateurs. Si vous configurez Unica Campaign ou une application associée à Unica afin de fonctionner avec plusieurs partitions, chaque partition apparaîtra aux yeux des utilisateurs comme une instance séparée de l'application, sans indication de l'existence d'autres partitions dans le même système.

A propos des groupes

Un sous-groupe hérite des rôles affectés à ses parents. L'administrateur peut définir un nombre illimité de groupes et n'importe quel utilisateur peut devenir membre de plusieurs groupes. Cela facilite la création de différentes combinaisons de rôles. Par exemple, un utilisateur peut être un administrateur d'Unica Deliver et un utilisateur de Unica Campaign sans privilèges d'administration.

Un groupe peut appartenir à une seule partition.

Gestion des données d'identification de source de données

Les utilisateurs et les administrateurs peuvent définir à l'avance les données d'identification de la source de données d'un utilisateur. L'utilisateur n'est alors pas invité à fournir les données d'identification de la source de données lorsqu'il utilise une application qui nécessite d'y accéder.

Intégration à des systèmes de gestion d'utilisateurs externes et de gestion des groupes

Unica Platform peut être configuré pour s'intégrer à des systèmes externes qui sont utilisés pour centraliser la gestion des utilisateurs et des ressources. Ces systèmes incluent Windows™ Active Directory Server, d'autres serveurs d'annuaire LDAP pris en charge et des plateformes de contrôle de l'accès Web telles que Netegrity SiteMinder et IBM® Security Access Manager. Cela permet de réduire les erreurs, les coûts de prise en charge et le temps nécessaire au déploiement d'une application dans la production.

Support SAML 2.0

Unica Platform prend en charge SAML (Security Assertion Markup Language) 2.0 pour les opérations suivantes.

- L'authentification fédérée SAML 2.0, qui permet une connexion unique entre diverses applications.

  Vous pouvez utiliser l'authentification fédérée pour implémenter la connexion unique entre des applications Unica et les autres applications ou applications tierces.

  L'installation de Unica Platform comporte les composants suivants qui prennent en charge l'authentification fédérée.

  - Fichier WAR d'un serveur de fournisseur d'identité.
  - Fichier JAR client pouvant être utilisé avec des applications Java™ et permettant de générer et d'analyser les assertions SAML 2.0. Les produits Java™ que vous intégrez à Unica utilisent les assertions pour communiquer avec le serveur fournisseur d'identité.
- Connexion unique SAML 2.0

Un serveur IdP SAML 2.0 totalement fonctionnel est un prérequis pour cette intégration.

Lorsque vous avez configuré les propriétés de configuration requises et un fichier de métadonnées, les utilisateurs qui tentent de se connecter via la page de connexion Unica Platform sont authentifiés via le serveur IdP (serveur de fournisseur d'identité) SAML 2.0 de votre entreprise.

Les utilisateurs qui sont connectés à une application qui utilise le serveur IdP pour l'authentification peuvent accéder à HCL Unica sans avoir à se reconnecter.

Filtres de données

Unica Platform prend en charge les filtres de données configurables qui permettent de définir des restrictions d'accès aux données dans les produits Unica. Les filtres de données permettent de restreindre les données du client qu'un utilisateur Unica peut consulter et utiliser dans les applications .

Gestion de la configuration

La page de configuration permet d'accéder aux propriétés de configuration centrale des applications Unica.

Les utilisateurs dotés de droits d'administrateur dans Unica Platform peuvent utiliser la page de configuration pour procéder aux opérations suivantes.

- Parcourir les propriétés de configuration, organisées par produit dans une hiérarchie de catégories et de sous-catégories.
- Editer les valeurs des propriétés de configuration.
- Supprimer certaines catégories (les catégories que vous pouvez supprimer sont précédées du lien **Supprimer la catégorie** sur la page Paramètres).

Vous pouvez effectuer des modifications supplémentaires dans la page Configuration en utilisant l'utilitaire configTool fourni avec Unica Platform.

Localisation dans Unica

Unica Platform prend en charge la localisation via son codage de jeux de caractères et en permettant à un administrateur de définir des préférences de paramètres régionaux pour des utilisateurs individuels ou tous les utilisateurs. Les utilisateurs peuvent également définir leurs propres préférences de paramètres régionaux.

Pour les utilisateurs internes et externes, vous pouvez définir les préférences de paramètres régionaux par utilisateur ou dans les applications d' qui prennent en charge cette fonctionnalité. Ce paramétrage des préférences affecte l'affichage de la langue, de l'heure, des nombres et des dates au sein des applications Unica.

Unica Platform prend en charge UTF-8 comme codage de jeu de caractères par défaut qui permet aux utilisateurs d'entrer des données dans n'importe quelle langue, telle que le chinois ou le japonais. Cependant, notez que le support complet d'un jeu de caractères dans Unica Platform dépend également de la configuration :

- de la base de données de la table système Unica Platform
- des machines et des navigateurs client permettant d'accéder à Unica.

Interface utilisateur commune

Unica Platform fournit un point d'accès et une interface utilisateur communs pour les applications Unica.

L'interface commune propose les fonctionnalités suivantes.

- Si plusieurs produits Unica sont installés, vous pouvez naviguer entre les produits sans lancer de nouvelles fenêtres.
- Vous pouvez consulter la liste des pages récemment visitées, puis naviguer vers l'une de ces pages à l'aide du menu **Récentes**.
- Vous pouvez définir une page Unica comme page d'accueil (la première page qui s'affiche lorsque vous vous connectez). Pour retourner à cette page à tout moment, cliquez sur l'icône Page d'accueil.
- Pour accéder à la fonction de recherche de chaque produit installé, utilisez la zone **Rechercher**. Le contexte de cette fonction de recherche est la page que vous

consultez. Par exemple, si vous consultez une liste de campagnes dans Unica Campaign, la recherche s'effectue dans toutes les campagnes. Si vous souhaitez rechercher un projet Unica Plan, la recherche s'effectue tout en consultant la liste des projets Unica Plan.

Connexion à Unica

Utilisez la procédure ci-dessous pour vous connecter à Unica.

Vous devez disposer des éléments suivants :

- Une connexion Intranet (réseau) permettant d'accéder à votre serveur Unica.
- Un navigateur pris en charge installé sur votre ordinateur.
- Un nom d'utilisateur et un mot de passe permettant de se connecter à Unica.
- Adresse URL permettant d'accéder à Unica sur votre réseau.

L'adresse URL est la suivante :

`http://host.domain.com:port/unica`

où

`host` est la machine où Unica Platform est installé.

`domain.com` est le domaine dans lequel réside la machine hôte.

`port` est le numéro de port sur lequel le serveur d'application Unica Platform écoute.

Remarque : La procédure suivante suppose que vous êtes connecté avec un compte disposant d'un accès Admin à Unica Platform.

Accédez à l'URL d'Unica à l'aide de votre navigateur.

- Si Unica est configuré pour s'intégrer à Windows™ Active Directory ou une plateforme de contrôle d'accès Web et que vous êtes connecté à ce système, la page du tableau de bord par défaut s'affiche. Votre connexion est terminée.
- Si l'écran de connexion s'affiche, connectez-vous à l'aide des droits d'administrateur par défaut. Dans un environnement à partition unique, utilisez l'identifiant `asm_admin`

et le mot de passe `password`. Dans un environnement à plusieurs partitions, utilisez l'identifiant `platform_admin` et le mot de passe `password`.

Vous êtes invité à changer de mot de passe. Vous pouvez réutiliser le mot de passe existant, mais pour des raisons de sécurité, il est conseillé d'en choisir un nouveau.

- Si Unica est configurée pour utiliser une connexion SSL, il vous sera éventuellement demandé lors de votre première connexion d'accepter un certificat de sécurité numérique. Cliquez sur **Oui** pour accepter le certificat.

Si votre connexion aboutit, Unica affiche la page du tableau de bord par défaut.

Avec les autorisations par défaut affectées aux comptes administrateur Unica Platform, vous pouvez administrer les comptes utilisateur et la sécurité en utilisant les options répertoriées dans le menu **Paramètres**. Pour effectuer les tâches d'administration de niveau supérieur d'Unica, vous devez vous connecter avec l'identifiant **platform_admin**.

Documentation et aide relatives à Unica Platform

Unica Platform fournit de la documentation et de l'aide pour les utilisateurs, les administrateurs et les développeurs.

Tableau 1. Se lancer immédiatement

Tâche	Documentation
Consulter une liste de nouvelles fonctions, de problèmes connus et de solutions de contournement	*Unica PlatformEdition Notes®*
Découvrir la structure de la base de données Unica Platform	*Unica Platform Guide des tables système*
Installation ou mise à niveau de Unica Platform et déploiement de l'application Web Unica Platform	L'un des guides suivants : • *Unica Platform Guide d'installation* • *Unica Platform - Guide de mise à niveau*

Tableau 1. Se lancer immédiatement (suite)

Tâche	Documentation
Implémenter les rapports Cognos® fournis avec Unica	Unica Reports - Guide d'installation et de configuration

Tableau 2. Configurer et utiliser Unica Platform

Tâche	Documentation
• Ajuster les paramètres de configuration et de sécurité pour les produits • Effectuer l'intégration avec des systèmes externes tels que LDAP et le contrôle de l'accès Web • Implémenter la connexion unique avec diverses applications à l'aide de l'authentification fédérée SAML 2.0 ou de la connexion unique • Exécuter des utilitaires de maintenance sur les produits • Configurer et utiliser le suivi des événements d'audit • Planifier des exécutions d'objets Unica	*Unica Platform Guide d'administration*

Octroi de licences - Présentation

Les produits HCL Unica sont basés sur des licences. Les utilisateurs doivent configurer les licences requises avec les produits pour commencer à les utiliser.

La liste suivante répertorie les produits Unica pour lesquels une licence est obligatoire :

- Unica Platform
- Unica Campaign
- Unica Interact
- Unica Deliver
- Unica Journey

Une fois que les utilisateurs ont effectué une nouvelle installation ou une mise à niveau à la version 12.1 des produits Unica et qu'ils ont déployé ces produits,

ils doivent configurer la licence. Lorsque l'utilisateur visite l'URL de l'application Unica Platform, cette URL redirige vers l'écran des détails de licence. Les utilisateurs doivent configurer les licences pour commencer à utiliser les produits Unica. Uniquement après avoir fourni des informations de licence valides, les utilisateurs sont redirigés vers l’écran de connexion à Unica Platform.

Portail des licences

Le portail de licences permet de distribuer et de gérer les logiciels de vos autorisations logicielles achetées via HCL Products and Platforms. Le portail vous offre contrôle et flexibilité au niveau du mode d'utilisation de vos licences. Il permet également d’enregistrer les licences. Généralement, une organisation dispose d'une personne identifiée comme le gestionnaire de licences, qui maîtrise le langage des licences. Il se peut que vous souhaitiez l'ajouter en tant qu'utilisateur. Si tel n'est pas le cas, ces instructions sont suffisantes pour vous permettre de commencer à utiliser votre logiciel HCL.

Licences et détails de consommation

Les utilisateurs peuvent vérifier les détails de consommation des licences sur le portail de licences HCL, ainsi que sur la page des détails de licence Unica Platform, en accédant à Paramètres > Page des détails de licence. Cliquez sur Afficher la page des détails de licence pour afficher le nombre de licences pour tous les produits autorisés. En cas d’absence de connectivité avec le serveur de licences, la consommation des licences peut être téléchargée et partagée avec Unica.

Nom du produit	Nom du produit HCL Unica pour lequel l’autorisation d'utilisation est attribuée
Type de licence	A durée limitée/Perpétuelle
Date de début	Date de début de l'autorisation d'utilisation
Date d'expiration	Date d’expiration de l'autorisation d'utilisation (non applicable pour la licence perpétuelle)

Autorisations d'utilisation disponibles	Nombre total d’autorisations d'utilisation attribuées pour un périphérique ou un serveur.
Droits consommés	Nombre d'autorisations d'utilisation consommées jusqu’à présent
Droits à découvert	Modèle de licence utilisé, le modèle actuel prend en charge des découverts illimités. (Non applicable pour la licence perpétuelle)
Découvert consommé	Différence entre les autorisations d'utilisation disponibles et les autorisations d'utilisation consommées. (Non applicable pour la licence perpétuelle)

Pour plus d’informations sur l’octroi de licence, voir le Guide d’octroi de licence HCL Unica.

Configuration de la licence

Les utilisateurs doivent configurer la licence avec les produits HCL Unica avant de commencer à les utiliser. Lorsque les utilisateurs accèdent à l'URL de connexion à Unica Platform, ils sont redirigés vers la page de configuration de la licence. Les utilisateurs doivent configurer les détails de la licence sur cette page. Unica Platform valide la licence et, une fois la licence bien configurée, les utilisateurs sont redirigés vers l’écran de connexion d'Unica Platform.

Serveur de licences	URL de l’API du serveur de licences. L’utilisateur peut obtenir l’URL du serveur de licences à partir du Portail de licences HCL.
Utilisateur	Serveur de licences HCL – Pour tout périphérique créé par défaut, l’utilisateur "admin" est pris en charge.
Mot de passe	Mot de passe du périphérique
Type d’environnement Unica	L’utilisateur peut indiquer s’il s’agit d’un environnement "de production" ou de "non production".

Proxy	Utilisez le serveur proxy pour vous connecter au portail de licences HCL. Utilisez le serveur proxy si vous ne disposez pas d'un accès sortant au portail de licences HCL.
Hôte proxy	Nom d'hôte ou adresse IP du serveur proxy
Port du proxy	Port du serveur proxy
Utilisateur proxy	Utilisateur du serveur proxy
Mot de passe du proxy	Mot de passe de l'utilisateur du serveur proxy

Tous ces détails du serveur de licences sont stockés dans Unica Platform. L'utilisateur peut accéder à Paramètres > Page des détails de licence si les détails de la licence doivent être modifiés.

Disponibilité du serveur de licences

Les produits HCL Unica doivent être toujours connectés au portail de licences HCL. Les produits HCL Unica deviennent inaccessibles s'il n'y a pas de connectivité pendant 5 heures entre les produits HCL Unica et le serveur de portail de licences HCL. Les utilisateurs sont redirigés vers la page des détails de licence. Une fois que la connectivité entre HCL Unica et le serveur de licences HCL est établie, les utilisateurs peuvent accéder à l'application. Les produits HCL Unica mettent à jour les détails de consommation sur le portail de licences HCL toutes les 10 minutes. En cas de problème de connectivité, les détails de consommation aident Unica Platform et une fois la connectivité établie, la consommation est mise à jour sur le portail de licences HCL.

Détails de la consommation des licences

Les utilisateurs peuvent vérifier les détails de consommation des licences sur le portail de licences HCL, ainsi que sur la page des détails de licence Unica Platform. L'utilisateur peut

accéder à Paramètres > Page des détails de licence. Cliquez sur Afficher la page des détails de licence pour afficher le nombre de licences pour tous les produits autorisés.

Nom du produit	Nom du produit HCL Unica pour lequel l’autorisation d'utilisation est attribuée
Type de licence	A durée limitée/Perpétuelle
Date de début	Date de début de l'autorisation d'utilisation
Date d'expiration	Date d’expiration de l'autorisation d'utilisation (non applicable pour la licence perpétuelle)
Autorisations d'utilisation disponibles	Nombre total d’autorisations d'utilisation attribuées pour un périphérique ou un serveur.
Droits consommés	Nombre d'autorisations d'utilisation consommées jusqu’à présent
Droits à découvert	Modèle de licence utilisé, le modèle actuel prend en charge des découverts illimités. (Non applicable pour la licence perpétuelle)
Découvert consommé	Différence entre les autorisations d'utilisation disponibles et les autorisations d'utilisation consommées. (Non applicable pour la licence perpétuelle)

La page des détails de licence affiche un message indiquant "Aucune licence configurée dans cet environnement, car cet environnement n’est pas un environnement de production" lorsque vous avez sélectionné un environnement hors production lors de la spécification des détails de la licence.

Si vous avez besoin de transformer un environnement hors production en environnement de production, vous pouvez modifier les détails de la licence et marquer le type d’environnement comme "production". Lorsque vous marquez cet environnement comme environnement de production, vous devez saisir tous les détails de la licence.

Remarque : La page de détails de licence n’affiche que les autorisations d'utilisation actives des produits HCL Unica.

Pour plus de détails, voir le document d'octroi de licences Unica.

Gestion des comptes utilisateur Unica

Vous pouvez gérer les attributs des comptes utilisateur créés dans l'interface utilisateur Unica Platform, appelés comptes internes. Ces comptes se distinguent des comptes utilisateur externes qui sont importés depuis un système externe, tel qu'un serveur LDAP ou un système de contrôle d'accès.

Les comptes externes sont gérés dans le système externe.

Types de compte utilisateur : Interne et externe

Lorsque Unica est intégré à un serveur externe (un serveur LDAP compatible ou un système de contrôle d'accès Web, par exemple), il prend en charge deux types de comptes utilisateur : interne et externe

- **Internes** – Comptes utilisateur créés dans Unica à l'aide de l'interface utilisateur de sécurité. Ces utilisateurs sont authentifiés via Unica.
- **Externes** – Comptes utilisateur importés dans Unica par synchronisation à l'aide d'un serveur externe. La synchronisation n'a lieu que si Unica a été configuré pour s'intégrer au serveur externe. Ces utilisateurs sont authentifiés via le serveur externe. Parmi les serveurs externes, citons les serveurs LDAP et de contrôle de l'accès Web.

Selon votre configuration, vous pouvez avoir uniquement des utilisateurs internes, uniquement des utilisateurs externes ou une combinaison des deux types d'utilisateur. Si vous intégrez Unica à Windows™ Active Directory et activez LDAP, vous ne pouvez utiliser que des utilisateurs externes.

Pour plus d'informations sur l'intégration de Unica à un serveur LDAP ou un serveur Windows™ Active Directory, voir les sections correspondantes dans ce guide.

Gestion des utilisateurs externes

En règle générale, les attributs de compte utilisateur externe sont gérés via le système externe. Dans Unica, vous pouvez contrôler les éléments suivants d'un compte utilisateur externe : sources de données, préférences de notification, préférence d'environnement local pour les applications Unica et appartenance aux groupes internes (mais pas aux groupes externes).

Identification des utilisateurs internes et externes dans l'interface d'Unica

Dans la section Utilisateurs d'Unica, les utilisateurs internes et externes ont différents icônes.

- Utilisateurs internes - 
- Utilisateurs externes - 

Propriétés des comptes utilisateur internes

Les administrateurs peuvent gérer les propriétés des comptes utilisateur qui ont été créés à l'aide de l'interface utilisateur Unica Platform.

Oubli du mot de passe par un utilisateur

Unica Platform enregistre les mots de passe des utilisateurs internes sous forme échantillonnée et ces mots de passe enregistrés ne peuvent pas être récupérés en texte clair. Vous devez affecter un nouveau mot de passe aux utilisateurs qui possèdent un compte interne et qui ont oublié leur mot de passe.

Réinitialisation d'un mot de passe

Les utilisateurs qui possèdent des comptes internes peuvent changer leurs propres mots de passe. Pour ce faire, ils saisissent le mot de passe d'origine, saisissent le nouveau mot de passe, puis le confirment. L'administrateur d'Unica peut également réinitialiser n'importe quel mot de passe utilisateur, le cas échéant.

Dates d'expiration des mots de passe

Dans la page Configuration, vous pouvez définir des fréquences d'expiration de mot de passe pour tous les utilisateurs. Vous pouvez également définir des dates d'expiration pour chaque utilisateur (lorsque la date d'expiration système n'est pas définie pour ne jamais expirer).

Etat système des comptes utilisateur

L'état système d'un utilisateur est Activé ou Désactivé. Un utilisateur dont le compte est désactivé ne peut pas se connecter à une application Unica. Si un compte utilisateur désactivé a précédemment été actif avec une appartenance à un ou plusieurs groupes, vous pouvez le réactiver. Lorsque vous réactivez un compte utilisateur désactivé, les appartenances au groupe sont conservées.

Autre identification de connexion

Vous pouvez définir des informations de connexion alternatives pour n'importe quel compte utilisateur. Une autre connexion est généralement nécessaire lorsque le module d'écoute de Unica Campaign s'exécute en tant que root sur un système UNIX™.

Sources de données

Un utilisateur doit disposer des données d'identification appropriées pour accéder aux sources de données utilisées par certaines applications Unica. Vous pouvez entrer ces données d'identification en tant que source de données dans les propriétés de compte utilisateur.

Lorsqu'un utilisateur travaille dans une application Unica, telle que Unica Campaign et que le système lui demande des informations de source de données, l'application Unica enregistre ces informations dans le magasin de données Unica Platform. Ces sources de données apparaissent dans la liste des sources de données de l'utilisateur dans Unica Platform, même si elles n'ont pas été créées en utilisant l'interface Unica.

Ajout de comptes utilisateur internes

Cette procédure permet d'ajouter des comptes utilisateur internes.

1. Cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur **Nouvel utilisateur**.
3. Remplissez le formulaire, puis cliquez sur **Enregistrer les modifications**.

   Soyez prudent si vous utilisez des caractères spéciaux dans les noms de connexion. Les caractères spéciaux autorisés sont répertoriés dans la référence de page Nouvel utilisateur.
4. Cliquez sur **OK**.

   Le nouveau nom d'utilisateur apparaît dans la liste.

Suppression de comptes utilisateur internes

Cette procédure permet de supprimer des comptes utilisateur internes.

Important : Si des droits Unica Campaign permettent à un seul utilisateur de détenir un objet Unica Campaign ou d'y accéder, la suppression du compte de cet utilisateur rend cet objet inaccessible. En revanche, vous devez désactiver ces comptes.

1. Cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur le nom d'utilisateur du compte à supprimer.
3. Cliquez sur **OK**.

Changement des dates d'expiration des mots de passe des utilisateurs internes

Cette procédure permet de changer les dates d'expiration des mots de passe des utilisateurs internes.

Restriction : Si la propriété d'expiration de mot de passe du système **Général | Paramètres de mot de passe | Validité (en jours)** a pour valeur zéro, vous ne pouvez pas changer la date d'expiration du mot de passe d'un utilisateur interne.

1. Cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur le nom d'utilisateur.
3. Cliquez sur le lien **Editer les propriétés** au bas de la page.
4. Modifiez la date dans la zone **Expiration du mot de passe**.
5. Cliquez sur **OK**.

Réinitialisation des mots de passe des utilisateurs internes

Cette procédure permet de réinitialiser les mots de passe des utilisateurs internes.

1. Cliquez sur **Paramètres > Utilisateurs**.

   La liste **Utilisateurs** s'affiche dans le panneau de gauche.
2. Cliquez sur le nom d'utilisateur à changer.
3. Cliquez sur le lien **Réinitialiser le mot de passe** au bas de la page.
4. Saisissez le nouveau mot de passe dans la zone **Mot de passe**.
5. Saisissez le même mot de passe dans la zone **Confirmer**.
6. Cliquez sur **Enregistrer les changements** pour enregistrer vos modifications.
7. Cliquez sur **OK**.

Remarque : Lorsque leurs mots de passe ont été réinitialisés, les utilisateurs sont invités à changer de mot de passe à la connexion suivante à une application Unica.

Changement des propriétés de compte des utilisateurs internes

Cette procédure permet de changer les propriétés d'un compte d'utilisateur interne.

1. Cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur le nom du compte à changer.
3. Cliquez sur le lien **Editer les propriétés** au bas de la page.
4. Editez les zones selon vos besoins.

5. Cliquez sur **Enregistrer les changements** pour enregistrer vos modifications.
6. Cliquez sur **OK**.

Changement du statut système des utilisateurs internes

Cette procédure permet de changer le statut système des utilisateurs internes.

1. Cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur le nom du compte à changer.
3. Cliquez sur le lien **Editer les propriétés** au bas de la page.
4. Sélectionnez l'état dans la liste déroulante **Etat**. Les options **ACTIF** et **DESACTIVE** sont disponibles.

   Remarque : Si vous sélectionnez **DESACTIVE**, l'utilisateur ne pourra plus se connecter à aucune application d'Unica. Les utilisateurs disposant d'un accès administrateur à Unica Platform ne peuvent pas se désactiver.

5. Cliquez sur **Enregistrer les changements** pour enregistrer vos modifications.
6. Cliquez sur **OK**.

Ajout de sources de données pour les utilisateurs internes

Cette procédure permet d'ajouter des sources de données pour les utilisateurs internes.

1. Cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur le nom du compte à changer.
3. Cliquez sur le lien **Modifier les sources de données** en bas de la page.
4. Cliquez sur **Ajouter nouveau**.
5. Renseignez le formulaire et cliquez sur **Enregistrer les modifications** pour enregistrer vos modifications.
6. Cliquez sur **OK**.

Changement des sources de données pour les utilisateurs internes

Cette procédure permet de changer les mots de passe ou les noms de connexion des sources de données.

1. Cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur le nom du compte à changer.
3. Cliquez sur le lien **Modifier les sources de données** en bas de la page.
4. Cliquez sur le **Nom de la source de données** à changer.
5. Editez les zones.

   Si vous ne définissez pas de nouveau mot de passe, l'ancien est conservé.
6. Renseignez le formulaire et cliquez sur **Enregistrer les modifications** pour enregistrer vos modifications.
7. Cliquez sur **OK**.

Suppression de sources de données pour les utilisateurs internes

Cette procédure permet de supprimer des sources de données pour les utilisateurs internes.

1. Cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur le nom du compte à changer.
3. Cliquez sur le lien **Modifier les sources de données** au bas de la page.
4. Cliquez sur le Nom de la source de données que vous souhaitez supprimer.
5. Cliquez sur **Supprimer**.
6. Cliquez sur **OK**.

Pages de gestion des utilisateurs

Voir le tableau suivant si vous avez besoin d'aide pour renseigner les zones de la page Utilisateurs.

Page Nouvel utilisateur

Tableau 3. Zones de la page Nouvel utilisateur

Zone	Description
Prénom	Prénom de l'utilisateur.
Nom	Nom de l'utilisateur.
Connexion	Nom de connexion de l'utilisateur. Il s'agit de la seule zone obligatoire. Seuls les caractères spéciaux suivants sont autorisés dans les noms de connexion : • Caractères alphabétiques en majuscules et minuscules (A-Z, a-z) • Nombres (0-9) • Signe arobase (@) • Trait d'union (-) • Trait de soulignement (_) • Point (.) • Caractères codés sur deux octets (caractères chinois, par exemple) N'ajoutez pas d'autres caractères spéciaux dans un nom de connexion (espaces compris).
Mot de passe	Mot de passe de l'utilisateur. Suivez ces règles lorsque vous créez un mot de passe. • La casse des mots de passe doit être respectée. Par exemple, `password` n'est pas identique à `Password`. • Vous pouvez utiliser n'importe quel caractère lorsque vous créez ou réinitialisez un mot de passe dans Unica. D'autres besoins relatifs aux mots de passe sont définis dans la page de configuration. Pour savoir ce à quoi ils correspondent

Tableau 3. Zones de la page Nouvel utilisateur (suite)

Zone	Description
	pour votre installation d'Unica, cliquez sur le lien **Règles du mot de passe** situé en regard de la zone **Mot de passe**.
Confirmer le mot de passe	Même mot de passe que celui saisi dans la zone **Mot de passe.**
Titre	Titre de l'utilisateur.
Service	Service de l'utilisateur.
Société	Société de l'utilisateur.
Pays	Pays de l'utilisateur.
Adresse	Adresse de l'utilisateur.
Téléphone bureau	Numéro de téléphone du bureau de l'utilisateur.
Téléphone cellulaire	Numéro de téléphone mobile de l'utilisateur.
Téléphone du domicile	Numéro de téléphone du domicile de l'utilisateur.
Adresse E-mail	Adresse e-mail de l'utilisateur. Cette zone doit se conformer aux formats d'adresses e-mail définis dans la norme RFC 821. Pour plus de détails, voir la norme RFC 821.
Autre identification de connexion	Nom de connexion UNIX™ de l'utilisateur, s'il existe. Une autre connexion est généralement nécessaire lorsque le module d'écoute de Unica Campaign s'exécute en tant que root sur un système UNIX™.
Statut	Sélectionnez ACTIVE ou DESACTIVE dans la liste déroulante. ACTIVE est sélectionné par défaut. Les utilisateurs inactifs ne peuvent se connecter à aucune application d'Unica.

Page Editer les propriétés

Les zones sont identiques à celles de la page Nouvel utilisateur, à l'exception de celles présentées dans le tableau ci-dessous.

Tableau 4. Zones de la page Editer les propriétés

Zone	Description
Mot de passe	Cette zone n'est pas disponible dans la fenêtre Editer les propriétés.
Connexion	Cette zone n'est pas disponible dans la fenêtre Editer les propriétés.
Expiration des mots de passe	Date au format approprié à vos paramètres régionaux (par exemple, le format approprié au paramètre régional en_US est `MM, dd, yyyy`). Vous ne pouvez pas changer la date d'expiration d'un utilisateur lorsqu'aucune date d'expiration n'est définie dans le système.
Nom d'utilisateur IBM® Digital Analytics	Lorsque l'intégration est activée avec IBM Digital Analytics et que vous choisissez de créer des utilisateurs manuellement, entrez le nom des utilisateurs Digital Analytics ici, pendant le processus de configuration.

Page Réinitialiser le mot de passe

Tableau 5. Zones de la page Réinitialiser le mot de passe

Zone	Description
Mot de passe	Nouveau mot de passe.
Confirmer	Même mot de passe que celui saisi dans la zone **Mot de passe**.

Pages Nouvelle source de données et Editer les propriétés de la source de données

Tableau 6. Zones des pages de sources de données

Zone	Description
Source de données	Nom d'une source de données dont vous souhaitez autoriser l'accès à un utilisateur à partir d'une application Unica. Les noms Unica conservent la casse pour l'affichage, mais ne la conservent pas pour la comparaison et la création (par exemple, vous ne pouvez pas créer de noms de sources de données `client` et `Client`).
Connexion à la source de données	Nom de connexion pour cette source de données.
Mot de passe de la source de données	Mot de passe pour cette source de données. Vous pouvez laisser cette zone vide si le compte de source de données ne possède pas de mot de passe.
Confirmer le mot de passe	Même mot de passe (laissez la zone vide si vous n'avez pas défini de mot de passe dans la zone **Mot de passe de la source de données**).

Préférences de paramètres régionaux

Vous pouvez définir les paramètres régionaux pour les utilisateurs internes et externes. Ce paramétrage affecte l'affichage de la langue, de l'heure, des nombres et des dates au sein des applications Unica.

Il existe deux manières de définir les paramètres régionaux dans Unica Platform.

Globalement

Une propriété de configuration (`Platform | Paramètre régional` dans la page **Paramètres > Configuration**) définit les paramètres régionaux de façon globale.

Par utilisateur

Un attribut de la page **Paramètres > Utilisateurs** définit les paramètres régionaux pour les utilisateurs individuels. Ce paramétrage remplace le paramétrage global.

La disponibilité des paramètres régionaux que vous pouvez définir par utilisateur ou globalement peut varier en fonction de l'application Unica, et toutes les applications Unica ne prennent pas en charge ce paramètre régional dans Unica Platform. Consultez la documentation spécifique au produit pour savoir si la propriété `Paramètre régional` est disponible et prise en charge.

Remarque : La disponibilité des paramètres régionaux que vous pouvez définir par utilisateur ou globalement peut varier en fonction de l'application Unica. Toutes les applications Unica ne prennent pas en charge ce paramètre régional. Consultez la documentation spécifique au produit pour savoir si les paramètres régionaux sont disponibles et pris en charge dans Unica.

Définition des préférences de paramètres régionaux d'un utilisateur

Utilisez la procédure ci-dessous pour définir les préférences de paramètres régionaux d'un utilisateur.

1. Cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur le nom d'utilisateur pour lequel vous souhaitez définir les préférences de paramètres régionaux.
3. Cliquez sur le lien **Editer les préférences** au bas de la page.
4. Cliquez sur **Unica Platform** dans le panneau de gauche.
5. Sélectionnez une option dans la liste déroulante **Région**.
6. Cliquez sur **Enregistrer les modifications**.

Synchronisation des utilisateurs externes

Lorsqu'Unica est configuré pour s'intégrer à un serveur Windows™ Active Directory ou un serveur LDAP, les utilisateurs et les groupes sont synchronisés automatiquement à une fréquence prédéfinie.

La synchronisation automatique a une fonctionnalité limitée.

- Les utilisateurs qui sont supprimés du serveur LDAP ne sont pas supprimés lors de la synchronisation automatique.

Vous pouvez forcer la synchronisation intégrale de tous les utilisateurs et tous les groupes en utilisant la fonction Synchroniser dans la zone Utilisateurs d'Unica.

Synchronisation forcée des utilisateurs externes

Utilisez la procédure ci-dessous pour forcer la synchronisation des utilisateurs lorsque Unica est intégré à un serveur LDAP ou un système de contrôle d'accès Web.

1. Connectez-vous à Unica, puis cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur **Synchroniser.**

   Les utilisateurs et les groupes sont synchronisés.

Gestion de la sécurité

Unica Platform prend en charge les rôles et les droits d'accès pour contrôler l'accès utilisateur aux objets et aux fonctionnalités contenus dans les applications Unica.

Généralement, seuls Unica Platform et Unica Campaign utilisent la page Rôles et autorisations utilisateur pour gérer en détail l'accès des utilisateurs aux applications.

Les autres produits Unica utilisent certains rôles d'accès à l'application de base définis dans la page Rôles et autorisations utilisateur et n'ont pas de paramètres de sécurité détaillés ou ont des paramètres qui ne sont pas gérés dans la page Rôles et autorisations utilisateur.

Par exemple, dans Unica Plan, la configuration des rôles de base dans la page Rôles et autorisations utilisateurs constitue uniquement le point de départ du développement d'un

schéma de sécurité personnalisé. Unica Plan possède un schéma de sécurité détaillé que vous pouvez gérer via une interface utilisateur dans les pages Unica Plan.

Ce guide vous explique comment utiliser les fonctions de la page Rôles et autorisations utilisateur et décrit les rôles et autorisations de sécurité de base affichés dans cette page pour les divers produits. Pour les produits autres que Unica Platform, si vous ne trouvez pas les informations de gestion de la sécurité dont vous avez besoin dans ce guide, reportez-vous à la documentation du produit.

Droits d'accès et tâches de l'administrateur de la sécurité dans Unica Platform

Seuls les utilisateurs ayant le rôle AdminRole ou PlatformAdminRole dans Unica Platform ont accès aux fonctions d'administration de la sécurité pour les comptes utilisateur autres que les leurs.

Dans un environnement à partitions multiples, seuls les utilisateurs qui possèdent le rôle PlatformAdminRole peuvent administrer les utilisateurs dans toutes les partitions. Les utilisateurs qui possèdent le rôle AdminRole ne peuvent administrer que les utilisateurs qui se trouvent dans leur propre partition.

L'administrateur de sécurité effectue les tâches suivantes sur les pages Groupes d'utilisateurs et Rôles et autorisations utilisateur :

- Créer des groupes internes et gérer leurs membres et leurs affectations de partition.
- Créer des rôles pour Unica Platform et Unica Campaign, si nécessaire, et affecter des autorisation à ces rôles.
- Gérez l'accès utilisateur à une application Unica en affectant des rôles aux utilisateurs individuels et/ou aux groupes internes et externes.

Lisez cette présentation pour comprendre ce qui suit.

- Différence entre groupes internes et groupes externes
- Processus de création de groupes internes et affectation de rôles et de droits d'accès
- Propriétés des groupes internes
- Comptes utilisateur, groupes et rôles prédéfinis dans Unica Platform

Caractères spéciaux dans les noms de rôle et de règle

Vous pouvez utiliser exclusivement les caractères suivants lorsque vous créez un nom de rôle ou de règle :

- Caractères alphabétiques en majuscules et minuscules (A-Z)
- Nombres (0-9)
- Guillemet simple (')
- Tiret (-)
- Souligné (_)
- Signe arobase (@)
- Barre oblique droite (/)
- Parenthèse
- Deux points (:)
- Point-virgule (;)
- Espace (excepté comme premier caractère)
- Caractères codés sur deux octets (caractères chinois, par exemple)

Rôles et droits d'accès de Unica Platform et Unica Campaign

Dans Unica Platform et Unica Campaign, les rôles constituent une collection configurable de droits d'accès. Dans Unica Platform et Unica Campaign, vous pouvez, pour chaque rôle, spécifier des droits d'accès à l'application.

Vous pouvez utiliser les rôles par défaut ou en créer de nouveaux. L'ensemble des droits d'accès disponibles est défini par le système, vous ne pouvez pas en créer vous-même.

A propos de l'affectation de rôles

En règle générale, vous devez affecter aux utilisateurs des rôles dont les droits d'accès correspondent tâches réalisées par les utilisateurs dans votre organisation lorsqu'ils utilisent Unica. Vous pouvez affecter des rôles à un groupe ou à un utilisateur en particulier. L'affectation de rôles à des groupes permet d'affecter une combinaison de rôles au groupe. Par la suite, si vous souhaitez changer cette combinaison, vous pouvez le faire en une seule fois, sans répéter l'opération pour chaque utilisateur. Lorsque vous affectez des rôles à

un groupe, vous ajoutez et supprimez des utilisateurs de vos groupes pour gérer l'accès utilisateur.

Evaluation des rôles par le système

Si un utilisateur dispose de plusieurs rôles, le système évalue les droits d'accès de l'ensemble de ces rôles. L'utilisateur est alors autorisé ou non à accomplir une fonction sur un objet particulier en fonction des droits d'accès agrégés de tous les rôles. Dans le cas de Unica Campaign, l'utilisateur est autorisé ou non à accomplir une fonction sur un objet particulier en fonction de la politique de sécurité de l'objet.

Présentation de la gestion de l'accès des utilisateurs aux applications dans Unica Platform

L'utilisation des fonctions d'administration de la sécurité Unica Platform pour gérer l'accès aux applications des utilisateurs est un processus à plusieurs étapes. La procédure suivante donne une présentation du processus de base, qui est décrit plus en détails dans le reste de ce guide.

1. Planifiez les rôles que vous voulez utiliser pour contrôler l'accès utilisateur aux produits Unica. Configurez les rôles et leurs droits d'accès, le cas échéant.
2. Planifiez les groupes dont vous avez besoin pour répondre à vos besoins de sécurité. Selon la configuration de votre système, vous pouvez posséder uniquement des groupes internes, uniquement des groupes externes ou une combinaison des deux types d'utilisateur.
3. Créez les groupes internes et externes dont vous avez besoin.
4. Affectez vos groupes aux rôles.
5. Si vous ne possédez que des comptes utilisateur internes, créez les comptes utilisateur internes, selon les besoins.
6. Affectez les utilisateurs aux groupes ou affectez les rôles à des utilisateurs individuels, en fonction de l'accès à une application que vous souhaitez donner aux utilisateurs.

Types de groupe : Interne et externe

Lorsque Unica est intégré à un serveur externe (un serveur LDAP ou un système de contrôle d'accès Web compatible), il prend en charge deux types de groupes : interne et externe

- **Internes** – Groupes créés dans Unica à l'aide de l'interface utilisateur de sécurité. Ces utilisateurs sont authentifiés via Unica.
- **Externes** – Groupes Unica mappés à des groupes du système externe. Parmi les serveurs externes, citons les serveurs LDAP et de contrôle de l'accès Web.

Avertissement : Un groupe référencé comme externe dans ce guide est en réalité créé dans Unica, mais est mappé à un système externe.

Selon votre configuration, vous pouvez avoir uniquement des groupes internes, uniquement des groupes externes ou une combinaison des deux types d'utilisateur.

Pour plus d'informations sur l'intégration de Unica à un serveur LDAP ou un serveur Windows™ Active Directory, voir les sections correspondantes dans ce guide.

Gestion des groupes externes

L'appartenance aux groupes externes est gérée dans le système externe.

Vous pouvez affecter des rôles à des groupes externes Unica de la même manière que vous le faites pour les groupes internes.

Gestion des groupes et des sous-groupes internes

Vous pouvez définir un nombre illimité de groupes internes. De plus, un utilisateur interne ou externe peut devenir membre de plusieurs groupes et sous-groupes internes.

Un sous-groupe n'hérite pas des membres affectés à ses parents. En revanche, il hérite des rôles attribués à ses parents. Un groupe et ses sous-groupes appartiennent toujours à une partition.

Seuls les groupes internes peuvent être affectés à une partition et seul l'utilisateur platform_admin ou un autre compte qui possède le rôle PlatformAdminRole peut créer des groupes dans toutes les partitions d'un environnement à partitions multiples.

Partitions et gestion de la sécurité

Les partitions de Unica Campaign et les produits associés permettent de sécuriser les données associées à différents groupes d'utilisateurs. Grâce au partitionnement, la partition d'un utilisateur apparaît comme s'il s'agissait d'une instance d'exécution distincte de Unica Campaign, sans indiquer que d'autres partitions sont en cours d'exécution sur le même système. Cette section porte sur les considérations spéciales de gestion de la sécurité dans un environnement à plusieurs partitions.

Utilisateurs membres d'une partition

Vous affectez les utilisateurs à une partition en fonction de leur appartenance à un groupe. Vous affectez un groupe à une partition, puis affectez les utilisateurs à un groupe pour leur donner accès à une partition.

Un groupe ou sous-groupe peut être affecté à une seule partition et les groupes parents n'acquièrent pas les affectations de partition de leurs sous-groupes. Seul l'utilisateur platform_admin ou un autre compte possédant le rôle PlatformAdminRole peut affecter un groupe à une partition.

Il est conseillé de définir un utilisateur membre d'une seule partition.

A propos des rôles et des partitions

Un rôle existe toujours dans le cadre d'une partition. Dans un environnement à partition unique, tous les rôles sont automatiquement créés dans la partition par défaut, partition1. Dans un environnement à partitions multiples, un rôle est créé dans la partition de l'utilisateur qui l'a créé. L'utilisateur platform_admin et les comptes qui possèdent le rôle PlatformAdminRole constituent l'exception à cette règle, car ces comptes peuvent créer des rôles dans une partition.

Informations supplémentaires sur les partitions

Cette section fournit des instructions sur l'affectation d'un groupe à une partition et l'affectation des utilisateurs aux groupes. Pour obtenir des informations complètes sur la configuration des partitions, consultez la documentation d'installation de Unica Campaign.

Utilisateurs et rôles préconfigurés

Lorsque vous installez Unica pour la première fois, trois utilisateurs sont prédéfinis et affectés des rôles définis par le système dans Unica Platform et Unica Campaign, comme indiqué dans cette section.

Le mot de passe par défaut de ces comptes utilisateur internes est "password".

Compte utilisateur platform_admin

Le compte platform_admin user permet à un administrateur Unica de gérer la configuration du produit, les utilisateurs et les groupes dans toutes les partitions d'un environnement multipartition et d'utiliser toutes les fonctions Unica Platform (à l'exception de la génération de rapports qui dispose de ses propres rôles) sans filtrage par partition. Par défaut, ce compte dispose des rôles suivants dans Unica Platform.

- Dans la partition par défaut, partition1, de Unica Platform
    - AdminRole
    - UserRole
    - PlatformAdminRole

  Ces rôles permettent à l'utilisateur platform_admin d'exécuter toutes les tâches d'administration dans Unica Platform, à l'exception des fonctions de génération de rapport. Lorsque des partitions supplémentaires sont créées, l'utilisateur platform_admin peut accéder aux utilisateurs, groupes, rôles et à la configuration et les administrer dans les partitions supplémentaires.

  Le rôle PlatformAdminRole est unique, car aucun utilisateur ne peut modifier les droits d'accès de ce rôle et seul un utilisateur qui possède ce rôle peut affecter le rôle PlatformAdminRole à un autre utilisateur.
- Dans la partition par défaut, partition1, de Unica Campaign
    - Rôle d'administration de règles globales

  Ce rôle permet à l'utilisateur platform_admin d'effectuer toutes les tâches dans Unica Campaign.

Par défaut, cet utilisateur n'a pas accès aux produits Unica, à l'exception de Unica Platform et Unica Campaign.

Compte utilisateur asm_admin

Le compte utilisateur asm_admin permet à un administrateur Unica de gréer les utilisateurs et les groupes d'un environnement à une seule partition et d'utiliser toutes les fonctions Unica Platform (à l'exception de la génération de rapports qui dispose de ses propres rôles). Ce compte possède les rôles ci-après.

- Dans la partition par défaut, partition1, de Unica Platform
  - AdminRole
  - UserRole

  A l'exception des cas mentionnés ci-après, ces rôles permettent à l'utilisateur asm_admin d'exécuter toutes les tâches d'administration dans Unica Platform dans la partition de asm_admin, la partition 1 par défaut.

  Ces rôles permettent à cet utilisateur d'administrer la page de configuration, qui n'effectue aucun filtrage par partition au niveau des utilisateurs. C'est la raison pour laquelle, vous devez supprimer l'autorisation sur la page Administrer la configuration du rôle AdminRole dans Unica Platform et réserver les tâches de configuration à l'utilisateur platform_admin.

  Vous trouverez les exceptions ci-dessous.

  - Pour accéder aux fonctions de génération de rapports, vous devez autoriser le rôle Reports System.
  - Cet utilisateur ne peut pas affecter le rôle PlatformAdminRole à un utilisateur ou à un groupe.

Compte demo

Le compte demo possède les rôles suivants.

- Dans la partition par défaut, partition1, de Unica Platform
  - UserRole

Ce rôle permet à l'utilisateur demo d'afficher et de modifier ses attributs de compte dans la page Utilisateurs, mais pas de changer les rôles ou les partitions de son compte ni d'accéder aux autres fonctions contenues dans Unica Platform. Par défaut, cet utilisateur n'est pas autorisé à accéder aux produits d'Unica.

- Dans la partition par défaut, partition1, de Unica Campaign
    - Rôle de révision des règles globales

  Ce rôle permet à l'utilisateur demo de créer des signets et d'afficher les campagnes, sessions, offres, segments et productions de rapports dans Unica Campaign.

Privilèges d'administration inter-partitions

Dans un environnement à partitions multiples, au moins un compte utilisateur disposant du rôle PlatformAdminRole dans Unica Platform est obligatoire pour vous permettre d'administrer la sécurité des utilisateurs Unica dans toutes les partitions.

Le compte platform_admin est préconfiguré avec le rôle PlatformAdminRole. Le compte platform_admin est un compte de superutilisateur qui ne peut pas être supprimé ou désactivé via les fonctions Utilisateurs d'Unica. Toutefois, ce compte est soumis aux contraintes de mot de passe des autres utilisateurs. Par exemple, quelqu'un qui tente de se connecter en tant que platform_admin peut entrer un mot de passe incorrect N fois dans une ligne. Selon les règles de mot de passe en vigueur, le compte platform_admin peut être désactivé dans le système. Pour rétablir ce compte, vous devez effectuer l'une des opérations suivantes :

- Si un autre utilisateur possède le rôle PlatformAdminRole dans Unica Platform, connectez-vous en tant que cet utilisateur et réinitialisez le mot de passe de l'utilisateur platform_admin ou créez un autre compte doté du rôle PlatformAdminRole dans Unica Platform.
- Si un seul utilisateur possède le rôle PlatformAdminRole dans Unica Platform (par exemple, platform_admin) et que cet utilisateur est désactivé, vous pouvez créer un nouveau compte platform_admin à l'aide de l'utilitaire `restoreAccess` fourni avec Unica Platform.

Pour éviter toute situation qui nécessite de rétablir l'accès à PlatformAdminRole à l'aide de l'utilitaire `restoreAccess`, il est recommandé de créer plusieurs comptes dotés des privilèges PlatformAdminRole.

Ajout d'un groupe interne

Utilisez la procédure ci-dessous pour ajouter un groupe interne.

1. Cliquez sur **Paramètres > Groupes d'utilisateurs**.
2. Cliquez sur **Nouveau groupe** au-dessus de la liste **Hiérarchie du groupe**.
3. Renseignez les zones **Nom de groupe** et **Description**.

   Important : Ne donnez pas à un groupe le même nom qu'un rôle défini par le système. Par exemple, n'utilisez pas "Admin" pour nommer un groupe car il s'agit d'un nom de rôle utilisé dans Unica Campaign. Vous rencontrerez des problèmes lors des mises à niveau sinon.

4. Cliquez sur **Enregistrer les modifications**.

   Le nom du nouveau groupe apparaît dans la liste **Hiérarchie du groupe**.

Ajout d'un sous-groupe

Cette procédure permet d'ajouter un sous-groupe interne.

1. Cliquez sur **Paramètres > Groupes d'utilisateurs**.
2. Cliquez sur le nom du groupe auquel vous souhaitez ajouter un sous-groupe.
3. Cliquez sur **Nouveau sous-groupe**.
4. Renseignez les zones **Nom de groupe** et **Description**.

   Important : Ne donnez pas à un sous-groupe le même nom qu'un rôle défini par le système. Par exemple, n'utilisez pas "Admin" pour nommer un sous-groupe car il s'agit d'un nom de rôle utilisé dans Unica Campaign. Vous rencontrerez des problèmes lors des mises à niveau sinon.

5. Cliquez sur **Enregistrer les modifications**.

   Le nouveau sous-groupe apparaît dans le groupe approprié de la liste **Hiérarchie des groupes**.

   Conseil : Si l'icône du dossier du groupe parent est fermée, cliquez sur le signe plus (+) pour développer la liste.

Suppression d'un groupe ou d'un sous-groupe

N'oubliez pas que lorsque vous supprimez un groupe ou un sous-groupe, les rôles qui lui sont affectés sont retirés à ses membres. Les parents de ce groupe ou sous-groupe perdent également ces rôles, excepté s'ils leur ont été affectés explicitement.

1. Cliquez sur **Paramètres > Groupes d'utilisateurs**.
2. Cliquez sur le nom du groupe ou du sous-groupe à supprimer.

   Remarque : Pour sélectionner un sous-groupe lorsque l'icône du dossier du groupe parent est fermée, cliquez sur le signe "plus" (+) pour développer la liste.

3. Cliquez sur le bouton **Supprimer le groupe** dans la partie supérieure du panneau de droite.
4. Cliquez sur **OK**.

Changement de la description d'un groupe ou d'un sous-groupe

Utilisez la procédure ci-dessous pour changer la description d'un groupe ou d'un sous-groupe.

1. Cliquez sur **Paramètres > Groupes d'utilisateurs**.
2. Cliquez sur le nom du groupe ou du sous-groupe dont vous souhaitez changer la description.

Remarque : Pour sélectionner un sous-groupe lorsque l'icône du dossier du groupe parent est fermée, cliquez sur le signe "plus" (+) pour développer la liste.

3. Cliquez sur **Editer les propriétés**.
4. Apportez les éditions souhaitées à la description.
5. Cliquez sur **Enregistrer les changements** pour enregistrer vos modifications.
6. Cliquez sur **OK**.

Affectation d'un groupe à une partition

Cette procédure est nécessaire uniquement si plusieurs partitions sont configurées pour Unica Campaign. Seul un compte ayant le rôle PlatformAdminRole, tel que l'utilisateur platform_admin, peut effectuer cette tâche.

1. Identifiez les groupes à affecter à chaque partition. Si nécessaire, créez des groupes.
2. Cliquez sur **Paramètres > Groupes d'utilisateurs**.
3. Cliquez sur le nom du groupe ou du sous-groupe à affecter à une partition.
4. Cliquez sur **Editer les propriétés**.
5. Sélectionnez la partition souhaitée dans la liste déroulante **ID de partition.**

   Cette zone est disponible uniquement si plusieurs partitions sont configurées.
6. Cliquez sur **Enregistrer les changements** pour enregistrer vos modifications.
7. Cliquez sur **OK**.

Ajout d'un utilisateur à un groupe ou un sous-groupe

Utilisez la procédure ci-dessous pour ajouter un utilisateur à un groupe ou un sous-groupe.

1. Cliquez sur **Paramètres > Utilisateurs**.

Remarque : Vous pouvez effectuer la même opération sur la page **Groupes d'utilisateurs** en cliquant sur le nom du groupe, puis sur **Editer utilisateurs**.

2. Cliquez sur le nom d'utilisateur à changer.
3. Cliquez sur le lien **Editer les groupes** au bas de la page.
4. Cliquez sur le nom d'un groupe dans la case **Groupes disponibles** pour le sélectionner.
5. Cliquez sur le bouton **Ajouter.**

   Le nom du groupe se déplace vers la zone **Groupes.**
6. Cliquez sur **Enregistrer les changements** pour enregistrer vos modifications.
7. Cliquez sur **OK**.

   Les informations du compte utilisateur s'affichent avec le groupe ou le sous-groupe que vous avez affecté.

Suppression d'un utilisateur d'un groupe ou d'un sous-groupe

Utilisez la procédure ci-dessous pour supprimer un utilisateur d'un groupe ou d'un sous-groupe.

Important : La suppression d'un utilisateur d'un groupe ou d'un sous-groupe supprime également les rôles affectés à ce groupe ou sous-groupe pour l'utilisateur.

1. Cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur le nom d'utilisateur à changer.
3. Cliquez sur le lien **Editer les groupes** au bas de la page.
4. Cliquez sur le nom d'un groupe dans la case **Groupes** pour le sélectionner.
5. Cliquez sur le bouton **Supprimer**.

   Le nom du groupe passe dans la zone **Groupes disponibles**.
6. Cliquez sur **Enregistrer les changements** pour enregistrer vos modifications.
7. Cliquez sur **OK**.
8. Cliquez sur le lien **Editer les propriétés** au bas de la page.
9. Apportez les changements nécessaires au nom ou à la description.
10. Cliquez sur **Enregistrer les changements** pour enregistrer vos modifications.
11. Cliquez sur **OK**.

Pages de gestion des groupes d'utilisateurs

Il s'agit des zones que vous utilisez pour configurer des groupes d'utilisateurs.

Zones des pages Nouveau groupe, Nouveau sous-groupe, Editer les propriétés

Tableau 7. Zones des pages Nouveau groupe, Nouveau sous-groupe, Editer les propriétés

Zone	Description
Nom du groupe	Nom du groupe. 64 caractères maximum. Vous pouvez utiliser les caractères suivants lorsque vous créez un nom de groupe. • Caractères alphabétiques en majuscules et minuscules (A-Z) • Nombres (0-9) • Guillemet simple (') • Tiret (-) • Souligné (_) • Signe arobase (@) • Barre oblique droite (/) • Parenthèse • Deux points (:) • Point-virgule (;) • Espace (excepté comme premier caractère) • Caractères codés sur deux octets (caractères chinois alphanumériques par exemple) Ne donnez pas à un groupe ou un sous-groupe le même nom qu'un rôle défini par le système. Par exemple, n'utilisez pas "Admin" pour nommer un groupe car il s'agit d'un nom de rôle utili-

Tableau 7. Zones des pages Nouveau groupe, Nouveau sous-groupe, Editer les propriétés (suite)

Zone	Description
	sé dans Unica Campaign. Vous rencontrerez des problèmes lors des mises à niveau sinon. Les noms Unica conservent la casse pour l'affichage, mais ne la conservent pas pour la comparaison et la création (par exemple, vous ne pouvez pas créer deux noms de groupes Admin et admin). Si vous créez un sous-groupe, il convient de donner à votre sous-groupe un nom associé à son groupe parent.
Description	Description du groupe. 256 caractères maximum. Il est utile d'inclure les rôles que vous envisagez d'attribuer au groupe ou au sous-groupe dans la description. Vous pouvez ainsi consulter en un coup d'œil les rôles et les utilisateurs dans la page de détails du groupe.
ID partition	Disponible uniquement si plusieurs partitions sont configurées. Si vous affectez une partition à un groupe, les membres de ce groupe sont des membres de cette partition. Un utilisateur ne peut être membre que d'une partition.

Zones des pages Editer les utilisateurs et Editer les rôles

Tableau 8. Zones des pages Editer les utilisateurs et Editer les rôles

Zone	Description
Groupes disponibles ou Rôles disponibles	Liste de groupes et de sous groupes ou de rôles auxquels l'utilisateur n'est pas affecté.

Tableau 8. Zones des pages Editer les utilisateurs et Editer les rôles (suite)

Zone	Description
Groupes ou Rôles	Liste de groupes et de sous groupes ou de rôles auxquels l'utilisateur est affecté

Création d'un rôle

Vous ne devez créer des rôles que pour les produits dotés de droits d'accès détaillés. La fonction de génération de rapport et certains produits Unica ne possèdent que des droits d'accès de base ; il n'est donc pas nécessaire de créer d'autres rôles pour ces produits.

1. Cliquez sur **Paramètres > Rôles et droits d'accès utilisateur**.
2. Cliquez sur le signe plus en regard du nom de produit dans la liste de gauche, puis cliquez sur le nom de la partition dans laquelle vous souhaitez créer le rôle.
3. Pour Unica Campaign uniquement, si vous souhaitez créer un rôle dans la stratégie globale, cliquez sur Stratégie globale.
4. Cliquez sur **Ajout de rôles et affectation de droits d'accès** .
5. Cliquez sur **Ajouter un rôle.**
6. Saisissez le nom et la description du rôle.
7. Cliquez sur **Enregistrer les modifications** pour enregistrer le rôle ou sur **Enregistrer et éditer les droits d'accès** pour accéder à la page Autorisations afin d'ajouter ou de modifier des droits pour les rôles de la liste.

Modification des droits des rôles

Cette procédure permet de modifier les droits des rôles.

1. Cliquez sur **Paramètres > Rôles et droits d'accès utilisateur**.
2. Cliquez sur le signe plus en regard d'un produit dans la liste de gauche, puis cliquez sur le nom de la partition dans laquelle vous souhaitez modifier un rôle.
3. Pour Unica Campaign uniquement, si vous souhaitez créer un rôle dans la stratégie globale ou une stratégie personnalisée, cliquez sur le nom de la stratégie.
4. Cliquez sur **Ajout de rôles et affectation de droits d'accès** .

5. Cliquez sur **Enregistrer et éditer les droits d'accès**.
6. Cliquez sur le signe plus en regard d'un groupe de rôles pour afficher tous les droits disponibles ainsi que l'état de ces droits dans chaque rôle.
7. Dans la colonne du rôle à modifier, sélectionnez la case à cocher des lignes de droits pour définir le droit sur Autorisé, Refusé ou Non autorisé.
8. Cliquez sur **Enregistrer les changements** pour enregistrer vos modifications.

   Vous pouvez cliquer sur **Restaurer** pour annuler les modifications effectuées depuis le dernier enregistrement et rester sur la page Droits d'accès ou sur **Annuler** pour ignorer les modifications apportées depuis le dernier enregistrement et revenir à la page de la partition ou de la stratégie.

Suppression d'un rôle du système

Cette procédure permet de supprimer un rôle d'Unica.

Important : Si vous supprimez un rôle, il est retiré à tous les utilisateurs et groupes auxquels il était affecté.

1. Cliquez sur **Paramètres > Rôles et droits d'accès utilisateur**.
2. Cliquez sur le signe plus en regard d'un produit dans la liste de gauche, puis cliquez sur le nom de la partition dans laquelle vous souhaitez créer le rôle.
3. Pour Unica Campaign uniquement, si vous souhaitez créer un rôle dans la stratégie globale, cliquez sur Stratégie globale.
4. Cliquez sur **Ajout de rôles et affectation de droits d'accès** .
5. Cliquez sur le lien **Supprimer** du rôle à supprimer.
6. Cliquez sur **Enregistrer les modifications**.

Affectation d'un rôle à un groupe ou suppression du rôle du groupe

Si vous affectez ou retirez un rôle à un groupe, les membres de ce groupe et acquièrent ou perdent ce rôle.

1. Cliquez sur **Paramètres > Groupes d'utilisateurs**.
2. Cliquez sur le nom du groupe concerné.
3. Cliquez sur **Affecter des rôles**.

   Les rôles qui ne sont pas affectés au groupe apparaissent dans la zone **Rôles disponibles** sur la gauche. Les rôles qui sont actuellement affectés au groupe apparaissent dans la zone **Rôles** sur la droite.
4. Cliquez sur le nom d'un rôle dans la zone Rôles disponibles pour le sélectionner.
5. Cliquez sur **Ajouter** ou **Supprimer** pour déplacer un rôle d'une zone à une autre.
6. Cliquez sur **Enregistrer les changements** pour enregistrer vos modifications.
7. Cliquez sur **OK**.

Affectation d'un rôle à un utilisateur ou suppression du rôle de l'utilisateur

Utilisez la fenêtre **Editer des rôles** pour affecter ou retirer un rôle à un utilisateur.

Effectuez les tâches suivantes pour affecter ou retirer un rôle à un utilisateur :

1. Cliquez sur **Paramètres > Utilisateurs**.
2. Cliquez sur le nom du compte utilisateur concerné.
3. Cliquez sur **Editer les rôles**.

   Les rôles qui ne sont pas affectés à l'utilisateur apparaissent dans la zone **Rôles disponibles** sur la gauche. Les rôles qui sont actuellement affectés à l'utilisateur apparaissent dans la zone **Rôles sélectionnés** sur la droite.
4. Sélectionnez un rôle dans la zone **Rôles disponibles**. Exécutez l'une des tâches suivantes :
   - Pour affecter un rôle à un utilisateur, sélectionnez un rôle dans la liste **Rôles disponibles** et cliquez sur **Ajouter**.
   - Pour retirer un rôle à un utilisateur, sélectionnez un rôle dans la liste **Rôles sélectionnés** et cliquez sur **Supprimer**.
5. Cliquez sur **Enregistrer les modifications**, puis cliquez sur **OK**.

Définition des états des droits d'accès

Pour chaque rôle, vous pouvez spécifier les droits d'accès accordés, non accordés ou refusés. Vous définissez ces droits d'accès sur la page **Paramètres > Rôles utilisateur et autorisations**.

Les états qui suivent ont les significations indiquées :

- **Accordé** - signalé par une coche . Autorise de façon explicite l'exécution de cette fonction particulière tant qu'aucun autre rôle de l'utilisateur ne refuse explicitement le droit d'accès.
- **Refusé** - signalé par un "X" . Refuse de façon explicite l'exécution de cette fonction particulière, sans tenir compte d'autres rôles de l'utilisateur susceptibles d'autoriser le droit d'accès.
- **Non accordé** : signalé par un cercle . N'autorise, ni ne refuse de façon explicite l'exécution d'une fonction particulière. Si le droit d'accès n'est pas accordé de façon explicite par l'un des rôles de l'utilisateur, l'utilisateur n'est pas autorisé à exécuter cette fonction.

Droits d'accès pour les produits n'utilisant que les rôles de base

La table suivante décrit les définitions fonctionnelles des rôles disponibles pour les produits d'Unica qui n'utilisent que les rôles de base. Pour en savoir plus, consultez la documentation du produit.

Tableau 9. Droits d'accès pour les produits n'utilisant que les rôles de base

Application	Rôles
Leads	Les rôles Leads sont réservés pour usage ultérieur.

Tableau 9. Droits d'accès pour les produits n'utilisant que les rôles de base (suite)

Application	Rôles
Rapports	• ReportsSystem - accorde le droit d'accès `report_system`, qui vous permet d'accéder aux options **Générateur SQL de rapports** et **Synchroniser les droits d'accès au dossier des rapports** du menu **Paramètres.** • ReportsUser - accorde le droit d'accès `report_user`, qui est utilisé par Authentication Provider, installé uniquement sur le système IBM® Cognos® 11 BI. Pour plus d'informations sur les options d'authentification de l'intégration IBM® Cognos® 11 BI et sur l'utilisation des autorisations de génération de rapports par Authentication Provider, voir le document Cognos Reports - Guide d'installation et de configuration.
Unica Deliver	• Deliver_Admin - accès complet à toutes les fonctionnalités. • Deliver_User - Réservé pour une utilisation future. Les stratégies de sécurité de Unica Campaign permettent de définir l'accès plus en détail. Pour plus d'informations, voir le Guide de démarrage et le Guide d'administration d'Unica Deliver.
Unica Interact	• InteractAdminRole - accès complet à toutes les fonctionnalités.
Unica Collaborate	• collab_admin - accès complet à toutes les fonctionnalités. • corporate – peut utiliser Unica Campaign et Unica Collaborate pour développer des listes réutilisables et des mo-

Tableau 9. Droits d'accès pour les produits n'utilisant que les rôles de base (suite)

Application	Rôles
	dèles de campagne à la demande. Possibilité de créer et d'exécuter des campagnes nationales. • field – peut participer aux campagnes nationales et créer et exécuter des listes et des campagnes à la demande dans Unica Collaborate.
Unica Plan	• PlanUserRole – par défaut, les utilisateurs qui possèdent ce rôle disposent d'un droit d'accès réduit à Unica Plan. Ils ne peuvent pas créer de plans, de programmes ou de projets et ont un accès limité aux paramètres d'administration. • PlanAdminRole – par défaut, les utilisateurs qui possèdent le rôle PlanAdminRole disposent d'un droit d'accès étendu à Unica Plan, notamment l'accès à tous les paramètres d'administration et de configuration, qui donnent droit à de nombreux accès. Les stratégies de sécurité de Unica Plan permettent de définir l'accès plus en détail.
Unica Journey	• JourneyAdmin : Les utilisateurs ont accès à tous les paramètres d’administration et de configuration, ce qui permet un large éventail d’accès. • JourneyUser : Les utilisateurs ont un accès limité aux paramètres d'administration et de configuration. Ils peuvent uniquement afficher les paramètres, mais ne peuvent pas effectuer d’opérations brutes sur eux.
Unica Centralized-Offer Management	OfferAdmin : Les utilisateurs ont accès à tous les paramètres d’administration et de configuration, ce qui permet un large éventail d’accès.

Tableau 9. Droits d'accès pour les produits n'utilisant que les rôles de base (suite)

Application	Rôles
	OfferUser : Les utilisateurs ont un accès limité aux paramètres d'administration et de configuration.
IBM SPSS Modeler Advantage Enterprise Marketing Management Edition	• SPSSUser – Les utilisateurs avec le rôle SPSSUser peuvent effectuer les actions suivantes : ◦ Exécuter des rapports ◦ Afficher des éléments dans leur référentiel de contenu ◦ Effectuer une évaluation • SPSSAdmin – Les utilisateurs qui possèdent le rôle SPSSAdmin ont tous les droits activés dans IBM SPSS Modeler Advantage Enterprise Marketing Management Edition, notamment l'accès à tous les paramètres d'administration et de configuration.

Droits d'accès pour Unica Platform

Le tableau ci-dessous décrit les droits d'accès que vous pouvez affecter aux rôles dans Unica Platform.

Tableau 10. Autorisation de l'Unica Platform

Autorisation	Description
Page d'administration des utilisateurs	Permet à un utilisateur d'effectuer toutes les tâches d'administration utilisateur sur la page Utilisateurs pour les comptes utilisateur de sa propre partition : ajouter et supprimer des comptes utilisateur internes, et modifier des attributs, des sources de données et des affectations de rôle
Accès à la page Utilisateurs	Permet à un utilisateur d'afficher la page Utilisateur.

Tableau 10. Autorisation de l'Unica Platform (suite)

Autorisation	Description
Page d'administration des groupes d'utilisateurs	Permet à un utilisateur d'effectuer toutes les actions sur la page Groupes d'utilisateurs, à l'exception de l'affectation d'une partition à un groupe, qui ne peut être effectuée que par l'utilisateur platform_admin. Ce droit d'accès permet à un utilisateur de créer, de modifier et de supprimer des groupes, de gérer une appartenance à un groupe et d'affecter des rôles à des groupes.
Page d'administration des rôles des utilisateurs	Permet à un utilisateur d'exécuter toutes les actions de la page Rôles d'utilisateur et Autorisations : créer, modifier et supprimer des rôles dans Unica Platform et Unica Campaign et affecter des rôles aux utilisateurs pour tous les produits Unica.
Administration de la page de configuration	Permet à un utilisateur d'exécuter toutes les actions sur la page de configuration : modifier les valeurs d'une propriété, créer de nouvelles catégories d'après des modèles, et supprimer des catégories associées au lien **Supprimer catégorie**.
Administration de la page Filtres de données	Permet à un utilisateur d'effectuer toutes les actions dans la page Filtres de données : attribuer et supprimer des affectations de filtres de données.
Administration de la page Tâches programmées	Permet à un utilisateur d'exécuter toutes les actions sur la page de gestion de la planification : afficher et modifier des définitions de planification et afficher les exécutions.
Administration des tableaux de bord	Permet à un utilisateur d'exécuter toutes les actions sur la page de configuration : créer, afficher, modifier et supprimer les tableaux de bord, affecter les administrateurs de tableaux de bord et administrer l'accès aux tableaux de bord.

Droits d'accès pour Opportunity Detect

Le tableau suivant décrit les droits que vous pouvez affecter aux rôles dans Opportunity Detect.

Tous les droits dont le statut est **Non accordé** sont traités comme **Refusés**.

Tableau 11. Droits dans Opportunity Detect

Autorisation	Description
Affichage uniquement	Permet d'accéder à toutes les interfaces utilisateur, en mode lecture seule.
Concevoir des déclencheurs	• Permet de créer des espaces de travail et de concevoir des systèmes de déclencheurs. • Permet de créer, modifier et supprimer toutes les ressources associées aux déclencheurs. • Permet d'accéder aux pages d'espace de travail, de composant, de niveau d'audience, de source de données, de liste de valeurs nommées. • Ne permet pas d'accéder à la page Groupes des serveurs ou à l'onglet Déploiement d'un espace de travail. • Ne permet pas de stopper une exécution par lots. • Ne permet pas d'administrer des objets créés par le service Web lorsque Opportunity Detect est intégré à Unica Interact.

Tableau 11. Droits dans Opportunity Detect (suite)

Autorisation	Description
Exécuter en mode test	• Déployer des configurations de déploiement et exécutez des configurations de déploiement par lots sur les groupes de serveurs non destinés à la production. • Permet d'accéder à la page Groupe de serveurs et à l'onglet Déploiement, mais ne permet de concevoir un groupe de serveurs pour la production. • Ne permet pas de déployer des configurations de déploiement ou d'exécuter des configurations de déploiement qui utilisent un groupe de serveurs de production.
Exécuter en mode production	• Déployer des configurations de déploiement et exécuter des configurations de déploiement par lots sur le groupe de serveurs de votre choix. • Effectuer toutes les actions de la page Groupe de serveurs et des onglets Déploiement et Exécution par lots d'un espace de travail et en particulier concevoir un groupe de serveurs pour la production.
Administrer en temps réel	Gérer des objets que le service Web crée lorsque Opportunity Detect est intégré à Unica Interact pour permettre le mode en temps réel. Permet les actions suivantes. • Supprimer des espaces de travail et des composants créés par le service Web. • Démarrer et arrêter les configurations de déploiement en temps réel et mettre à jour leur niveau de journalisation. L'utilisateur disposant uniquement de ce droit ne peut pas commencer d'exécution pour les configurations de déploiement en temps réel.

Tableau 11. Droits dans Opportunity Detect (suite)

Autorisation	Description
	Aucun utilisateur, y compris disposant de ce droit, ne peut effectuer les actions suivantes. • Supprimer et mettre à jour les niveaux d'audience, les sources de données, les listes de valeurs nommées, les groupes de serveurs ou les configurations de déploiement créées par le service Web. • Créer et déployer des configurations de déploiement créées par le service Web.

Gestion de la configuration

Lorsque vous installez Unica pour la première fois, la page Configuration contient uniquement les propriétés utilisées pour configurer Unica Platform, ainsi que certaines propriétés de configuration globales. Lorsque vous installez des applications supplémentaires Unica, les propriétés utilisées pour configurer ces applications sont enregistrées dans Unica Platform. Ces propriétés sont ensuite affichées sur la page de configuration, à partir de laquelle vous pouvez définir ou modifier leurs valeurs.

Il se peut que certaines applications disposent de propriétés de configuration supplémentaires non stockées dans le référentiel central. Consultez la documentation des applications pour en savoir plus sur toutes les options de configuration de chaque application.

Catégories de propriétés

Les catégories **Rapports**, **Général** et **Unica Platform** sont présentes lorsque Unica Platform est installé pour la première fois. Ces catégories contiennent des propriétés qui s'appliquent à toutes les applications Unica installées dans une suite.

- Propriété des paramètres régionaux par défaut
- Catégorie **Sécurité** et les sous-catégories qui comportent des propriétés qui spécifient des modes de connexion et des paramètres spécifiques à chaque mode.
- Paramètres de mot de passe
- Propriétés qui configurent les filtres de données
- Propriétés qui configurent les planifications
- Propriétés qui configurent la fonction de génération de rapports
- Propriétés qui configurent la façon dont les alertes sont gérées

En fonction des applications d'Unica installées, des catégories supplémentaires peuvent contenir des propriétés et sous-catégories spécifiques à une application. Par exemple, après l'installation de Unica Campaign, la catégorie **Campaign** contient des propriétés et des sous-catégories liées à Unica Campaign.

Types de catégorie

Une catégorie peut correspondre à l'un des trois types identifiés par des icônes différentes.

Tableau 12. Icônes de types de catégorie

Type de catégorie	Icône
Catégories qui ne contiennent aucune propriété configurable	
Catégories qui contiennent des propriétés configurables	
Catégories de modèle que vous pouvez utiliser pour créer une catégorie Les noms de catégories de modèle sont en italiques et sont placés entre parenthèses.	

Modèles permettant de dupliquer des catégories

Les propriétés d'une application Unica sont enregistrées dans Unica Platform lors de l'installation de l'application. Lorsqu'une application requiert que les utilisateurs créent des catégories en double à des fins de configuration, un modèle de catégorie est fourni.

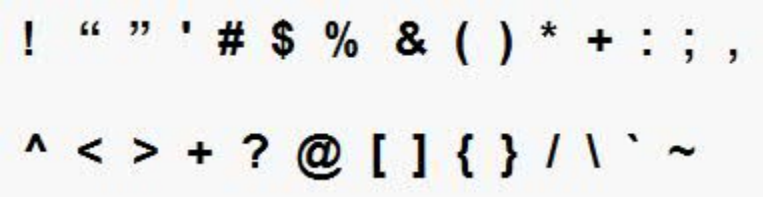
Pour créer une catégorie, dupliquez le modèle. Par exemple, vous pouvez créer une nouvelle partition de Unica Campaign ou une source de données en dupliquant le modèle approprié.

Toute catégorie que vous créez à partir d'un modèle peut être supprimée.

Restrictions de dénomination des catégories

Les restrictions suivantes s'appliquent lorsque vous nommez une catégorie créée à partir d'un modèle :

- Le nom doit être unique parmi les catégories liées dans l'arborescence (c'est-à-dire les catégories qui partagent une même catégorie parent).
- Les caractères suivants ne sont pas autorisés dans les noms de catégorie :



En outre, le nom ne peut pas commencer par un point.

Descriptions des propriétés

Vous pouvez naviguer vers la description d'une propriété de deux façons :

- Cliquez sur **Aide > Aide pour cette page** pour lancer l'aide en ligne et afficher une rubrique qui décrit toutes les propriétés pour la page que vous visualisez.
- Cliquez sur **Aide > Documentation sur le produit** pour lancer une page qui vous donne accès à la documentation de tous les produits au format PDF ou en ligne. Toutes les descriptions de propriétés sont incluses sous forme d'annexe dans Unica Platform - Guide d'administration.

Fonction d'actualisation

Un bouton d'actualisation  situé dans la partie supérieure de l'arborescence de navigation de configuration offre les fonctions suivantes.

- Il actualise le contenu de l'arborescence, ce qui se révèle utile lorsque vous souhaitez obtenir les informations les plus récentes concernant des paramètres de configuration. Il se peut que ces paramètres aient été mis à jour pendant que vous consultiez l'arborescence (par exemple, lorsqu'une application a été enregistrée ou désenregistrée ou lorsque un tiers a mis à jour les paramètres).
- Il rétablit l'arborescence de navigation dans l'état dans lequel elle se trouvait lorsque vous avez sélectionné un nœud pour la dernière fois, en la réduisant ou la développant.

Important : Si vous êtes en mode édition lorsque vous cliquez sur **Actualiser**, la page passe en mode de lecture. Les changements non enregistrés sont perdus.

Préférences de paramètres régionaux par défaut d'un utilisateur

Unica Platform contient un attribut d'environnement régional par défaut qui s'applique à toutes les applications Unica qui l'implémentent.

Vous pouvez définir cet attribut par défaut en définissant la valeur de la propriété **Paramètre régional** de la catégorie **Platform**.

Pour en savoir plus sur cette propriété, consultez l'aide en ligne dans la zone Configuration ou le document Unica Platform - Guide d'administration. Pour savoir si une application Unica implémente cet attribut, consultez la documentation de cette application.

En outre, vous pouvez remplacer ces valeurs par défaut pour chaque utilisateur en modifiant la valeur de la propriété dans le compte de l'utilisateur.

Accès à une catégorie

Utilisez la procédure ci-dessous pour accéder à une catégorie dans la page Configuration.

1. Connectez-vous à Unica.
2. Cliquez sur **Paramètres > Configuration** dans la barre d'outils.

   La page de configuration affiche l'arborescence des catégories de configuration.
3. Sous la catégorie souhaitée, cliquez sur le signe plus.

   La catégorie s'ouvre et affiche des sous-catégories. Si la catégorie contient des propriétés, celles-ci sont répertoriées avec leurs valeurs actuelles.

   Les noms internes des catégories s'affichent sous le titre de la page. Utilisez ces noms internes pour importer ou exporter manuellement des catégories et leurs propriétés en utilisant l'utilitaire `configTool`.
4. Continuez de développer les catégories et les sous-catégories jusqu'à ce que la propriété que vous souhaitez modifier s'affiche.

Edition des valeurs des propriétés

Utilisez la procédure ci-dessous pour modifier une valeur de propriété dans la page Configuration.

1. Accédez à la catégorie contenant la propriété à définir.

   La page des paramètres de la catégorie affiche une liste de toutes les propriétés de la catégorie ainsi que de leurs valeurs actuelles.
2. Cliquez sur **Editer paramètres**.

La page d'édition des paramètres de la catégorie affiche les valeurs de propriété dans des zones modifiables.

3. Entrez ou éditez les valeurs, selon vos besoins.

   Dans UNIX™, tous les noms de fichier et de répertoire sont sensibles à la casse. La casse d'un nom de fichier ou de dossier que vous entrez doit correspondre à celle du nom de fichier ou dossier sur la machine UNIX™.
4. Cliquez sur **Enregistrer les changements** pour enregistrer vos modifications ou sur **Annuler** pour quitter la page sans effectuer d'enregistrement.

Création d'une catégorie depuis un modèle

Utilisez la procédure ci-dessous pour créer une catégorie depuis un modèle dans la page Configuration.

1. Sur la page Configuration, naviguez vers la catégorie du modèle que vous souhaitez dupliquer.

   Contrairement aux autres catégories, les libellés de catégorie de modèle sont en italique, entre parenthèses.
2. Cliquez sur la catégorie du modèle.
3. Saisissez un nom dans la zone **Nom de la nouvelle catégorie** (obligatoire).
4. Vous pouvez éditer les propriétés dans la nouvelle catégorie maintenant ou ultérieurement.
5. Cliquez sur **Enregistrer les changements** pour enregistrer la nouvelle configuration.

La nouvelle catégorie s'affiche dans l'arborescence.

Suppression d'une catégorie

Utilisez la procédure ci-dessous pour supprimer une catégorie dans la page Configuration.

Sur la page Configuration, certaines catégories peuvent être supprimées, d'autres non. Toute catégorie que vous créez à partir d'un modèle peut être supprimée. De plus, lorsqu'un

produit Unica est enregistré, son ensemble de catégories peut inclure des catégories qui peuvent être supprimées.

1. Sur la page Configuration, accédez à la catégorie à supprimer et cliquez pour la sélectionner et ouvrir la page Paramètres.

   Si la catégorie que vous avez sélectionnée peut être supprimée, vous voyez apparaître un lien **Supprimer une catégorie**.
2. Cliquez sur le lien **Supprimer une catégorie**.

   Le message Voulez-vous vraiment supprimer "category name" ? s'affiche.
3. Cliquez sur **OK**.

La catégorie n'apparaît plus dans l'arborescence.

Gestion des tableaux de bord

Les tableaux de bord sont des pages que vous pouvez configurer pour y inclure des informations utiles aux groupes d'utilisateurs qui remplissent différents rôles dans votre société. Les composants des tableaux de bord sont appelés des portlets. Les tableaux de bord peuvent contenir des portlets prédéfinis ou des portlets créés par les utilisateurs.

Vous pouvez créer et configurer vous-mêmes vos tableaux de bord ou utiliser des tableaux de bord préassemblés. Les tableaux de bord préassemblés contiennent des portlets prédéfinis combinés de manière à pouvoir remplir différents rôles dans votre organisation.

Vous pouvez également créer des portlets personnalisés à partir des pages de produit Unica présentes sur l'intranet de votre société ou de pages disponibles sur Internet.

Planification des tableaux de bord

Pour planifier la manière dont votre organisation utilise les tableaux de bord, convenez des points suivants avec votre équipe de gestion marketing.

- De quels tableaux de bord vos utilisateurs ont besoin.
- Quels utilisateurs ont accès à quels tableaux de bord.
- Quels portlets doivent être inclus dans chaque tableau de bord.

- Qui doit être l'administrateur de chaque tableau de bord après l'agrégation des tableaux de bord. L'administrateur du tableau de bord gère l'accès utilisateur au tableau de bord et peut modifier le contenu et la disposition de chaque tableau de bord.

Audiences de tableau de bord

Vous pouvez contrôler qui visualise vos tableaux de bord en les associant à des groupes ou en leur affectant des utilisateurs individuels. Les membres d'un groupe peuvent accéder au(x) tableau(s) de bord associé(s) à ce groupe, tandis que les non-membres ne peuvent pas visualiser ces tableaux de bord.

Vous pouvez également créer un ou plusieurs tableaux de bord globaux, qui peuvent être visualisés par tous les utilisateurs Unica dans une partition, indépendamment de leur appartenance à un groupe ou des affectations individuelles.

Lors de la création d'un tableau de bord global, vous devez inclure des portlets susceptibles d'intéresser le plus d'utilisateurs possible. Par exemple, si vous installez Unica Campaign, vous pouvez installer le portlet Mes Signets personnalisés, l'un des portlets prédéfinis d'Unica.

Droits d'accès utilisateur nécessaires pour afficher les tableaux de bord

Les tableaux de bord permettent aux utilisateurs Unica de consulter des pages issues de plusieurs produits (notamment de Unica Plan et de Unica Campaign) à partir d'une seule page et ce quels que soient les droits d'accès dont ces utilisateurs disposent dans ces produits.

Certains portlets de tableau de bord permettent aux utilisateurs de travailler dans un produit Unica en cliquant sur un lien dans un portlet pour ouvrir une page sur laquelle ils peuvent travailler. Si l'utilisateur ne dispose pas des droits d'accès appropriés, la page ne s'affiche pas.

Certains éléments de contenu des portlets sont filtrés en fonction de l'utilisateur. Par exemple, si un utilisateur ne se sert jamais directement des campagnes, le portlet Mes campagnes récentes peut n'afficher aucun lien.

Portlets prédéfinis

Unica fournit deux types de portlets de tableau de bord prédéfinis que vous pouvez activer, puis ajouter à un tableau de bord que vous créez.

Les portlets prédéfinis Unica utilisent le mécanisme de connexion unique Unica Platform pour accéder au contenu d'Unica. Les utilisateurs ne sont pas invités à entrer leurs données d'identification lorsqu'ils consultent un tableau de bord contenant ces portlets.

- Liste : une liste d'objets d'Unica spécifiques à l'utilisateur. Mes campagnes récentes (Unica Campaign), Mes alertes (Unica Plan et l'état récapitulatif des continents (Digital Analytics for On Premises) sont des exemples de portlet de liste.
- IBM® Cognos® ou des rapports Unica Insights : Une version spécialement formatée des rapports Unica.

Vous pouvez également créer vos propres portlets de tableau de bord personnalisés.

Disponibilité des portlets prédéfinis

Unica fournit des portlets prédéfinis avec un grand nombre de ses produits. La disponibilité des portlets prédéfinis dépend des produits Unica que vous avez installés. En outre, les portlets de rapports sont disponibles uniquement lorsque la fonction de génération de rapport de Unica Insights ou IBM Cognos est implémentée.

Vous devez activer les portlets prédéfinis dans Unica Platform pour pouvoir les utiliser dans un tableau de bord. Les portlets Unica sont listés dans Unica Platform, que le produit auquel ils appartiennent soit installé ou non. Il est recommandé de n'activer que les portlets qui font partie de produits installés. Seuls les portlets activés apparaissent dans la liste des portlets que vous pouvez ajouter à un tableau de bord.

Portlets de rapport Unica Plan

La table suivante décrit les portlets de tableau de bord Unica Plan qui sont disponibles après l'installation d'Unica Insights ou du groupe de rapports Cognos Unica Plan.

Tableau 13. Portlets de rapport Unica Plan standard

Rapport	Description
Budget par type de projet	Cet exemple de rapport montre un diagramme à secteurs en 3D des budgets par type de projet pour l'année calendaire en cours. Ce rapport requiert le module de gestion financière.
Projets terminés par trimestre	Cet exemple de rapport montre un graphique à barres 3D des projets terminés avant l'échéance, à l'échéance ou en retard pour le trimestre en cours.
Prévision par type de projet	Cet exemple de rapport montre un diagramme à secteurs en 3D des dépenses prévisionnelles par type de projet pour l'année calendaire en cours.
Récapitulatif des approbations du chef d'équipe	Cet exemple de rapport montre des données sur les approbations actives et terminées pour tous les projets en cours répertoriés dans le système.
Récapitulatif des tâches du chef d'équipe	Cet exemple de rapport montre des données sur les tâches actives et terminées pour tous les projets en cours.
Position financière marketing	Cet exemple de rapport montre un échéancier avec les montants budgétés, prévisionnels, engagés et réels pour tous les plans quel qu'en soit l'état pour l'année calendaire en cours. Ce rapport requiert le module de gestion financière.
Récapitulatif de mes tâches	Cet exemple de rapport montre des données sur toutes les tâches actives et terminées associées à l'utilisateur pour tous les projets en cours.
Récapitulatif de mes approbations	Cet exemple de rapport montre des données sur les approbations actives et terminées associées à l'utilisateur pour tous les projets en cours.

Tableau 13. Portlets de rapport Unica Plan standard (suite)

Rapport	Description
Projets par type de projet	Cet exemple de rapport montre un graphique sectoriel de tous les projets en cours répertoriés dans le système par type de modèle.
Projets par statut	Cet exemple de rapport montre un graphique à barres 3D de tous les projets en cours par état : brouillon, en cours, en attente, annulé et terminé.
Projets demandés et terminés	Cet exemple de rapport montre un diagramme de calendrier des demandes de projet et des projets terminés par mois. Ce rapport compte uniquement les demandes de projet avec les états suivants Soumis, Accepté ou Renvoyé.
Dépense par type de projet	Cet exemple de rapport montre un diagramme à secteurs en 3D des dépenses réelles par type de projet pour l'année calendaire en cours. Ce rapport requiert le module de gestion financière.

Portlets de liste Unica Plan

Si le package de rapports de Unica Plan n'est pas installé, vous avez toujours accès aux portlets de liste Unica Plan disponibles sur votre tableau de bord.

Votre administrateur système sélectionne les portlets que les membres de votre organisation peuvent ajouter au tableau de bord. Pour gérer vos tableaux de bord et y ajouter des portlets, sélectionnez **Tableau de bord > Créer un tableau de bord**.

Tableau 14. Portlets de liste standard de Unica Plan

Rapport	Description
Approbations en attente d'action	Liste des approbations en attente de votre intervention.

Tableau 14. Portlets de liste standard de Unica Plan (suite)

Rapport	Description
Gérer Mes tâches	Répertorie vos tâches en attente et actives ainsi que les approbations non démarrées et en cours. Une option permettant de changer le statut de chaque élément apparaît. • Pour les tâches, vous pouvez remplacer le statut par Terminer ou Ignorer. • Pour les approbations Non démarrées, vous pouvez remplacer le statut par Soumettre ou Annuler. • Pour les approbations en cours dont vous êtes propriétaire, vous pouvez remplacer le statut par Arrêter, Terminer ou Annuler. • Pour les approbations en cours que vous êtes chargé de valider, vous pouvez remplacer le statut par Valider ou Rejeter.
Mes projets actifs	Répertorie vos projets actifs.
Mes alertes	Répertorie vos alertes Unica Plan.
Santé de mon projet	Indique le nom, l'état de santé, le pourcentage d'avancement et le nombre de tâches qui vous sont affectées pour chaque projet qui vous appartient ou dont vous êtes réviseur ou membre. Le pourcentage d'avancement se calcule comme suit : `(Number of Finished Tasks + Number of Skipped Tasks)/ Total Number of Workflow Tasks` • Pour recalculer l'état de santé du projet, cliquez sur  . Le système recalcule l'état de santé à afficher par ce portlet uniquement. Ce rapport ne fonctionne pas ailleurs dans Unica Plan.

Tableau 14. Portlets de liste standard de Unica Plan (suite)

Rapport	Description
	Remarque : Le calcul de l'état de santé du projet ne peut s'effectuer que par intervalles de 5 minutes. • Si vous avez plus de 100 projets, cliquez sur **Afficher tout** pour ouvrir la liste dans une nouvelle boîte de dialogue. • Pour exporter dans un fichier CSV les données de projet affichées, cliquez sur **Exporter**. • Vous pouvez afficher des informations récapitulatives sur un projet dans l'onglet **Récapitulatif**. Pour afficher d'autres indicateurs de l'état de santé du projet, cliquez sur l'indicateur du pourcentage d'avancement. Pour afficher la liste **Mes tâches**, cliquez sur le nombre dans la colonne Tâches.
Mes demandes	Répertorie les demandes dont vous êtes propriétaire.
Mes tâches	Répertorie les tâches dont vous êtes propriétaire.
Projets dépassant le budget	Répertorie tous les projets qui dépassent le budget pour l'année calendaire. **Remarque :** Ce rapport requiert le module de gestion financière.

Portlets de rapport pour Unica Campaign

Les portlets de rapport Unica Insights ou IBM® Cognos® sont fournis avec le package de rapports Unica Campaign. Utilisez les portlets de rapport pour analyser les taux de réponse et l'efficacité de la campagne.

Vous pouvez activer, puis ajouter des portlets de tableau de bord prédéfinis à un tableau de bord que vous créez. Pour gérer vos tableaux de bord et y ajouter des portlets, cliquez sur **Tableau de bord > Créer un tableau de bord**.

Tableau 15. Portlets de rapport IBM® Cognos® pour Unica Campaign

Rapport	Description
Comparaison des retours sur investissement Unica Campaign	Rapport qui compare, à un niveau élevé, les retours sur investissement des campagnes créées ou mises à jour par l'utilisateur qui consulte le rapport.
Comparaison des taux de réponses Unica Campaign	Rapport qui compare les taux de réponse d'une ou plusieurs campagnes créées ou mises à jour par l'utilisateur qui consulte le rapport.
Comparaison des chiffres d'affaires par offre Unica Campaign	Rapport qui compare les revenus perçus à ce jour pour les campagnes contenant des offres créées ou mises à jour par l'utilisateur qui consulte le rapport.
Réponses aux offres au cours des 7 derniers jours	Rapport qui compare le nombre de réponses reçues au cours des 7 derniers jours pour chaque offre créée ou mise à jour par l'utilisateur qui consulte le rapport.
Comparaison des taux de réponses aux offres	Rapport qui compare les taux de réponse pour les offres créées ou mises à jour par l'utilisateur qui consulte le rapport.
Répartition des réponses par offre	Rapport contenant les offres actives créées ou mises à jour par l'utilisateur qui consulte le rapport, divisées en fonction de leur statut.

Portlets de liste Unica Campaign

Les portlets de liste standard de Unica Campaign sont utilisables sur les tableaux de bord, même si le package de rapports de Unica Campaign n'est pas installé.

Tableau 16. Portlets de liste Unica Campaign

Rapport	Description
Mes signets personnalisés	Liste de liens vers des sites Web ou fichiers créés par l'utilisateur qui consulte le rapport.
Mes campagnes récentes	Liste des campagnes les plus récentes créées par l'utilisateur qui consulte le rapport.
Mes sessions récentes	Liste des sessions les plus récentes créées par l'utilisateur qui consulte le rapport.
Portlet de contrôle de campagne	Une liste des campagnes qui ont été exécutées ou qui sont exécutées et qui ont été créées par l'utilisateur qui consulte le rapport.

Portlets de rapport Unica Deliver

Unica Insights et le package de rapports Unica Deliver contient les portlets de tableau de bord suivants.

Rapport	Description
Mes récentes réponses de rebond des e-mails	Ce rapport de tableau de bord présente des données sur différents types de refus d'e-mail sous la forme d'un diagramme à barres. Le graphique présente les réponses refusées actuelles pour les cinq derniers mailings envoyés avant la date en cours.
Campagnes par e-mail récentes envoyées	Ce rapport de tableau de bord fournit un récapitulatif des dernières activités de mailing. Il indique les totaux pour la transmission des messages, les réponses des destinataires et les refus d'e-mail pour les cinq derniers mailings envoyés avant la date en cours.

Portlet de rapport Unica Interact

Performances du point d'interaction : indique le nombre d'offres acceptées par point d'interaction sur une période de sept jours.

Ce tableau de bord est configuré de sorte à signaler le canal interactif portant l'ID n°1. Pour créer des versions supplémentaires de ce rapport (afin de produire des rapports sur des canaux interactifs supplémentaires) ou changer l'ID du canal interactif que ce rapport désigne, consultez Configuration du portlet de tableau de bord Performances du point d'interaction (à la page 65).

Configuration du portlet de tableau de bord Performances du point d'interaction

Unica Interact comporte un rapport de tableau de bord Cognos® : Récapitulatif du nom du point d'interaction Etant donné que les rapports de tableau de bord n'invitent pas les utilisateurs à saisir des paramètres de requête, l'ID du canal interactif du rapport Performances du point d'interaction est une valeur statique. Par défaut, l'ID du canal pour ce rapport est réglée sur 1. Si cet ID n'est pas adapté à votre mise en oeuvre, vous pouvez personnaliser le rapport et changer l'ID du canal dans l'expression de filtre du rapport.

Pour personnaliser des rapports Cognos®, vous devez savoir comment les produire des rapports Cognos®. Pour obtenir une documentation détaillée sur la création et la modification de rapports Cognos® BI, consultez la documentation Cognos® BI, et plus particulièrement le manuel Cognos® BI Report Studio Professional Authoring - Guide d'utilisation correspondant à votre version de Cognos®.

Pour en savoir plus sur les éléments de requête et de données du rapport Performances du point d'interaction, consultez la documentation de référence fournie dans le package de rapports Unica Interact.

Pour afficher un diagramme pour plusieurs canaux interactifs dans le tableau de bord, faites une copie du rapport de tableau de bord et modifiez l'ID du canal. Créez ensuite un portlet de tableau de bord pour le nouveau rapport et ajoutez-le à vos tableaux de bord.

Portlets de liste Unica Collaborate

Cette section décrit les portlets standard de Unica Collaborate qui peuvent être utilisés dans les tableaux de bord.

Tableau 17. Portlets de liste Unica Collaborate

Rapport	Description
Gestion des listes	Listes actives pour l'utilisateur qui consulte le rapport.
Gestion des campagnes	Liste des campagnes nationales et à la demande actives pour l'utilisateur qui consulte le rapport.
Gestion des abonnements	Liste des abonnements aux campagnes nationales pour l'utilisateur actuel.
Calendrier	Calendrier qui présente la planification des campagnes nationales et à la demande actives.

Portlets de liste Unica Optimize

Portlets standard de Unica Optimize utilisables dans les tableaux de bord.

Ces portlets ne peuvent être utilisés que dans le tableau de bord Unica.

Tableau 18. Portlets de liste Unica Optimize

Tableau à deux colonnes décrivant les portlets de listes de Unica Optimize.

Rapport	Description
Mes sessions Unica Optimize récentes	Liste des 10 dernières sessions Unica Optimize exécutées par l'utilisateur qui consulte le rapport dans les 30 derniers jours.
Mes occurrences d'exécution Unica	Liste des 10 dernières sessions Unica Optimize exécutées par l'utilisateur qui consulte le rapport qui se sont terminées correctement dans les 30 derniers jours.

Tableau 18. Portlets de liste Unica Optimize

Tableau à deux colonnes décrivant les portlets de listes de Unica Optimize.

(suite)

Rapport	Description
Optimize ayant récemment réussi	
Mes occurrences d'exécution Unica Optimize ayant récemment échoué	Liste des 10 dernières sessions Unica Optimize exécutées par l'utilisateur qui consulte le rapport qui se sont terminées incorrectement dans les 30 derniers jours.

Tableaux de bord préassemblés

Unica fournit des tableaux de bord préassemblés contenant des portlets adaptés à divers utilisateurs.

Disponibilité des tableaux de bords préassemblés

Ces tableaux de bord sont accessibles dès que vous installez Unica Platform. Toutefois, pour implémenter totalement ces tableaux de bord, vous devez également installer tous les produits requis pour prendre en charge leurs portlets et vous devez aussi activer les portlets.

Pour qu'un tableau de bord préassemblé soit disponible, vous devez installer au moins un des produits qui le prennent en charge. Par exemple, si un tableau de bord préassemblé comprend des portlets issus de Unica Campaign et de Unica Deliver, ce tableau de bord est disponible uniquement si l'un de ces produits est installé. Si aucun de ces produits n'est installé, le tableau de bord n'apparaît pas dans l'interface utilisateur. Si l'un des deux produits est manquant, les portlets qui dépendent de ce produit apparaissent mais un message indique qu'ils ne sont pas disponibles.

Liste des tableaux de bord préassemblés

Le tableau suivant décrit les tableaux de bord préassemblés, leur finalité, les portlets qu'ils contiennent et les produits requis pour leur fonctionnement.

Tableau 19. Liste des tableaux de bord préassemblés

Tableau de bord préassemblé	Objectif	Portlets	Produits requis
Gestion des campagnes	Ce tableau de bord indique les résultats financiers des campagnes.	• Récapitulatif financier des campagnes par offre • Comparaison des performances de la campagne	• Unica Campaign • Unica Insights ou groupe de rapports Unica Campaign
Gestion des projets et du trafic	Ce tableau de bord indique les mises à jour de statut des projets.	• Mes tâches • Mes alertes • Mes projets actifs • Récapitulatif de mes tâches • Projets demandés et terminés • Approbations en attente d'action • Récapitulatif de mes approbations • Projets par statut	• Unica Plan • Unica Insights ou groupe de rapports Unica Plan

Tableau 19. Liste des tableaux de bord préassemblés (suite)

Tableau de bord préassemblé	Objectif	Portlets	Produits requis
Membre du projet	Ce tableau de bord indique les tâches qui demandent une action et permet de clore les tâches terminées.	• Mes tâches • Mes projets actifs • Mes alertes • Mes demandes	Unica Plan
Demandes et approbations de projets	Ce tableau de bord indique les tâches qui demandent une action, les mise à jour de statut des projets, il fournit une vue générale de la situation marketing et financière du projet et montre l'affectation des fonds dépensés.	• Approbations en attente d'action • Mes alertes • Position financière marketing • Projets par type de projet • Budget par type de projet • Dépense par type de projet • Projets terminés par trimestre	• Unica Plan avec le module de gestion financière • Unica Insights ou groupe de rapports Unica Plan
Etats financiers du projet	Ce tableau de bord fournit une vue générale de la situation marketing et financière du projet et	• Approbations en attente d'action • Position financière marketing	• Unica Plan avec le module de gestion financière

Tableau 19. Liste des tableaux de bord préassemblés (suite)

Tableau de bord préassemblé	Objectif	Portlets	Produits requis
	montre l'affectation des fonds dépensés.	• Alertes • Projets par type • Projets terminés par trimestre	• Unica Insights ou groupe de rapports Unica Plan

Points à prendre en considération en ce qui concerne les performances des rapports IBM® Cognos®

Les rapports constituent des éléments visuels qui facilitent l'analyse de grandes quantités de données. Il est donc utile de les ajouter aux tableaux de bord. Toutefois, les rapports nécessitent des ressources de traitement supplémentaires et vous pouvez rencontrer des problèmes de performances lorsque de nombreux utilisateurs accèdent régulièrement à des tableaux de bord qui contiennent une grande quantité de rapports.

Bien que les organisations utilisent les données de façons différentes adaptées à leurs besoins, nous allons donner ici quelques conseils d'ordre général qui devraient vous aider à améliorer les performances des tableaux de bord qui contiennent des rapports IBM® Cognos®. Tous ces conseils s'appliquent aux portlets IBM® Cognos® de rapports, qui sont les plus gourmands en ressources.

Planification des exécutions dans IBM® Cognos®

Il est possible de planifier l'exécution de rapports IBM® Cognos® à des intervalles réguliers. Lorsqu'un rapport est planifié, il ne s'exécute pas à chaque fois qu'un utilisateur accède à un tableau de bord qui le contient. La planification permet ainsi d'améliorer les performances des tableaux de bord qui contiennent le rapport.

Les rapports Unica ne contenant pas de paramètre d'ID utilisateur sont les seuls à pouvoir être planifiés dans Cognos®. Les rapports qui n'utilisent pas ce paramètre présentent les

mêmes données à tous les utilisateurs, sans les filtrer en fonction de l'utilisateur. Il n'est pas possible de planifier les portlets suivants.

- Tous les portlets Unica Campaign prédéfinis
- Les portlets prédéfinis Récapitulatif de mes tâches et Récapitulatif de mes approbations de Unica Plan

La planification de rapports est une tâche que vous effectuez dans IBM® Cognos®. Consultez la documentation Cognos® pour plus d'informations sur la planification en général. Pour les besoins spécifiques à la planification pour les portlets de tableau de bord, consultez Planification d'un rapport de tableau de bord (à la page 72).

Observations relatives aux données

Vous devez planifier les exécutions en fonction des données contenues dans le rapport. Par exemple, il convient d'exécuter le rapport de tableau de bord Réponses aux offres au cours des sept derniers jours toutes les nuits, afin qu'il contienne les informations relatives aux sept jours précédents. En revanche, vous pouvez exécuter le rapport de tableau de bord Position financière marketing seulement une fois par semaine, car ce rapport compare des indicateurs financiers trimestriels.

Attentes des utilisateurs

Il convient également de tenir compte de la fréquence d'actualisation du rapport attendue par l'utilisateur dudit rapport. Demandez l'avis des utilisateurs lors de la planification.

Instructions

Voici quelques conseils généraux qui vous aideront à planifier l'exécution de rapports IBM® Cognos® de tableaux de bord.

- Les rapports qui incluent des informations cumulées doivent généralement être planifiés pour être exécutés chaque nuit.
- Les rapports qui contiennent de nombreux calculs doivent être planifiés.

Planification d'un rapport de tableau de bord

Pour planifier un rapport de tableau de bord (portlet prédéfini ou créé par un utilisateur), vous devez d'abord créer une vue et la planifier, puis configurer le portlet comme décrit ici.

Remarque : Vous ne pouvez planifier que les rapports non filtrés par l'utilisateur.

1. Dans Cognos®, copiez le rapport et enregistrez-le sous un nouveau nom.
2. Dans Cognos®, ouvrez le rapport que vous avez copié et enregistrez-le en tant que vue portant le même nom que le rapport d'origine. Enregistrez-la dans le dossier `Unica Dashboard/Product` , où `Product` correspond au dossier produit approprié.
3. Dans Cognos®, planifiez la vue.
4. Sous Unica, ajoutez le rapport au tableau de bord, si ce n'est pas déjà fait.
5. Si le rapport correspond à un portlet prédéfini, et uniquement dans ce cas, suivez la procédure ci-après dans Unica.
    - Dans la page Administration de tableau de bord, cliquez sur l'icône **Editer le portlet** située en regard du portlet.
    - Sélectionnez **Oui** en regard de **Ce rapport a-t-il été planifié ?**.
    - Cliquez sur **Sauvegarder**.

Configuration des tableaux de bord

Les rubriques de cette section expliquent comment configurer des tableaux de bord.

Droits d'accès requis pour l'administration des tableaux de bord

Seuls les utilisateurs disposant de droits d'administration de tableau de bord dans une partition peuvent administrer tous les tableaux de bord de cette partition. Par défaut, cette autorisation est accordée aux utilisateurs ayant le rôle AdminRole dans Unica Platform.

Lorsque vous installez Unica Platform pour la première fois, l'utilisateur prédéfini asm_admin dispose de ce rôle pour la partition par défaut Partition 1. Pour obtenir les données d'identification d'administrateur de tableau de bord appropriées, adressez-vous à votre administrateur.

Un utilisateur ayant le rôle AdminRole dans Unica Platform peut affecter n'importe quel utilisateur Unica pour administrer les tableaux de bord individuels dans la partition à laquelle l'utilisateur appartient. L'administration des tableaux de bord s'effectue dans la zone correspondante de Unica Platform.

Mise en forme du tableau de bord

La première fois que vous ajoutez un portlet à un nouveau tableau de bord, une fenêtre vous demande de sélectionner et d'enregistrer une présentation. Vous pouvez ensuite modifier cette présentation en sélectionnant l'onglet du tableau de bord puis en choisissant une autre mise en forme.

Les options disponibles sont les suivantes :

- 3 colonnes, largeur égale
- 2 colonnes, largeur égale
- 2 colonnes, 2/3 à 1/3 de la largeur
- 1 colonne, toute la largeur
- Personnalisé

Tableaux de bord et partitions

Si vous administrez des tableaux de bord dans un environnement comportant plusieurs partitions, lisez cette section pour comprendre comment plusieurs partitions ont une incidence sur les tableaux de bord.

Dans un environnement comportant plusieurs partitions, un utilisateur peut afficher ou administrer uniquement les tableaux de bord associés à la partition dont il fait partie.

Lorsqu'un administrateur de tableau de bord crée un tableau de bord, les règles suivantes liées à la partition s'appliquent.

- Tout tableau de bord créé n'est accessible qu'aux membres de la même partition que celle de l'utilisateur qui l'a créée.
- Seuls les portlets prédéfinis activés dans la partition dont fait partie l'administrateur peuvent être inclus dans le tableau de bord.
- Seuls les groupes et utilisateurs affectés à la même partition que l'administrateur peuvent être affectés au tableau de bord.

Présentation de l'utilisation des tableaux de bord dans un environnement à plusieurs partitions

Lorsque plusieurs partitions sont configurées, la procédure de configuration des tableaux de bord est la suivante :

1. Avant d'utiliser les tableaux de bord, associez un ou plusieurs groupes à chaque partition, puis affectez les utilisateurs appropriés à chaque groupe.

   Seul l'utilisateur platform_admin ou un autre utilisateur disposant des droits PlatformAdminRole peut effectuer cette tâche.
2. Pour chaque partition, vérifiez qu'au moins un utilisateur dispose des droits d'administration de tableau de bord, puis prenez note de ces noms d'utilisateur.

   Le rôle AdminRole de Unica Platform dispose par défaut de ces droits, mais vous pouvez être amené à créer un rôle doté d'un accès plus restreint pour les administrateurs de tableau de bord. Ces administrateurs de tableau de bord peuvent administrer tous les tableaux de bord au sein de leur partition.
3. Pour chaque partition configurée sur votre système, procédez comme suit :
   a. Utilisez un compte qui fait partie de la partition et qui peut administrer tous les tableaux de bord d'une partition pour la connexion à Unica.

      Reportez-vous à la liste des utilisateurs que vous avez créés à l'étape précédente.
   b. Sur la page **Paramètres > Portlets de tableau de bord**, activez des portlets prédéfinis, selon vos besoins.
   c. Sur la page Administration des tableaux de bord, créez des tableaux de bord nécessaires, puis ajoutez des portlets.

d. Pour chaque tableau de bord non global, affectez des utilisateurs pouvant afficher le tableau de bord.

   Vous pouvez affecter des utilisateurs ou groupes individuels au tableau de bord.

e. Pour chaque tableau de bord, affectez un ou plusieurs utilisateurs en tant qu'administrateur de tableau de bord.

Activation ou désactivation des portlets prédéfinis

Effectuez cette tâche avant de créer des tableaux de bord. Vous devez activer uniquement des portlets qui se réfèrent aux produits Unica que vous avez installés.

1. Connectez-vous à Unica et sélectionnez **Paramètres > Portlets de tableau de bord**.
2. Cliquez sur la case à cocher en regard des noms de portlet pour les activer ou les désactiver.

   Cochez la case pour activer un portlet et désélectionnez la case pour le désactiver.

   Les portlets sélectionnés sont activés et peuvent être inclus aux tableaux de bord.

Création d'un tableau de bord non préassemblé

Utilisez la procédure ci-dessous pour créer un tableau de bord non préassemblé.

1. Dans Unica, sélectionnez **Tableau de bord** pour ouvrir la page d'administration Tableau de bord.

   Tous les tableaux de bord associés à votre partition sont affichés.
2. Cliquez sur **Créer un tableau de bord** pour ouvrir la page Créer un tableau de bord.
3. Entrez un titre unique (obligatoire) et une description (facultative).
4. Sélectionnez les droits d'accès de base.
   - Si vous souhaitez limiter l'accès aux utilisateurs appartenant à un groupe associé au tableau de bord, sélectionnez **Tableau de bord spécifique d'un utilisateur ou d'un groupe**.
   - Si vous souhaitez que tous les utilisateurs de la partition puissent afficher le tableau de bord, sélectionnez **Tableau de bord global pour tout le monde**.
5. Dans la zone **Type**, sélectionnez **Créer un tableau de bord**.

6. Cliquez sur **Sauvegarder**.

   Votre nouveau tableau de bord apparaît sous la forme d'un onglet sur la page Administration des tableaux de bord. Il est répertorié sous l'onglet Administration.

Vous pouvez maintenant ajouter les portlets.

Création d'un tableau de bord préassemblé

Utilisez la procédure ci-dessous pour créer un tableau de bord préassemblé.

1. Vérifiez que les portlets qui contiendront le tableau de bord préassemblé que vous voulez créer sont activés.
2. Dans Unica, sélectionnez **Tableau de bord** pour ouvrir la page d'administration Tableau de bord.
3. Cliquez sur **Créer un tableau de bord**.
4. Dans la zone **Type**, sélectionnez **Utiliser des tableaux de bord préassemblés**.

   La vue affiche les tableaux de bord préassemblés disponibles.
5. Sélectionnez le tableau de bord préassemblé que vous voulez utiliser puis cliquez sur **Suivant**.

   La vue affiche les portlets qui contiennent le tableau de bord préassemblé sélectionné. La liste indique si un portlet est indisponible, soit parce que le produit requis n'est pas installé soit parce que le portlet n'est pas activé.
6. Cliquez sur **Enregistrer** pour terminer la création du tableau de bord.

   Votre nouveau tableau de bord apparaît sous la forme d'un onglet sur la page Administration des tableaux de bord. Il est répertorié sous l'onglet Administration. Vous pouvez maintenant modifier les portlets qu'il contient si vous le souhaitez.

Ajout d'un portlet prédéfini à un tableau de bord

Utilisez la procédure ci-dessous pour ajouter un portlet prédéfini à un tableau de bord.

1. Dans Unica, sélectionnez **Tableau de bord**, puis l'onglet du tableau de bord souhaité.
2. Cliquez sur **Gérer les portlets** pour afficher la liste des portlets activés.

Vous pouvez également accéder à la page Gérer les portlets dans l'onglet d'administration, en cliquant sur l'icône de gestion de portlets sur le tableau de bord.

3. Cochez la case en regard d'un ou plusieurs portlets pour les sélectionner afin de les ajouter au tableau de bord.

   Les fonctionnalités ci-dessous vous aident à sélectionner des portlets.

   - Filtrez la liste des portlets par nom ou en fonction du produit source du portlet.
   - Affichez tous les portlets en une seule fois ou en faisant défiler la liste.
   - Cliquez sur les en-têtes de colonne pour trier la liste dans l'ordre alphabétique par source ou par nom de portlet, dans l'ordre ascendant ou descendant.

4. Cliquez sur **Mettre à jour**.

   Les portlets sélectionnés s'ajoutent au tableau de bord.

Suppression d'un portlet d'un tableau de bord

Utilisez la procédure ci-dessous pour supprimer un portlet d'un tableau de bord.

1. Dans Unica, sélectionnez **Tableau de bord**.

   Une page Administration des tableaux de bord s'ouvre. Tous les tableaux de bord associés à votre partition sont affichés, de même que leurs portlets.

2. Dans le tableau de bord dans lequel vous souhaitez supprimer un portlet, cliquez sur l'icône **Supprimer** située en regard du portlet à supprimer.
3. Cliquez sur **Oui, Supprimer** dans l'invite.

   Le portlet est supprimé du tableau de bord.

Modification du nom ou des propriétés d'un portlet

Utilisez la procédure ci-dessous pour modifier le nom ou les propriétés d'un portlet.

1. Dans Unica, sélectionnez **Tableau de bord**.

   Une page Administration des tableaux de bord s'ouvre. Tous les tableaux de bord associés à votre partition sont affichés, de même que leurs portlets.

2. Dans le tableau de bord que vous souhaitez gérer, cliquez sur l'icône **Editer le portlet** en regard du portlet dont vous voulez changer le nom.

   Une fenêtre Editer le portlet s'ouvre.
3. Editez le nom, la description, l'URL ou les variables masquées du portlet.
4. Cliquez sur **Sauvegarder**.

Modification du nom ou des propriétés d'un tableau de bord

Utilisez la procédure ci-dessous pour changer le nom ou les propriétés d'un tableau de bord.

1. Dans Unica, sélectionnez **Tableau de bord**.

   Une page Administration des tableaux de bord s'ouvre. Tous les tableaux de bord associés à votre partition sont affichés.
2. Dans le tableau de bord que vous souhaitez gérer, cliquez sur l'icône **Gérer les paramètres** dans la partie inférieure du tableau de bord.

   Un onglet Paramètres s'ouvre.
3. Cliquez sur l'icône **Editer le tableau de bord**.

   Une fenêtre Editer le tableau de bord s'ouvre.
4. Editez le titre, la description ou le type du tableau de bord, activez ou désactivez le tableau de bord, ou indiquez si les utilisateurs peuvent ou non changer la disposition.
5. Cliquez sur **Sauvegarder**.

Suppression d'un tableau de bord

Cette procédure permet de supprimer un tableau de bord.

1. Dans Unica, sélectionnez **Tableau de bord**.

   Une page Administration des tableaux de bord s'ouvre. Tous les tableaux de bord associés à votre partition sont affichés.
2. Dans le tableau de bord que vous souhaitez gérer, cliquez sur l'icône **Supprimer un tableau de bord** située au bas du tableau de bord.
3. Lorsque vous y êtes invité, cliquez sur **Oui, Supprimer**.

   Le tableau de bord est supprimé.

Affection d'un administrateur de tableau de bord ou changement de l'administrateur de tableau de bord

Utilisez la procédure ci-dessous pour affecter ou changer un administrateur de tableau de bord.

1. Dans Unica, sélectionnez **Tableau de bord**.

   Une page Administration des tableaux de bord s'ouvre. Tous les tableaux de bord associés à votre partition sont affichés, de même que leurs portlets.
2. Cliquez sur l'icône **Gérer les autorisations** située au bas du tableau de bord que vous voulez gérer.
   Un onglet Gérer les autorisations s'ouvre.
3. Cliquez sur l'icône **Gérer les administrateurs de tableaux de bord**.
   Une page Gérer les administrateurs de tableaux de bord s'ouvre. Tous les tableaux de bord associés à votre partition sont affichés, de même que leurs portlets.
4. Sélectionnez ou désélectionnez des noms.

   Les utilisateurs dont le nom est sélectionné disposent de droits d'administrateur pour ce tableau de bord.

   Pour rechercher des utilisateurs, procédez comme suit :

   - Filtrez la liste en entrant la totalité ou une partie d'un nom d'utilisateur dans la zone **Rechercher**.
   - Affichez tous les utilisateurs, uniquement les utilisateurs non affectés ou uniquement les utilisateurs affectés.
   - Triez la liste en cliquant sur des en-têtes de colonne.
   - Affichez tous les utilisateurs en même temps (en fonction de vos critères de filtrage) ou faites défiler la liste.
5. Cliquez sur **Mettre à jour**.

Page Gérer les portlets

Voir le tableau suivant si vous avez besoin d'aide pour renseigner les zones de la page Gérer les portlets.

Tableau 20. Zones de la page Gérer les portlets

Zone	Description
Filtrer	Pour filtrer la liste des portlets sur la base du produit qui fournit le rapport ou du nom du portlet, entrez tout ou partie du nom de ce produit.
Créer un portlet personnalisé	Cliquez sur cette option pour ouvrir une page dans laquelle vous pouvez créer un portlet utilisant une adresse URL obtenue préalablement.
Créer un portlet de lien rapide	Cliquez sur cette option pour ouvrir une page dans laquelle vous pouvez créer un portlet de lien rapide.

Portlets de lien rapide

Les liens rapides sont des liens prédéfinis avec les produits Unica. Certains liens rapides permettent aux utilisateurs d'effectuer des actions de base dans le produit Unica à l'intérieur d'un tableau de bord sans accéder au produit. Vous pouvez configurer des portlets contenant un ensemble de liens rapides que vous choisissez.

Les liens rapides des produits Unica sont installés en même temps que les produits eux-mêmes. Dans la version 9.0.0, les liens rapides ne sont disponibles que pour Unica Plan. Les principes de sécurité applicables aux liens rapides sont les mêmes que ceux des portlets prédéfinis.

Pour ajouter un portlet de lien rapide à l'un de vos tableaux de bord, cliquez sur **Gérer les portlets > Créer un portlet de lien rapide** puis sélectionnez les liens rapides que vous souhaitez ajouter.

Le tableau suivant décrit les liens rapides qui sont disponibles quand vous installez Unica Plan.

Tableau 21. Liste des portlets de lien rapide

Lien rapide	Fonction
Créer une nouvelle demande de projet	Ouvre une fenêtre instantanée dans laquelle vous pouvez choisir un modèle de projet afin de créer une demande de projet. Vous pouvez également cliquer sur **Continuer** pour ouvrir l'assistant Demande de projet dans l'application.
Créer un nouveau projet	Ouvre une fenêtre instantanée dans laquelle vous pouvez choisir un modèle de projet afin de créer un projet. Vous pouvez également cliquer sur **Continuer** pour ouvrir l'assistant Projet dans l'application.
Ajouter une facture	Ouvre l'assistant Ajouter une facture dans l'application.
Projets	Ouvre la page Liste des projets dans l'application.
Rapports	Ouvre la page **Analyse > Analyse opérationnelle**.
Bibliothèque de ressources	Ouvre la page Bibliothèque de ressources dans l'application.
Approbations	Ouvre la page Liste des approbations dans l'application.

Création d'un portlet de lien rapide

Utilisez la procédure ci-dessous pour créer un portlet de lien rapide.

1. Cliquez sur **Gérer les portlets** dans le tableau de bord auquel vous souhaitez ajouter un portlet de lien rapide.

   La page Gérer les portlets s'ouvre. Elle affiche la liste des portlets prédéfinis.
2. Cliquez sur **Créer un portlet de lien rapide**.
3. Entrez un nom et une description pour le portlet, puis sélectionnez les liens rapides que vous souhaitez inclure dans le portlet.
4. Cliquez sur **Enregistrer** pour terminer la création du portlet et l'ajouter au tableau de bord.

Portlets personnalisés

Les rubriques de cette section expliquent comment créer et utiliser des portlets personnalisés.

Types de portlet personnalisé et disponibilité

Vous pouvez créer des portlets à partir des pages d'Unica.

- N'importe quel rapport Cognos®, y compris les rapports de performances des points d'interaction Unica Interact que vous avez personnalisés pour les faire pointer sur des canaux interactifs supplémentaires. Vous pouvez personnaliser les rapports de tableau de bord existants, comme décrit dans ce guide, de même que les autres types de rapports. Pour savoir comment personnaliser un rapport autre qu'un rapport de tableau de bord, voir le document *Unica Guide d'installation et de configuration des rapports*.
- Les portlets de lien rapide, que vous pouvez créer avec des liens prédéfinis avec les produits Unica.
- Tout rapport Digital Analytics for On Premises, rapport à la demande Digital Analytics for On Premises ou tableau de bord mis à jour automatiquement.
- N'importe quel rapport IBM Digital Analytics.

En outre, vous pouvez créer un portlet à partir d'une page Web ou de l'intranet de votre société.

Les portlets que vous avez créés vous-même sont utilisables dans tous les tableaux de bord. Vos portlets personnalisés sont répertoriés dans la fenêtre de Gérer les portlets dans laquelle vous pouvez choisir de les ajouter à un tableau de bord.

Remarques sur l'authentification pour les portlets personnalisés

Si vous envisagez de créer des portlets, gardez à l'esprit les remarques suivantes relatives à l'authentification.

- Si le portlet est un rapport Digital Analytics for On Premises d'une installation configurée pour utiliser Unica Platform pour l'authentification ou ne pas utiliser l'authentification, ou un rapport de tableau de bord d'un autre produit Unica qui utilise Unica Platform pour l'authentification, le système demande aux utilisateurs leurs données d'identification lorsqu'ils affichent le portlet.
- Si le portlet est un rapport Digital Analytics for On Premises d'une installation qui n'est pas configurée pour utiliser Unica Platform pour l'authentification, l'utilisateur doit entrer ses données d'identification une fois par session de navigation.
- Si votre portlet est un rapport NetInsight OnDemand ou une page Web ou intranet qui requiert une authentification, le portlet se comporte comme un navigateur. L'utilisateur doit saisir ses données d'identification de connexion dans le contenu de la page à la première consultation de celle-ci dans une session de navigation et des cookies sont utilisés pour permettre de maintenir l'utilisateur connecté.
- Si votre portlet est un rapport IBM Digital Analytics, vous ne pouvez consulter que les rapports pour lesquels vous disposez de droits d'accès dans Digital Analytics. De même, si la connexion unique est activée avec Digital Analytics, vous pouvez afficher des rapports Digital Analytics dans les tableaux de bord de Unica Platform sans entrer vos données d'identification. Dans le cas contraire, vous devez entrer vos données d'identification Digital Analytics pour afficher des rapports Digital Analytics dans les tableaux de bord Unica Platform.

Présentation du processus de création d'un portlet

Cette section donne une présentation des étapes de création de portlet, qui sont décrites en détail dans une autre section de ce guide.

Voir les références connexes si vous avez besoin d'informations supplémentaires sur l'exécution de cette procédure.

1. Obtenez et préparez l'URL de la page que vous souhaitez utiliser en tant que portlet.

   Pour cela, obtenez l'URL et modifiez-la selon vos besoins.

   Vous pouvez créer des portlets à partir des sources suivantes :

- Rapport Digital Analytics for On Premises
- IBM Cognos® rapport
- Rapport Digital Analytics
- Rapport et pages NetInsight OnDemand sur Internet ou sur l'intranet de votre société

2. Ajoutez l'URL au fichier `Platform_Admin_URL.properties`.

   Le fichier `Platform_Admin_URL.properties` se trouve dans le répertoire `conf` dans votre installation de Unica Platform.
3. Arrêtez et redémarrez l'application Web Unica Platform.
4. Ajoutez le portlet à un tableau de bord.

Préparation de l'URL à partir d'un rapport Digital Analytics for On Premises

Utilisez la procédure ci-dessous pour les rapports d'une installation Digital Analytics for On Premises.

1. Dans Digital Analytics for On Premises, affichez le rapport que vous souhaitez exporter.

   Si vous utilisez un tableau de bord Digital Analytics for On Premises, seul le rapport situé en haut à gauche du tableau est exporté.
2. Cliquez sur l'icône **Exporter**  située dans la barre d'outils dans l'angle supérieur droit du rapport.

   La fenêtre des options d'exportation s'ouvre.
3. Renseignez les zones comme suit :
   - Sélectionnez **URL du portlet** dans le menu déroulant **Type d'exportation.**
   - Sélectionnez `Navigateur Web` dans le menu déroulant **Format du rapport.**
   - Spécifiez le nombre de valeurs à inclure dans le rapport.
   - Spécifiez la largeur du graphique de rapport, en pixels. Quelle que soit la largeur spécifiée, les rapports de chemin ajustent leur taille par eux-mêmes. Les

rapports de barres empilées augmentent automatiquement la largeur spécifiée de 30 %.
- Etant donné que le titre du portlet peut être édité, choisissez de masquer l'en-tête du rapport.

4. Cliquez sur **Exporter**.

   L'URL de rapport s'affiche dans une boîte de dialogue.
5. Copiez l'URL et collez-la dans un éditeur de texte.
6. Ajoutez les éléments suivants au début de l'URL du rapport :

   Your_HCL_Unica_URL/suiteSignOn?target=

   où *Your_HCL_Unica_URL* correspond à l'URL de connexion de votre installation de Unica.

   Par exemple, supposons que vous disposiez des informations suivantes :

   - Votre URL de rapport est `MyReportURL`
   - L'URL de connexion pour votre installation de Unica est `http://myHost.myDomain:7001/unica`

   Votre URL finale sera `http://myHost.myDomain:7001/unica/suiteSignOn?target=MyReportURL`

Préparation de l'URL depuis un rapport de tableau de bord IBM® Cognos®

Le format d'une URL de portlet de tableau de bord IBM® Cognos® est le suivant.

Pour plus d'informations sur la création de rapports de tableau de bord avec IBM® Cognos®, voir le document Unica Reports Installation and Configuration Guide.

`http(s)://`*`HOST.DOMAIN`*`:`*`port`*`/unica/reports/jsp/dashboard_portlet.jsp?product=`*`Product`*`& report=`*`ReportName`*

où

- *Product* est le nom du sous-dossier de l'application Unica dans le dossier **Tableaux de bord Unica** sur le système IBM® Cognos®. A savoir : Campaign, Interact ou Plan pour Unica Plan. (Plan est l'ancien nom de l'application Unica Plan).
- *ReportName* correspond au nom du rapport de tableau de bord. Par exemple : Comparaison des performances de la campagne

Par exemple,

```
http://serverX.example.com:7001/unica/reports/jsp/dashboard_portlet.jsp?
product=Campaign&report=Campaign Performance Comparison
```

Si vous avez planifié le rapport, ajoutez ce qui suit à la fin de l'URL :

```
&isView=true
```

Préparation de l'URL à partir d'un rapport Digital Analytics

Utilisez cette procédure pour les rapports Digital Analytics.

Si vous voulez que les utilisateurs puissent consulter les rapports Digital Analytics dans des tableaux de bord sans avoir à s'identifier dans Digital Analytics, vous devez activer la connexion unique entre Unica et Digital Analytics.

1. Connectez-vous à Digital Analytics et recherchez le rapport que vous souhaitez ajouter en tant que portlet.
2. Copiez l'URL affichée dans votre navigateur.

   Le lien est copié dans votre presse-papiers et vous pouvez le coller immédiatement dans la zone URL d'IBM® Digital Analytics, dans la fenêtre Créer un portlet personnalisé de Unica Platform.

   Pour être certain que l'adresse URL ne sera pas écrasée dans le cas où vous devriez copier autre chose avant de l'utiliser pour créer le portlet, vous pouvez la copier dans un éditeur de texte.

Préparation de l'URL depuis une page intranet ou internet

Pour des portlets créés à partir de pages intranet ou internet, notamment des pages Digital Analytics for On Premises, faites pointer votre navigateur vers la pages souhaitée et copiez l'adresse URL depuis la zone d'adresse de votre navigateur.

Utilisez l'adresse URL copiée lorsque vous créez votre portlet personnalisé.

Ajout d'un portlet personnalisé à un tableau de bord

Exécutez cette procédure pour ajouter un portlet personnalisé à un tableau de bord.

Avant d'exécuter cette procédure, vous devez avoir effectué les opérations suivantes.

- Préparé une URL, comme indiqué dans cette section.
- Ajouté l'URL au fichier `Platform_Admin_URL.properties`, qui se trouve dans le répertoire `conf` de votre installation Unica Platform.
- Arrêté et redémarré l'application Web Unica Platform.

1. Dans Unica, sélectionnez **Tableau de bord**, puis l'onglet du tableau de bord souhaité.
2. Cliquez sur **Gérer les portlets**.

   Une fenêtre **Gérer les portlets** s'ouvre.
3. Cliquez sur **Créer un portlet personnalisé**.

   Une fenêtre **Créer un portlet personnalisé** s'ouvre.
4. Exécutez l'une des procédures suivantes selon le type de portlet que vous ajoutez :

   Si vous créez un portlet autre qu'un portlet de rapport Digital Analytics, procédez comme suit :

   - Dans la zone **Type**, sélectionnez **Personnalisé**.
   - Renseignez les zones **Nom** et **Description**.
   - Collez le contenu du presse-papiers (qui contient l'adresse URL que vous avez obtenue plus tôt) dans la zone **URL**.

   Si vous créez un portlet de rapport Digital Analytics, procédez comme suit :

- Dans la zone **Type**, sélectionnez **IBM Digital Analytics**.
- Renseignez les zones **Nom** et **Description**.
- Collez le contenu du presse-papiers (qui contient l'adresse URL que vous avez obtenue plus tôt) dans la zone **URL IBM Digital Analytics**.

5. Cliquez sur **Sauvegarder**.

   La fenêtre se ferme et vous revenez à l'onglet Administration. Le nouveau portlet se trouve dans l'angle supérieur gauche, où il est possible qu'il recouvre un portlet précédemment ajouté. Cliquez et faites glisser l'en-tête du portlet afin de placer ce dernier correctement dans le tableau de bord.

Jetons dynamiques

Lorsque vous définissez un portlet de tableau de bord personnalisé, vous pouvez utiliser des jetons prédéfinis qui sont remplacés par les valeurs stockées dans Unica Platform pour l'utilisateur en cours lorsque le portlet est appelé.

Cette fonctionnalité n'est pas disponible pour les portlets personnalisés depuis Digital Analytics.

Les jetons suivants sont pris en charge.

- `<user_name>`
- `<user_first_name>`
- `<user_last_name>`
- `<user_email>`

L'URL est appelée avec des variables masquées transmises en tant que paramètres de demande.

Les valeurs doivent figurées dans les détails de l'utilisateur dans Unica Platform. De plus, vous devez connaître les noms des variables utilisées par le site Web cible.

Pour utiliser ces jetons, entrez les paires de valeurs de nom dans la zone **Variables cachées** de la page Créer un portlet personnalisé. Si vous utilisez plusieurs jetons, séparez-les par un point-virgule.

Par exemple, supposons que vous souhaitez envoyer le nom et le prénom d'un utilisateur dans une adresse URL de portlet. Dans cet exemple, le site Web de destination s'attend à ce que les zones `fname` et `lname` contiennent respectivement le prénom et le nom de l'utilisateur. Vous devez compléter les zones **URL** et **Variables cachées** comme suit.

- **URL** - `www.example.com`
- **Variables cachées** - `fname=<user_first_name>;lname=<user_last_name>`

Page Créer un portlet personnalisé

Voir le tableau suivant si vous avez besoin d'aide pour renseigner les zones de la page Créer un portlet personnalisé.

Tableau 22. Zones de la page Créer un portlet personnalisé

Zone	Description
Type	Sélectionnez le type de portlet désiré : un portlet non issu de Digital Analytics ou un portlet issu de Digital Analytics.
Nom	Entrez un nom approprié pour le portlet.
Description	Entrez une description du portlet pour indiquer aux autres administrateurs pourquoi il fait partie de ce tableau de bord.
URL ou URL de Digital Analytics	Collez l'URL que vous avez préparée.
Variables cachées	Disponible uniquement pour un portlet non issu de Digital Analytics. Si votre portlet nécessite que les utilisateurs se connectent, vous pouvez entrer des paires nom-valeur pour envoyer en toute sécurité ces données d'identification au site. Vous devez obtenir sur le site Web le nom de variable attendu.

Administration de l'appartenance à un tableau de bord

Les rubriques de cette section expliquent comment gérer les membres du tableau de bord.

Administrateur de tableau de bord

Si vous êtes l'administrateur d'un tableau de bord, vous devez gérer les membres, la présentation et le contenu de ce tableau de bord. Cette section explique comment gérer les membres du tableaux de bord.

Ajout ou retrait d'un membre de tableau de bord

Utilisez la procédure ci-dessous pour ajouter ou retirer un membre dans un tableau de bord.

1. Dans Unica, sélectionnez **Tableau de bord**, puis l'onglet du tableau de bord souhaité.
2. Cliquez sur l'icône **Gérer les autorisations** située au bas du tableau de bord que vous voulez gérer.

   Un onglet Gérer les autorisations s'ouvre.
3. Cliquez sur l'icône **Gérer les utilisateurs de tableaux de bord**.

   Une page Gérer les utilisateurs des tableaux de bord s'ouvre.
4. Cochez ou décochez la case pour autoriser ou interdire l'accès au tableau de bord.

   Les utilisateurs dont le nom est sélectionné peuvent visualiser le tableau de bord.

   Pour rechercher des utilisateurs, procédez comme suit :

   - Filtrez la liste en entrant la totalité ou une partie d'un nom d'utilisateur dans la zone **Rechercher**.
   - Affichez tous les utilisateurs, uniquement les utilisateurs non affectés ou uniquement les utilisateurs affectés.
   - Triez la liste en cliquant sur des en-têtes de colonne.
   - Affichez tous les utilisateurs en même temps (en fonction de vos critères de filtrage) ou faites défiler la liste.
5. Cliquez sur **Mettre à jour**.

Planificateur Unica

Le planificateur Unica vous permet de configurer l’exécution d’un processus à des intervalles définis par vos soins.

Eléments pouvant être planifiés

Vous pouvez planifier les opérations suivantes.

- Exécutions de diagramme Unica Campaign

  Remarque : Le planificateur Unica est complètement indépendant du processus de planification dans Unica Campaign.

- Exécutions de diagramme de post-optimisation et de session d'optimisation de Unica Optimize
- Mailings Unica Deliver
- Désactivations Unica Plan en bloc
- Appels d'API externes
- Alertes et notifications Unica
- Scripts par lots ou shell externes

Planifications et exécutions

Le planificateur utilise deux concepts de base : les planifications et les exécutions.

- Une planification est une tâche exécutable une fois ou de façon récurrente. Lorsque vous définissez une planification, vous spécifiez l'objet Unica, les dates de début et de fin et, éventuellement, la fréquence à laquelle la tâche est exécutée (appelé modèle de récurrence).
- Une exécution est l'instance d'exécution d'une planification.

Types de planifications

Il existe trois types de planifications :

- Date : les exécutions sont effectuées aux dates spécifiées.
- Déclencheur : les exécutions sont effectuées lorsqu'une planification reçoit un déclencheur spécifié (par exemple, lorsqu'une autre planification envoie un

déclencheur en cas de réussite ou d'échec de son exécution ou lorsque l'utilitaire du planificateur envoie un déclencheur).
- Exécutions multiples : les exécutions sont dépendantes des autres planifications et ne se produisent que lorsque plusieurs autres planifications ont terminé leur exécution

Notifications de planification

Vous pouvez configurer des notifications qui vous sont envoyées pour les planifications que vous avez créées et les administrateurs peuvent configurer des notifications qui sont envoyées aux groupes d'utilisateurs pour les planifications créées par une personne quelconque.

Déclencheurs du planificateur envoyés en cas de réussite ou d'échec des exécutions

Lorsque vous créez ou éditez une planification, vous pouvez configurer un déclencheur qui sera envoyé par la planification en cas de succès ou d'échec d'une exécution et vous pouvez aussi configurer une ou plusieurs planifications afin qu'elles soient à l'écoute de ces déclencheurs.

Les déclencheurs fonctionnent sur tous les produits. Par exemple, un diagramme Unica Campaign peut envoyer un déclencheur qui lance un mailing Unica Deliver.

Un déclencheur est une chaîne de texte que le déclencheur Unica peut envoyer lors de la réussite ou de l'échec d'une exécution. Chaque planification peut envoyer un déclencheur en cas de réussite d'une exécution et un déclencheur en cas d'échec d'une exécution. De même, chaque planification peut se mettre à l'écoute d'un déclencheur de réussite et d'un déclencheur d'échec.

Toutes les planifications configurées pour écouter un déclencheur reçoivent tous les déclencheurs envoyés, mais une planification ne lance une exécution que si elle reçoit le déclencheur à l'écoute duquel elle se trouve. Vous pouvez créer de cette manière un nombre illimité de dépendances entre les planifications.

Après avoir créé un déclencheur, le déclencheur apparaît dans une liste déroulante de déclencheurs dans l'interface utilisateur du planificateur, ce qui permet de le réutiliser aisément.

Exemple de déclencheur

Vous pouvez planifier l'exécution simultanée d'un ensemble de diagrammes Unica Campaign en les configurant pour qu'ils écoutent tous le même déclencheur, qui peut être envoyé par n'importe quelle autre planification ou par une application externe en utilisant l'utilitaire scheduler_console_client (à la page 360). Vous pouvez également utiliser les déclencheurs pour définir l'exécution séquentielle d'un ensemble de diagrammes.

L'exemple suivant présente la façon de configurer l'exécution d'une série de diagrammes dans un ordre spécifié.

- Le diagramme 1 est planifié avec un déclencheur "Flowchart 1 run complete" qui est envoyé lorsque l'exécution réussit.
- Le diagramme 2 est planifié comme suit.
  - Démarre lors de la réception d'un déclencheur "Flowchart 1 run complete".
  - Envoie un déclencheur "Flowchart 2 complete" lorsque l'exécution réussit.
- Le diagramme 3 est planifié pour démarrer lors de la réception d'un déclencheur "Flowchart 2 run complete".

A propos des déclencheurs de début

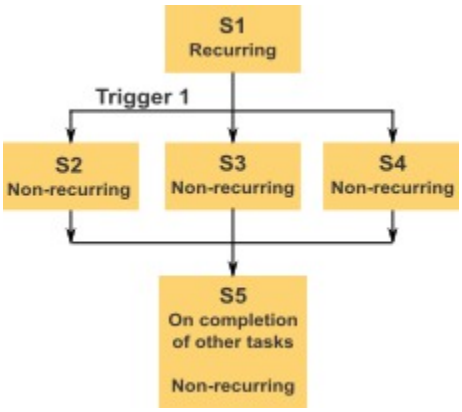
Une planification configurée avec un déclencheur de début commence à écouter un déclencheur dès qu'il est créé, quelle que soit la date de début. Toutefois, le déclencheur ne remplace pas la date de début. Par exemple, si la date de début d'une planification est le 12 décembre 2016 et qu'elle reçoit son déclencheur de début le 5 décembre 2016, l'exécution ne démarre pas avant le 12 décembre 2016.

Planifications dépendant de l'achèvement de plusieurs exécutions

Vous pouvez configurer une planification de manière à ce qu'elle s'exécute uniquement lorsque l'exécution de plusieurs autres planifications est terminée à l'aide de l'option **Lorsque d'autres tâches s'achèvent** dans la liste déroulante **Quand démarrer**.

Par exemple, supposons que vous avez une planification S1 qui est configurée à l'aide d'un modèle de récurrence. S1 dispose d'un déclencheur envoyé chaque fois

que l'exécution de S1 aboutit. Trois planifications, S2, S3 et S4, sont configurées pour démarrer lorsqu'elles reçoivent le déclencheur sortant de S1. Vous pouvez définir une planification supplémentaire, S5, qui s'exécute lorsque S2, S3 et S4 aboutissent. S5 s'exécute uniquement lorsque les trois exécutions dont elle dépend aboutissent. Le diagramme suivant illustre cet exemple :



Pour configurer un scénario tel que celui décrit dans l'exemple, configurez S5 à l'aide de l'option **Lorsque d'autres tâches s'achèvent** dans la liste déroulante **Quand démarrer**.

Lorsque vous configurez de cette manière une exécution de sorte qu'elle dépende d'autres exécutions vous devez prendre en considération les remarques suivantes :

- Les planifications dont dépend la planification que vous configurez doivent être non récurrentes. Dans l'exemple ci-dessus, S2, S3 et S4 doivent être non récurrentes. Cependant, étant donné que S1 se reproduit, S2, S3 et S4 se reproduisent, en fonction des exécutions de S1.
- La planification qui dépend d'autres planifications doit également être non récurrente. Dans l'exemple, S5 doit être non récurrente. Une fois encore, étant donné que S1 se reproduit, S5 se reproduit également.
- La planification qui dépend d'autres planifications ne peut pas être utilisée comme l'un des critères de l'option **Lorsque d'autres tâches s'achèvent** pour toute autre planification. Dans l'exemple, S5 ne peut pas servir de critère dans l'option **Lorsque d'autres tâches s'achèvent** pour toute autre planification.

- Avant de pouvoir supprimer une planification configurée à l'aide de l'option **Lorsque d'autres tâches s'achèvent**, vous devez changer la configuration pour supprimer l'option **Lorsque d'autres tâches se terminent**. Vous pouvez ensuite supprimer la planification.

Planification des déclencheurs envoyés à partir d'un script externe

Le planificateur Unica peut répondre aux déclencheurs envoyés par une application externe. L'utilitaire `scheduler_console_client` active cette fonctionnalité. Il émet des déclencheurs qui peuvent lancer une ou plusieurs planifications configurées pour être à l'écoute de ce déclencheur.

Comme `scheduler_console_client` est une application de script de traitement par lots, il peut être appelé par des applications externes, utilisant éventuellement un autre script de traitement par lots.

Par exemple, si vous configurez une planification qui est à l'écoute d'un "T1", vous pourrez exécuter l'utilitaire `scheduler_console_client` avec la commande suivante pour envoyer T1 : `scheduler_console_client.bat -v -t T1`

L'utilitaire peut :

- fournir la liste des planifications qui sont configurées pour être à l'écoute de n'importe quel déclencheur donné
- indiquer si le déclencheur a été envoyé avec succès. Notez que l'utilitaire est incapable de signaler si la planification qui est à l'écoute du déclencheur s'est exécutée de manière satisfaisante. Ces informations sont disponibles dans les pages de gestion du planificateur.

Vous ne pouvez pas utiliser cet utilitaire pour configurer une planification afin qu'elle se mette à l'écoute d'un déclencheur ou qu'elle modifie un déclencheur pour lequel une planification est à l'écoute. Vous devez effectuer les actions suivantes dans l'interface utilisateur du planificateur :

Exemple de script

Voici un exemple de script qui provoque l'affichage de la chaîne "example_trigger" par l'utilitaire `scheduler_console_client`. Ce déclencheur désactive l'exécution d'une planification configurée pour écouter "example_trigger".

Vous pouvez appeler un script tel que celui-ci à partir d'une application externe lorsque cette application génère un événement.

Cet exemple de script suppose que le script se trouve dans le même répertoire que l'utilitaire.

```
@rem**************************************************
@rem This script is used to call the Platform
@rem scheduler_console_client.
@rem**************************************************

echo Now starting scheduler trigger.
set JAVA_HOME=c:\jdk15_12
call scheduler_console_client.bat -v -t example_trigger

@rem**************************************************
```

Considérations relatives à la sécurité

La planification dans des applications d'entreprise est considérée comme une activité d'administrateur. On part du principe qu'un utilisateur disposant du droit d'exécution dans le système d'exploitation hôte pour l'utilitaire `scheduler_console_client` est également autorisé à émettre des déclencheurs.

Pour empêcher un utilisateur d'émettre un déclencheur à l'aide de cet utilitaire, vous devez révoquer le droit d'exécution de l'utilitaire `scheduler_console_client` pour cet utilisateur.

Modèles de récurrence du planificateur

Vous pouvez configurer l'exécution récurrente d'une planification. Pour ce faire, configurez un modèle de récurrence. Le modèle de récurrence défini démarre après l'heure de début spécifiée.

Il existe plusieurs options de modèle de récurrence.

- Prédéfini : ensemble de modèles de récurrence communs à partir duquel vous pouvez effectuer la sélection
- xpression Cron : chaîne composée de 6 ou 7 zones séparées par un blanc, qui représente un jeu de données temporelles
- Modèle de récurrence personnalisé simple : interface utilisateur permettant de créer des modèles de récurrence, identique à de nombreux planificateurs de réunion

Tous les modèles de récurrence du planificateur se basent sur les expressions cron. Le planificateur fournit des modèles prédéfinis dans l'interface utilisateur afin de faciliter la création de ces expressions cron. Si vous écrivez une expression cron personnalisée, il est recommandé de fournir une description pertinente du modèle de récurrence, afin de faciliter la compréhension du modèle pour les personnes peu familiarisées avec la lecture de ces expressions.

Important : Tous les modèles de récurrence se réinitialisent à la fin du plus long intervalle suivant. Par exemple, si vous définissez l'exécution d'un modèle hebdomadaire personnalisé toutes les trois semaines, il s'exécute la troisième semaine de chaque mois, car le modèle se réinitialise à la fin de chaque mois. Il s'agit d'une caractéristique partagée par toutes les expressions cron. Pour définir l'exécution d'une planification les semaines 3, 6, 9, 12, etc., vous devez créer des planifications séparées pour chaque date d'exécution souhaitée.

Prise en charge des fuseaux horaires

Vous pouvez planifier les exécutions de sorte qu'elles se produisent dans le contexte d'un des nombreux fuseaux horaires dans le monde.

Lors de la création d'une planification, la valeur par défaut correspond toujours au fuseau horaire du serveur sur lequel Unica Platform est installé. Cependant, vous pouvez sélectionner n'importe quel autre fuseau horaire dans la liste déroulante **Sélectionner un fuseau horaire**. Ces options sont exprimées en heures GMT, suivies du le terme couramment utilisé pour ce fuseau horaire. Par exemple, (GMT-08:00) Îles Pitcairn ou (GMT-08:00) Heure du Pacifique (Etats-Unis et Canada).

Le fuseau horaire sélectionné est appliqué à tous les aspects de la planification, y compris les suivants :

- Informations affichées sur les onglets Planifications et Exécutions
- Modèles de récurrence et déclencheurs

Régulation du planificateur

La régulation permet de gérer les performances lorsqu'un grand nombre de processus sollicitent les ressources du système. La régulation se base sur les groupes du planificateur, que vous configurez dans la page **Paramètres > Configuration**. Vous affectez un seuil de régulation à un groupe, puis associez des planifications à ce groupe.

Le seuil de régulation est le plus grand nombre d'exécutions associées à ce groupe qui peuvent être lancées de façon simultanée. Pour réduire l'utilisation des ressources du serveur, vous pouvez réduire le seuil de régulation. Seules les planifications créées dans Unica Scheduler font l'objet d'une régulation.

Seuil illimité dans le groupe par défaut

Toutes les planifications doivent appartenir à un groupe de régulation. Si vous ne souhaitez pas activer la régulation pour une planification, définissez-la comme membre du groupe Planificateur par défaut (option sélectionnée par défaut dans la zone **Groupe du planificateur** lorsque vous créez une planification). Ce groupe possède un seuil de régulation élevé, ce qui signifie qu'aucune régulation n'est définie.

Exception de régulation

Si vous exécutez un diagramme à partir de Unica Campaign ou de l'aide de Unica Campaign `unica_svradm`, ces exécutions ne sont pas comptabilisées dans le seuil de régulation et elles sont lancées immédiatement.

Exemples de régulation

- Si les ressources système constituent un problème, vous pouvez utiliser la régulation pour gérer la charge sur un serveur. Par exemple, si vous devez exécuter de nombreux diagrammes Unica Campaign complexes, vous pouvez les affecter à un groupe de régulation qui limite le nombre de diagrammes pouvant être exécutés en même temps. Cette régulation permet de gérer la charge du serveur Unica Campaign ou la base de données marketing.
- Vous pouvez utiliser la régulation pour définir les priorités des planifications. L'affectation de planifications de priorité haute à un groupe qui possède un seuil de régulation élevé garantit une exécution aussi efficace que possible des planifications à l'aide des ressources système. Vous devez affecter des planifications de priorité inférieure aux groupes qui possèdent des seuils de régulation inférieurs.
- Si un diagramme est planifié avec un modèle de récurrence, vous pouvez utiliser la régulation pour vous assurer que les exécutions sont effectuées de façon séquentielle et sans chevauchement. Par exemple, supposons que vous avez planifié un diagramme avec un modèle de récurrence défini pour lancer une exécution toutes les heures pendant 10 heures. Si le diagramme met plus d'une heure pour effectuer une exécution, l'exécution suivante peut tenter de commencer avant la fin de l'exécution précédente et générer un échec, car le diagramme en cours d'exécution serait verrouillé. Pour éviter cela, vous pouvez créer un groupe de régulation qui possède un seuil de `1`, puis affecter la planification du diagramme à ce groupe.

Configuration de la régulation pour le planificateur Unica

Vous devez configurer un groupe de régulation spécifiquement pour chaque type d'objet planifié.

1. Dans la page de configuration, naviguez vers l'un des modèles de groupe de régulation sous `Plateforme > Planificateur > Planifier les enregistrements > [Produit] > [Objet] > Groupe de régulation`.
2. Créez une catégorie depuis le modèle de groupe de régulation.

   La valeur affectée à la propriété `Seuil de régulation` correspond au nombre maximal d'exécutions simultanées associées à ce groupe. Les programmes dont l'exécution est possible qui dépassent le seuil de régulation sont mis en file d'attente pour être exécutés dans l'ordre dans lequel le planificateur reçoit les notifications.

   Les groupes de planificateurs configurés apparaissent dans la liste déroulante **Groupe du planificateur** de l'interface utilisateur du planificateur pour la création et le changement de planifications.

   Vous devez créer un groupe de régulation de chaque type d'objet dont vous souhaitez contrôler les exécutions de cette manière. Par exemple, les groupes de régulation de diagramme sont disponibles uniquement pour la planification de diagrammes et les groupes de régulation de mailing pour la planification de mailings.
3. Affectez un ou plusieurs programmes au groupe si nécessaire.

Configuration de liste blanche requise pour les tâches externes (avec le groupe de correctifs 10.0.0.1 seulement)

Une configuration de liste blanche requise doit être satisfaite pour les tâches externes que vous créez afin de planifier des appels API ou des scripts, uniquement si vous avez appliqué le groupe de correctifs de Unica Platform 10.0.0.1.

Pour pouvoir planifier une tâche externe, vous devez ajouter l'API ou le script à une liste blanche située dans le répertoire `conf` dans votre installation de Unica Platform.

Ajout d'un script à la liste blanche

Ne suivez cette procédure avant de créer des tâches externes planifiant un script que si vous avez appliqué le groupe de correctifs de Unica Platform 10.0.0.1.

Le script doit se trouver sur le serveur d'applications Web sur lequel Unica Platform est déployé.

1. Ouvrez le fichier de liste blanche pour les scripts dans un éditeur de texte.

   Le fichier de liste blanche pour les scripts s'appelle `Platform_Admin_Scheduler_Scripts.properties`. Ce fichier se trouve dans le répertoire `conf` dans votre installation de Unica Platform.
2. Entrez le chemin complet d'accès au script batch ou shell que vous prévoyez de planifier et incluez le nombre de paramètres qui sont utilisés dans le script que vous planifiez.

   Par exemple, imaginez que vous voulez planifier un script appelé `RunETLJobs.bat`, qui admet les trois paramètres suivants : username, password, db_table.

   Vous devez créer l'entrée ci-après dans le fichier de liste blanche. L'entrée inclut le chemin d'accès absolu au script, suivi d'un espace et du nombre de paramètres utilisés. Le nombre de paramètres doit correspondre exactement au nombre de paramètres utilisés dans le script planifié.

   ```
   C:\Scripts\RunETLJobs.bat 3
   ```

   Lorsque vous créez la planification, vous placez les noms de paramètre entre des dièses (##) suivis d'un espace dans la zone **Paramètres d'exécution**, conformément à l'exemple suivant :

   ```
   C:\Scripts\RunETLJobs.bat ##username## ##password##
   ##db_table##
   ```
3. Sauvegardez et fermez le fichier de liste blanche.

   A présent, vous pouvez planifier le script dans l'onglet Planifications de la page **Paramètres > Gestion des plannings**.

Ajout d'une API à la liste blanche

Ne suivez cette procédure avant de créer des tâches externes planifiant un appel API que si vous avez appliqué le groupe de correctifs de Unica Platform 10.0.0.1.

1. Ouvrez et éditez le fichier de liste blanche pour les API dans un éditeur de texte.

   Le fichier de liste blanche pour les API s'appelle `Platform_Admin_Scheduler_API.properties`. Il se trouve dans le répertoire `conf` dans votre installation de Unica Platform.
2. Entrez l'URI de l'API que vous prévoyez de planifier, et si des paramètres de requête sont utilisés, incluez leurs noms sans les valeurs.

   Par exemple, imaginez que vous voulez planifier l'appel API suivant, avec tous les paramètres de requête affichés :

   ```
   http://www.example.com/tickets?
   fields=id&state=open&sort=updated_at
   ```

   Vous devez créer l'entrée suivante dans le fichier de liste blanche, en répertoriant tous les paramètres :

   ```
   http://www.example.com/tickets?fields&state&sort
   ```

   Avec cette entrée de liste blanche, vous pouvez planifier des appels API qui utilisent une partie ou l'ensemble des paramètres répertoriés. Par exemple :

   - `http://www.example.com/tickets`
   - `http://www.example.com/tickets?fields=id`
   - `http://www.example.com/tickets?fields=id&state=open`
   - `http://www.example.com/tickets?fields=id&state=open&sort=updated_at`
   - `http://www.example.com/tickets?fields=id&sort=updated_at`
   - `http://www.example.com/tickets?fields=id&state=open`

   Les appels API qui utilisent des paramètres de requête non répertoriés ne peuvent pas être planifiés. La validation du planificateur échoue si des paramètres qui n'apparaissent pas dans la liste blanche sont utilisés.
3. Sauvegardez et fermez le fichier de liste blanche.

   A présent, vous pouvez planifier l'appel API dans l'onglet Planifications de la page **Paramètres > Gestion des plannings**.

Pratiques recommandées pour la configuration des planifications

Voici certaines des pratiques recommandées pour la planification et la configuration des exécutions planifiées des objets Unica.

Pour garantir des performances optimales et une certaine facilité de maintenance, gardez à l'esprit les instructions ci-après.

- Etant donné que les exécutions planifiées sont exécutées sur le système sur lequel le produit client est installé, tenez compte des capacités de mise à l'échelle du système client. Echelonnez les exécutions ou utilisez une limitation pour régler le système.
- Lorsque cela est possible, planifiez les travaux intensifs pendant les heures où les chargements système sont faibles.
- Evitez que les exécutions ne se chevauchent car cela génère des échecs d'exécution.
    - Soyez prudent si vous utilisez le même objet dans plusieurs planifications. Par exemple, si vous utilisez le diagramme F1 dans trois planifications, ces définitions de planification peuvent provoquer le démarrage d'une exécution avant la fin de l'exécution précédente et provoquer un échec d'exécution.
    - Si une exécution de diagramme est lancée manuellement ou par un script interne, la tentative suivante d'exécution du diagramme par quelque moyen que ce soit échoue avec une erreur de verrouillage si l'exécution précédente n'est pas terminée.
- Le planificateur crée de grandes quantités de données. Si vous constatez des problèmes de performances au niveau du planificateur, vous pouvez supprimer les définitions de planification devenues inutiles.

Important : La suppression d'une définition de planification entraîne celle de l'historique d'exécution associé dans la base de données.

Assistant de création d'une planification

Cette section décrit en détails les pages que vous utilisez lorsque vous créez une planification.

Le tableau suivant décrit les zones que vous utilisez lorsque vous planifiez l'exécution de diagrammes Unica Campaign, de mailings Unica Deliver, de sessions Unica Optimize, de scripts externes et d'appels de l'API.

Tableau 23. Zones de l'assistant de création d'une planification

Zone	Description
Sélection d'un type de tâche	Type d'objet à planifier. Les options suivantes sont disponibles. • **Tâche externe - script** Permet de planifier l'appel de tâches définies dans des scripts batch ou shell externes dans Unica. Le script doit être répertorié dans un fichier de liste blanche situé dans le répertoire `conf` dans votre installation de Unica Platform, uniquement si vous avez appliqué le groupe de correctifs de Unica Platform 1.0.0.1. De plus, le script doit se trouver sur le serveur d'applications Web sur lequel Unica Platform est déployé. • **Tâche externe - API** Permet de planifier l'appel d'API externes à Unica. L'API être répertoriée dans un fichier de liste blanche situé dans le répertoire `conf` dans votre installation de Unica Platform, uniquement si vous avez appliqué le groupe de correctifs de Unica Platform 1.0.0.1. • **Unica Campaign diagramme** Permet de planifier l'appel de diagrammes Unica Campaign. La sélection de cette option ouvre la page de liste Unica Campaign, dans laquelle vous pouvez sélectionner une campagne, éventuellement définir des paramètres de remplacement de diagramme et planifier l'exécution d'un diagramme. • **Unica Optimize session**

Tableau 23. Zones de l'assistant de création d'une planification (suite)

Zone	Description
	Permet de planifier l'appel de sessions Unica Optimize. La sélection de cette option ouvre la page de liste des sessions Unica Optimize, dans laquelle vous pouvez sélectionner une session et la planifier. • **Unica Deliver mailing** Permet de planifier l'appel de mailings Unica Deliver. La sélection de cette option ouvre la page de liste de mailings Unica Deliver, dans laquelle vous pouvez sélectionner et planifier le mailing. • **Unica Plan Désactivation en masse** Permet de planifier la désactivation en masse de projets dans Unica Plan. La sélection de cette option ouvre la page Paramètres d'administration de Unica Plan, dans laquelle vous pouvez cliquer sur **Administration des désactivations** et planifier la désactivation en masse. • **Alerte** Permet de planifier des alertes pour des utilisateurs d'Unica. La sélection de cette option ouvre une fenêtre dans laquelle vous pouvez définir le titre, le corps et la gravité du message. Lorsque vous cliquez sur **Planifier cette alerte**, vous pouvez créer une planification pour l'alerte. Les utilisateurs peuvent gérer leurs abonnements aux notifications en fonction de la gravité. • **Notification** Permet de planifier des notifications pour les utilisateurs d'Unica. La sélection de cette option ouvre une fenêtre dans laquelle vous pouvez définir le titre, le corps et la gravité du

Tableau 23. Zones de l'assistant de création d'une planification (suite)

Zone	Description
	message. Lorsque vous cliquez sur **Planifier cette notification**, vous pouvez créer une planification pour la notification. Les utilisateurs peuvent gérer leurs abonnements aux notifications en fonction de la gravité.
Nom du planning	Entrez un nom pour l'examen planifié.
Groupe de planificateurs	Si vous avez créé plusieurs groupes de régulation, vous pouvez associer cette planification à un groupe pour limiter le nombre d'exécutions de cette planification qui peuvent s'exécuter en même temps. Des groupes de régulation configurés dans la page Configuration sont proposés comme options dans cette zone.
Description	Saisissez la description de la planification.
Paramètres d'exécution	Utilisés lorsque vous planifiez des API et des scripts. Une configuration de liste blanche requise doit être satisfaite pour les tâches externes que vous créez afin de planifier des appels API ou des scripts, uniquement si vous avez appliqué le groupe de correctifs de Unica Platform 10.0.0.1. Pour pouvoir planifier une tâche externe, vous devez ajouter l'API ou le script à une liste blanche située dans le répertoire `conf` dans votre installation de Unica Platform. • Pour les planifications d'API, entrez l'URI ainsi que les paramètres de votre choix au format présenté dans les exemples. API sans paramètres : `http://example.com` API avec paramètres : `http://www.example.com/tickets?fields=id&state=open&sort=updated_at` Les jetons Unica Platform ne sont actuellement pas pris en charge dans l'identificateur URI.

Tableau 23. Zones de l'assistant de création d'une planification (suite)

Zone	Description

	• Pour les planifications de script, entrez le chemin d'accès complet au script sur le serveur Unica Platform, ainsi que les paramètres de votre choix au format présenté dans les exemples. Placez les noms de paramètre entre des dièses (##) suivis d'un espace.
	◦ Windows™ exemples
	Script sans paramètres : `C:\Scripts\ExecuteDatabaseJob.bat`
	Script avec paramètres :
	`C:\Scripts\RunETLJobs.bat ##username## ##password## ##db_table##`
	◦ UNIX™ exemples
	Script sans paramètres : `/opt/ExecuteDatabaseJob.sh`
	Script avec paramètres :
	`/opt/RunETLJobs.sh ##username## ##password## ##db_table##`
	L'exécution de ces tâches est asynchrone. Unica Platform ne contrôle pas le succès ou l'échec des tâches de script et d'API. Le statut indique uniquement si les tâches ont été lancées avec succès.

En cas de succès, envoyer un déclencheur	Si vous souhaitez que des exécutions de cette planification envoient un déclencheur en cas de succès, saisissez le texte du déclencheur ici. D'autres planifications peuvent être définies pour écouter ce déclencheur.

Tableau 23. Zones de l'assistant de création d'une planification (suite)

Zone	Description
En cas d'erreur, envoyer un déclencheur	Si vous souhaitez que des exécutions de cette planification envoient un déclencheur en cas de d'erreur, saisissez le texte du déclencheur ici. D'autres planifications peuvent être définies pour écouter ce déclencheur.
Balises/Mots clés de recherche	Entrez les balises que vous souhaitez associer à la planification pour les utiliser dans des recherches. Séparez les entrées par une virgule.
Statut du planning	Indique si la planification est activée ou désactivée. La désactivation d'une planification s'applique uniquement à ses exécutions futures ou en file d'attente. Les exécutions en cours ne sont pas affectées. Le statut par défaut est **Activé**.
Sélectionner le fuseau horaire	Si vous sélectionnez une option autre que l'option par défaut du serveur, les colonnes **Début**, **Fin** et **Dernière mise à jour** de la page Gestion de la planification affichent à la fois l'heure par défaut du serveur et l'heure dans la zone sélectionnée.
Quand démarrer	Sélectionnez l'une des options suivantes pour spécifier la première exécution de la planification. L'heure de début ne s'applique qu'à la première exécution. Elle définit l'heure à laquelle une planification peut s'exécuter pour la première fois. La première exécution réelle peut se produire après la date de début si l'une des conditions suivantes existe : • La planification est configurée pour l'attente d'un déclencheur. • La planification est membre d'un groupe de régulation. • La planification utilise un modèle de récurrence.

Tableau 23. Zones de l'assistant de création d'une planification (suite)

Zone	Description
	• **Maintenant** • **Selon l'horodatage** : sélectionnez une date et une heure. • **Selon le trigger** : sélectionnez un trigger existant ou entrez-en un nouveau. Si vous en définissez un nouveau, vous devez configurer une planification pour envoyer cette même chaîne en cas de réussite ou d'erreur. • **Selon le trigger après la date** : sélectionnez un trigger existant ou entrez-en un nouveau et sélectionnez une date et une heure. Si vous en entrez un nouveau, vous devez configurer une planification pour envoyer cette même chaîne en cas de réussite ou d'échec. • **Lorsque d'autres tâches s'achèvent** : sélectionnez à partir d'une liste de planifications existantes. La planification s'exécute uniquement lorsque les autres planifications sélectionnées ont terminé leur exécution.
Nombre d'exécutions	Sélectionnez l'une des options suivantes pour spécifier le nombre d'exécutions. • **Exécuter une fois seulement** : la planification ne s'exécute qu'une seule fois. Son exécution peut démarrer à la date et à l'heure de début spécifiées. • **Arrêter après n occurrences** : les exécutions s'arrêtent après le nombre d'exécutions spécifié (en cas d'échec ou de réussite) ou une fois la date de fin atteinte. • **Arrêter selon l'horodatage** : les exécutions sont lancées le nombre de fois défini, jusqu'à ce que la date et l'heure de fin spécifiées soient atteintes. Une exécution peut être lan-

Tableau 23. Zones de l'assistant de création d'une planification (suite)

Zone	Description
	cée après l'arrêt si l'exécution a été retardée en raison de contraintes de régulation. • **Lorsque d'autres tâches s'achèvent** : la planification ne s'exécute que lorsque toutes les autres tâches sélectionnées pour cette option aboutissent. Lorsque vous cliquez sur le bouton **Set up recurrences**, vous pouvez sélectionner l'une des options suivantes. • **Utiliser un modèle de récurrence prédéfini** : sélectionnez un modèle dans la liste. Unica Platform fournit un ensemble de modèles prédéfinis. Vous pouvez également créer vos propres modèles en ajoutant des propriétés dans la page de configuration. • **Utiliser un modèle de récurrence personnalisé simple** : sélectionnez un intervalle. • **Utiliser une expression de récurrence Cron** : entrez une expression Cron valide.

Exécuter les exclusions

10.0.0.2 Depuis la version 10.0, groupe de correctifs 2, vous pouvez créer des règles d'exclusion pour exclure l'exécution du planificateur pour certains jours ou heures. Vous pouvez ajouter plusieurs règles pour diverses planifications.

Vous pouvez créer des règles d'exclusion pour des planifications spécifiques ou appliquer une même règle à plusieurs planifications. Vous pouvez également activer ou désactiver les règles, ou supprimez les règles d'exclusion si elles ne sont plus requises.

La fonctionnalité d'exécution d'exclusions est disponible lorsque vous effectuez une mise à niveau vers la version 10.0, groupe de correctifs 2.

Deux nouvelles tables système ont été introduites pour cette fonctionnalité. Pour plus de détails sur les tables système, reportez-vous au document Unica Platform - Tables système.

Affichage des règles d'exclusion

Les règles d'exclusions déjà définies pour des planifications peuvent être affichées à partir de l'onglet d'exécution d'exclusions de la page Gestion des planifications.

Les informations de la zone **Exécution précédente et deux suivantes** sont affichées conformément à la définition du planificateur. Elles ne sont actuellement pas validées par rapport aux règles d'exclusion.

Pour afficher les règles d'exclusion, procédez comme suit :

1. Connectez-vous à Unica Platform en tant qu'administrateur.
2. Cliquez sur **Paramètres > Gestion des planifications**.
3. Cliquez sur l'option d'**exécution d'exclusions**.

Vous pouvez afficher les règles d'exclusion et effectuer diverses tâches pour les règles. Vous pouvez également afficher le statut des règles, les diverses planifications auxquelles elles s'appliquent, la période d'exclusion et le type d'exclusion des règles.

Vous pouvez également rechercher des règles d'exclusion à l'aide d'une recherche générique dans la zone de texte **Filtre**.

Ajout de règles d'exclusion

Des règles d'exclusion peuvent être ajoutées pour des planifications et des exécutions. Vous pouvez ajouter des règles absolues ou relatives et sélectionner les planifications auxquelles les règles s'appliqueront.

Les règles d'exclusion absolues sont définies pour une période spécifique. Les règles d'exclusion relatives ne sont définies qu'une seule fois et sont limitées à une fois par an. Depuis la version 11.0, en plus de la date relative annuelle, l'horodatage hebdomadaire et mensuel peut être configuré. Les règles d'exclusion peuvent être activées ou désactivées, et être appliquées à plusieurs planifications.

Pour ajouter une règle d'exclusion, procédez suit :

1. Connectez-vous à Unica Platform en tant qu'administrateur.
2. Cliquez sur **Paramètres > Gestion des planifications**.
3. Dans l'onglet d'**exécution d'exclusions**, cliquez sur l'option permettant d'**ajouter une règle d'exclusion**.
4. Dans l'onglet **Définition de règle**, spécifiez le **Nom de la règle**.
5. **Facultatif :** Spécifiez la **description**.
6. Pour le **statut de la règle**, sélectionnez **Activé** ou **Désactivé**.

   Par défaut, **Activé** est sélectionné.
7. Sélectionnez le **type d'exclusion**.

   Si vous sélectionnez Absolue, procédez comme suit :
   a. Sélectionnez le **Fuseau horaire**.

      Par défaut, le fuseau horaire par défaut du serveur est sélectionné.
   b. Sélectionnez **la date et l'heure de début**.
   c. Sélectionnez **la date et l'heure de fin**.

   Si vous sélectionnez **Relative**, procédez comme suit :
   a. Sélectionnez le Fuseau horaire. Par défaut, le fuseau horaire par défaut du serveur est sélectionné.
   b. Sélectionnez le moment où vous voulez démarrer. 1.Maintenant 2.Selon l'horodatage : sélectionnez une date et une heure.
   c. Configuration du modèle de récurrence pour définir l'exclusion d'exécution relative. Le modèle de récurrence défini démarre après l'heure de début et de fin spécifiées. Les modèles de récurrence disponibles sont les suivants : 1.Un utilisateur hebdomadaire doit être en mesure de sélectionner un ou plusieurs jours de la semaine, associés à une heure de début et de fin. 2.Un utilisateur mensuel doit être en mesure de sélectionner un jour d'un mois, associé à une heure de début et de fin. 3.Un utilisateur annuel doit être en mesure de sélectionner un jour de l'année, associé à une heure de début et de fin.

d. Sélectionnez Arrêter après n occurrences : la règle d'exclusion d'exécution relative s'arrête après le nombre d'exécutions spécifié (en cas d'échec ou de réussite).
e. Sélectionnez Arrêter selon l'horodatage : la règle d'exclusion d'exécution relative est lancée le nombre de fois défini, jusqu'à ce que la date et l'heure de fin spécifiées soient atteintes.

Remarque : il n'est possible de sélectionner qu'une seule date de l'année en cours. Les planifications sont ignorées pour toute la journée si vous sélectionnez une date relative.

8. Dans l'onglet de **planifications éligibles**, sélectionnez la planification pour laquelle vous souhaitez appliquer la règle d'exclusion, de la manière suivante :

   a. Recherchez les planifications disponibles en entrant une recherche générique dans la zone de texte **Filtre**.

   b. Dans les **planifications disponibles**, sélectionnez les planifications.

   c. Cliquez sur >>.

      Les planifications sélectionnées sont déplacées vers la table des **planifications sélectionnées**.

   d. Cliquez sur **Sauvegarder**.
9. Cliquez sur **Sauvegarder**.

Suppression de règles d'exclusion

Vous ne pouvez supprimer les règles d'exclusion disponibles sur votre système que si les règles ne sont pas associées à des planifications ou des exécutions.

Pour supprimer une règle d'exclusion, procédez comme suit :

1. Dans l'onglet d'**exécution d'exclusions**, sélectionnez la règle à supprimer.

   Remarque : Vérifiez que la règle d'exclusion à supprimer n'est associée à aucune planification ou exécution.

2. Cliquez sur **Supprimer**.
3. Confirmer la suppression.

Activation et désactivation des règles d'exclusion

Vous pouvez activer et désactiver des règles d'exclusion lorsque vous créez les règles ou après. Par défaut, une nouvelle règle créée est toujours activée.

Si des règles d'exclusion appliquées à des planifications sont désactivées, toutes les exécutions des planifications se poursuivent comme auparavant. Si les règles d'exclusion sont activées, elles sont appliquées aux planifications et ces dernières sont exécutées conformément aux critères d'exclusion appliqués.

Pour activer ou désactiver une règle d'exclusion, procédez comme suit :

1. Dans l'onglet d'**exécution d'exclusions**, sélectionnez une règle désactivée.
2. Cliquez sur **Activer**.

   Le statut de la règle passe à Activé.
3. Pour désactiver une règle, sélectionnez une règle activée.
4. Cliquez sur **Désactiver**.

   Le statut de la règle passe à Désactivé.

Importation de règles d'exclusion

Vous pouvez importer des règles d'exclusion pour les appliquer à des planifications ou des exécutions sur le système. Vous pouvez importer ces règles par l'intermédiaire d'un fichier XML.

Le fichier XML au format spécifique doit être disponible pour pouvoir importer les règles d'exclusion. Le format du fichier XML est visible lorsque vous cliquez sur l'option permettant d'**importer des règles d'exclusion** dans l'interface utilisateur.

Un exemple de fichier de règles d'exclusion est fourni avec l'installation. Il est disponible dans le répertoire `<platform_home>\conf\` en tant que fichier `Exclusion_Rule.xml`.

Pour importer des règles d'exclusion, procédez comme suit :

1. Dans l'onglet d'**exécution d'exclusions**, cliquez sur l'option permettant d'**importer des règles d'exclusion**.
2. Utilisez le format fourni pour créer le fichier XML permettant d'importer les règles.
3. Cliquez sur **Parcourir** pour sélectionner le fichier.
4. Cliquez sur **Sauvegarder**.

Comprendre le fichier XML permettant d'importer des règles d'exclusion

Le fichier XML qui permet d'importer des règles d'exclusion contient certaines balises qui définissent les règles d'exclusion.

Balises du fichier XML

Le tableau ci-après répertoire les balises du fichier XML qui permettent d'importer des règles d'exclusion.

Tableau 24. Balises du fichier XML

Balise	Description
ruleName	Nom de la règle d'exclusion.
ruleDescription	Description de la règle d'exclusion.
ruleStartDate	Date à laquelle la règle d'exclusion démarre. Le format de la date doit être MM/JJ/AAAA.

Tableau 24. Balises du fichier XML (suite)

Balise	Description
ruleStartTime	Heure à laquelle la règle d'exclusion démarre. Le format de l'heure doit être HH:MM:SS.
ruleEndDate	Date à laquelle la règle d'exclusion se termine. Le format de la date doit être MM/JJ/AAAA.
ruleEndTime	Heure à laquelle la règle d'exclusion se termine. Le format de l'heure doit être HH:MM:SS.
SchedulerID	ID du planificateur sur lequel la règle d'exclusion doit être appliquée. Il est possible de spécifier plusieurs ID tâche de planificateur. Les ID des tâches de planificateur sont disponibles dans la table `USCH_TASK` de la base de données.
ruleStatus	Statut de la règle d'exclusion. La valeur peut être `Enabled` ou `Disabled`.

A l'aide des balises, vous pouvez définir plusieurs règles d'exclusion. Réutilisez les balises de règle et modifiez-les au besoin pour définir plusieurs règles.

Exemple de fichier XML permettant d'importer des règles d'exclusion

Un exemple de fichier XML permettant d'importer des règles d'exclusion est fourni aux utilisateurs afin que ces derniers puissent en modifier les valeurs et créer un nouveau fichier XML en fonction de leurs besoins.

Les balises XML suivantes peuvent être utilisées pour créer un fichier XML permettant d'importer des règles d'exclusion.

```
<rules>
 <rule>
  <ruleName>Rule1</ruleName><!-- specify rule name -->
```

```
 <ruleDescription>Rule for skipping 1/13 to 1/19.</ruleDescription><!--
specify rule description -->
 <ruleStartDate>1/13/2017</ruleStartDate><!-- specify exclusion start
date. This should be of format MM/DD/YYYY -->
 <ruleStartTime>8:00:00</ruleStartTime><!-- specify exclusion start time.
This should be of format HH:MM:SS-->
 <ruleEndDate>1/19/2017</ruleEndDate><!-- specify exclusion end date. This
should be of format MM/DD/YYYY -->
 <ruleEndTime>18:15:00</ruleEndTime><!-- specify exclusion end time. This
should be of format HH:MM:SS -->
 <SchedulerIDs>
  <SchedulerID>10</SchedulerID> <!-- specify scheduler task Ids, on which
this rule should get applied. This needs to be obtained from database. -->
  <SchedulerID>15</SchedulerID>
 </SchedulerIDs>
 <ruleStatus>Enabled</ruleStatus> <!-- specify exclusion rule status.
valid values Enabled/Disabled -->
</rule>
</rules>
<rules>
 <rule>
  <ruleName>Rule2</ruleName><!-- specify rule name -->
  <ruleDescription>Rule for skipping 2/6 to 2/10</ruleDescription><!--
specify rule description -->
  <ruleStartDate>2/6/2017</ruleStartDate><!-- specify exclusion start date.
This should be of format MM/DD/YYYY -->
  <ruleStartTime>00:00:00</ruleStartTime><!-- specify exclusion start time.
This should be of format HH:MM:SS-->
  <ruleEndDate>2/10/2017</ruleEndDate><!-- specify exclusion end date. This
should be of format MM/DD/YYYY -->
  <ruleEndTime>23:59:59</ruleEndTime><!-- specify exclusion end time. This
should be of format HH:MM:SS -->
```

```
  <SchedulerIDs>
   <SchedulerID>45</SchedulerID> <!-- specify scheduler task Ids, on which
 this rule should get applied. This needs to be obtained from database. -->
   <SchedulerID>88</SchedulerID>
  </SchedulerIDs>
  <ruleStatus>Disabled</ruleStatus> <!-- specify exclusion rule status.
 valid values Enabled/Disabled -->
 </rule>
</rules>
```

Eléments à prendre en compte lors de l'utilisation du planificateur avec Unica Campaign

Une configuration spéciale s'applique lorsque vous utilisez le planificateur Unica avec Unica Campaign

- Le démarrage manuel des exécutions de diagramme ou les commandes de diagramme de ligne de commande n'ont pas d'impact sur le planificateur et inversement, sauf dans le cas suivant. Si une exécution de diagramme est lancée par n'importe quel moyen, la tentative suivante d'exécution du diagramme par n'importe quel moyen échoue avec une erreur de verrouillage si l'exécution précédente n'est pas terminée.
- Les déclencheurs du planificateur n'interagissent en aucune manière avec les déclencheurs de diagramme de Unica Campaign. Les déclencheurs envoyés par le processus de planification ou par l'utilitaire de déclenchement Unica Campaign `unica_actrg` ne peuvent pas déclencher l'exécution des planifications dans le planificateur Unica et inversement.

Différence entre le processus de planification d' Unica Campaign et Unica Scheduler

Avec la sortie de la révision 8.0 de Unica Platform, Unica Scheduler, remplace le processus de planification de Unica Campaign pour la planification des exécutions d'un diagramme

complet. Unica Scheduler est plus efficace, car il n'utilise aucune ressource serveur lorsque le diagramme est inactif.

Unica Scheduler démarre un diagramme même s'il n'est pas en cours d'exécution, tandis que le processus de planification de Unica Campaign ne fonctionne que si le diagramme est en cours d'exécution.

Le processus de planification de Unica Campaign est conservé à des fins de compatibilité complète avec les versions antérieures et pour les situations non gérées par Unica Scheduler. Par exemple, vous pouvez être amené à utiliser le processus de planification de Unica Campaign pour envoyer des déclencheurs de Unica Campaign ou pour retarder l'exécution des processus dépendants.

N'utilisez pas Unica Scheduler pour planifier un diagramme qui utilise le processus de planification de Unica Campaign en tant que processus de haut niveau qui démarre l'exécution d'un diagramme. En règle générale, vous n'avez besoin que de l'un ou de l'autre. Toutefois, si le processus de planification apparaît dans un diagramme démarré par Unica Scheduler, il fonctionne conformément à sa configuration. Les conditions requises par Unica Scheduler et le processus de planification doivent donc être respectées avant l'exécution des processus suivants.

A la différence d'Unica Scheduler, le processus de planification de Unica Campaign peut envoyer des déclencheurs externes pour appeler des scripts en ligne de commande. Unica Scheduler ne peut envoyer de déclencheurs qu'à ses propres planifications.

Droits d'accès à la planification des diagrammes

La planification de diagrammes Unica Campaign en utilisant Unica Scheduler nécessite les autorisations suivantes.

Tableau 25. Droits d'accès à la planification

Autorisation	Description
Planifier diagrammes de traitement par lots	Permet de planifier les diagrammes à l'aide de paramètres d'exécution par défaut

Tableau 25. Droits d'accès à la planification (suite)

Autorisation	Description
Planifier remplacement diagrammes de traitement par lots	Permet de remplacer les paramètres d'exécution par défaut pour la planification des diagrammes
Exécuter diagrammes de traitement par lots	Permet d'exécuter des diagrammes (nécessaire pour la bonne exécution des diagrammes planifiés)

Remarque : Un diagramme planifié est exécuté par l'utilisateur de Unica Platform qui a créé la tâche planifiée. Si ce compte utilisateur est activé ou supprimé, l'exécution des diagrammes précédemment planifiés par ce serveur échouera.
Si vous voulez désactiver ce compte utilisateur, mais autoriser l'exécution des diagrammes précédemment planifiés, maintenez le statut du compte utilisateur sur "actif" avec uniquement le droit d'accès Exécuter diagrammes de traitement par lots.

Création d'une planification de diagramme à l'aide des paramètres par défaut

Procédez comme suit pour planifier un diagramme à l'aide des paramètres par défaut.

1. Dans l'onglet **Diagramme** en mode **Vue**, cliquez sur l'icône **Planifications** et sélectionnez **Planifier**. Cela permet d'ouvrir la fenêtre Remplacer les paramètres du diagramme. Tous les paramètres de cet écran sont facultatifs.
2. Cliquez sur le bouton **Planifier une exécution** dans le panneau inférieur. Une fenêtre s'ouvre pour que vous puissiez planifier un diagramme à l'aide des paramètres par défaut.
3. Complétez les zones de la boîte de dialogue **Planifier un diagramme**. Si vous choisissez d'exécuter le diagramme à plusieurs reprises, cliquez sur **Définir les récurrences** pour définir un modèle de récurrence.
4. Cliquez sur **Exécuter** selon cette planification.

Remplacement des paramètres par défaut des planifications d'exécution des diagrammes Unica Campaign

Vous pouvez remplacer les paramètres par défaut d'exécution lorsque vous planifiez une exécution de diagramme.

Lorsque vous planifiez une exécution de diagramme Unica Campaign, le planificateur utilise les paramètres d'exécution par défaut définis pour le diagramme. Ces paramètres incluent les éléments suivants :

- Catalogue de tables contenant les mappages de tables utilisés par le diagramme.
- Variables utilisateur définies dans le diagramme.
- Informations de connexion des sources de données auxquelles accède le diagramme. Par défaut, il s'agit de l'utilisateur qui planifie le diagramme.

Unica Campaign vous permet de remplacer ces valeurs par défaut afin de lancer une exécution dans différentes sources de données ou d'obtenir d'autres résultats, comme le permet l'utilitaire `unica_svradm`. Par exemple, vous pouvez planifier plusieurs exécutions d'un même diagramme afin de tester différentes combinaisons de valeurs dans les variables utilisateur. Vous pouvez spécifier un autre catalogue de tables afin de basculer de votre base de données de production à un exemple de base de données dans le cadre de ces exécutions en test. Si votre organisation a besoin de différentes connexions à la base de données dans le cadre des exécutions en test et des exécutions en production, vous pouvez spécifier les informations de connexion appropriées.

Paramètres d'exécution de la planification des diagrammes Unica Campaign

Si vous planifiez un diagramme Unica Campaign, le diagramme peut passer une chaîne comportant des paramètres d'exécution à Unica Scheduler. Cette chaîne est ensuite repassée à Unica Campaign au début d'une exécution.

Dans Unica Campaign, toutes les valeurs définies dans la boîte de dialogue **Remplacer les paramètres de diagramme** sont envoyées au planificateur dans une seule chaîne. Cette chaîne s'affiche dans la zone **Paramètres d'exécution**.

Création d'une planification de diagramme

Pour planifier un diagramme, procédez comme suit.

1. Dans un onglet de diagramme en mode **Vue**, cliquez sur l'icône **Planifications** et sélectionnez **Planification**.

   La boîte de dialogue Remplacer les paramètres de diagramme s'affiche.
2. Si vous souhaitez remplacer les paramètres de diagramme par défaut, renseignez les zones de la boîte de dialogue pour indiquer vos paramètres de diagramme. Cette étape est facultative.

   Vous pouvez ajouter plusieurs variables utilisateur et sources de données en cliquant sur les liens **Ajouter variable utilisateur** et **Ajouter source de données**.

   Le système ne vérifie pas la syntaxe des paramètres que vous entrez dans ces zones. Assurez-vous de saisir les valeurs correctes avant de poursuivre la procédure.

   Si vous ne souhaitez pas remplacer les paramètres de diagramme par défaut, passez à l'étape suivante.
3. Cliquez sur **Planifier une exécution** pour ouvrir la boîte de dialogue Création d'un planning.

   Vous pouvez définir le moment de l'exécution de la planification et éventuellement configurer les récurrences, les déclencheurs et la régulation.
4. Cliquez sur **Exécuter selon cette planification**.

Important : Lorsque vous planifiez un diagramme, la tâche planifiée est basée sur le nom dudit diagramme. Si vous modifiez le nom du diagramme après avoir créé une tâche planifiée, l'exécution de cette dernière échoue.

Page Remplacer les paramètres du diagramme

Le tableau suivant décrit les zones de la boîte de dialogue Remplacer les paramètres de diagramme. Toutes les zones modifiables de cette boîte de dialogue sont facultatives. Le système ne vérifie pas la syntaxe des paramètres que vous entrez dans ces zones. Assurez-vous de saisir les valeurs correctes avant de poursuivre la procédure.

Les valeurs que vous entrez dans cette boîte de dialogue sont affichées sur la page suivante de l'assistant dans la zone **Paramètres d'exécution**.

Tableau 26. Zones de la page Remplacer les paramètres du diagramme

Zone	Description
ID de diagramme	ID unique du diagramme. Cette zone en lecture seule est automatiquement renseignée.
Campagne - Nom du diagramme	Nom de campagne, code de campagne et nom du diagramme. Cette zone en lecture seule est automatiquement renseignée.
Nom du fichier catalogue	Spécifiez un fichier de catalogue des tables stockées à utiliser dans le cadre de cette exécution.
Nom de la variable utilisateur	Entrez le nom d'une variable utilisateur qui a été définie dans le diagramme.
Valeur	Entrez une valeur pour la variable utilisateur.
Nom de la source de données	Entrez le nom d'une source de données à laquelle le diagramme accède.
Connexion	Utilisez cette zone pour remplacer le nom de connexion par défaut de la source de données spécifiée. Par défaut, il s'agit du nom de connexion de l'utilisateur qui crée la planification.
Mot de passe	Utilisez cette zone pour remplacer le mot de passe par défaut de la source de données spécifiée. Par défaut, il s'agit du mot de passe de l'utilisateur qui crée la planification.

Notifications de planification

Vous pouvez configurer des notifications pour toute planification, afin d'être alerté du statut des exécutions planifiées. En outre, les utilisateurs ayant les droits Administrateur dans Unica Platform peuvent configurer les groupes auxquels sont envoyées les notifications.

Notifications de planifications individuelles

Vous pouvez créer des notifications pour vos planifications uniquement après avoir créé et sauvegardé la planification, et non pendant sa création. Vous pouvez configurer les statuts qui déclenchent une notification, et indiquer si les notifications de chaque planification sont envoyées à votre compte de courrier électronique, ou apparaissent dans votre boîte de notification, ou les deux.

Notifications de planifications de groupe

Si vous souhaitez que des utilisateurs autres que le créateur d'une planification reçoivent des notifications de planification, vous pouvez activer des notifications basées sur un groupe. Vous devez posséder les droits de l'administrateur dans Unica Platform pour configurer des notifications de groupe.

La propriété de configuration **Nom du groupe devant recevoir les notifications de travail** est incluse pour chaque type d'objet sous la catégorie **Platform | Planificateur | Planifier les enregistrements | [Produit] | [Type d'objet]** dans la page **Paramètres > Configuration**. Tous les membres du groupe spécifié dans cette propriété de configuration reçoivent des notifications pour toutes les planifications pour ce type d'objet (par exemple, les diagrammes Campaign).

Les membres du groupe reçoivent des notifications configurées pour les exécutions planifiées qui ont le statut **Longue durée** ou **Non démarré/placé en file d'attente**. Ils ne reçoivent pas de notifications pour les exécutions ayant le statut **Echec**, **Succès**, ou **Problème inconnu/autre**.

En ajoutant ou supprimant des utilisateurs dans un groupe, vous pouvez contrôler les destinataires de ces notifications.

Configuration des notifications pour les planifications vous créez

Utilisez cette procédure pour configurer des notifications pour les planifications que vous créez. Vous pouvez créer des notifications uniquement lorsqu'une planification a été créée et sauvegardée, et non pendant sa création.

1. Sélectionnez **Paramètres > Gestion de la planification** et cliquez sur le nom de la planification pour laquelle vous souhaitez configurer des notifications.
2. Cliquez sur **Editer des notifications de travaux** pour ouvrir la fenêtre Mes notifications de travaux, puis cliquez sur **Nouveau**.
3. Renseignez les zones et cliquez sur **Enregistrer**.

Suppression ou modification des notifications pour les planifications que vous créez

Vous pouvez supprimer ou modifier des notifications vous avez créées.

1. Sélectionnez **Paramètres > Mes notifications de travaux** pour ouvrir la fenêtre Mes notifications de travaux.
2. Pour supprimer des notifications, sélectionnez les notifications à supprimer et cliquez sur **Supprimer**.
3. Pour modifier des notifications, cliquez sur le nom de la notification à modifier pour ouvrir la fenêtre Editer une notification de travail, dans laquelle vous pouvez effectuer et sauvegarder les modifications.

Configuration de notifications de planifications pour un groupe d'utilisateurs

Utilisez cette procédure pour configurer des notifications pour toutes les planifications envoyées aux groupes d'utilisateurs que vous spécifiez. Vous devez posséder les droits de l'administrateur dans Unica Platform pour exécuter cette procédure.

1. Sur la page **Paramètres > Configuration**, accédez à la catégorie **Unica Platform | Planificateur | Planifier les enregistrements**.
2. Pour chaque type d'objet pour lequel vous souhaitez activer des notifications de groupe, définissez la valeur de la propriété **Nom du groupe devant recevoir les notifications de travail** sur le nom du groupe que vous avez configuré pour recevoir des notifications pour ce type d'objet.

   Vous pouvez utiliser des groupes existants ou créer des groupes pour ces notifications.

Vous pouvez souhaiter configurer un groupe pour chaque type d'objet pour lequel vous voulez activer des notifications basées sur les groupes.

3. Sur la page Groupes d'utilisateurs, affectez des utilisateurs au(x) groupe(s) spécifiés à l'étape précédente, comme nécessaire.

Page Mes notifications de travaux

Vous pouvez configurer des notifications planifiées sur la page Mes notifications de travaux.

Tableau 27. Zones de la page Mes notifications de travaux

Zone	Définitions
Titre de la notification	Entrez un nom pour la notification.
Condition	Sélectionnez la condition de statut qui entraîne l'envoi d'une notification. Vous pouvez créer une autre notification pour chaque statut qui doit déclencher une notification.
Envoyer la notification à	Sélectionnez le mode de réception de la notification. La notification peut être envoyée au compte de courrier électronique associé à votre compte utilisateur Unica, elle peut apparaître dans vos notifications de l'interface utilisateur, ou les deux.
Statut de notification	Sélectionnez si cette notification est active ou inactive. Si vous sélectionnez inactive, aucune notification n'est envoyée.

Gestion des plannings

Vous pouvez gérer toutes les planifications à partir de la page **Paramètres > Gestion de la planification**. Vous devez disposer du droit d'accès à Administration de la pages Tâches programmées dans Unica Platform pour gérer les planifications.

Voici les onglets composant la page Tâches planifiées.

- Planifications - dans cet onglet, vous pouvez créer des planifications et afficher ou supprimer des définitions de planification. Vous pouvez cliquer sur le nom de la planification pour modifier une définition, notamment ajouter des notifications et activer ou désactiver la planification.
- Exécutions - dans cette onglet, vous pouvez consulter les exécutions mises en file d'attente et terminées pour chaque planification, annuler une exécution mise en file d'attente, et supprimer une exécution. Vous pouvez cliquer sur le nom de la planification pour modifier une définition, notamment ajouter des notifications et activer ou désactiver la planification.

Planifications et partitions

Dans un environnement à partitions multiples, vous ne pouvez consulter que les planifications qui sont créées dans la partition à laquelle vous appartenez, à moins que vous ne disposiez du rôle PlatformAdminRole qui vous permet de consulter les exécutions planifiées de toutes les partitions.

Statut inconnu

S'il existe un grand nombre d'exécutions avec le statut Inconnu, vous pouvez régler la fréquence d'interrogation du planificateur en définissant la propriété **Platform | Planificateur | Nombre maximal d'interrogations de statut inconnu** dans la page **Paramètres > Configuration**. Cette propriété indique le nombre de fois que le planificateur vérifie le statut d'une exécution avant de signaler un statut Inconnu.

Le statut Inconnu indique que Unica Platform ne peut pas déterminer si le travail est encore en cours d'exécution, terminé, ou s'il a échoué.

Si votre organisation possède un grand nombre de travaux planifiés, l'augmentation de la fréquence d'interrogation peut affecter les performances.

Filtre de la liste des planifications

Vous pouvez filtrer la liste des planifications dans les onglets Exécutions et Planifications.

Vous pouvez entrer du texte dans la zone située dans la partie supérieure droite de la liste pour obtenir un filtre rapide qui compare votre terme de recherche aux valeurs de toutes

les colonnes de la liste. Si votre chaîne de recherche se trouve dans l'une des colonnes, la planification ou l'exécution est incluse au résultat de la recherche.

Pour une recherche avancée, cliquez sur **Edition du filtre de liste de plannings** pour ouvrir une fenêtre dans laquelle vous pouvez définir des critères à évaluer par rapport aux attributs des planifications ou des exécutions répertoriées.

Désactivation et activation de plusieurs planifications (avec le groupe de correctifs 10.0.0.1 seulement)

Si vous avez appliqué le groupe de correctifs de Unica Platform 10.0.0.1, vous pouvez sélectionner plusieurs planifications dans l'onglet Planifications, ou les désactiver ou les activer en cliquant sur le bouton **Désactiver** ou **Activer** en haut de la liste.

Vous pouvez utiliser cette fonction de désactivation et d'activation en bloc en conjonction avec le filtre afin d'obtenir la liste des planifications à désactiver ou activer. Par exemple, si vous avez ajouté des balises de recherche lors de la création des planifications, vous pouvez filtrer la liste pour n'afficher que les planifications comportant une balise spécifique. Ensuite, vous pouvez sélectionner toutes ces planifications et les désactiver ou les activer en un seul clic.

Lorsque vous désactivez une tâche planifiée, les planifications qui dépendent d'un déclencheur provenant de cette tâche désactivée ne sont pas désactivées, mais elles ne s'exécuteront pas car elles ne recevront pas le déclencheur.

Pages de gestion du planificateur

Vous accédez aux pages de gestion du planificateur en sélectionnant **Paramètres > Gestion des plannings** ou **Vue de la planification** dans le menu **Exécuter** d'un diagramme.

Onglet Planification

Tableau 28. Zones et liens de l'onglet Planifications

Zone ou lien	Description
 Désactiver	Désactivez une ou plusieurs planifications sélectionnées. Disponible uniquement si vous avez appliqué le groupe de correctifs de Unica Platform 10.0.0.1.
 Activer	Activez une ou plusieurs planifications sélectionnées. Disponible uniquement si vous avez appliqué le groupe de correctifs de Unica Platform 10.0.0.1.
Création d'un planning	Cliquez pour ouvrir un assistant dans lequel vous pouvez définir une planification.
Edition du filtre de liste de plannings	Cliquez pour créer un filtre avancé pour la liste.
Supprimer	Supprimez une ou plusieurs planifications sélectionnées. Vous pouvez sélectionner des planifications en cliquant sur la colonne située à gauche de la planification. Pour sélectionner toutes les planifications, cliquez en haut de la colonne de gauche.
Actualiser	Cliquez sur actualiser la liste.
Filtrer	Cliquez pour créer un filtre simple pour la liste.
Nom du planning	Planification dont l'exécution est une instance.
Etat du planning	Indique si la planification est activée ou désactivée.
Elément planifié	Nom de l'objet à exécuter.
Type d'élément	Type d'élément à exécuter.
Créé par	Nom de l'utilisateur du compte ayant créé la planification.

Tableau 28. Zones et liens de l'onglet Planifications (suite)

Zone ou lien	Description
Déclencheur de début	Si la planification dépend d'un déclencheur, déclencheur qui entraîne l'exécution de la planification.
Démarrer	Date et heure de planification de la première exécution de cette tâche.
Modèle de récurrence	Description du modèle de récurrence.
Mettre fin	Date et heure de la dernière exécution de cette tâche. **Remarque :** S'applique uniquement aux tâches planifiées.
Exécution précédente et deux suivantes	Date et heure de l'exécution précédente et des deux prochaines exécutions planifiées. **Remarque :** S'applique uniquement aux tâches planifiées. Les informations sur l'exclusion d'exécution précédente et les deux suivantes sont affichées conformément à la définition du planificateur. Elles ne sont actuellement pas validées par rapport aux règles d'exclusion.
Dépendances	Si l'objet planifié dépend d'autres objets, ils sont répertoriés ici.
Déclencheur en cas de succès	Chaîne renvoyée si le produit rapporte qu'une exécution de cette planification a réussi. Cette zone est en blanc si aucun déclencheur en cas de réussite n'est spécifié.
Déclencheur en cas d'échec	Chaîne renvoyée si le produit rapporte qu'une exécution de cette planification a échoué. Cette zone est en blanc si aucun déclencheur en cas d'échec n'est spécifié.

Onglet Exécutions

Tableau 29. Zones et liens de l'onglet Exécutions

Zone ou lien	Description
Edition du filtre de liste de plannings	Cliquez pour créer un filtre avancé pour la liste.
Supprimer	Supprimez une ou plusieurs planifications sélectionnées. Vous pouvez sélectionner des planifications en cliquant sur la colonne située à gauche de la planification. Pour sélectionner toutes les planifications, cliquez en haut de la colonne de gauche.
Marquer comme annulé	Annulez une ou plusieurs planifications sélectionnées.
Actualiser	Cliquez sur actualiser la liste.
Filtrer	Cliquez pour créer un filtre simple pour la liste.
ID exécution	Numéro d'identification affecté à l'exécution dans les tables système Unica Platform.
Nom du planning	Nom attribué à la planification par son créateur.
Elément planifié	Nom de l'objet à exécuter.
Type d'élément	Type d'élément à exécuter.
Démarrer	Date et heure auxquelles l'exécution est démarrée.
Dernière mise à jour	Date et heure auxquelles les informations relatives à cette exécution ont été mises à jour.
Etat d'exécution	Etat de l'exécution tel qu'il est défini dans le planificateur, comme suit.

Tableau 29. Zones et liens de l'onglet Exécutions (suite)

Zone ou lien	Description
	• **Planifiée** : l'exécution n'a pas commencé. • **En attente** : le planificateur a lancé l'exécution mais le produit Unica n'a pas commencé l'exécution planifiée en raison de contraintes de limitation. • **Terminée** : l'exécution s'est terminée et a renvoyé le statut Echec ou Réussi. • **Annulée** : un utilisateur a annulé une exécution en cliquant sur **Marquer comme annulé** sur la page Exécutions planifiées. Si l'exécution a été mise en file d'attente lorsque l'utilisateur l'a marquée comme annulée, elle ne s'exécute pas. Si l'exécution était en cours, cette action ne l'arrête pas, mais est marquée comme annulée et les déclencheurs éventuels configurés pour cette exécution ne sont pas envoyés. De même, les exécutions qui dépendent de celle annulée ne sont pas lancées. • **Inconnu** : indique que Unica Platform ne peut pas déterminer si le travail est encore en cours d'exécution, terminé, ou s'il a échoué.
Statut d'exécution	Etat de l'exécution de l'objet, tel que défini par le produit qui procède à l'exécution. Si l'exécution renvoie le statut Annulée et qu'elle est relancée ultérieurement et qu'elle renvoie un autre statut au planificateur, le statut est mis à jour dans cette zone.
Détails	Informations sur l'exécution, fournies par le produit. Par exemple, en ce qui concerne l'exécution d'un diagramme, les détails incluent le nom et l'ID du diagramme, l'erreur en cas d'échec de l'exécution et le temps écoulé en cas de réussite.

Edition du filtre de liste de plannings - Planifications

Tableau 30. Edition du filtre de liste de plannings dans l'onglet Planifications

Colonne	Description
Filtrer par balises/mots clés de recherche	Cochez cette case si vous souhaitez inclure des balises de recherche ou des mots clés à votre filtre. La chaîne que vous entrez ici est mise en correspondance avec les chaînes entrées dans les zones **Rechercher des balises / mots clés** lorsque des planifications sont créées.
Balises/Mots clés de recherche	Entrez les balises de recherche ou les mots clés que vous souhaitez utiliser dans votre filtre.
Filtrer sur d'autres critères	Cochez cette case si vous souhaitez inclure d'autres critères à votre filtre.
Exécution des métadonnées	Sélectionnez l'une des options suivantes à inclure à votre règle. Options disponibles : • **Nom du planning** • **Etat de la planification** • **Type d'élément** • **Créé(e) par** • **Elément planifié**
Condition	Sélectionnez l'une des options suivantes pour déterminer de quelle manière votre règle est évaluée. • **Correspond à** • **Commence par** • **Se termine par** • **Contient**

Tableau 30. Edition du filtre de liste de plannings dans l'onglet Planifications (suite)

Colonne	Description
Valeur	Entrez ou sélectionnez la valeur que vous souhaitez appliquer à la règle. Les options varient en fonction des métadonnées que vous sélectionnez pour la règle. • **Nom du planning** Entrez n'importe quels caractères. • **Etat de la planification** Les options de valeur sont **Activé** et **Désactivé**. • **Type d'élément** Les options de valeur sont les divers types de planification. • **Créé(e) par** Entrez n'importe quels caractères. Votre valeur est comparée avec les noms de connexion utilisateur. • **Elément planifié** Entrez n'importe quels caractères. La chaîne que vous entrez ici est comparée avec le texte de la colonne **Elément planifié**.
Et/Ou	Sélectionnez l'un de ces opérateurs pour chaque règle que vous créez.

Edition du filtre de liste de plannings - Runs

Tableau 31. Edition du filtre de liste de plannings dans l'onglet Runs

Colonne	Description
Filtre basé sur le temps	Cochez cette case si vous souhaitez afficher des exécutions qui se sont produites dans un intervalle de temps spécifié.
Fuseau horaire	Si vous sélectionnez une option autre que le serveur par défaut, la recherche utilise le fuseau horaire sélectionné pour calculer les pla-

Tableau 31. Edition du filtre de liste de plannings dans l'onglet Runs (suite)

Colonne	Description
	nifications qui sont comprises dans la plage de dates que vous spécifiez.
Afficher les exécutions pour les dernières instances n	Pour les exécutions récurrentes, indiquez le nombre d'exécutions précédentes à afficher dans la liste.
Afficher les exécutions de	Indiquez un intervalle de temps pour les exécutions affichées dans la liste.
Filtrer sur d'autres critères	Cochez cette case si vous souhaitez inclure d'autres critères à votre filtre.
Exécution des métadonnées	Sélectionnez l'une des options suivantes à inclure à votre filtre. Options disponibles : • **Nom du planning** • **Etat d'exécution** • **Statut d'exécution** • **Elément planifié**
Condition	Sélectionnez l'une des options suivantes pour déterminer de quelle manière vos critères sont évalués. • **Correspond à** • **Commence par** • **Se termine par** • **Contient**
Valeur	Entrez ou sélectionnez la valeur que vous souhaitez appliquer au filtre. Les options varient en fonction des métadonnées que vous sélectionnez pour la règle.

Tableau 31. Edition du filtre de liste de plannings dans l'onglet Runs (suite)

Colonne	Description
	• **Nom du planning** Entrez n'importe quels caractères. • **Etat d'exécution** Les options de valeurs sont : ◦ **Mis en file d'attente** ◦ **Exécution en cours** ◦ **Terminé** ◦ **Inconnu** ◦ **Annulé** • **Statut d'exécution** Les options de valeur sont **Réussi**, **En cours d'exécution**, **Annulé**,**Echec** et **Inconnu**. • **Elément planifié** Entrez n'importe quels caractères. La chaîne que vous entrez ici est comparée avec le texte de la colonne **Elément planifié**.
Et/Ou	Sélectionnez l'un de ces opérateurs pour chaque règle que vous créez.

Authentification fédérée basée sur SAML 2.0

Unica Platform implémente un fournisseur d'identité (IdP) basé sur SAML 2.0 qui active une fédération de connexion unique parmi les produits Unica ou entre les produits Unica et les applications tierces.

Une fédération est un groupe de fournisseurs d'identité et d'applications qui fonctionnent ensemble dans un environnement de confiance et se fournissent des services selon les standards SAML 2.0 (Security Assertion Markup Language).

Les applications qui sont membres d'une fédération sont appelées des fournisseurs de services (SP). Le serveur d'identité et les fournisseurs de services peuvent être hébergés sur le site ou sur le cloud.

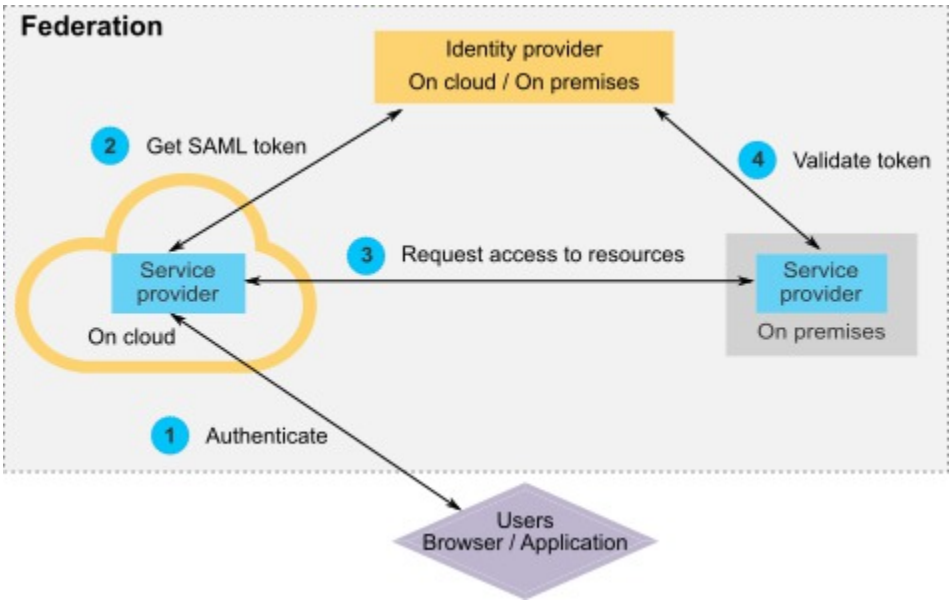
Une fédération SAML 2.0 prend en charge un grand nombre de mécanismes d'authentification pour la connexion unique. Par exemple, un utilisateur peut être authentifié dans un fournisseur de services par le mécanisme d'authentification de cette application (par exemple, application interne, OAuth, OpenId, SAML, Kerberos), puis il peut accéder à d'autres fournisseurs de service par la connexion unique fédérée, sous réserve que les applications fassent partie de la même fédération et que l'utilisateur soit mappé de façon adéquate.

Le serveur d'identité crée, valide ou supprime des jetons en fonction du mappage des utilisateurs. Les objets d'accès aux données sont implémentées pour les types de base de données pris en charge, et sont incorporés au serveur d'identité.

Un administrateur mappe les ID utilisateurs entre les fournisseurs de service pour leur fournir la connexion unique. Supposons par exemple que Fournisseur_A et Fournisseur_B soient tous les deux membres d'une fédération. Utilisateur_1 est un compte de Fournisseur_A et Utilisateur_2 est un compte de Fournisseur_B. Le compte Utilisateur_1 est mappé au compte Utilisateur_2 dans la fédération. Lorsqu'un utilisateur se connecte à Fournisseur_A avec les données d'identification d'Utilisateur_1, il dispose de l'accès à Fournisseur_B grâce à la connexion unique. De la même manière, lorsqu'un utilisateur se connecte à Fournisseur_B avec les données d'identification d'Utilisateur_2, il dispose de l'accès à Fournisseur_A grâce à la connexion unique.

Diagramme

Le diagramme suivant illustre la fédération.



Composants de l'implémentation HCL

L'implémentation de la connexion unique fédérée basée sur SAML 2.0 est constituée des composants suivants.

Ces composants sont dans le répertoire `tools/lib` de votre installation Unica Platform.

- Un serveur d'identité SAML 2.0, fourni sous la forme d'un fichier WAR : `idp-server.war`
- Une façade client : `idp-client.jar`

  La façade client du fournisseur d'identité est une implémentation Java™ avec une API qui fonctionne avec des jetons de sécurité. Elle est fournis sous la forme d'un fichier JAR. La documentation Javadoc™ de l'API est intégrée à celle de Unica Platform Javadoc™.

  La façade client du fournisseur d'identité permet aux fournisseurs de services Java™ de s'intégrer rapidement au serveur d'identité pour faire partie de la fédération.

Cas d'utilisation pris en charge

L'implémentation actuelle permet aux fournisseurs de services de gérer les jetons de sécurité pour établir l'authentification par connexion unique entre eux.

Génération d'un jeton SAML

L'implémentation peut générer un jeton SAML pour un utilisateur qui lance une demande d'authentification par la connexion unique. Cet utilisateur doit être mappé au serveur d'identité. A partir des données d'identification et du mappage des utilisateurs du tiers de confiance, le serveur d'identité crée un jeton de sécurité et l'émet dans une assertion SAML 2.0.

Par exemple, si Utilisateur_1 de Fournisseur_A est mappé avec Utilisateur_2 de Fournisseur_B sur le serveur d'identité et tente d'accéder aux ressources de Fournisseur_B, le serveur d'identité génère un jeton de sécurité pour Utilisateur_1 en tant que tiers de confiance.

Validation d'un jeton SAML existant

L'implémentation peut valider un jeton SAML existant présenté par un fournisseur de services qui reçoit la demande d'accès d'un utilisateur d'un autre fournisseur de services. Le fournisseur de services commence par valider le jeton de sécurité et le mappage du client auprès du serveur d'identité pour identifier l'utilisateur mappé dans son propre domaine.

Par exemple, lorsque Fournisseur_A tente d'accéder aux ressources de Fournisseur_B pour le compte d'Utilisateur_1 et présente le jeton de sécurité du fournisseur d'identité, Fournisseur_B transmet ce jeton au serveur d'identité. Si le jeton est valide et si Utilisateur_1 est mappé à un utilisateur de Fournisseur_B, le serveur d'identité résout l'utilisateur de Fournisseur_B dans le domaine de Fournisseur_B et renvoie l'assertion.

Suppression d'un jeton SAML existant

L'implémentation peut supprimer un jeton SAML existant lorsqu'un utilisateur d'un fournisseur de services se déconnecte du système ou qu'une session inactive expire. A partir des données d'identification et du mappage des utilisateurs du tiers de confiance, le serveur d'identité supprime le jeton et réinitialise l'horodatage du dernier accès lorsqu'il reçoit la demande de déconnexion. Le mappage de l'utilisateur n'est PAS supprimé.

Limitations

L'implémentation actuelle ne prend pas en charge les cas d'utilisation suivants.

- Création d'un mappage entre les utilisateurs des fournisseurs de services par une interface utilisateur ou une API
- Mise à jour d'un mappage existant entre les utilisateurs des fournisseurs de services par une interface utilisateur ou une API
- Suppression d'un mappage existant entre les utilisateurs des fournisseurs de services par une interface utilisateur ou une API

Authentification fédérée et partitions

Si votre environnement Unica comporte plusieurs partitions, vous pouvez configurer une authentification fédérée SAML 2.0 distincte pour chacune d'entre elles. Dans ce cas, sur la page **Paramètres > Configuration** , vous devez créer un ensemble de propriétés dans la catégorie **Unica Platform | Sécurité | Authentification fédérée | partitions | partition[n]** pour chaque partition.

Implémentation de l'authentification fédérée

Suivez les procédures décrites dans cette section pour implémenter l'authentification fédérée SAML 2.0 avec les produits ExperienceOne.

Création du référentiel de données

Créez deux tables de base de données, `TP_MASTER` et `TP_MAPPING`, pour contenir les mappages d'utilisateur. Tout schéma peut servir à créer les tables.

Les exemples de script SQL suivants sont fournis dans le répertoire `scripts` du fichier `idp-server.war`.

- `DatabaseScript_DB2.sql`
- `DatabaseScript_Oracle.sql`
- `DatabaseScript_SQL.sql`

Les tableaux suivants décrivent les zones de table de base de données créées par les scripts.

Tableau 32. Zones dans la table `TP_MASTER`

Zone	Description
`TP_ID`	Clé primaire. ID unique d'un fournisseur de services enregistré.
`TP_NAME`	Nom du fournisseur de services.
`TP_INFO`	Description du fournisseur de services.
`KEY_ALIAS`	Clé unique. Le nom d'alias du fichier de clés du fournisseur de services. Impose un nom d'alias unique. Vous pouvez supprimer la contrainte UNIQUE si vous souhaitez utiliser le même alias de fichier de clés pour plusieurs fournisseurs de services.

Tableau 33. Zones dans la table `TP_MAPPING`

Zone	Description
`TP_CLIENT_ID`	Clé externe. `TP_ID` du fournisseur de services demandeur. Partie d'une clé primaire composite constituée de quatre colonnes, garantissant qu'il n'y a pas de mappage en double dans cette table.
`TP_FOR_USER_ID`	ID de l'utilisateur du fournisseur de services demandeur qui effectue la demande. Partie d'une clé primaire composite constituée de quatre colonnes, garantissant qu'il n'y a pas de mappage en double dans cette table. Doit contenir entre 4 et 24 caractères (caractères alphanumériques, tirets et traits de soulignement exclusivement) : `[a-zA-Z0-9_-]`
`TP_SP_ID`	Clé externe. `TP_ID` du fournisseur de services serveur.

Tableau 33. Zones dans la table `TP_MAPPING` (suite)

Zone	Description
	Partie d'une clé primaire composite constituée de quatre colonnes, garantissant qu'il n'y a pas de mappage en double dans cette table. Doit contenir entre 4 et 24 caractères (caractères alphanumériques, tirets et traits de soulignement exclusivement) : `[a-zA-Z0-9_-]`
`TP_MAPPED_USER_ID`	ID de l'utilisateur du fournisseur de services serveur. Partie d'une clé primaire composite constituée de quatre colonnes, garantissant qu'il n'y a pas de mappage en double dans cette table.
`SAML_TOKEN`	Clé unique. ID du jeton SAML. Impose la génération d'un jeton unique. Vous pouvez supprimer la contrainte UNIQUE si vous souhaitez utiliser le même jeton pour plusieurs fournisseurs de services.
`LAST_REQUEST`	Horodatage de la dernière demande qui a abouti.

Configuration de la source de données d'identité dans le serveur d'applications Web

Tomcat, WebSphere® et WebLogic sont les serveurs d'applications Web pris en charge pour le serveur d'identité. Lorsque le serveur d'identité est déployé sur le serveur d'applications Web, vous devez configurer une source de données JNDI pour le connecter au référentiel de données.

Consultez la documentation de votre serveur d'applications Web pour plus de détails sur la manière de configurer une source de données JNDI.

Par exemple, la configuration suivante est requise pour créer la source de données d'une base de données Oracle dans un serveur Tomcat. Dans le fichier `conf/context.xml` de votre installation Tomcat, définissez une nouvelle ressource.

```
<Resource name="idp_datasource"
auth="Container"
type="javax.sql.DataSource"
maxActive="100" maxIdle="30" maxWait="10000"
username="your_username" password="your_password"
driverClassName="com.microsoft.sqlserver.jdbc.SQLServerDriver"
url="jdbc:sqlserver://localhost:1433;DatabaseName=IdPServer"/>
```

Enregistrez cette ressource dans le fichier `conf/web.xml` de votre installation Tomcat.

```
<resource-ref>
<description>SQL Server Datasource example</description>
<res-ref-name>idp_datasource</res-ref-name>
<res-type>javax.sql.DataSource</res-type>
<res-auth>Container</res-auth>
</resource-ref>
```

Configuration des chemins d'accès aux classes pour la façade client du fournisseur d'identité d'IBM®

Si vous souhaitez utiliser la façade client du fournisseur d'identité d'IBM®, vous devez ajouter des fichiers JAR dans le chemin d'accès aux classes de votre serveur d'identité et des fournisseurs de services.

1. Obtenez les fichiers JAR requis, comme indiqué ci-dessous, et placez-les sur votre serveur IdP et les serveurs qui hébergent vos fournisseurs de services.
    - Localisez le fichier `unica.war` dans le répertoire d'installation Unica Platform. Extrayez le fichier `unica.war`, accédez au répertoire `WEB-INF\lib` et copiez les fichiers JAR suivants.
        - `bcprov-jdk15.jar`
        - `esapi-2.0.1.jar`
        - `jersey-core-1.17.jar`
        - `jersey-server-1.17.jar`
        - `jersey-servlet-1.17.jar`
        - `joda-time-2.2.jar`
        - `opensaml-2.6.1.jar`
        - `openws-1.5.1.jar`
        - `xmlsec-1.5.6.jar`
        - `xmltooling-1.4.1.jar`
    - `asm-3.1.jar`

      Procédez au téléchargement depuis http://mvnrepository.com/artifact/asm/asm/3.1.
    - `jcl-over-slf4j-1.7.5.jar`

      Procédez au téléchargement depuis http://mvnrepository.com/artifact/org.slf4j/jcl-over-slf4j/1.7.5.
    - `slf4j-api-1.7.5.jar`

      Procédez au téléchargement depuis http://mvnrepository.com/artifact/org.slf4j/slf4j-api/1.7.5.
2. Ajoutez les fichiers JAR obtenus à l'étape précédente au chemin d'accès aux classes de votre serveur IdP et au chemin d'accès aux classes de chacun de vos fournisseurs de services.
3. Pour chaque fournisseur de services que vous souhaitez inclure à la fédération, ajoutez également le fichier JAR de façade client au chemin d'accès aux classes : : `idp-client.jar`
   Ce fichier JAR est fourni avec votre installation Unica Platform.

Déploiement du serveur d'identité

Le fichier `IdP-Server.war` peut être déployé avec le fichier WAR de Unica Platform sur le même serveur, ou séparément. Il n'y a pas de dépendance directe entre ces deux fichiers WAR.

Configuration du serveur d'identité

Le serveur d'identité stocke son fichier de clés dans sa configuration pour vérifier le jeton SAML provenant des fournisseurs de services. Les configurations sont stockées dans le fichier `IdPServerConfig.properties` du répertoire `conf` du serveur d'applications Web sur lequel le serveur d'identité est déployé.

Les requêtes indiquées dans cette section sont génériques. Si vous avez besoin de modifier la requête pour votre type de base de données, utilisez l'un des suffixes suivants dans la clé et entrez votre nouvelle requête à la place de la valeur.

- `Sql`
- `Oracle`
- `db2`

Par exemple, pour modifier la requête dans la propriété `com.ibm.ocm.idp.server.query.token.create` pour DB2®, modifiez la propriété de la manière suivante.

`com.ibm.ocm.idp.server.query.token.create.db2 = new query`

Remarque : La séquence et le nombre des colonnes dans votre requête modifiée doivent être identiques à ceux de la demande d'origine.

Référence : fichier IdPServerConfig.properties

Cette section répertorie les valeurs par défaut des propriétés du fichier de configuration, et toutes les valeurs admises.

`com.ibm.ocm.idp.server.keystore.path`

Chemin absolu du fichier de clés sur la machine hôte du serveur d'applications Web.

Valeur par défaut : path/idp.jks

`com.ibm.ocm.idp.server.keystore.passkey`

Clé d'accès au fichier de clés.

Valeur par défaut : `idp001`

`com.ibm.ocm.idp.server.keystore.alias`

Alias du fichier de clés.

Valeur par défaut : `idp`

`com.ibm.ocm.idp.server.certificate.issuer`

URL de l'émetteur du certificat.

Valeur par défaut : `http://localhost:8080/idp/`

`com.ibm.ocm.idp.server.token.validity`

Période de validité du jeton, en secondes.

Valeur par défaut : `3600`

`com.ibm.ocm.idp.server.enable`

Consignateur du serveur d'identité.

Valeur par défaut : True

`com.ibm.ocm.idp.server.dao.class`

Implémentation des objets d'accès aux données spécifiques des bases de données.

Les objets d'accès aux données pris en charge sont :

`com.ibm.ocm.idp.server.dao.IdPServerSQLDAO`

`com.ibm.ocm.idp.server.dao.IdPServerOracleDAO`

`com.ibm.ocm.idp.server.dao.IdPServerDB2DAO`

Valeur par défaut : `com.ibm.ocm.idp.server.dao.IdPServerSQLDAO`

`com.ibm.ocm.idp.server.datasource.name`

Nom JNDI de la source de données défini dans le serveur d'applications.

Valeur par défaut : `idp_datasource`

`com.ibm.ocm.idp.server.query.token.create`

Requête pour créer le jeton.

Valeur par défaut :

```
UPDATE TP_MAPPING
SET SAML_TOKEN = ?, LAST_REQUEST = ?
WHERE TP_CLIENT_ID = ?
AND TP_FOR_USER_ID = ?
AND TP_SP_ID = ?
```

`com.ibm.ocm.idp.server.query.token.get`

Requête pour obtenir le jeton.

Valeur par défaut :

```
SELECT SAML_TOKEN,
LAST_REQUEST FROM TP_MAPPING
WHERE TP_CLIENT_ID = ?
AND TP_FOR_USER_ID = ?
AND TP_SP_ID = ?
```

`com.ibm.ocm.idp.server.query.mapping.validate`

Requête pour valider un mappage d'utilisateur.

Valeur par défaut :

```
SELECT TP_MAPPED_USER_ID FROM TP_MAPPING
WHERE TP_CLIENT_ID = ?
AND TP_FOR_USER_ID = ?
AND TP_SP_ID = ?
```

`com.ibm.ocm.idp.server.query.token.delete`

Requête pour supprimer le jeton.

Valeur par défaut :

```
UPDATE TP_MAPPING SET SAML_TOKEN = null,
LAST_REQUEST = null
WHERE TP_CLIENT_ID = ?
AND TP_FOR_USER_ID = ?
AND TP_SP_ID = ?
```

`com.ibm.ocm.idp.server.query.client.get`

Requête pour obtenir des détails du client.

Valeur par défaut :

```
SELECT TP_ID, TP_NAME, TP_INFO, KEY_ALIAS
FROM TP_MASTER
WHERE TP_ID = ?
```

Récupération des fichiers de clés et importation dans le serveur d'identité

Pour établir la vérification du tiers de confiance, des fichiers de clés individuels sont requis pour chaque application intégrée et pour le serveur d'identité.

Vous devez obtenir les fichiers de clés du serveur d'identité et de tous les fournisseurs d'accès à inclure dans la fédération. Vous pouvez générer les fichiers de clés à l'aide de l'utilitaire Java™ keytool, ou les obtenir auprès d'une autorité de certification.

Si vous générez les fichiers de clés avec keytool, voici un flux de travaux classique pour cette tâche, avec des exemples de commande. Dans ces exemples, le chemin de Java™ 6 keytool est`C:\Program Files (x86)\Java\jre7\bin\keytool`.

- L'administrateur d'identité génère un fichier de clés pour le serveur d'identité et exporte le certificat.

```
# Generate IdP JKS from keytool
c:\temp> "keytool_path\keytool" -genkey -keyalg RSA -alias idp
-keystore idp.jks -storepass idp001 -validity 360 -keysize 2048
# Export IdP certificate from JKS
c:\temp> "keytool_path\keytool" -export -alias idp -file idp.cer
-keystore idp.jks
```

- Un administrateur de fournisseur de services génère un fichier de clés et l'exporte.

```
# Generate Service Provider JKS from keytool
c:\temp> "keytool_path\keytool" -genkey -keyalg RSA -alias SP_1
-keystore SP_1.jks -storepass SP001 -validity 360 -keysize 2048
# Export Service Provider certificate from JKS
c:\temp> "keytool_path\keytool" -export -alias SP_1 -file SP_1.cer
-keystore SP_1.jks
```

  L'administrateur de fournisseur de services envoie le certificat à l'administrateur d'identité.
- L'administrateur d'identité importe le certificat du fournisseur de services dans le serveur d'identité.

```
# Import Service Provider certificate into IdP JKS
c:\temp> "keytool_path\keytool" -import -alias SP_1
-trustcacerts -file SP_1.cer -keystore idp.jks
```

Définition des propriétés de configuration dans la page Configuration

Définition des propriétés de configuration dans la page **Paramètres > Configuration** pour configurer l'authentification fédérée dans Unica.

Définissez les propriétés de configuration dans les catégories suivantes.

- **Unica Platform | Sécurité | Authentification fédérée**
- **Unica Platform | Sécurité | Authentification fédérée | partitions | partition[n]**

Consultez l'aide contextuelle de chaque propriété ou les liens des rubriques connexes de cette section pour obtenir des instructions sur le paramétrage des valeurs.

Inscription des fournisseurs de service et des utilisateurs

L'administrateur du serveur d'identité doit créer une entrée (une seule fois) dans la table `TP_MASTER` pour inscrire les fournisseurs de services et les utilisateurs.

Voici un exemple de code SQL pour l'inscription d'un fournisseur de services.

```
INSERT INTO TP_MASTER
 (TP_ID, TP_NAME, TP_INFO, KEY_ALIAS)
 VALUES
 ('SP_Id', 'SP display name', 'SP description', 'keystore alias name')
```

Une fois les tiers de confiance enregistrés auprès du serveur d'identité, l'administrateur du serveur peut mapper les utilisateurs les faire participer à la connexion unique fédérée.

Le mappage des utilisateurs doit être strictement de un à un entre deux fournisseurs de services. Par exemple, Utilisateur_1 de Fournisseur_A doit être mappé à UN SEUL utilisateur de Fournisseur_B. Cependant, Utilisateur_1 de Fournisseur_A peut être mappé à un autre utilisateur de Fournisseur_C dans la même fédération.

Voici un exemple de requête pour l'ajout d'utilisateurs dans la table `TP_MAPPING`.

```
INSERT INTO TP_MAPPING
(TP_CLIENT_ID, TP_FOR_USER_ID, TP_SP_ID, TP_MAPPED_USER_ID, SAML_TOKEN)
VALUES
(’SP1_Id’, ’SP1_user_Id’, ’SP2_Id’, ’SP2_user_id’,'dummy1')
```

Remarque : Les entrées pour `TP_SP_ID` et `TP_FOR_USER_ID` doivent comporter entre 4 (au moins) et 24 caractères, et contenir uniquement des caractères alphanumériques, des tirets et des traits de soulignement : `[a-zA-Z0-9_-]`.

Insérez des entrées factices uniques pour la colonne `SAML_TOKEN`, cette colonne ne permettant pas les valeurs NULL et les doublons.

Utilisation de la façade client du fournisseur d'identité pour générer des jetons et les transmettre aux fournisseurs de service

Lorsqu'un utilisateur est authentifié et souhaite accéder aux services d'un autre fournisseur de services, appelez le code suivant du côté du fournisseur de services.

Le code génère le jeton fédéré.

```
// One time properties to initialize the IdP client.
Properties properties = new Properties();
properties.put(IdPClient.IDP_SERVER_URL, "URL");
properties.put(IdPClient.IDP_CLIENT_CERTIFICATE_ISSUER, "URL");
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_PATH, "JKS file path");
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_PASSKEY, "JKS passkey");
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_ALIAS, "Certificate alias");
// Get the IdP client factory singleton instance
//with the specified parameters.
IdPClientFactory clientFactory = IdPClientFactory.getInstance(properties);
// Get the partition specific client facade to do the assertion.
IdPClientFacade clientFacade = clientFactory.getIdPClientFacade(partition);
// Establish SSO Login with the IdP server
IdPClientToken token = clientFacade.doIdPLogin(clientId, forUserId, spId);
```

Le jeton obtenu peut être transmis aux fournisseurs de services cible pour accéder à leurs ressources en fonction des rôles et des droits de l'utilisateur mappé.

```
// Security token is validated at Service Provider side.
IdPClientAssertion assertion = spFacade.assertIdPToken(clientId, forUserId,
 spId,
token.getTokenId());
```

```
// Retrieve the principal from the assertion, if there is no exception.
String principal = assertion.getMappedUser();
```

La façade client accepte les services partagés et peut être utilisée pour configurer chaque partition séparément. Pour utiliser cette fonction, ajoutez l'ID client à chaque nom de propriété. Par exemple :

```
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_PATH +
".partition1", "JKS file path");
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_PASSKEY +
".partition1", "JKS passkey");
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_ALIAS +
".partition1", "Certificate alias");
```

Référence : Services RESTful

Utilisez ces informations pour traiter les problèmes liés à l'utilisation de la façade client, ou pour développer votre propre implémentation SAML 2.0 avec le serveur d'identité fourni par IBM.

Les API REST sont implémentées à l'aide d'un contenu de données XML. L'assertion SAML est directement transmise aux méthodes POST avec des signatures numériques.

Seule la méthode POST est prise en charge, pour unifier la méthode d'accès et appliquer les vérifications de sécurité, en fonction du contenu XML. Les autres méthodes, telles que GET, PUT et DELETE, renvoient un message d'erreur. Le tableau suivant représente les instructions qui implémentent les cas d'utilisation pris en charge.

Tableau 34. Instructions prises en charge

Ressource	Publier
`<idp>/saml/token/clientId/forUserId/spId/create`	Générer un nouveau jeton SAML.
`<idp>/saml/token/clientId/forUserId/spId/validate`	Valider un jeton SAML existant.

Tableau 34. Instructions prises en charge (suite)

Ressource	Publier
`<idp>/saml/token/clientId/forUserId/spId/delete`	Supprimer un jeton SAML existant.

Concepts associés

Cette section contient des informations générales sur les technologies utilisées dans l'implémentation ExperienceOne de la fonction de connexion unique fédérée SAML 2.0.

Security Assertion Markup Language 2.0 (SAML 2.0)

SAML 2.0 est une version du standard SAML d'échange des données d'authentification et d'autorisation entre les domaines de sécurité. SAML 2.0 est un protocole XML qui utilise des jetons de sécurité contenant des assertions pour transmettre des informations relatives à un principal (généralement un utilisateur final) entre une autorité SAML, c'est-à-dire un fournisseur d'identité, et un consommateur SAML, c'est-à-dire un fournisseur de services. SAML 2.0 Web permet la mise en œuvre de l'authentification Web et des scénarios d'autorisation, y compris la connexion unique (SSO) interdomaine, réduisant ainsi la charge administrative liée à la distribution de plusieurs jetons d'authentification à l'utilisateur. Pour plus d'informations, voir http://en.wikipedia.org/wiki/SAML_2.0.

Fournisseur d'identité (IdP)

Egalement appelé fournisseur de vérification d'identité, le fournisseur d'identité fournit des informations d'identification pour tous les fournisseurs de services qui interagissent dans le système ou lui fournissent des services. Dans cette méthode, la vérification d'un jeton de sécurité par un module d'authentification remplace l'authentification explicite de l'utilisateur dans le domaine de sécurité. Dans l'authentification périmétrique, l'utilisateur doit être authentifié une seule fois (connexion unique) et transmettre un jeton de sécurité qui est traité par un fournisseur d'identité, pour chaque système auquel il a besoin d'accéder. Pour plus d'informations, voir http://en.wikipedia.org/wiki/Identity_provider.

Chiffrement à clé publique

Aussi appelé chiffrement asymétrique, cet algorithme de chiffrement requiert deux clés distinctes, l'une secrète (ou privée) et l'autre publique. Bien que distinctes, les deux parties de cette paire de clés sont liées mathématiquement. La clé publique est utilisée pour chiffrer du texte brut ou vérifier une signature numérique, alors que la clé privée est utilisée pour déchiffrer du texte chiffré ou créer une signature numérique. Pour plus d'informations, voir http://en.wikipedia.org/wiki/Public-key_cryptography.

Connexion unique entre Unica et IBM Digital Analytics

Si votre organisation utilise IBM Digital Analytics, vous pouvez activer la connexion unique entre Digital Analytics et Unica.

La connexion unique permet aux utilisateurs de naviguer vers les rapports Digital Analytics à partir de l'interface utilisateur Unica sans être invité à se connecter.

De même, si les rapports Digital Analytics sont référencés dans des tableaux de bord Unica, la connexion unique permet aux utilisateurs d'afficher ces rapports (s'ils y ont accès dans Digital Analytics).

Deux options permettant d'activer la connexion unique entre Unica et IBM Digital Analytics

Vous pouvez choisir entre deux options pour l'activation de la connexion unique.

- Vous pouvez configurer Digital Analytics pour créer automatiquement un compte utilisateur Digital Analytics lorsqu'un utilisateur Unica navigue pour la première fois vers Digital Analytics.

  Vous pouvez être amené à choisir cette option si vous souhaitez que tous les utilisateurs Unica disposent d'une connexion unique avec Digital Analytics.
- Vous pouvez configurer des comptes utilisateur Unica pour la connexion unique en ajoutant le nom de connexion Digital Analytics existant de chaque utilisateur à sa page de détails dans Unica.

Lorsque vous choisissez cette option, les utilisateurs nécessitant un accès à Digital Analytics doivent posséder un compte Digital Analytics.

Vous pouvez être amené à choisir cette option si vous souhaitez qu'un sous-ensemble des utilisateurs Unica dispose d'une connexion unique avec Digital Analytics.

Droits d'accès dans Digital Analytics pour les utilisateurs de connexion unique

Lorsque l'option de création automatique de compte n'est **PAS** sélectionnée dans Digital Analytics, les utilisateurs de connexion unique disposent des droits dans Digital Analytics qu'ils auraient s'ils se connectaient directement à Digital Analytics.

Lorsque l'option de création automatique de compte est sélectionnée dans Digital Analytics, les utilisateurs de connexion unique disposent des droits dans Digital Analytics comme indiqué ci-après.

- Par défaut, les utilisateurs disposent des droits accordés au groupe Digital Analytics que l'administrateur a configuré pour tous les utilisateurs créés automatiquement.

  Les administrateurs peuvent modifier les droits associés à ce groupe.
- En outre, l'administrateur peut remplacer la création automatique de compte pour les utilisateurs qui ont déjà un compte Digital Analytics. Si le remplacement est en place pour un utilisateur, ce dernier dispose des droits qu'il aurait en se connectant directement à Digital Analytics.

Coordination de l'horloge du serveur

L'horloge du serveur sur lequel Unica Platform est déployé doit correspondre à l'heure de l'horloge du serveur Digital Analytics. Pour la connexion unique, le serveur Digital Analytics admet jusqu'à 15 minutes d'écart (900 secondes) entre les heures d'horloge de serveur.

Il est recommandé de synchroniser les horloges des serveurs. Pour garantir la synchronisation, vous devez utiliser le protocole NTP (Network Time Protocol).

Si vous n'arrivez pas à synchroniser l'horloge de votre serveur et qu'il y a peut-être au moins quinze minutes de différence entre les horloges, vous pouvez donner à la propriété

de configuration **Clock skew adjustment (seconds)** qui se trouve dans la catégorie Coremetrics® de Unica Platform une valeur qui reflète la différence entre les horloges.

Configuration de la connexion unique entre Unica et Digital Analytics en utilisant la création automatique de compte utilisateur

Utilisez la procédure ci-dessous pour configurer la connexion unique entre Unica et Digital Analytics en utilisant la création automatique de compte utilisateur.

1. Déterminez l'ID client Digital Analytics que vous souhaitez utiliser pour la connexion unique entre Unica et Digital Analytics.

   Notez l'ID client, dans la mesure où vous en aurez besoin ultérieurement.
2. Connectez-vous à Digital Analytics en tant qu'utilisateur administrateur ayant accès à l'ID client que vous avez sélectionné à l'étape précédente, cliquez sur le lien Admin, puis naviguez vers la page d'authentification d'utilisateur globale.
   - Dans le champ **Secret partagé d'Enterprise Marketing Management**, entrez une chaîne conforme aux règles indiquées dans les instructions figurant à côté du champ en question.

     Prenez note de cette chaîne, dans la mesure où vous en aurez besoin ultérieurement.
   - Dans la page de création automatique de compte utilisateur, cliquez sur **Activé**.
   - Sélectionnez un groupe d'utilisateurs auquel vous souhaitez que tous les utilisateurs automatiquement créés appartiennent.

     Ce groupe doit disposer au moins des droits d'analyse Web ci-dessous.
     - Tableaux de bord > Vue des tableaux de bord standard
     - Rapports > Indicateurs de site
     - Rapports > Vues d'ensemble
3. Connectez-vous à Unica en tant qu'utilisateur administrateur et accédez à la page **Paramètres > Utilisateurs**.
4. Sélectionnez ou créez un utilisateur, puis configurez une source de données pour cet utilisateur comme suit.

- **Source de données** - Entrez un nom.
- **Connexion à la source de données** - Entrez l'ID client que vous avez noté à l'étape 1.
- **Mot de passe de la source de données** - Entrez le secret partagé que vous avez noté à l'étape 2.

Si vous possédez plusieurs partitions, vous devez effectuer cette tâche dans chacune des partitions dont les utilisateurs doivent disposer de la connexion unique.

Vous avez également la possibilité d'utiliser le compte utilisateur platform_admin pour cette étape. Dans la mesure où cet utilisateur est un membre de toutes les partitions, la source de données associée est disponible dans toutes les partitions.

5. Dans Unica Platform, accédez à la page **Paramètres > Groupes d'utilisateurs** et procédez comme suit.
    - Créer un groupe et ajoutez le rôle CMUser à ce groupe.
    - Faites en sorte que chaque utilisateur devant posséder une connexion unique fasse partie de ce groupe.

    Si vous possédez plusieurs partitions, vous devez effectuer cette tâche dans chacune des partitions dont les utilisateurs doivent disposer de la connexion unique.
6. Dans Unica Platform, accédez à la page **Paramètres > Configuration** et définissez les propriétés de configuration comme suit.

Tableau 35. Propriétés de configuration permettant d'activer la connexion unique avec Digital Analytics

Propriété	Valeur
Digital Analytics | Activer IBM Digital-Analytics	True
Digital Analytics | Intégration | partitions | partition[n] |Utilisateur de la plateforme pour le compte IBM Digital Analytics	Entrez le nom de connexion du compte utilisateur Unica Platform que vous avez utilisé à l'étape 4.
Digital Analytics | Intégration | partitions | partition[n] | Source de don-	Entrez le nom de la source de données que vous avez créé à l'étape 4.

Propriété	Valeur
nées pour le compte IBM Digital Analytics	

Si vous possédez plusieurs partitions, vous devez utiliser **Digital Analytics | Intégration | partitions | partitionTemplate** pour créer un ensemble de propriétés de configuration pour chacune des partitions dont les utilisateurs doivent disposer de la connexion unique.

Le nom de la catégorie que vous créez à l'aide du modèle doit correspondre exactement au nom de la partition Unica Campaign correspondante.

7. Pour tous les utilisateurs pour lesquels vous voulez remplacer la création automatique de compte, procédez comme suit :
   - Dans Unica Platform, accédez à la page **Paramètres > Utilisateurs**.
   - Entrez le nom de connexion Digital Analytics de l'utilisateur dans la zone **Nom d'utilisateur Digital Analytics** de la page de détails de l'utilisateur.

   Cela ne fonctionne que pour les utilisateurs qui possèdent déjà un compte Digital Analytics.

   Remarque : Si aucun compte portant ce nom de connexion n'existe dans Digital Analytics, un compte est créé pour cet utilisateur à l'aide du nom que vous entrez ici, et non avec le nom de connexion Unica Platform de l'utilisateur.

8. Configurez votre serveur d'applications Web pour la connexion unique avec Digital Analytics.

Configuration de la connexion unique entre Unica et Digital Analytics en utilisant la création manuelle de compte utilisateur

Utilisez la procédure ci-dessous pour configurer la connexion unique entre Unica et Digital Analytics en utilisant la création manuelle de compte utilisateur.

1. Déterminez l'ID client Digital Analytics que vous souhaitez utiliser pour la connexion unique entre Unica et Digital Analytics.

   Notez l'ID client, dans la mesure où vous en aurez besoin ultérieurement.
2. Connectez-vous à Digital Analytics en tant qu'utilisateur administrateur ayant accès à l'ID client que vous avez sélectionné à l'étape précédente, cliquez sur le lien Admin, puis naviguez vers la page d'authentification d'utilisateur globale.
   - Dans le champ **Secret partagé d'Enterprise Marketing Management**, entrez une chaîne conforme aux règles indiquées dans les instructions figurant à côté du champ en question.

     Prenez note de cette chaîne, dans la mesure où vous en aurez besoin ultérieurement.
   - Dans la page de création automatique de compte utilisateur, cliquez sur **Désactivé**.
3. Connectez-vous à Unica en tant qu'utilisateur administrateur et accédez à la page **Paramètres > Utilisateurs**.
4. Sélectionnez ou créez un utilisateur, puis configurez une source de données pour cet utilisateur comme suit.
   - **Source de données** - Entrez un nom.
   - **Connexion à la source de données** - Entrez l'ID client que vous avez noté à l'étape 1.
   - **Mot de passe de la source de données** - Entrez le secret partagé que vous avez noté à l'étape 2.

   Si vous possédez plusieurs partitions, vous devez effectuer cette tâche dans chacune des partitions dont les utilisateurs doivent disposer de la connexion unique.

   Vous avez également la possibilité d'utiliser le compte utilisateur platform_admin pour cette étape. Dans la mesure où cet utilisateur est un membre de toutes les partitions, la source de données associée est disponible dans toutes les partitions.
5. Dans Unica Platform, accédez à la page **Paramètres > Groupes d'utilisateurs** et procédez comme suit.

- Créez un groupe et ajoutez le rôle DMUser à ce groupe.
- Faites en sorte que chaque utilisateur devant posséder une connexion unique fasse partie de ce groupe.

Si vous possédez plusieurs partitions, vous devez effectuer cette tâche dans chacune des partitions dont les utilisateurs doivent disposer de la connexion unique.

6. Dans Unica Platform, accédez à la page **Paramètres > Configuration** et définissez les propriétés de configuration comme suit.

Tableau 36. Propriétés de configuration permettant d'activer la connexion unique avec Digital Analytics

Propriété	Valeur
Digital Analytics | Activer IBM Digital-Analytics	True
Digital Analytics | Intégration | partitions | partition[n] |Utilisateur de la plateforme pour le compte IBM Digital Analytics	Entrez le nom de connexion du compte utilisateur Unica Platform que vous avez utilisé au cours de l'étape 4.
Digital Analytics | Intégration | partitions | partition[n] | Source de données pour le compte IBM Digital Analytics	Entrez le nom de la source de données que vous avez créé à l'étape 4.

Si vous possédez plusieurs partitions, vous devez utiliser **Digital Analytics \| Intégration \| partitions \| partitionTemplate** pour créer un ensemble de propriétés de configuration pour chacune des partitions dont les utilisateurs doivent disposer de la connexion unique.

Le nom de la catégorie que vous créez à l'aide du modèle doit correspondre exactement au nom de la partition Unica Campaign correspondante.

7. Dans Unica Platform, accédez à la page **Paramètres > Utilisateurs**.

8. Pour chaque utilisateur pour lequel vous souhaitez activer la connexion unique, entrez le nom de connexion Digital Analytics de cet utilisateur dans la zone **Nom d'utilisateur IBM Digital Analytics** de la page Editer propriétés de l'utilisateur.

   Remarque : Si un utilisateur possède exactement les mêmes noms de connexion dans Unica et Digital Analytics, vous n'avez pas besoin d'effectuer cette étape.

9. Configurez votre serveur d'applications Web pour la connexion unique avec Digital Analytics.

Configuration de WebLogic pour la connexion unique entre Digital Analytics et Unica

Exécutez la procédure ci-dessous dans le domaine WebLogic où Unica Platform est déployé pour que les utilisateurs puissent afficher les rapports Digital Analytics dans les tableaux de bord sans avoir à se connecter.

1. Ouvrez le script `setDomainEnv` situé dans le répertoire `bin` sous le répertoire de domaine WebLogic.
2. Ajoutez `-Dweblogic.security.SSL.ignoreHostnameVerification=true` à `JAVA_OPTIONS`.

Configuration de WebSphere® pour la connexion unique entre Digital Analytics et Unica

Exécutez la procédure ci-dessous dans la cible et le nœud WebSphere® dans lesquels Unica Platform est déployé afin que les utilisateurs puissent visualiser les rapports Digital Analytics dans les tableaux de bord sans avoir à se connecter.

1. Connectez-vous à la console d'administration WebSphere®.
2. Développez **Sécurité** et cliquez sur **Certificat SSL et gestion des clés**.
3. Sous **Paramètres de configuration**, cliquez sur **Gérer les configurations de sécurité du nœud final**.

4. Accédez à la configuration sortante de la cible et du noeud où Unica Platform est déployé.
5. Sous **Eléments connexes**, cliquez sur **Magasins de clés et certificats** et cliquez sur le magasin de clés **NodeDefaultTrustStore**.
6. Sous **Propriétés supplémentaires**, cliquez sur **Certificats de signataire** et **Récupérer depuis le port**.

   Remplissez les zones comme suit.

   - **Nom d'hôte** : `welcome.coremetrics.com`
   - **Port** : `443`
   - **Alias** : `coremetrics_cert`

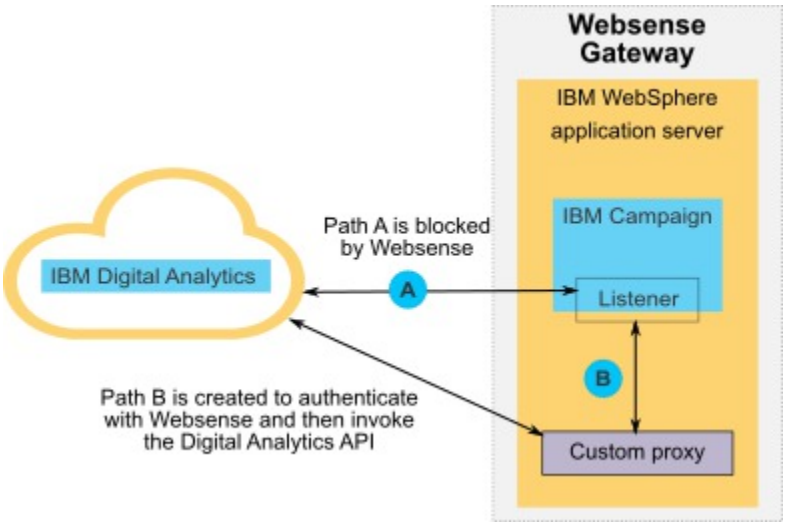
Intégration de Digital Analytics à Websense à l'aide d'un proxy personnalisé

Unica Platform fournit un proxy personnalisé pour permettre l'intégration entre Unica Campaign hébergé sur site et Digital Analytics hébergé sur le cloud lorsque Websense est un composant requis de l'environnement.

Le proxy personnalisé est uniquement pris en charge avec le serveur d'application WebSphere.

Une fois le proxy personnalisé installé, vous pouvez configurer la connexion unique et l'intégration entre Digital Analytics et Unica Campaign.

Le proxy personnalisé est une implémentation de servlet Java qui agit en tant que proxy direct. Il est injecté entre le programme d'écoute Unica Campaign et Digital Analytics. Le proxy personnalisé agit en tant que point final pour le programme d'écoute Unica Campaign pour appeler des API Digital Analytics. En interne, il s'authentifie lui-même avec la passerelle de contenu Websense, puis appelle les API en dehors du réseau de manière sécurisée.



Déploiement du proxy personnalisé sur WebSphere

Exécutez cette procédure pour installer le proxy personnalisé. Ce proxy personnalisé est uniquement pris en charge avec le serveur d'application WebSphere.

Notez que vous pouvez déployer l'application ProxyServer sur le même profil WebSphere que celui sur lequel vous avez déployé Unica Campaign, ou vous pouvez utiliser un autre profil WebSphere.

1. Copiez le fichier `ProxyServer.war` à un emplacement accessible depuis le serveur WebSphere.

   Le fichier `ProxyServer.war` se trouve dans le répertoire `tools\lib` de votre installation Unica Platform.
2. Déployez le fichier `ProxyServer.war` en procédant comme suit.
   - Sélectionnez le chemin **Detailed - Show all installation options and parameters** pour l'installation.
   - Vous pouvez fournir n'importe quel nom d'application.
   - Vous n'avez pas besoin de sélectionner **Précompiler les fichiers JavaServer Pages**.
   - Sur la page Initialize parameters for servlets, renseignez les zones comme suit.

- **proxy_host** - URL ou adresse IP hôte du serveur Websense
- **proxy_port** - Numéro de port du serveur Websense
- **proxy_username** - Nom d'utilisateur pour l'authentification Websense
- **Proxy_password** - Mot de passe pour l'authentification Websense
- **target_url** - URL de point final de Digital Analytics, déjà configurée dans Unica Campaign

- Sur la page Mappage des racines de contexte des modules Web, définissez la racine de contexte sur `proxy`.
- Lorsque le déploiement est terminé, accédez à l'application ProxyServer dans un navigateur, à l'adresse `http://WebSphere_host:Port/proxy`.

  Vous devriez recevoir le message : IBM OCM Secure Proxy Server V.x

Importation du certificat Digital Analytics lorsque WebSphere ne dispose pas d'un accès sortant

Utilisez cette procédure lorsque WebSphere ne dispose pas d'un accès sortant au serveur Digital Analytics.

1. Extrayez le certificat numérique depuis le site Digital Analytics.

   Pour extraire le certificat, accédez à l'URL Digital Analytics et cliquez sur l'icône de verrou dans la zone d'adresse de votre navigateur. Votre navigateur ouvre une fenêtre dans laquelle vous pouvez télécharger le certificat.
2. Importez le certificat dans la machine virtuelle Java WebSphere à l'aide de l'outil de clé Java.

   Par exemple (retours à la ligne ajoutés) :

   ```
   /keytool -import -file DA_Certificate.cer
   -alias da_alias
   -keystore WebSphere_JRE_home/lib/security/cacerts
   ```

   Indiquez le mot de passe. Le mot de passe par défaut de l'outil de clé est changeit.
3. Dans la console d'administration WebSphere, ajoutez les propriétés personnalisées suivantes.

- javax.net.ssl.trustStore *WebSphere_JRE_home*/lib/security/cacerts
- javax.net.ssl.trustStorePassword : *your_password*
- javax.net.ssl.trustStoreType: jks

Importation du certificat Digital Analytics lorsque WebSphere dispose d'un accès sortant

Utilisez cette procédure lorsque WebSphere dispose d'un accès sortant au serveur Digital Analytics.

1. Dans la console d'administration WebSphere, développez **Sécurité** et cliquez sur **SSL certificate and key management**.
2. Sous **Paramètres de configuration**, cliquez sur **Gérer les configurations de sécurité du nœud final**.
3. Sélectionnez la configuration sortante appropriée pour accéder à la portée de la gestion **(cible) :..Node0xCell:(nœud) :..Node0x**
4. Sous **Eléments connexes**, cliquez sur **Magasins de clés et certificats**, puis cliquez sur le magasin de clés **NodeDefaultTrustStore** (ou le magasin de clés que vous avez utilisé sur le serveur d'application WebSphere).
5. Sous **Propriétés supplémentaires**, cliquez sur **Certificats de signataires** et sur **Récupérer depuis le port**.
    a. Dans la zone **Host**, entrez le nom du serveur Digital Analytics.

       Par exemple, `export.coremetrics.com`.

    b. Dans la zone **Port**, entrez `443`.

    c. Dans la zone **Alias**, entrez un nom d'alias.
6. Cliquez sur **Retrieve Signer Information** et vérifiez que les informations de certificat sont celles d'un certificat de confiance.
7. Appliquez et enregistrez votre configuration.

Etapes suivantes

Après l'installation du serveur proxy personnalisé et l'importation du certificat Digital Analytics, les étapes suivantes consistent à activer la connexion unique et à configurer l'intégration entre Digital Analytics et Unica Campaign.

Pour terminer la configuration de votre environnement, exécutez les procédures suivantes.

- Configurez la connexion unique comme indiqué dans le manuel *Unica Platform - Guide d'administration, au chapitre "Connexion unique entre Unica et Digital Analytics."*
- Configurez l'intégration comme indiqué dans le manuel *Unica Campaign - Guide d'administration*, au chapitre "Intégration Unica Campaign avec d'autres produits ".

Important : La procédure d'intégration inclut la définition de la propriété de configuration `ServiceURL` sous **Campaign | partitions | partition[n] | Coremetrics**. Lorsque vous utilisez le proxy personnalisé, vous devez définir cette propriété sur `http://WebSphere_host:Port/proxy` et redémarrer l'application Web Unica Platform.

Intégration entre Unica et Windows™ Active Directory

Unica Platform peut être configuré pour être intégré au serveur Windows™ Active Directory ou à un autre serveur LDAP (Lightweight Directory Access Protocol). L'intégration d'Unica à un serveur d'annuaire vous permet de centraliser l'emplacement des utilisateurs et des groupes. L'intégration permet d'étendre de manière flexible les stratégies d'autorisation d'entreprise dans les applications d'Unica. Elle permet également de réduire les coûts de support et le temps nécessaire pour déployer une application en production.

Pour obtenir la liste des serveurs d'annuaire pris en charge, consultez le document Environnements logiciels recommandés et configuration minimale requise.

Fonctionnalités d'intégration d'Active Directory

L'intégration de Unica Platform à Windows™ Active Directory fournit les fonctions décrites dans cette section.

Authentification avec intégration à Active Directory

Les applications Unica recherchent des informations d'autorisation utilisateur sur Unica Platform.

- Les versions précédentes de Unica Platform prenaient en charge la connexion intégrée à Microsoft Windows basée sur le protocole NTLM v1. Avec l'arrivée de Microsoft Windows 2008 Server et de Microsoft Windows 7, la valeur standard minimale par défaut a changé et nécessite le protocole NTLMv2. NTLMv2 n'est pas nativement pris en charge par Unica Platform.

  Vous pouvez toutefois configurer l'authentification NTLMv2, de sorte que les utilisateurs sont authentifiés dans toutes les applications Unica lorsqu'ils se connectent au réseau de l'entreprise et qu'aucun mot de passe n'est requis pour se connecter aux applications Unica. L'authentification des utilisateurs repose sur leur données de connexion Windows™ en ignorant les écrans de connexion des applications.

  Pour configurer l'authentification NTLMv2, effectuez les étapes décrites dans ce chapitre.
- Si l'authentification NTLMv2 n'est pas activée, les utilisateurs doivent toujours se connecter sur l'écran de connexion Unica en utilisant leurs données d'identification Windows™.

Gestion des utilisateurs internes et externes

Lorsque l'authentification NTLMv2 est activée, tous les utilisateurs sont créés et gérés sur le serveur Active Directory. (Vous ne pouvez pas créer des utilisateurs dans Unica Platform (appelés utilisateurs internes dans ce guide)). Si vous voulez pouvoir créer des utilisateurs internes, n'activez pas l'authentification NTLMv2.

Une fois l'intégration configurée, vous ne pouvez ni ajouter, ni modifier ni supprimer les comptes utilisateur importés dans Unica Platform. Vous devez effectuer ces tâches de gestion au niveau de LDAP et les modifications sont importées au moment de la synchronisation. Si vous modifiez des comptes utilisateur importés dans Unica Platform, les utilisateurs risquent de rencontrer des problèmes au moment de l'authentification.

Les comptes utilisateur que vous supprimez au niveau de LDAP ne sont pas supprimés de Unica Platform. Vous devez désactiver manuellement ces comptes dans Unica Platform. Il est préférable de désactiver ces comptes utilisateur plutôt que de les supprimer car les utilisateurs possèdent des droits de propriété sur les dossiers dans Unica Campaign et, si vous supprimez un compte utilisateur qui possède un dossier, les objets contenus dans ce dossier ne seront plus disponibles.

Synchronisation

Si Unica est configuré pour s'intégrer à un serveur Windows Active Directory, les utilisateurs et les groupes sont automatiquement synchronisés à des intervalles prédéfinis.

La synchronisation automatique a une fonctionnalité limitée.

- Les utilisateurs qui sont supprimés du serveur LDAP ne sont pas supprimés lors de la synchronisation automatique.

Vous pouvez forcer la synchronisation intégrale de tous les utilisateurs et tous les groupes en utilisant la fonction Synchroniser dans la zone Utilisateurs d'Unica. Sinon, vous pouvez contacter Services pour demander la définition d'une propriété de configuration masquée qui déclenche une synchronisation automatique complète.

Importation d'utilisateurs basée sur des groupes ou des attributs

Si vous importez des comptes utilisateur à partir du serveur LDAP dans Unica Platform, vous avez le choix entre deux types de filtrage lors de la sélection de ces comptes utilisateur.

Vous devez choisir entre l'importation basée sur des groupes ou l'importation basée sur des attributs. Ces méthodes ne peuvent pas être prises en charge simultanément.

Importation basée sur le groupe

Unica Platform importe les groupes et les utilisateurs à partir de la base de données de serveur d'annuaire via une tâche de synchronisation périodique qui extrait automatiquement les informations à partir du serveur d'annuaire. Si Unica Platform importe les utilisateurs et les groupes à partir de la base de données du serveur, les appartenances de groupe ne sont pas modifiées. Pour sélectionner ces modifications, vous devez effectuer une synchronisation manuelle.

Vous pouvez accorder des privilèges Unica en mappant un groupe Active Directory à un groupe Unica. Ce mappage permet aux nouveaux utilisateurs ajoutés au groupe Active Directory mappé de disposer des privilèges définis pour le groupe d'Unica.

Un sous-groupe existant dans Unica Platform n'hérite pas des mappages Active Directory ou des appartenances d'utilisateur de ses parents.

La configuration de l'importation par groupe est détaillée dans la suite de ce chapitre.

Importation basée sur l'attribut

Si vous ne voulez pas créer sur votre serveur Active Directory de groupes qui soient spécifiques aux produits Unica, vous pouvez contrôler quels utilisateurs seront importés en spécifiant des attributs. Pour ce faire, vous devez procéder comme suit pendant la configuration.

1. Déterminez la chaîne utilisée sur votre serveur Active Directory pour l'attribut à partir duquel vous voulez effectuer le filtrage.
2. Attribuez la valeur `DN` à la propriété **Unica Platform | Sécurité | Synchronisation LDAP | Nom d'attribut de référence de l'utilisateur LDAP**.

   Cela signale à Unica Platform que la synchronisation n'est pas basée sur un groupe avec des références de membres, mais sur une unité organisationnelle ou une organisation (Org Unit ou Org).
3. Lorsque vous configurez la propriété **Mappe de référence LDAP**, définissez la portion Filter de la valeur avec l'attribut sur lequel vous voulez effectuer la recherche. Pour le filtre, utilisez la chaîne que vous avez déterminée au point 1.

Lorsque vous utilisez une synchronisation basée sur des attributs, la synchronisation périodique est toujours une synchronisation complète et non une synchronisation partielle,

comme c'est le cas pour la synchronisation basée sur des groupes. Pour la synchronisation basée sur des attributs, vous devez donner à la propriété **Intervalle de synchronisation LDAP** une valeur élevée ou une valeur `0` si vous voulez désactiver la synchronisation automatique et vous contenter de la synchronisation complète manuelle lorsque des utilisateurs sont ajoutés à l'annuaire.

Suivez les instructions fournies dans la suite de ce chapitre pour configurer l'intégration et reportez-vous aux instructions ci-dessus quand vous devrez définir les propriétés de configuration.

A propos d'Active Directory et des partitions

Dans des environnements à plusieurs partitions, l'appartenance à une partition d'un utilisateur est déterminée par le groupe dont fait partie l'utilisateur lorsque ce groupe est affecté à une partition. Un utilisateur ne peut faire partie que d'une seule partition à la fois. Si l'utilisateur fait partie de plusieurs groupes Active Directory mappés à des groupes d'Unica eux-mêmes affectés à différentes partitions, le système doit choisir une seule partition pour cet utilisateur.

Essayez d'éviter cette situation. Si toutefois elle venait à se produire, la partition du groupe d'Unica à laquelle appartient l'utilisateur est celle qui a été la plus récemment mappée à un groupe Active Directory. Pour déterminer le dernier groupe Active Directory qui a été mappé, consultez les mappages de groupe LDAP affichés dans la zone Configuration. Ils s'affichent dans l'ordre chronologique, le plus récent étant le dernier élément de la liste.

Caractères spéciaux dans les noms de connexion

Seuls trois caractères spéciaux sont autorisés dans les noms de connexion : le point (.), le trait de soulignement (_) et le trait d'union (-). S'il figure d'autres caractères spéciaux (notamment des espaces) dans le nom de connexion d'un utilisateur que vous envisagez d'importer dans Unica Platform depuis un serveur Active Directory, vous devez modifier ce nom de connexion afin que l'utilisateur ne rencontre pas de problèmes lors de sa déconnexion ou lorsqu'il exécutera des tâches d'administration (s'il a les droits requis pour cela).

Conditions requises pour l'intégration à Active Directory

Pour tirer parti des fonctions d'intégration à Windows™ Active Directory, vous devez installer les applications Unica sur un système d'exploitation compatible.

En outre, pour implémenter l'authentification NTLMv2, les utilisateurs qui accèdent aux applications Unica doivent :

- Utiliser un système exécutant un système d'exploitation Windows™ compatible.
- Se connecter comme membre du domaine Windows™ Active Directory par rapport auquel Unica exécute l'authentification.
- Utiliser un navigateur pris en charge.

Organisation du processus de configuration : intégration avec Active Directory

Cette feuille de route du processus de configuration permet d'analyser les tâches requises pour intégrer Unica avec Windows™ Active Directory. La colonne Rubrique contient des liens vers les rubriques qui décrivent les tâches en détail.

Tableau 37. Organisation du processus de configuration : intégration avec Active Directory

Sujet	Informations
Obtention des informations requises *(à la page 173)*	Obtenez des informations sur votre serveur Windows™ Active Directory ; elles sont nécessaires pour l'intégration à Unica.
Appartenance à un groupe, mappage et accès à une application *(à la page 175)*	Si vous utilisez une synchronisation basée sur les groupes, identifiez ou créez les groupes dans Unica Platform auxquels vous allez mapper vos groupes Active Directory.
Stockage des données d'identification du serveur d'annuaire dans Unica Platform *(à la page 176)*	Si votre serveur d'annuaire n'autorise pas les accès anonymes (configuration la plus courante), configurez un compte utilisateur

Tableau 37. Organisation du processus de configuration : intégration avec Active Directory (suite)

Sujet	Informations
	Unica comportant un nom d'utilisateur et un mot de passe d'administrateur de serveur d'annuaire.
• Définition des propriétés de connexion de la méthode de connexion LDAP dans Unica *(à la page 178)* • Définition des propriétés de synchronisation LDAP *(à la page 178)* • Définition des propriétés de mappage des attributs utilisateur *(à la page 179)* • Mappage de groupes LDAP à des groupes Unica *(à la page 181)*	Définissez des valeurs sur la page de configuration pour configurer Unica Platform pour l'intégration.
Test de la synchronisation *(à la page 182)*	Vérifiez que l'importation des utilisateurs se passe comme prévu et, si vous utilisez une synchronisation basée sur les groupes, vérifiez que les utilisateurs et les groupes se synchronisent correctement.
Configuration d'un utilisateur Active Directory disposant de droits PlatformAdminRole *(à la page 182)*	Définissez l'accès administrateur à Unica Platform ; cela est nécessaire lorsque l'authentification NTLMv2 est activée.
Définition du mode de sécurité pour l'activation de l'authentification NTLMv2 *(à la page 182)*	Définissez les valeurs du mode de sécurité sur la page de configuration.
Configuration d'Internet Explorer *(à la page)*	Définissez un niveau de sécurité personnalisé dans chaque instance d'Internet Explorer utilisée pour accéder à Unica. Cette

Tableau 37. Organisation du processus de configuration : intégration avec Active Directory (suite)

Sujet	Informations
	opération est nécessaire avec l'authentification NTLMv2 pour ne pas afficher l'écran de connexion Unica pour les utilisateurs.
Redémarrage du serveur d'applications Web *(à la page 183)*	Cette étape est obligatoire pour s'assurer que tous les changements sont appliqués.
Test de la connexion en tant qu'utilisateur Active Directory *(à la page 183)*	Vérifiez que vous pouvez vous identifier en tant qu'utilisateur Active Directory dans Unica.

Obtention des informations requises

Procurez-vous les informations requises sur le serveur d'annuaire avec lequel vous souhaitez effectuer l'intégration. Vous pouvez utiliser ces informations durant le processus de configuration pour stocker les données d'identification du serveur d'annuaire et pour définir les valeurs des propriétés de configuration.

Collectez les informations suivantes.

- Procurez-vous le nom d'hôte du serveur et le port associé.
- Identifiez un utilisateur autorisé à effectuer des recherches sur le serveur d'annuaire et collectez les informations suivantes à propos de cet utilisateur.
  - nom de connexion
  - mot de passe
  - Nom distinctif (DN)
- Procurez-vous les informations suivantes sur le serveur d'annuaire.
  - Nom de système hôte qualifié complet ou adresse IP
  - Port d'écoute du serveur
- Déterminez quelle chaîne votre serveur d'annuaire utilise pour l'attribut utilisateur dans l'objet Groupe. En général, la valeur est `uniquemember` pour les serveurs LDAP

et `member` pour les serveurs Windows™ Active Directory. Vérifiez-la au niveau de votre serveur d'annuaire.

- Procurez-vous les attributs utilisateur obligatoires suivants.
  - Déterminez quelle chaîne votre serveur d'annuaire utilise pour l'attribut de connexion utilisateur. Cette chaîne est toujours obligatoire. Généralement, cette valeur est `uid` dans les serveurs LDAP, et `sAMAccountName` dans les serveurs Windows™ Active Directory. Vérifiez cette chaîne sur votre serveur d'annuaire.
  - Seulement si Unica Campaign est installé dans un environnement UNIX™, déterminez quelle chaîne votre serveur d'annuaire utilise pour l'attribut Autre connexion.
- Si vous utilisez une synchronisation basée sur des attributs, procurez-vous les chaînes utilisées pour les attributs (une ou plusieurs) que vous voulez utiliser à cette fin.
- Si vous souhaitez que Unica Platform importe des attributs utilisateur supplémentaires (facultatif) stockés dans votre serveur d'annuaire, déterminez quelles chaînes votre serveur d'annuaire utilise pour les attributs suivants.
  - Prénom
  - Nom
  - Titre de l'utilisateur
  - Service
  - Société
  - Pays
  - Adresse e-mail de l'utilisateur
  - Adresse 1
  - Téléphone bureau
  - Téléphone cellulaire
  - Téléphone du domicile

A propos des noms uniques

Pour permettre l'intégration du serveur d'annuaire dans Unica, vous devez définir le nom unique (DN) d'un utilisateur et de groupes. Le DN d'un objet du serveur d'annuaire est le chemin d'accès complet à cet objet dans la structure d'arborescence du serveur d'annuaire.

Les noms uniques possèdent les composants suivants :

- Unité organisationnelle. Cet attribut permet de définir un espace de nom en fonction de la structure organisationnelle. Une unité organisationnelle est généralement associée à un conteneur ou dossier de serveurs d'annuaire créé par un utilisateur.
- Nom courant. Cet attribut représente l'objet lui-même dans le serveur d'annuaire.
- Composant de domaine. Nom unique qui utilise les attributs de composant de domaine et possède un composant de domaine pour chaque niveau de domaine sous la racine. En d'autres termes, chaque élément séparé par un point dans le nom du domaine possède un attribut de composant de domaine.

Pour déterminer le nom unique d'un objet, aidez-vous de la console d'administration du serveur d'annuaire.

Appartenance à un groupe, mappage et accès à une application

Lorsque vous planifiez le mappage de vos groupes de serveur d'annuaire aux groupes Unica Platform, procédez comme indiqué ci-après.

- Identifiez ou créez les groupes de serveurs d'annuaire dont vous souhaitez importer les membres dans Unica Platform. Lorsque ces groupes sont mappés à des groupes Unica Platform, leurs membres sont automatiquement créés en tant qu'utilisateurs Unica.

  Les membres des sous-groupes du serveur d'annuaire ne sont pas importés automatiquement. Pour les importer, vous devez mapper les sous-groupes à des groupes ou sous-groupes Unica Platform.

  Mappez uniquement des groupes de serveur d'annuaire statiques. Les groupes dynamiques ou virtuels ne sont pas pris en charge.
- Identifiez ou créez les groupes Unica Platform auxquels vous allez mapper les groupes de serveurs d'annuaire.
- Affectez l'accès d'application approprié aux groupes que vous souhaitez mapper.

Stockage des données d'identification du serveur d'annuaire dans Unica Platform

Si le serveur d'annuaire n'autorise pas l'accès anonyme, vous devez configurer un compte utilisateur Unica afin qu'il contienne le nom d'utilisateur et le mot de passe d'un utilisateur du serveur d'annuaire, comme décrit dans la procédure suivante.

1. Connectez vous à Unica en tant qu'utilisateur avec des droits d'administrateur.
2. Sélectionnez ou créez un compte utilisateur Unica devant contenir les données d'identification du serveur d'annuaire d'un utilisateur LDAP disposant d'un accès en lecture à toutes les informations relatives aux utilisateurs et aux groupes du serveur LDAP. Respectez les consignes décrites ci-après.
   - Vous définirez ultérieurement la propriété de configuration `Unica Platform pour les données d'identification LDAP` sur le nom d'utilisateur associé à ce compte utilisateur Unica. La valeur par défaut de cette propriété est `asm_admin`, qui correspond à un utilisateur présent dans toute nouvelle installation de Unica Platform. Vous pouvez utiliser le compte `asm_admin` pour enregistrer les données d'identification du serveur d'annuaire.
   - Le nom d'utilisateur de ce compte utilisateur d'Unica ne doit pas correspondre à celui d'un utilisateur du serveur d'annuaire.
3. Ajoutez une source de données à ce compte utilisateur Unica afin de stocker les données d'identification utilisées par Unica Platform pour se connecter au serveur LDAP. Respectez les consignes décrites ci-après.

Tableau 38. Zones de source de données pour le stockage des données d'identification

Zone	Instruction
Nom de la source de données	Vous pouvez entrer n'importe quel nom, mais notez que le nom de source de données que vous indiquez doit correspondre à la valeur de la propriété `Source de données pour les données d'identification LDAP` que vous définirez ultérieurement. Afin qu'il y ait une correspondance avec la

Zone	Instruction
	valeur par défaut de cette propriété et que vous n'ayez pas à définir la valeur, nommez la source de données `LDAPServer`.

Connexion à la source de données	Entrez le nom unique (DN) de l'utilisateur qui dispose de droits d'administration et d'un accès en lecture à toutes les informations relatives aux utilisateurs et aux groupes du serveur d'annuaire qui seront synchronisées avec Unica. Le DN se présente comme suit :
	`uidcn=user1,ou=someGroup,dc=systemName,dc=com`
	Vous pouvez aussi utiliser le compte utilisateur racine qui a accès à tous les groupes sur le serveur LDAP. L'utilisateur racine par défaut et le mode de spécification de cet utilisateur pour les serveurs d'annuaire pris en charge sont les suivants :
	• L'utilisateur racine pour le serveur Active Directory est Administrator. Vous pouvez définir cet utilisateur comme suit :
	`domain\`*`ldap_admin_username`*
	• L'utilisateur racine pour Oracle Directory Server est Directory Manager. Vous pouvez définir cet utilisateur comme suit :
	`cn=Directory Manager`
	• L'utilisateur racine pour IBM Security Directory Server est root. Vous pouvez définir cet utilisateur comme suit :
	`cn=root`

Mot de passe de la source de données	Entrez le mot de passe de l'administrateur dont vous avez entré le nom de connexion dans la zone **Connexion à la source de données**.

Définition des propriétés de connexion de la méthode de connexion LDAP dans Unica

Les propriétés de la méthode de connexion LDAP définissent les détails de connexion utilisés par le système pour se connecter au serveur d'annuaire.

1. Cliquez sur **Paramètres > Configuration** et sélectionnez la catégorie **Unica Platform | Sécurité | Détails du mode de connexion | LDAP**.
2. Définissez les valeurs des propriétés de configuration suivantes.

   Voir la référence associée pour plus de détails sur la façon de définir chaque propriété.

   - Nom de serveur hôte LDAP
   - Port de serveur LDAP
   - Filtre de recherche utilisateur
   - Utiliser les données d'identification stockées dans Unica Platform
   - Utilisateur d'Unica Platform pour les données d'identification LDAP
   - Source de données pour les données d'identification LDAP
   - Nom distinctif de base
   - SSL requis pour la connexion LDAP

Définition des propriétés de synchronisation LDAP

Les propriétés de synchronisation LDAP définissent les détails qui sont utilisés par le système pour se connecter au serveur d'annuaire et pour identifier les utilisateurs à importer. Certaines de ces propriétés contrôlent également la fréquence et les autres détails du processus de synchronisation automatique.

1. Cliquez sur **Paramètres > Configuration** et sélectionnez la catégorie **Platform | Sécurité | Synchronisation LDAP**.
2. Définissez les propriétés de configuration suivantes dans la section **Propriétés LDAP**.

   Consultez l'aide contextuelle de chaque propriété ou le lien de la rubrique connexe de cette section pour obtenir des instructions sur le paramétrage des valeurs.

- Synchronisation LDAP activée
- Intervalle de synchronisation LDAP
- Retard de synchronisation LDAP
- Délai d'attente de synchronisation LDAP
- Portée de la synchronisation LDAP
- URL du fournisseur LDAP
- SSL requis pour la connexion LDAP (facultatif)
- Délimiteur de groupe Unica Platform de configuration LDAP
- Délimiteur de configuration de référence LDAP
- Utilisateur d'Unica Platform pour les données d'identification LDAP
- Source de données pour les données d'identification LDAP
- Nom d'attribut de référence de l'utilisateur LDAP
- Recherche périodique de nom distinctif de base LDAP désactivée
- Nom de connexion de l'utilisateur
- Différents attributs utilisateur tels que le service, le pays et titre de l'utilisateur (facultatif)

Définition des propriétés de mappage des attributs utilisateur

Ces propriétés définissent les attributs utilisateur que le système importe à partir du serveur d'annuaire.

1. Cliquez sur **Paramètres > Configuration** et sélectionnez la catégorie **Platform | Sécurité | Synchronisation LDAP**.
2. Configurez les valeurs de la section **Mappage des attributs utilisateur** pour mapper les attributs répertoriés de l'utilisateur d'Unica aux attributs utilisateur de votre serveur d'annuaire.

   Si vous utilisez une synchronisation basée sur des groupes, la seule propriété que vous êtes obligé de mapper est `User login` (Nom de connexion de l'utilisateur). Généralement, cette valeur est `uid` dans les serveurs LDAP, et `sAMAccountName` dans les serveurs Windows™ Active Directory. Utilisez la valeur observée comme décrit dans "Obtention des informations requises."

Si vous utilisez une synchronisation basée sur des attributs, mappez les attributs sur lesquels vous voulez effectuer la recherche.

Prenez connaissance des informations suivantes.

- Les propriétés que vous mappez ici sont remplacées pour les utilisateurs importés à chaque synchronisation de Unica Platform avec votre serveur d'annuaire.
- Dans Unica Platform, les formats d'adresses e-mail doivent être conformes à la définition de la norme RFC 821. Si ce n'est pas le cas, ne les mappez pas en tant qu'attributs à importer.
- Si la base de données de votre serveur d'annuaire accepte qu'un attribut comporte davantage de caractères que les tables système Unica Platform, comme indiqué dans le tableau ci-dessous, la valeur de l'attribut est tronquée.

Tableau 39. Nombre de caractères autorisés pour les attributs utilisateur

Attribut	Longueur autorisée
Connexion de l'utilisateur (obligatoire)	256
Prénom	128
Nom	128
Titre de l'utilisateur	128
Service	128
Société	128
Pays	128
Adresse e-mail de l'utilisateur	128
Adresse 1	128
Téléphone bureau	20

Attribut	Longueur autorisée
Téléphone cellulaire	20
Téléphone du domicile	20
Connexion alternative (requise sur UNIX™)	256

Mappage de groupes LDAP à des groupes Unica

Les utilisateurs des groupes de serveurs d'annuaire que vous mappez ici sont importés et deviennent membres des groupes Unica Platform spécifiés.

Important : Ne mappez aucun des groupes qui possèdent l'utilisateur `asm_admin` comme membre.

1. Cliquez sur **Paramètres > Configuration** et accédez à la catégorie **Unica | Unica Platform | Sécurité | Synchronisation LDAP | Référence LDAP à la mappe du groupe Unica Platform**.
2. Pour chaque groupe de serveurs d'annuaire que vous souhaitez mapper à un groupe Unica Platform, créez une catégorie **Référence LDAP au groupe Unica Platform** à l'aide du modèle *(LDAP reference to Unica Platform group map)* . Définissez les propriétés suivantes.
   - `Nom de la nouvelle catégorie`
   - `Mappe de référence LDAP`
   - `Groupe Unica Platform`

   Par exemple, les valeurs suivantes mappent le groupe LDAP `MarketingPlatformUsers` aux groupes Unica Platform `marketingopsUsers` et `campaignUsers` (`FILTER` est omis).

   - `Référence LDAP : cn=MarketingPlatformUsers,cn=Users, dc=myCompany,dc=com`
   - `Groupe Unica Platform : marketingopsUsers;campaignUsers`

Test de la synchronisation

Vérifiez que les utilisateurs et les groupes sont correctement synchronisés entre les serveurs.

1. Connectez-vous à Unica en tant qu'utilisateur Unica disposant de droits administrateur (pas en tant qu'utilisateur du serveur d'annuaire).
2. Forcez la synchronisation en cliquant sur **Synchroniser** dans la page **Paramètres > Utilisateurs**.
3. Effectuez les vérifications suivantes :
    - Vérifiez que les utilisateurs sont importés à partir du serveur LDAP comme prévu.
    - Si vous utilisez une synchronisation basée sur des groupes, vérifiez que les appartenances aux groupes Unica Platform correspondent bien au mappage attendu pour les groupes de serveurs d'annuaire.

Configuration d'un utilisateur Active Directory disposant de droits PlatformAdminRole

Lorsque l'authentification NTLMv2 est activée, vous ne pouvez pas vous connecter à Unica comme `platform_admin` et vous devez donc exécuter la procédure suivante pour disposer d'un accès administrateur à Unica Platform.

1. Connectez-vous à Unica en tant qu'utilisateur interne (utilisateur créé dans Unica Platform et non importé depuis Active Directory). Il doit s'agir d'un utilisateur disposant de droits PlatformAdminRole dans Unica Platform.
2. Créez un groupe Unica Platform auquel vous affecterez le rôle PlatformAdminRole.
3. Vérifiez qu'au moins un utilisateur Windows™ Active Directory est membre de ce groupe.

Définition du mode de sécurité pour l'activation de l'authentification NTLMv2

Définissez des propriétés de configuration comme indiqué dans cette procédure uniquement si vous souhaitez activer l'authentification NTLMv2.

Configurez l'authentification NTLMv2.

Cliquez sur **Paramètres > Configuration** et définissez des propriétés de configuration comme indiqué dans le tableau suivant.

Tableau 40. Valeurs des propriétés de configuration de NTLMv2

Propriété	Valeur
Platform | Sécurité | Méthode de connexion	Sélectionnez l'option `Contrôle de l'accès Web`.
Platform | Sécurité | Détails du mode de connexion | Contrôle d'accès Web | Variable d'en-tête de contrôle d'accès Web	Entrez le nom de la variable, comme indiqué dans les règles de réécriture.
Platform | Sécurité | Détails du mode de connexion | Contrôle de l'accès Web | Modèle de nom d'utilisateur	Entrez `\w*`
Général | Navigation | URL de Platform	Entrez l'URL du site IIS.

Redémarrage du serveur d'applications Web

Redémarrez le serveur d'applications Web pour vous assurer que toutes les modifications de configuration sont appliquées.

Test de la connexion en tant qu'utilisateur Active Directory

Vérifiez la configuration en vous connectant à Unica avec un compte utilisateur Windows™ Active Directory approprié.

1. Connectez-vous à Windows™ comme utilisateur Active Directory membre d'un groupe Active Directory associé à un groupe Unica Platform affecté d'un rôle dans Unica Platform.
2. Faites pointer votre navigateur vers l'URL de Unica.

   Si vous avez activé l'authentification NTLMv2, vous ne devriez pas voir l'écran de connexion d'Unica, et vous devriez avoir accès à l'interface utilisateur d'Unica.

Si vous n'avez pas activé l'authentification NTLMv2, vous devriez pouvoir vous connecter avec vos données d'identification Windows.

Si vous ne parvenez pas à vous connecter, consultez restoreAccess (à la page 357).

Intégration entre les serveurs Unica et LDAP

Unica Platform peut être configuré pour être intégré au serveur Windows™ Active Directory ou à un autre serveur LDAP (Lightweight Directory Access Protocol). L'intégration d'Unica à un serveur d'annuaire vous permet de centraliser l'emplacement des utilisateurs et des groupes. L'intégration permet d'étendre de manière flexible les stratégies d'autorisation d'entreprise dans les applications d'Unica. Elle permet également de réduire les coûts de support et le temps nécessaire pour déployer une application en production.

Pour obtenir la liste des serveurs d'annuaire pris en charge, consultez le document Environnements logiciels recommandés et configuration minimale requise.

Fonctionnalités d'intégration LDAP

L'intégration de Unica Platform avec LDAP permet d'obtenir les fonctionnalités décrites dans cette section.

Authentification avec intégration à LDAP

Les applications Unica recherchent des informations d'autorisation utilisateur sur Unica Platform. Lorsque l'intégration à LDAP est implémentée, les utilisateurs saisissent leur nom d'utilisateur et mot de passe LDAP valides afin de s'authentifier auprès des applications d'Unica.

Gestion des utilisateurs internes et externes

Une fois l'intégration configurée, vous ne pouvez ni ajouter, ni modifier ni supprimer les comptes utilisateur importés dans Unica Platform. Vous devez effectuer ces tâches de gestion au niveau de LDAP et les modifications seront importées au moment de la synchronisation. Si vous modifiez des comptes utilisateur importés dans Unica Platform, les utilisateurs risquent de rencontrer des problèmes au moment de l'authentification.

Les comptes utilisateur que vous supprimez au niveau de LDAP ne sont pas supprimés de Unica Platform. Vous devez désactiver manuellement ces comptes dans Unica Platform. Il est préférable de désactiver ces comptes utilisateur plutôt que de les supprimer car les utilisateurs possèdent des droits de propriété sur les dossiers dans Unica Campaign et, si vous supprimez un compte utilisateur qui possède un dossier, les objets contenus dans ce dossier ne seront plus disponibles.

Synchronisation

Si Unica est configuré pour s'intégrer à un serveur LDAP, les utilisateurs et les groupes seront automatiquement synchronisés à des intervalles prédéfinis.

La synchronisation automatique a une fonctionnalité limitée.

- Les utilisateurs qui sont supprimés du serveur LDAP ne sont pas supprimés lors de la synchronisation automatique.

Vous pouvez forcer la synchronisation intégrale de tous les utilisateurs et tous les groupes en utilisant la fonction Synchroniser dans la zone Utilisateurs d'Unica. Sinon, vous pouvez contacter Services pour demander la définition d'une propriété de configuration masquée qui déclenche une synchronisation automatique complète.

Importation d'utilisateurs basée sur des groupes ou des attributs

Si vous importez des comptes utilisateur à partir du serveur LDAP dans Unica Platform, vous avez le choix entre deux types de filtrage lors de la sélection de ces comptes utilisateur.

Vous devez choisir entre l'importation basée sur des groupes ou l'importation basée sur des attributs. Ces méthodes ne peuvent pas être prises en charge simultanément.

Importation basée sur le groupe

Unica Platform importe les groupes et les utilisateurs à partir de la base de données de serveur d'annuaire via une tâche de synchronisation périodique qui extrait automatiquement les informations à partir du serveur d'annuaire. Si Unica Platform importe les utilisateurs et les groupes à partir de la base de données du serveur, les appartenances de groupe

ne sont pas modifiées. Pour sélectionner ces modifications, vous devez effectuer une synchronisation manuelle.

Remarque : Les groupes LDAP doivent avoir un nom unique, même s'ils sont configurés pour des partitions séparés.

Vous pouvez accorder des privilèges Unica en mappant un groupe LDAP à un groupe d'Unica. Ce mappage permet aux nouveaux utilisateurs ajoutés au groupe LDAP mappé de disposer des privilèges définis pour le groupe d'Unica.

Un sous-groupe existant dans Unica Platform n'hérite pas des mappages LDAP ou des appartenances d'utilisateur de ses parents.

La configuration de l'importation par groupe est détaillée dans la suite de ce chapitre.

Importation basée sur l'attribut

Si vous ne voulez pas créer sur votre serveur LDAP de groupes qui soient spécifiques aux produits Unica, vous pouvez contrôler quels utilisateurs sont importés en spécifiant des attributs. Pour ce faire, vous devez procéder comme suit pendant la configuration de LDAP.

1. Déterminez la chaîne utilisée sur votre serveur LDAP pour l'attribut à partir duquel vous voulez effectuer le filtrage.
2. Attribuez la valeur `DN` à la propriété **Platform | Sécurité | Synchronisation LDAP | Nom d'attribut de référence de l'utilisateur LDAP**.

   Cela signale à Unica Platform que la synchronisation n'est pas basée sur un groupe avec des références de membres, mais sur une unité organisationnelle ou une organisation (Org Unit ou Org).
3. Lorsque vous configurez la propriété **Mappe de référence LDAP**, définissez la portion Filter de la valeur avec l'attribut sur lequel vous voulez effectuer la recherche. Pour le filtre, utilisez la chaîne que vous avez déterminée au point 1.

Lorsque vous utilisez une synchronisation basée sur des attributs, la synchronisation périodique est toujours une synchronisation complète et non une synchronisation partielle, comme c'est le cas pour la synchronisation basée sur des groupes. Pour la synchronisation

basée sur des attributs, vous devez donner à la propriété **Intervalle de synchronisation LDAP** une valeur élevée ou une valeur `0` si vous voulez désactiver la synchronisation automatique et vous contenter de la synchronisation complète manuelle lorsque des utilisateurs sont ajoutés à l'annuaire.

A propos de LDAP et des partitions

Dans des environnements à plusieurs partitions, l'appartenance à une partition d'un utilisateur est déterminée par le groupe dont fait partie l'utilisateur lorsque ce groupe est affecté à une partition. Un utilisateur ne peut faire partie que d'une seule partition à la fois. Si l'utilisateur fait partie de plusieurs groupes LDAP mappés à des groupes d'Unica eux-mêmes affectés à différentes partitions, le système doit choisir une seule partition pour cet utilisateur.

Essayez d'éviter cette situation. Si toutefois elle venait à se produire, la partition du groupe d'Unica à laquelle appartient l'utilisateur est celle qui a été la plus récemment mappée à un groupe LDAP. Pour déterminer le groupe LDAP qui a été le plus récemment mappé, consultez les mappages de groupe LDAP affichés dans la zone Configuration. Ils s'affichent dans l'ordre chronologique, le plus récent étant le dernier élément de la liste.

Prise en charge des utilisateurs internes et externes

Unica prend en charge deux types de comptes et groupes d'utilisateur.

- **Interne** - Comptes et groupes d'utilisateurs créés dans Unica à l'aide de l'interface utilisateur de sécurité d'Unica. Ces utilisateurs sont authentifiés via Unica Platform.
- **Externe** – Comptes et groupes d'utilisateurs importés dans Unica par synchronisation avec un serveur LDAP pris en charge. La synchronisation n'a lieu que si Unica a été configuré pour s'intégrer au serveur LDAP. Ces utilisateurs sont authentifiés via le serveur LDAP.

Il est préférable de disposer des deux types d'utilisateur et de groupe si, par exemple, vous souhaitez autoriser les clients à accéder aux applications d'Unica sans les ajouter au serveur LDAP en tant qu'utilisateurs jouissant de tous les droits.

L'utilisation de ce modèle d'authentification hybride nécessite davantage de maintenance qu'un modèle d'authentification LDAP standard.

Caractères spéciaux dans les noms de connexion

Seuls trois caractères spéciaux sont autorisés dans les noms de connexion : le point (.), le trait de soulignement (_) et le trait d'union (-). Si d'autres caractères spéciaux (notamment des espaces) figurent dans le nom de connexion d'un utilisateur que vous envisagez d'importer dans Unica Platform depuis un serveur LDAP, vous devez modifier ce nom de connexion afin que l'utilisateur ne rencontre pas d'incident lors de sa déconnexion ou lorsqu'il exécutera des tâches d'administration (s'il a les droits requis pour cela).

Conditions requises pour l'intégration à LDAP

Pour tirer parti des fonctions d'intégration à LDAP, vous devez installer les applications Unica sur un système d'exploitation compatible.

Organisation du processus de configuration : Intégration LDAP

Cette feuille de route du processus de configuration permet d'analyser les tâches requises pour intégrer Unica avec LDAP. La colonne Rubrique contient des liens vers les rubriques qui décrivent les tâches en détail.

Tableau 41. Organisation du processus de configuration : Intégration LDAP

Sujet	Informations
Obtention des informations requises *(à la page 173)*	Procurez-vous les informations relatives à votre serveur LDAP qui sont requises pour l'intégration à Unica.
Appartenance à un groupe, mappage et accès à une application *(à la page 175)*	Si vous utilisez une synchronisation basée sur les groupes, identifiez ou créez dans Unica Platform les groupes auxquels vous allez mapper vos groupes LDAP.

Tableau 41. Organisation du processus de configuration : Intégration LDAP (suite)

Sujet	Informations
Stockage des données d'identification du serveur d'annuaire dans Unica Platform *(à la page 176)*	Si votre serveur d'annuaire n'autorise pas les accès anonymes (configuration la plus courante), configurez un compte utilisateur Unica comportant un nom d'utilisateur et un mot de passe d'administrateur de serveur d'annuaire.
• Définition des propriétés de connexion de la méthode de connexion LDAP dans Unica *(à la page 178)* • Définition des propriétés de synchronisation LDAP *(à la page 178)* • Définition des propriétés de mappage des attributs utilisateur *(à la page 179)* • Mappage de groupes LDAP à des groupes Unica *(à la page 181)*	Définissez des valeurs sur la page de configuration pour configurer Unica Platform pour l'intégration.
Test de la synchronisation *(à la page 182)*	Vérifiez que l'importation des utilisateurs se passe comme prévu et, si vous utilisez une synchronisation basée sur les groupes, vérifiez que les groupes se synchronisent correctement.
Définition du mode de sécurité sur LDAP *(à la page 199)*	Définissez les valeurs du mode de sécurité sur la page de configuration.
Redémarrage du serveur d'applications Web *(à la page 183)*	Cette étape est obligatoire pour s'assurer que tous les changements sont appliqués.
Test de la connexion en tant qu'utilisateur LDAP *(à la page 199)*	Vérifiez que vous pouvez vous identifier en tant qu'utilisateur LDAP sous Unica.

Obtention des informations requises

Procurez-vous les informations requises sur le serveur d'annuaire avec lequel vous souhaitez effectuer l'intégration. Vous pouvez utiliser ces informations durant le processus de configuration pour stocker les données d'identification du serveur d'annuaire et pour définir les valeurs des propriétés de configuration.

Collectez les informations suivantes.

- Procurez-vous le nom d'hôte du serveur et le port associé.
- Identifiez un utilisateur autorisé à effectuer des recherches sur le serveur d'annuaire et collectez les informations suivantes à propos de cet utilisateur.
    - nom de connexion
    - mot de passe
    - Nom distinctif (DN)
- Procurez-vous les informations suivantes sur le serveur d'annuaire.
    - Nom de système hôte qualifié complet ou adresse IP
    - Port d'écoute du serveur
- Déterminez quelle chaîne votre serveur d'annuaire utilise pour l'attribut utilisateur dans l'objet Groupe. En général, la valeur est `uniquemember` pour les serveurs LDAP et `member` pour les serveurs Windows™ Active Directory. Vérifiez-la au niveau de votre serveur d'annuaire.
- Procurez-vous les attributs utilisateur obligatoires suivants.
    - Déterminez quelle chaîne votre serveur d'annuaire utilise pour l'attribut de connexion utilisateur. Cette chaîne est toujours obligatoire. Généralement, cette valeur est `uid` dans les serveurs LDAP, et `sAMAccountName` dans les serveurs Windows™ Active Directory. Vérifiez cette chaîne sur votre serveur d'annuaire.
    - Seulement si Unica Campaign est installé dans un environnement UNIX™, déterminez quelle chaîne votre serveur d'annuaire utilise pour l'attribut Autre connexion.
- Si vous utilisez une synchronisation basée sur des attributs, procurez-vous les chaînes utilisées pour les attributs (une ou plusieurs) que vous voulez utiliser à cette fin.

- Si vous souhaitez que Unica Platform importe des attributs utilisateur supplémentaires (facultatif) stockés dans votre serveur d'annuaire, déterminez quelles chaînes votre serveur d'annuaire utilise pour les attributs suivants.
    - Prénom
    - Nom
    - Titre de l'utilisateur
    - Service
    - Société
    - Pays
    - Adresse e-mail de l'utilisateur
    - Adresse 1
    - Téléphone bureau
    - Téléphone cellulaire
    - Téléphone du domicile

A propos des noms uniques

Pour permettre l'intégration du serveur d'annuaire dans Unica, vous devez définir le nom unique (DN) d'un utilisateur et de groupes. Le DN d'un objet du serveur d'annuaire est le chemin d'accès complet à cet objet dans la structure d'arborescence du serveur d'annuaire.

Les noms uniques possèdent les composants suivants :

- Unité organisationnelle. Cet attribut permet de définir un espace de nom en fonction de la structure organisationnelle. Une unité organisationnelle est généralement associée à un conteneur ou dossier de serveurs d'annuaire créé par un utilisateur.
- Nom courant. Cet attribut représente l'objet lui-même dans le serveur d'annuaire.
- Composant de domaine. Nom unique qui utilise les attributs de composant de domaine et possède un composant de domaine pour chaque niveau de domaine sous la racine. En d'autres termes, chaque élément séparé par un point dans le nom du domaine possède un attribut de composant de domaine.

Pour déterminer le nom unique d'un objet, aidez-vous de la console d'administration du serveur d'annuaire.

Appartenance à un groupe, mappage et accès à une application

Lorsque vous planifiez le mappage de vos groupes de serveur d'annuaire aux groupes Unica Platform, procédez comme indiqué ci-après.

- Identifiez ou créez les groupes de serveurs d'annuaire dont vous souhaitez importer les membres dans Unica Platform. Lorsque ces groupes sont mappés à des groupes Unica Platform, leurs membres sont automatiquement créés en tant qu'utilisateurs Unica.

  Les membres des sous-groupes du serveur d'annuaire ne sont pas importés automatiquement. Pour les importer, vous devez mapper les sous-groupes à des groupes ou sous-groupes Unica Platform.

  Mappez uniquement des groupes de serveur d'annuaire statiques. Les groupes dynamiques ou virtuels ne sont pas pris en charge.
- Identifiez ou créez les groupes Unica Platform auxquels vous allez mapper les groupes de serveurs d'annuaire.
- Affectez l'accès d'application approprié aux groupes que vous souhaitez mapper.

Stockage des données d'identification du serveur d'annuaire dans Unica Platform

Si le serveur d'annuaire n'autorise pas l'accès anonyme, vous devez configurer un compte utilisateur Unica afin qu'il contienne le nom d'utilisateur et le mot de passe d'un utilisateur du serveur d'annuaire, comme décrit dans la procédure suivante.

1. Connectez vous à Unica en tant qu'utilisateur avec des droits d'administrateur.
2. Sélectionnez ou créez un compte utilisateur Unica devant contenir les données d'identification du serveur d'annuaire d'un utilisateur LDAP disposant d'un accès en lecture à toutes les informations relatives aux utilisateurs et aux groupes du serveur LDAP. Respectez les consignes décrites ci-après.
   - Vous définirez ultérieurement la propriété de configuration `Unica Platform pour les données d'identification LDAP` sur le nom d'utilisateur associé à ce compte utilisateur Unica. La valeur par défaut de cette propriété est `asm_admin`, qui correspond à un utilisateur présent dans toute nouvelle

installation de Unica Platform. Vous pouvez utiliser le compte `asm_admin` pour enregistrer les données d'identification du serveur d'annuaire.

- Le nom d'utilisateur de ce compte utilisateur d'Unica ne doit pas correspondre à celui d'un utilisateur du serveur d'annuaire.

3. Ajoutez une source de données à ce compte utilisateur Unica afin de stocker les données d'identification utilisées par Unica Platform pour se connecter au serveur LDAP. Respectez les consignes décrites ci-après.

Tableau 42. Zones de source de données pour le stockage des données d'identification

Zone	Instruction
Nom de la source de données	Vous pouvez entrer n'importe quel nom, mais notez que le nom de source de données que vous indiquez doit correspondre à la valeur de la propriété `Source de données pour les données d'identification LDAP` que vous définirez ultérieurement. Afin qu'il y ait une correspondance avec la valeur par défaut de cette propriété et que vous n'ayez pas à définir la valeur, nommez la source de données `LDAPServer`.
Connexion à la source de données	Entrez le nom unique (DN) de l'utilisateur qui dispose de droits d'administration et d'un accès en lecture à toutes les informations relatives aux utilisateurs et aux groupes du serveur d'annuaire qui seront synchronisées avec Unica. Le DN se présente comme suit : `uidcn=user1,ou=someGroup,dc=systemName,dc=com` Vous pouvez aussi utiliser le compte utilisateur racine qui a accès à tous les groupes sur le serveur LDAP. L'utilisateur racine par défaut et le mode de spécification de cet utilisateur pour les serveurs d'annuaire pris en charge sont les suivants :

Zone	Instruction

	• L'utilisateur racine pour le serveur Active Directory est Administrator. Vous pouvez définir cet utilisateur comme suit :
	`domain\ldap_admin_username`
	• L'utilisateur racine pour Oracle Directory Server est Directory Manager. Vous pouvez définir cet utilisateur comme suit :
	`cn=Directory Manager`
	• L'utilisateur racine pour IBM Security Directory Server est root. Vous pouvez définir cet utilisateur comme suit :
	`cn=root`

Mot de passe de la source de données	Entrez le mot de passe de l'administrateur dont vous avez entré le nom de connexion dans la zone **Connexion à la source de données**.

Définition des propriétés de connexion de la méthode de connexion LDAP dans Unica

Les propriétés de la méthode de connexion LDAP définissent les détails de connexion utilisés par le système pour se connecter au serveur d'annuaire.

1. Cliquez sur **Paramètres > Configuration** et sélectionnez la catégorie **Unica Platform | Sécurité | Détails du mode de connexion | LDAP**.
2. Définissez les valeurs des propriétés de configuration suivantes.

   Voir la référence associée pour plus de détails sur la façon de définir chaque propriété.

   - `Nom de serveur hôte LDAP`
   - `Port de serveur LDAP`
   - `Filtre de recherche utilisateur`

- Utiliser les données d'identification stockées dans Unica Platform
- Utilisateur d'Unica Platform pour les données d'identification LDAP
- Source de données pour les données d'identification LDAP
- Nom distinctif de base
- SSL requis pour la connexion LDAP

Définition des propriétés de synchronisation LDAP

Les propriétés de synchronisation LDAP définissent les détails qui sont utilisés par le système pour se connecter au serveur d'annuaire et pour identifier les utilisateurs à importer. Certaines de ces propriétés contrôlent également la fréquence et les autres détails du processus de synchronisation automatique.

1. Cliquez sur **Paramètres > Configuration** et sélectionnez la catégorie **Platform | Sécurité | Synchronisation LDAP**.
2. Définissez les propriétés de configuration suivantes dans la section **Propriétés LDAP**.

   Consultez l'aide contextuelle de chaque propriété ou le lien de la rubrique connexe de cette section pour obtenir des instructions sur le paramétrage des valeurs.

   - Synchronisation LDAP activée
   - Intervalle de synchronisation LDAP
   - Retard de synchronisation LDAP
   - Délai d'attente de synchronisation LDAP
   - Portée de la synchronisation LDAP
   - URL du fournisseur LDAP
   - SSL requis pour la connexion LDAP (facultatif)
   - Délimiteur de groupe Unica Platform de configuration LDAP
   - Délimiteur de configuration de référence LDAP
   - Utilisateur d'Unica Platform pour les données d'identification LDAP
   - Source de données pour les données d'identification LDAP
   - Nom d'attribut de référence de l'utilisateur LDAP
   - Recherche périodique de nom distinctif de base LDAP désactivée

- `Nom de connexion de l'utilisateur`
- Différents attributs utilisateur tels que le service, le pays et titre de l'utilisateur (facultatif)

Définition des propriétés de mappage des attributs utilisateur

Ces propriétés définissent les attributs utilisateur que le système importe à partir du serveur d'annuaire.

1. Cliquez sur **Paramètres > Configuration** et sélectionnez la catégorie **Platform | Sécurité | Synchronisation LDAP**.
2. Configurez les valeurs de la section **Mappage des attributs utilisateur** pour mapper les attributs répertoriés de l'utilisateur d'Unica aux attributs utilisateur de votre serveur d'annuaire.

   Si vous utilisez une synchronisation basée sur des groupes, la seule propriété que vous êtes obligé de mapper est `User login` (Nom de connexion de l'utilisateur). Généralement, cette valeur est `uid` dans les serveurs LDAP, et `sAMAccountName` dans les serveurs Windows™ Active Directory. Utilisez la valeur observée comme décrit dans "Obtention des informations requises."

   Si vous utilisez une synchronisation basée sur des attributs, mappez les attributs sur lesquels vous voulez effectuer la recherche.

   Prenez connaissance des informations suivantes.

   - Les propriétés que vous mappez ici sont remplacées pour les utilisateurs importés à chaque synchronisation de Unica Platform avec votre serveur d'annuaire.
   - Dans Unica Platform, les formats d'adresses e-mail doivent être conformes à la définition de la norme RFC 821. Si ce n'est pas le cas, ne les mappez pas en tant qu'attributs à importer.
   - Si la base de données de votre serveur d'annuaire accepte qu'un attribut comporte davantage de caractères que les tables système Unica Platform, comme indiqué dans le tableau ci-dessous, la valeur de l'attribut est tronquée.

Tableau 43. Nombre de caractères autorisés pour les attributs utilisateur

Attribut	Longueur autorisée
Connexion de l'utilisateur (obligatoire)	256
Prénom	128
Nom	128
Titre de l'utilisateur	128
Service	128
Société	128
Pays	128
Adresse e-mail de l'utilisateur	128
Adresse 1	128
Téléphone bureau	20
Téléphone cellulaire	20
Téléphone du domicile	20
Connexion alternative (requise sur UNIX™)	256

Mappage de groupes LDAP à des groupes Unica

Les utilisateurs des groupes de serveurs d'annuaire que vous mappez ici sont importés et deviennent membres des groupes Unica Platform spécifiés.

Important : Ne mappez aucun des groupes qui possèdent l'utilisateur `asm_admin` comme membre.

1. Cliquez sur **Paramètres > Configuration** et accédez à la catégorie **Unica | Unica Platform | Sécurité | Synchronisation LDAP | Référence LDAP à la mappe du groupe Unica Platform**.
2. Pour chaque groupe de serveurs d'annuaire que vous souhaitez mapper à un groupe Unica Platform, créez une catégorie **Référence LDAP au groupe Unica Platform** à l'aide du modèle *(LDAP reference to Unica Platform group map)* . Définissez les propriétés suivantes.
    - `Nom de la nouvelle catégorie`
    - `Mappe de référence LDAP`
    - `Groupe Unica Platform`

    Par exemple, les valeurs suivantes mappent le groupe LDAP `MarketingPlatformUsers` aux groupes Unica Platform `marketingopsUsers` et `campaignUsers` (`FILTER` est omis).

    - `Référence LDAP : cn=MarketingPlatformUsers,cn=Users, dc=myCompany,dc=com`
    - `Groupe Unica Platform : marketingopsUsers;campaignUsers`

Test de la synchronisation

Vérifiez que les utilisateurs et les groupes sont correctement synchronisés entre les serveurs.

1. Connectez-vous à Unica en tant qu'utilisateur Unica disposant de droits administrateur (pas en tant qu'utilisateur du serveur d'annuaire).
2. Forcez la synchronisation en cliquant sur **Synchroniser** dans la page **Paramètres > Utilisateurs**.
3. Effectuez les vérifications suivantes :
    - Vérifiez que les utilisateurs sont importés à partir du serveur LDAP comme prévu.
    - Si vous utilisez une synchronisation basée sur des groupes, vérifiez que les appartenances aux groupes Unica Platform correspondent bien au mappage attendu pour les groupes de serveurs d'annuaire.

Définition du mode de sécurité sur LDAP

Définissez les propriétés du mode de sécurité afin de permettre aux utilisateurs LDAP de se connecter aux applications Unica.

1. Connectez-vous à Unica, cliquez sur **Paramètres > Configuration**, puis accédez à **Unica Platform | Sécurité**.
2. Définissez la propriété `Méthode de connexion` sur `LDAP`.

Redémarrage du serveur d'applications Web

Redémarrez le serveur d'applications Web pour vous assurer que toutes les modifications de configuration sont appliquées.

Test de la connexion en tant qu'utilisateur LDAP

Testez votre configuration en vous connectant à Unica en tant qu'utilisateur LDAP membre d'un groupe LDAP mappé vers un groupe Unica Platform qui dispose d'un accès à Unica Platform.

Intégration aux plateformes de contrôle de l'accès Web

Les organisations utilisent les plateformes de contrôle de l'accès Web pour consolider leurs systèmes de sécurité, qui fournissent un portail de régulation de l'accès utilisateur aux sites Web. Cette section offre une présentation de l'intégration d'Unica aux plateformes de contrôle de l'accès Web.

Authentification

Lorsque des utilisateurs accèdent à une application via un portail de contrôle de l'accès Web, leur authentification est traitée dans le système de contrôle de l'accès Web. Les utilisateurs du contrôle de l'accès Web qui sont également membres d'un groupe LDAP qui est synchronisé avec Unica sont authentifiés dans toutes les applications d'Unica lorsqu'ils se connectent au système de contrôle de l'accès Web. Ces utilisateurs ne voient pas les écrans de connexion des applications Unica.

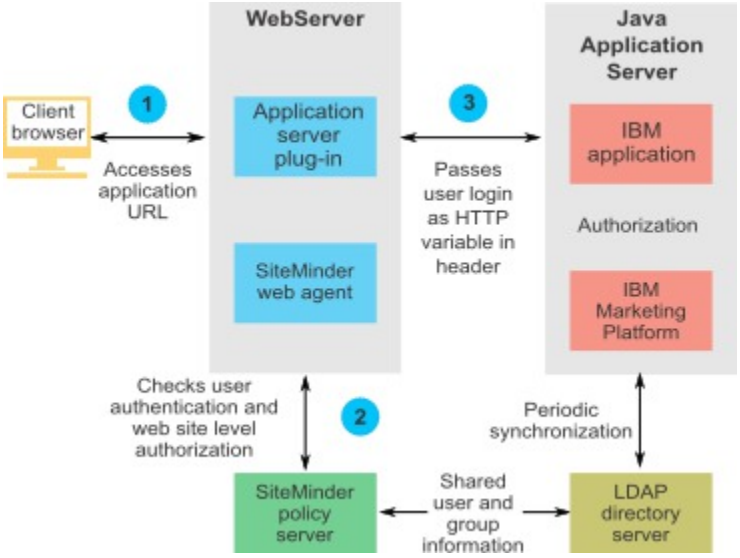
Autorisation

Les applications Unica recherchent des informations d'autorisation utilisateur sur Unica Platform. Unica Platform importe les groupes et leurs utilisateurs à partir de la base de données LDAP via une tâche de synchronisation périodique qui extrait automatiquement les informations à partir du serveur LDAP. Si Unica Platform importe les utilisateurs et les groupes à partir de la base de données LDAP, les appartenances de groupe sont conservées. Ces utilisateurs LDAP sont également exposés dans le système de contrôle de l'accès Web. Ainsi, le système de contrôle de l'accès Web et Unica référencent un ensemble cohérent d'utilisateurs.

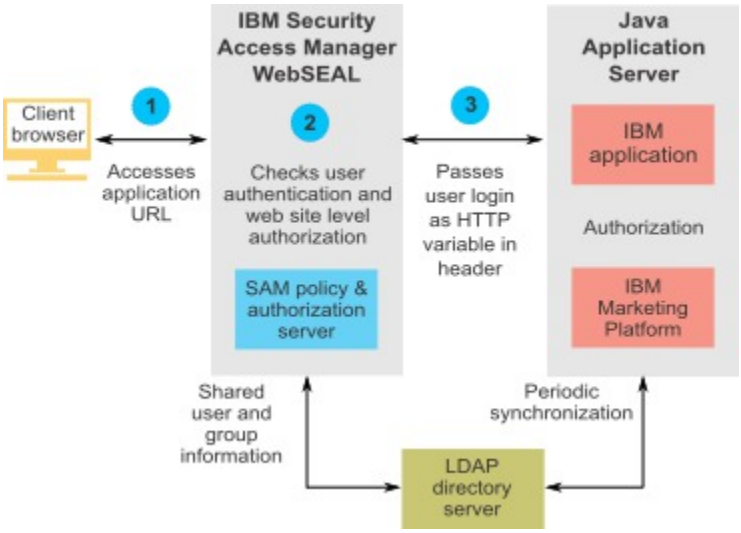
Les contrôles d'autorisation supplémentaires, notamment le contrôle sur les URL d'application auxquelles les utilisateurs ont accès, sont également disponibles via la plupart des systèmes de contrôle de l'accès Web.

Diagrammes d'intégration du contrôle de l'accès Web

La figure suivante illustre le fonctionnement d'Unica avec SiteMinder et un serveur d'annuaire LDAP pour s'authentifier et autoriser les utilisateurs.



La figure suivante illustre le fonctionnement d'Unica avec IBM Security Access Manager et un serveur d'annuaire LDAP pour authentifier et autoriser les utilisateurs.



A propos des racines de contexte

Vous devez déprotéger les URL dans le système de contrôle d'accès Web pour activer les diverses fonctions des produits Unica. Pour cela, vous devez inclure les racines de contexte du produit dans les URL.

La table suivante fournit une liste des racines de contexte par défaut pour les produits Unica mentionnés dans ce chapitre. Il peut arriver que votre installation utilise des racines de contexte autres que les racines de contexte par défaut, mais la plupart des installations acceptent les racines de contexte par défaut.

Les exemples fournis dans ce chapitre utilisent les racines de contexte par défaut. Si votre environnement utilise une racine de contexte non standard, vous devez remplacer la racine de contexte présentée dans les exemples d'URL par celle utilisée dans votre environnement.

Tableau 44. Racines de contexte pour les produits Unica

Produit	Racine de contexte
Unica Platform	unica
Unica Campaign	Campaign
Unica Optimize	Campaign/optimize

Tableau 44. Racines de contexte pour les produits Unica (suite)

Produit	Racine de contexte
Unica Plan	plan
Unica Collaborate	collaborate
Unica Interact	Campaign/interact

Conditions requises pour l'intégration à SiteMinder

Les conditions suivantes doivent être satisfaites pour effectuer l'intégration d'Unica à Netegrity SiteMinder.

- SiteMinder doit être configuré pour utiliser un agent Web et un serveur de stratégies.
- SiteMinder doit être configuré pour transmettre le nom de connexion en tant que variable HTTP dans la demande d'URL à l'application Unica.
- L.a propriété Unica **Variable d'en-tête du contrôle de l'accès Web** doit être définie sur le nom de la variable utilisée par SiteMinder pour les noms de connexion.

  Le nom par défaut de la variable de nom de connexion SiteMinder est `sm_user`.
- Le serveur de règles SiteMinder doit être configuré pour utiliser LDAP comme référentiel de stockage des membres de groupe et des propriétés utilisateur.
- Les URL d'application Unica fournies par le serveur Web qui héberge SiteMinder et le serveur d'applications Java™ qui héberge l'application Unica doivent faire référence au même chemin.
- Le serveur Web qui héberge SiteMinder doit être configuré pour rediriger les demandes vers l'URL d'application Unica sur le serveur d'applications Java™.
- Tous les utilisateurs qui ont besoin d'accéder aux applications d'Unica doivent jouir d'une autorisation d'accès dans SiteMinder aux applications Web d'Unica pour les demandes HTTP `GET` et `POST` via SiteMinder.

Consultez la suite de cette section pour en savoir plus sur les paramètres requis pour l'activation des fonctionnalités spécifiques ou pour la prise en charge de certains produits Unica.

Configuration de SiteMinder pour les produits Unica

Déprotégez les objets dans SiteMinder pour permettre le bon fonctionnement de vos produits Unica, comme indiqué dans cette procédure.

1. Connectez-vous à la zone **Administrer le serveur de stratégie** de SiteMinder et cliquez sur **Domaines**.
2. Sélectionnez le domaine qui s'applique à vos installations , cliquez avec le bouton droit de la souris sur **unprotecturl**, puis sélectionnez **Propriétés du domaine**.
3. Pour chacune des URL applicables décrites dans le tableau suivant, saisissez l'URL dans la zone de texte **Filtre des ressources** et sous **Protection des ressources par défaut**, sélectionnez **Non protégé**.

Table 45. Objets non protégés requis pour les produits Unica

Produit ou fonction	Objets
Unica Campaign	• `/Campagne/services/CampagneServices30Service` • `/Campaign/api/campaign/rest` • `/Campagne/FlowchartNotifyScheduler` • `/Campagne/OperationMonitor` • `http://host:port/Campaign/api/campaign/rest/deepsearch/partition` Remplacez partition par le nom de la partition. Les éléments suivants s'appliquent lorsque l'intégration à Engage est mise en œuvre. Dans les URLs suivantes, remplacez partition par le nom de la partition. • `http://host:port/Campaign/jsp/engage/engageHome.jsp` • `http://host:port/Campaign/api/campaign/rest/engage/offers`

Produit ou fonction	Objets
	• `http://host:port/Campaign/api/campaign/rest/engage/offer` • `http://host:port/Campaign/servlet/EngageUpload` • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition` • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/jobid` Cette URL est destinée à la vérification du statut d'un travail d'importation. Remplacez jobid par votre identifiant de travail. • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/schedule` • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/channel/schedule` Cette URL est destinée à l'envoi d'une commande push ou de messages SMS. Le canal est soit un `sms` soit un `push`.
Unica Journey	• `/journey/api/platformlogin` • `/journey/api/datadefinitions` • `/journey/api/entrysources` • `/journey/api/journeys` • `/journey/api/folders` • `/journey/api/permissions` • `/unica/api/manager/authentication/login` • `/unica/api/manager/user/user-details` • `/unica/api/manager/configuration/get`

Produit ou fonction	Objets
	• `/unica/api/manager/policy/roles-permissions` • `/unica/api/manager/license/7` • `/unica/api/manager/datasource` • `/journey/api/thirdpartylogin`
Unica Collaborate	• `/collaborate/affiniumcollaborate.jsp` • `/collaborate/services/CollaborateIntegrationServices1.0` • `/collaborate/flowchartRunNotifyServlet` • `/collaborate/js/js_messages.jsp` • `/collaborate/js/format_symbols.jsp` • `/collaborate/alertsService`
Unica Deliver	`/Campaign/deliver/eventSinkServlet`
Unica Interact	• `/Campaign/interact/saveFlowchartAction.udo` • `/Campaign/interact/flowchartEventPatterns.udo` • `/Campaign/interact/testRunFlowchart.udo` • `/Campaign/interact/getProfileDataAction.udo` • `/Campaign/interact/manageIPB.udo` • `/Campaign/interact/flowchartRTAttrs.udo` • `/Campaign/initOfferListResolution.udo` • `/Campaign/getOfferListResolutionStatus.udo`
Unica Plan	• `/plan/errorPage.jsp` • `/plan/alertsService` • `/plan/services` • `/plan/services/collabService`

Produit ou fonction	Objets
	• `/plan/services/PlanIntegrationServices/1.0` • `/plan/affiniumplan.jsp` • `/plan/invalid_user.jsp` • `/plan/js/js_messages.jsp` • `/plan/js/format_symbols.jsp` • `/unica/servlet/AJAXProxy` • `/plan/api/plan/flowchartApproval/flowchartApproval/validate`
Unica Optimize	• `/Campaign/optimize/ext_runOptimizeSession.do` • `/Campaign/optimize/ext_optimizeSessionProgress.do` • `/Campaign/optimize/ext_doLogout.do`
IBM SPSS Modeler Advantage Enterprise Marketing Management Edition	`/unica/rest/spssUser`
Unica Platform filtres de données	`/unica/servlet/DataFiltering`
Unica notifications	• `unica/servlet/alertAJAXProxy` • `unica/notification/alertsCount`
Unica Planificateur	`/unica/servlet/SchedulerAPIServlet`

Activation des déconnexions uniques avec SiteMinder

Pour autoriser une déconnexion de SiteMinder lorsqu'un utilisateur se déconnecte d'une application Unica, configurez SiteMinder comme suit :

1. Connectez-vous à la zone **Administer Policy Server** (Administrer le serveur de règles) de SiteMinder et définissez la propriété `logoffUri` sur l'URI de la page de déconnexion d'Unica.

   Par exemple : `/sm_realm/unica/j_spring_security_logout` où *`sm_realm`* représente le domaine de sécurité SiteMinder et`unica`, la racine de contexte Unica Platform.
2. Déprotégez la page de déconnexion d'Unica, `/unica/jsp/frameworklogout.jsp`, afin que SiteMinder ne force par l'utilisateur à s'identifier de nouveau pour visualiser la page de déconnexion.

Activation des déconnexions personnalisées avec SiteMinder

Pour activer les déconnexions personnalisées avec SiteMinder, définissez `unica.sm.logouturl` sous `Affinium|suite|security|loginModes|siteMinderPartitionLogin` en suivant la procédure ci-dessous.

1. Obtenez l'ID de configuration de l'élément de configuration masqué unica.sm.logouturl de Platform à l'aide de la requête suivante.

   ```
   select ID from USM_CONFIGURATION where INTERNAL_NAME =
   'unica.sm.logouturl'
   ```
2. Mettez à jour la valeur de l'élément de configuration unica.sm.logouturl :

   ```
   update USM_CONFIGURATION_VALUES set STRING_VALUE='<custom logout url>'
   where CONFIGURATION_ID=<ID obtained from above query>
   ```

Conditions requises pour l'intégration à IBM Security Access Manager

Les conditions suivantes doivent être satisfaites pour pouvoir intégrer Unica à IBM Security Access Manager.

- La jonction WebSeal d'IBM Security Access Manager doit être configurée pour transmettre le nom d'utilisateur (abrégé, pas le nom distinctif (DN) complet) en tant que variable HTTP dans la demande d'URL adressée à l'application Unica.
- La propriété Unica `Web access control header variable` doit être définie sur le nom de la variable utilisée par Security Access Manager pour les noms de connexion.

  Le nom par défaut de la variable de nom de connexion Security Access Manager est `iv-user`.
- Le serveur de règles IBM Security Access Manager doit être configuré pour utiliser LDAP comme référentiel de stockage des membres de groupe et des attributs utilisateur.
- Les URL d'application Unica définies par une jonction WebSEAL et le serveur d'applications Java™ qui héberge l'application Unica doivent faire référence au même chemin.
- Tous les utilisateurs qui doivent avoir accès à Unica doivent appartenir à un groupe ajouté à une liste de contrôle d'accès avec les droits d'accès appropriés. Une jonction WebSEAL qui désigne un serveur d'applications où Unica Platform est déployé doit être jointe à cette liste de contrôle d'accès.
- Pour ignorer l'authentification de base lors de la configuration d'ISAM, vous devez définir `Ignore HTTP Basic Authentication header`. Accédez à **Gestion des jonctions -> <Editer la jonction> -> Onglet Identité** et sélectionnez **Ignorer** pour En-tête d'authentification de base HTTP.

Remarque : Lorsque les utilisateurs se déconnectent d'une application Unica, ils ne sont pas automatiquement déconnectés d'IBM Security Access Manager. Ils doivent fermer leur navigateur après s'être déconnectés d'une application Unica pour se déconnecter d'IBM Security Access Manager.

Configuration d'IBM Security Access Manager pour les produits Unica

Déprotégez les objets dans IBM Security Access Manager pour permettre le bon fonctionnement de vos produits Unica, comme indiqué dans cette procédure.

1. Utilisez Web Portal Manager pour vous connecter au domaine en tant qu'administrateur de domaine.
2. Cliquez sur **ACL > Create ACL**, remplissez les champs **Name** et **Description**, puis cliquez sur **Apply**.
3. Cliquez sur **ACL > List ACL**, et dans la page Manage ACLs, cliquez sur le lien de votre politique ACL.
4. Dans la page Propriétés de l'ACL, cliquez sur **Créer**, et créez deux entrées pour votre ACL, comme suit.
    - Pour la première entrée, définissez le type d'entrée sur **non authentifié** et accordez les autorisations **Trx - Traverse, lecture, suppression et exécution**.
    - Pour la deuxième entrée, définissez le type d'entrée sur **Tout autre** et accordez les autorisations **Trx - Traverse, lecture, suppression et exécution**.
5. Sur la page Propriétés de l'ACL, dans l'onglet Attacher, attachez des obejectifs non protégés, comme requis pour vos installations de produits.

   Utilisez le chemin d'accès complet dans IBM Security Access Manager, en commençant par WebSEAL.

Table 46. Objets non protégés requis pour les produits Unica

Produit ou fonction	Objets
Unica Campaign	• `/WebSEAL jonction/Campaign/optimize/ext_runOptimizeSession.do` • `/WebSEAL jonction/Campaign/optimize/ext_optimizeSessionProgress.do` • `/WebSEAL jonction/Campaign/optimize/ext_doLogout.do` • `/WebSEAL jonction/Campaign/interact/flowchartEventPatterns.udo` • `/WebSEAL jonction/Campaign/interact/saveFlowchartAction.udo` • `/WebSEAL jonction/Campaign/interact/testRunFlowchart.udo`

Produit ou fonction	Objets
	• /WebSEAL jonction/Campaign/interact/getProfileDataAction.udo • /WebSEAL jonction/Campaign/interact/manageIPB.udo • /WebSEAL jonction/Campaign/servlet/EngageUpload • /WebSEAL jonction/Campaign/api/campaign/rest/engageimportlist/partition • /WebSEAL jonction/Campaign/api/campaign/rest/engageimportlist/partition/schedule • /WebSEAL jonction/Campaign/api/campaign/rest/engageimportlist/partition/channel/schedule • /WebSEAL jonction/Campaign/interact/interactiveChannelSimulator.do • /WebSEAL jonction/Campaign/interact/interactiveChannelOfferMapping.do • /WebSEAL jonction/Campaign/services/CampaignServices30Service • /WebSEAL jonction/Campaign/FlowchartNotifyScheduler • /WebSEAL jonction/Campaign/OperationMonitor • /WebSEAL jonction/Campaign/initOfferListResolution.udo • /WebSEAL jonction/Campaign/getOfferListResolutionStatus.udo • /WebSEAL jonction/Campaign/moveCampaignsSubmit.do • /WebSEAL jonction/Campaign/interact/interactiveChannelStrategy.do

Produit ou fonction	Objets
	• `/WebSEAL jonction/Campaign/api/interact/rest` • `/WebSEAL jonction/Campaign/api/campaign/rest` • `/WebSEAL jonction/Campaign/interact/flowchartRTAttrs.udo` • `/WebSEAL jonction/Campaign/api/campaign/rest/ deepsearch/partition` • `/WebSEAL jonction/Campaign/api/interact/rest/v2` • `/WebSEAL jonction/Campaign/api/interact/rest/v2/channels?page=0&size=1000` • `/WebSEAL jonction/journey/api/campaign` • `WebSEAL jonction/Campaign/services/CampaignServices30Service` • `WebSEAL jonction/Campaign/api/campaign/rest` • `WebSEAL jonction/Campaign/FlowchartNotifyScheduler` • `WebSEAL jonction/Campaign/initOfferListResolution.udo` • `WebSEAL jonction/Campaign/getOfferListResolutionStatus.udo` • `WebSEAL jonction/Campaign/OperationMonitor` • `WebSEAL jonction/Campaign/api/campaign/rest` • `http://host:port/Campaign/api/campaign/rest/deepsearch/partition` Remplacez partition par le nom de la partition. Les éléments suivants s'appliquent lorsque l'intégration à Engage est mise en œuvre. Dans les URLs suivantes, remplacez partition par le nom de la partition.

Produit ou fonction	Objets
	• `http://host:port/Campaign/jsp/engage/engage-Home.jsp` • `http://host:port/Campaign/api/campaign/rest/engage/offers` • `http://host:port/Campaign/api/campaign/rest/engage/offer` • `http://host:port/Campaign/servlet/EngageU-pload` • `http://host:port/Campaign/api/campaign/rest/engageimportlist` • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition` • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/jobid` Cette URL est destinée à la vérification du statut d'un travail d'importation. Remplacez jobid par votre identifiant de travail. • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/schedule` • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/channel/schedule` Cette URL est destinée à l'envoi d'une commande push ou de messages SMS. Le canal est soit un `sms` soit un `push`.
Unica Collaborate	• *`WebSEAL jonction`*`/collaborate/affiniumcollab-orate.jsp` • *`WebSEAL jonction`*`/collaborate/services/Col-laborateIntegrationServices1.0` • *`WebSEAL jonction`*`/collaborate/flowchartRunNo-tifyServlet`

Produit ou fonction	Objets
	• *WebSEAL jonction*/collaborate/js/js_messages.jsp • *WebSEAL jonction*/collaborate/js/format_symbols.jsp • *WebSEAL jonction*/collaborate/alertsService
Unica Journey	• /WebSEAL/<nom de l'instance>/<nom de la jonction>/journey/api/platformlogin • /WebSEAL/<nom de l'instance>/<nom de la jonction>/journey/api/datadefinitions • /WebSEAL/<nom de l'instance>/<nom de la jonction>/journey/api/entrysources • /WebSEAL/<nom de l'instance>/<nom de la jonction>/journey/api/journeys • /WebSEAL/<nom de l'instance>/<nom de la jonction>/journey/api/folders • /WebSEAL/<nom de l'instance>/<nom de la jonction>/journey/api/permissions • /WebSEAL/<nom de l'instance>/<nom de la jonction>/unica/api/manager/authentication/login • /WebSEAL/<nom de l'instance>/<nom de la jonction>/unica/api/manager/user/user-details • /WebSEAL/<nom de l'instance>/<nom de la jonction>/unica/api/manager/configuration/get • /WebSEAL/<nom de l'instance>/<nom de la jonction>/unica/api/manager/policy/roles-permissions • /WebSEAL/<nom de l'instance>/<nom de la jonction>/unica/api/manager/license/7

Produit ou fonction	Objets
	• /WebSEAL/<nom de l'instance>/<nom de la jonction>/unica/api/manager/datasource • /WebSEAL/<nom de l'instance>/<nom de la jonction>/journey/api/thirdpartylogin
Unica Deliver	*WebSEAL jonction*/Campaign/deliver/eventSinkServlet
Unica Interact	• *WebSEAL jonction*/Campaign/interact/flowchartEventPatterns.udo • *WebSEAL jonction*/Campaign/interact/saveFlowchartAction.udo • *WebSEAL jonction*/Campaign/interact/testRunFlowchart.udo • *WebSEAL jonction*/Campaign/interact/getProfileDataAction.udo • *WebSEAL jonction*/Campaign/interact/manageIPB.udo • *WebSEAL jonction*/Campaign/initOfferListResolution.udo • *WebSEAL jonction*/Campaign/getOfferListResolutionStatus.udo • *WebSEAL jonction*/Campaign/interactiveChannelOfferMapping.do • *WebSEAL jonction*/Campaign/interactiveChannelStrategy.do • WebSEAL jonction/Campaign/interact/interactiveChannelOfferMapping.do • WebSEAL jonction/Campaign/FlowchartNotifyScheduler • WebSEAL jonction/Campaign/OperationMonitor

Produit ou fonction	Objets
	• `WebSEAL jonction/Campaign/initOfferListResolution.udo` • `WebSEAL jonction/Campaign/getOfferListResolutionStatus.udo` • `WebSEAL jonction/interact/servlet/InteractJSService` • `WebSEAL jonction/interact/servlet/RestServlet` • `WebSEAL jonction/interact/services/InteractService` • `WebSEAL jonction/Campaign/api/campaign/rest` • `WebSEAL jonction/Campaign/moveCampaignsSubmit.do` • `WebSEAL jonction/Campaign/interact/flowchartRTAttrs.udo` • `WebSEAL jonction/Campaign/interact/interactiveChannelStrategy.do` • `WebSEAL jonction/Campaign/api/interact/rest`
Unica Plan	• *`WebSEAL jonction`*`/plan/services` • *`WebSEAL jonction`*`/plan/errorPage.jsp` • *`WebSEAL jonction`*`/plan/alertsService` • *`WebSEAL jonction`*`/plan/services/collabService` • *`WebSEAL jonction`*`/plan/services/PlanIntegrationServices/1.0` • *`WebSEAL jonction`*`/plan/affiniumplan.jsp` • *`WebSEAL jonction`*`/plan/invalid_user.jsp` • *`WebSEAL jonction`*`/plan/js/js_messages.jsp` • *`WebSEAL jonction`*`/plan/js/format_symbols.jsp`

Produit ou fonction	Objets
	• *WebSEAL jonction*/unica/servlet/AJAXProxy • *WebSEAL jonction*//plan/api/plan/flowchartApproval/flowchartApproval/validate
Unica Optimize	• *WebSEAL jonction*/Campaign/optimize/ext_runOptimizeSession.do • *WebSEAL jonction*/Campaign/optimize/ext_optimizeSessionProgress.do • *WebSEAL jonction*/Campaign/optimize/ext_doLogout.do
IBM SPSS Modeler Advantage Enterprise Marketing Management Edition	*WebSEAL jonction*/unica/rest/spssUser
Unica Platform filtres de données	*WebSEAL jonction*/unica/servlet/DataFiltering.
Unica notifications	• *WebSEAL jonction*/unica/servlet/DataFiltering • *WebSEAL jonction*/unica/servlet/alertAJAXProxy • *WebSEAL jonction*/unica/notification/alertsCount
Unica Planificateur	*WebSEAL jonction*/unica/servlet/SchedulerAPIServlet
Activer une déconnexion d'IBM Security Access Manager lorsqu'un utilisateur	• *WebSEAL jonction*/unica/j_spring_security_logout • *WebSEAL jonction*/unica/jsp/frameworklogout.jsp

Produit ou fonction	Objets
se déconnecte d'une application Unica	
Unica Platform	*WebSEAL jonction*WebSEAL junction/unica/css/access_control.css

Organisation du processus de configuration : intégration d'Unica avec un système de contrôle d'accès Web

Cette feuille de route du processus de configuration permet d'analyser les tâches requises pour intégrer Unica avec un système de contrôle de l'accès Web. La colonne Rubrique contient des liens vers les rubriques qui décrivent les tâches en détail.

Tableau 47. Organisation du processus de configuration : intégration d'Unica avec un système de contrôle d'accès Web

Sujet	Informations
Exécution de l'intégration LDAP *(à la page 218)*	Suivez les instructions relatives à l'intégration de LDAP, en vous arrêtant à l'étape "Test de la synchronisation".
Définition des propriétés de connexion du contrôle d'accès Web dans Unica *(à la page 218)*	Définissez les propriétés d'intégration du contrôle de l'accès Web sur la page de configuration.
Redémarrage du serveur d'applications Web *(à la page 183)*	Cette étape est obligatoire pour s'assurer que tous les changements sont appliqués.

Tableau 47. Organisation du processus de configuration : intégration d'Unica avec un système de contrôle d'accès Web (suite)

Sujet	Informations
Test de la synchronisation du contrôle d'accès Web et de la connexion à Unica *(à la page 220)*	Vérifiez la bonne synchronisation des utilisateurs et des groupes à votre système de contrôle d'accès Web et la connexion à Unica.

Exécution de l'intégration LDAP

Exécutez toutes les étapes requises pour l'intégration LDAP.

Définition des propriétés de connexion du contrôle d'accès Web dans Unica

Pour configurer l'intégration du contrôle d'accès Web, vous devez définir certaines propriétés de configuration.

Dans la page **Paramètres et Configuration**, définissez les valeurs des propriétés comme décrit dans le tableau ci-après.

Voir la référence associée pour plus de détails sur la façon de définir chaque propriété.

Tableau 48. Propriétés permettant de configurer l'intégration du contrôle d'accès Web

Propriété	Valeur
Unica | Unica Platform | Securité | Détails du mode de connexion	Sélectionnez `Contrôle de l'accès Web.`
Unica | Unica Platform | Security | Login method details|	Les variables séparées par des virgules spécifiées sont recherchées dans l'en-tête HTTP, lors de la journalisation via le logiciel de contrôle d'accès Web. Si le journal d'audit est activé, ces va-

Propriété	Valeur
Web access control | Additional header variables	riables sont capturées et stockées dans l'événement Authentification sous les journaux Audit. Les variables HTTP capturées peuvent être consultées en cliquant sur "Plus" sous "Détails de l'événement". **Remarque :** Cette propriété est disponible à partir de la version 12.1.0.3.
Unica | Unica Platform | Securité | Détails du mode de connexion | Contrôle de l'accès Web | Modèle de nom d'utilisateur	Expression régulière Java™ utilisée pour extraire les informations de connexion de l'utilisateur de la variable d'en-tête HTTP dans le logiciel de contrôle de l'accès Web. Vous devez ajouter des caractères d'échappement à tous les caractères XML de l'expression régulière. La valeur recommandée pour SiteMinder et IBM Security Access Manager est `\w*`.
Unica | Unica Platform | Securité | Détails du mode de connexion | Contrôle de l'accès Web | Variable d'en-tête du contrôle d'accès Web	Variable d'en-tête HTTP configurée dans le logiciel de contrôle de l'accès Web, qui est soumise au serveur d'applications Web. Par défaut, SiteMinder utilise `sm_user` et IBM Security Access Manager utilise `iv-user`. Pour IBM Security Access Manager, définissez cette valeur sur le composant nom d'utilisateur de la chaîne brute IBM®, et non sur la chaîne HTTP IBM®.
Unica | Général | Navigation | Unica Platform URL	Définissez `http://`*`sm_host`*`:`*`sm_port`*`/`*`sm_realm`*`/unica` où • *`sm_host`* représente le nom de la machine sur laquelle SiteMinder est installé • *`sm_port`* `représente le numéro de port de SiteMinder` • *`sm_realm`* représente le domaine de SiteMinder

Redémarrage du serveur d'applications Web

Redémarrez le serveur d'applications Web pour vous assurer que toutes les modifications de configuration sont appliquées.

Test de la synchronisation du contrôle d'accès Web et de la connexion à Unica

Suivez cette procédure pour tester votre intégration.

1. Connectez-vous au système de contrôle de l'accès Web avec un compte LDAP qui a été synchronisé dans le système de contrôle de l'accès Web et qui a accès à Unica Platform.
2. Vérifiez que :
    - Les utilisateurs sont importés correctement
    - Les groupes sont importés correctement
    - Unica les appartenances aux groupes correspondent à la correspondance attendue avec les groupes LDAP
3. Faites pointer votre navigateur vers l'URL d'Unica Platform et connectez-vous.

   Vous devriez pouvoir accéder à Unica sans passer par l'écran de connexion d'Unica.
4. Suivez les instructions ci-après pour résoudre les problèmes rencontrés avec le logiciel de contrôle de l'accès Web Netegrity SiteMinder.
    - Si un écran de connexion d'Unica s'affiche, cela signifie que le compte utilisateur utilisé pour la connexion n'a peut-être pas été synchronisé dans SiteMinder.
    - Si vous n'arrivez pas à vous connecter à Unica, vérifiez que votre configuration de SiteMinder est correcte. Vous pouvez utiliser l'outil de test de SiteMinder pour vérifier que le compte utilisateur utilisé a été autorisé et qu'il a accès aux URL d'Unica dans SiteMinder.
    - Si vous pouvez accéder à Unica, mais que la navigation ne fonctionne pas correctement ou que les images ne s'affichent pas, vérifiez que le serveur Web hébergeant SiteMinder et le serveur d'applications Java™ hébergeant Unica Platform utilisent le même chemin pour se référer à Unica Platform.

Vérifier les en-têtes supplémentaires dans les journaux d'audit

Assurez-vous que les journaux d'audit sont activés. Sous la propriété "Contrôle d'accès Web | Variables d'en-tête supplémentaires", spécifiez les noms des variables d'en-tête HTTP à capturer. Après une connexion réussie, vérifiez les rapports d'événements d'audit et vérifiez les détails de l'événement pour les variables capturées.

Configuration de l'intégration avec une jonction WebSeal de type SSL

Suivez cette procédure pour configurer l'intégration de Unica Platform à IBM Security Access Manager à l'aide d'une jonction WebSeal de type SSL.

Pour plus d'informations sur ces procédures, consultez la documentation fournie avec IBM Security Access Manager et votre serveur d'applications Web.

1. Générez ou achetez des certificats SSL et configurez votre serveur d'applications Web pour pouvoir les utiliser.
2. Créez un certificat webSEAL et configurez IBM Security Access Manager pour l'utiliser.
3. Importez votre certificat webSEAL sur votre serveur d'applications Web.
4. Importez votre certificat de serveur d'applications Web dans IBM Security Access Manager.
5. Créez une jonction WebSeal de type SSL dans IBM Security Access Manager.

   Si vous installez plusieurs produits Unica, créez une jonction distincte pour chaque produit.
6. Définissez la propriété de configuration de l'URL de navigation sur la page **Paramètres et Configuration** pour chaque produit installé.

   La valeur doit refléter la jonction WebSeal utilisée pour ce produit. Suivez ce modèle :

   ```
   https://machine_name_or_IP_address.domain_name:port_number/webSEAL_junction/context-root
   ```

   Pour accéder à Unica, utilisez une URL telle que la suivante :

```
https://machine_name_or_IP_address.domain_name:port_number/
webSEAL_junction//unica
```

7. Déprotégez les URL dans IBM Security Access Manager, comme décrit dans ce guide.

Gestion des alertes et des notifications

Unica Platform prend en charge les alertes et notifications système envoyées par les produits Unica.

Les alertes système et les notifications aux utilisateurs envoyées par les produits apparaissent dans l'interface utilisateur comme décrit ci-après.

- Les **alertes** contiennent des informations sur les événements du système. Elles apparaissent dans une fenêtre instantanée quand un utilisateur se connecte.

  Par exemple, des alertes signalent les arrêts de serveur prévus ou imprévus.
- Les **notifications** contiennent des informations spécifiques aux utilisateurs, par exemple des informations relatives aux modifications des éléments qui les intéressent ou aux tâches qu'ils doivent effectuer. L'utilisateur peut voir ces notifications en cliquant sur l'icône d'enveloppe placée en haut à droite dans la fenêtre.

  Exemples : mises à jour apportées à un diagramme ou une liste de mailing ou rappels relatifs à l'échéance d'une tâche affectée.

Les utilisateurs peuvent également s'abonner pour recevoir des alertes et des notifications par e-mail si Unica Platform est configuré pour en envoyer.

Dans Unica Platform, le planificateur Unica utilise la fonction de notification.

Abonnement aux alertes et aux notifications

Les utilisateurs peuvent demander de recevoir les alertes et les notifications système par courrier électronique si Unica Platform est configuré pour en envoyer. Ils peuvent également choisir un niveau d'abonnement.

Par exemple, ils peuvent choisir de ne recevoir que les alertes système critiques, mais toutes les notifications. Le niveau d'abonnement diffère selon le produit qui envoie les alertes système et les notifications.

Remarque : Les alertes système sont toujours communiquées via des fenêtres instantanées lorsque l'utilisateur se connecte à Unica. Les utilisateurs ne peuvent pas modifier cette caractéristique.

Lorsque les utilisateurs se connectent à Unica, la fenêtre **Alertes système** s'affiche uniquement si des alertes nouvelles ou non lues sont présentes. Les utilisateurs peuvent marquer une alerte comme lue en la sélectionnant et en cliquant sur **Marquer comme lu** dans la fenêtre **Alertes système**.

Définition des abonnements aux notifications et aux alertes système

Les utilisateurs non administratifs peuvent définir leurs propres abonnements aux alertes et aux notifications système en procédant comme suit.

1. Connectez-vous à Unica, puis sélectionnez `Paramètres > Utilisateurs`.

   La page des détails de votre compte s'ouvre.
2. Cliquez sur **Abonnement aux notifications** dans la page des détails du compte.
3. Utilisez les cases à cocher pour choisir le niveau des notifications que vous souhaitez recevoir et indiquer si vous voulez les afficher dans l'interface utilisateur, les recevoir par courrier électronique, les deux, ou pas du tout.
4. Cliquez sur **Soumettre** pour enregistrer vos modifications.

Configuration des notifications par e-mail dans Unica

Pour configurer Unica Platform de façon à envoyer des alertes système et des notifications par e-mail aux utilisateurs, procédez comme suit. Un serveur de messagerie doit être configuré préalablement.

Collectez les informations suivantes sur votre serveur de messagerie :

- Protocole utilisé par le serveur de messagerie
- Port d'écoute du serveur de messagerie
- Nom de l'ordinateur qui héberge le serveur de messagerie
- Si le serveur de messagerie demande l'authentification
- Si le serveur de messagerie demande l'authentification, nom de compte et mot de passe utilisés pour accéder au serveur de messagerie

Conseil : Voir les références connexes si vous avez besoin de plus d'informations sur l'exécution de cette procédure.

1. Si votre serveur de messagerie demande l'authentification, enregistrez un nom de compte de serveur de messagerie et un mot de passe comme source de données dans un compte utilisateur Unica Platform.

   Utilisez un compte utilisateur Unica Platform interne, pas un compte utilisateur importé depuis un serveur LDAP.

   Notez par écrit le nom d'utilisateur Unica Platform et le nom de la source de données car vous en aurez besoin à l'étape 3.
2. Connectez vous à Unica en tant qu'utilisateur avec des droits d'administrateur sur Unica Platform.
3. Dans la page **Paramètres > Configuration**, définissez les propriétés de configuration dans les catégories suivantes :
   - `Général | Communication | E-mail`
   - `Platform | Notifications`

   Servez-vous des informations de votre serveur de messagerie pour déterminer les valeurs requises.

Implémentation du protocole SSL unidirectionnel

Cette section décrit le protocole SSL unidirectionnel dans Unica.

Le protocole Secure Sockets Layer (SSL) permet de sécuriser toute communication entre deux applications qui se connectent sur un réseau.

Le protocole SSL garantit des connexions sécurisées :

- En autorisant une application à authentifier l'identité d'une autre application
- En utilisant une clé privée pour chiffrer et déchiffrer les données transférées sur la connexion SSL

Lorsque des applications sont configurées pour SSL, le trafic Web se fait sur HTTPS plutôt que sur HTTP, comme le montrent les URL.

Lorsque les processus communiquent entre eux, le processus qui effectue une requête fait office de client et le processus qui répond à la requête fait office de serveur. Pour une sécurité complète, le protocole SSL doit être implémenté pour toutes les formes de communication avec les produits d'Unica.

Le protocole SSL peut être unidirectionnel ou bidirectionnel. Dans un protocole SSL unidirectionnel, le serveur doit présenter un certificat au client, mais le client n'a pas l'obligation de présenter un certificat au serveur. Pour négocier la connexion SSL avec succès, le client doit authentifier le serveur. Le serveur accepte une connexion à partir d'un client.

Présentation des certificats SSL

Lisez cette section pour comprendre les certificats SSL en général.

Qu'est-ce qu'un certificat ?

Un certificat est une signature numérique identifiant le serveur en tant qu'identité portant un nom. Les certificats peuvent être signés par une autorité de certification qui se porte garante de l'identité du serveur. Sinon, ils peuvent être autosignés. Comme autorités de certification, citons Verisign et Thawte. Un certificat autosigné est un certificat dans lequel l'autorité de certification est la même entité que celle que le certificat cherche à identifier.

Certificats côté serveur

Chaque serveur destiné à fournir une communication SSL, qu'il s'agisse d'un serveur d'applications ou d'une application Unica, telle que le programme d'écoute de Unica Campaign, doit être régi par un certificat.

Fichiers de clés certifiées côté client

Lorsque le client reçoit le certificat du serveur, il doit déterminer s'il s'agit d'un certificat de confiance. Un client fait confiance automatiquement au certificat d'un serveur si ce certificat existe dans le fichier de clés certifiées du client. Un fichier de clés certifiées est une base de données de certificats dignes de confiance.

Les navigateurs modernes disposent d'un fichier de clés certifiées qui contient les certificats communs validés par des autorités de certification. Voilà pourquoi aucune invite ne s'affiche lorsque vous entrez dans le site sécurisé des principaux sites Web marchands. Ils utilisent les certificats signés par une autorité de certification. Toutefois, lors d'une connexion à une application HCL qui utilise un certificat autosigné, cette invite apparaît.

Les navigateurs vérifient si le nom d'hôte du serveur correspond au nom de l'objet dans le certificat (généralement le nom commun utilisé comme nom unique, que vous fournissez lorsque vous demandez un certificat). Il se peut que le navigateur émette un avertissement si ces deux noms ne correspondent pas.

Lorsqu'un navigateur accède à une application HCL sécurisée avec un certificat non reconnu (par exemple, un certificat autosigné), une boîte de dialogue s'ouvre pour demander à l'utilisateur s'il souhaite continuer. Si l'utilisateur choisit d'installer le certificat dans le fichier de clés certifiées local, l'invite n'apparaît plus.

Rôles client et serveur dans Unica

Les composants d'application Unica peuvent faire office de client ou de serveur dans une communication, selon la situation.

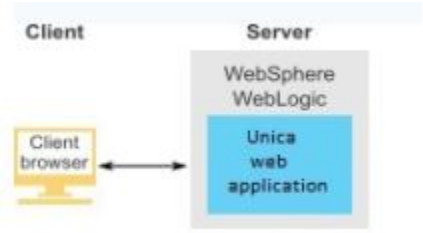
La plupart des applications d'Unica se composent de deux parties.

- Application Web. L'application Web est le composant auquel les utilisateurs accèdent via un navigateur.
- Serveur (par exemple, le programme d'écoute de Unica Campaign et le serveur d'applications de Unica Platform). Ce composant est accessible par programme.

Les exemples et schémas suivants illustrent les rôles joués par les composants d'HCL au sein de différents types de communication.

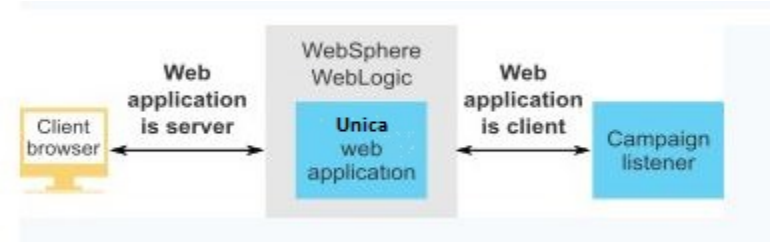
Exemple 1 : communication entre un navigateur et une application Web d'Unica

Lorsque des utilisateurs communiquent avec des applications Web d'Unica par le biais d'un navigateur, ce dernier est le client et l'application Web Unica est le serveur.



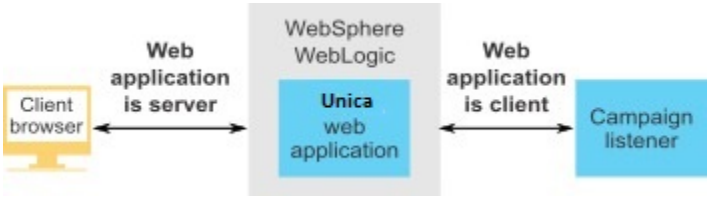
Exemple 2 : communication entre composants d'une application d'Unica

Les deux composants d'une application d'Unica peuvent également communiquer entre eux à l'aide d'un programme. Par exemple, lorsque l'application Web de Unica Campaign envoie une requête au programme d'écoute de Unica Campaign, l'application Web de Unica Campaign est le client et le module d'écoute est le serveur.



Exemple 3 - composants Unica jouant les deux rôles

Un composant d'application d'Unica peut communiquer en tant que client dans le cadre de certains échanges, et en tant que serveur dans d'autres. Un exemple de ces relations est illustré dans le diagramme ci-dessous.



SSL dans Unica

De nombreux composants d'application d' peuvent faire office de serveur et de client dans le cadre des opérations normales, et certains composants d' sont écrits en Java™, et d'autres en C++. Cela détermine le format des certificats que vous utilisez. Vous spécifiez le format lorsque vous créez un certificat autosigné ou que vous en achetez un auprès de l'autorité de certification.

Les applications n'ont pas besoin de fichiers de clés certifiées lorsqu'ils font office de client faisant des requêtes SSL unidirectionnelles vers un composant serveur .

Composant Java™ qui fait office de serveur

Pour les applications d' écrites en Java™ à l'aide de la mise en œuvre SSL JSSE et déployées sur un serveur d'applications, vous devez configurer le serveur d'applications pour utiliser votre certificat. Le certificat doit être enregistré au format JKS.

Vous ne pouvez pas utiliser le certificat par défaut fourni avec le serveur d'application.

Vous pouvez créer des certificats JKS pour vos applications Java à l'aide de l'outil de clé Java.

Composant C++ qui fait office de serveur

Le programme d'écoute de Campaign et le composant serveur d'Optimize sont écrits en C++ et requièrent un certificat généré par OpenSSL.

Composant Java™ faisant office de client

Pour les applications écrites en Java™ et déployées sur un serveur d'applications, aucun fichier de clés certifiées n'est nécessaire. Afin de simplifier la configuration, les applications

Java™ faisant office de client n'authentifient pas le serveur pendant des communications SSL unidirectionnelles. Toutefois, le chiffrement est effectué.

Composants C/C++ faisant office de client

Pour les applications écrites en C/C++ à l'aide de la mise en œuvre OpenSSL, aucun fichier de clés certifiées n'est nécessaire. Le programme d'écoute de Campaign fait partie de cette catégorie.

Combien de certificats ?

Dans l'idéal, vous devriez utiliser un certificat différent pour chaque machine qui héberge un composant faisant office de serveur.

Si vous ne souhaitez pas utiliser plusieurs certificats, vous pouvez utiliser le même certificat pour tous les composants d' qui font office de serveurs. Si vous utilisez un seul certificat pour toutes les applications et si les utilisateurs accèdent aux applications d' pour la première fois, le navigateur leur demande s'ils souhaitent accepter le certificat.

Organisation du processus de configuration : Mise en œuvre de SSL dans Unica

Cette feuille de route du processus de configuration permet d'analyser les tâches requises pour implémenter SSL dans Unica avec LDAP. La colonne Rubrique contient des liens vers les rubriques qui décrivent les tâches en détail.

Tableau 49. Organisation du processus de configuration : Mise en œuvre de SSL dans Unica

Sujet	Informations
Obtenez des certificats *(à la page)*	Obtenez ou créez des certificats si vous ne souhaitez pas utiliser les certificats par défaut fournis par HCL et votre serveur d'applications.
Configuration des serveurs d'applications Web pour le	Activez un port SSL sur chaque serveur d'applications sur lequel une application HCL est déployée. Si vous n'utilisez pas le certi-

Tableau 49. Organisation du processus de configuration : Mise en œuvre de SSL dans Unica (suite)

Sujet	Informations
protocole SSL *(à la page 240)*	ficat par défaut du serveur d'applications, configurez le serveur pour qu'il utilise votre certificat.
Configurer HCL U-nica pour SSL *(à la page 241)*	Paramétrez les propriétés de configuration dans Unica.
Vérification de la configuration SSL *(à la page 256)*	Connectez-vous à chacune de vos applications Unica.

Certificats de SSL

Cette procédure décrit comment créer et configurer vos propres certificats. Exécutez la même procédure pour chaque Unica configuré pour utiliser SSL. Si vous configurez l'intégration Unica Campaign + Engage, voir Unica Campaign and Engage Integration Guide for IBM Marketing Cloud.

Il existe plusieurs moyens d'obtenir ou de créer des certificats. Vous pouvez créer des certificats autosignés ou obtenir des certificats d'une autorité de certification.

Les certificats d'auto-signature

Vous pouvez créer des certificats autosignés.

Pour les composants C++ agissant en tant que serveur, utilisez openSSL pour créer un certificat `.pem`. Le programme d'écoute de Campaign implémente le protocole SSL à l'aide de la bibliothèque HCL OpenSSL. La bibliothèque openSSL est installée avec Campaign et inclut un programme de ligne de commande nommé `openSSL`, qui peut créer un fichier de certificat.

Pour les composants Java agissant en tant que serveur, utilisez l'outil de clé Java pour créer un certificat JKS.

Certificats d'une autorité de certification

Vous pouvez obtenir des certificats auprès d'une autorité de certification.

Vous pouvez utiliser openSSL pour créer des requêtes à envoyer à une autorité de certification afin de créer des certificats signés. Vous pouvez également obtenir des certificats directement auprès de l'autorité de certification.

Consultez la documentation de votre autorité de certification pour en savoir plus sur l'obtention d'un certificat signé.

Obtenez ou créez des certificats.

Pour créer et utiliser un certificat autosigné et l'utiliser avec HCL Unica, procédez comme suit :

1. Créez un certificat pour les composants HCL Unica de l'application C++.
2. Créez un certificat pour les composants Java Unica de l'application C++.

Créez un certificat pour les composants HCL Unica de l'application C++.

Le programme d'écoute Campaign implémente le protocole SSL à l'aide de la bibliothèque OpenSSL. La distribution OpenSSL inclut un programme de ligne de commande nommé `openssl` qui peut créer un fichier de certificat. Pour plus d'informations sur l'utilisation de ce programme, consultez la documentation OpenSSL. Vous pouvez aussi accéder à l'aide en ligne en saisissant `-help` lors de l'exécution du programme.

Effectuez les étapes suivantes pour créer un certificat auto-signé et configurer un composant Unica HCL C ++ pour SSL.

1. Exécutez `openssl` depuis la ligne de commande. Le programme et le fichier de configuration associé `openssl.cnf` sont inclus dans le répertoire bin de l'installation de Campaign. Ces éléments sont également disponibles avec la distribution OpenSSL.
2. Générez une clé. L'exemple de commande suivant crée une clé nommée `key.pem`.

   ```
   set OPENSSL_CONF=CAMPAIGN_HOME\bin\openssl.cnf

   openssl genrsa -out key.pem 4096
   ```

3. Générez une demande. L'exemple de commande suivant crée une clé nommée `request.pem`.

   ```
   openssl req -config openssl.cnf -new -key key.pem -out request.pem
   ```

   L'outil affiche une série de questions. Si vous saisissez un point (.), la zone reste en blanc. Pour un certificat autosigné, vous devez au moins saisir le nom courant.

   Si vous utilisez l'outil openssl à partir du répertoire `Campaign/bin`, ajoutez le paramètre `-config` avec une valeur qui pointe vers le fichier `openssl.cnf` dans le même répertoire. Par exemple : `openssl req -config openssl.cnf -x509 -key key.pem -in request.pem -days 1000 -out certificate.pem`
4. Générez un certificat. L'exemple de commande suivant crée un certificat nommé `certificate.pem` qui expire dans 10 000 jours à compter de sa date de création, avec les fichiers `request.pem` et `key.pem`.

   ```
   openssl req -x509 -key key.pem -in request.pem -days 10000 -out certificate.pem
   ```

   Si vous utilisez l'outil openssl à partir du répertoire `Campaign/bin`, ajoutez le paramètre `-config` avec une valeur qui pointe vers le fichier `openssl.cnf` dans le même répertoire. Par exemple :

   ```
   openssl req -config openssl.cnf -x509 -key key.pem -in request.pem -days 10000 -out certificate.pem
   ```
5. Créez un exemple de fichier de certificat campaign.pem
6. Copiez le contenu des fichiers key.pem et certificate.pem dans ce nouveau fichier, en le séparant par une nouvelle ligne.

Créez un certificat pour les composants Java HCL Unica

Les composants d'application Web HCL Unica écrits en Java utilisent la bibliothèque JSSE. Le JDK de Sun inclut un programme intitulé `keytool` qui peut créer un fichier de certificat. Pour plus d'informations sur l'utilisation de ce programme, consultez la documentation Java. Vous pouvez aussi accéder à l'aide en ligne en saisissant `-help` lors de l'exécution du programme.

Effectuez les étapes suivantes pour créer un certificat auto-signé et configurer un composant Unica HCL Java pour SSL.

1. Exécutez `keytool` depuis la ligne de commande. Ce programme se trouve dans le répertoire bin du kit JDK Java Sun.
2. Générez un fichier de clés d'identité. L'exemple de commande suivant crée un fichier de magasin de clés nommé `UnicaClientIdentity.jks`.

   ```
   keytool -genkey -alias UnicaClientIdentity -keyalg RSA -keystore UnicaClientIdentity.jks -keypass clientPwd -validity 1000 -dname "CN=hostName, O=myCompany" -storepass clientPwd
   ```

   Prenez connaissance des informations suivantes :
   - Notez la valeur `-storepass` (clientPwd dans l'exemple), car vous en aurez besoin lors de la configuration du serveur d'applications.
   - Notez la valeur `-alias` (UnicaClientIdentity dans l'exemple), car vous en aurez besoin pour la suite de la procédure.
   - Le nom courant du nom unique doit correspondre au nom d'hôte utilisé pour accéder à HCL Unica. Par exemple, si l'URL d'HCL Unica est https://hostName.companyDomain.com:7002/unica/jsp, le nom courant doit être hostName.companyDomain.com. La partie "nom courant" du nom unique est la seule qui soit obligatoire. Les parties "Organisation" (O) et "Unité organisationnelle" (OU) sont facultatives.
   - Pour WebSphere 6.0, le mot de passe du fichier de clés et celui de la clé doivent être identiques.
3. Générez un certificat à partir du fichier de clés d'identité que vous avez créé. The following sample command creates a keystore named `UnicaCertificate.cer`. La valeur `-alias` correspond à l'alias défini pour le fichier de clés d'identité (UnicaClientIdentity dans l'exemple).

   ```
   keytool -export -keystore UnicaClientIdentity.jks -storepass clientPwd-alias UnicaClientIdentity -file UnicaCertificate.cer
   ```
4. Générez un fichier de clés certifiées à partir du certificat que vous avez créé. L'exemple de commande suivant crée un fichier de clés approuvé nommé `UnicaTrust.jks`.

```
keytool -import -alias UnicaClientIdentity -file UnicaCertificate.cer-
keystore UnicaTrust.jks -storepass trustPwd
```

Prenez connaissance des informations suivantes :

- Appuyez sur la touche `Y` lorsque vous êtes invité à approuver le certificat.
- La valeur `-alias` correspond à l'alias défini pour le fichier de clés d'identité (`UnicaClientIdentity` dans l'exemple).
- Notez la valeur `-storepass` (`trustPwd` dans l'exemple), car vous en aurez besoin lors de la configuration du serveur d'applications.

Importer un certificat Open SSL dans le fichier de clés Java

```
keytool -import -alias ListenerKey -file CAMPAIGN_HOME\bin\certificate.pem
-keystore PlatformClientIdentity.jks -storepass password
```

```
keytool -import -file CAMPAIGN_HOME\bin\certificate.pem -alias ListenerKey
-keystore <APP_SERVER_JAVA>\jre\lib\security\cacerts
```

Comment obtenir des certificats signés

Vous pouvez utiliser les programmes OpenSSL et keytool pour créer des requêtes à envoyer à une autorité de certification afin de créer des certificats signés. Vous pouvez également obtenir des certificats directement auprès de l'autorité de certification.

Remarque :

- Pour les applications HCL Unica écrites en C++, procurez-vous un certificat au format PEM.
- Pour toutes les autres applications HCL Unica, procurez-vous un certificat au format JKS.

Consultez la documentation de votre autorité de certification pour en savoir plus sur l'obtention d'un certificat signé.

Création et configuration de certificats pour un environnement de cluster

Cette procédure décrit comment créer et configurer vos propres certificats pour un environnement de cluster.

L'application Web Campaign doit être configurée pour SSL via les certificats par défaut.

La procédure suivante décrit comment créer et configurer des certificats autosignés pour Unica Campaign et Unica Platform.

Dans un environnement de cluster où un serveur IBM HTTP Server précède l'application Web Unica Campaign et le programme d'écoute de Campaign, procédez comme suit pour configurer celui-ci dans SSL.

Vous pouvez utiliser ces étapes comme guide pour la configuration de certificats pour d'autres produits Unica.

Cette procédure s'applique aux certificats par défaut fournis par IBM WebSphere Application Server. Si vous utilisez des certificats de sécurité personnalisés, vous devez suivre la procédure correspondant aux certificats personnalisés utilisés par IBM WebSphere Application Server.

Pour configurer IBM HTTP Server dans SSL, procédez comme suit.

1. Utilisez GSKit pour générer des certificats SSL comme suit.

    a. Créez et initialisez une nouvelle base de données de clés.

    Par exemple :

    ```
    gsk8capicmd_64 -keydb -create -populate -db IHS.kdb -pw password
    -stash
    ```

    L'option `-stash` est obligatoire pour Unica Campaign.

    b. Utilisez GSKit pour générer un certificat autosigné pour Unica Campaign et le stocker dans la base de données de clés, comme suit.

    Par exemple :

```
gsk8capicmd_64 -cert -create -db IHS.kdb -dn "CN=*.in.ibm.com"
-expire 3650 -pw password -size 1024 -label key -default_cert yes
```

c. Extrayez la partie publique du certificat dans un fichier.

Pour que les clients fassent confiance à un certificat, la partie publique de ce dernier doit être distribuée aux clients et stockée dans leurs bases de données de clés. Dans cette étape, vous exportez la partie publique du certificat Unica Campaign. Vous l'importez lors d'une étape ultérieure.

Par exemple :

```
gsk8capicmd_64 -cert -extract -db IHS.kdb -stashed -label key
-target IHS.arm
```

d. Activez le module suivant dans le fichier `httpd.conf`.

Par exemple :

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so

Listen 443
<VirtualHost *:443>
SSLEnable
</VirtualHost>
KeyFile /data/webservers/IBM/IHS/ssl/IHS.kdb
SSLStashFile /data/webservers/IBM/IHS/ssl/IHS.sth
SSLDisable
```

e. Indiquez le chemin d'accès au fichier de clés dans le fichier `httpd.conf`.

f. Redémarrez le serveur IBM HTTP.

2. Générez les fichiers base de données de magasin de clés correspondant au serveur qui héberge le programme d'écoute d'Unica Campaign.

a. Sur le serveur qui héberge le programme d'écoute d'Unica Campaign, exécutez les commandes suivantes à partir de n'importe quel emplacement et prenez note du chemin.

```
gsk8capicmd_64 -keydb -create -populate -db Key.kdb -pw password
 -stash
gsk8capicmd_64 -cert -create -db Key.kdb -dn "CN=*.in.ibm.com"
 -expire 3650 -pw password -size 1024
  -label key -default_cert yes
gsk8capicmd_64 -cert -extract -db Key.kdb -stashed -label key
 -target Key.arm
```

b. Vérifiez que les fichiers suivants sont générés à l'emplacement à partir duquel vous avez exécuté les commandes ci-dessus.
   - `Key.arm`
   - `Key.crl`
   - `Key.kdb`
   - `Key.rdb`
   - `Key.sth`

3. Importez les fichiers `Key.arm` et `HIS.arm` sur le serveur d'applications où l'application Web de Campaign est déployée.

   a. Copiez les fichiers `Key.arm` et `HIS.arm` sur le serveur d'applications Web de Campaign.

   b. Ajoutez les fichiers `Key.arm` et `HIS.arm` à la clé **NodeDefaultTrustStore** de WebSphere Application Server de la manière suivante :
      i. Cliquez sur **Sécurité > Certificat SSL et gestion des clés > Magasins de clés et certificats**.
      ii. Cliquez sur **NodeDefaultTrustStore > Certificats de signataire**.
      iii. Cliquez sur **Ajouter** et spécifiez l'**alias** et le chemin d'accès dans lequel les fichiers `Key.arm` et `HIS.arm` sont copiés.
      iv. Cliquez sur **OK**.

4. Extrayez le certificat personnel et le certificat de signataire d'IBM WebSphere Application Server.
    a. Cliquez sur **Sécurité > Certificat SSL et gestion des clés > Magasins de clés et certificats**.
    b. Cliquez sur **NodeDefaultTrustStore > Certificats personnels**.
    c. Sélectionnez le certificat par défaut.
    d. Ajoutez le nom du fichier de certificat personnel avec le chemin valide dans le serveur d'applications Web d'Unica Campaign. Par exemple, `/opt/HCL/HCLUnica101/ClientPersonal.cer`.
    e. Cliquez sur **OK**.
    f. Cliquez sur **NodeDefaultTrustStore > Certificats de signataire**.
    g. Sélectionnez le certificat par défaut.
    h. Ajoutez le nom du fichier de certificat de signataire avec le chemin valide dans le serveur d'applications Web d'Unica Campaign. Par exemple, `/opt/HCL/HCLUnica101/ClientSigner.cer`.
    i. Naviguez jusqu'au dossier et vérifiez que les deux certificats y sont présents.
5. Importez le certificat personnel et le certificat de signataire dans les bases de données de fichiers de clés du programme d'écoute d'Unica Campaign et d'HCL HTTP Server.

    a. Copiez les certificats `ClientPersonal.cer` et `ClientSigner.cer` sur le serveur du programme d'écoute. Vous pouvez utiliser l'emplacement où le fichier `key.kdb` a été créé.

    b. Importez le certificat personnel et le certificat de signataire dans la base de données de fichiers de clés du programme d'écoute à l'aide de la commande gsk8capicmd_64 à partir de l'emplacement de création de la base de données de fichiers de clés du programme d'écoute (`key.kdb`).

```
gsk8capicmd_64 -cert -add -db Key.kdb -stashed -label
 ClientPersonalKey -file ClientPersonal.cer
gsk8capicmd_64 -cert -add -db Key.kdb -stashed -label
 ClientSignerlKey -file ClientSigner.cer
```

c. Copiez les certificats `ClientPersonal.cer` et `ClientSigner.cer` sur HCL HTTP Server. Vous pouvez utiliser l'emplacement où le fichier `IHS.kdb` a été créé.

d. Importez le certificat personnel et le certificat de signataire dans la base de données de fichiers de clés du programme d'écoute à l'aide de la commande gsk8capicmd_64 à partir de l'emplacement de création de la base de données de fichiers de clés d'HCL HTTP Server (`IHS.kdb`).

6. Importez la clé du programme d'écoute de Campaign dans la base de données de fichiers de clés d'HCL HTTP Server et importez la clé HCL HTTP Server dans la base de données de fichiers de clés Campaign.

a. Copiez la clé HCL HTTP Server (`IHS.arm`) dans le serveur du programme d'écoute.

b. Importez la clé HCL HTTP Server dans la base de données de fichiers de clés du programme d'écoute à l'aide de la commande gsk8capicmd_64 à partir de l'emplacement de création de la base de données de fichiers de clés du programme d'écoute de Campaign (`key.kdb`).

```
gsk8capicmd_64 -cert -add -db Key.kdb -stashed -label IHSKey
 -file IHS.arm
```

c. Copiez la clé du programme d'écoute Campaign (`Key.arm`) dans le serveur de programme d'écoute.

d. Importez la clé du programme d'écoute de Campaign dans la base de données de fichiers de clés d'HCL HTTP Server à l'aide de la commande gsk8capicmd_64 à partir de l'emplacement de création de cette base de données (`IHS.kdb`).

```
gsk8capicmd_64 -cert -add -db IHS.kdb -stashed -label IHSKey
 -file Key.arm
```

7. Redémarrez le serveur d'applications d'HCL Campaign, HCL HTTP Server, puis le programme d'écoute d'Unica Campaign.

Configuration des serveurs d'applications Web pour le protocole SSL

Pour tous les serveurs d'applications sur lesquels une application Unica est déployée, vous devez configurer le serveur d'applications Web pour qu'il utilise les certificats que vous avez décidé d'employer.

Pour plus d'informations sur l'exécution de ces procédures, consultez la documentation du serveur d'applications Web.

Mise en œuvre de la sécurité des cookies

Certains cookies peuvent ne pas être sécurisés correctement dans le navigateur client. Ne pas sécuriser les cookies rend l'application vulnérable à l'interposition (man in the middle) et aux attaques de piratage de session. Pour résoudre ce problème, prenez les précautions suivantes.

- Appliquez l'utilisation de SSL en permanence afin de réduire le risque d'interception des cookies sur la connexion.
- Dans le serveur d'applications Web, définissez les indicateurs `secure` et `httponly` sur tous les cookies.
    - L'indicateur `secure` indique au navigateur d'envoyer le cookie uniquement une connexion HTTPS. Vous devez activer SSL sur toutes les applications qui communiquent entre elles si vous définissez cet indicateur.
    - L'indicateur `httponly` empêche l'accès des cookies via un script côté client.

Configuration des indicateurs SSL dans WebSphere®

Pour configurer les indicateurs `secure` et `httponly` dans WebSphere®, utilisez la procédure suivante.

Vous définissez les indicateurs `secure` et `httponly` dans la console administrative WebSphere®.

Conseil : Pour plus d'informations, voir la documentation WebSphere®.

1. Au niveau application de Unica Platform, accédez à **Session Management** (Gestion de session) et cliquez sur **Enable cookies** (Activer les cookies).
2. Sélectionnez **Restrict cookies to HTTPS sessions** (Limiter les cookies aux sessions HTTP) et **Set session cookies to HTTPOnly to help prevent cross-site scripting attacks** (Associer les cookies de session à la valeur HTTPOnly pour éviter les attaques de script CCS).
3. Sauvegardez et appliquez vos modifications.
4. Arrêtez et redémarrez l'application Unica Platform.

Configuration des indicateurs SSL dans WebLogic

Pour configurer les indicateurs `secure` et `httponly`, utilisez la procédure suivante.

Conseil : Voir la documentation de WebLogic pour des détails complets.

1. Si Unica Platform est déployé et est en cours d'exécution, arrêtez-le et annulez le déploiement.
2. Extrayez le fichier WAR Unica Platform.
3. Editez le fichier `weblogic.xml` pour définir les indicateurs `secure` et `httponly`.
4. Recréez le fichier WAR Unica Platform, redéployez et redémarrez.

Configurer HCL Unica pour SSL

Pour configurer les applications Unica afin qu'elles utilisent le protocole SSL, vous devez définir certaines propriétés de configuration. Suivez les procédures décrites dans cette section relatives à l'installation des produits Unica et aux communications que vous souhaitez sécuriser au moyen du protocole SSL.

Si vous accédez à l'installation d'Unica via une connexion sécurisée, et si vous définissez des propriétés de navigation telles que décrites dans les procédures suivantes, vous devrez utiliser `https` et le numéro de port sécurisé dans l'URL. Le port SSL par défaut est `7002` pour WebLogic et `8002` pour WebSphere®.

Configuration de SSL dans Unica Platform

Cette procédure permet de configurer SSL dans Unica Platform.

1. Connectez-vous à Unica, puis cliquez sur **Paramètres > Configuration**.
2. Attribuez la valeur de l'URL Unica Platform à la propriété `Général | Navigation | URL Unica Platform`.

   Par exemple : `https://`*`host.domain:SSL_port`*`/unica`

   où :

   - *`host`* est le nom ou l'adresse IP de la machine sur laquelle Unica Platform est installé.
   - *`domain`* désigne le domaine de la société dans lequel les produits Unica sont installés.
   - *`SSL_Port`* désigne le port SSL dans le serveur d'applications sur lequel Unica Platform est déployé.

   Notez que l'URL commence par `https`.
3. Dans la catégorie `Navigation`, recherchez les propriétés de chaque produit d'Unica installé pour lequel vous avez défini les ports HTTP et HTTPS. Le nom des propriétés peut varier selon le produit, mais leur fonction doit être évidente. Pour chaque produit, paramétrez ces valeurs sur les ports HTTP et HTTPS du serveur d'applications sur lequel le produit est déployé.
4. Si vous avez implémenté l'intégration LDAP, effectuez la procédure décrite dans "Configuration de SSL dansUnica Platform avec intégration LDAP."
5. Si vous envisagez d'utiliser la fonction de filtrage des données, suivez la procédure décrite dans "Configuration de SSL dans Unica Platform avec filtres de données."

Configuration de SSL dans Platform pour un environnement de cluster

Pour configurer SSL dans Platform dans un environnement de cluster, procédez comme suit.

1. Connectez-vous à HCL Unica, puis cliquez sur **Paramètres** > **Configuration**.
2. Sous `Affinium | Manager | Navigation`, définissez l'URL d'Unica Platform dans URL d'**Unica Platform**.

   Par exemple : `https://<IHS_Host>/unica`.
3. Sous `Affinium | Campaign | Navigation`, définissez l'URL d'Unica Campaign dans **serverURL**.

   Par exemple : `https://<IHS_Host>/Campaign`.
4. Sous `Affinium | Campaign | server`, définissez l'URL d'Unica Campaign dans **fullContextPath**.

   Par exemple : `https://<IHS_Host>/Campaign`.
5. Sous `Affinium | Campaign | unicaACListener`, définissez **serverhost** sur l'`<hôte IHS>` et définissez **useSSL** sur `True`.

Configuration de SSL dans Unica Platform avec intégration LDAP

Cette procédure permet de configurer SSL dans Unica Platform.

1. Suivez la procédure décrite dans "Configuration de SSL dans Unica Platform" si vous ne l'avez pas encore fait.
2. Connectez-vous à Unica, puis cliquez sur **Paramètres > Configuration**.

   La page Configuration s'affiche.
3. Accédez à la catégorie `Unica | Unica Platform | Sécurité | Détails du mode de connexion | LDAP` et définissez la valeur de la propriété `SSL requis pour la connexion LDAP` sur `true`.

   Cette valeur requiert la connexion de Unica Platform au serveur LDAP à l'aide de SSL lorsque les utilisateurs se connectent.
4. Accédez à la catégorie `Unica | Unica Platform | Sécurité | Synchronisation LDAP` et définissez les valeurs suivantes.
   - Affectez à la propriété `URL du fournisseur LDAP` la valeur : `ldaps://`*`host`*`.`*`domain`*`:`*`SSL_Port`*

     où :

- *host* correspond au nom ou à l'adresse IP du serveur LDAP.
- *domain* est le domaine du serveur LDAP.
- *SSL_Port* correspond au port SSL du serveur LDAP.

Par exemple : `ldaps://LDAPMachine.myCompany.com:636`

Notez la présence de `ldaps` dans l'URL.

Le port SSL par défaut des serveurs LDAP est `636`.

- Affectez à la propriété `SSL requis pour la connexion LDAP` la valeur `True`.

  Cette valeur requiert la connexion de Unica Platform au serveur LDAP à l'aide de SSL lors de la synchronisation avec le serveur LDAP.

Configuration de SSL dans Unica Platform avec filtres de données

Si Unica Platform est déployé avec SSL et que vous souhaitez utiliser la fonctionnalité de filtrage de données, vous devez exécuter cette procédure pour ajouter les options SSL qui établissent la liaison.

1. Suivez la procédure décrite dans "Configuration de SSL dans Unica Platform" si vous ne l'avez pas encore fait.
2. Collectez les informations suivantes.
   - Une copie du fichier certificat que vous avez créé dans Obtention ou création de certificats *(à la page)*
   - Le mot de passe du certificat
3. Placez le fichier certificat dans le répertoire *JAVA_HOME*`/jre/lib/security` où *JAVA_HOME* est le répertoire Java™ spécifié dans le script `tools/bin/setenv` sous votre installation Unica Platform.

   Le script `setenv` spécifie l'instance Java™ utilisée par les utilitaires Unica Platform.
4. Utilisez le programme `keytool` pour importer le certificat dans le fichier `cacerts` pour votre instance Java™.

   Vous pouvez utiliser l'exemple de commande suivant comme guide.

```
keytool -import -trustcacerts -file name_of_your_certificate.cer
-keystore cacerts
```

Entrez le mot de passe du certificat lorsque vous y êtes invité.

Configuration de SSL dans Unica Plan

Cette procédure permet de configurer SSL dans Unica Plan.

1. Connectez-vous à Unica, puis cliquez sur **Paramètres > Configuration**.
2. Paramétrez la valeur de la propriété `Marketing Operations | navigation | serverURL` sur l'URL de l'application Web Unica Plan.

   Par exemple : `serverURL=https://host:SSL_port/plan`

   où :

   - *`host`* est le nom ou l'adresse IP de la machine sur laquelle Unica Plan est installé.
   - *`SSL_Port`* est le port SSL de l'application Web Unica Plan.

   Notez que l'URL commence par `https`.
3. Ouvrez le fichier `plan_config.xml` dans un éditeur de texte ou XML.

   Le fichier `plan_config.xml` se trouve dans le répertoire `conf` de votre installation d'Unica Plan.
4. Définissez la propriété `UAPInitParam notifyPlanBaseURL` de votre connexion SSL.

   Par exemple : `<UAPInitParam notifyPlanBaseURL="https://host:SSL_Port/plan/affiniumplan.jsp"/>`

   où :

   - *`host`* est le nom ou l'adresse IP de la machine sur laquelle Unica Plan est installé.
   - *`SSL_Port`* est le port SSL de l'application Web Unica Plan.

   Notez que l'URL commence par `https`.
5. Pour que la fonctionnalité Adobe™ Acrobat Online Markup fonctionne avec Unica Plan sur HTTPS, définissez la propriété `markupServerURL` de la connexion SSL.

Par exemple : `<UAPInitParam markupServerURL="https://host:SSLport/plan/services/collabService?WSDL">`

où :

- *host* est le nom ou l'adresse IP de la machine sur laquelle Unica Plan est installé.
- *SSL_Port* est le port SSL de l'application Web Unica Plan.

Notez que l'URL commence par `https`.

6. Enregistrez et fermez le fichier `plan_config.xml`.

Configuration de SSL dans Unica Campaign

Cette procédure permet de configurer SSL dans Unica Campaign.

Remarque : Si vous configurez SSL dans Unica Campaign, vous devez également configurer le programme d'écoute de Campaign Listener dans SSL. Dans le cas contraire, l'organigramme du planning risque d'afficher le statut `Unknown`.

1. Ouvrez le fichier `config.xml` dans un éditeur de texte ou XML.

   Le `config.xml file` se trouve dans le répertoire `conf` dans votre installation de Unica Campaign.
2. Définissez les valeurs suivantes dans le fichier `config.xml`.
   - `unicaServerSSLFile = PATH_TO_OPENSSL_PEM/campaign.pem`
3. Enregistrez et fermez le fichier `config.xml`.
4. Connectez-vous à Unica Platform, puis cliquez sur **Paramètres > Configuration**.

   La page Configuration s'affiche.
5. Définissez la propriété `Campaign | unicaACListener | useSSL` sur `Oui`.
6. Si vous avez déployé l'application Web sur un port SSL, définissez la propriété `Campaign | navigation | serverURL` sur l'URL de l'application. Par exemple :

   `serverURL=https://host:SSL_port/Campaign`

   où :

- `hôte` représente le nom ou l'adresse IP de la machine sur laquelle l'application Web est installée.
- `SSL_Port` est le port SSL de l'application Web.

Notez que l'URL commence par https.

7. Si vous utilisez la surveillance opérationnelle, configurez-la pour le protocole SSL en paramétrant la valeur de la propriété `Campaign | surveillance | serverURL` de sorte à pouvoir utiliser HTTPS. Par exemple :

   ```
   serverURL=https://host:SSL_port/Campaign/OperationMonitor
   ```

   où :

   - `hôte` représente le nom ou l'adresse IP de la machine sur laquelle l'application Web est installée.
   - `SSL_Port` est le port SSL de l'application Web.

   Notez que l'URL commence par `https`.

Configuration de la liste des chiffrements dans Unica Campaign

Prérequis : Unica Campaign doit être configuré avec SSL.

Si l'application Unica Campaign et le programme d'écoute sont configurés avec les options SSL en tant que `TRUE`, les 98 chiffrements par défaut sont alors pris en charge pour activer la communication SSL entre l'application Unica Campaign (serveur) et le programme d'écoute.

Pour interdire les chiffrements faibles dans cette liste de chiffrements par défaut, les utilisateurs peuvent avoir recours à la balise ou à la propriété `<SSLCipherList>` dans le fichier config.xml.

Pour supprimer la prise en charge des chiffrements faibles, les utilisateurs doivent ajouter la ligne suivante dans le fichier config.xml. Elle indique que la prise en charge des chiffrements par défaut exclut `AES256-SHA, CAMELLIA256-SHA, AES128-SHA, SEED-SHA, CAMELLIA128-SHA, DES-CBC3-SHA, IDEA-CBC-SHA`.

```
<property name="SSLCipherList"><value>DEFAULT:!AES256-SHA:!CAMELLIA256-SHA:!AES128-SHA:!SEED-SHA:!CAMELLIA128-SHA:!DES-CBC3-SHA:!IDEA-CBC-SHA</value></property>
```

Cela désactive les chiffrements susmentionnés, qui sont inclus dans la balise `<SSLCipherList>` du fichier config.xml.

Si les clients ou les utilisateurs ne mentionnent pas la balise SSLCipherList dans le fichier config.xml, la liste de chiffrement par défaut est prise en compte et 98 chiffrements sont pris en charge.

Remarque : Le programme d'écoute ne démarre pas et les erreurs suivantes sont générées dans le fichier unica_aclsnr.log, si les utilisateurs ou les clients désactivent tout chiffrement requis par le certificat ou le navigateur.

```
Error enabling SSL connection.

SOCKET BIND port=4664: ERRNO 10048: Unknown error
```

Configuration de SSL dans Unica Campaign pour un environnement de cluster

Pour configurer SSL dans un serveur de programme d'écoute Unica Campaign dans un environnement de cluster, procédez comme suit.

1. Ouvrez le fichier `config.xml` du serveur de programme d'écoute dans un éditeur de texte ou XML.

   Le `config.xml file` se trouve dans le répertoire `conf` dans votre installation de Unica Campaign.
2. Définissez les valeurs suivantes dans le fichier `config.xml`.

- Définissez **configurationServerBaseURL** sur l'URL de la couche SSL de Campaign. Il s'agit de l'URL d'HCL HTTP Server.
- Définissez le chemin où le fichier de mot de passe est enregistré dans **unicaServerSSLFile**.
- Définissez le chemin où le fichier de mot de passe est enregistré dans **unicaServerSSLFilePwd**.

Par exemple :

```
<configuration name="bootstrap">
   <category name="bootstrap">
      <property name="suiteName"><value>Affinium</value></property>
      <property name="clientType"><value>HTTP</value></property>
      <!-- configurationServerBaseURL value will be set by
 AffiniumSuite assembly installer -->
      <property
 name="configurationServerBaseURL"><value>https://<IHS_Host>/Campaign<
/value></property>
      <property
 name="trustedApplication"><value>false</value></property>
      <property name="unicaClientKeystore"><value></value></property>
      <property
 name="unicaClientKeystorePwd"><value></value></property>
      <property
 name="unicaServerSSLFile"><value>/PATH_TO_OPENSSL_PEM/campaign.pem</v
alue></property>
   <property name="unicaServerSSLFilePwd"><value></value></property>
   </category>
</configuration>
```

3. Enregistrez et fermez le fichier `config.xml`.

Configuration de Campaign en mode SSL et du programme d'écoute de Campaign en mode non SSL

Si votre configuration comporte Campaign en mode SSL et le programme d'écoute de Campaign en mode non SSL, vous devez configurer des paramètres pour que les applications fonctionnent parfaitement.

L'application Web Campaign doit être configurée dans SSL via les certificats par défaut.

Toutes les configurations sont applicables à WebSphere Application Server for Campaign. La configuration des modes SSL et non SSL est une procédure en plusieurs étapes. Chacune d'entre elles peut comporter des sous-étapes.

Pour configurer Campaign en mode SSL et le programme d'écoute de Campaign en mode non SSL, procédez comme suit :
Procédez comme suit.

Tableau 50. Configuration de Campaign en mode SSL et du programme d'écoute de Campaign en mode non SSL

#	Etape	Sous-étapes

1	Générez et utilisez un fichier `.pem` (certificat).	Exécutez les commandes suivantes à partir de n'importe quel emplacement et prenez note des chemins. Créez un nouvel exemple de fichier de certificat campaign.pem (copiez le contenu des fichiers key.pem et certificate.pem dans ce nouveau fichier, en le séparant par une nouvelle ligne)
		`set OPENSSL_CONF=CAMPAIGN_HOME\bin\openssl.cnf`
		`openssl genrsa -out key.pem 4096`
		`openssl req -config openssl.cnf -new -key key.pem -out request.pem`
		`openssl req -config openssl.cnf -x509 -key key.pem -in request.pem -days 1000 -out certificate.pem`
		Les fichiers suivants sont générés à l'emplacement à partir duquel vous avez exécuté les commandes.

#	Etape	Sous-étapes
		• key.pem • request.pem • certificate.pem • campaign.pem
2	Importez le fichier `campaign.pem` sur le serveur d'applications où l'application Web de Campaign est déployée.	a. Copiez le fichier `campaign.pem` sur le serveur d'applications Web de Campaign. b. Ajoutez le fichier `campaign.pem` à la clé **NodeDefaultTrustStore** de WebSphere Application Server de la manière suivante : i. Cliquez sur **Sécurité > Certificat SSL et gestion des clés > Magasins de clés et certificats**. ii. Cliquez sur **NodeDefaultTrustStore > Certificats de signataire**. iii. Cliquez sur **Ajouter** et spécifiez l'**alias** et le chemin d'accès dans lequel le fichier `campaign.pem` est copié. iv. Cliquez sur **OK**. La clé du programme d'écoute est ajoutée au serveur d'applications.

3	Modifiez le fichier `config.xml` sur le serveur de programme d'écoute.	Indiquez les informations suivantes :
		
		• **configurationServerBaseURL** : indiquez l'URL de la couche SSL Campaign.
		• **unicaServerSSLFile** : indiquez le chemin d'accès au fichier `PATH_TO_OPENSSL_PEM/campaign.pem`.
		• **unicaServerSSLFilePwd** : indiquez le chemin d'accès correspondant au fichier `password`.
		
		`<configuration name="bootstrap">`
		`<category name="bootstrap">`

#	Etape	Sous-étapes
		<property name="suiteName"><value>Affinium</value></property> <property name="clientType"><value>HTTP</value></property> <!-- configurationServerBaseURL value will be set by AffiniumSuite assembly installer --> <property name="configurationServerBaseURL"> <value>https://eagle191.hcl.com:9447/Campaign</value> </property> <property name="trustedApplication"><value>false</value></property> <property name="unicaClientKeystore"><value></value></property> <property name="unicaClientKeystorePwd"><value></value></property> <property name="unicaServerSSLFile"> <value>PATH_TO_OPENSSL_PEM/campaign.pem</value> </property> <property name="unicaServerSSLFilePwd"> <value> password </value> </property>

#	Etape	Sous-étapes
		</category> </configuration>
4	Dans les paramètres **unicaACListener**, définissez **useSSL** sur **TRUE**.	-
5	Redémarrez le serveur d'applications de Campaign et le programme d'écoute de Campaign.	-

Configuration de SSL dans Unica Optimize

Cette procédure permet de configurer SSL dans Unica Optimize.

1. Ouvrez dans un éditeur de texte ou XML le fichier `config.xml` qui se trouve dans le répertoire `conf` de votre installation d'Unica Optimize.
2. Définissez la valeur `unicaServerSSLFile` sur le chemin complet du certificat que vous utilisez.
3. Enregistrez et fermez le fichier `config.xml`.
4. Pour la propriété de configuration `Campaign| unicaACOListener | useSSL`, spécifiez `oui`.
5. Si vous utilisez l'outil de ligne de commande Unica Optimize `ACOOptAdmin`, effectuez les étapes suivantes.

a. Collectez les informations suivantes.
   - Une copie du fichier certificat que vous avez créé dans Obtention ou création de certificats *(à la page)*
   - Le mot de passe du certificat

b. Placez le fichier certificat dans le répertoire *JAVA_HOME*`/jre/lib/security`, où *JAVA_HOME* est le répertoire Java™ spécifié dans le script `ACOOptAdmin`.

c. Utilisez le programme `keytool` pour importer le certificat dans le fichier `cacerts` pour votre instance Java™.

   Vous pouvez utiliser l'exemple de commande suivant comme guide.

   ```
   keytool -import -trustcacerts -file name_of_your_certificate.cer
   -keystore cacerts
   ```

   Entrez le mot de passe du certificat lorsque vous y êtes invité.

Configuration de SSL dans Unica Interact

Vous pouvez configurer la communication SSL pour Unica Interact dans trois emplacements, bien que cette procédure puisse considérablement diminuer les performances.

Les emplacements pouvant utiliser SSL sont les suivants :

- L'environnement de conception est le client et l'environnement d'exécution, le serveur.

  Utilisez https dans l'URL faisant référence au serveur d'exécution d'Unica Interact. Par exemple, définissez `Campaign | partitions | partition[n] | Interact | ServerGroups | [GroupeDeServeurs] | instanceURLs | [URLD'Instance] | instanceURL` sur `https://myserver.domain.com:7007/interact`.
- L'environnement d'exécution est le client et Unica Platform le serveur.
- Votre point de contact est le client et l'environnement d'exécution, le serveur.

Spécifiez l'URL HTTPS avec la méthode `getInstance`. Si vous utilisez un équilibreur de charge, vous devrez peut-être le configurer également pour SSL.

- Si le serveur de conception et le serveur d'exécution Unica Interact sont sur des hôtes distincts utilisant SSL, importez les certificats de sécurité sur les deux serveurs pour permettre l'établissement de liaison SSL.

Important : La configuration d'un composant d'Unica Interact pour communiquer à l'aide de SSL a une incidence sur les performances. Il n'est pas recommandé de configurer Unica Interact pour utiliser SSL.

Configuration de SSL dans Unica Collaborate

Après avoir configuré Unica Campaign pour utiliser le protocole SSL, aucune autre configuration supplémentaire n'est nécessaire pour configurer Unica Collaborate pour ce protocole.

Configuration de SSL dans les rapports

Cette procédure permet de configurer SSL dans les rapports.

1. Configurez Cognos® avec le protocole SSL, comme décrit dans la documentation Cognos®.
2. Configurez Apache avec le protocole SSL, comme décrit dans la documentation Apache.
3. Enregistrez le certificat Cognos® dans Unica, comme indiqué dans la documentation Cognos®.
4. Enregistrez les certificats Unica dans Cognos®, comme indiqué dans la documentation Cognos®.

Configuration de SSL dans Digital Analytics for On Premises

Digital Analytics for On Premises n'accepte aucune demande : il sert toujours de client au sein des communications HTTP et HTTPS en vue de résoudre les titres de page sur le site Web analysé. Pour résoudre les titres des pages d'un site qui utilise SSL, vous devez

simplement vous assurer que l'URL entrée dans les options de profil du site Web ou des serveurs en clusters analysés est correcte et qu'elle inclut le protocole HTTPS.

Digital Analytics for On Premises ne communique pas avec Unica Platform.

Vérification de la configuration SSL

Cette procédure permet de vérifier la configuration SSL.

1. Lancez chacune de vos applications Unica.
2. Connectez-vous à Unica et accédez à chacune de vos applications Web Unica installées.
3. Pour les serveurs d'exécution Unica Interact uniquement, testez la connexion avec l'URL `https://host:port/interact/jsp/admin.jsp`.
4. Si vous utilisez un certificat autosigné, dirigez votre navigateur vers chaque composant serveur d'Unica et vérifiez que les informations contenues dans le certificat que vous avez reçu correspondent à celles attendues.

   Par exemple, si le programme d'écoute Unica Campaign s'exécute sur le port 4664 d'un hôte nommé `campaignHost`, faites pointer votre navigateur vers `https://campaignHost:4664`.

   Votre navigateur affiche une fenêtre vous invitant à accepter le certificat, et vous pouvez consulter des informations détaillées à propos du certificat.

Liens utiles pour le protocole SSL

Ces liens fournissent des informations supplémentaires sur les tâches requises pour implémenter SSL dans Unica.

- Documentation OpenSSL - https://www.openssl.org/
- Documentation de l'outil de clé Java - http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/keytool.html
- Liste des autorités de certification - https://curlie.org/Computers/Security/Public_Key_Infrastructure/PKIX/Tools_and_Services/Third_Party_Certificate_Authorities/

Paramètres de qualité de protection de WebLogic

Vous devez définir les paramètres de qualité de protection lorsque vous configurez des applications HCL Unica pour utiliser SSL.

Les paramètres de qualité de protection suivants sont pris en charge pour WebLogic :

- TLS11
- TLS12

Pour modifier les paramètres de qualité de protection, procédez comme suit :
Ajoutez l'option suivante à la variable `JAVA_OPTIONS` :

- Pour TLS11- `-Dweblogic.security.SSL.protocolVersion=TLSv1.1`
- Pour TLS12- `-Dweblogic.security.SSL.protocolVersion=TLSv1.2`

Paramètres de qualité de protection de WebSphere

Vous devez définir les paramètres de qualité de protection lorsque vous configurez des applications HCL Unica pour utiliser SSL.

Les paramètres de qualité de protection suivants sont pris en charge pour WebSphere :

- SSL_TLS
- SSL
- TLS
- TLSv1
- SSL_TLSv2
- TLSv1.1
- TLSv1.2

Pour modifier les paramètres de qualité de protection, procédez comme suit :

1. Accédez à la page **Sécurité > Certificat SSL et gestion des clés > SSL configurations**
2. Sélectionnez la configuration SSL obligatoire.

3. Sous **Propriétés supplémentaires**, cliquez sur **Paramètres de qualité de protection (QoP)**.
4. Dans la sous-fenêtre **Paramètres de qualité de protection (QoP)**, sélectionnez les paramètres de qualité de protection obligatoires dans la liste déroulante **Protocole**.
5. Cliquez sur **Sauvegarder**.
6. Dans le fichier `ssl.client.props` situé dans le dossier `WAS_install\profiles\AppSrv01\properties`, mettez à jour les éléments suivants :

   ```
   com.ibm.ssl.protocol=<Specify required QoP settings>
   ```

7. Redémarrez le serveur d'applications.

Infrastructure de sécurité des API Unica

Unica Platform fournit l'infrastructure de sécurité des API implémentées par les produits Unica.

Un ensemble de propriété de configuration sur la page **Paramètres > Configuration** permet aux développeurs de définir la sécurité suivante pour les API fournies par les produits Unica.

- Pour une API de produit spécifique, vous pouvez bloquer l'accès au produit.
- Pour une API de produit spécifique, vous pouvez exiger HTTPS pour la communication entre l'API spécifiée et le produit.
- Pour une API de produit spécifique, vous pouvez exiger l'authentification pour la communication entre l'API spécifiée et le produit.

Les propriétés de configuration qui contrôlent la sécurité de l'API se trouvent sous la catégorie **Unica Platform | Sécurité | Gestion de l'API**. Chaque produit dispose d'un modèle de propriété de configuration que vous pouvez utiliser pour créer de nouveaux paramètres de sécurité pour les API fournies par ce produit.

Vous pouvez définir et modifier les paramètres de sécurité d'une API de manière appropriée pour les tests d'unités ou le déploiement ou au cours du cycle de vie des API.

L'infrastructure de sécurité prend actuellement uniquement en charge les API de Unica Campaign.

L'infrastructure de sécurité Unica Platform prend en charge les deux options d'authentification suivantes pour l'accès aux API protégées. Vous pouvez utiliser l'une ou l'autre, en fonction de votre environnement.

- Les utilisateurs internes qui sont enregistrés sur Unica Platform peuvent être authentifiés à l'aide de leurs données d'identification de connexion Unica Platform pour obtenir un jeton sécurisé.
- Les utilisateurs externes qui font partie d'une fédération Unica Platform qui est configuré pour utilisation, peuvent être authentifiés via le serveur du fournisseur d'identité.

Authentification d'utilisateurs internes avec l'API de connexion Unica Platform

Pour authentifier des utilisateurs internes dans des applications client, utilisez l'API Unica Platform `login` afin de générer des jetons sécurisés. Vous pouvez ensuite appeler n'importe quelle API protégée en transmettant les paramètres requis dans l'en-tête de requête, en plus des paramètres attendus par l'API.

Le filtre de sécurité intercepte ces demandes protégées, les valide et les transmet pour traitement.

Une fois l'utilisateur Unica Platform authentifié, le filtre de sécurité Unica Platform ajoute le nom de connexion de l'utilisateur à la demande en tant qu'attribut de la clé `USER_NAME_STRING` avant de le transmettre au produit pour traitement.

Les jetons sécurisés ont un cycle de vie par défaut de 15 secondes. Une fois ce délai expiré, le jeton ne peut plus être utilisé pour appeler une API protégée. Chaque fois que l'API Unica Platform `login` est appelée pour un utilisateur, l'intégralité des jetons de sécurité précédents pour cet utilisateur est invalidée.

Vous pouvez changer le cycle de vie des jetons sécurisés en définissant la valeur de la propriété **Token lifetime** située sur la page **Paramètres > Configuration** sous la catégorie **Général | Divers**.

Exemple d'URL

`http[s]://`*`host`*`:`*`port`*`/unica/api/manager/authentication/login/`

Paramètres d'en-tête

Tableau 51. Paramètres d'en-tête de l'API de connexion avec des utilisateurs internes

Paramètre	Description
`m_user_name`	Nom de connexion Unica Platform de l'utilisateur interne.
`m_user_password`	Mot de passe Unica Platform en texte en clair de l'utilisateur interne.

Réponse

Lorsque la connexion aboutit, la réponse est HTTP 200 avec les données JSON suivantes.

- `m_tokenId` - jeton généré de manière aléatoire
- `m_user_name` - nom de l'utilisateur connecté
- `createDate` - horodatage au format affiché dans l'exemple suivant, où le fuseau horaire est IST (heure normale de l'Inde) :

  ```
  Mon Jul 06 18:23:35 IST 2015
  ```

Lorsque la connexion échoue avec des données d'identification incorrectes, la réponse est HTTP 401 (non autorisé). Lorsque l'API de `login` est configurée pour être bloquée, la réponse est 403 (interdit). Lorsque l'API de `login` est configurée pour utiliser HTTPS, et si elle est appelée sur HTTP, la réponse est 403 (interdit).

Pour déconnecter des utilisateurs internes, utilisez l'API de Unica Platform `logout`.

Déconnexion d'utilisateurs internes avec l'API de déconnexion Unica Platform

Utilisez l'API de Unica Platform `logout` pour déconnecter des utilisateurs internes et supprimer le jeton sécurisé.

L'API de `logout` est protégée par défaut. Les paramètres d'authentification sont prévus dans l'en-tête de requête en regard des clés prédéfinies.

Exemple d'URL

`http[s]://host:port/unica/api/manager/authentication/logout/`

Paramètres d'en-tête

Tableau 52. Paramètres d'en-tête de l'API de déconnexion

Paramètre	Description
`m_user_name`	Nom de connexion Unica Platform de l'utilisateur interne.
`m_tokenId`	Jeton sécurisé obtenu via l'authentification.
`api_auth_mode`	Utilisez la valeur `manager` pour les utilisateurs internes.

Réponse

Lorsque l'authentification aboutit, la réponse est `HTTP 200` et le jeton sécurisé est supprimé. Si la réponse est HTTP 200, l'application client doit confirmer la déconnexion.

Lorsque l'authentification échoue, la réponse est `HTTP 401`.

Authentification des utilisateurs externes et déconnexion via une fédération

Lorsque Unica Platform est intégré avec une fédération prise en charge, les utilisateurs peuvent se connecter à leur propre système et l'application client obtient un jeton via le serveur IdP (Identity Provider) fourni par Unica Platform.

Une fois qu'un utilisateur fédéré est authentifié, son nom de connexion Unica Platform correspondant est ajouté à la requête comme attribut de la clé `USER_NAME_STRING`.

La déconnexion doit être effectuée sur le serveur IdP.

Paramètres d'en-tête

Le tableau suivant décrit les paramètres d'en-tête à utiliser lors de l'authentification via le serveur IdP fourni par Unica Platform.

Tableau 53. Paramètres d'en-tête avec une fédération

Paramètre	Description
f_userId	ID utilisateur dans la fédération.

Tableau 53. Paramètres d'en-tête avec une fédération (suite)

Paramètre	Description
f_clientId	ID client dans la fédération.
f_spId	ID de fournisseur de services dans la fédération.
f_tokenId	Jeton de connexion unique du serveur IdP.
api_auth_mode	Utilisez la valeur `fsso` pour l'authentification fédérée.

Réponse

La réponse est `HTTP 200`, avec des éléments supplémentaires en fonction de l'API.

Création et gestion des filtres de données

Les filtres de données permettent de restreindre les données du client qu'un utilisateur Unica peut consulter et utiliser dans les applications Unica. Les données que vous sécurisez à l'aide d'un filtre de données correspondent à un jeu de données défini par les zones des tables client que vous spécifiez.

Les différentes applications Unica utilisent les filtres de données de manières différentes. Consultez la documentation des produits individuels pour déterminer si le produit utilise le filtrage des données et, si c'est le cas, obtenir des informations relatives au filtrage des données dans ce produit.

Présentation de la création de filtres de données

Unica Platform offre les fonctions suivantes utilisées par les administrateurs d'Unica pour configurer les filtre de données.

- Utilitaire de définition des filtres de données.
- Interface utilisateur pour affecter les utilisateurs et les groupes dans des filtres de données et afficher les filtres de données affectés.

Associations de filtres de données pour limiter l'accès utilisateur

Pour restreindre l'accès aux données d'utilisateurs ou de groupes d'utilisateurs, affectez-les à des filtres de données. Vous pouvez affecter des filtres de données à tous les utilisateurs et groupes d'utilisateurs d'Unica.

Vous pouvez affecter des utilisateurs et des groupes à un filtre de données unique. Vous pouvez également affecter un utilisateur ou un groupe d'utilisateurs à plusieurs filtres de données.

Remarque : Les groupes n'acquièrent pas les affectations de filtres de données de leurs sous-groupes.

Un utilisateur affecté à plusieurs filtres de données peut consulter les enregistrements autorisés par tous ces filtres de données.

Deux méthodes de création de filtres de données : la génération automatique et la spécification manuelle

Unica Platform possède un utilitaire, `datafilteringScriptTool`, qui traite le fichier XML pour créer les filtres de données dans les tables système de Unica Platform. Vous pouvez utiliser cet utilitaire de deux façons distinctes selon la façon dont vous écrivez le fichier XML : en génération automatique ou en spécification manuelle.

Génération automatique

L'utilitaire `datafilteringScriptTool` peut générer automatiquement les filtres de données à partir d'une table ou d'une vue de base de données, accessible via JDBC. L'utilitaire crée automatiquement des filtres de données en fonction de combinaisons uniques de valeurs dans des zones spécifiées dans le fichier XML (un filtre de données pour chaque combinaison unique).

Vous pouvez être amené à utiliser cette méthode si vous devez créer un grand nombre de filtres de données à partir de combinaisons uniques de valeurs dans différentes zones.

Spécification manuelle

L'utilitaire `datafilteringScriptTool` permet de créer des filtres de données de façon séquentielle, en fonction des valeurs de zone que vous avez spécifiées.

Il est conseillé d'utiliser cette méthode si vous souhaitez créer un ensemble de filtres de données qui n'inclut pas chaque combinaison unique de valeurs de zone.

Deux façons d'affecter des utilisateurs et des groupes : dans l'interface utilisateur et dans le code XML

Vous disposez de deux possibilités pour affecter des utilisateurs et des groupes à des filtres de données : via l'interface utilisateur ou dans le code XML que vous utilisez pour créer les filtres de données. L'affectation d'utilisateurs dans le code XML est une méthode pratique lorsque vous avez de nombreux utilisateurs et que chacun d'entre eux a besoin d'un filtre distinct.

L'affectation d'utilisateurs dans le code XML n'est possible que lorsque vous créez des filtres de données à l'aide d'une spécification **manuelle**. Lorsque vous affectez les utilisateurs dans le code XML, vous avez besoin de l'ID du filtre de données pour définir l'affectation, et cet ID n'est disponible que lorsque vous définissez le filtre manuellement, et non automatiquement.

L'utilisation de ces deux méthodes pour affecter des utilisateurs et des groupes est décrite en détail dans ce chapitre.

Concepts des filtres de données

Pour comprendre comment configurer des filtres de données, vous devez être familiarisé avec certains concepts utilisés dans la fonctionnalité de filtre de données, aux bases de données en général et à Unica Campaign en particulier, si vous configurez des filtres de données qui seront utilisés dans une application de la gamme de Unica Campaign.

- **configuration des données** – Une configuration de données regroupe un ensemble de filtres de données. Tous les filtres de données qui sécurisent les données connexes sont associés à la même configuration de données.
- **audience** - La ou les zone(s) des tableaux clients créée(s) dans Unica Campaign en tant que niveau d'audience. Les niveaux d'audience classiques sont foyer et individu.
- **nom de zone physique** – Les noms physiques des zones du tableau de base de données sont les noms que vous voyez lorsque vous visualisez les tableaux directement à partir du client de base de données. Si le filtre de données est utilisé, il utilise le nom physique dans les recherches à l'intérieur de la base de données client.
- **nom de la zone logique** – Lorsque vous définissez les filtres de données, vous donnez des noms logiques aux zones physiques. Si vous configurez des filtres de données qui seront utilisés dans une application de la famille Unica Campaign, ces noms logiques devront être identiques aux noms donnés aux zones dans Unica Campaign. Ce nom sera utilisé par l'utilitaire lors de la génération des filtres de données.

Organisation du processus de configuration : crée des filtres de données

Cette feuille de route du processus de configuration permet d'analyser les tâches requises pour configurer les filtres de données. La colonne Rubrique contient des liens vers les rubriques qui décrivent les tâches en détail.

Tableau 54. Feuille de route du processus de configuration des filtres de données

Sujet	Informations
• Planification des critères de filtre de données : génération automatique *(à la page 267)* • Planification des critères de filtre de données : manual generation *(à la page 268)*	Définissez les données client à sécuriser.

Tableau 54. Feuille de route du processus de configuration des filtres de données (suite)

Sujet	Informations
Obtention du pilote JDBC pour votre base de données : génération automatique uniquement *(à la page 269)*	pour génération automatique uniquement : Procurez-vous le pilote JDBC de type4 pour la connexion à la base de données qui contient la table sur laquelle vous souhaitez baser vos filtres de données.
Obtention des informations requises *(à la page 269)*	Collectez les informations requises sur la base de données, ainsi que des informations relatives à Unica Campaign si vous prévoyez d'utiliser les filtres de données avec une application de la famille de Unica Campaign.
Création du fichier XML de spécification des filtres de données *(à la page 270)*	Créez le fichier XML qui spécifie les données client utilisées comme critères dans chaque filtre de données.
Définition des propriétés de configuration requises pour les filtres de données *(à la page 271)*	Définissez les propriétés de configuration pour activer le filtrage de données.
Remplissage des tables système des filtres de données *(à la page 272)*	Exécutez l'utilitaire `datafilteringScriptTool`, qui remplit les tables système de Unica Platform utilisées pour les filtres de données à partir de votre fichier XML.
Affectation d'utilisateurs et de groupes à des filtres de données *(à la page 273)*	Si vous n'affectez pas d'utilisateurs et de groupes aux filtres de données dans le XML, utilisez l'interface utilisateur du filtre de données Unica pour effectuer des recherches d'utilisateurs, de groupes et de filtres de données, puis sélectionnez des éléments parmi les résultats des recherches et affectez-les.

Planification des critères de filtre de données : génération automatique

Les critères des filtres de données sont basés sur vos données client. Avant de définir les filtres, vous devez définir les données client à sécuriser.

Par exemple, vous pouvez avoir besoin de limiter l'accès aux données client en fonction du pays, de la ville et de l'état de résidence du client. Si votre base de données client comporte une table qui contient des zones de pays, de ville et d'état, vous devrez peut-être choisir de baser un groupe de filtres de données sur ces zones. Vous utiliserez ensuite ces valeurs lors de la spécification de vos filtres.

Tenez compte des concepts suivants lorsque vous planifiez la création de filtres de données selon la méthode de génération automatique.

- **Zone profil** - Zone dont la valeur est prise en compte lorsque l'utilitaire de génération de filtre de données recherche des combinaisons de valeurs uniques. L'utilitaire crée un filtre de données pour chaque combinaison de valeurs unique. Lorsque le filtre de données est en vigueur dans une application Unica, cette valeur est utilisée dans une clause WHERE lors de l'interrogation d'enregistrements client. Etant donné que cette clause vérifie l'égalité, les zones de profil doivent être définies sur des zones qui prennent en charge un nombre limité de valeurs.
- **Zone fixe** - Zone facultative permettant de limiter le nombre d'enregistrements pris en considération par l'utilitaire de génération de filtre de données lors de recherches de combinaisons uniques de valeurs de zone de profil. La valeur spécifiée est également incluse dans chaque filtre de données généré. Lorsque le filtre de données est en vigueur dans une application Unica, cette valeur est utilisée dans une clause WHERE lors de l'interrogation d'enregistrements client. Etant donné que cette clause vérifie l'égalité, les zones fixes doivent être définies sur des zones qui prennent en charge un nombre limité de valeurs.

Dans l'exemple ci-dessus, vous allez sans doute créer une zone fixe pour un pays et des zones de profil pour la ville et l'état. L'utilitaire de génération de filtre de données crée un filtre de données pour chaque combinaison unique de valeurs qu'il trouve dans ces zones.

Un utilisateur Unica affecté à un ou plusieurs filtres de données ne devrait être en mesure de visualiser et d'utiliser uniquement les données appartenant aux clients vivant dans les pays, villes et états correspondant au(x) filtre(s) de données spécifiés.

Il est possible que vos tables client ne contiennent pas toutes les valeurs pour lesquelles vous souhaitez créer un filtre de données. Par exemple, vous ne trouverez peut-être pas de clients dans chaque pays et statut, mais souhaiterez éventuellement préparer des filtres de données pour chaque pays et état pour une utilisation ultérieure. Dans ce cas, vous pouvez référencer une table qui inclut chaque pays et état et l'utiliser dans la section GenerateDataFilters de votre spécification XML. Lorsque vous avez terminé de créer vos filtres de données avec l'utilitaire, vous pouvez supprimer cette table fictive.

Planification des critères de filtre de données : manual generation

Les critères des filtres de données sont basés sur vos données client. Avant de définir les filtres, vous devez définir les données client à sécuriser.

Par exemple, vous pouvez être amené à limiter l'accès aux données client en fonction du territoire de vente géographique auquel l'utilisateur Unica est affecté. Si la zone Région de votre base de données client est liée aux secteurs de vente, vous pouvez choisir de baser un groupe de filtres de données sur cette zone.

Vous devez être familiarisé avec le concept de **contraintes de zone**, un concept que vous devez comprendre pour pouvoir créer des filtres de données selon une méthode de spécification manuelle. Une contrainte de zone est une paire zone/ valeur utilisée pour spécifier un filtre de données. Cette valeur est utilisée dans une clause WHERE lors de l'interrogation d'enregistrements client. Etant donné que cette clause vérifie l'égalité, les contraintes de zone doivent être définies sur des zones qui prennent en charge un nombre limité de valeurs.

Dans l'exemple, la zone Région peut contenir les régions suivantes : Asie, Moyen-Orient, Amérique du Nord et Amérique du Sud. Vous utiliserez ces valeurs lors de la spécification de contraintes de zone pour vos filtres. Définissez un filtre de données différent pour chaque secteur de vente en utilisant les valeurs de la zone Région de vos tables client en tant que contraintes de zone.

Un utilisateur Unica affecté à un ou plusieurs filtres de données ne devrait être en mesure de visualiser et d'utiliser uniquement les données appartenant aux clients appartenant au(x) territoire(s) de vente correspondant au(x) filtre(s) de données spécifiés.

Les filtres de données que vous créez à l'aide de la méthode manuelle peuvent être affectés aux utilisateurs par l'interface utilisateur ou en entrant les affectations dans le code XML.

Obtention du pilote JDBC pour votre base de données : génération automatique uniquement

L'utilitaire `datafilteringScriptTool` requiert un pilote JDBC pour la génération automatique de filtres de données.

1. Procurez-vous le pilote JDBC de type 4 pour la connexion à la base de données qui contient la table sur laquelle vous souhaitez baser vos filtres de données.
2. Placez le pilote sur la machine sur laquelle Unica Platform est installé.
3. Notez le nom de la classe et le chemin d'accès.

Obtention des informations requises

Pour créer des filtres de données, vous devez collecter des informations sur vos données et sur la manière dont elles sont mappées dans vos produits Unica.

Pour **spécification manuelle** uniquement : Collectez les informations suivantes.

- Le nom physique de la table qui contient les zones à utiliser.
- Le jeu limité de données des zones à utiliser pour les contraintes de zone.
- Si vous envisagez d'utiliser les filtres de données au sein d'une application appartenant à la famille Unica Campaign, procurez-vous les noms attribués aux zones suivantes dans Unica Campaign :
    - Les zones assistance
    - Les zones que vous prévoyez d'utiliser pour les contraintes de zone.

pour **génération automatique** uniquement : Collectez les informations suivantes.

- Pour la base de données qui contient la table à utiliser dans la définition des filtres de données : le type de base de données, le nom ou l'adresse IP et le port.
- Les données d'identification (nom d'utilisateur et mot de passe) qui permettent de se connecter à la base de données.
- Le nom physique de la table qui contient les zones à utiliser.
- Le nom physique des zones à utiliser pour les zones d'analyse et les zones fixes, ces derniers étant facultatifs.
- Si vous envisagez d'utiliser les filtres de données au sein d'une application appartenant à la famille Unica Campaign, procurez-vous les noms attribués aux zones suivantes dans Unica Campaign :
    - Les zones de référentiel.
    - Les zones que vous prévoyez d'utiliser pour les zones fixes et d'analyse.

Remarque : Lorsque vous définissez des filtres de données qui seront utilisés au sein d'une application appartenant à la famille de produits Unica Campaign, les noms logiques des zones spécifiées dans le fichier XML définissant les filtres de données doivent correspondre aux noms donnés à ces zones dans Unica Campaign.

Création du fichier XML de spécification des filtres de données

Créez le fichier XML qui spécifie les données client utilisées comme critères dans chaque filtre de données. Exécutez ensuite un utilitaire qui remplit les tables système à l'aide de ces spécifications.

Pour créer les filtres de données, l'utilitaire `datafilteringScriptTool` utilise une représentation XML des données pour insérer des entrées dans la base de données de la table système Unica Platform.

Voici une présentation des éléments du code XML que vous créez.

- `<Execute Batch>` - Commande d'initialisation du processus d'insertion des données. Cette commande est répétée plusieurs fois dans le fichier XML.
- `<AddDataConfiguration>` - Définit les configurations de données, qui sont des groupes de filtres de données associés.
- `<AddLogicalFields>` - Définit les zones d'application des filtres, et leurs types de données.
- `<AddDataFilter>` - En cas d'utilisation d'une **spécification manuelle**, référence une zone logique définie et spécifie les contraintes de zone.
- `<GenerateDataFilters>` - En cas d'utilisation d'une **spécification automatique**, référence les zones et les valeurs qui limitent les enregistrements pris en compte pour des combinaisons uniques de valeurs utilisées pour définir un ensemble de filtres de données.
- `<AddDataTable>` - Définit la relation entre les zones logiques et les tables et les colonnes physiques correspondantes. Une zone logique peut s'appliquer à différentes tables physiques, ce qui permet à un filtre de s'appliquer à plusieurs tables.
- `<addAudiences>` - Référence une zone logique définie, et spécifie le niveau d'audience défini dans Unica Campaign.
- `<addAudienceTableAssociations>` - Définit la relation entre un niveau d'audience et la table définie, et la configuration de filtre de données définie.
- `<AddAssignments>` - Lorsque **les affectations sont créées dans le XML plutôt qu'avec l'interface utilisateur**, associe des utilisateurs ou des groupes d'utilisateur individuels à des filtres de données définis.

Pour des informations supplémentaires, y compris la description des éléments supplémentaires imbriqués dans les éléments décrits ci-dessus, consultez les rubriques suivantes dans ce chapitre :

- La description détaillée de chaque élément du fichier XML
- Le XML fourni dans les exemples de scénario

Définition des propriétés de configuration requises pour les filtres de données

Définissez les propriétés de configuration requises pour activer le filtrage de données.

Sur la page **Paramètres & Configuration**, naviguez jusqu'à la catégorie **Général | Filtrage des données** et définissez les propriétés suivantes.

- Nom de la table par défaut
- Nom de l'audience par défaut

Consultez l'aide contextuelle de chaque propriété ou le lien de la rubrique connexe de cette section pour obtenir des instructions sur le paramétrage des valeurs.

Propriété de configuration facultative pour améliorer les performances des filtres de données

Vous pouvez activer le cache du filtre de données pour améliorer les performances.

Pour améliorer les performances, définissez la valeur de la propriété **Général | Filtrage des données | Activer le cache du filtre de données** sur **true**. Cette propriété spécifie si Unica Platform extrait des définitions de filtre de données de la base de données ou d'un cache. Lorsque cette valeur est **true**, les définitions de filtre de données sont stockées dans le cache et le cache est mis à jour dès que le filtre de données est modifié.

Vous devez redémarrer l'application Web Unica Platform après avoir modifié cette valeur de propriété, pour qu'elle prenne effet.

Remplissage des tables système des filtres de données

Exécutez l'utilitaire `datafilteringScriptTool`, qui utilise votre code XML pour remplir les tables système des filtres de données.

Pour plus d'informations sur l'utilisation de l'utilitaire `datafilteringScriptTool`, voir la description complète une autre section de ce guide.

Remarque : Si vous devez supprimer des filtres de données, exécutez le script `ManagerSchema_PurgeDataFiltering.sql`, décrit dans une autre section de ce guide.

Affectation d'utilisateurs et de groupes à des filtres de données

Si vous n'affectez pas les utilisateurs ou les groupes dans le XML que vous créez, utilisez l'interface utilisateur du filtre de données Unica pour effectuer des recherches d'utilisateurs, de groupes et de filtres de données, puis sélectionnez des éléments parmi les résultats des recherches et affectez-les.

Informations de référence XML pour les filtres de données

Cette section décrit les éléments XML pour lesquels vous devez fournir des valeurs.

A propos des ID dans le fichier XML

Certains objets nécessitent des ID. Par exemple, les configurations de données, les zones logiques et les tables de données nécessitent de spécifier des ID. Les ID que vous spécifiez doivent être uniques dans une catégorie d'objet.

Certains objets référencent d'autres objets à l'aide d'ID. Par exemple, les tables référencent les zones logiques. Lorsque vous devez référencer un autre objet, utilisez l'ID spécifié pour cet objet.

Le fichier XML utilise la convention suivante pour les noms d'élément d'ID. Cette convention vous permet de savoir quand créer un ID unique et quand référencer un autre ID dans le fichier XML.

- Lorsque vous devez créer un ID unique, l'élément s'appelle `id`.
- Lorsque vous devez référencer un autre ID d'objet, l'élément porte le nom de l'objet. Par exemple, l'élément ID dans lequel vous référencez une zone logique s'appelle `logicalFieldId`.

Les ID affectés à un objet ne sont pas les ID que Unica Platform affecte à l'objet. Les ID que vous affectez ne sont utilisés que dans le cadre du référencement de l'objet dans le fichier XML.

AddDataConfiguration | dataConfiguration

Ce groupe d'éléments permet de définir des configurations de données que vous utilisez pour regrouper des filtres de données associés. Vous devez créer une configuration de données pour chaque ensemble de filtres de données associés.

Tableau 55. AddDataConfiguration | dataConfiguration

Elément	Description	Table système
`id`	ID unique affecté à cette configuration de données.	S/O
`nom`	Nom affecté à ce groupe de filtres de données.	Table : df_config Zone : nom_config

AddLogicalFields | logicalFields | LogicalField

Ce groupe d'éléments permet de définir les zones logiques qui correspondent aux zones de la table client que vous utilisez pour définir vos filtres de données. Créez une zone logique pour chaque zone depuis laquelle vous voulez créer des contraintes de zone et une zone logique pour chaque type d'utilisateur.

Tableau 56. AddLogicalFields | logicalFields | LogicalField

Elément	Description	Table système
`id`	ID unique affecté à cette zone logique.	S/O
`nom`	Nom logique de cette zone ou de cette audience. S'il est utilisé avec une application de la gamme de Unica Campaign, il doit être identique au nom de zone ou d'audience utilisé dans Unica Campaign.	Table : df_logical_field Zone : logical_name

Tableau 56. AddLogicalFields | logicalFields | LogicalField (suite)

Elément	Description	Table système
`type`	Type de données de la zone dans la table client. Les valeurs admises sont les suivantes : • java.lang.String • java.lang.Long • java.lang.Double • java.lang.Boolean • java.lang.Date (le format de date est mois/jour/année et chaque élément est exprimé sous la forme d'un nombre.)	Table : df_logical_field Zone : type

GenerateDataFilters

Ce groupe d'éléments permet de générer des filtres de données lorsque vous utilisez une **génération automatique**.

Tableau 57. GenerateDataFilters

Elément	Description	Table système
`tableName`	Nom physique de la table à partir de laquelle vous voulez générer des filtres de données, y compris nom du schéma de base de données. Si la base de données est sensible à la casse, la casse doit correspondre à celle utilisée dans la base de données.	Table : df_table Zone : table_name

Tableau 57. GenerateDataFilters (suite)

Elément	Description	Table système
`configurationName`	Nom de la configuration de données dans l'élément `Add-DataConfiguration | data-Configuration` auquel cet ensemble de filtres de données est associé.	S/O
`jdbcUrl`	Référence de l'URL de la base de données client qui contient la table sur laquelle vous souhaitez baser les filtres de données.	S/O
jdbcUser	Nom d'utilisateur d'un compte qui dispose d'un accès à la base de données client.	S/O
`jdbcPassword`	Mot de passe du compte qui dispose d'un accès à la base de données client.	S/O
`jdbcDriverClass`	Nom du pilote JDBC qui fournit une connectivité à la base de données client.	S/O
`jdbcDriverClass-Path | chaîne`	Chemin du pilote JDBC.	S/O

GenerateDataFilters | fixedFields | FixedField

Ce groupe d'éléments permet de spécifier les zones facultatives et les valeurs qui limitent les enregistrements pris en compte lorsque l'utilitaire de génération des filtres de données

recherche des combinaisons uniques de valeurs pour définir un ensemble de filtres de données. Utilisé uniquement avec la **génération automatique**.

Tableau 58. GenerateDataFilters | fixedFields | FixedField

Elément	Description	Table système
`expression`	Un élément des données de la zone, qui sera utilisée dans une clause WHERE lors de la création de filtres de données et de l'extraction de données pour un utilisateur affecté à ce filtre. Si la base de données est sensible à la casse, la casse doit correspondre à celle utilisée dans la base de données.	Table : df_field_constraint Zone : expression
`logicalFieldName`	Nom de la zone logique dans l'élément AddLogicalFields | logicalFields | LogicalField. Ce nom apparaît sous la forme d'un libellé dans la zone de recherche avancée dans l'interface utilisateur Filtre des données dans Unica Platform.	Table : df_logical_field Zone : logical_name
`physicalFieldName`	Nom physique de la zone. Si la base de données est sensible à la casse, la casse doit correspondre à celle utilisée dans la base de données.	S/O

GenerateDataFilters | profileField | ProfileField

Ce groupe d'éléments permet de spécifier les zones dont les combinaisons uniques de valeurs sont utilisées pour définir un ensemble de filtres de données. Utilisé uniquement avec la **génération automatique**.

Tableau 59. GenerateDataFilters | profileField | ProfileField

Elément	Description	Table système
`logicalFieldName`	Nom de la zone logique dans l'élément `AddLogicalFields | logicalFields | Logical-Field`.	Table : df_logical_field Zone : logical_name
`physicalFieldName`	Nom physique de la zone. Si la base de données est sensible à la casse, la casse doit correspondre à celle utilisée dans la base de données.	S/O

AddDataTable | dataTable

Ce groupe d'éléments permet d'affecter des ID à des tables client.

Tableau 60. AddDataTable | dataTable

Elément	Description	Table système
`id`	ID unique affecté à cette table.	S/O
`nom`	Nom physique de la table client que vous voulez sécuriser. Si la base de données est sensible à la casse, la casse doit correspondre à celle utilisée dans la base de données.	Table : df_table Zone : table_name

AddDataFilters | dataFilters | DataFilter

Ce groupe d'éléments permet de créer un filtre de données lorsque vous utilisez une **spécification manuelle**.

Tableau 61. AddDataFilters | dataFilters | DataFilter

Elément	Description	Table système
`configId`	ID de la configuration de données dans l'élément AddDataConfiguration | dataConfiguration auquel ce filtre est associé.	S/O
`id`	ID unique que vous affectez.	S/O

AddDataFilters | dataFilters | DataFilter | fieldConstraints | FieldConstraint

Ce groupe d'éléments permet de spécifier les données dans une zone utilisée pour définir un filtre de données lorsque vous utilisez **spécification manuelle**.

Tableau 62. AddDataFilters | dataFilters | DataFilter | fieldConstraints | FieldConstraint

Elément	Description	Table système
`logicalFieldId`	ID du champ logique dans l'élément `AddLogicalFields | logicalFields | LogicalField`.	S/O
`expression`	Un élément des données d'une zone, qui est utilisée dans une clause `WHERE` lors de la création de filtres de données et de l'extraction de données pour un utilisateur affecté à ce filtre. Si la base de données est sensible	Table : df_fieldconstraint Zone : expression

Tableau 62. AddDataFilters | dataFilters | DataFilter | fieldConstraints | FieldConstraint (suite)

Elément	Description	Table système
	à la casse, la casse doit correspondre à celle utilisée dans la base de données.	

AddDataTable | dataTable | fields | TableField

Ce groupe d'éléments permet de mapper les zones physiques de la table client en zones logiques définies par vos soins.

Tableau 63. AddDataTable | dataTable | fields | TableField

Elément	Description	Table système
`nom`	Nom physique de la zone dans la table client. Si la base de données est sensible à la casse, la casse doit correspondre à celle utilisée dans la base de données.	Table : df_table_field Zone : physical_name
`logicalFieldId`	ID de la zone logique dans l'élément `AddLogicalFields | logicalFields | LogicalField`.	S/O

AddAudience | audience

Ce groupe d'éléments permet de définir le nom attribué dans Unica Campaign à un niveau d'audience utilisé dans la famille de produits Unica Campaign.

Tableau 64. AddAudience | audience

Elément	Description	Table système
`id`	ID unique affecté à cette audience.	S/O
`nom`	Nom de l'audience, comme indiqué dans Unica Campaign.	Table : df_audience Zone : audience_name

AddAudience | audience | champs | AudienceField

Ce groupe d'éléments permet de définir les zones des table client que vous utilisez comme zones d'audience.

Tableau 65. AddAudience | audience | champs | AudienceField

Elément	Description	Table système
`logicalFieldId`	ID du champ logique dans l'élément `AddLogicalFields | logicalFields | LogicalField`. S'il est utilisé avec une application de la gamme de Unica Campaign, il doit s'agir du même nom logique que celui utilisé dans Unica Campaign.	S/O
`fieldOrder`	Pour une utilisation ultérieure. Définissez la valeur sur `0`.	S/O

addAudienceTableAssociations | addAudienceTableAssociation | audienceTableAssociation

Ce groupe d'éléments permet d'associer des paires de zones assistance et de tables à des configurations de données. Créez une association pour chaque zone assistance.

Tableau 66. addAudienceTableAssociations | addAudienceTableAssociation | audienceTableAssociation

Elément	Description	Table système
`audienceId`	ID de l'audience à utiliser dans cette association. Il doit s'agir d'une valeur d'ID d'un élément `AddAudience | audience`.	S/O
`tableId`	ID de la table à utiliser dans cette association. Il doit s'agir d'une valeur d'ID d'un élément `AddDataTable | dataTable`. La table doit être celle qui contient l'audience spécifiée dans l'élément audienceID. Si l'audience existe dans plusieurs tables, créez plusieurs associations.	S/O
`configId`	ID de la configuration des données à utiliser dans cette association. Il doit s'agir d'une valeur d'ID d'un élément `AddDataConfiguration | dataConfiguration`.	S/O

AddAssignments | assignments | AssignmentByName

Vous pouvez utiliser ce groupe d'éléments pour associer des utilisateurs ou des groupes à des filtres de données. Facultatif. Vous pouvez également effectuer ces affectations dans l'interface utilisateur.

Tableau 67. AddAssignments | assignments | AssignmentByName

Elément	Description	Table système
`namespaceId`	Nom de la configuration de données dans l'élément `AddDataConfiguration | dataConfiguration` auquel cet ensemble de filtres de données est associé.	S/O
`dataObjectId`	ID du filtre à utiliser dans cette association. Doit être une valeur d'ID dans un élément `DataFilter`.	S/O
`principalType`	Type d'affectation. • 1 affecte un filtre de données à un utilisateur individuel • 2 affecte un filtre de données à un groupe d'utilisateurs	Table : ols_assignment Zone : principal_type
`principalName`	• Si la valeur de principalType est `1`, définissez la valeur sur le nom de connexion Unica Platform de l'utilisateur à affecter au filtre de données référencé. • Si la valeur de principalType est `2`, définissez la valeur sur le nom du groupe Unica Platform	Table : ols_assignment Zone : principal_id

Tableau 67. AddAssignments | assignments | AssignmentByName (suite)

Elément	Description	Table système
	dont vous voulez affecter les membres au filtre de données référencé.	

Exemple : Spécification manuelle de filtres de données

Jacques doit créer un jeu de filtres de données en fonction des secteurs de vente.

Dans Unica Campaign, les tables client ont été mappées et les niveaux d'audience ont été définis.

Obtention des informations

Jacques détermine que la table Territoire contient les zones dont il a besoin pour spécifier les contraintes de zone dans les filtres de données.

La table suivante contient les informations que Jacques obtient sur les zones du client et leurs mappages de Unica Campaign.

Tableau 68. Zones table Territoire

Zones (nom physique)	Zones (nom dans Unica Campaign)	Data	Type de données
cust_region	CustomerRegion	• Afrique • Asie • Europe • Moyen-Orient • Amérique du Nord	java.lang.String
hh_id	HouseholdID	S/O	java.lang.Long
indiv_id	IndividualID	S/O	java.lang.Long

Jacques apprend que les noms d'audience utilisés dans Unica Campaign sont foyer et individu. Il remarque que la table Territoire contient deux zones assistance. La zone hh_id correspond à l'audience du foyer. La zone indiv_id de la table Territoire correspond à l'audience de l'individu.

Etant donné que Jacques doit créer une zone logique pour chaque audience et une autre pour la contrainte de zone, il sait qu'il a besoin d'un total de trois zones d'analyse.

Jacques sait également qu'il a besoin de regrouper les filtres de données dans une configuration de données. Il décide de nommer sa configuration de données Territoire.

Jacques est prêt à créer le fichier XML.

Création du fichier XML

Voici le fichier XML que Jacques a créé. Les valeurs basées sur les informations qu'il a obtenues sont indiquées en **gras** .

```
<ExecuteBatch>
                <!-- ********************************* -->
                <!--          Data configuration       -->
                <!-- ********************************* -->
  <name>SeedData</name>
  <operations>
      <ExecuteBatch>
        <name>DataFilters</name>
        <operations>
          <AddDataConfiguration>
            <dataConfiguration>
                <id>1</id>
                <name>Territory</name>
            </dataConfiguration>
           </AddDataConfiguration>
         </operations>
       </ExecuteBatch>
                <!-- ********************************* -->
```

```
            <!--         Logical fields             -->
            <!-- ********************************** -->
    <AddLogicalFields>
      <logicalFields>
          <LogicalField>
              <id>1</id>
              <name>CustomerRegion</name>
              <type>java.lang.String</type>
          </LogicalField>
          <LogicalField>
              <id>2</id>
              <name>HouseholdID</name>
              <type>java.lang.Long</type>
          </LogicalField>
          <LogicalField>
              <id>3</id>
              <name>IndividualID</name>
              <type>java.lang.Long</type>
          </LogicalField>
          </logicalFields>
     </AddLogicalFields>
            <!-- ********************************** -->
            <!--    Territory field constraints     -->
            <!-- ********************************** -->
    <AddDataFilters>
      <dataFilters>
        <DataFilter>
          <configId>1</configId>
          <id>1</id>
          <fieldConstraints>
            <FieldConstraint>
              <logicalFieldId>1</logicalFieldId>
```

```
            <expression>Africa</expression>
          </FieldConstraint>
        </fieldConstraints>
      </DataFilter>
      <DataFilter>
        <configId>1</configId>
        <id>2</id>
        <fieldConstraints>
          <FieldConstraint>
            <logicalFieldId>1</logicalFieldId>
            <expression>Asia</expression>
          </FieldConstraint>
        </fieldConstraints>
      </DataFilter>
      <DataFilter>
        <configId>1</configId>
        <id>3</id>
        <fieldConstraints>
          <FieldConstraint>
            <logicalFieldId>1</logicalFieldId>
            <expression>Europe</expression>
          </FieldConstraint>
        </fieldConstraints>
      </DataFilter>
      <DataFilter>
        <configId>1</configId>
        <id>4</id>
        <fieldConstraints>
          <FieldConstraint>
            <logicalFieldId>1</logicalFieldId>
            <expression>Middle East</expression>
          </FieldConstraint>
```

```
            </fieldConstraints>
          </DataFilter>
          <DataFilter>
            <configId>1</configId>
            <id>5</id>
            <fieldConstraints>
              <FieldConstraint>
                <logicalFieldId>1</logicalFieldId>
                <expression>North America</expression>
              </FieldConstraint>
            </fieldConstraints>
          </DataFilter>
        </dataFilters>
      </AddDataFilters>
                <!-- ********************************* -->
                <!--   Map physical to logical fields   -->
                <!-- ********************************* -->
      <ExecuteBatch>
        <name>addTables</name>
        <operations>
          <AddDataTable>
            <dataTable>
            <id>1</id>
            <name>Territory</name>
            <fields>
              <TableField>
                <name>cust_region</name>
                <logicalFieldId>1</logicalFieldId>
              </TableField>
              <TableField>
                <name>hh_id</name>
                <logicalFieldId>2</logicalFieldId>
```

```
              </TableField>
              <TableField>
                <name>indiv_id</name>
                <logicalFieldId>3</logicalFieldId>
              </TableField>
            </fields>
            </dataTable>
          </AddDataTable>
        </operations>
      </ExecuteBatch>
                <!--
*********************************************************** -->
                <!--              Audience table associations
   -->
                <!--
*********************************************************** -->
       <ExecuteBatch>
              <name>addAudiences</name>
              <operations>
              <AddAudience>
                <audience>
                <id>1</id>
                <name>household</name>
                <fields>
                  <AudienceField>
                    <logicalFieldId>2</logicalFieldId>
                    <fieldOrder>0</fieldOrder>
                  </AudienceField>
                </fields>
              </audience>
            </AddAudience>
            <AddAudience>
```

```
               <audience>
               <id>2</id>
               <name>individual</name>
               <fields>
                 <AudienceField>
                   <logicalFieldId>3</logicalFieldId>
                   <fieldOrder>0</fieldOrder>
                 </AudienceField>
               </fields>
               </audience>
             </AddAudience>
             </operations>
      </ExecuteBatch>
               <!--
************************************************** -->
               <!--            Associate table-audience pairs
 -->
               <!--               with data configuration
 -->
               <!--
************************************************** -->
      <ExecuteBatch>
            <name>addAudienceTableAssociations</name>
            <operations>
            <AddAudienceTableAssociation>
                <audienceTableAssociation>
                  <audienceId>1</audienceId>
                  <tableId>1</tableId>
                  <configId>1</configId>
              </audienceTableAssociation>
            </AddAudienceTableAssociation>
            <AddAudienceTableAssociation>
```

```
                <audienceTableAssociation>
                  <audienceId>2</audienceId>
                  <tableId>1</tableId>
                  <configId>1</configId>
                </audienceTableAssociation>
            </AddAudienceTableAssociation>
            </operations>
       </ExecuteBatch>
    </operations>
</ExecuteBatch>
```

Renseignement des tables système

Jacques a nommé son fichier XML de filtre de données `regionDataFilters.xml` et l'a enregistré dans le répertoire `tools/bin` sous cette installation de Unica Platform. Il ouvre une invite de commande et exécute l'utilitaire datafilteringScriptTool pour remplir les tables système du filtre de données.

Affectation d'utilisateurs et de groupes dans les filtres de données

Enfin, Jacques se connecte à Unica avec un compte qui possède l'accès Admin dans Unica Platform.

Il sait quels groupes ont déjà été configurés dans Unica, avec des utilisateurs affectés par région.

Il accède à la section Filtre de données et constate que les contraintes de zone de ses filtres de données sont disponibles dans la recherche avancée des filtres de données. Il effectue une recherche de filtre de données à l'aide du critère de recherche Afrique. Le filtre de données qu'il a configuré pour la région Afrique s'affiche dans les résultats de recherche.

Jacques lance ensuite une recherche sur le groupe d'utilisateurs Afrique, lequel a été configuré dans Unica de sorte à regrouper tous les spécialiste du marketing opérationnel responsables du marketing client en Afrique. Le groupe Afrique s'affiche dans les résultats de recherche.

Jacques sélectionne ensuite le groupe et le filtre de données dans les résultats de recherche, puis affecte le groupe au filtre de données en cliquant sur le bouton Affecter.

Il poursuit la recherche des filtres de données et des groupes jusqu'à l'obtention de toutes les affectations.

Exemple : Génération automatique d'un ensemble de filtres de données

Jacques doit créer un jeu de filtres de données en fonction des pays, des villes et des Etats.

Dans Unica Campaign, les tables client ont été mappées et les niveaux d'audience ont été définis.

Obtention du pilote JDBC

Jacques sait que la base de données client de sa société est Microsoft™ SQL Server. Il télécharge le pilote Type 4 approprié et le place sur la machine sur laquelle Unica Platform est installé, en prenant note du nom et du chemin du pilote.

- Nom de classe du pilote JDBC - `com.microsoft.sqlserver.jdbc.SQLServerDriver`
- Chemin du pilote JDBC - `C:\tools\Java\MsJdbc\sqljdbc.jar`

Obtention des informations

Jacques obtient le nom, l'hôte et le port de la base de données client, ainsi que les données d'identification dont il a besoin pour s'y connecter.

- Nom de la base de données : Customers
- Nom d'hôte de la base de données : companyHost
- Port de la base de données : 1433
- Nom d'utilisateur : sa
- Mot de passe : myPassword

Jacques recherche les données dans la base de données client de sa société et constate qu'il existe des clients dans chaque pays, ville et Etat pour lesquels il souhaite créer un filtre

de données. Il détermine que la table Géographie contient les zones dont il a besoin pour spécifier les zones fixes et les zones de profil des filtres de données.

La table suivante contient les informations que Jacques obtient sur les zones du client et leurs mappages de Unica Campaign.

Tableau 69. Zones table Géographie

Zones (Nom physique)	Zones (nom dans Unica Campaign)	Data	Type de données
country	Pays	• USA • France • Grande-Bretagne	java.lang.String
ville	Ville	Ensemble limité de villes	java.lang.String
état	Etat	Ensemble limité d'états (ou toute autre dénomination de région propre à chaque pays)	java.lang.String
hh_id	HouseholdID	S/O	java.lang.Long
indiv_id	IndividualID	S/O	java.lang.Long

Jacques apprend que les noms d'audience utilisés dans Unica Campaign sont foyer et individu. Il remarque que la table Géographie contient deux zones assistance.

- La zone `hh_id` correspond à l'audience du foyer.
- La zone `indiv_id` de la table Géographie correspond à l'audience de l'individu.

Etant donné que Jacques doit créer une zone logique pour chaque audience et une autre pour chaque zone fixe et de profil, il sait qu'il a besoin d'un total de cinq zones d'analyse.

Jacques sait également qu'il a besoin de regrouper les filtres de données dans une configuration de données. Il décide de nommer sa configuration de données Géographie.

Jacques est prêt à créer le fichier XML.

Création du fichier XML

Voici le fichier XML que Jacques a créé. Les valeurs basées sur les informations qu'il a obtenues ou choisies d'utiliser sont indiquées en **gras**.

```
<ExecuteBatch>
                <!-- ********************************* -->
                <!--          Data configuration       -->
                <!-- ********************************* -->
  <name>SeedData</name>
  <operations>
      <ExecuteBatch>
        <name>DataFilters</name>
        <operations>
            <AddDataConfiguration>
                <dataConfiguration>
                    <id>1</id>
                    <name>Geographic</name>
                </dataConfiguration>
                </AddDataConfiguration>
        </operations>
      </ExecuteBatch>
                <!-- ********************************* -->
                <!--         Logical fields            -->
                <!-- ********************************* -->
      <AddLogicalFields>
        <logicalFields>
            <LogicalField>
                <id>1</id>
                <name>Country</name>
```

```
                <type>java.lang.String</type>
            </LogicalField>
            <LogicalField>
                <id>2</id>
                <name>City</name>
                <type>java.lang.String</type>
            </LogicalField>
            <LogicalField>
                <id>3</id>
                <name>State</name>
                <type>java.lang.String</type>
            </LogicalField>
            <LogicalField>
                <id>4</id>
                <name>HouseholdID</name>
                <type>java.lang.Long</type>
            </LogicalField>
            <LogicalField>
                <id>5</id>
                <name>IndividualID</name>
                <type>java.lang.Long</type>
            </LogicalField>
            </logicalFields>
     </AddLogicalFields>
                <!-- ********************************* -->
                <!--       Generate data filters       -->
                <!-- ********************************* -->
     <GenerateDataFilters>
                <!--
*************************************************** -->
                <!-- Specify the table to be scanned for unique
combinations -->
```

```
               <!-- of values  from which data filters will be defined.
 -->
               <!--
****************************************************** -->
             <tableName>Geographic</tableName>
               <!--
****************************************************** -->
               <!-- Identify the data configuration  with which
 -->
               <!-- generated data filters will be associated.
 -->
               <!--
****************************************************** -->
            <configurationName>Geographic</configurationName>
             <!-- Specify the data source connection information. -->
            <jdbcUrl>
              jdbc:sqlserver://localhost:1433;databaseName=Customers
            </jdbcUrl>
            <jdbcUser>sa</jdbcUser>
            <jdbcPassword>myPassword</jdbcPassword>
            <jdbcDriverClass>

 com.microsoft.sqlserver.jdbc.SQLServerDriver</jdbcDriverClass>
            <jdbcDriverClassPath>
                  <string>C:\tools\Java\MsJdbc\sqljdbc.jar</string>
            </jdbcDriverClassPath>
               <!-- ********************************* -->
               <!--      Specify the fixed fields      -->
               <!-- ********************************* -->
             <fixedFields>
                <FixedField>
                   <expression>USA</expression>
```

```
                <logicalFieldName>Country</logicalFieldName>
                <physicalFieldName>country</physicalFieldName>
            </FixedField>
            <FixedField>
                <expression>France</expression>
                <logicalFieldName>Country</logicalFieldName>
                <physicalFieldName>country</physicalFieldName>
            </FixedField>
            <FixedField>
                <expression>Britain</expression>
                <logicalFieldName>Country</logicalFieldName>
                <physicalFieldName>country</physicalFieldName>
            </FixedField>
        </fixedFields>
        <!-- Specify the profile fields. -->
        <profileFields>
            <ProfileField>
                <logicalFieldName>State</logicalFieldName>
                <physicalFieldName>state</physicalFieldName>
            </ProfileField>
            <ProfileField>
                <logicalFieldName>City</logicalFieldName>
                <physicalFieldName>city</physicalFieldName>
            </ProfileField>
        </profileFields>
</GenerateDataFilters>
          <!-- ********************************* -->
          <!--   Map physical to logical fields   -->
          <!-- ********************************* -->
<ExecuteBatch>
        <name>addTables</name>
        <operations>
```

```
            <AddDataTable>
                <dataTable>
                <id>1</id>
                <name>Geographic</name>
                <fields>
                   <TableField>
                          <name>country</name>
                          <logicalFieldId>1</logicalFieldId>
                   </TableField>
                   <TableField>
                          <name>city</name>
                          <logicalFieldId>2</logicalFieldId>
                   </TableField>
                   <TableField>
                          <name>state</name>
                          <logicalFieldId>3</logicalFieldId>
                   </TableField>
                   <TableField>
                          <name>hh_id</name>
                          <logicalFieldId>4</logicalFieldId>
                   </TableField>
                   <TableField>
                          <name>indiv_id</name>
                          <logicalFieldId>5</logicalFieldId>
                   </TableField>
                </fields>
                </dataTable>
                </AddDataTable>
            </operations>
      </ExecuteBatch>
               <!--
************************************************************ -->
```

```
               <!--              Audience table associations
   -->
               <!--
********************************************************** -->
      <ExecuteBatch>
             <name>addAudiences</name>
             <operations>
             <AddAudience>
                 <audience>
                 <id>1</id>
                 <name>household</name>
                 <fields>
                    <AudienceField>
                       <logicalFieldId>4</logicalFieldId>
                       <fieldOrder>0</fieldOrder>
                    </AudienceField>
                 </fields>
                 </audience>
             </AddAudience>
             <AddAudience>
                 <audience>
                 <id>2</id>
                 <name>individual</name>
                 <fields>
                    <AudienceField>
                      <logicalFieldId>5</logicalFieldId>
                      <fieldOrder>0</fieldOrder>
                    </AudienceField>
                 </fields>
                 </audience>
             </AddAudience>
             </operations>
```

```
      </ExecuteBatch>
               <!--
*******************************************************  -->
               <!--            Associate table-audience pairs
 -->
               <!--               with data configuration
 -->
               <!--
*******************************************************  -->
      <ExecuteBatch>
             <name>addAudienceTableAssociations</name>
             <operations>
             <AddAudienceTableAssociation>
                <audienceTableAssociation>
                    <audienceId>1</audienceId>
                    <tableId>1</tableId>
                    <configId>1</configId>
                </audienceTableAssociation>
             </AddAudienceTableAssociation>
             <AddAudienceTableAssociation>
                <audienceTableAssociation>
                    <audienceId>2</audienceId>
                    <tableId>1</tableId>
                    <configId>1</configId>
                </audienceTableAssociation>
             </AddAudienceTableAssociation>
             </operations>
      </ExecuteBatch>
   </operations>
</ExecuteBatch>
```

Renseignement des tables système

Jacques a nommé son fichier XML de filtre de données `geographicDataFilters.xml` et l'a enregistré dans le répertoire `tools/bin` sous cette installation de Unica Platform. Il ouvre une invite de commande et exécute l'utilitaire `datafilteringScriptTool` pour remplir les tables système du filtre de données.

L'utilitaire crée un grand nombre de filtres de données. Dans chaque filtre de données, les critères se composent d'un pays (zone fixe) et d'une combinaison unique de villes et d'Etats obtenue lorsque l'utilitaire effectue une recherche dans les enregistrements qui contiennent la valeur fixe. Toutes les combinaisons uniques de ville et d'Etat sont utilisées pour chaque pays spécifié comme zone fixe.

Affectation d'utilisateurs et de groupes dans les filtres de données

Enfin, Jacques se connecte à Unica Platform avec un compte ayant un accès Admin dans Unica Platform.

Il sait quels groupes ont déjà été configurés dans Unica Platform, avec des utilisateurs affectés par ville.

Il accède à la section Filtre de données et constate que les valeurs des pays, villes et Etats de ses filtres de données sont disponibles dans la recherche avancée des filtres de données. Il effectue une recherche de filtre de données à l'aide du critère de recherche Lille, ville de France. Le filtre de données Lille s'affiche dans les résultats de recherche.

Ensuite, Jacques recherche le groupe d'utilisateurs Lille défini dans Unica Platform pour contenir tous les spécialistes du marketing opérationnel responsables du marketing des clients à Lille. Le groupe Lille s'affiche dans les résultats de recherche.

Jacques sélectionne ensuite le groupe et le filtre de données dans les résultats de recherche, puis affecte le groupe au filtre de données en cliquant sur le bouton Affecter.

Il poursuit la recherche des filtres de données et des groupes jusqu'à l'obtention de toutes les affectations.

A propos de l'affectation des utilisateurs et des groupes dans le code XML

L'affectation d'utilisateurs ou de groupes aux filtres de données dans le XML constitue une alternative au filtrage dans l'interface utilisateur. Cette méthode n'est possible qu'en cas de spécification manuelle des filtres à créer.

Vous pouvez utiliser une chaîne générique, `#user_login#`, qui crée automatiquement des filtres de données à partir du nom de connexion de l'utilisateur de Unica Platform.

Vous utilisez le bloc d'élément XML `AddAssignments` pour associer des utilisateurs ou des groupes à vos filtres de données.

Scénario utilisé dans l'exemple

L'exemple utilise le scénario suivant.

Une organisation utilise Unica Collaborate et souhaite créer des filtres de données qui permettent aux spécialistes du marketing opérationnel de n'afficher que les clients de la région à laquelle ils sont affectés. Par conséquent, chaque utilisateur requiert son propre filtre de données.

La liste s'affiche dans Unica Collaborate et les modèles de formulaire sont configurés en fonction de la région. Cette configuration est décrite plus en détails dans le manuel Unica Collaborate - Guide d'administration.

Le niveau d'audience est Client.

Les filtres de données sont créés en fonction de quatre tables de la base de données `exampleSchema`, décrites dans le tableau suivant.

Tableau 70. Tables et zones utilisées dans les exemples

Tableau	Zones
`exampleSchema.Corporate_Lists`	`UserID`, `State` et `RegionID`. Table d'affichage des listes configurée dans Unica Collaborate. La colonne UserID contient les noms de connexion Unica Platform des

Tableau 70. Tables et zones utilisées dans les exemples (suite)

Tableau	Zones
	spécialistes marketing. Cet table associe les noms de connexion Unica Platform à la région affectée.
`exampleSchema.customer_contact`	Zones `Indiv_ID`, `Region_ID` et `State` pour les clients
`exampleSchema.lkup_state`	Table de recherche pour la zone `state_name`
`exampleSchema.lkup_region`	Table de recherche pour la zone `region_id`

Exemple : Utilisation de la chaîne générique pour affecter les membres d'un groupe aux filtres de données

Pour créer un filtre de données distinct pour chaque membre d'un groupe donné, procédez de la manière suivante.

- Créez des zones logiques comme d'habitude.
- Créez un filtre de données unique avec la chaîne générique `#user_login#` dans l'élément `expression`.
- Sous l'élément `AssignmentByName`, définissez `principalType` sur `2`, définissez l'élément `principalName` sur le nom du groupe, et définissez l'élément `dataObjectId` sur l'ID du filtre de données utilisant la chaîne générique.
- Créez des associations d'audience comme d'habitude.

Le code XML suivant illustre cette méthode pour le scénario décrit ci-dessus.

```
<ExecuteBatch>
                <!-- ********************************* -->
                <!--          Data configuration       -->
                <!-- ********************************* -->
    <name>SeedData</name>
    <operations>
```

```
        <ExecuteBatch>
            <name>DataFiltering</name>
            <operations>
                <AddDataConfiguration>
                    <dataConfiguration>
                        <id>1</id>
                        <name>collaborate</name>
                    </dataConfiguration>
                </AddDataConfiguration>
            </operations>
        </ExecuteBatch>
                <!-- ******************************** -->
                <!--         Logical fields           -->
                <!-- ******************************** -->
        <AddLogicalFields>
            <logicalFields>
                <LogicalField>
                    <id>1</id>
                    <name>Customer_ID</name>
                    <type>java.lang.String</type>
                </LogicalField>

                <LogicalField>
                    <id>2</id>
                    <name>AudienceLevel</name>
                    <type>java.lang.String</type>
                </LogicalField>

                <LogicalField>
                    <id>3</id>
                    <name>UserID</name>
                    <type>java.lang.String</type>
```

```
            </LogicalField>

            <LogicalField>
                <id>4</id>
                <name>State_code</name>
                <type>java.lang.String</type>
            </LogicalField>

            <LogicalField>
                <id>5</id>
                <name>Region</name>
                <type>java.lang.Long</type>
            </LogicalField>
        </logicalFields>
    </AddLogicalFields>
            <!-- ********************************* -->
            <!--       Wild card data filter       -->
            <!-- ********************************* -->
    <AddDataFilters>
        <dataFilters>
            <DataFilter><
                <configId>1</configId>
                <id>1</id>
                <fieldConstraints>
                    <FieldConstraint>
                        <logicalFieldId>3</logicalFieldId>
                        <expression>#user_login#</expression>
                    </FieldConstraint>
                </fieldConstraints>
            </DataFilter>
        </dataFilters>
    </AddDataFilters>
```

```
               <!--
*********************************************************** -->
               <!--                       Add data tables
   -->
               <!--
*********************************************************** -->


       <ExecuteBatch>
           <name>addTables</name>
           <operations>
               <!--
*********************************************************** -->
               <!--           Table exampleSchema.Corporate_Lists
   -->
               <!--
*********************************************************** -->
                <AddDataTable>
                   <dataTable>
                       <id>1</id>
                       <name>exampleSchema.Corporate_Lists</name>
                       <fields>
                           <TableField>
                               <tableId>1</tableId>
                               <name>UserID</name>
                               <logicalFieldId>3</logicalFieldId>
                           </TableField>
                           <TableField>
                               <tableId>1</tableId>
                               <name>State</name>
                               <logicalFieldId>4</logicalFieldId>
                           </TableField>
                           <TableField>
```

```
                            <tableId>1</tableId>
                            <name>Region_ID</name>
                            <logicalFieldId>5</logicalFieldId>
                        </TableField>
                    </fields>
                </dataTable>
            </AddDataTable>
            <!--
********************************************************** -->
            <!--           Table exampleSchema.customer_contact
   -->
            <!--
********************************************************** -->
            <AddDataTable>
                <dataTable>
                    <id>2</id>
                    <name>exampleSchema.customer_contact</name>
                    <fields>
                        <TableField>
                            <tableId>2</tableId>
                            <name>Indiv_ID</name>
                            <logicalFieldId>1</logicalFieldId>
                        </TableField>
                        <TableField>
                            <tableId>2</tableId>
                            <name>Region_ID</name>
                            <logicalFieldId>5</logicalFieldId>
                        </TableField>
                        <TableField>
                            <tableId>2</tableId>
                            <name>State</name>
                            <logicalFieldId>4</logicalFieldId>
```

```
                        </TableField>
                    </fields>
                </dataTable>
            </AddDataTable>
            <!--
****************************************************** -->
            <!--              Table exampleSchema.lkup_state
   -->
            <!--
****************************************************** -->
            <AddDataTable>
                <dataTable>
                    <id>3</id>
                    <name>example.schema.lkup_state</name>
                    <fields>
                        <TableField>
                            <tableId>3</tableId>
                            <name>state_name</name>
                            <logicalFieldId>4</logicalFieldId>
                        </TableField>
                    </fields>
                </dataTable>
            </AddDataTable>
            <!--
****************************************************** -->
            <!--              Table exampleSchema.lkup_region
   -->
            <!--
****************************************************** -->
            <AddDataTable>
                <dataTable>
                    <id>4</id>
```

```
                        <name>exampleSchema.lkup_region</name>
                        <fields>
                            <TableField>
                                <tableId>4</tableId>
                                <name>Region_ID</name>
                                <logicalFieldId>5</logicalFieldId>
                            </TableField>
                        </fields>
                    </dataTable>
                </AddDataTable>
            </operations>
        </ExecuteBatch>
                <!--
********************************************************** -->
                <!--              Audience table associations
   -->
                <!--
********************************************************** -->
        <ExecuteBatch>
            <name>addAudiences</name>
            <operations>
                <AddAudience>
                    <audience>
                        <id>1</id>
                        <name>Customer</name>
                        <fields>
                            <AudienceField>
                                <logicalFieldId>2</logicalFieldId>
                                <fieldOrder>0</fieldOrder>
                            </AudienceField>
                        </fields>
                    </audience>
```

```
            </AddAudience>

            <AddAudience>
                <audience>
                    <id>2</id>
                    <name>default</name>
                    <fields>
                        <AudienceField>
                            <logicalFieldId>2</logicalFieldId>
                            <fieldOrder>0</fieldOrder>
                        </AudienceField>
                    </fields>
                </audience>
            </AddAudience>
        </operations>
    </ExecuteBatch>

    <ExecuteBatch>
        <name>addAudienceTableAssociations</name>
        <operations>
            <AddAudienceTableAssociation>
                <audienceTableAssociation>
                    <audienceId>1</audienceId>
                    <tableId>1</tableId>
                    <configId>1</configId>
                </audienceTableAssociation>
            </AddAudienceTableAssociation>

            <AddAudienceTableAssociation>
                <audienceTableAssociation>
                    <audienceId>1</audienceId>
                    <tableId>2</tableId>
```

```
                    <configId>1</configId>
                </audienceTableAssociation>
            </AddAudienceTableAssociation>

            <AddAudienceTableAssociation>
                <audienceTableAssociation>
                    <audienceId>2</audienceId>
                    <tableId>3</tableId>
                    <configId>1</configId>
                </audienceTableAssociation>
            </AddAudienceTableAssociation>

            <AddAudienceTableAssociation>
                <audienceTableAssociation>
                    <audienceId>2</audienceId>
                    <tableId>4</tableId>
                    <configId>1</configId>
                </audienceTableAssociation>
            </AddAudienceTableAssociation>

        </operations>
    </ExecuteBatch>
            <!--
********************************************************** -->
            <!--           Link filters (dataObjectId) to group
   -->
            <!--
********************************************************** -->
    <AddAssignments>
        <assignments>
             <AssignmentByName>
                <namespaceId>1</namespaceId>
```

```
                    <dataObjectId>1</dataObjectId>
                    <principalType>2</principalType>
                    <principalName>FieldMarketer</principalName>
                </AssignmentByName>
            </assignments>
        </AddAssignments>
    </operations>
</ExecuteBatch>
```

A propos de l'affectation des utilisateurs et des groupes dans l'interface utilisateur

Vous pouvez affecter des utilisateurs et des groupes à des filtres de données sur les pages **Paramètres > Filtres de données**.

Pour pouvoir travailler avec des filtres de données dans les pages **Paramètres > Filtres de données**, les éléments suivants doivent être validés.

- Les filtres de données doivent être définis dans les tables système Unica Platform.
- Vous devez vous connecter en tant qu'utilisateur possédant le droit d'accès Unica Platform **Administrer la page Filtres de données**. Le rôle préconfiguré Unica Platform **AdminRole** possède ce droit d'accès.

Recherche avancée

Unica Platform fournit une interface utilisateur pour affecter des utilisateurs et des groupes aux filtres de données. Cette interface utilisateur se base sur une fonctionnalité de recherche avancée qui permet d'obtenir des listes d'utilisateurs, de groupes et de filtres de données. Vous pouvez sélectionner des utilisateurs et des groupes à partir de ces listes, puis les affecter aux filtres de données que vous sélectionnez.

Recherche de filtres de données

La fonctionnalité de recherche des filtres de données fournit des critères de recherche qui sont identiques aux critères spécifiés lors de la configuration des filtres de données. Par exemple, supposons qu'un jeu de filtres de données se base sur une zone qui contient les données suivantes relatives aux secteurs de vente.

- Afrique
- Asie
- Europe
- Moyen-Orient
- Amérique du Nord

La recherche avancée des filtres de données fournit ces données dans une liste déroulante, à partir de laquelle vous pouvez faire votre sélection lors de la recherche de filtres de données.

Recherche d'utilisateurs et de groupes

La fonction de recherche avancée d'utilisateurs et de groupes fournit une zone de texte dans laquelle vous pouvez saisir le texte à rechercher.

Lorsqu'un onglet qui contient la recherche avancée d'utilisateurs et de groupes se charge pour la première fois, les zones de texte Utilisateur et Groupe contiennent un caractère générique (*). Une recherche effectuée à l'aide de ce caractère générique renvoie tous les enregistrements.

Si vous supprimez le caractère générique et que vous n'entrez pas d'autre texte, aucun enregistrement ne sera renvoyé. Par exemple, si vous effectuez une recherche avec la zone de texte Utilisateur blanche et un astérisque dans la zone Groupe, les résultats ne contiendront que des groupes.

Si vous laissez les zones de texte Utilisateur et Groupe en blanc dans l'onglet Afficher les affectations, aucun enregistrement ne sera renvoyé, quels que soient les critères de filtre de données sélectionnés.

Lorsque vous entrez du texte dans la zone, la recherche correspond aux caractères que vous entrez dans la zone de texte, dans leur ordre de saisie. Par exemple, pour obtenir un groupe nommé Amérique du Nord, vous pouvez saisir une lettre ou un groupe de lettres (dans l'ordre) présent dans le nom. Les résultats contiennent Amérique du Nord si vous avez saisi "nord" ou "d" mais ne contiennent pas Amérique du Nord si vous avez saisi "dron".

La recherche n'est pas sensible à la casse. "North" est identique à "north."

Affichage des filtres de données affectés

Utilisez la procédure ci-dessous pour afficher les filtres de données affectés

1. Connectez-vous à Unica comme utilisateur avec le rôle Unica Platform AdminRole et cliquez sur **Filtrage des données**.

   La page Filtres de données s'affiche.
2. Cliquez sur **Afficher les filtres de données affectés**.
3. Exécutez une recherche avancée sur les filtres de données affectés.

Une liste des filtres de données qui répondent à ces critères s'affiche.

Affectation d'utilisateurs et de groupes à des filtres de données

Cette procédure permet d'affecter des utilisateurs et des groupes à des filtres de données.

1. Connectez-vous à Unica comme utilisateur avec le rôle Unica Platform AdminRole et cliquez sur **Paramètres > Filtres de données**.

   La page Filtres de données s'affiche.
2. Cliquez sur **Affecter des utilisateurs ou des groupes**.
3. Exécutez une recherche avancée sur les filtres de données.
4. Effectuez une recherche avancée pour les utilisateurs, les groupes, ou les deux afin d'obtenir une liste d'utilisateurs et de groupes.
5. Dans les listes de résultats des recherches, sélectionnez les filtres de données et les utilisateurs et/ou les groupes que vous souhaitez leur affecter.
6. Cliquez sur **Affecter**.

Les utilisateurs et groupes sélectionnés sont affectés aux filtres de données sélectionnés.

Suppression des affectations de filtres de données

Utilisez la procédure ci-dessous pour supprimer les affectations de filtres de données.

1. Connectez-vous à Unica comme utilisateur avec le rôle Unica Platform AdminRole et cliquez sur **Paramètres > Filtres de données**.

   La page Filtres de données s'affiche.
2. Cliquez sur **Afficher les filtres de données affectés**.
3. Exécutez une recherche avancée sur les filtres de données pour obtenir les filtres que vous souhaitez sélectionner.
4. Dans la liste de résultats de recherche, sélectionnez les filtres de données dont vous souhaitez supprimer les affectations.
5. Cliquez sur **Désaffecter**.

Les affectations sélectionnées sont supprimées. Les filtres de données eux-mêmes ne sont pas supprimés.

Ajout de filtres de données après la création du groupe initial

Vous pouvez continuer à ajouter des filtres de données après avoir créé le jeu initial. Par exemple, vous pouvez créer un jeu de filtres de données basé sur les pays et leurs combinaisons ville/état, puis décider par la suite de créer un autre jeu basé sur les codes postaux.

Vous pouvez procéder de différentes manières pour obtenir un fichier XML pour de nouveaux filtres de données.

- Modifiez le fichier XML d'origine pour y ajouter de nouveaux filtres. Lorsque vous alimentez la base de données à l'aide de l'utilitaire `dataFilteringScriptTool`, Unica Platform crée uniquement les nouveaux filtres de données.
- Créez un fichier XML spécifiant les nouveaux filtres de données. Lorsque vous alimentez la base de données à l'aide de l'utilitaire `dataFilteringScriptTool`, les filtres de données existants ne sont pas supprimés.

Après avoir créé le fichier XML, remplissez les tables des filtres de données et affectez des utilisateurs et des groupes en procédant comme indiqué dans ce guide.

Suivi des événements d'audit dans Unica

Vous pouvez configurer quels événements sont suivis et affecter un niveau de gravité à chaque événement suivi.

Deux types d'événements d'audit sont suivis :

- Les événements liés à la sécurité, comme les modifications d'état de l'utilisateur, l'appartenance à un groupe et les droits d'accès
- Les modifications apportées aux propriétés de configuration d'Unica qui sont gérées sur la page **Paramètres > Configuration**

Les informations d'événement d'audit sont indépendantes du journal système et la configuration que vous effectuez pour le journal système n'affecte pas le suivi des événements d'audit.

Le rapport d'événements d'audit fournit une méthode adaptée pour afficher les événements suivis. Vous pouvez configurer le contenu du rapport, filtrer les informations affichées dans le rapport et exporter les données qu'il contient.

Vous devez disposer du rôle AdminRole ou PlatformAdminRole dans Unica Platform pour configurer le rapport d'événements d'audit et les sauvegardes d'audit ou pour afficher le rapport.

Restrictions sur le suivi des événements d'audit

Si vous configurez le suivi de la propriété de configuration des événements d'audit, ces modifications ne sont suivies que lorsqu'elles sont effectuées via la page **Paramètres > Configuration**.

Par exemple, les changements suivants de la propriété de configuration ne sont pas suivis :

- Changements effectués via l'utilitaire Unica Platform `configTool`
- Changements effectués durant l'installation et la mise à niveau des produits Unica

De même, lorsque vous ajoutez manuellement des utilisateurs, des rôles et des droits d'accès par défaut pour Unica Platform et Unica Campaign à l'aide de l'utilitaire Unica Platform `populateDB`, ces changements ne font pas l'objet d'un suivi.

Evénements d'audit existants

Dans les précédentes versions de Unica Platform, les événements d'audit étaient sauvegardés dans les tables système Unica Platform alors qu'aucun rapport n'était disponible. Si vous effectuez une mise à niveau à partir d'une version antérieure à 9.1.1, le rapport d'événements d'audit inclut ces événements existants.

Les événements d'audit existants sont affichés dans le rapport comme décrit ci-après.

- La colonne **Severity** (Gravité) contient **No severity (Legacy)** (Pas de gravité (existant)) pour indiquer que ces enregistrements d'audit ont été stockés avant que le rapport d'audit ne soit disponible.
- Dans un environnement ayant une seule partition, la colonne **Partition** contient l'ID de la partition par défaut.
- Dans un environnement à plusieurs partitions, la colonne **Partition** contient **-1 (Legacy)** pour indiquer qu'il n'est pas possible de déterminer la partition à laquelle l'événement appartient.

Les événements existants suivants peuvent apparaître après la mise à niveau :

- User authentication succeeded (L'authentification de l'utilisateur a abouti).
- User authentication failed (L'authentification de l'utilisateur a échoué).
- Authentication failed because a user attempted to log in with too many concurrent sessions (L'authentification a échoué car un utilisateur a tenté de se connecter avec un trop grand nombre de sessions simultanées).
- User logged off and the corresponding session ended (Utilisateur déconnecté et session correspondante terminée).
- User's password changed (Le mot de passe utilisateur a changé).

Les événements d'audit existants ne sont visibles dans les rapports que lorsque vous accédez au rapport avec un compte ayant le rôle PlatformAdminRole dans Unica Platform. L'utilisateur platform_admin prédéfini possède ce rôle.

Modifications rétroactives

En cas de modification du prénom, du nom ou de l'adresse e-mail d'un compte utilisateur, tous les événements d'audit suivis de cet utilisateur reflètent ces modifications. Cela est vrai même pour les événements suivis avant que les modifications du profil de l'utilisateur ne soient effectuées.

Droits d'affichage du rapport des événements d'audit dans un environnement à plusieurs partitions

Dans un environnement à plusieurs partitions, l'appartenance à une partition de l'administrateur visualisant le rapport des événements d'audit détermine les événements qui sont inclus lors de la visualisation du rapport par l'administrateur.

Pour tous les événements d'audit, à l'exception des événements de configuration, le rapport affiche uniquement ceux qui ont eu lieu dans la partition de l'administrateur qui visualise le rapport. Les événements qui ont eu lieu dans les autres partitions ne sont pas affichés dans le rapport.

Il y a une exception à cette règle : les administrateurs ayant le rôle PlatformAdminRole, qui peuvent visualiser les événements se produisant dans toutes les partitions.

Tous les événements de configuration sont visibles pour tous les administrateurs pouvant afficher le rapport.

Activation et désactivation de l'audit des événements

Par défaut, l'audit des événements est désactivé. Pour activer l'audit des événements, vous devez paramétrer la propriété de configuration **Unica Platform | Evénements d'audit | L'audit d'événements est-il activé ?** sur True.

Cette propriété de configuration affecte uniquement les événements d'audit répertoriés sous **Unica Platform | Evénements d'audit** de la page Configuration. Les événements suivis dans le journal système ne sont pas affectés.

Vous pouvez désactiver l'audit des événements à tout moment en paramétrant la propriété de configuration **L'audit des événements est-il activé** sur False.

Le rapport d'événements d'audit n'inclut pas les événements contrôlés par la propriété **L'audit des événements est-il activé** qui se sont produits à un moment où la propriété était définie sur **False**.

Configuration des événements d'audit qui apparaissent dans le rapport

Pour définir les événements d'audit qui sont disponibles dans le rapport d'audit et leur niveau de gravité, vous devez définir les propriétés correspondantes dans la page **Paramètres > Configuration**.

1. Accédez à la page **Paramètres > Configuration** et développez la catégorie **Unica Platform | Evénements d'audit | Configuration des événements d'audit** .
2. Sélectionnez les événements à suivre.

   Les événements suivis peuvent être inclus dans le rapport d'audit.
3. Développez la catégorie **Unica Platform | Evénements d'audit | Configuration de la gravité des événements d'audit** et cliquez sur **Modifier les paramètres**.
4. Indiquez le niveau de gravité à affecter à chacun des événements suivis.

   Sélectionnez l'une des options suivantes :

- No severity (Sans gravité)
- Messages d'information
- Avertissement
- Critique

La gravité spécifiée apparaît dans le rapport d'audit et peut être utilisée pour le filtrage du rapport.

Si vous souhaitez effectuer le suivi de l'événement de session utilisateur **Record login and logout events for members of the HighSeverityAccounts group**, ajoutez les utilisateurs pour lesquels vous souhaitez suivre les événements de connexion et de déconnexion au groupe **highSeverityAccounts**. Pour cela, utilisez la page **Paramètres > Groupes d'utilisateurs**.

Ce groupe est automatiquement créé dans la partition par défaut lors de l'installation. Dans un environnement multipartition, ce groupe est créé automatiquement lorsque vous créez une partition avec l'utilitaire Unica Platform `partitionTool`.

Modification du contenu et de l'affichage des rapports d'audit

Vous pouvez ajouter et supprimer des événements et des colonnes, réorganiser et trier les colonnes, définir l'intervalle de temps, définir les événements suivis à afficher dans le rapport et filtrer les informations.

Lorsque vous ouvrez le rapport d'audit sans avoir défini de paramètres de rapport, les paramètres par défaut suivants sont utilisés.

- Tous les événements sélectionnés dans la page **Paramètres > Configuration** sous la catégorie **Unica Platform | Evénements d'audit | Configuration des événements d'audit** sont affichés (sur plusieurs pages si nécessaire).
- Aucun critère de date n'est appliqué.
- Les événements sont triés comme suit : Date/Heure d'événement (ordre décroissant), Nom de connexion (ordre croissant), Niveau de gravité (ordre croissant)

Procédez comme suit pour modifier ces paramètres :

1. Accédez à **Analyse > Platform**.
2. Pour modifier le contenu du rapport, procédez comme suit :

    a. Cliquez sur **Paramètres du rapport**.

    La fenêtre Paramètres du rapport s'ouvre.

    b. Renseignez les zones.

    Pour définir l'ordre de tri dans le rapport, vous pouvez sélectionner l'un des ordres de tri prédéfinis dans cette fenêtre. Vous pouvez aussi cliquer sur les en-têtes de colonne du rapport pour effectuer le tri en fonction de ces colonnes.

    c. Cliquez sur **Suivant** pour accéder à une page permettant de sélectionner les événements à afficher dans le rapport.

    d. Cliquez sur **Enregistrer et Fermer** pour appliquer vos sélections aux rapports.
3. Pour filtrer le rapport, entrez le texte ou les chiffres dans la zone **Filtre** et cliquez sur le bouton **Filtrer**.

    Le rapport affiche alors uniquement les événements qui contiennent les caractères de filtre dans les colonnes affichées dans le rapport.

    Pour effacer le filtre, cliquez sur la croix **X** dans la zone Filtre.

Zones de la fenêtre Paramètres du rapport

Les zones de la page Paramètres du rapport permettent de configurer le mode d'affichage du rapport d'audit.

Tableau 71. Zones de la fenêtre Paramètres du rapport

Zone	Description
Trier	Sélectionnez un ordre de tri dans le menu déroulant. Diverses combinaisons de tri de colonne sont listées, ainsi que le sens du tri (ordre croissant ou décroissant). Vous pouvez également trier les colonnes à l'aide des contrôles situés dans la page du rapport.

Tableau 71. Zones de la fenêtre Paramètres du rapport (suite)

Zone	Description
Plage de temps	Sélectionnez l'une des plages de temps prédéfinies dans la liste déroulante ou entrez les dates de début et de fin pour une plage personnalisée.
Evénements	Sélectionnez les événements facultatif que vous souhaitez inclure dans le rapport. Pour qu'un événement soit disponible dans le rapport, il doit être sélectionné dans la catégorie **Unica Platform | Evénements d'audit | Configuration des événements d'audit** de la page **Paramètres > Configuration**.
Colonnes	Les boutons **Ajouter** et **Supprimer** permettent de spécifier les colonnes facultatives devant apparaître dans le rapport.

Zones et boutons du rapport d'événements d'audit

Les zones du rapport d'événements d'audit fournit des détails sur le système et les événements utilisateur dans Unica.

Tableau 72. Zones et boutons du rapport d'événements d'audit

Zone ou bouton	Description
Filtrer	Pour filtrer le rapport, entrez du texte ou des chiffres dans la zone Filtre et cliquez sur le bouton. Le rapport affiche alors uniquement les événements qui contiennent les caractères de filtre dans les colonnes affichées dans le rapport.
 Paramètres du rapport	Cliquez ici pour ouvrir une fenêtre dans laquelle vous pouvez changer les colonnes affichées dans le rapport, définir un intervalle de temps et sélectionner un des ordres de tri prédéfinis.
	Cliquez ici pour ouvrir une fenêtre à partir de laquelle vous pouvez exporter le rapport au format CSV ou texte.

Tableau 72. Zones et boutons du rapport d'événements d'audit (suite)

Zone ou bouton	Description
Exporter	
 Actualiser	Cliquez ici pour actualiser les données du rapport.
Zones par défaut	
Date/Heure de l'événement (abrégée)	Date et heure de l'événement sur le serveur sur lequel Unica Platform est déployé.
Nom de l'événement	Evénement faisant l'objet du suivi. Les événements qui font l'objet d'un suivi sont spécifiés dans la page **Paramètres > Configuration**.
Détails de l'événement	Détails sur l'événement suivi. Lorsqu'un lien est présent, vous pouvez cliquer dessus pour voir la totalité des détails.
Nom de connexion	Nom de connexion de l'utilisateur qui a effectué l'action.
Nom, prénom	Nom et prénom de l'utilisateur qui a effectué l'action.
Gravité	Degré de gravité affecté à l'événement dans la page **Unica Platform | Evénements d'audit | Configuration de la gravité des événements d'audit**.
Zones facultatives de la fenêtre Paramètres du rapport	
Navigateur	Navigateur utilisé par la personne qui a effectué l'action.
Nom d'hôte	Nom ou adresse IP de la machine à partir de laquelle l'action a été effectuée.
Demande de	Identificateur URI à partir duquel la demande HTTP a été émise.

Tableau 72. Zones et boutons du rapport d'événements d'audit (suite)

Zone ou bouton	Description
Date/Heure de l'événement (longue)	Date et heure de l'événement sur le serveur sur lequel Unica Platform est déployé (en incluant le fuseau horaire).
Adresse e-mail de l'utilisateur	Adresse e-mail de l'utilisateur qui a effectué l'action.
Partition	Partition dont est membre l'utilisateur qui a effectué l'action.

Evénements d'audit archivés

Vous pouvez configurer la sauvegarde des événements d'audit en définissant la valeur des propriétés de configuration dans la catégorie **Unica Platform | Evénements d'audit | Configuration des événements d'audit** de la page **Paramètres > Configuration**.

Les données archivées sont stockées dans la table `USM_AUDIT_BACKUP` et peuvent être incluses dans le rapport d'événements d'audit (Audit Events) lorsque vous définissez une plage de dates personnalisée incluant des données provenant de l'archive. Le chargement d'un rapport contenant des données archivées peut prendre plus de temps que celui d'un rapport n'en contenant pas.

Le système envoie une notification lorsqu'un processus de sauvegarde d'audit est terminé. Vous pouvez également configurer un groupe d'utilisateurs afin qu'il reçoive ces notifications par e-mail.

Définissez les propriétés suivantes pour configurer la sauvegarde des événements d'audit.

- **Activer la sauvegarde d'audit**
- **Archiver les données après le nombre de jours défini ici**
- **Conserver les enregistrements d'audit principalement pour le nombre de jours défini ici**
- **Archive start time (Archiver l'heure de début)**
- **Nom de groupe pour recevoir les notifications de sauvegarde d'audit**

Configuration de notifications de sauvegarde d'audit

Pour informer des utilisateurs du statut de la sauvegarde d'événements d'audit, faites-en des membres d'un groupe que vous spécifiez ensuite dans une propriété de configuration.

1. Déterminez le groupe dont les membres devront recevoir les notifications par e-mail des sauvegardes de données d'audit.

   Vous pouvez utiliser un groupe existant ou en créer un nouveau dans la page **Paramètres > Groupes d'utilisateurs**.

   Vous ne pouvez spécifier qu'un seul groupe devant recevoir les notifications.
2. Accédez à la page **Paramètres > Configuration** et développez la catégorie **Unica Platform | Evénements d'audit | Configuration des événements d'audit**.
3. Définissez la valeur de la propriété **Name of group to receive audit backup notifications** (Nom du groupe devant recevoir les notifications de sauvegarde d'audit) sur le nom du groupe sélectionné.
4. Ajoutez au groupe les utilisateurs devant recevoir les notifications.
5. Les utilisateurs que vous avez ajoutés au groupe doivent s'abonner aux notifications dans la page **Paramètres > Utilisateurs**.

   Un administrateur peut faire cela pour chaque utilisateur ; vous pouvez aussi informer les utilisateurs qu'ils doivent accéder à leur compte, cliquer sur **Abonnements aux notifications** et s'abonner au notifications **Audit backup** (Sauvegarde d'audit).

Chaque fois que le système sauvegarde des données d'audit, une notification par e-mail et une notification par interface utilisateur sont générées pour les membres du groupe spécifié s'ils se sont abonnés aux notifications Audit Event (Evénement d'audit).

Exportation du rapport des événements d'audit

Vous pouvez exporter le rapport d'audit de sécurité dans un fichier texte ou CSV.

1. Accédez à **Analyse > Marketing Platform**.
2. Cliquez sur le bouton **Exporter**.
3. Dans la fenêtre d'exportation des rapports d'audit, entrez un nom pour le rapport exporté et sélectionnez le format d'exportation.

Les formats possibles sont :

- **CSV** (liste séparée par des virgules pouvant être ouverte par Microsoft™ Excel)
- **TXT** (texte)

  Si vous sélectionnez le format texte, vous devez aussi choisir le séparateur. Les options sont les suivantes :

  - **Nombre de**
  - **|**
  - **TABULATION**

4. Cliquez sur **Exporter**, indiquez si vous souhaitez ouvrir ou enregistrer le rapport exporté, puis fermez la fenêtre du rapport.

Optimisation de l'exportation des rapports d'événements d'audit ayant un gros volume

Si vous souhaitez exporter des rapports d'événements d'audit ayant un gros volume, par exemple, les rapports contenant plus de 65 000 enregistrements correspondant aux critères de filtrage des événements d'audit, l'exportation peut faire l'objet d'un dépassement de délai. Pour contourner ce problème, procédez comme indiqué ci-après.

Cette procédure s'applique lorsque vous utilisez Internet Explorer pour accéder au rapport d'événements d'audit.

1. Editez le registre Windows™ comme indiqué ci-après.

   a. Ouvrez l'éditeur de registre Windows™ et accédez à `HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Internet Settings`.

   b. S'il n'existe pas d'entrée DWORD nommée `ReceiveTimeout`, créez-en une.

      Pour créer une entrée DWORD, procédez comme suit :

      - Cliquez avec le bouton droit de la souris sur `Internet Settings` et sélectionnez **Nouveau >Valeur DWORD (32 bits)**.
      - Indiquez `ReceiveTimeout` comme nom pour la nouvelle entrée.

c. Donnez à l'entrée `ReceiveTimeout` existante ou à la nouvelle entrée la valeur indiquée ci-après.
   - Cliquez avec le bouton droit de la souris sur l'entrée `ReceiveTimeout` et sélectionnez **Modifier**.
   - Sous **Base**, sélectionnez **Décimale**.
   - Indiquez l'intervalle de délai d'attente en millisecondes.

     Par exemple, pour indiquer 3 heures, vous devez entrer 10800000, ce qui représente 180 minutes * 60 secondes * 1 000.

2. Configurez Internet Explorer comme suit :
   a. Sélectionnez **Outils > Options Internet** et cliquez sur l'onglet Sécurité.
   b. Sélectionnez la zone dans laquelle vous accédez à Unica Platform. Par exemple, Sites certifiés.
   c. Cliquez sur **Personnaliser le niveau**.
   d. Sous **Téléchargements**, activez **Demander confirmation pour les téléchargements de fichiers**.
   e. Redémarrez Internet Explorer.

Journal système de Unica Platform

Vous devez d'abord vérifier le journal système si l'application Unica Platform présente un dysfonctionnement. Le journal système est indépendant des informations d'audit de sécurité, qui sont stockées dans les tables système. Le journal système effectue le suivi de certaines des informations contenues dans les rapports d'audit de sécurité, mais il contient aussi des informations utiles pour l'identification des problèmes liés à Unica Platform.

Le journal système contient les informations suivantes.

- Informations de configuration, erreurs et informations de débogage de Unica Platform.
- Enregistrement d'événements clé qui surviennent sur le serveur de Unica Platform (demandes, autorisations, révocations et échecs).

A propos des paramètres de configuration affichés dans le journal système

Remarque : Si un problème se produit lorsque le système tente d'écrire dans le fichier journal du système, le système écrit dans stdout (ligne de commande) plutôt que dans le fichier.

Format d'entrée du journal système

Les entrées du journal système possèdent le format suivant.

```
Horodatage | Niveau de gravité de l'événement | Message
```

- **Timestamp** : période à laquelle s'est produit l'événement.
- **Event Severity Level** : niveau de journalisation de l'événement.
- **Message** : description de l'événement. Si l'entrée est une demande dans le serveur, le message contient généralement la fonction appelée par la demande. Les entrées de réponse enregistrent les résultats des demandes.

Configuration du journal système

Vous configurez le journal système à l'aide du fichier `log4j.properties`, situé par défaut dans le répertoire `conf` de votre installation Unica Platform. Les changements apportés à ce fichier prennent effet 30 secondes après l'enregistrement du fichier.

Note : Vous configurez le journal système à l'aide du fichier `log4j.xml`, situé par défaut dans le répertoire `conf` de votre installation Unica Platform. Les changements apportés à ce fichier prennent effet 30 secondes après l'enregistrement du fichier.

La configuration que vous effectuez sur le journal système n'affecte pas la sécurité des rapports d'audit.

Paramètres par défaut du journal système

Par défaut, le journal système est configuré comme suit :

- Nom du fichier journal : `platform.log`
- Répertoire des journaux : `Unica/Platform/logs`
- Niveau du journal : `WARN`
- Nombre de sauvegardes : 10
- Taille maximale des fichiers journaux : 10MB

Prenez connaissance des informations suivantes.

- Si vous augmentez le nombre de sauvegardes ou la taille des fichiers journaux, vérifiez que la machine sur laquelle les journaux sont enregistrés dispose de suffisamment de mémoire.
- La définition d'un niveau de journalisation supérieur au niveau par défaut peut avoir une incidence sur les performances.

Niveaux de journalisation dans le journal système

Les niveaux de journalisation possibles dans le journal système sont les suivants, dans l'ordre croissant.

- `ERREUR`
- `WARN`
- `INFO`
- `DEBUG`
- `TRACE`

Les niveaux supérieurs contiennent les informations de tous les autres niveaux. Par exemple, la définition du niveau `DEBUG` active les traces `DEBUG`, `INFO`, `WARN` et `ERROR`.

Si le niveau de journalisation est défini sur DEBUG, les messages de réponse contiennent les requêtes SQL effectuées dans le magasin de données de Unica Platform.

Paramètres de niveau de journalisation pour l'ensemble du système Unica Platform

Vous pouvez modifier le niveau de journalisation pour tous les composants de Unica Platform en .décommentant la ligne souhaitée dans la section Exemples du fichier. Pour

décommenter une ligne, supprimez le caractère <userinput>#</userinput> au début de la ligne. Si vous effectuez cette modification, veillez à ajouter le symbole <userinput>#</userinput> au début de la ligne spécifiant le niveau de journalisation précédent.

Note : Vous pouvez changer le niveau de journalisation pour tous les composants de Unica Platform en modifiant le niveau de journalisation dans la balise Root définie sous la balise Loggers.

Définition des niveaux de journalisation pour les composants de Unica Platform

Vous pouvez définir le niveau de journalisation de composants spécifiques de Unica Platform dans le système. Ils comprennent :

- Localisation
- le traitement des utilisateurs et des groupes,
- Migration des données
- l'intégration LDAP,
- l'authentification (traitement côté serveur),
- les pages Configuration,
- Accès à la base de données
- des bibliothèques tierces (par exemple, ibatis).

Par défaut, le niveau de journalisation du composant est désactivé. Pour déboguer un module spécifique, enlevez le caractère # en début chaque ligne du module dans le fichier log4j.properties.

Note : Pour déboguer un module spécifique, supprimez le symbole `<!--` au début de chaque balise <Logger> et `-->` à la fin de chaque balise <Logger> du module dans le fichier log4j.xml.

Informations supplémentaires sur log4j

Vous pouvez trouver des informations supplémentaires sur log4j comme suit.

- Voir les commentaires dans le fichier `log4j.properties`.
- Voir http://logging.apache.org/log4j/docs/documentation.html..
- Voir les commentaires dans le fichier `log4j.xml`.
- Voir https://logging.apache.org/log4j/2.x/manual/configuration.html

Note : Les utilisateurs peuvent désactiver les avertissements de JDBC en définissant la propriété suivante `hibernate.jdbc.log.warnings=false` dans le fichier `platform_home/tools/bin/jdbc.properties`.

Activation de la journalisation pour utilisateur unique

Vous pouvez activer la journalisation pour utilisateur unique en la configurant pour utiliser le fichier XML, puis en éditant celui-ci.

La journalisation est configurée à l'aide de l'un des deux fichiers suivants : log4j.properties ou log4j.xml. Par défaut, le fichier log4j.properties est utilisé.

Vous pouvez activer la journalisation par utilisateur en la configurant pour utiliser le fichier XML, puis en éditant celui-ci. Si Unica Platform est configuré dans un déploiement en cluster, copiez le fichier XML sur chaque nœud.

- Vous pouvez activer la journalisation mono-utilisateur en modifiant le fichier XML.
- La journalisation est configurée à l'aide de `log4j.xml`, qui est le fichier de configuration par défaut.
- Si Unica Platform est configuré dans un déploiement de cluster, copiez le fichier XML sur chaque noeud.

lorsque la journalisation XML est activée, une unité d'exécution, qui vérifie régulièrement si un fichier de configuration XML a été créé ou si le fichier de configuration XML a été modifié, est créée. Si une modification ou une création de fichier est détectée, le fichier XML est lu pour configurer log4j. L'intervalle d'interrogation est de 60 secondes.

1. Configurez la journalisation pour utiliser log4j.xml en définissant le paramètre JVM suivant.

   `-DENABLE_PLATFORM_LOG4J_XML_LOGGING=true`

   La valeur doit être définie sur true pour activer la journalisation par utilisateur.

   Si Unica Platform est configuré dans un déploiement en cluster, définissez ce paramètre JVM dans chaque nœud du cluster.
2. Pour spécifier le compte utilisateur à enregistrer dans la journalisation par utilisateur, modifiez le fichier log4j.xml et ajoutez les utilisateurs dans la balise filter. Les journaux pour les utilisateurs qui sont ajoutés dans la balise de filtre.
   - Vous pouvez ajouter plusieurs balises dans le fichier `log4j.xml` pour créer des fichiers journaux distincts pour des utilisateurs spécifiques. Vous devez ajouter un nouvel appender pour chaque nouveau fichier journal spécifique à un utilisateur.
   - Par défaut, le fichier journal est créé dans le dossier `Platform_Home / Platform/logs` et est nommé `platform.log.` Vous pouvez indiquer un autre chemin valide et un autre nom de fichier. Vous devez indiquer le chemin d'accès absolu ou complet pour générer les fichiers journaux dans les dossiers correspondants.
   - Si des journaux spécifiques à chaque utilisateur et des journaux valides pour tous les utilisateurs sont obligatoires, ajoutez une balise appender avec un nouveau nom et sans balise filter définie. L'appender doit avoir un nom unique.
   - Ajoutez une entrée correspondante sous la balise de racine de ce nouvel appender.
3. Si Unica Platform est configuré dans un déploiement en cluster, copiez le fichier XML modifié sur chaque nœud du cluster.

   Vous pouvez utiliser une commande similaire à l'exemple suivant :

   `-DPLATFORM_LOG4J_XML_FILE=log4j_node1.xml`

   Le fichier `log4j_node1.xml` est une copie du fichier `log4j.xml`. Vous pouvez utiliser le nom de votre choix pour le fichier copié. Le fichier journal est également créé avec ce nouveau nom comme log4j_node1.log automatiquement au lieu du nom par défaut platform.log.

Considérons l'exemple suivant où les journaux sont collectés pour l'utilisateur asm_admin et pour tous les autres utilisateurs.

```
<appender name="Console" class="org.apache.log4j.ConsoleAppender">
<param name="ImmediateFlush" value="true"/> <layout
class="org.apache.log4j.PatternLayout"> <param
name="ConversionPattern" value="%-5p %c - %m%n"/> </layout>
<filter class="com.unica.manager.logger.UserMatchFilter"> <param
name="StringToMatch" value="asm_admin" /> </filter> </appender>
<appender name="Console" class="org.apache.log4j.ConsoleAppender">
<param name="ImmediateFlush" value="true"/> <layout
class="org.apache.log4j.PatternLayout"> <param
name="ConversionPattern" value="%-5p %c - %m%n"/> </layout>
<filter class="com.unica.manager.logger.UserMatchFilter">
<param name="StringToMatch" value="asm_admin" />
</filter> </appender> </appender> <!-- <logger
name="com.unica.manager.configuration.ConfigurationManager">
<level value="TRACE"/> </logger> <logger
name="com.unica.suite.scheduler.server.manager.TaskManager">
<level value="DEBUG"/> </logger> <logger
name="org.hibernate.util.JDBCExceptionReporter"> <level
value="ERROR"/> </logger> --> <root> <level value="WARN"/>
<appender-ref ref="System"/> <appender-ref ref="Console"/>
<appender-ref ref="SystemAllUsers"/> </root>
```

1. Pour spécifier le compte d'utilisateur à enregistrer dans la journalisation par utilisateur, modifiez le fichier `log4j.xml` et décommentez la balise RollingFile avec le nom UserLogAppender. Ajoutez l'identifiant de l'utilisateur dans la balise du filtre. Les journaux pour l'utilisateur qui est ajouté dans la balise de filtre sont enregistrés dans le fichier qui est mentionné dans cet appender. Définissez le paramètre JVM ci-dessous s'il n'est pas déjà défini,

   `-DUNICA_PLATFORM_HOME= <platform_home_directory_path>`

- Vous pouvez ajouter plusieurs balises dans le fichier `log4j.xml` pour créer des fichiers journaux distincts pour des utilisateurs spécifiques. Vous devez ajouter un nouvel appender pour chaque nouveau fichier journal spécifique à un utilisateur.
- Par défaut, le fichier journal est créé dans le dossier `Platform_Home / Platform/logs` et est nommé `platform.log.` Vous pouvez indiquer un autre chemin valide et un autre nom de fichier. Vous devez indiquer le chemin d'accès absolu ou complet pour générer les fichiers journaux dans les dossiers correspondants.
- Si des journaux spécifiques à chaque utilisateur et des journaux valides pour tous les utilisateurs sont obligatoires, ajoutez une balise appender avec un nouveau nom et sans balise filter définie. L'appender doit avoir un nom unique.
- Ajoutez une entrée correspondante sous la balise de racine de ce nouvel appender.

2. Si Unica Platform est configuré dans un déploiement de cluster, copiez le fichier XML édité sur chaque noeud du cluster.

   Vous pouvez utiliser une commande similaire à l'exemple suivant :

   `-DPLATFORM_LOG4J_XML_FILE=log4j_node1.xml`

   Le fichier `log4j_node1.xml` est une copie du fichier `log4j.xml`. Vous pouvez utiliser le nom de votre choix pour le fichier copié. Le fichier journal est également créé avec ce nouveau nom comme log4j_node1.log automatiquement au lieu du nom par défaut platform.log.

Considérons l'exemple suivant où les journaux sont collectés pour l'utilisateur `asm_admin` et pour tous les autres utilisateurs.

```
<?xml version="1.0" encoding="UTF-8"?> <Configuration
 packages="com.unica.manager.logger" monitorInterval="60">
 <Appenders> < !-- Console Log Appender -> <Console name="CONSOLE_LOG"
 target="SYSTEM_OUT" immediateFlush="true"> <PatternLayout pattern="%-5p
 %c - %m%n"> </Console> < !-- System Log Appender --> <!-- La
 section suivante concerne les journaux de tous les utilisateurs-->
```

```
<RollingFile name="SYS_LOG" fileName="${sys:UNICA_PLATFORM_LOG_FILE}"
filePattern="${sys:UNICA_PLATFORM_LOG_FILE}.%d{yyyy-MM-dd}-%i"
immediateFlush="true" append="true" > <PatternLayout pattern="%d{DATE}
- %-5p - %m%n" /> <Policies> <TimeBasedTriggeringPolicy interval="1"
modulate="true"/> <TimeBasedTriggeringPolicySizeBasedTriggeringPolicy
size="10 MB" /> </Policies> <DefaultRolloverStrategy max="10"/>
</RollingFile> < !-- La section suivante concerne les journaux spécifiques
à l'utilisateur asm_admin--> <RollingFile name="UserLogAppender"
fileName="${sys:UNICA_PLATFORM_HOME}/logs/asm_admin.log"
filePattern="${sys:UNICA_PLATFORM_HOME}/logs/asm_admin.log.%d{yyyy-MM-dd}"
immediateFlush="true" append="true" > <PatternLayout
pattern="%d{yyyy-MM-dd HH:mm:ss} [%X{user}] %-5p %F.%M:%L :
%m%n" /> <Politiques> <SizeBasedTriggeringPolicy size="10
MB" /> </Politiques> <Politiques> <...DefaultRolloverStrategy
max="10"/> <UserMatchFilter user="asm_admin" onMatch="ACCEPT"
onMismatch="NEUTRAL"/> </RollingFile> </Appenders> <Loggers> <Root
level="WARN" includeLocation="true"> <AppenderRef ref="SYS_LOG">
<AppenderRef ref="CONSOLE_LOG"> < !-- <AppenderRef ref="UserLogAppender"/>
--> </Root> <!-- <Logger name="com.unicacorp" level="INFO"> -->
<!-- <AppenderRef ref="UserLogAppender"/> --> < !-- </Logger> -->
<!-- <Logger name="com.unica" level="INFO"> --> <!-- <AppenderRef
ref="UserLogAppender"> --> <!-- </Logger> --> </Loggers> </Configuration>
```

Utilitaires Unica Platform

Cette section fournit une présentation des utilitaires Unica Platform, notamment des détails qui s'appliquent à tous les utilitaires et qui ne sont pas inclus dans les descriptions individuelles des utilitaires.

Emplacement des utilitaires

Les utilitaires Unica Platform se trouvent dans le répertoire `tools/bin` sous votre installation de Unica Platform.

Liste et descriptions des utilitaires

Unica Platform fournit les utilitaires suivants.

- Clientdetails *(à la page 347)* - Génère une clé pour une application client telle que Unica Journey pour s'authentifier auprès d'une instance Unica Platform.
- alertConfigTool *(à la page 340)* : enregistre les alertes et les configurations définies pour les produits Unica
- configTool *(à la page 341)* : importe, exporte et supprime les paramètres de configuration, y compris les enregistrements de produits
- datafilteringScriptTool *(à la page 348)* : crée des filtres de données
- encryptPasswords *(à la page 350)* : chiffre et stocke les mots de passe
- encryptTomcatDBPasswords *(à la page 352)* : chiffre les mots de passe de base de données que le serveur d'applications Tomcat utilise en interne
- partitionTool *(à la page 353)* : crée les entrées de base de données pour les partitions
- populateDb *(à la page 356)* : remplit la base de données Unica Platform
- quartzjobtool *(à la page 363)* - Met à jour les travaux du planificateur créés dans la version 11.1 et dans les versions ultérieures
- restoreAccess *(à la page 357)* : restaure un utilisateur avec le rôle platformAdminRole
- scheduler_console_client *(à la page 360)* : répertorie et démarre les travaux du planificateur d'Unica qui sont configurés pour écouter un déclencheur.
- insightsdbutil - Le programme d'installation place les fichiers de conception de rapport qui possèdent des jetons de connexion à la base de données. Vous devez les mettre à jour pour la base de données de votre système. Vous devez exécuter l'utilitaire `insightsdbutil.sh/bat` pour la mettre à jour. Pour en savoir plus, consultez le document Unica Insights - Guide d'installation et de configuration.

Conditions requises pour l'exécution des utilitaires Unica Platform

Les conditions requises pour l'exécution de tous les utilitaires Unica Platform sont les suivantes.

- Exécutez tous les utilitaires depuis le répertoire où ils se trouvent (par défaut, le répertoire `tools/bin` sous votre installation de Unica Platform).
- Sous UNIX™, la meilleure pratique consiste à exécuter les utilitaires avec le même compte utilisateur que celui exécutant le serveur d'applications sur lequel Unica Platform est déployé. Si vous exécutez un utilitaire avec un autre compte utilisateur, réglez les droits au niveau du fichier `platform.log` pour permettre au compte utilisateur d'y accéder en écriture. Si vous ne réglez pas les droits, l'utilitaire n'est pas en mesure d'écrire dans le fichier journal et vous pourriez rencontrer certains messages d'erreur, bien que l'outil fonctionne toujours correctement.

Authentification des utilitaires

Les utilitaires tels que `configTool` ou les utilitaires d'arrière-plan Unica sont conçus pour être utilisés par des administrateurs système et exigent un accès physique aux serveurs hôtes pour pouvoir être appelés. C'est pourquoi leur authentification a été conçue pour être indépendante du mécanisme d'authentification de l'interface utilisateur. L'accès à ces utilitaires est disponible aux utilisateurs disposant de droits d'administrateur Unica Platform. Il doit être défini en interne dans Unica Platform et authentifié par rapport aux mêmes conditions.

Dépannage des problèmes de connexion

Tous les utilitaires Unica Platform, sauf `encryptPasswords`, interagissent avec les tables système Unica Platform. Pour vous connecter à la base de données des tables système, ces utilitaires utilisent les informations de connexion suivantes qui sont définies par le programme d'installation à l'aide des informations fournies lors de l'installation de Unica Platform. Ces informations sont stockées dans le fichier `jdbc.properties`, situé dans le répertoire `tools/bin` sous votre installation de Unica Platform.

- Nom du pilote JDBC
- URL de connexion JDBC (qui inclut l'hôte, le port et le nom de la base de données)
- Identifiant de connexion à la source de données
- Mot de passe de la source de données (chiffré)

En outre, ces utilitaires se basent sur la variable d'environnement `JAVA_HOME`, définie soit dans le script `setenv` situé dans le répertoire `tools/bin` de votre installation de Unica Platform, soit sur la ligne de commande. Le programme d'installation de Unica Platform doit avoir défini cette variable automatiquement dans le script `setenv`, mais il s'agit également d'une bonne pratique que de vérifier que la variable `JAVA_HOME` est définie si vous rencontrez un problème d'exécution d'un utilitaire. Le kit JDK doit être la version de Sun (et non, par exemple, le kit JDK JRockit disponible avec WebLogic).

Caractères spéciaux

Les caractères désignés comme caractères réservés dans le système d'exploitation doivent être évités. Consultez la documentation de votre système d'exploitation pour obtenir une liste des caractères réservés et comment les éviter.

Options standard des utilitaires Unica Platform

Les options suivantes sont disponibles dans tous les utilitaires Unica Platform.

`-l logLevel`

Définit le niveau des informations de journal affichées dans la console. Les options sont `high` (haut), `medium` (moyen) et `low` (bas). La valeur par défaut est `low`.

`-L`

Définit les paramètres régionaux pour les messages de la console. Les paramètres régionaux par défaut sont en_US. Les valeurs disponibles sont déterminées par les langues dans lesquelles Unica Platform a été traduit. Spécifiez les paramètres régionaux à l'aide de l'identificateur des paramètres régionaux ICU, conformément aux normes ISO 639-1 et ISO 3166.

`-h`

Affiche un message d'utilisation court dans la console.

`-m`

Affiche la page de manuel de cet utilitaire dans la console.

`-v`

Affiche davantage de détails d'exécution dans la console.

Configuration des utilitaires Unica Platform sur des machines supplémentaires

Sur la machine sur laquelle Unica Platform est installé, vous pouvez exécuter les utilitaires Unica Platform sans configuration supplémentaire. Cependant, vous pouvez souhaiter exécuter les utilitaires depuis une autre machine sur le réseau. Cette procédure décrit les étapes requises pour cette opération.

Assurez-vous que la machine sur laquelle vous effectuez cette procédure remplit les conditions suivantes.

- Le pilote JDBC approprié doit être présent sur la machine ou accessible à partir de la machine.
- La machine doit disposer d'un accès réseau aux tables système Unica Platform.
- L'environnement d'exécution Java™ doit être installé sur la machine ou accessible à partir de la machine.

1. Rassembles les informations ci-dessous concernant les tables système Unica Platform.
    - Chemin d'accès complet du ou des fichiers de pilote JDBC sur votre système.
    - Chemin d'accès complet à une installation de l'environnement d'exécution Java™.

      La valeur par défaut du programme d'installation est le chemin d'accès à la version prise en charge de l'environnement d'exécution Java que le programme place dans le répertoire d'installation d'Unica. Vous pouvez accepter ce chemin par défaut ou en indiquer un autre.
    - Type de la base de données
    - Hôte de la base de données
    - Port de la base de données
    - Nom/ID système de la base de données
    - Nom de l'utilisateur de la base de données
    - Mot de passe de la base de données

2. Exécutez le programme d'installation Unica et installez Unica Platform.

   Entrez les informations de connexion à la base de données que vous avez rassemblées pour les tables système Unica Platform. Si vous n'êtes pas familiarisé avec le programme d'installation Unica, reportez-vous au guide d'installation de Unica Campaign ou de Unica Plan.

   Vous n'avez pas besoin de déployer l'application Web Unica Platform si vous installez seulement les utilitaires.

Utilitaires

Cette section décrit les utilitaires Unica Platform et propose des détails, la syntaxe et des exemples d'utilisation.

alertConfigTool

Les types de notifications disponibles sont spécifiques à chacun des produits Unica. L'utilitaire `alertConfigTool` sert à enregistrer les types de notifications lorsque le programme d'installation ne l'a pas fait de manière automatique pendant l'installation ou la mise à niveau.

Syntaxe

`alertConfigTool -i -f` ***`importFile`***

Commandes

`-i -f` *`importFile`*

Importer des alertes et des types de notifications depuis un fichier XML spécifié.

Exemple

- Importer des alertes et des types de notifications depuis un fichier nommé `Platform_alerts_configuration.xml` situé dans le répertoire `tools\bin`, dans le répertoire d'installation de Unica Platform.

  ```
  alertConfigTool -i -f Platform_alerts_configuration.xml
  ```

configTool

Les propriétés et les valeurs de la page **Configuration** sont enregistrées dans les tables du système Unica Platform. Vous pouvez utiliser l'utilitaire `configTool` pour importer et exporter les paramètres de configuration depuis et vers les tables du système.

Quand utiliser configTool

Vous pourriez vouloir utiliser `configTool` pour les raisons suivantes.

- Pour importer les modèles de partition et de source de données fournis avec Unica Campaign, que vous pouvez ensuite modifier et dupliquer à l'aide de la page **Configuration**.
- Pour enregistrer (importer les propriétés de configuration) des produits Unica si le programme d'installation du produit n'est pas en mesure d'ajouter automatiquement les propriétés à la base de données.
- Pour exporter une version XML des paramètres de communication à des fins de sauvegarde ou d'importation vers une autre installation d'Unica.
- Pour supprimer les catégories qui n'ont pas le lien **Supprimer la catégorie**. Pour ce faire, utilisez `configTool` pour exporter votre configuration, puis supprimez manuellement le XML qui crée la catégorie et utilisez `configTool` pour importer le XML modifié.

Important : Cet utilitaire modifie les tables `usm_configuration` et `usm_configuration_values` dans la base de données des tables système Unica Platform, qui contient les propriétés de configuration et leurs valeurs. Pour de meilleurs résultats, créez des copies de sauvegarde de ces tables ou exportez vos configurations existantes à l'aide de `configTool` et sauvegardez le fichier résultant afin de pouvoir restaurer votre configuration en cas d'erreur lors de l'importation à l'aide de `configTool`.

Syntaxe

```
configTool -d -p "elementPath" [-o]
```

```
configTool -i -p "parent ElementPath" -f importFile [-o]

configTool -x -p "elementPath" -f exportFile

configTool -vp -p "elementPath" -f importFile [-d]

configTool -r productName -f registrationFile [-o] configTool -u nomduproduit
```

Commandes

-d -p "*elementPath*" [o]

Supprimez les propriétés de configuration et leurs paramètres, tout en spécifiant un chemin pour leur hiérarchie.

Le chemin d'élément doit utiliser les noms internes des catégories et des propriétés. Vous pouvez les obtenir en allant sur la page **Configuration**, en sélectionnant la catégorie ou la propriété souhaitée, et en regardant le chemin d'accès qui s'affiche entre parenthèses dans le volet de droite. Délimitez un chemin d'accès dans la hiérarchie des propriétés de configuration en utilisant le caractère `|`, et entourez le chemin d'accès de guillemets doubles.

Prenez connaissance des informations suivantes.

- Seules les catégories et propriétés d'une application, et non les applications entières, peuvent être supprimées à l'aide de cette commande. Utilisez la commande `-u` pour désenregistrer une application entière.
- Pour supprimer les catégories qui n'ont pas le lien **Supprimer la catégorie** sur la page de **configuration**, utilisez l'option `-o`.

Lorsque vous utilisez `-d` avec la commande `-vp`, le configTool supprime tous les noeuds enfants dans le chemin que vous spécifiez si ces noeuds ne sont pas inclus dans le fichier XML que vous spécifiez.

-i -p "*parentElementPath*" -f *importFile* [o]

Importez les propriétés de configuration et leurs paramètres depuis un fichier XML spécifié.

Pour effectuer l'importation, spécifiez un chemin vers l'élément parent sous lequel vous souhaitez importer vos catégories. L'utilitaire `configTool` importe les propriétés sous la catégorie que vous spécifiez dans le chemin d'accès.

Vous pouvez ajouter des catégories à tout niveau situé sous le niveau supérieur. Toutefois, vous ne pouvez pas ajouter une catégorie au même niveau que le niveau supérieur.

Le chemin d'élément doit utiliser les noms internes des catégories et des propriétés. Vous pouvez les obtenir en vous rendant sur la page **Configuration**, en sélectionnant la catégorie ou la propriété requise et en consultant le chemin d'accès qui s'affiche entre parenthèses dans le volet de droite. Délimitez un chemin dans la hiérarchie des propriétés de configuration en utilisant le caractère `|` et entourez le chemin de guillemets doubles.

Vous pouvez spécifier un emplacement de fichier d'importation relatif au répertoire `tools/bin` ou vous pouvez spécifier un chemin de répertoire complet. Si vous spécifiez un chemin relatif ou aucun chemin, `configTool` recherche d'abord le fichier relatif au répertoire `tools/bin`.

Par défaut, cette commande n'écrase pas une catégorie existante, mais vous pouvez utiliser l'option `-o` pour forcer l'écrasement.

`-x -p "`*`elementPath`*`" -f` ***`exportFile`***

Exporte les propriétés de configuration et leurs paramètres dans un fichier XML spécifié.

Vous pouvez exporter toutes les propriétés de configuration ou limiter l'exportation à une catégorie spécifique. Pour ce faire, spécifiez un chemin dans la hiérarchie des propriétés de configuration.

Le chemin d'accès de l'élément doit utiliser les noms internes des catégories et des propriétés, que vous pouvez obtenir en allant sur la page **Configuration**, en sélectionnant la catégorie ou la propriété souhaitée et en regardant le chemin d'accès qui s'affiche entre parenthèses dans le volet de droite. Délimitez un chemin dans la hiérarchie des propriétés de configuration en utilisant le caractère `|` et entourez le chemin de guillemets doubles.

Vous pouvez spécifier l'emplacement d'un fichier d'exportation dans le répertoire actuel ou un chemin de répertoire complet. Si la spécification du fichier ne contient pas de séparateur (/ sous UNIX™, / ou \ sous Windows™), `configTool` écrit le fichier dans le répertoire

`tools/bin` de votre installation Unica Platform. Si vous ne fournissez pas l'extension `xml`, `configTool` l'ajoute.

`-vp -p "elementPath" -f importFile [-d]`

Cette commande est principalement utilisée dans les mises à niveau manuelles, pour importer des propriétés de configuration. Si vous avez appliqué un groupe de correctifs qui contient une nouvelle propriété de configuration, puis que vous mettez à niveau, l'importation d'un fichier de configuration dans le cadre d'un processus de mise à niveau manuelle peut remplacer des valeurs qui ont été définies lorsque le groupe de correctifs a été appliqué. La commande `-vp` garantit que l'importation ne remplace pas les valeurs de configuration précédemment définies.

Important : Après avoir utilisé l'utilitaire `configTool` avec l'option -vp, vous devez redémarrer le serveur d'applications Web sur lequel Unica Platform est déployé pour que les modifications soient appliquées.

Lorsque vous utilisez `-d` avec la commande `-vp`, le configTool supprime tous les noeuds enfants dans le chemin que vous spécifiez si ces noeuds ne sont pas inclus dans le fichier XML que vous spécifiez.

`-r productName -f registrationFile`

Enregistrez l'application. L'emplacement du fichier d'enregistrement peut être relatif au répertoire `tools/bin` ou peut être un chemin complet. Par défaut, cette commande n'écrase pas une configuration existante, mais vous pouvez utiliser l'option `-o` pour forcer l'écrasement. Le paramètre *`productName`* doit être l'un des noms énumérés ci-dessus.

Prenez connaissance des informations suivantes.

- Lorsque vous utilisez la commande `-r`, le fichier d'enregistrement doit avoir `<application>` comme première balise dans le XML.

  D'autres fichiers peuvent être fournis avec votre produit, que vous pouvez utiliser pour insérer des propriétés de configuration dans la base de données de Unica Platform. Pour ces fichiers, utilisez la commande `-i`. Seul le fichier ayant la balise `<application>` comme première balise peut être utilisé avec la commande `-r`.

- Le fichier d'enregistrement du site Unica Platform est nommé `Manager_config.xml`, et la première balise est `<Suite>`. Pour enregistrer ce fichier sur une nouvelle installation, utilisez l'utilitaire `populateDb` ou exécutez à nouveau le programme d'installation Unica Platform comme décrit dans le *guide d'installationUnica Platform*.
- Après l'installation initiale, pour réenregistrer des produits autres que le Unica Platform, utilisez `configTool` avec la commande `-r` et `-o` pour écraser les propriétés existantes.

L'utilitaire `configTool` utilise les noms de produits comme paramètres avec les commandes qui enregistrent et désenregistrent les produits. Dans la révision 8.5.0 d'Unica, de nombreux produits ont changé de nom. Cependant, les noms qui sont reconnus par `configTool` n'ont pas changé. Les noms de produits valides à utiliser avec `configTool` sont énumérés ci-dessous, ainsi que les noms actuels des produits.

Table 73. Noms de produits pour l'enregistrement et l'annulation de l'enregistrement de configTool

Nom du produit	Nom utilisé dans configTool
Unica Platform	`Gestionnaire`
Unica Campaign	`Campaign`
Unica Collaborate	`Collaborate`
Unica Deliver	`Envoyer`
Unica Journey	`Journey`
Unica Insights	`UnicaInsights`
Intégration de contenu Unica	`assetPicker`
Offre Unica	`Offre`
Unica Interact	`interact`
Unica Optimize	`Optimisation`

Table 73. Noms de produits pour l'enregistrement et l'annulation de l'enregistrement de configTool (continued)

Nom du produit	Nom utilisé dans configTool
Unica Plan	`Plan`
Opportunity Detect	`Détecter`
IBM SPSS Modeler Advantage Enterprise Marketing Management Edition	`SPSS`
Digital Analytics	`Coremetrics`

`-u` *`productName`*

Désenregistrer une application qui est spécifiée par *`productName`*. Il n'est pas nécessaire d'inclure un chemin vers la catégorie du produit. Le nom du produit est suffisant et il est obligatoire. Ce processus supprime toutes les propriétés et tous les paramètres de configuration du produit.

Options

`-o`

Lorsqu'il est utilisé avec `-i` ou `-r`, il écrase l'enregistrement d'une catégorie ou d'un produit existant (nœud).

Lorsqu'il est utilisé avec `-d`, vous pouvez supprimer une catégorie (nœud) qui n'a pas le lien **Supprimer la catégorie** sur la page de **Configuration**.

Exemples

- Importez les paramètres de configuration d'un fichier nommé `Product_config.xml` dans le répertoire `conf` de l'installation Unica Platform.

  ```
  configTool -i -p "Affinium" -f Product_config.xml
  ```
- Importez l'un des modèles de source de données Unica Campaign fournis dans la partition Unica Campaign par défaut, partition1. L'exemple suppose que vous avez

placé le modèle de source de données Oracle, `OracleTemplate.xml`, dans le répertoire `tools/bin` de l'installation Unica Platform.

```
configTool -i -p "Affinium|Campaign|partitions|partition1|dataSources" -f
OracleTemplate.xml
```

- Exportez tous les paramètres de configuration vers un fichier nommé `myConfig.xml` dans le répertoire `D:\backups`.

```
configTool -x -f D:\backups\myConfig.xml
```

- Exportez une partition existante de Unica Campaign (avec les entrées de la source de données), enregistrez-la dans un fichier nommé `partitionTemplate.xml`, et stockez-la dans le répertoire `tools/bin` par défaut de l'installation Unica Platform.

```
configTool -x -p "Affinium|Campaign|partitions|partition1" -f
partitionTemplate.xml
```

- Enregistrez manuellement une application nommée NomProduit, en utilisant un fichier nommé `app_config.xml` dans le répertoire `tools/bin` par défaut de l'installation Unica Platform, et forcez-la à écraser un enregistrement existant de cette application.

```
configTool -r product Name -f app_config.xml -o
```

- Annulez l'enregistrement d'une application nom_produit.

```
configTool -u productName
```

- Exécutez la commande suivante pour activer la fonction encodeCSV :

```
configTool -vp -p "Affinium|Plan|umoConfiguration" -f Plan_Home\conf
\Plan_encodeProperty_11.1.xml
```

- Enregistrez les paramètres d'Unica Interact en tant que menu de configuration sous `AffiniumWebApps\Campaign\interact\conf\interact_setup_navigation.xml` à l'aide des éléments suivants

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|settingsMenu" -f
"interact_setup_navigation.xml"
```

Clientdetails

Cet utilitaire génère des clés pour l’application client, comme Unica Journey pour s’authentifier auprès d’une instance Platform.

Il enregistre la clé dans la base de données de Platform et l'imprime dans la console. La clé peut ensuite être copiée et collée dans l'application cible.

Syntaxe

```
clientDetails -a appName
```

Commandes

```
-a appName
```

Générez la clé pour l'application spécifiée. Les valeurs possibles pour appName sont Manager (pour Unica Platform) et Journey (pour Unica Journey)

Exemples

Générer la clé pour Unica Journey

```
clientDetails -a Journey
```

datafilteringScriptTool

L'utilitaire `datafilteringScriptTool` lit un fichier XML pour remplir les tables de filtrage des données dans la base de données des tables système Unica Platform.

Selon la manière dont vous écrivez le code XML, vous pouvez utiliser cet utilitaire de deux manières.

- En utilisant un groupe d'éléments XML, vous pouvez générer automatiquement des filtres de base de données en fonction des combinaisons uniques des valeurs de zone (un filtre de données pour chaque combinaison unique).
- En utilisant un groupe d'éléments XML légèrement différent, vous pouvez définir chaque filtre de données que crée l'utilitaire.

Voir le document Unica Platform - Guide d'administration pour plus d'informations.

Quand utiliser datafilteringScriptTool ?

Vous devez utiliser `datafilteringScriptTool` lorsque vous créez des filtres de données.

Prérequis

Unica Platform doit être déployé et actif.

Utilisation de datafilteringScriptTool avec SSL

Lorsque Unica Platform est déployé en utilisant SSL unidirectionnel, vous devez modifier le script datafilteringScriptTool pour ajouter les options SSL d'établissement de liaison. Pour modifier le script, vous devez disposer des informations suivantes.

- Nom et chemin de fichier de clés certifiées
- Mot de passe de fichier de clés certifiées

Dans un éditeur de texte, ouvrez le script datafilteringScriptTool (`.bat` ou `.sh`) et recherchez les lignes semblables aux lignes suivantes (exemples pour Windows™).

```
:callexec

"%JAVA_HOME%\bin\java" -DUNICA_PLATFORM_HOME="%UNICA_PLATFORM_HOME%"

com.unica.management.client.datafiltering.tool.DataFilteringScriptTool %*
```

Editez ces lignes pour qu'elles soient similaires à celles qui apparaissent en **gras**). Remplacez le chemin et le nom de fichier de clés certifiées `myTrustStore.jks` et `myPassword` par les vôtres.

```
:callexec

SET SSL_OPTIONS=-Djavax.net.ssl.keyStoreType="JKS"

-Djavax.net.ssl.trustStore="C:\security\myTrustStore.jks"

-Djavax.net.ssl.trustStorePassword=myPassword

"%JAVA_HOME%\bin\java" -DUNICA_PLATFORM_HOME="%UNICA_PLATFORM_HOME%"
%SSL_OPTIONS%

com.unica.management.client.datafiltering.tool.DataFilteringScriptTool %*
```

Syntaxe

`datafilteringScriptTool -r` *`path`*`file`

Commandes

`-r path_file`

Importer des spécifications de filtre de données depuis un fichier XML défini. Si le fichier ne se trouve pas dans le répertoire `tools/bin` de l'installation, fournissez un chemin et placez le paramètre *`path`*`_file` entre guillemets.

Exemple

- Utilisez le fichier `collaborateDataFilters.xml`, situé dans le répertoire `C:\unica\xml`, pour remplir les tables système des filtres de données.

  ```
  datafilteringScriptTool -r "C:\unica\xml\collaborateDataFilters.xml"
  ```

encryptPasswords

L'utilitaire `encryptPasswords` permet de chiffrer et de stocker l'un ou l'autre des deux mots de passe utilisés en interne par Unica Platform.

Les deux mots de passe que l'utilitaire peut chiffrer sont les suivants.

- Mot de passe utilisé par Unica Platform pour accéder à ses tables système. L'utilitaire remplace un mot de passe chiffré existant (enregistré dans le fichier `jdbc.properties` et situé dans le répertoire `tools\bin` de votre installation Unica Platform) par un nouveau mot de passe.
- Mot de passe du fichier de clés utilisé par Unica Platform lorsqu'il est configuré afin d'utiliser un protocole SSL avec un certificat autre que celui fourni avec Unica Platform ou le serveur d'applications Web. Le certificat peut être un certificat autosigné ou un certificat obtenu auprès d'une autorité de certification.

Quand utiliser encryptPasswords

Utilisez `encryptPasswords` pour les raisons suivantes.

- Lorsque vous changez le mot de passe du compte utilisé pour accéder à votre base de données des tables système Unica Platform.
- Lorsque vous avez créé un certificat autosigné ou obtenu un certificat d'une autorité de certification.

Prérequis

- Avant d'exécuter `encryptPasswords` pour chiffrer et stocker un nouveau mot de passe de base de données, effectuez une copie de sauvegarde du fichier `jdbc.properties`, situé dans le répertoire `tools/bin` sous votre installation de Unica Platform.
- Avant d'exécuter `encryptPasswords` pour chiffrer et stocker le mot de passe de fichier de clés, vous devez créer ou obtenir un certificat numérique et connaître le mot de passe de fichier de clés.

Syntaxe

`encryptPasswords -d databasePassword`

`encryptPasswords -k keystorePassword`

Options

`-ddatabasePassword`

Chiffre le mot de passe de la base de données.

`-k keystorePassword`

Chiffre le mot de passe de la base de données et le stocke dans un fichier nommé `pfile`.

Exemples

- Lors de l'installation de Unica Platform, l'identifiant du compte de la base de données des tables système a été défini sur `myLogin`. Quelque temps après l'installation, vous avez remplacé le mot de passe de ce compte par `newPassword`. Exécutez `encryptPasswords` comme suit pour chiffrer et stocker le mot de passe de la base de données.

  ```
  encryptPasswords -d newPassword
  ```

- Vous configurez une application Unica pour utiliser SSL et avez créé et obtenu un certificat numérique. Exécutez `encryptPasswords` comme suit pour chiffrer et stocker le mot de passe de fichier de clés.

  ```
  encryptPasswords -k myPassword
  ```

encryptTomcatDBPasswords

L'utilitaire `encryptTomcatDBPasswords` chiffre les mots de passe de base de données que le serveur d'applications Tomcat utilise en interne. Il sert à chiffrer des mots de passe de base de données utilisés dans Campaign.xml et unica.xml. Cet utilitaire peut chiffrer le mot de passe de base de données d'application Unica. L'utilitaire imprime le mot de passe chiffré dans la ligne de commande.

Quand utiliser encryptTomcatDBPasswords

Utilisez l'utilitaire `encryptTomcatDBPasswords` lorsque vous souhaitez utiliser un mot de passe chiffré sous des configurations Tomcat. Il peut ensuite être utilisé lorsque le mot de passe Campaign ou Unica System DB a expiré ou a été modifié. Vous pouvez utiliser cet utilitaire et chiffrer le mot de passe qui sera remplacé dans Campaign.xml, unica.xml et plan.xml sous `<instanceHome>\conf\Catalina\localhost`.

Syntaxe

```
encryptTomcatDBPasswords -d databasePassword
```

Commandes

`-ddatabasePassword`

Chiffre le mot de passe de la base de données.

Remarque :

Cet utilitaire est uniquement disponible lorsque l'utilisateur sélectionne Tomcat comme serveur d'applications en installant Unica Platform.

Il peut uniquement être utilisé lorsque l'utilisateur souhaite utiliser des mots de passe chiffrés au lieu de mots de passe en texte clair, sous des configurations Tomcat.

Pour plus d'informations, voir la documentation Tomcat.

partitionTool

Les partitions sont associées aux stratégies et rôles Unica Campaign. Ces associations de stratégies et rôles et de leur partitions sont stockées dans les tables système Unica Platform. L'utilitaire `partitionTool` ensemence les tables du système Unica Platform avec des informations de base sur la politique et les rôles des partitions.

Quand utiliser partitionTool

Pour chaque partition que vous créez, vous devez utiliser `partitionTool` pour ensemencer les tables du système Unica Platform avec des informations de base sur les stratégies et les rôles.

Consultez le guide d'installation approprié pour votre version de Unica Campaign pour obtenir des instructions détaillées sur la configuration de plusieurs partitions dans Unica Campaign.

Caractères spéciaux et espaces

Toute description de partition ou tout nom d'utilisateur, de groupe ou de partition qui contient des espaces doit être placé entre guillemets.

Syntaxe

`partitionTool -c -s` *`sourcePartition`* `-n` *`newPartitionName`* `[-u` *`admin_user_name`*`]`
`[-d` *`partitionDescription`*`] [-g` *`groupName`*`] [-a application]`

Commandes

Les commandes suivantes sont disponibles dans l'utilitaire `partitionTool`.

`-c`

Réplique (clone) les politiques et les rôles d'une partition existante spécifiée à l'aide de l'option `-s`, et utilise le nom spécifié à l'aide de l'option `-n`. Ces deux options sont requises avec `c`. Cette commande effectue les opérations suivantes.

- Crée un nouvel utilisateur Unica avec le rôle Admin dans la stratégie Rôles d'administration et la stratégie globale de Unica Campaign. Le nom de partition que vous spécifiez est défini automatiquement comme mot de passe de l'utilisateur.
- Crée un nouveau groupe Unica Platform et fait du nouvel utilisateur Admin un membre de ce groupe.
- Crée un nouvel objet de partition.
- Réplique toutes les stratégies associées à la partition source et les associe à la nouvelle partition.
- Pour chaque stratégie répliquée, réplique tous les rôles associés à la stratégie.
- Pour chaque rôle répliqué, mappe toutes les fonctions de la même manière qu'elles l'étaient dans le rôle source.
- Affecte le nouveau groupe Unica Platform au dernier rôle Admin défini par le système lors de la réplication du rôle. Si vous clonez la partition par défaut, partition1, ce rôle est le rôle d'administration par défaut (Admin).

Options

`-d` *`partitionDescription`*

Facultatif, utilisé avec `-c` uniquement. Spécifie une description qui apparaît dans la sortie de la commande `-list`. Doit être inférieure ou égale à 32 caractères. Placez entre guillemets si la description contient des espaces.

`-une` *`application`*

Facultatif, utilisé uniquement avec `-c`, `-n`, `-g`, et `-u`. Clone les données de la partition source pour la partition d'application seulement spécifiée. L'application doit être une application Unica Suite.

`-g` *`groupName`*

Facultatif, utilisé avec `-c` uniquement. Spécifie le nom du groupe d'administration de Unica Platform créé par l'utilitaire. Le nom doit être unique dans cette instance de Unica Platform

S'il n'est pas défini, le nom prend par défaut la valeur de `partition_nameAdminGroup`.

`-n` *`partitionName`*

Facultatif avec `-list`, obligatoire avec `-c`. Doit être inférieure ou égale à 32 caractères.

Utilisé avec `-list`, spécifie la partition dont les informations sont listées.

Lorsqu'il est utilisé avec `-c`, spécifie le nom de la nouvelle partition, et le nom de la partition que vous spécifiez est utilisé comme mot de passe pour l'utilisateur Admin. Le nom de la partition doit correspondre au nom que vous avez donné à la partition lorsque vous l'avez configurée (à l'aide du modèle de partition sur la page de Configuration).

`-s` *`sourcePartition`*

Requis, utilisé avec `-c` uniquement. Nom de la partition source à répliquer.

`-u` *`adminUserName`*

Facultatif, utilisé avec `-c` uniquement. Spécifie le nom de l'utilisateur Admin pour la partition répliquée. Le nom doit être unique dans cette instance de Unica Platform.

S'il n'est pas défini, le nom prend par défaut la valeur *`partitionNameAdminUser`*.

Le nom de partition est automatiquement défini comme mot de passe de l'utilisateur.

Exemples

- Créez une partition avec les caractéristiques suivantes.
  - Clonée à partir de partition1
  - Le nom de la partition est `myPartition`
  - Utilise le nom d'utilisateur (`myPartitionAdminUser`) et le mot de passe (`myPartition`) par défaut.
  - Utilise le nom de groupe par défaut (`myPartitionAdminGroup`)
  - A la description "ClonedFromPartition1"
  - `partitionTool -c -s partition1 -n maPartition -d "ClonedFromPartition1"`
- Créez une partition avec les caractéristiques suivantes.
  - Clonée à partir de partition1
  - Le nom de la partition est `partition2`

    - Spécifie le nom d'utilisateur du `client A` avec le mot de passe attribué automatiquement à la `partition 2`.
    - Spécifie le nom de groupe de `customerAGroup`
    - A la description "PartitionForCustomerAGroup"
    - `partitionTool -c -s partition1 -n partition2 -u customerA -g customerAGroup -d "PartitionForCustomerAGroup"`
- Mettez à jour une partition avec les caractéristiques suivantes.
    - Clonée à partir de partition1
    - Le nom de la partition est partition2
    - Spécifier le nom de l'utilisateur admin et le groupe d'utilisateurs admin de la partition2
    - `partitionTool -c -s partition1 -n partition2 -u partition2AdminUser -a Journey`

Note : En utilisant l'option `-a`, assurez-vous de spécifier le nom du groupe, si le nom du groupe a été spécifié explicitement lorsque la partition a été créée par l'utilitaire.

```
partitionTool -c -s partition1 -n partition2 -u partition2AdminUser -g [nom du groupe partition2] -a Journey
```

populateDb

L'utilitaire `populateDb` insère les données (alimentation) par défaut dans les tables système Unica Platform.

Le programme d'installation d'Unica peut remplir les tables système de Unica Platform avec les données par défaut de Unica Platform et de Unica Campaign. Toutefois, si vos règles d'entreprise n'autorisent pas le programme d'installation à changer la base de données ou que le programme d'installation ne parvient pas à se connecter aux tables système de Unica Platform, vous devez insérer les données par défaut dans les tables système de Unica Platform à l'aide de cet utilitaire.

Pour Unica Campaign, ces données comportent les rôles et autorisations de sécurité pour la partition par défaut. Pour Unica Platform, elles incluent les utilisateurs et les groupes par défaut, ainsi que les rôles de sécurité et les droits de la partition par défaut.

Syntaxe

`populateDb -n` *`productName`*

Commandes

`-n` *`productName`*

Insérez les données par défaut dans les tables système Unica Platform. Les noms de produit valides sont `Manager` (pour Unica Platform) et `Campaign` (pour Unica Campaign).

Exemples

- Insérez manuellement les données par défaut Unica Platform.

  ```
  populateDb -n Manager
  ```
- Insérez manuellement les données par défaut Unica Campaign.

  ```
  populateDb -n Campaign
  ```

restoreAccess

L'utilitaire `restoreAccess` permet de rétablir l'accès à Unica Platform si tous les utilisateurs qui possèdent des privilèges PlatformAdminRole ont été involontairement verrouillés ou si toute possibilité de connexion à Unica Platform est perdue.

Quand utiliser restoreAccess

Vous pouvez être amené à exécuter `restoreAccess` dans les deux situations décrites dans cette section.

Utilisateurs PlatformAdminRole désactivés

Il est possible que tous les utilisateurs qui possèdent les privilèges PlatformAdminRole dans Unica Platform soient désactivés dans le système. Voici un exemple qui montre

comment le compte utilisateur platform_admin peut être désactivé. Supposons qu'un seul utilisateur dispose des privilèges PlatformAdminRole (utilisateur platform_admin). Supposons que la propriété `Tentatives max. de connexion autorisées` de la catégorie **Général | Paramètres de mot de passe** de la page Configuration est paramétrée sur `3`. Supposons ensuite qu'un utilisateur qui tente de se connecter en tant que platform_admin entre un mot de passe incorrect trois fois de suite. En raison de ces échecs de connexion, le compte platform_admin est désactivé dans le système.

Dans ce cas, vous pouvez utiliser `restoreAccess` pour ajouter un utilisateur qui possède les privilèges PlatformAdminRole dans les tables système de Unica Platform sans accéder à l'interface Web.

Lorsque vous exécutez `restoreAccess` de cette manière, l'utilitaire crée un utilisateur qui possède le nom de connexion et le mot de passe spécifiés, ainsi que les privilèges PlatformAdminRole.

Si un nom de connexion utilisateur existe dans Unica Platform en tant qu'utilisateur interne, le mot de passe de cet utilisateur est changé.

Seul un utilisateur qui possède le nom de connexion PlatformAdmin et les privilèges PlatformAdminRole peut administrer tous les tableaux de bord. Par conséquent, si l'utilisateur platform_admin est désactivé et que vous créez un utilisateur avec `restoreAccess`, vous devez créer un utilisateur qui possède le nom de connexion platform_admin.

Configuration incorrecte de l'authentification NTLMv2

Si vous implémentez l'authentification NTLMv2 avec une configuration incorrecte et que vous ne parvenez plus à vous connecter, utilisez `restoreAccess` pour pouvoir vous reconnecter.

Lorsque vous exécutez `restoreAccess` de cette manière, l'utilitaire modifie la valeur de la propriété `Platform | Sécurité | Méthode de connexion` par `Unica Platform`. Ce changement vous permet de vous connecter à l'aide de n'importe quel compte utilisateur qui existait avant le verrouillage. Vous avez également la possibilité de spécifier un nouveau nom de connexion et un nouveau mot de passe. Vous devez redémarrer le

serveur d'application Web sur lequel Unica Platform est déployé si vous exécutez l'utilitaire `restoreAccess` de cette manière.

Observations relatives aux mots de passe

Gardez à l'esprit les points suivants relatifs aux mots de passe lorsque vous utilisez `restoreAccess`.

- L'utilitaire `restoreAccess` ne prend pas en charge les mots de passe en blanc et n'impose pas de règles relatives aux mots de passe.
- Si vous spécifiez un nom d'utilisateur utilisé, l'utilitaire réinitialise le mot de passe de cet utilisateur.

Syntaxe

`restoreAccess -u *loginName* -p *password*`

`restoreAccess -r`

Commandes

`-r`

Utilisée sans l'option `-u *loginName*`, réinitialise la valeur de la propriété `Platform | Sécurité | Méthode de connexion` sur `Unica Platform`. Requiert le redémarrage du serveur d'application Web pour être prise en compte.

Utilisée avec l'option `-u *loginName*`, crée un utilisateur PlatformAdminRole.

Options

`-u *loginNname*`

Crée un utilisateur qui possède les privilèges PlatformAdminRole et le nom de connexion spécifié. Doit s'utiliser avec l'option `-p`.

`-p *password*`

Spécifie le mot de passe de l'utilisateur en cours de création. Obligatoire avec l'option `-u`.

Exemples

- Créez un utilisateur qui possède les privilèges PlatformAdminRole. Le nom de connexion est `tempUser` et le mot de passe est `tempPassword`.

  ```
  restoreAccess -u tempUser -p tempPassword
  ```
- Remplacez la valeur de la méthode de connexion par `Platform`, puis créez un utilisateur doté des privilèges PlatformAdminRole. Le nom de connexion est `tempUser` et le mot de passe est `tempPassword`.

  ```
  restoreAccess -r -u tempUser -p tempPassword
  ```

scheduler_console_client

Les tâches configurées dans Unica Scheduler peuvent être répertoriées et déclenchées par cet utilitaire, si elles sont configurées pour intercepter un déclencheur.

Que faire si SSL est activé

Lorsque l'application web Unica Platform est configurée pour utiliser SSL, la JVM utilisée par l'utilitaire `scheduler_console_client` doit utiliser le même certificat SSL que celui utilisé par le serveur d'applications Web sur lequel le site Unica Platform est déployé.

Pour importer le certificat SSL, procédez comme suit :

- Déterminer l'emplacement du JRE utilisé par le `scheduler_console_client`.
  - Si `JAVA_HOME` est défini comme une variable d'environnement système, le JRE vers lequel il pointe est celui utilisé par l'utilitaire `scheduler_console_client`.
  - Si `JAVA_HOME` n'est pas défini comme variable d'environnement système, l'utilitaire `scheduler_console_client` utilise le JRE défini soit dans le script `setenv` situé dans le répertoire `tools/bin` de votre installation Unica Platform, soit sur la ligne de commande.
- Importez le certificat SSL utilisé par le serveur d'application web sur lequel le site Unica Platform est déployé dans le JRE utilisé par `scheduler_console_client`.

  Le Sun JDK comprend un programme appelé `keytool` que vous pouvez utiliser pour importer le certificat. Consultez la documentation Java™ pour obtenir des détails

complets sur l'utilisation de ce programme ou accédez à l'aide en saisissant `-help` lorsque vous exécutez le programme.

Note : En cas de mise à jour, le JRE livré avec Unica est écrasé. Veillez donc à réimporter les certificats dans le JRE si vous utilisez le même JRE.

- Ouvrez le fichier `tools/bin/schedulerconsoleclient` dans un éditeur de texte et ajoutez les propriétés suivantes. Elles dépendent du serveur d'applications web sur lequel Unica Platform est déployé.
  - Pour WebSphere®, ajoutez ces propriétés au fichier.

    -Djavax.net.ssl.keyStoreType=JKS

    -Djavax.net.ssl.keyStore="Chemin d'accès au fichier JKS de votre magasin de clés".

    -Djavax.net.ssl.keyStorePassword="Le mot de passe de votre magasin de clés".

    -Djavax.net.ssl.trustStore="Chemin vers le fichier JKS de votre magasin de confiance".

    -Djavax.net.ssl.trustStorePassword="Votre mot de passe du magasin de confiance"

    -DisUseIBMSSLSocketFactory=false
  - Pour WebLogic, ajoutez ces propriétés au fichier.

    -Djavax.net.ssl.keyStoreType="JKS"

    -Djavax.net.ssl.trustStore="Chemin vers le fichier JKS de votre magasin de confiance".

    -Djavax.net.ssl.trustStorePassword="Votre mot de passe du magasin de confiance"

Si les certificats ne correspondent pas, le fichier journal de Unica Platform contient une erreur telle que la suivante :

```
Causé par : sun.security.provider.certpath.SunCertPathBuilderException :
Impossible de trouver un chemin de certification valide pour la cible
demandée.
```

Prérequis

Unica Platform doit être installé, déployé et en cours d'exécution.

Syntaxe

`scheduler_console_client -v -t *trigger_name user_name*`

`scheduler_console_client -s -t *trigger_name user_name*`

Commandes

`-v`

Répertorier les tâches du planificateur configurées pour écouter le déclencheur spécifié.

Doit être utilisé avec l'option `-t`.

`-s`

Envoyer le déclencheur spécifié.

Doit être utilisé avec l'option `-t`.

Options

`-t *trigger_name*`

Nom du déclencheur défini dans le planificateur.

Exemple

- Listez les travaux configurés pour écouter un déclencheur nommé `trigger1`.

  ```
  scheduler_console_client -v -t trigger1 myLogin
  ```
- Exécuter les travaux configurés pour écouter un déclencheur nommé `trigger1`.

  ```
  scheduler_console_client -s -t trigger1 myLogin
  ```

quartzjobtool

Les travaux du planificateur créés dans la version 11.1 et dans les versions ultérieures doivent être mis à jour pour exécuter la version 12.0. Mettez à jour les travaux du planificateur à l'aide de quartzjobtool. Lorsque le programme d'installation ne l'a pas fait automatiquement lors de l'installation ou de la mise à niveau. Cet outil lit les variables d'environnement du script `setenv_quartz`. Le programme d'installation d'Unica Platform doit avoir défini cette variable automatiquement, mais il est également conseillé de vérifier que la variable `JAVA_HOME` est définie si vous rencontrez un problème d'exécution d'un utilitaire. Le kit JDK doit être la version de Sun (et non, par exemple, le kit JDK JRockit disponible avec WebLogic).

Syntaxe

quartzjobtool

Mettez à jour les travaux du planificateur à l'aide de quartzjobtool. Cette étape est obligatoire. Si cet outil de mise à niveau n'est pas exécuté, aucun travail du planificateur existant ne pourra démarrer. L'outil quartzjobtool se trouve dans le répertoire tools\bin de l'emplacement d'installation d'Unica Platform. Exécutez cet utilitaire à partir du répertoire `tools\bin`.

Exemple de commande (Windows) : quartzjobtool.bat

Exemple de commande (Unix) : ./quartzjobtool.sh

Exemple

Mettre à jour les travaux du planificateur quartzjobtool.

Scripts SQL de Unica Platform

Cette section décrit les scripts SQL fournis avec Unica Platform pour effectuer différentes tâches relatives aux tables système de Unica Platform.

Les scripts SQL de Unica Platform se trouvent dans le répertoire `db` sous votre installation de Unica Platform.

Les scripts sont conçus pour être exécutés sur les tables système de Unica Platform, à l'aide du client de base de données.

ManagerSchema_DeleteAll.sql

Le script `Manager_Schema_DeleteAll.sql` supprime toutes les données des tables système Unica Platform sans supprimer les tables elles-mêmes. Ce script supprime tous les utilisateurs, groupes, droits d'accès de sécurité, filtres de données et paramètres de configuration de Unica Platform.

Quand utiliser ManagerSchema_DeleteAll.sql

Vous souhaiterez peut-être utiliser `ManagerSchema_DeleteAll.sql` si des données corrompues vous empêchent d'utiliser une instance de Unica Platform.

Conditions supplémentaires

Pour rendre Unica Platform opérationnel après avoir exécuté `ManagerSchema_DeleteAll.sql` vous devez effectuer les étapes suivantes.

- Exécutez l'utilitaire `populateDB`. L'utilitaire `populateDB` restaure les propriétés de configuration, les utilisateurs, les rôles et les groupes par défaut mais ne restaure pas les utilisateurs, les rôles et les groupes que vous avez créés ou importés après l'installation initiale.
- Employez l'utilitaire configTool avec le fichier `config_navigation.xml` pour importer des éléments de menu.
- Si vous avez effectué une configuration après l'installation (par exemple, la création de filtres de données ou l'intégration à un serveur LDAP ou à une plate-forme de contrôle d'accès Web), vous devez effectuer ces configurations à nouveau.
- Si vous souhaitez restaurer des filtres de données qui existaient précédemment, exécutez l'utilitaire `datafilteringScriptTool` à l'aide du fichier XML créé à l'origine pour spécifier les filtres de données.

ManagerSchema_PurgeDataFiltering.sql

Le script `ManagerSchema_PurgeDataFiltering.sql` supprime toutes les données de filtrage des données des tables système Unica Platform sans supprimer les tables de filtrage des données elles-mêmes. Ce script supprime tous les filtres de données, configurations de filtre de données, audiences et affectations de filtre de données de Unica Platform.

Quand utiliser ManagerSchema_PurgeDataFiltering.sql

Vous souhaiterez peut-être utiliser `ManagerSchema_PurgeDataFiltering.sql` si vous devez supprimer tous les filtres de données sans supprimer d'autres données dans les tables système Unica Platform.

Important : Le script `ManagerSchema_PurgeDataFiltering.sql` ne réinitialise pas les valeurs des deux propriétés de filtrage des données, `Nom de la table par défaut` et `Nom de l'audience par défaut`. Si ces valeurs ne sont plus valides pour les filtres de données que vous souhaitez utiliser, vous devez définir les valeurs manuellement sur la page de Configuration.

ManagerSchema_DropAll.sql

Le script `ManagerSchema_DropAll.sql` supprime toutes les tables système Unica Platform d'une base de données. Ce script supprime tous les utilisateurs, tables, groupes, droits d'accès de sécurité et paramètres de configuration de Unica Platform.

Remarque : Si vous exécutez ce script sur une base de données contenant une version antérieure des tables système Unica Platform, vous risquez de recevoir des messages d'erreur dans votre client de base de données indiquant que les contraintes n'existent pas. Vous pouvez ignorer ces messages.

Quand utiliser ManagerSchema_DropAll.sql

Vous souhaiterez peut-être utiliser `ManagerSchema_DropAll.sql` si vous avez désinstallé une instance de Unica Platform sur laquelle les tables système sont dans une base de données qui contient d'autres tables que vous voulez continuer d'utiliser.

Conditions supplémentaires

Pour disposer d'une version de Unica Platform opérationnelle après l'exécution de ce script, vous devez effectuer les étapes suivantes.

- Exécutez le script SQL approprié pour recréer les tables système.
- Exécutez l'utilitaire `populateDB`. L'exécution de l'utilitaire `populateDB` restaure les propriétés de configuration, les utilisateurs, les rôles et les groupes par défaut mais ne restaure pas les utilisateurs, les rôles et les groupes que vous avez créés ou importés après l'installation initiale.
- Employez l'utilitaire `configTool` avec le fichier `config_navigation.xml` pour importer des éléments de menu.
- Si vous avez effectué une configuration après l'installation (par exemple, la création de filtres de données ou l'intégration à un serveur LDAP ou à une plate-forme de contrôle d'accès Web), vous devez effectuer ces configurations à nouveau.

Scripts SQL pour la création des tables système

Utilisez les scripts présentés dans la table suivante pour créer des tables système de Unica Platform manuellement, lorsque les règles d'entreprise ne vous permettent pas d'utiliser le programme d'installation pour les créer automatiquement.

Les scripts sont indiqués dans l'ordre dans lequel vous devez les exécuter.

Tableau 74. Scripts de création des tables système

Type de source de données	Noms de scripts
IBM® DB2®	• `ManagerSchema_DB2.sql` Si vous prévoyez de prendre en charge des caractères multioctets (par exemple : chinois, japonais, ou coréens), utilisez le script `ManagerSchema_DB2_unicode.sql`. • `ManagerSchema__DB2_CeateFKConstraints.sql` • `active_portlets.sql` • `notification_rules.sql`
Microsoft™ SQL Server	• `ManagerSchema_SqlServer.sql` • `ManagerSchema__SqlServer_CeateFKConstraints.sql` • `active_portlets.sql` • `notification_rules.sql`
MariaDB	• `ManagerSchema_MariaDB.sql` • `ManagerSchema_MariaDB_StoredProcedures.sql` • `ManagerSchema_MariaDB_CreateFKConstraints.sql` • `active_portlets.sql` • `notification_rules.sql`
Oracle	• `ManagerSchema_Oracle.sql` • `ManagerSchema__Oracle_CeateFKConstraints.sql` • `active_portlets.sql` • `notification_rules_Oracle.sql`

Si vous envisagez d'utiliser la fonction Planificateur qui permet de configurer un diagramme qui s'exécute à une fréquence prédéfinie, vous devez également créer les tables qui prennent en charge cette fonction. Pour créer les tables de planificateur, exécutez le script approprié, comme indiqué dans le tableau suivant.

Tableau 75. Scripts d'activation d'Unica Scheduler

Type de source de données	Nom du script
DB2®	`quartz_db2.sql`
Microsoft™ SQL Server	`quartz_sqlServer.sql`
Oracle	`quartz_oracle.sql`
MariaDB	`quartz_MariaDB.sql`

Quand utiliser les scripts de tables système

Vous devez utiliser ces scripts lorsque vous installez ou mettez à niveau Unica Platform si vous n'avez pas autorisé le programme d'installation à créer automatiquement les tables système ou si vous avez utilisé `ManagerSchema_DropAll.sql` pour supprimer toutes les tables système Unica Platform de votre base de données.

Propriétés de configuration de Unica

Cette section décrit les propriétés de configuration de la page **Paramètres et Configuration**.

Propriétés de configuration d' Unica Platform

Cette section décrit les propriétés de configuration de Unica Platform dans la page de configuration.

Unica Platform

Les propriétés de cette catégorie vous permettent de définir les paramètres régionaux par défaut ainsi que les indicateurs définissant si l'installation de Unica Platform s'effectue en cluster, si Unica Plan est intégré à Unica Campaign et si l'intégration d'offre est activée pour l'intégration.

Région

Description

Indique la préférence de paramètres régionaux pour les utilisateurs Unica. Lorsque vous définissez cette propriété dans la page de configuration, le paramètre que vous appliquez correspond au paramètre par défaut dans Unica et ce, pour tous les utilisateurs, à l'exception de ceux ayant configuré leurs préférences de paramètres régionaux par le biais de la page Utilisateur de Unica Platform. Lorsque vous définissez cette propriété pour un utilisateur individuel, le paramètre que vous appliquez remplace le paramètre par défaut.

Ce paramétrage des préférences affecte l'affichage de la langue, de l'heure, des nombres et des dates au sein des applications Unica.

La disponibilité des paramétrages régionaux peut varier en fonction de l'application Unica ; en outre, cette propriété des paramètres régionaux n'est pas prise en charge par toutes les applications dans Unica Platform. Consultez la documentation spécifique au produit pour savoir si la propriété `Paramètre régional` est disponible et prise en charge.

Valeur par défaut

`Anglais (États-Unis)`

Serveur d'aide

Description

L'URL du serveur sur lequel est installée l'aide en ligne hébergée par . Si les utilisateurs Unica ont accès à Internet, ne changez pas la valeur par défaut, qui se réfère au serveur d'aide en ligne géré et actualisé par .

Valeur par défaut

URL du serveur d'aide hébergé.

Valeurs valides

N'importe quel serveur sur lequel est installée l'aide hébergée par .

Intégration Unica Plan - Unica Campaign

Description

Indicateur spécifiant si Unica Plan et Unica Campaign sont installés ensemble et intégrés. Pour plus d'informations sur la configuration de cette intégration, voir Unica Plan et Unica Campaign Integration Guide.

Valeur par défaut

`Faux`

Valeurs valides

`True | False`

Unica Plan - Intégration d'offre

Description

Pour les systèmes intégrant Unica Plan à Unica Campaign, cet indicateur indique si l'intégration d'offre est également activée ou non. L'intégration d'offre permet d'utiliser Unica Plan pour effectuer des tâches de gestion de cycle de vie d'offre. Pour plus d'informations sur la configuration de cette intégration, voir Unica Plan et Unica Campaign Integration Guide.

Valeur par défaut

`Faux`

Valeurs valides

`True | False`

Page de démarrage

Description

L'URL de la page qui s'affiche lorsque les utilisateurs se connectent à Unica. La valeur par défaut est le tableau de bord par défaut.

Valeur par défaut

Tableau de bord par défaut.

Valeurs valides

N'importe quel URL Unica, à l'exception des pages de soumission de formulaires, d'édition et de résultats de recherche.

Nom du domaine

Description

Nom du domaine sur lequel Unica est installé. La valeur est définie au cours de l'installation. Vous ne devez pas la changer à moins que le nom de domaine ne soit modifié.

Si des utilisateurs accèdent aux produits Unica depuis le navigateur Chrome, utilisez le nom de domaine complet. Si vous n'utilisez pas le nom de domaine complet, le navigateur Chrome ne pourra pas accéder aux adresses URL de produit.

Valeur par défaut

Non défini

Désactiver de balisage de page

Description

Si la valeur par défaut `False` est spécifiée, utilise le code ID site entré lors de l'installation de Unica Platform pour collecter les statistiques de base qui suivent les tendances d'utilisation globales du produit pour développer et améliorer les produits . envoie les informations à `http://pt200201.unica.com` via HTTP.

Si vous ne souhaitez pas que ces informations soient collectées, affectez à cette propriété la valeur `True`.

Valeur par défaut

`Faux`

Valeurs valides

`True | False`

Ce déploiement est-il effectué en cluster ?

Description

Si vous installez Unica Platform dans un déploiement en cluster, affectez à cette propriété la valeur `True`. Sinon, conservez la valeur par défaut `False`.

Si vous modifiez cette propriété alors que Unica Platform est en cours d'exécution, vous devez redémarrer Unica Platform pour que les modifications entrent en vigueur.

Valeur par défaut

`Faux`

Valeurs valides

`True | False`

Appliquer la sécurité à du contenu statique pour toutes les applications

Description

Lorsque cette valeur est définie sur `Yes`, si un utilisateur authentifié tente d'accéder directement à un contenu statique tel qu'une image, un contrôle est effectué pour vérifier l'authentification de l'utilisateur. Si l'utilisateur est authentifié, le contenu est rendu. Si l'utilisateur n'est pas authentifié, il est envoyé vers la page de connexion. Ce paramètre s'applique dans tous les produits Unica.

Valeur par défaut

`Non`

Valeurs valides

`Oui | Non`

Unica | Général | Navigation

Les propriétés de cette catégorie spécifient les valeurs utilisées en interne pour la navigation dans les produits Unica.

Port TCP des connexions sécurisées

Description

Spécifie le port SSL du serveur d'applications Web sur lequel Unica Platform est déployé. Cette propriété est utilisée en interne pour établir la communication entre les produits d'Unica.

Valeur par défaut

`7001`

Port TCP des connexions standard

Description

Spécifie le port HTTP du serveur d'applications Web sur lequel Unica Platform est déployé. Cette propriété est utilisée en interne pour établir la communication entre les produits d'Unica.

Valeur par défaut

`7001`

URL de l'Unica Platform

Description

Spécifie l'URL utilisée pour Unica Platform. Cette propriété est définie au moment de l'installation et ne doit généralement pas être changée. Notez que l'URL contient le nom de domaine, comme illustré ci-après.

`protocole://nom_ou_adresse_IP_machine.nom_domaine:numéro_port/racine_contexte`

Le nom de la machine ne doit pas être `localhost`.

Si des utilisateurs accèdent aux produits Unica depuis le navigateur Chrome, utilisez le nom de domaine complet dans l'adresse URL. Si vous n'utilisez pas le nom de domaine complet, le navigateur Chrome ne pourra pas accéder aux adresses URL de produit.

Important : Si des produits Unica sont installés dans un environnement distribué, vous devez utiliser le nom de machine plutôt qu'une adresse IP dans l'URL de navigation pour toutes les applications de la suite. En outre, si vous disposez d'un environnement groupé et que vous choisissez d'utiliser d'autres ports que les ports par défaut `80` ou `443` pour votre déploiement, n'utilisez pas un numéro de port qui se trouve dans cette propriété.

Valeur par défaut

Non défini

Exemple

Dans un environnement configuré pour SSL, l'URL peut se présenter de la façon suivante :

```
https://machineName.companyDomain.com:8080/unica
```

Unica | Général | Filtrage des données

Les propriétés de cette catégorie définissent les valeurs utilisées lorsqu'un filtrage des données est implémenté.

Nom de la table par défaut

Description

Cette propriété de configuration est requise pour l'activation des filtres de données.

Définissez la valeur de cette propriété pour qu'elle corresponde exactement au nom utilisé pour l'élément `addTables | AddDataTable | dataTable | nom` dans le XML utilisé pour créer les filtres de données.

Valeur par défaut

Non défini

Valeurs valides

Au maximum, 50 caractères du type varchar.

Nom de l'audience par défaut

Description

Cette propriété de configuration est requise pour l'activation des filtres de données.

Définissez la valeur de cette propriété pour qu'elle corresponde exactement au nom utilisé pour l'élément `AddAudience | audience | nom` dans le XML utilisé pour créer les filtres de données.

Valeur par défaut

Non défini

Valeurs valides

Au maximum, 50 caractères du type varchar.

Activer le cache du filtre de données

Description

Cette propriété est facultative, et peut être définie pour améliorer les performances des filtres de données.

Cette propriété spécifie si Unica Platform extrait des définitions de filtre de données de la base de données ou d'un cache. Lorsque cette valeur est **true**, les définitions de filtre de données sont stockées dans le cache et le cache est mis à jour dès que le filtre de données est modifié.

Vous devez redémarrer l'application Web Unica Platform après avoir modifié cette valeur de propriété, pour qu'elle prenne effet.

Valeur par défaut

`Faux`

Unica | Général | Paramètres du mot de passe

Les propriétés dans la catégorie **Général** | **Paramètres du mot de passe** spécifient les politiques qui s'appliquent à Unica mots de passe. La plupart de ces options s'appliquent uniquement aux mots de passe des utilisateurs internes (créés dans Unica Platform), et non pas aux utilisateurs externes (importés à partir d'un système externe).

L'exception est la propriété `Maximum de tentatives de connexion échouées autorisées`, qui affecte les utilisateurs internes et externes. Veuillez également noter que cette propriété ne remplace pas les éventuelles restrictions similaires définies dans un système externe.

tentatives max. de connexion autorisées

La description

Permet de spécifier le nombre maximum de fois qu'un mot de passe non valide peut être saisi à chaque connexion utilisateur. Une fois le maximum atteint, l'utilisateur est désactivé dans le système Unica ; personne ne peut se connecter sous cet identifiant.

Si la valeur est définie sur zéro ou moins, le système autorise un nombre illimité de tentatives consécutives.

Valeur par défaut

3

Valeurs valides

Entier

nombre d'historique de mot de passe

La description

Nombre d'anciens mots de passe conservés par le système pour chaque utilisateur. L'utilisateur n'est pas autorisé à réutiliser les mots de passe qui figurent dans cette liste. Si la valeur est définie sur zéro ou moins, aucun historique n'est conservé et l'utilisateur peut réutiliser le même mot de passe

indéfiniment. Notez que le nombre d'historique de mot de passe ne prend pas en compte le mot de passe affecté à un compte utilisateur lors de sa création.

Valeur par défaut

`0`

Valeurs valides

Entier

validité (en jours)

La description

Indique le nombre de jours avant l'expiration d'un mot de passe utilisateur.

Si la valeur est définie sur zéro ou moins, le mot de passe n'expire pas.

Si la valeur est supérieure à zéro, les utilisateurs doivent changer leur mot de passe lors de leur première connexion, et l'intervalle d'expiration est calculé sur la base de cette première connexion.

Si vous changez cette valeur après la création des utilisateurs et des mots de passe, la nouvelle date d'expiration prend effet lorsque les utilisateurs existants modifient leur mot de passe.

Valeur par défaut

`30`

Valeurs valides

Entier

les mots de passe en blanc sont autorisés

La description

Spécifie si un mot de passe vide est autorisé. Si vous mettez cette option à true, vous devriez également mettre `Minimum character length=0`.

Valeur par défaut

`true`

Valeurs valides

`true | false`

autoriser un nom d'utilisateur et un mot de passe identiques

La description

Indique s'il est possible que le mot de passe de l'utilisateur soit identique à son nom de connexion.

Valeur par défaut

`false`

Valeurs valides

`true | false`

Un nombre minimal de caractères numériques

La description

Nombre minimum de chiffres requis par un mot de passe. Si la valeur est définie sur zéro ou moins, il n'y a pas de minimum.

Valeur par défaut

`0`

Valeurs valides

Entier

nombre minimum de caractères alphabétiques

La description

Nombre minimum de lettres requises par un mot de passe. Si la valeur est définie sur zéro ou moins, il n'y a pas de minimum.

Valeur par défaut

`0`

Valeurs valides

Entier

nombre minimum de caractères

La description

Longueur minimum d'un mot de passe. Si la valeur est définie sur zéro ou moins, il n'y a pas de minimum. Si vous définissez la valeur sur une valeur supérieure à `0`, vous devez également définir `Mots de passe vides autorisés=faux`.

Valeur par défaut

`4`

Valeurs valides

Entier

Nombre minimum de caractères spéciaux

La description

Spécifie le nombre minimum de caractères spéciaux requis dans un mot de passe. Ceci est applicable pour les valeurs supérieures à zéro. Vous ne pouvez utiliser que les caractères spéciaux suivants lorsque vous créez un mot de passe.

- Astérisque "*"
- Exclamation "!"
- Le signe at "@"
- Dollar "$"
- Esperluette "&"
- Hash "#"

Valeur par défaut

0

Valeurs valides

Entier

Nombre minimum de caractères minuscules

La description

Spécifie le nombre minimum de lettres minuscules requises dans un mot de passe. Il s'applique aux valeurs supérieures à 0, où vous devez définir la valeur correspondante pour le `Nombre minimum de caractères de lettres`.

Valeur par défaut

0

Valeurs valides

Entier

Nombre minimum de caractères majuscules

La description

Spécifie le nombre minimum de lettres majuscules requises dans un mot de passe. Il s'applique aux valeurs supérieures à 0, où vous devez définir la valeur correspondante pour le `Nombre minimum de caractères de lettres`.

Valeur par défaut

0

Valeurs valides

Entier

Longueur maximale des caractères

La description

Spécifie la longueur maximale d'un mot de passe. Il est applicable aux valeurs supérieures à 0.

Valeur par défaut

0

Valeurs valides

Entier

Unica | Général | Divers

Les propriétés de cette catégorie spécifient les valeurs utilisées en interne ainsi que la valeur à définir pour les paramètres régionaux.

Durée de vie de jeton

Description

Spécifie le laps de temps, en secondes, pendant lequel un jeton généré par Unica Platform reste valide. Cette valeur fait partie intégrante de la mise en œuvre de l'identification de la suite. Il est conseillé de ne pas changer cette valeur.

Valeur par défaut

`15`

Valeurs valides

Tout nombre entier positif

Langue par défaut

Description

Définit la langue par défaut utilisée pour Unica Platform. Si vous envisagez d'installer Unica Campaign, vous devez définir cette valeur pour qu'elle corresponde au paramètre régional de Unica Campaign dans la propriété `defaultLocale` de Unica Campaign.

Valeur par défaut

`Anglais`

Valeurs valides

Paramètres régionaux pris en charge

Unica | Général | Communication | E-mail

Les propriétés de cette catégorie servent à configurer Unica Platform pour envoyer des courriers électroniques d'alerte système et de notification aux utilisateurs.

Activer la communication par e-mail

Description

Si la valeur est `True`, Unica Platform envoie des courriers électroniques d'alerte système et des notifications aux utilisateurs. Vous devez également définir les autres propriétés de cette catégorie pour activer cette fonctionnalité.

Valeur par défaut

`Faux`

Protocole du serveur de messagerie

Description

Spécifie le protocole utilisé sur le serveur de messagerie employé pour envoyer les alertes système et les notifications aux utilisateurs. Obligatoire pour les notifications par e-mail.

Valeur par défaut

`smtp`

Hôte du serveur de messagerie

Description

Spécifie le nom du serveur de messagerie employé pour envoyer les alertes système et les notifications aux utilisateurs. Obligatoire pour les notifications par e-mail.

Valeur par défaut

`localhost`

Port de serveur de messagerie

Description

Spécifie le port du serveur de messagerie employé pour envoyer les alertes système et les notifications aux utilisateurs. Obligatoire pour les notifications par e-mail.

Valeur par défaut

25

Adresse de l'émetteur des e-mails

Description

Spécifie le compte utilisé pour envoyer les alertes système et les notifications par courrier électronique. Si votre serveur de messagerie nécessite l'authentification, indiquez l'adresse électronique que vous avez utilisée lorsque vous avez enregistré un nom de compte de serveur de messagerie et un mot de passe comme source de données dans le compte utilisateur Unica Platform. Obligatoire pour les notifications par e-mail.

Valeur par défaut

Non défini

Authentification requise pour le serveur de messagerie ?

Description

Indique si le serveur de messagerie demande l'authentification.

Valeur par défaut

Faux

Utilisateur Unica du compte de messagerie

Description

Spécifie le nom d'utilisateur du compte Unica Platform dans lequel les données d'identification sont stockées en tant que source de données.

Obligatoire pour les notifications, uniquement si votre serveur de messagerie demande l'authentification.

Valeur par défaut

`asm_admin`

Source de données du compte de messagerie

Description

Spécifie le nom de la source de données définie dans le compte Unica Platform dans lequel les données d'identification sont stockées.

Obligatoire pour les notifications, uniquement si votre serveur de messagerie demande l'authentification.

Valeur par défaut

`emailDS`

Unica Platform | Planificateur

Les propriétés de cette catégorie permettent d'activer et de régler les performances du planificateur Unica.

Intervalle d'attente de sondage du client (ms)

Catégorie de configuration

`Platform|Scheduler`

Description

Unica Campaign lance des recherches sur des tâches au niveau du planificateur Unica et ce, à intervalles réguliers en millisecondes spécifiés par cette valeur. La valeur par défaut est 60 secondes. Evitez d'affecter à cette propriété une valeur inférieure à 10 000 (10 secondes), car cela pourrait diminuer les performances de la campagne.

Valeur par défaut

`60 000`

Retard d'initialisation du client (ms)

Description

Durée d'attente en millisecondes avant que l'unité d'exécution du planificateur Unica Campaign n'interroge le planificateur Unica à la recherche de tâches lors de la mise en marche initiale de Unica Campaign. Paramétrez cette valeur de sorte que la durée soit au moins égale au temps nécessaire au démarrage complet de Unica Campaign sur votre système. La valeur par défaut est de cinq minutes.

Valeur par défaut

`300 000`

Valeurs valides

Entier

Nombre maximal d'interrogations de statut inconnu

Description

Définit le nombre de fois que le planificateur vérifie le statut d'une exécution planifiée dont le statut ne peut pas être déterminé. Lorsque la limite est atteinte, le statut d'exécution est Inconnu sur la page **Paramètres > Gestion de la planification**.

Valeur par défaut

`5`

Valeurs valides

Entier

Activation du planificateur

Description

Indique si le planificateur est activé. Définissez cette propriété sur False si vous ne voulez pas que les utilisateurs utilisent le planificateur. Le paramètre False désactive le planificateur pour tous les produits qui l'utilisent.

Vous devez redémarrer l'application Web Unica Platform lorsque vous activez ou désactivez le planificateur.

Valeur par défaut

`True`

Valeurs valides

`True | False`

Unica Platform | Planificateur | Définitions des récurrences

Les propriétés de cette catégorie définissent les modèles de récurrence pour le planificateur Unica. Elles sont visibles dans la boîte de dialogue que vous utilisez si vous définissez un modèle de récurrence lors de la création d'un programme. Vous pouvez utiliser le modèle Récurrence pour créer votre propre modèle de récurrence à l'aide d'une expression Cron valide.

Toutes les heures

Description

La tâche est déclenchée toutes les heures.

Valeur par défaut

`0 0 0/1 * * ?`

Tous les jours

Description

La tâche est déclenchée toutes les 24 heures.

Valeur par défaut

`0 0 0 * * ?`

Tous les [jour de la semaine] à 12 h 00

Description

La tâche est déclenchée le jour indiqué de la semaine à 12 h 00.

Valeur par défaut

- Lundi - `0 0 0 ? * LUN`
- Mardi - `0 0 0 ? * MAR`
- Mercredi - `0 0 0 ? * MER`
- Jeudi - `0 0 0 ? * JEU`
- Vendredi - `0 0 0 ? * VEN`
- Samedi - `0 0 0 ? * SAM`
- Dimanche - `0 0 0 ? * DIM`

Le [premier|dernier] jour de chaque mois à 12 h 00

Description

Le travail est déclenché le jour indiqué (premier ou dernier) du mois à 12 h 00.

Valeur par défaut

- Premier jour de chaque mois - `0 0 0 1 * ?`
- Dernier jour de chaque mois - `0 0 0 L * ?`

Le [premier|dernier] jour de chaque trimestre à 12 h 00

Description

Le travail est déclenché le jour indiqué (premier ou dernier jour) du trimestre à 12 h 00.

Valeur par défaut

- Premier jour de chaque trimestre - `0 0 0 1 * JAN,APR,JUL,OCT`
- Dernier jour de chaque trimestre - `0 0 0 L * MAR,JUN,SEP,DEC`

Le [premier|dernier] jour de chaque année à 12 h 00

Description

La tâche est déclenchée le jour indiqué (premier ou dernier) de l'année à 12 h 00.

Valeur par défaut

- Premier jour de chaque année - `0 0 0 1 ? JAN *`
- Dernier jour de chaque année - `0 0 0 L ? DEC *`

Tous les [mois] à 12 h 00

Description

La tâche est déclenchée le premier jour du mois indiqué à 12 h 00.

Valeur par défaut

- Chaque mois de janvier - `0 0 0 1 ? JAN *`
- Chaque mois de février - `0 0 0 1 ? FEB *`
- Chaque mois de mars - `0 0 0 1 ? MAR *`
- Chaque mois d'avril - `0 0 0 1 ? APR *`
- Chaque mois de mai - `0 0 0 1 ? MAY *`
- Chaque mois de juin - `0 0 0 1 ? JUN *`
- Chaque mois de juillet - `0 0 0 1 ? JUL *`
- Chaque mois d'août - `0 0 0 1 ? AUG *`
- Chaque mois de septembre - `0 0 0 1 ? SEP *`
- Chaque mois d'octobre - `0 0 0 1 ? OCT *`
- Chaque mois de novembre - `0 0 0 1 ? NOV *`
- Chaque mois de décembre - `0 0 0 1 ? DEC *`

Unica Platform | Planificateur | Planifier les enregistrements | [Produit] | [Type d'objet]

Il existe une catégorie différente pour chaque type d'objet pouvant être planifié à l'aide du planificateur Unica. En règle générale, les propriétés de ces catégories ne doivent pas être modifiées.

Nom de classe de l'exécuteur

Description

Classe utilisée par le planificateur Unica pour déclencher l'exécution d'un diagramme ou d'un mailing.

Valeur par défaut

Intervalle d'attente de sondage du statut

Catégorie de configuration

`Platform|Scheduler|Schedule registrations|[Product]|[Object type]`

Pour les diagrammes Unica Campaign, le chemin de cette propriété est `Platform|Scheduler|Schedule registrations|Campaign|Flowchart`.

Description

Le planificateur Unica interroge (sonde) le produit à intervalles réguliers pour obtenir le statut d'exécution des objets planifiés (par exemple, diagrammes ou mailings) qui n'ont pas signalé de statut. L'intervalle est spécifié en millisecondes. La valeur par défaut est de dix minutes. Si vous définissez un intervalle de sondage plus restreint (valeur plus basse), les performances du système peuvent en être affectées. Si vous définissez un intervalle de sondage plus large (valeur plus élevée), la charge est réduite sur le système. Pour Unica Campaign, définissez un intervalle de sondage plus élevé lorsque vous avez un grand nombre de diagrammes Unica Campaign dont l'exécution prend plus de 10 minutes.

Valeur par défaut

`600000`

Nom de groupe pour recevoir les notifications de travail

Description

Les notifications pour toutes les planifications de chaque type d'objet sont envoyées à tous les membres du groupe que vous indiquez ici.

Unica Platform | Planificateur | Planifier les enregistrements | [Produit] | [Type d'objet] | [Groupe de régulation]

Il existe deux groupes de régulation par défaut pour chaque type d'objet pouvant être planifié à l'aide du planificateur Unica. Notez que ces groupes par défaut n'apparaissent pas sur la page Groupes d'utilisateurs. Vous pouvez utiliser le modèle de groupe de régulation pour créer des groupes supplémentaires.

Seuil de régulation

Description

Nombre maximum de programmes associés à ce groupe qui peuvent être exécutés simultanément. Les groupes que vous spécifiez ici apparaissent dans la liste déroulante **Groupe du planificateur** dans l'interface utilisateur du planificateur pour la création et l'édition de planifications. Le groupe de régulation par défaut est défini sur 999, ce qui ne constitue en fait aucune limite. Etant donné que tous les programmes doivent appartenir à un groupe de limitation, cette valeur ne doit pas être modifiée afin que les programmes que vous ne souhaitez pas limiter puissent être affectés à ce groupe.

Valeur par défaut

Valeurs valides

Un nombre entier positif.

Unica Platform | Sécurité

La propriété de cette catégorie définit le mode de connexion pour les produits Unica.

Méthode de connexion

Description

Spécifie de la façon suivante le mode d'authentification pour tous les produits Unica installés et configurés pour fonctionner ensemble :

- Si vous spécifiez la valeur `Unica Platform` , les produits Unica utilisent Unica Platform pour l'authentification et l'autorisation.
- Si vous spécifiez la valeur `LDAP`, les produits Unica utilisent un serveur LDAP pour l'authentification.
- Si vous spécifiez la valeur `Contrôle de l'accès Web`, les produits Unica utilisent le logiciel de contrôle de l'accès Web pour l'authentification.
- Si vous définissez la valeur sur `SAML 2.0`, les produits Unica utilisent votre serveur IdP pour l'authentification.

Si vous modifiez ce paramètre, arrêtez et redémarrez l'application Web Unica Platform pour que vos modifications prennent effet.

Valeur par défaut

`Unica Platform`

Valeurs valides

`Unica Platform | LDAP | Contrôle de l'accès Web`

Unica Platform | Sécurité | Détails du mode de connexion | LDAP

Les propriétés de cette catégorie sont utilisées pour configurer l'intégration LDAP.

Nom de serveur hôte LDAP

Description

Spécifie le nom ou l'adresse IP du serveur LDAP. Définissez la valeur sur le nom ou l'adresse IP de la machine du serveur LDAP. Par exemple : `machineName.companyDomain.com`

Si vous procédez à l'intégration à Windows™ Active Directory, utilisez le nom de serveur à la place du nom DNS.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Port du serveur LDAP

Description

Spécifie le port d'écoute du serveur LDAP. Définissez la valeur sur le numéro de port approprié. En règle générale, le numéro de port est `389` (`636` si SSL est utilisé).

Valeur par défaut

`389`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Filtre de recherche utilisateur

Description

Spécifie le filtre à utiliser pour rechercher des utilisateurs. Les valeurs valides incluent n'importe quel filtre de recherche LDAP valide (voir la norme RFC 2254). Notez que vous devez ajouter des caractères d'échappement à tous les caractères XML de cette valeur.

En règle générale, la valeur de l'attribut d'identification de connexion de l'utilisateur est `uid` pour les serveurs LDAP et `sAMAccountName` pour les serveurs Windows™ Active Directory. Vérifiez cette valeur sur votre serveur LDAP ou Active Directory. Si votre serveur LDAP est Windows™ Active Directory, vous devez changer la valeur par défaut de cette propriété afin d'utiliser `sAMAccountName` à la place de `uid`. Par exemple :

```
(&(|(objectClass=user)(objectClass=person))(sAMAccountName={0}))
```

Valeur par défaut

```
(&(|(objectClass=user)(objectClass=person))(uid={0}))
```

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Utiliser les données d'identification stockées dans Unica Platform

Description

Indique si Unica Platform utilise les données d'identification de la base de données de Unica Platform pendant la recherche du serveur LDAP ou Windows™ Active Directory au cours de l'authentification d'utilisateur (lors de la connexion).

Si cette valeur est `true`, Unica Platform utilise les données d'identification de la base de données de Unica Platform et vous devez définir les valeurs appropriées pour les propriétés Utilisateur `Unica Platform pour les données d'identification LDAP` et `Source de données pour les données d'identification LDAP` de cette catégorie.

Si votre serveur LDAP ou Windows™ Active Directory n'accepte pas les accès anonymes, paramétrez cette valeur sur `true`.

Si cette valeur est paramétrée sur `false`, Unica Platform se connecte au serveur LDAP ou Windows™ Active Directory de façon anonyme. Vous pouvez paramétrer cette valeur sur `false` si votre serveur LDAP ou Windows™ Active Directory autorise l'accès anonyme.

Valeur par défaut

`false`

Valeurs valides

`true | false`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Utilisateur Unica Platform pour les données d'identification LDAP

Description

Spécifie le nom de l'utilisateur d'Unica disposant de données d'identification de connexion d'administrateur LDAP. Définissez cette valeur si vous avez affecté la valeur `true` à la propriété `Utiliser les données d'identification stockées dans Unica Platform` de cette catégorie.

Donnez à cette propriété le nom d'utilisateur créé pour l'utilisateur d'Unica lors de la configuration de l'intégration LDAP. Cette propriété fonctionne conjointement avec la propriété `Source de données pour les données d'identification LDAP` de cette catégorie.

Valeur par défaut

`asm_admin`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Source de données pour les données d'identification LDAP

Description

Spécifie la source de données Unica Platform associée aux données d'identification de l'administrateur LDAP. Définissez cette valeur si vous avez affecté la valeur `true` à la propriété`Utiliser les données d'identification stockées dans Unica Platform` de cette catégorie.

Donnez à cette propriété le nom de source de données créé pour l'utilisateur d'Unica lors de la configuration de l'intégration LDAP. Cette propriété fonctionne conjointement avec la propriété `Unica Platform utilisateur pour les données d'identification LDAP` de cette catégorie.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Nom distinctif de base

Description

Spécifie le nom unique de base qui permet d'accéder à la racine de la structure du répertoire LDAP.

Valeur par défaut

`[CHANGE ME]`

Valeurs valides

N'importe quel nom distinctif valide (voir les normes RFC 1779, RFC 2253)

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

SSL requis pour la connexion LDAP

Chemin

`Unica Platform | Sécurité | LDAP`

Description

Indique si Unica Platform utilise SSL lorsqu'il se connecte au serveur LDAP pour authentifier les utilisateurs. Si vous définissez la valeur sur `true`, la connexion sera sécurisée par le biais du protocole SSL.

Valeur par défaut

`false`

Valeurs valides

`true | false`

Platform | Sécurité | Détails du mode de connexion | Contrôle de l'accès Web

Les propriétés de cette catégorie sont utilisées pour configurer l'intégration avec les logiciels de contrôle de l'accès au Web.

Modèle de nom d'utilisateur

La description

Expression régulièreJava™ utilisée pour extraire le login de l'utilisateur à partir de la variable d'en-tête HTTP dans un logiciel de contrôle d'accès web. Notez que vous devez ajouter des caractères d'échappement à tous les caractères XML de l'expression régulière. La valeur recommandée pour SiteMinder et IBM Security Access Manager est `\w*`.

Vous devez également utiliser cette valeur lorsque vous utilisez un proxy personnalisé pour intégrer Unica Campaign hébergé sur site et Digital Analytics dans le cloud.

Valeur par défaut

Non défini

Valeurs valides

Toute expression régulière Java™.

Disponibilité

Cette propriété s'utilise uniquement lorsque Unica Platform est configuré de façon à s'intégrer au logiciel de contrôle de l'accès Web.

Variable d'en-tête du contrôle de l'accès Web

La description

Spécifie la variable d'en-tête HTTP configurée dans le logiciel de contrôle de l'accès Web, qui est soumise au serveur d'applications Web. Par défaut, SiteMinder utilise `sm_user` et IBM Security Access Manager (SAM) utilise `iv-`

`user`. Pour SAM, définissez cette valeur sur le composant nom d'utilisateur de la chaîne Raw, et non sur la chaîne HTTP.

Valeur par défaut

Non défini

Valeurs valides

N'importe quelle chaîne

Disponibilité

Cette propriété s'utilise uniquement lorsque Unica Platform est configuré de façon à s'intégrer au logiciel de contrôle de l'accès Web.

Variables d'en-tête supplémentaires

La description

Spécifie une liste, séparée par des virgules, de variables d'en-tête HTTP supplémentaires à capturer lors de la connexion au logiciel de contrôle d'accès Web. Les variables d'en-tête HTTP spécifiées sont capturées et stockées dans le journal d'audit d'authentification si les journaux d'audit sont activés.

Valeur par défaut

Non défini

Valeurs valides

Toute chaîne de caractères séparée par une virgule

Disponibilité

Cette propriété est utilisée uniquement lorsque la plate-forme Unica est configurée pour s'intégrer à un logiciel de contrôle d'accès web.

Platform | Sécurité | Détails du mode de connexion | SAML 2.0

Les propriétés de cette catégorie configurent la connexion unique via un serveur IdP SAML 2.0.

URL du serveur IdP pour la connexion unique

La description

URL de la page qui s'affiche lorsque des utilisateurs ouvrent l'URL de connexion unique dans Unica.

Valeur par défaut

[CHANGE ME]

URL du serveur IdP pour la déconnexion unique

La description

Facultatif. Lorsque des utilisateurs se déconnectent, ils peuvent être redirigés vers la page que vous définissez ici pour que leur déconnexion les déconnecte également du serveur IdP. Votre serveur IdP peut fournir une URL pour cette opération.

Valeur par défaut

[CHANGE ME]

URL de page d'erreur pour erreur de connexion unique

La description

Si une erreur se produit lors de la connexion unique en raison d'un problème de configuration ou d'intégration, les utilisateurs peuvent être redirigés vers la page spécifiée ici. Ce paramètre remplace la page d'erreur par défaut fournie par Unica Platform.

Valeur par défaut

[CHANGE ME]

URL de destination

La description

URL du fournisseur de services (application) vers laquelle l'utilisateur est redirigé après l'authentification réussie via le serveur IdP. Cette URL s'affiche dans chaque requête SAML sous la balise <AuthnRequest Destination>.

Valeur par défaut

[CHANGE ME]

URL du service consommateur

La description

URL du service consommateur d'assertion qui est utilisée et analysée par le fournisseur de services (application) pour les assertions SAML. Cette URL s'affiche dans chaque requête SAML sous la balise <AuthnRequest AssertionConsumerServiceURL>. Cette valeur peut être la même que celle de la propriété **URL de destination**.

Valeur par défaut

[CHANGE ME]

ID application

La description

ID d'application affecté à Unica Platform sur le serveur IdP. Cet ID est inclus dans chaque requête SAML au serveur IdP. Il s'affiche dans chaque requête SAML sous la balise <Issuer>.

Valeur par défaut

[CHANGE ME]

Identificateur du nom du fournisseur de services

La description

Identificateur du nom du fournisseur de services. Cet identificateur de nom s'affiche dans chaque requête SAML sous la balise <NameIDPolicy SPNameQualifier>.

Valeur par défaut

[CHANGE ME]

Chemin des métadonnées

La description

L'emplacement du fichier de métadonnées IDP sur le serveur de la plate-forme Unica. Ce fichier de métadonnées IDP est fourni par le serveur IDP.

Valeur par défaut

[CHANGE ME]

ID entité

La description

ID d'entité du serveur IdP. Définissez cette propriété à la valeur de *entityID* dans la déclaration XML en haut du fichier de métadonnées produit par le serveur IdP.

Unica Platform utilise cet ID pendant la validation de l'assertion pour charger les configurations de l'IdP et le certificat numérique.

Valeur par défaut

[CHANGE ME]

Attributs NVP pour l'analyse syntaxique des réponses

La description

Des attributs de compte utilisateur sont envoyés à Unica Platform par le serveur IdP. Vous pouvez utiliser cette propriété de configuration pour capturer les attributs des utilisateurs créés dans Unica Platform automatiquement, lorsque la propriété **Ajouter des utilisateurs authentifiés à la plate-forme** est activée.

Le serveur IdP peut utiliser un autre nom pour un attribut que celui utilisé par Unica Platform. Vous pouvez utiliser cette propriété pour mapper l'attribut IdP vers l'attribut correspondant dans Unica Platform. Cette opération élimine le besoin de modifier le code.

Par exemple, le serveur IdP peut utiliser **emailAddress** comme nom pour un attribut nommé **Email** dans Unica Platform. Vous devez entrer **Email=emailAddress** comme valeur dans cette propriété pour mapper l'attribut.

Utilisez les valeurs suivantes pour les attributs utilisateur dans Unica Platform.

- FirstName
- Nom
- Service
- Organisation
- Pays
- Adresse e-mail
- Adresse 1
- Adresse 2
- Téléphone 1

  Travail
- Téléphone 2

  Portable
- Téléphone 3

  Domicile
- AltLogin
- ExternalUsersGroup

  Si vous activez la propriété **Ajouter des utilisateurs authentifiés à Unica Platform** , un utilisateur authentifié à partir du serveur IdP est créé dans Unica Platform si cet utilisateur n'a pas encore de compte Unica Platform. Ces utilisateurs sont automatiquement ajoutés à un groupe d'utilisateurs par défaut, **ExternalUsersGroup**. Toutefois, vous pouvez également spécifier un groupe personnalisé auquel vous ajoutez des utilisateurs. Si vous mettez en œuvre cette option, définissez la valeur de l'attribut **ExternalUsersGroup** sur le nom du groupe d'utilisateurs personnalisé. Par exemple, si vous voulez qu'un utilisateur soit ajouté à

un nom de groupe identifié par l'attribut SAML MyGroup, vous définissez cette valeur comme **ExternalUsersGroup=MyGroup.** Les utilisateurs seront ajoutés au nom du groupe qui est spécifié dans l'attribut SAML MyGroup.

Séparez les paires nom-valeur par des point-virgules.

Valeur par défaut

```
omit-xml-declaration=yes ;
```

Traitement d'une réponse IdP chiffrée

La description

Si votre serveur IdP est configuré pour envoyer des réponses chiffrées, activez cette propriété pour indiquer que la réponse SAML du serveur IdP doit être chiffrée à l'aide de la clé partagée configurée avant que Unica Platform ne la traite.

Si vous activez cette propriété, vous devez également définir la valeur de **Clé secrète partagée** sur la clé secrète utilisée pour déchiffrer la réponse.

Valeur par défaut

```
Désactivé
```

Clé secrète partagée

La description

Lorsque l'option **Traiter la réponse IdP chiffrée** est activée, définissez cette valeur de propriété sur le chemin du fichier keystore.

Valeur par défaut

```
[CHANGE ME]
```

Détenteur des données d'identification du magasin de clés

La description

Définissez cette valeur sur le nom de connexion du compte utilisateur Unica qui détient le secret partagé SAML dans une source de données.

Valeur par défaut

[CHANGE ME]

Source des données d'identification du magasin de clés

La description

Définissez cette valeur sur le nom de la source de données créée pour maintenir le secret partagé utilisé pour le chiffrement. Le mot de passe de la source de données est le mot de passe du fichier de clés.

Valeur par défaut

[CHANGE ME]

Alias de certificat

La description

Lorsque l'option **Traiter la réponse IdP chiffrée** est activée, définissez cette valeur de propriété sur l'alias de certificat de la clé privée stockée dans le fichier keystore. Il est utilisé pour déchiffrer la réponse SAML chiffrée envoyée par le serveur IDP.

Valeur par défaut

[CHANGE ME]

Ajouter des utilisateurs authentifiés à Platform

La description

Lorsque cette option est activée, un utilisateur authentifié à partir du serveur IdP est créé dans Unica Platform, s'il ne dispose pas déjà d'un compte Unica Platform.

Les utilisateurs nouvellement créés sont automatiquement ajoutés à un groupe par défaut, **ExternalUsersGroup**.

Le **ExternalUsersGroup** ne possède que le Unica Platform **UserRole**. Un administrateur doit accorder des droits supplémentaires aux utilisateurs nouvellement créés pour qu'ils puissent accéder aux produits Unica et les utiliser. Il peut accorder des droits supplémentaires en rendant les utilisateurs membres de groupes avec différents niveaux d'accès aux applications.

Sinon, la réponse SAML peut contenir un nom de groupe d'utilisateurs personnalisé, et les utilisateurs nouvellement créés sont ajoutés à ce groupe.

Lorsque cette option est activée, un utilisateur authentifié à partir du serveur IdP ne peut pas accéder à Unica Platform s'il ne dispose pas d'un compte dans Unica Platform.

Valeur par défaut

`Désactivé`

Redirection vers la connexion unique

La description

Lorsque cette valeur est **True**:

- Les utilisateurs qui se connectent à Unica sont redirigés vers la page de connexion unique IdP.
- Une fois les utilisateurs connectés, ils accèdent à la page d'arrivée Unica Platform standard.
- L'écran de connexion standard de Unica Platform n'est jamais disponible.

Note :

- **Définition du format de nameID**

  Par défaut, la demande SAML est générée avec le format nameID comme transitoire. Si vous souhaitez construire une demande SAML avec un format nameID persistant, vous devez définir ce paramètre JVM.

  `-DENABLE_PERSISTENT_NAMEID_FORMAT=true`

- **Configuration de la création d'un utilisateur authentifié SAML pour une partition non par défaut**

  Si vous activez la propriété `Ajouter des utilisateurs authentifiés à Unica Platform`, un utilisateur authentifié à partir du serveur IdP est créé dans Unica Platform si cet utilisateur n'a pas encore de compte Unica Platform. Ces utilisateurs sont automatiquement ajoutés sous la partition par défaut, c'est-à-dire sous la partition avec l'ID 1.

  Cependant, si vous voulez qu'un utilisateur soit ajouté sous une partition différente, cela doit être spécifié comme attribut SAML.

  Exemple : `PartitionId=<partitionid>`
- **Configuration de RequestedAuthnContext dans la demande SAMLSi vous activez la propriété Add authenticated users to Unica Platform, un utilisateur authentifié à partir du serveur IdP est créé dans Unica Platform si cet utilisateur n'a pas déjà un compte Unica Platform.**

  Par défaut, la demande SAML est générée avec `RequestedAuthnContext` dans la demande SAML.

  Certains serveurs IDP n'exigent pas `RequestedAuthnContext` dans la demande SAML. Pour le supprimer de la demande, vous devez définir ce paramètre JVM.

  ```
  -REMOVE_REQUESTED_AUTHN_CONTEXT=true
  ```

Platform | Sécurité | Synchronisation LDAP

Les propriétés de synchronisation LDAP définissent les détails qui sont utilisés par le système pour se connecter au serveur d'annuaire et pour identifier les utilisateurs à importer. Certaines de ces propriétés contrôlent également la fréquence et les autres détails du processus de synchronisation automatique.

Synchronisation LDAP activée

Description

Définissez la valeur sur `true` pour activer la synchronisation LDAP ou Active Directory.

Valeur par défaut

`false`

Valeurs valides

`true | false`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Intervalle de synchronisation LDAP

Description

Unica Platform entre en synchronisation avec le serveur LDAP ou Active Directory à intervalles réguliers (exprimés en secondes). Si la valeur est inférieure ou égale à zéro, Unica Platform n'effectue pas de synchronisation. Si la valeur est paramétrée sur un nombre entier positif, la nouvelle valeur prendra effet dans les 10 prochaines minutes sans qu'il devoir redémarrer le système. Les changements ultérieurs prennent effet dans le laps de temps configuré.

Valeur par défaut

`600`, soit 10 minutes

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Retard de synchronisation LDAP

Description

Laps de temps (au format 24 heures) après lequel la synchronisation périodique avec le serveur LDAP commence dès lors que Unica Platform est

lancé. Par exemple, un `Délai de synchronisation LDAP` défini sur 23:00 et un `Intervalle de synchronisation LDAP` défini sur 600 signifie que lorsque Unica Platform est démarré, la synchronisation périodique s'exécute toutes les 10 minutes (600 secondes) à partir de 23 heures.

Valeur par défaut

`23:00`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Délai de synchronisation LDAP

Description

La propriété d'expiration de synchronisation du LDAP spécifie un délai maximal en minutes à partir du début d'une synchronisation, et avant que Unica Platform ne marque la fin du processus. Platform ne permet l'exécution que d'un seul processus de synchronisation à la fois. En cas d'échec d'une synchronisation, celle-ci est marquée comme étant terminée dans tous les cas.

Ceci s'avère particulièrement utile dans le cadre d'un environnement en clusters. Par exemple, si Unica Platform est déployé au sein d'un cluster, un serveur du cluster peut lancer une synchronisation LDAP et se déconnecter avant que le processus ne soit considéré comme étant terminé. Dans ce cas, Unica Platform attend le temps spécifié au niveau de cette propriété avant de lancer la prochaine synchronisation planifiée.

Valeur par défaut

`600`, (600 minutes ou dix heures)

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Portée de la synchronisation LDAP

Description

Contrôle la portée de la requête initiale pour récupérer l'ensemble des utilisateurs. Il est conseillé de conserver la valeur par défaut, SUBTREE, pour permettre la synchronisation avec la plupart des serveurs LDAP.

Valeur par défaut

SUBTREE

Valeurs valides

Les valeurs sont des termes de recherche LDAP standard.

- OBJECT : recherche uniquement l'entrée au niveau du nom distinctif de base. Ainsi, seule cette entrée est renvoyée.
- ONE_LEVEL : recherche toutes les entrées un niveau en dessous du nom distinctif de base sans inclure celui-ci.
- SUBTREE : recherche toutes les entrées à tous les niveaux en dessous du nom distinctif de base spécifié en incluant celui-ci.

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

URL du fournisseur LDAP

Description

Pour la plupart des mises en oeuvre, vous pouvez définir l'URL du serveur LDAP ou Active Directory pour qu'il se présente sous l'une des formes suivantes :

- `ldap://IP_address:port_number`
- `ldap://nom_machine.domaine.com:numéro_port`

En règle générale, le numéro de port des serveurs LDAP est `389` (`636` si SSL est utilisé).

Si Unica est intégré à un serveur Active Directory et que votre mise en oeuvre Active Directory emploie une liaison sans serveur, configurez l'URL de votre serveur Active Directory en tant que valeur pour cette propriété, à l'aide de la formule suivante :

```
ldap:///dc=exemple,dc=com
```

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

SSL requis pour la connexion LDAP

Chemin

`Platform | Sécurité | Synchronisation LDAP`

Description

Indique si Unica Platform utilise SSL lorsqu'il se connecte au serveur LDAP pour synchroniser les utilisateurs. Si vous définissez la valeur sur `true`, la connexion sera sécurisée par le biais du protocole SSL.

Valeur par défaut

`false`

Valeurs valides

`true | false`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Délimiteur de groupe Unica Platform de configuration LDAP

Description

Dans la catégorie `Référence LDAP au mappage du groupe  Unica Platform`, si vous souhaitez mapper un groupe LDAP ou Active Directory à plusieurs groupes Unica Platform, utilisez le délimiteur spécifié ici. Il peut s'agir de n'importe quel caractère unique ne figurant pas dans les noms qu'il sépare.

Valeur par défaut

`;` (point-virgule)

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Délimiteur de configuration de référence LDAP

Description

Spécifie le délimiteur qui sépare les composants `SEARCHBASE` et `FILTER`, qui permettent de créer la référence LDAP ou Active Directory (comme décrit dans la catégorie `Références LDAP pour création d'utilisateur  Unica Platform`).

`FILTER` est facultatif : si vous l'omettez, le serveur Unica Platform crée le filtre de façon dynamique d'après la valeur de la propriété `Nom d'attribut de référence de l'utilisateur LDAP`.

Valeur par défaut

`;` (point-virgule)

Valeurs valides

N'importe quel caractère unique ne figurant pas dans les noms qu'il sépare.

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Utilisateur Unica Platform pour les données d'identification LDAP

Description

Spécifie le nom de l'utilisateur Unica disposant de données d'identification de connexion d'administrateur LDAP.

Donnez à cette propriété le nom d'utilisateur créé pour l'utilisateur d'Unica lors de la configuration de l'intégration LDAP. Cette propriété fonctionne conjointement avec la propriété `Source de données pour les données d'identification LDAP` de cette catégorie.

Valeur par défaut

`asm_admin`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Source de données pour les données d'identification LDAP

Description

Spécifie la source de données Unica Platform associée aux données d'identification de l'administrateur LDAP.

Donnez à cette propriété le nom de source de données créé pour l'utilisateur d'Unica lors de la configuration de l'intégration LDAP. Cette propriété fonctionne conjointement avec la propriété `Unica Platform utilisateur pour les données d'identification LDAP` de cette catégorie.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Nom d'attribut de référence de l'utilisateur LDAP

Description

Pour l'importation d'utilisateurs basée sur un groupe, cette propriété est définie sur le nom que le serveur LDAP ou Active Directory utilise comme attribut utilisateur dans l'objet Groupe. En général, la valeur est `uniquemember` pour les serveurs LDAP et `member` pour les serveurs Windows™ Active Directory.

Pour l'importation d'utilisateurs basée sur un attribut, définissez cette propriété sur `DN`, puis, lorsque vous configurez la propriété **Mappe de référence LDAP**, définissez la partie FILTER de la valeur sur la chaîne utilisée par le serveur LDAP pour l'attribut à rechercher.

Valeur par défaut

`member`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Recherche périodique de nom distinctif de base LDAP désactivée

Description

Quand cette propriété a la valeur `True`, Unica Platform exécute la recherche de synchronisation LDAP avec le nom distinctif défini dans la propriété `Nom distinctif de base`, dans la catégorie **Unica Platform | Sécurité | LDAP**. Quand cette propriété a la valeur `False`, Unica Platform exécute la recherche de synchronisation LDAP avec les groupes mappés aux groupes LDAP définis dans **Référence LDAP à la mappe du groupe Unica Platform**.

Le tableau suivant indique si les modifications sont prélevées lors de la synchronisation périodique, selon la valeur définie pour cette propriété.

Tableau 76. Effet de cette propriété sur le comportement de la synchronisation périodique

Modifier	La modification est-elle prélevée lorsque la valeur est True ?	La modification est-elle prélevée lorsque la valeur est False ?
Dans Unica Platform, suppression d'un utilisateur synchronisé à partir du serveur LDAP	Oui	Non
Suppression d'un utilisateur d'un groupe LDAP mappé à un groupe Unica Platform	Non	Non
Dans Unica Platform, suppression d'un utilisateur d'un groupe Unica Platform mappé à un groupe LDAP.	Non	Non
Ajout d'un nouvel utilisateur au serveur LDAP La modification est uniquement utilisée lorsque la méthode de connexion configurée est LDAP. Si la méthode de connexion est LDAP, le système importera de nouveaux utilisateurs à partir de LDAP via la synchronisation automatique.	Oui	Oui
Ajout d'un utilisateur à un groupe LDAP mappé à un groupe Unica Platform	Oui	Non

Tableau 76. Effet de cette propriété sur le comportement de la synchronisation périodique (suite)

Modifier	La modification est-elle prélevée lorsque la valeur est True ?	La modification est-elle prélevée lorsque la valeur est False ?
Modification des attributs utilisateur sur le serveur LDAP	Oui	Oui

Valeur par défaut

`Faux`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Connexion utilisateur

Description

Mappe le nom de connexion de l'utilisateur Unica à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory. `Connexion de l'utilisateur` est le seul mappage requis. En général, la valeur de cet attribut est `uid` pour les serveurs LDAP et `sAMAccountName` pour les serveurs Windows™ Active Directory. Vérifiez cette valeur sur votre serveur LDAP ou Active Directory.

Valeur par défaut

`uid`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Prénom

Description

Mappe l'attribut utilisateur Prénom utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

`givenName`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Nom

Description

Mappe l'attribut utilisateur Nom utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

`sn`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Titre de l'utilisateur

Description

Mappe l'attribut utilisateur Titre de l'utilisateur utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

`title`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Service

Description

Mappe l'attribut utilisateur Service utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Société

Description

Mappe l'attribut utilisateur Société utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Pays

Description

Mappe l'attribut utilisateur Pays utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Adresse e-mail de l'utilisateur

Description

Mappe l'attribut Adresse e-mail de l'utilisateur utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

`mail`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Adresse 1

Description

Mappe l'attribut utilisateur Adresse utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Téléphone bureau

Description

Mappe l'attribut utilisateur Téléphone bureau utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

`telephoneNumber`

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Téléphone cellulaire

Description

Mappe l'attribut utilisateur Téléphone mobile utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Téléphone du domicile

Description

Mappe l'attribut utilisateur Téléphone domicile utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Autre identification de connexion

Description

Mappe l'attribut utilisateur Autre de connexion utilisé dans Unica Platform à l'attribut utilisateur équivalent de votre serveur LDAP ou Active Directory.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Platform | Sécurité | Synchronisation LDAP | Référence LDAP à la mappe du groupe Unica Platform

Les propriétés de cette catégorie sont utilisées pour configurer l'intégration LDAP.

Mappage de référence LDAP

Description

Les utilisateurs membres du groupe LDAP ou Active Directory spécifié ici sont importés vers le groupe de Unica Platform spécifié dans la propriété `Unica PlatformGroupe`.

Paramétrez la valeur de cette propriété en observant la syntaxe suivante : `SEARCHBASE DELIMITER FILTER` où :

`SEARCHBASE` est le nom unique (DN) de l'objet.

`DELIMITER` est la valeur de la propriété `Délimiteur de groupe Unica de configuration LDAP`.

`FILTER` est le filtre d'attribut de LDAP ou d'Active Directory. `FILTER` est facultatif lorsque vous utilisez l'importation basée sur le groupe : si vous l'omettez, le serveur Unica Platform crée le filtre de façon dynamique d'après la valeur de la propriété `Nom d'attribut de référence de l'utilisateur LDAP`.

Si vous utilisez une importation basée sur un attribut, définissez la valeur de `FILTER` sur la chaîne utilisée par le serveur LDAP pour les attributs à rechercher. Vous devez également affecter à la propriété **Nom d'attribut de référence de l'utilisateur LDAP** la valeur `DN`.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Unica Platform groupe

Description

Les utilisateurs membres du groupe LDAP ou Active Directory spécifié dans la propriété `Groupe de référence LDAP` sont importés vers le groupe de Unica Platform spécifié ici.

Valeur par défaut

Non défini

Disponibilité

Cette propriété est utilisée uniquement lorsque Unica Platform est configuré de façon à s'intégrer dans un serveur Windows™ Active Directory ou LDAP.

Platform | Sécurité | Authentification fédérée

Les propriétés de cette catégorie sont utilisées pour implémenter l'authentification fédérée basée sur SAML (Security Assertion Markup Language) 2.0, qui active la fonction de connexion unique entre les diverses applications.

Allow federated login (Autoriser la connexion fédérée)

Description

Cochez la case présente dans cette propriété pour activer l'authentification fédérée dans un environnement intégré.

Valeur par défaut

Désactivé

Identity provider URL (URL du fournisseur d'identité)

Description

URL du serveur du fournisseur d'identité.

Certificate issuer (Emetteur du certificat)

Description

URL de l'autorité de certification qui a émis le certificat sur le serveur du fournisseur d'identité. Si vous générez vos propres certificats à l'aide de l'utilitaire Java™ keytool, définissez cette valeur sur l'URL du serveur d'identité.

Platform | Sécurité | Authentification fédérée | partitions | partition[n]

Les propriétés de cette catégorie sont utilisées dans l'implémentation de l'authentification fédérée SAML (Security Assertion Markup Language) 2.0 entre les applications Unica et d'autres applications d' et d'autres fournisseurs.

Chemin du magasin de clés

Description

L'emplacement du fichier de clés certifiées dans le serveur d'applications Web.

Clé d'accès du fichier de clés

Description

Clé d'accès du fichier de clés dans le serveur d'applications Web.

Alias du fichier de clés

Description

Alias du fichier de clés dans le serveur d'applications Web.

Unica Platform | Sécurité | Gestion de l'API

Les propriétés de cette catégorie configurent le comportement d'authentification qui s'applique à toutes les API Unica.

Activer l'authentification de l'API par session

Description

Si vous cochez la case correspondant à cette propriété pour l'activer, les utilisateurs qui sont authentifiés en se connectant à Unica n'ont pas à se reconnecter lorsqu'ils accèdent à une API sécurisée à partir d'une application Unica pendant la session pour laquelle ils sont authentifiés.

Par exemple, lorsque cette propriété est activée, et qu'un utilisateur Unica Interact authentifié appelle une API Unica Campaign pendant sa session, aucune autre connexion n'est requise.

Valeur par défaut

Désactivé

Supprimer le jeton de sécurité après une utilisation

Description

Si vous cochez la case correspondant à cette propriété pour l'activer, le jeton généré pour un utilisateur authentifié est détruit lorsqu'il est utilisé pour la première fois pour accéder à une API sécurisée. Cette opération permet d'améliorer la sécurité en empêchant toute autre utilisation du jeton.

Valeur par défaut

Activé

Platform | Sécurité | Gestion de l'API | [Produit] | (Modèle de configuration de l'API)

Utilisez les modèles de cette catégorie pour configurer l'authentification des API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

Non défini

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Désactivé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Unica Platform | Sécurité | Gestion de l'API | [Produit] | Unica Platform | Authentification

(Affinium|suite|security|apiSecurity|manager|managerAuthentication)Utilisez les modèles de cette catégorie pour configurer l'authentification pour les API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

/authentication/login

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Désactivé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Related information

Infrastructure de sécurité des API Unica *(on page 258)*

Unica Platform | Sécurité | Gestion de l'API | [Produit] | Unica Platform | Utilisateur

(Affinium|suite|security|apiSecurity|manager|managerUser)Utilisez les modèles de cette catégorie pour configurer l'authentification pour les API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

/user/partitions/*

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Activé)

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Activé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est

valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Related information

Infrastructure de sécurité des API Unica *(on page 258)*

Unica Platform | Sécurité | Gestion de l'API | [Produit] | Unica Platform | Stratégie

(Affinium|suite|security|apiSecurity|manager|managerPolicy)Utilisez les modèles de cette catégorie pour configurer l'authentification pour les API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

/policy/partitions/*

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Activé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Related information

Infrastructure de sécurité des API Unica *(on page 258)*

Unica Platform | Sécurité | Gestion de l'API | [Produit] | Unica Platform | Configuration

(Affinium|suite|security|apiSecurity|manager|managerConfiguration)Utilisez les modèles de cette catégorie pour configurer l'authentification pour les API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

/datasource/config

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Activé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est

valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Related information

Infrastructure de sécurité des API Unica *(on page 258)*

Unica Platform | Sécurité | Gestion de l'API | [Produit] | Unica Platform | Source de données

(Affinium|suite|security|apiSecurity|manager|managerDatasource)Utilisez les modèles de cette catégorie pour configurer l'authentification pour les API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

/datasource

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Activé)

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Activé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Related information

Infrastructure de sécurité des API Unica *(on page 258)*

Unica Platform | Sécurité | Gestion de l'API | [Produit] | Unica Platform | Connexion

(Affinium|suite|security|apiSecurity|manager|managerLogin)Utilisez les modèles de cette catégorie pour configurer l'authentification pour les API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

/authentication/v1/login

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Désactivé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est

valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Related information

Infrastructure de sécurité des API Unica *(on page 258)*

Unica Platform | Sécurité | Gestion de l'API | [Produit] | Unica Marketing Campaign | Collection Interact

(Affinium|suite|security|apiSecurity|campaign|Interact Collection)Utilisez les modèles de cette catégorie pour configurer l'authentification pour les API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

/rest/v1/interactCollection/*

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Désactivé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Related information

Infrastructure de sécurité des API Unica *(on page 258)*

Unica Platform | Sécurité | Gestion de l'API | [Produit] | Unica Marketing Campaign | Messages déclenchés

(Affinium|suite|security|apiSecurity|campaign|Interact Collection)Utilisez les modèles de cette catégorie pour configurer l'authentification pour les API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

/rest/v1/triggeredMessages/*

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Désactivé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est

valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Related information

Infrastructure de sécurité des API Unica *(on page 258)*

Unica Platform | Sécurité | Gestion de l'API | [Produit] | Unica Marketing Campaign | Filtre d'API REST Campaign

(Affinium|suite|security|apiSecurity|campaign|Campaign REST API Filter)Utilisez les modèles de cette catégorie pour configurer l'authentification pour les API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

/rest/v1/*

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Activé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Related information

Infrastructure de sécurité des API Unica *(on page 258)*

Unica Platform | Sécurité | Gestion de l'API | [Produit] | Unica Marketing Campaign | Filtre d'API REST Engage

(Affinium|suite|security|apiSecurity|campaign|Engage REST API Filter)Utilisez les modèles de cette catégorie pour configurer l'authentification pour les API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

/rest/engage/*

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Désactivé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est

valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Related information

Infrastructure de sécurité des API Unica *(on page 258)*

Unica Platform | Sécurité | Gestion de l'API | [Produit] | Unica Marketing Campaign | Filtre d'API REST Campaign V2

(Affinium|suite|security|apiSecurity|campaign|Campaign REST API V2 Filter)Utilisez les modèles de cette catégorie pour configurer l'authentification pour les API Unica. Vous pouvez bloquer l'accès, exiger l'utilisation du protocole HTTPS ou exiger l'authentification des API.

URI de l'API

La description

Pour chaque produit, la première partie de l'URI est résolue par le cadre de sécurité, comme suit: `http[s]://host:port/context root/api/product`

Par conséquent, vous ne devez entrer dans cette zone que le ou les noms de ressource de l'API que vous souhaitez configurer. Vous pouvez obtenir la chaîne que vous devez entrer dans la documentation d'API du produit.

La valeur utilisée pour cette propriété doit commencer par une barre oblique (/). Si ce n'est pas le cas, la configuration est ignorée par l'infrastructure de sécurité.

Cette propriété prend en charge une correspondance exacte d'URL ainsi qu'une correspondance de critères pour les API configurées.

- Pour une correspondance exacte, l'URI peut se terminer par une barre oblique (/) ou le nom de la ressource.
- Pour un correspondance de critères, l'URI doit se terminer par un astérisque (*).

Si vous définissez la valeur de cette propriété sur `/*` les paramètres que vous utilisez pour les autres propriétés de la catégorie s'appliquent à toutes les API du produit.

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est en lecture seule.

Valeur par défaut

/rest/v2/*

Bloquer l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez empêcher une API d'accéder à un produit. Cette option n'est pas sélectionnée par défaut.

Lorsqu'une API est bloquée, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Sécuriser l'accès à l'API sur HTTPS

La description

Sélectionnez cette option lorsque vous souhaitez autoriser l'API à accéder à un produit uniquement sur HTTPS. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible sur HTTP plutôt que sur HTTPS, le filtre de sécurité renvoie le code de statut HTTP 403 (interdit).

Valeur par défaut

(Désactivé)

Demander l'authentification pour l'accès à l'API

La description

Sélectionnez cette option lorsque vous souhaitez authentifier une API avant d'accéder à un produit. Cette option est sélectionnée par défaut.

Lorsqu'une API avec cette propriété activée est accessible avec des données d'identification invalides, le filtre de sécurité renvoie le code de statut HTTP 401 (non autorisé).

Note : Pour l'API Unica Platform`connexion`, cette propriété de configuration est désactivée, car cette API est la première à être appelée pour l'authentification de l'API.

Valeur par défaut

(Activé)

Mode d'authentification

La description

Sélectionnez cette option lorsque vous souhaitez authentifier l'API avec l'authentification de base ou l'authentification par jeton porteur. Lorsque l'authentification de base ou le jeton porteur est sélectionné, l'identifiant et le mot de passe correspondants doivent être conservés dans la source de données de l'utilisateur. Pour le mode d'authentification Manager, il se comporte de la même manière en utilisant le paramètre `api_auth_mode = Manager` dans l'en-tête de la demande. Cette sélection déroulante n'est valable que si l'option "Exiger une authentification pour l'accès à l'API" est sélectionnée.

Valeur par défaut

Gestionnaire

Détenteur de l'accréditation de la source de données

La description

Spécifiez le nom de l'utilisateur, qui contient la source de données avec les informations d'authentification requises. La source de données contient l'identifiant et le mot de passe de l'utilisateur si l'authentification de base est sélectionnée dans la liste déroulante du mode d'authentification. La source de données contient le jeton du porteur si le jeton du porteur est sélectionné dans la liste déroulante du mode d'authentification.

Valeur par défaut

asm_admin

Source de données

La description

Spécifiez le nom de la source de données qui est créée sous l'utilisateur spécifié dans 'Data source credential holder'.

Valeur par défaut

API_SECRET_DS

Related information

Infrastructure de sécurité des API Unica *(on page 258)*

Platform | Sécurité | Authentification JWT

L'authentification JWT est utilisée pour Journey Designer+Unica Campaign. Elle permet la connexion unique pour toutes les applications.

Enable JWT authentication

Description

Lorsque la case de cette propriété est cochée, l'authentification JWT est activée.

Cette propriété n'est valable que dans les environnements dans lesquels Journey Designer est intégré à Unica Campaign.

Valeur par défaut

`disabled`

JWT service URL

Description

URL du service JWT. Cette valeur diffère selon que vous avez appliqué ou non le groupe de correctifs de Unica Platform 10.0.0.1.

- Si vous n'avez **pas** appliqué le groupe de correctifs 10.0.0.1 :

  `http://IP_ADDRESS/jwt/api/v1/tokens`

- Si vous avez appliqué le groupe de correctifs 10.0.0.1 :

  `http://IP_ADDRESS/api/v1/keys`

Cette propriété n'est valable que dans les environnements dans lesquels Journey Designer est intégré à Unica Campaign.

JWT shared secret

Description

Clé secrète partagée qui est envoyée depuis Unica Platform au service JWT pour l'authentification. Cette clé est partagée entre Unica Platform et Journey Designer. L'émetteur JWT est mappé vers le secret partagé JWT dans le service JWT.

Cette propriété n'est valable que dans les environnements dans lesquels Journey Designer est intégré à Unica Campaign, et dans lesquels la version de Unica Platform est 10.0.0.0 (c'est-à-dire dans lesquels le groupe de correctifs de Unica Platform 10.0.0.1 n'a **pas** été appliqué).

JWT issuer

Description

Nom et version de l'émetteur envoyés depuis Unica Platform au service JWT pour l'authentification.

Cette propriété n'est valable que dans les environnements dans lesquels Journey Designer est intégré à Unica Campaign.

Platform | Notifications

Les propriétés de cette catégorie contrôlent le comportement du système concernant les notifications que les produits Unica peuvent envoyer aux utilisateurs.

Nombre de jour de conservation des alertes

Description

Spécifie la durée en jours pendant laquelle une alerte système est conservée dans l'historique du système après sa date d'expiration, laquelle est fournie par l'application ayant envoyé l'alerte. Lorsque l'ancienneté d'une alerte dépasse le nombre de jours défini, l'alerte est supprimée du système.

Valeur par défaut

`90`

Fréquence d'envoi des e-mails (en minutes)

Description

Indique le délai en minutes pendant lequel le système attend avant d'envoyer des nouveaux courriers électroniques de notification.

Valeur par défaut

`30`

Nombre maximal de nouvelles tentatives pour l'envoi des e-mails

Description

Indique le nombre de tentatives que le système doit effectuer lorsque le premier envoi d'un courrier électronique de notification échoue.

Valeur par défaut

`1`

Platform | Evénements d'audit

La propriété figurant dans cette page détermine si un suivi des événements d'audit est réalisé.

L'audit d'événements est-il activé ?

Description

Indique si les événements d'audit bénéficient d'un suivi.

Valeur par défaut

`Faux`

Valeurs valides

`True | False`

Platform | Evénements d'audit | Configuration des événements d'audit

Les événements que vous sélectionnez dans cette page sont disponibles dans les rapports d'audit de sécurité.

Record login and logout events for all accounts (Enregistrer les événements de connexion et déconnexion pour tous les comptes)

Description

Indique s'il faut effectuer le suivi du nom d'utilisateur ainsi que de la date et de l'heure pour les événements de connexion et déconnexion pour tous les comptes utilisateur.

Record when user sessions time out for all accounts (Enregistrer lorsque les sessions utilisateur dépassent le délai pour tous les comptes)

Description

Indique s'il faut effectuer le suivi du nom d'utilisateur du compte ainsi que de la date et l'heure des sessions qui sont automatiquement mises hors délai.

Record login and logout events for members of the HighSeverityAccounts group (Enregistrer les événements de connexion et déconnexion des membres du groupe HighSeverityAccounts)

Description

Indique s'il faut effectuer le suivi du nom d'utilisateur ainsi que de la date et de l'heure des événements de connexion et déconnexion des comptes qui sont

membres du groupe **highSeverityAccounts** dans Unica Platform. Pour activer cette fonction, vous devez définir un niveau de gravité pour cette propriété de configuration et ajouter des utilisateurs au groupe highSeverityAccounts.

Record LDAP group membership changes (Enregistrer les changements d'appartenance au groupe LDAP)

Description

Indique s'il faut enregistrer l'ajout ou la suppression de comptes, ainsi que les noms d'utilisateur et la date et l'heure de ces actions, pour les comptes utilisateur synchronisés à partir d'un serveur LDAP. Cette propriété s'applique uniquement lorsque Unica Platform est intégré à un serveur LDAP pris en charge, tel que le serveur IBM Security Directory ou Windows™ Active Directory.

Record when accounts are enabled and disabled (Enregistrer l'activation ou la désactivation des comptes)

Description

Indique s'il faut enregistrer le nom d'utilisateur du compte ainsi que la date et l'heure d'activation et de désactivation des comptes.

Record when account passwords change (Enregistrer le changement des mots de passe de compte)

Description

Indique s'il faut enregistrer le nom d'utilisateur du compte ainsi que la date et l'heure de changement des mots de passe utilisateur.

Record when account passwords are locked (Enregistrer le verrouillage des mots de passe de compte)

Description

Indique s'il faut enregistrer le nom d'utilisateur du compte ainsi que la date et l'heure de verrouillage d'un mot de passe en cas de dépassement du nombre maximum d'échecs de connexion.

Record when groups are created or deleted in Platform (Enregistrer la création ou la suppression de groupes dans Platform)

Description

Indique s'il faut enregistrer l'ajout ou la suppression de groupes.

Record Platform group membership changes (Enregistrer les changements d'appartenance aux groupes Platform)

Description

Indique s'il faut enregistrer l'ajout ou la suppression de comptes utilisateur dans un groupe.

Record Platform group permission changes (Enregistrer les changements des droits des groupes Platform)

Description

Indique s'il faut enregistrer les changements de droits des groupes.

Record role creation or deletion (Enregistrer la création ou la suppression de rôles)

Description

Indique s'il faut enregistrer l'ajout ou la suppression de rôles. Seuls les rôles affichés sur la page **Paramètres > Rôles utilisateur et autorisations** font l'objet d'un suivi.

Record role membership changes (Enregistrer les changements d'appartenance à un rôle)

Description

Indique s'il faut enregistrer les changements d'appartenance à un rôle. Seuls les rôles affichés sur la page **Paramètres > Rôles utilisateur et autorisations** font l'objet d'un suivi.

Record role permission changes (Enregistrer les changements de droits des rôles)

Description

Indique s'il faut enregistrer les changements de droits des rôles. Seuls les rôles affichés sur la page **Paramètres > Rôles utilisateur et autorisations** font l'objet d'un suivi.

Record changes to properties on the configuration page (Enregistrer les changements de propriétés dans la page de configuration)

Description

Indique s'il faut enregistrer les changements des propriétés de configuration dans la page **Paramètres > Configuration**. Les changements effectués par les utilisateurs dans la page Configuration ou par les utilisateurs exécutant `configTool` font l'objet d'un suivi. Par contre, les changements de configuration effectués par les programmes d'installation lors de l'installation ou de la mise à niveau ne sont pas suivis.

Enable audit backup (Activer la sauvegarde d'audit)

Description

Indique s'il faut sauvegarder les données d'audit dans la table `USM_AUDIT_BACKUP`.

Important : Etant donné qu'il s'agit d'une propriété d'amorce qui est lue au démarrage de l'application Web Unica Platform, vous devez arrêter puis redémarrer l'application Web Unica Platform lorsque vous modifiez la valeur de cette propriété.

Valeur par défaut

`Faux`

Valeurs valides

`True | False`

Archive data after the number of days specified here (Archiver les données à l'issue du nombre de jours indiqué ici)

Description

Indique l'intervalle, en jours, entre les sauvegardes d'audit. Les données archivées sont stockées dans la table `USM_AUDIT_BACKUP` et peuvent être incluses dans le rapport d'événements d'audit (Audit Events) lorsque vous définissez une plage de dates personnalisée incluant des données provenant de l'archive.

Important : Etant donné qu'il s'agit d'une propriété d'amorce qui est lue au démarrage de l'application Web Unica Platform, vous devez arrêter puis redémarrer l'application Web Unica Platform lorsque vous modifiez la valeur de cette propriété.

Keep Audit records in primary for number days specified here (Conserver les enregistrements d'audit pendant le nombre de jours indiqué ici)

Description

Indique le nombre de jours de données à conserver dans la table `USM_AUDIT` pour le rapport d'événements d'audit. Lorsque ce rapport est défini par ses paramètres par défaut, seules les données de la table `USM_AUDIT` sont affichées dans le rapport.

Important : Etant donné qu'il s'agit d'une propriété d'amorce qui est lue au démarrage de l'application Web Unica Platform, vous devez arrêter puis redémarrer l'application Web Unica Platform lorsque vous modifiez la valeur de cette propriété.

Archive start time (Archiver l'heure de début)

Description

Indique l'heure à laquelle le système déplace les données d'audit dans une archive. Utilisez un format 24 heures pour cette valeur.

Important : Etant donné qu'il s'agit d'une propriété d'amorce qui est lue au démarrage de l'application Web Unica Platform, vous devez arrêter puis redémarrer l'application Web Unica Platform lorsque vous modifiez la valeur de cette propriété.

Name of group to receive audit backup notifications (Nom du groupe qui doit recevoir les notifications de sauvegarde d'audit)

Description

Indique le groupe Unica dont les membres doivent recevoir une notification des sauvegardes d'archives. Vous ne pouvez indiquer qu'un seul groupe pour cette propriété. Les utilisateurs de ce groupe peuvent gérer leur abonnement à la notification en allant dans **Paramètres > Utilisateurs** et en cliquant sur **Abonnements au notifications**.

Platform | Evénements d'audit | Configuration de la gravité des événements d'audit

Le niveau de gravité que vous indiquez pour chaque événement dans cette page apparaît dans le rapport d'événements d'audit (Audit Events). Vous pouvez utiliser le niveau de gravité pour trier et filtrer les données du rapport. Les événements sont identiques à ceux de la catégorie **Platform | Evénements d'audit | Configuration des événements d'audit**.

Propriétés de configuration de Digital Analytics

Cette section décrit les propriétés de configuration de Digital Analytics dans la page de configuration.

Ces propriétés de configuration sont utilisées lors de la configuration de la connexion unique entre Digital Analytics et Unica. Pour plus de détails sur cette intégration, voir Unica Platform - Guide d'administration.

Digital Analytics®

La propriété de cette catégorie fait partie de la configuration et permet la connexion unique entre Digital Analytics et Unica.

Activer l'analyse Coremetrics®

Description

Cela fait partie de la configuration permettant d'activer la connexion unique entre Digital Analytics et Unica.

Affectez la valeur `true` comme l'une des étapes d'activation de la connexion unique.

Pour plus de détails sur cette intégration, voir Unica Platform - Guide d'administration.

Valeur par défaut

`false`

Digital Analytics® | Intégration | partitions | partition[n]|

Les propriétés de cette catégorie font partie de la configuration et permettent d'activer la connexion unique entre Digital Analytics et Unica.

Utilisateur de la plateforme pour le compte Coremetrics®

Description

Indique le nom de connexion du compte utilisateur Unica détenant le secret partagé par Digital Analytics dans une source de données.

Cela fait partie de la configuration permettant d'activer la connexion unique entre Digital Analytics et Unica. Pour plus de détails sur cette intégration, voir Unica Platform - Guide d'administration.

Valeur par défaut

`asm_admin`

Source de données du compte Coremetrics®

Description

Indique le nom de la source de données créée pour détenir le secret partagé par Digital Analytics.

Cela fait partie de la configuration permettant d'activer la connexion unique entre Digital Analytics et Unica. Pour plus de détails sur cette intégration, voir Unica Platform - Guide d'administration.

Valeur par défaut

`CoremetricsDS`

Propriétés de configuration des rapports

Les propriétés de configuration des rapports pour Unica sont disponibles dans **Paramètres > Configuration > Rapports**.

Pour générer des rapports, la suite Unica s'intègre à Cognos®, une application de business intelligence. Vous utilisez les propriétés **Integrations > Cognos** pour identifier votre système Cognos®. Puis, pour Unica Campaign, Unica Deliver et Unica Interact, vous devez configurer des propriétés supplémentaires pour définir et personnaliser les schémas de génération de rapports. Pour plus de détails sur les propriétés de configuration, reportez-vous au guide d'installation et de configuration Cognos Reports.

Unica Plan propriétés de configuration

Les propriétés de configuration de Unica Plan sont disponibles sur la page **Paramètres > Configuration**. Pour plus de détails sur les propriétés de configuration, consultez le Guide de l'administrateur de Plan.

Propriétés de configuration de Unica Campaign

Les propriétés de configuration de Unica Campaign sont situées dans **ParamètresConfiguration**. Pour plus d'informations sur les propriétés de configuration, consulter le Guide d'administration de Campaign.

Propriétés de configuration de Unica Deliver

Les propriétés de configuration de Unica Deliver sont disponibles sur la page Configuration. Pour plus d'informations sur les propriétés de configuration, consulter le Guide de démarrage et d'administration de Deliver.

Propriétés de configuration de Unica Interact

Les propriétés de configuration de Unica Interact sont disponibles sur la page Configuration. Pour plus d'informations sur les propriétés de configuration, consulter le Guide d'administration d'Interact.

Propriétés de configuration d'Unica Journey

Les propriétés de configuration d'Unica Journey sont disponibles sur la page **Paramètres > Configuration**. Pour plus d'informations sur les propriétés de configuration, consulter le Guide d'administration de Journey.

Propriétés de configuration d'Unica Content Integration

Les propriétés de configuration d'Unica Content Integration sont disponibles sur la page **Paramètres > Configuration**. Pour plus d'informations sur les propriétés de la page Configuration, consulter le Guide d'administration de Content Integration.

Propriétés de configuration de Unica Collaborate

Les propriétés de configuration d'Unica Collaborate Integration sont disponibles sur la page **Paramètres > Configuration**. Pour plus d'informations sur les propriétés de configuration, consultez Unica Collaborate - Guide d'administration.

Des propriétés de configuration supplémentaires existent dans les fichiers XML situés dans le répertoire d'installation de Unica Collaborate.

Propriétés de configuration de IBM SPSS Modeler Advantage Enterprise Marketing Management Edition

Les propriétés de cette catégorie spécifient les valeurs qui sont utilisées pour configurer Unica pour la connexion unique avec IBM SPSS Modeler Advantage Enterprise Marketing Management Edition.

Voir le manuel Unica Campaign and IBM SPSS Modeler Advantage Enterprise Marketing Management Edition Integration Guide pour des instructions complètes sur la configuration de la connexion unique avec IBM SPSS Modeler Advantage Enterprise Marketing Management Edition.

SPSS® | intégration

Les propriétés de cette catégorie permettent de configurer Unica Platform pour la connexion unique avec IBM SPSS Modeler Advantage Enterprise Marketing Management Edition.

Utilisateur de la plateforme pour le compte IBM® SPSS®

Description

Entrez le nom de connexion associé au compte IBM SPSS Modeler Advantage Enterprise Marketing Management Edition que vous avez créé ou identifié pour la connexion unique avec IBM SPSS Modeler Advantage Enterprise Marketing Management Edition.

Valeur par défaut

`asm_admin`

Disponibilité

Cette propriété est utilisée uniquement pour configurer Unica Platform pour la connexion unique avec IBM SPSS Modeler Advantage Enterprise Marketing Management Edition.

Source de données du compte IBM® SPSS®

Description

Affectez à cette propriété le nom de la source de données que vous avez créée pour l'utilisateur système lorsque vous avez configuré la connexion unique avec IBM SPSS Modeler Advantage Enterprise Marketing Management Edition. Si vous avez utilisé **SPSS_MA_ADMIN_DS** comme nom de source de données, vous pouvez conserver la valeur par défaut de cette propriété.

Valeur par défaut

SPSS_MA_ADMIN_DS

Disponibilité

Cette propriété est utilisée uniquement pour configurer Unica Platform pour la connexion unique avec IBM SPSS Modeler Advantage Enterprise Marketing Management Edition.

Ce score concerne-t-il seulement l'intégration ?

Description

Non pris en charge.

Valeur par défaut

FAUX

Disponibilité

Cette propriété est utilisée uniquement pour configurer Unica Platform pour la connexion unique avec IBM SPSS Modeler Advantage Enterprise Marketing Management Edition.

SPSS® | Intégration | partitions | partition[n]|

La propriété de cette catégorie permet de configurer Unica Platform pour la connexion unique avec IBM SPSS Modeler Advantage Enterprise Marketing Management Edition.

Activer IBM® SPSS®

Description

Paramétrez cette propriété sur TRUE pour permettre la connexion unique avec IBM SPSS Modeler Advantage Enterprise Marketing Management Edition.

Pour chaque partition où des utilisateurs devraient disposer de la connexion unique, vous devez utiliser **SPSS MA EMM Edition | Intégration | partitions | partitionTemplate** pour créer la propriété de configuration **enableSPSS** pour cette partition. Le nom de la catégorie que vous créez à l'aide du modèle doit correspondre exactement au nom de la partition Campaign correspondante. La partition1 par défaut comporte déjà la propriété de configuration **Activer IBM SPSS** de sorte que vous n'avez pas à utiliser le modèle pour la créer.

Valeur par défaut

FAUX

Disponibilité

Cette propriété est utilisée uniquement pour configurer Unica Platform pour la connexion unique avec IBM SPSS Modeler Advantage Enterprise Marketing Management Edition.

SPSS® | navigation

Les propriétés de cette catégorie affectent l'intégration IBM SPSS Modeler Advantage Enterprise Marketing Management Edition à Unica Campaign. Ces propriétés définissent l'emplacement du serveur Decision Management et du serveur IBM SPSS Collaboration and Deployment Services.

Adresse URL d'IBM® SPSS® Decision Management Server

Description

URL du serveur Decision Management SPSS®. Configurez cette URL avec le nom de serveur ou l'adresse IP de serveur suivi du port sur lequel IBM SPSS Modeler Advantage Enterprise Marketing Management Edition est hébergé sur le serveur.

Valeur par défaut

L'un des formats suivants :

- `http://<server name>:<port>/DM`
- `http://<server IP address>:<port>/DM`

Valeurs valides

URL du serveur Decision Management SPSS®.

Serveur C&DS

Description

Nom du serveur IBM SPSS Collaboration and Deployment Services.

Valeur par défaut

Aucun

Valeurs valides

Nom du serveur ou adresse IP du serveur valide sur lequel IBM SPSS Collaboration and Deployment Services est installé et configuré.

Port C&DS

Description

Port sur lequel se trouve IBM SPSS Collaboration and Deployment Services.

Valeur par défaut

Aucun

Valeurs valides

Numéro de port valide sur lequel IBM SPSS Collaboration and Deployment Services est hébergé.

Propriétés de configuration d'Opportunity Detect et d'Unica Interact Advanced Patterns

Cette section décrit les propriétés de configuration d'Opportunity Detect et d'Unica Interact Advanced Patterns sur la page Configuration.

Opportunity Detect and Interact Advanced Patterns | Navigation

Les propriétés de cette catégorie spécifient les valeurs utilisées en interne pour la navigation dans les produits Unica.

welcomePageURI

Description

Identificateur URI de la page d'index d' Opportunity Detect. Cette valeur est utilisée en interne par les applications Unica. Il n'est pas recommandé de modifier cette valeur.

Valeur par défaut

`/index.jsp`

seedName

Description

Utilisée en interne par les applications d'Unica. Il n'est pas recommandé de modifier cette valeur.

Valeur par défaut

`Detect`

type

Description

Utilisée en interne par les applications d'Unica. Il n'est pas recommandé de modifier cette valeur.

Valeur par défaut

`Detect`

httpPort

Description

Numéro de port utilisé par le serveur d'applications pour les connexions à l'application Opportunity Detect .

Valeur par défaut

`7001`

httpsPort

Description

Numéro de port utilisé par le serveur d'applications pour les connexions sécurisées à l'application Opportunity Detect .

Valeur par défaut

`7001`

serverURL

Description

Adresse URL de l'installation Opportunity Detect. Ce paramètre le protocole HTTP ou HTTPS. Si vous disposez d'un environnement groupé et que vous choisissez d'utiliser d'autres ports que les ports par défaut `80` ou `443` pour votre déploiement, n'utilisez pas un numéro de port qui se trouve dans cette propriété.

Si des utilisateurs accèdent à Opportunity Detect depuis le navigateur Chrome, utilisez le nom de domaine complet dans l'adresse URL. Si vous n'utilisez pas le nom de domaine complet, le navigateur Chrome ne pourra pas accéder aux adresses URL de produit.

Important : Si les produits Unica sont installés dans un environnement réparti, vous devez utiliser le nom de machine plutôt que l'adresse IP dans l'URL de navigation pour toutes les applications de la suite.

Valeur par défaut

[server-url]

logoutURL

Description

Pour usage interne. Il n'est pas recommandé de modifier cette valeur.

Unica Platform utilise cette valeur pour appeler le gestionnaire de déconnexion de chaque application enregistrée si l'utilisateur clique sur le lien de déconnexion dans Unica.

serverURLInternal

Description

Pour usage interne. Il n'est pas recommandé de modifier cette valeur.

displayName

Description

Pour usage interne. Il n'est pas recommandé de modifier cette valeur.

Valeur par défaut

```
Opportunity Detect
```

Opportunity Detect and Interact Advanced Patterns | Système | Service Web de contrôle à distance Streams

La propriété de cette catégorie spécifie l'URL du service Web de contrôle à distance InfoSphere Streams. Opportunity Detect Design Time communique avec Opportunity Detect Run Time pour ce service.

ServerURL

Description

La personne qui installe le produit définit la valeur de cette propriété lors de l'installation. Le numéro de port par défaut est 8080.

Valeur par défaut

```
http://[SRCSHost]:[SRCSPort]/axis2/services/RemoteControl
```

Opportunity Detect and Interact Advanced Patterns | Système | Real Time Connector

La propriété de cette catégorie définit l'URL du service Web utilisé lorsque Unica Interact est intégré à Unica Interact Advanced Patterns ou lorsque le connecteur du service Web est utilisé pour les données d'entrée.

ServerURL

Description

La personne qui installe le produit définit la valeur de cette propriété lors de l'installation. Le numéro de port par défaut est 8282.

Valeur par défaut

```
http://[RealTimeConnectorHost]:[RealTimeConnectorPort]/servlets/
StreamServlet
```

Opportunity Detect and Interact Advanced Patterns | Système | Surveillance

Les propriétés de cette catégorie indiquent les valeurs qui affectent l'outil de contrôle.

Poll Interval (In Seconds)

Description

Nombre de secondes pendant lequel le service de surveillance attend entre deux interrogations successives du serveur Streams pour les statistiques. La valeur par défaut est de 300 secondes (ou 5 minutes).

Valeur par défaut

```
300
```

Retaining Time (In Days)

Description

Nombre de jours pendant lequel le service de surveillance doit conserver les données interrogées dans la base de données. La valeur par défaut est 10 jours. Les données qui sont antérieures à la date spécifiée ici sont purgées.

Valeur par défaut

`10`

Opportunity Detect and Interact Advanced Patterns | Système | Options de traitement

Les propriétés de cette catégorie indiquent les valeurs qui affectent l'outil de contrôle.

Enregistrements de profil en mémoire cache

Description

Opportunity Detect peut mettre les données de profil en cache, pour une performance optimale. Pour activer la mise en cache des données de profil, associez cette propriété à la valeur `True`.

Si vous disposez d'ensembles de données de profil très volumineux, vous pouvez conserver la valeur par défaut de cette propriété, à savoir `False`. Vous désactivez ainsi la mise en cache des données de profil et éliminez les éventuels problèmes de mémoire insuffisante pouvant résulter de la mise en cache de grandes quantités de données de profil.

Si vous changez la valeur de cette propriété, vous devez redémarrer votre serveur d'applications Web, l'instance Streams et le service StreamsRCS, puis redéployer tous les déploiements affectés.

Valeur par défaut

`Faux`

Opportunity Detect and Interact Advanced Patterns | journalisation

La propriété de cette catégorie définit l'emplacement du fichier journal d'Opportunity Detect.

log4jConfig

Description

Emplacement du fichier de configuration que Opportunity Detect utilise pour la journalisation. Cette valeur est définie automatiquement lors de l'installation, mais si vous changez ce chemin, vous devez redémarrer le serveur d'applications Web pour que la modification soit prise en compte.

Valeur par défaut

```
[absolute-path]/conf/detect_log4j.properties
```

Unica Interact Advanced Patterns | Système | Service de conception Interact

La propriété de cette catégorie définit l'URL du service Web qui permet à Interact de créer et de déployer automatiquement des modèles avancés lorsque Unica Interact est intégré à Unica Interact Advanced Patterns.

ServerURL

Description

Ce service Web est le point d'intégration entre Unica Interact et la phase de conception Unica Interact Advanced Patterns. La personne qui installe le produit définit la valeur de cette propriété lors de l'installation. Le numéro de port par défaut est 8181.

Valeur par défaut

```
http://[InteractServiceHost]:[InteractServicePort]/axis2/services/
InteractDesignService
```

Voici les propriétés de configuration établies par le programme d'installation.

Insights | navigation

La suite Unica s'intègre à Unica Insights pour générer des rapports.

Cette page affiche les propriétés qui définissent les URL et les autres paramètres utilisés par le système Unica Insights.

Nom de la valeur de départ

Description

Utilisé en interne par les applications HCL Unica. Il n'est pas recommandé de modifier cette valeur.

Valeur par défaut

Insights

httpPort

Description

Cette propriété spécifie le port utilisé par le serveur d'applications Web d'Unica Insights. Si votre installation d'Unica Insights utilise un port différent du port par défaut, vous devez éditer la valeur de cette propriété.

Valeur par défaut

7001

httpsPort

Description

Si SSL est configuré, cette propriété spécifie le port utilisé par le serveur d'applications Web d'Unica Insights pour les connexions sécurisées. Si votre installation d'Unica Insights utilise un port sécurisé différent du port par défaut, vous devrez éditer la valeur de cette propriété.

Valeur par défaut

7001

serverURL

Description

Spécifie l'URL de l'application Web Unica Insights. Utilisez un nom de système hôte qualifié complet en incluant le nom de domaine (et de sous-domaine, le cas échéant) spécifié dans la propriété Domaine. Par exemple : http://MyReportServer.MyCompanyDomain.com:7001/ Insights

Valeur par défaut

`http://[CHANGE ME]/hcl-birt`

Valeurs valides

Une URL de forme valide.

logoutURL

Description

La propriété logoutURL est utilisée en interne pour appeler le gestionnaire de déconnexion de l'application enregistrée si l'utilisateur clique sur le lien de déconnexion. Ne modifiez pas cette valeur.

Valeur par défaut

`/j_spring_security_logout`

Activé

Description

Définir la valeur sur `TRUE` permet de garantir qu'Unica Insights sera utilisé comme moteur de génération de rapports.

Remarque : Si vous mettez à niveau à la version 12.0 et que des packs de rapports Campaign/Plan/Interact et Unica Platform sont installés, vous avez le choix entre les rapports Cognos et les rapports Unica Insights.

Valeur par défaut

`False`

Valeurs valides

`FALSE | TRUE`

Pour le moment, les rapports Unica Insights sont pris en charge pour les bases de données Oracle, SQL Server et DB2.

Personnalisation des feuilles de style et des images dans l'interface utilisateur Unica

Vous pouvez personnaliser l'apparence de l'interface utilisateur dans laquelle la plupart des pages du produit Unica s'affichent. Editez une feuille de style en cascade et fournissez vos propres graphiques pour changer les images, polices et couleurs de l'interface utilisateur.

Cette opération est souvent appelée redésignation, car vous pouvez remplacer le logo et les couleurs d'HCL par le logo et les couleurs de votre société.

Feuilles de style

L'agencement de cadres d' HTML est formaté par plusieurs feuilles de style en cascade, situées dans le répertoire `css` du fichier `unica.war`. Plusieurs de ces feuilles de style importent une feuille de style `corporatetheme.css` dans le répertoire `css\theme`. Par défaut, ce fichier `corporatetheme.css` est blanc. Lorsque vous remplacez le fichier blanc par un fichier qui utilise vos couleurs et vos images, vous changez l'apparence de l'agencement de cadres.

fournit également un exemple de fichier `corporatetheme.css`, dans le répertoire `css \theme\DEFAULT` du fichier `unica.war`. Cet exemple de feuille de style contient toutes les spécifications personnalisables ainsi que les commentaires qui expliquent les zones de l'agencement de cadres affectées par chaque spécification. Vous pouvez utiliser ce fichier comme modèle afin d'effectuer vos propres changements, comme décrit dans les instructions de cette section.

Images

Vos images peuvent être au format PNG, GIF ou JPEG.

utilise des sprites pour certains de ses boutons et icônes. L'utilisation des sprites permet de réduire le nombre de demandes http qui parviennent au serveur et les risques de scintillement. Si utilise des sprites, le nom de l'image inclut la chaîne `_sprites`. Si vous souhaitez remplacer ces images, il est recommandé d'utiliser des sprites avec les mêmes dimensions afin d'effectuer un minimum de modifications dans la feuille de style. Si vous n'êtes pas familiarisé avec les sprites, des informations sont disponibles à ce sujet sur Internet.

Préparation de votre thème d'entreprise

Suivez les instructions mentionnées ici pour créer votre thème d'entreprise pour l'agencement de cadres Unica.

1. Lors de l'installation de Unica Platform, vous avez peut-être créé un fichier EAR qui contient le fichier `unica.war` ou installé le fichier `unica.war`. Dans les deux cas, décompressez le fichier `unica.war` installé pour accéder aux fichiers et répertoires qu'il contient.
2. Localisez le fichier `corporatetheme.css` dans le répertoire `css\theme\DEFAULT`.
3. Pour savoir quelle zone du cadre est concernée par chaque spécification de la feuille de style, consultez les commentaires du fichier `corporatetheme.css`.
4. Reportez-vous aux images du répertoire `css\theme\img` pour créer vos images.
5. Créez votre thème dans le programme graphique de votre choix et notez les noms des images, les polices et les spécifications hexadécimales pour les couleurs de police et d'arrière-plan.
6. Editez le fichier `corporatetheme.css` pour utiliser vos polices, couleurs et images.

Application de votre thème d'entreprise

Utilisez la procédure indiquée ici pour fournir votre thème d'entreprise à l'interface utilisateur Unica.

1. Placez les images à utiliser (logo, boutons et icônes, par exemple) dans un répertoire accessible à partir de la machine sur laquelle vous avez installé Unica Platform. Consultez le fichier modifié `corporatetheme.css` créé selon la procédure décrite à

la section "Préparation de votre thème d'entreprise" pour déterminer où placer les images.

2. Si Unica Platform est déployé, annulez le déploiement.
3. Lors de l'installation de Unica Platform, vous avez peut-être créé un fichier EAR qui contient le fichier `unica.war` ou installé le fichier `unica.war`. Dans les deux cas, suivez la procédure ci-dessous.
    - Sauvegardez votre fichier WAR ou EAR sous un autre nom (par exemple, `original_unica.war`). Vous pourrez ainsi reprendre la version d'origine du fichier si nécessaire.
    - Décompressez le fichier `unica.war` installé pour accéder aux fichiers et répertoires qu'il contient.
4. Placez le fichier modifié `corporatetheme.css` modifié (créé selon la procédure décrite à la section "Préparation de votre thème d'entreprise"), dans le répertoire `css\theme`.

   Il écrase le fichier `corporatetheme.css` à blanc qui se trouve initialement dans ce répertoire.
5. Recréez le fichier `unica.war` et, si nécessaire, le fichier EAR dans lequel il se trouvait.
6. Déployez le fichier WAR ou EAR.
7. Videz le cache de votre navigateur et connectez-vous à Unica.

   Votre nouveau thème doit avoir été appliqué.