IBM Cognos Analytics
Version 11.0

# *Installation et configuration*

©

## Informations sur le produit

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Le présent document s'applique à IBM Cognos Analytics version 11.0.0 et peut aussi s'appliquer aux éditions ultérieures de ce produit.

## Copyright

# Table des matières

# Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

## Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

## Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

| **IBM France** | **IBM Canada** |
|---|---|
| ingénieur commercial | représentant |
| agence commerciale | succursale |
| ingénieur technico-commercial | informaticien |
| inspecteur | technicien du matériel |

## Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

## OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

## Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

| France | Canada | Etats-Unis |
|---|---|---|
| (Pos1) | | Home |
| Fin | Fin | End |
| (PgAr) | | PgUp |
| (PgAv) | | PgDn |
| Inser | Inser | Ins |
| Suppr | Suppr | Del |
| Echap | Echap | Esc |
| Attn | Intrp | Break |
| Impr écran | ImpEc | PrtSc |
| Verr num | Num | Num Lock |
| Arrêt défil | Défil | Scroll Lock |
| (Verr maj) | FixMaj | Caps Lock |
| AltGr | AltCar | Alt (à droite) |

## Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

## Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

# Chapitre 1. Préparation de l'installation

Avant d'installer IBM® Cognos Analytics, vous devez configurer des ressources de votre environnement, afin que les composants puissent fonctionner. Par exemple, vous devez créer une base de données à utiliser en tant que magasin de contenu pour Cognos Analytics, et créer un compte utilisateur pour Cognos Analytics.

Si vous utilisez l'option **Installation facile** (anciennement nommée **Prêt à fonctionner !**) pour installer Cognos Analytics (sous Windows uniquement), il ne vous est pas nécessaire de créer et de configurer une base de données servant de magasin de contenu. Une base de données Informix est déjà configurée en tant que magasin de contenu, directement utilisable par Cognos Analytics.

Après avoir effectué ces tâches, passez à la section Chapitre 4, «Installation et configuration des composants du serveur», à la page 57.

## Consultation des notes sur l'édition

Consultez les notes sur l'édition avant d'installer le produit. Les notes sur l'édition contiennent des informations de dernière minute, les problèmes connus, ainsi que des mises à jour de la documentation et des avis relatifs à l'obsolescence.

Les notes sur l'édition sont disponibles dans le Knowledge Center IBM Cognos Analytics (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html).

## Opérations de configuration critiques à réaliser en premier

Ces opérations de configuration sont indispensables au succès de votre installation. Réalisez les opérations suivantes une fois les composants installés.

### Vérifiez que les pilotes JDBC se trouvent au bon emplacement

Pour la version 11.0.x d'IBM Cognos Analytics, les pilotes JDBC doivent être copiés dans le répertoire *emplacement_installation*\drivers.

L'utilisation du répertoire *emplacement_installation*\webapps\p2pd\WEB-INF\lib pour les pilotes JDBC n'est pas prise en charge.

### Remplacez le pilote JSQL pour Microsoft SQL Server par le pilote JDBC de Microsoft

A partir de la version 11.0.5 d'IBM Cognos Analytics, le pilote JSQL pour Microsoft SQL Server est remplacé par le pilote JDBC de Microsoft. Vous devez télécharger et placer le fichier JAR requis dans le répertoire *emplacement_installation*\drivers. Pour plus d'informations, voir Configuration pour le magasin de contenu Microsoft SQL Server.

### Spécifiez la propriété Groupe de configuration

Si vous avez installé IBM Cognos Analytics par le biais d'une installation de type **Personnalisé**, ouvrez IBM Cognos Configuration et définissez la propriété **Groupe**

**de configuration**. Pour plus d'informations, voir Gestion du groupe de configuration.

### Activez ou désactivez la modélisation Web

Par défaut, les connexions de source de données JDBC qui ont été créées dans IBM Cognos Administration ne sont pas disponibles pour les modules de données dans l'interface d'administration **Gérer** > **Serveurs de données**. Si vous voulez utiliser vos connexions de source de données existantes (mises à niveau) pour créer des modules de données, vous devez activer la modélisation Web sur ces connexions.

Certaines sources de données ne sont pas aptes à être utilisées comme sources pour la création de modules de données. Dans ce cas, vous pouvez interdire l'utilisation de la modélisation Web sur les connexions de la source de données.

Pour activer ou désactiver la modélisation Web pour vos connexions de source de données, procédez comme suit :

1. Dans IBM Cognos Analytics, accédez à **Gérer** > **Console d'administration**.
2. Dans IBM Cognos Administration, dans l'onglet **Configuration**, sélectionnez **Connexions de source de données**.
3. Localisez la source de données et cliquez sur **Définir les propriétés**.
4. Dans l'onglet **Connexion**, sélectionnez ou désélectionnez la case **Autoriser la modélisation Web**.

## Présentation des environnements pris en charge

Afin de garantir le bon fonctionnement de votre produit, veillez à appliquer tous les correctifs minimaux requis pour le système d'exploitation et à n'utiliser que les versions prises en charge des produits tiers.

Pour consulter la liste actualisée des environnements pris en charge par les produits IBM Cognos Analytics, y compris des informations sur les systèmes d'exploitation, les correctifs, les navigateurs, les serveurs Web, les serveurs d'annuaire, les serveurs de base de données et les serveurs d'applications, consultez la page IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

## Vérification de la configuration système requise

Vérifiez dans les tableaux ci-dessous les configurations matérielles et logicielles minimales requises pour installer et exécuter les composants d'IBM Cognos Analytics sur un ordinateur. D'autres ressources peuvent s'avérer nécessaires pour les environnements répartis ou les environnements de production.

Le tableau ci-dessous présente les configurations et les spécifications matérielles requises pour une installation sur un ordinateur unique.

## Configuration matérielle requise

*Tableau 1. Configuration matérielle requise pour une installation d'ordinateur unique*

| Configuration requise | Spécification |
|---|---|
| Système d'exploitation | Microsoft Windows<br><br>UNIX<br><br>Linux |
| RAM | Au minimum 10 Go. Pour en savoir davantage, reportez-vous à la section «Paramètres de mémoire», à la page 4. |
| Spécifications pour le système d'exploitation | Limite de descripteur de fichier fixée à 8192 sous UNIX et Linux. |
| Espace disque | Un minimum de 3,5 Go d'espace libre est requis pour installer le logiciel, ainsi que 5 Go d'espace libre sur l'unité contenant le répertoire temporaire utilisé par les composants d'IBM Cognos.<br><br>Une variable d'environnement pointe vers le répertoire temporaire. Sous Windows, cette variable est TMP. Sous UNIX et Linux, cette variable est IATEMPDIR.<br><br>La taille de toutes les bases de données augmente au fil du temps. Prévoyez suffisamment d'espace disque pour la suite. |
| Imprimante | Pour vous assurer que les rapports s'impriment correctement sous Windows, Adobe Reader requiert la configuration d'au moins une imprimante sur l'ordinateur où vous installez les composants du groupe de serveurs d'applications. Tous les rapports, quel que soit le format d'impression choisi, sont envoyés en tant que fichiers PDF temporaires vers Adobe Reader pour impression. |
| Serveur de messagerie | Pour envoyer des rapports par courrier électronique, le système requiert la possibilité d'utiliser un serveur de messagerie et d'y accéder. |

## Configuration logicielle requise

Le tableau suivant présente les configurations et spécifications logicielles requises pour une installation sur un ordinateur unique.

*Tableau 2. Configuration logicielle requise pour une installation d'ordinateur unique*

| Configuration requise | Spécification |
|---|---|
| Java™ Runtime Environment (JRE) | L'installation d'IBM Cognos Analytics vous fournit un environnement d'exécution Java IBM sur tous les systèmes d'exploitation. |

*Tableau 2. Configuration logicielle requise pour une installation d'ordinateur unique (suite)*

| Configuration requise | Spécification |
|---|---|
| Base de données | Vous devez disposer de l'une des bases de données suivantes pour le stockage des données d'IBM Cognos :<br>• Oracle<br>• IBM Db2<br>• Microsoft SQL Server<br>• Informix<br><br>L'option Simple (anciennement appelée Prêt à fonctionner !) installe et configure une base de données Informix en tant que magasin de données.<br><br>La connectivité TCP/IP est requise pour tous les types de base de données. |
| Navigateur Web | Pour tous les navigateurs Web, les éléments suivants doivent être activés :<br>• Cookies<br>• JavaScript<br><br>Pour Microsoft Internet Explorer uniquement, les fonctions suivantes doivent être activées :<br>• Exécuter les contrôles ActiveX et les plug-in<br>• Contrôles ActiveX reconnus sûrs pour l'écriture de scripts<br>• Active Scripting<br>• META REFRESH autorisé |

### Conditions requises pour la visualisation des cartes

Les cartes que vous créez dans les tableaux de bord et les rapports utilisent un service sur cloud de cartes en mosaïque et de polygones. Pour que votre navigateur Web puisse accéder au service via une connexion HTTPS, vous devez disposer d'un accès à Internet depuis votre poste de travail.

L'accès Internet au service n'est pas requis depuis un serveur Cognos Analytics. Le service fournit les polygones et les cartes de base uniquement. Aucune donnée utilisateur n'est envoyée au service de cloud.

## Paramètres de mémoire

Les paramètres de mémoire dépendent d'un grand nombre de facteurs, comme le niveau d'activité attendu sur le serveur, la complexité des applications IBM Cognos, le nombre d'utilisateurs et de demandes et les temps de réponse acceptables.

Si votre environnement prend en charge plus de 100 utilisateurs nommés, s'il est complexe et s'il présente des périodes de pic d'utilisation ou s'il combine un ou plusieurs de ces facteurs, il convient d'envisager l'élaboration d'un plan de capacité. Pour plus d'informations, voir la page des services IBM Cognos Analytics (www.ibm.com/software/analytics/cognos/services/).

Pour déterminer les paramètres les mieux adaptés à votre environnement, il est conseillé d'effectuer un test de performance.

Utilisez les paramètres de mémoire suivants comme point de départ et ajustez-les en fonction de l'utilisation de la mémoire du système.

- 2 Go pour le système d'exploitation de base et les logiciels associés, comme l'antivirus, le logiciel de sauvegarde et le logiciel de gestion d'entreprise
- 4 Go pour la machine virtuelle Java du répartiteur (Content Manager ou groupe de serveurs d'application)
- 2 Go pour la machine virtuelle Java de Cognos Graphics Service
- 8 Go pour la machine virtuelle Java du service de requête/de jeu de données
- 2 Go par coeur pour les processus du serveur de rapports (BIBus)

## Définition des valeurs ulimit sur les systèmes d'exploitation UNIX et Linux

La définition des valeurs ulimit appropriées sur votre système d'exploitation UNIX ou Linux peut affecter les performances d'IBM Cognos Analytics.

Par exemple, sur les systèmes d'exploitation Linux, les problèmes qui sont causés par les paramètres ulimit de pile comprennent les erreurs liées à une consommation de la mémoire anormalement élevée par BIBusTKServerMain ou BIBusTKServerMain lors du traitement de rapports volumineux.

Si vous utilisez le service de rapports sur les systèmes d'exploitation Linux, l'exécution de rapports ou des processus BIBusTKServerMain inactifs peuvent utiliser toute votre mémoire RAM disponible.

En revanche, sur les systèmes d'exploitation UNIX, des paramètres ulimit de pile trop bas peuvent générer des problèmes.

La définition de paramètres ulimit de pile adaptés peut éviter ces problèmes.

Les paramètres ulimit recommandés pour une nouvelle installation sont les suivants :

**IBM AIX**

- Temps UC (secondes) : ulimit -t unlimited
- Taille de fichier (blocs) : ulimit -f unlimited
- Taille de mémoire maximale (ko) : ulimit -m unlimited
- Nombre maximal de processus utilisateur : ulimit -u unlimited
- Fichiers ouverts : ulimit -n 8192 (valeur minimale)
- Taille de pile (ko) : ulimit -s 8192 (valeur minimale)
- Mémoire virtuelle (ko) : ulimit -v unlimited

**Oracle Solaris**

- Temps UC (secondes) : ulimit -t unlimited
- Taille de fichier (blocs) : ulimit -f unlimited
- Nombre maximal de processus utilisateur : ulimit -u unlimited
- Mémoire (ko) : ulimit -m unlimited
- Fichiers ouverts : ulimit -n 8192 (valeur minimale)
- Taille de pile (ko) : ulimit -s 8192 (valeur minimale)
- Mémoire virtuelle (ko) : ulimit -v unlimited

**Linux (x, z et p)**

- Temps UC (secondes) : ulimit -t unlimited

- Taille de fichier (blocs) : ulimit -f unlimited
- Taille de mémoire maximale (ko) : ulimit -m unlimited
- Nombre maximal de processus utilisateur : ulimit -u unlimited
- Fichiers ouverts : ulimit -n 8192 (valeur minimale)
- Taille de pile (ko) : ulimit -s unlimited
- Mémoire virtuelle (ko) : ulimit -v unlimited

**Remarque :** Ces paramètres devront éventuellement être adaptés à votre environnement au cours du cycle de vie de l'application.

## Configuration requise pour Java

Pour qu'IBM Cognos Analytics prenne en charge les services cryptographiques, il peut être nécessaire de mettre à jour votre version de Java ou de définir une variable d'environnement JAVA_HOME. En fonction des exigences de règle de sécurité, il peut également être nécessaire d'installer le fichier de règles JCE (Java Cryptography Extension) à accès illimité.

Vous pouvez utiliser un JRE (Java Runtime Environment) existant ou le JRE fourni avec IBM Cognos Analytics.

### Normes cryptographiques

Les services cryptographiques IBM Cognos utilisent un fichier JAR (Java Archive) spécifique, nommé `bcprov-jdknn-nnn.jar` qui doit se trouver dans votre JRE (Java Runtime Environment). Ce fichier fournit des routines de chiffrement et de déchiffrement supplémentaires qui ne sont pas appliquées dans le cadre d'une installation de machine virtuelle Java (JVM) par défaut. Pour des raisons de sécurité, le fichier de chiffrement doit être chargé par la machine virtuelle Java en utilisant le répertoire des extensions Java.

1. Accédez au répertoire `emplacement_installation/jre/lib/ext`.
2. Copiez le fichier `bcprov-jdk14-145.jar` dans votre répertoire `$JAVA_HOME/lib/ext`.

Par défaut, IBM Cognos Analytics est configuré pour utiliser la norme de sécurité NIST SP800-131a. Pour vous conformer à cette norme de sécurité, vous devez utiliser un environnement JRE prenant également en charge cette norme.

Pour en savoir davantage sur les versions Java prises en charge pour IBM Cognos Analytics, consultez le site IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

Pour plus d'informations sur cette norme de sécurité, voir le Knowledge Center d'IBM SDK, Java Technology Edition (www.ibm.com/support/knowledgecenter/SSYKE2/welcome_javasdk_family.html).

### JAVA_HOME

Définissez une variable d'environnement JAVA_HOME si vous souhaitez utiliser votre propre environnement Java.

Assurez-vous que la version JRE est prise en charge par les produits IBM Cognos.

Sous Microsoft Windows, si vous ne disposez pas d'une variable JAVA_HOME, les fichiers JRE fournis avec l'installation sont utilisés.

Pour vérifier que votre JRE est pris en charge, consultez le site IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

### Fichier de règles JCE à accès illimité

Les environnements JRE incluent un fichier de règles à accès limité qui vous cantonne à certains algorithmes de cryptographie et à certaines suites de chiffrement. Si vous avez besoin d'algorithmes de cryptographie et de suites de chiffrement plus nombreux que ceux indiqués dans IBM Cognos Configuration, vous pouvez télécharger et installer le fichier de règles JCE à accès illimité.

Pour Java fourni par IBM, le fichier de règles JCE à accès non limité est disponible sur le site Web d'IBM (www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).

## Vérification des paramètres de port par défaut

Après installation, vous pouvez utiliser l'outil de configuration pour modifier les paramètres par défaut d'IBM Cognos Analytics. L'installation **Simple** sélectionne automatiquement les paramètres de port.

**Important :** Ces ports doivent être ouverts pour le trafic entrant et sortant.

### Paramètres de port par défaut des composants Cognos Analytics

Le tableau ci-dessous répertorie les ports et les paramètres d'URI par défaut de la solution IBM Cognos Analytics.

*Tableau 3. Paramètres de port par défaut des composants Cognos Analytics*

| Paramètre | Valeur par défaut | Description |
|---|---|---|
| URI de Content Manager | `http://localhost:9300/p2pd/servlet` | Indique l'URI de Content Manager. |
| URI de la passerelle | `http://`*`nom_ordinateur`*`:`*`port`*`/bi/v1/disp` | Indique l'URI de la passerelle. |
| URI du répartiteur<br><br>(Interne, externe) | `http://localhost:9300/p2pd/servlet/dispatch` | Indique l'URI du répartiteur. |
| URI du répartiteur pour les applications externes | `http://localhost:9300/bi/v1/disp` | Indique l'URI du répartiteur. |
| Ports du serveur de journalisation | 9362 | Indique le port utilisé par le serveur de journalisation local. |
| Port de synchronisation de membre | 4300 | Port local utilisé pour la communication réseau qui transfère et synchronise les informations de configuration d'un serveur à l'autre. |

*Tableau 3. Paramètres de port par défaut des composants Cognos Analytics (suite)*

| Paramètre | Valeur par défaut | Description |
|---|---|---|
| Port de coordination de membre | 5701 | Port local utilisé pour la communication réseau pour la coordination de groupe. Ce port est utilisé pour détecter et rejoindre un groupe, ainsi que pour conserver une liste à jour des membres du groupe de configuration. |
| Port de service de jeu de données | 9301 | Port local utilisé pour la communication inter-processus. Ce port est affecté lors du premier démarrage de Cognos Analytics. Le numéro de port vaut le numéro de port du répartiteur Cognos Analytics plus 1. Par exemple, 9300 +1 = 9301. |

Pour en savoir davantage, voir «Paramètres de port et d'URI», à la page 151.

## Instructions pour la création du magasin de contenu

Le magasin de contenu est une base de données utilisée par Content Manager pour stocker des données de configuration globales, des paramètres généraux (par exemple, la langue et l'unité monétaire utilisées dans l'interface), des connexions à des sources de données et du contenu spécifique aux produits. Vous devez utiliser l'une des bases de données de niveau entreprise prises en charge en tant que magasin de contenu dans un environnement de production.

Les modèles de conception et les fichiers journaux ne sont pas stockés dans le magasin de contenu.

Vous devez créer le magasin de contenu avant d'utiliser votre produit IBM Cognos Analytics. Si vous utilisez l'option Simple (anciennement appelée Prêt à fonctionner !), Informix est installé et configuré comme magasin de contenu.

Si vous utilisez IBM Db2 pour votre magasin de données, vous pouvez générer une DDL pour permettre à votre administrateur de base de données de créer une base de données Db2 appropriée pour le magasin. Pour plus d'informations, voir «Génération d'un fichier script pour créer une base de données pour un magasin de contenu IBM Db2», à la page 69.

### Propriétés de la base de données

Vous devez créer la base de données du magasin de contenu à partir de l'une de celles mentionnées dans le tableau ci-dessous.

Le tableau suivant indique le codage des caractères et le protocole utilisés par les différents types de bases de données.

*Tableau 4. Codage de caractères et protocoles pour la base de données du magasin de contenu*

| Base de données | Codage de caractères | Protocole |
|---|---|---|
| Db2 | UTF-8 | TCP/IP |
| Oracle | AL32UTF8 ou AL32UTF16 | TCP/IP |
| Microsoft SQL Server | UTF-8 ou UTF-16 | TCP/IP |
| Informix | UTF-8 | TCP/IP |

### Séquence de classement

Cognos Analytics fait appel à un ordre de tri unique spécifiant les règles utilisées par la base de données pour interpréter, collecter, comparer et présenter les données de texte. Un ordre de tri définit, par exemple, si la lettre A possède une valeur de position inférieure, égale ou supérieure à la lettre B, si le classement est sensible à la casse et si celui-ci est sensible à l'accentuation. Pour plus d'information sur les séquences de classement et sur le classement, consultez le site Web ICU - International Components for Unicode (http://site.icu-project.org/), sélectionnez User Guide, puis cliquez sur Collation.

## Paramètres suggérés pour la création du magasin de contenu sous IBM Db2 on Linux, Windows et UNIX

La base de données créée sous Microsoft Windows, Linux ou UNIX pour Content Store doit contenir les paramètres de configuration définis.

Pour que l'installation aboutisse, utilisez les instructions suivantes lors de la création du magasin de contenu. Utilisez les mêmes directives pour créer une base de données des messages de journal.

### Instructions pour la création du magasin de contenu

Utilisez la liste de contrôle ci-dessous pour vous guider dans le processus de configuration du magasin de contenu sur Db2.

- Définissez les variables d'environnement appropriées pour Db2 qui sont présentées dans le tableau suivant.

*Tableau 5. Variables d'environnement de Db2*

| Variable d'environnement | Description |
|---|---|
| DB2PATH | Répertoire de premier niveau contenant le logiciel client ou l'installation complète de la base de données. |

*Tableau 5. Variables d'environnement de Db2 (suite)*

| Variable d'environnement | Description |
|---|---|
| LD_LIBRARY_PATH | Chemin d'accès à la bibliothèque de chargement.<br><br>Ajoutez l'emplacement du pilote au chemin, puis remplacez le symbole double dièse par `64-bit`.<br><br>Pour Windows : `LD_LIBRARY_PATH= $DB2_location/sqllib/lib##: $LD_LIBRARY_PATH`<br><br>Pour Solaris et Linux : `LD_LIBRARY_PATH= $DB2DIR/lib##: $LD_LIBRARY_PATH`<br><br>Pour AIX : `LIBPATH=$DB2DIR/lib##:$LIBPATH` |
| DB2INSTANCE | Connexion au serveur de base de données par défaut. |
| DB2CODEPAGE | L'affectation de la valeur 1208 à cette variable d'environnement facultative permet la prise en charge de bases de données multilingues.<br><br>Pour des informations sur l'usage de cette variable d'environnement, reportez-vous à la documentation sur Db2. |
| COGUDA_EXTENDEDCHAR_SUPPORT | Certaines bases de données offrent des fonctions de chaîne de caractères à l'aide d'une schématique à base d'octets par défaut. Cela peut entraîner des problèmes avec le traitement des chaînes. Par exemple, la base de données Db2 avec le jeu de caractères UTF-8 renvoie un nombre d'octets non souhaité au lieu du nombre de caractères de la fonction LENGTH.<br><br>Pour éviter ce type de problème, définissez cette variable sur `T` ou `t`. Le logiciel IBM Cognos spécifie alors l'unité de chaîne CODEUNIT32 pour les expressions substring, character_length et position dans le SQL Db2 pour que ces expressions fonctionnent sur la schématique à base de caractères.<br><br>N'utilisez pas cette variable dans le mode de requête dynamique. |

- Lorsque vous créez la base de données, utilisez **UTF-8** comme valeur de jeu de codes.

  Pour vérifier que votre base de données dispose de l'ensemble de codes approprié, saisissez à l'invite dans l'interface de ligne de commande :

  `db2 get database configuration for` *`nom_base_de_données`*

  La valeur du jeu de codes est UTF-8 et celle de la page de codes est 1208.
- Veillez à définir les paramètres de configuration tels qu'indiqués dans le tableau suivant.

*Tableau 6. Paramètres de configuration d'Db2*

| Propriété | Paramètre |
|---|---|
| Taille de segment mémoire de l'application<br><br>(applheapsz) | AUTOMATIQUE ou au moins 1024 Ko<br><br>Si la valeur de segment mémoire de l'application est trop faible, des erreurs de mémoire insuffisante risquent de se produire en présence d'un trop grand nombre d'utilisateurs. |
| Délai d'attente de verrouillage (locktimeout) | 240 secondes<br><br>Ne définissez pas de délai d'attente infini pour cette propriété. |
| Variable de registre Db2 (DB2_INLIST_TO_NLJN) | OUI<br><br>En définissant cette variable sur OUI, vous améliorez la performance. |

- Créez un groupe de mémoire tampon doté d'une taille de page de 32 Ko et un autre doté d'une taille de page de 8 Ko.
- Créez un espace de table système temporaire à l'aide du groupe de mémoire tampon de 32 Ko créé à l'étape précédente.
- Créez un espace de table temporaire d'utilisateur à l'aide du groupe de mémoire tampon de 8 Ko créé précédemment.

  Les tables temporaires globales sont créées dans l'espace de table utilisateur temporaire.
- Créez un espace de table standard d'utilisateur à l'aide du groupe de mémoire tampon de 8 Ko créé précédemment.

  Si vous créez également une base de données de journalisation, créez un autre espace de table utilisateur standard, doté d'une taille de page de 8 Ko.
- Accordez les privilèges d'accès à la base de données suivants au compte utilisateur qu'IBM Cognos Analytics utilisera pour accéder à la base de données :
  - Connexion à la base de données
  - Création de tables
  - Création implicite de schémas

  **Conseil :** Si vous voulez héberger plusieurs magasins de contenu sur votre instance Db2 et les utiliser simultanément, utilisez un compte utilisateur différent pour chacun, pour que chaque instance d'IBM Cognos Analytics soit parfaitement isolée des autres.
- Assurez-vous que le compte utilisateur dispose des privilèges d'accès Use pour l'espace de table utilisateur temporaire et pour les autres espaces de table appropriés associés à la base de données.
- Créez un schéma pour le compte utilisateur IBM Cognos Analytics que vous utiliserez pour accéder à la base de données et vérifiez que l'utilisateur dispose de droits de création, de suppression et de modification sur le schéma.
- Créez un profil qui extrait le fichier `sqllib/db2profile` du répertoire de base de l'utilisateur Db2. Par exemple, le contenu de votre profil sera semblable à ce qui suit :

```
   if
[ -f /home/db2user/sqllib/db2profile ]; then
./home/db2user/sqllib/db2profile
fi
```

- L'administrateur des bases de données doit effectuer une sauvegarde régulière des bases de données IBM Cognos Analytics, car elles contiennent toutes les données IBM Cognos. Pour garantir la sécurité et l'intégrité des bases de données, protégez-les contre tout accès non autorisé ou inapproprié.

## Paramètres suggérés pour la création du magasin de contenu sous IBM Db2 on z/OS

La base de données créée pour Content Store doit contenir les paramètres de configuration définis.

Pour que l'installation aboutisse, utilisez les instructions suivantes lors de la création du magasin de contenu.

Utilisez la liste de contrôle ci-dessous pour vous guider dans le processus de configuration du magasin de contenu dans Db2 on z/OS.

- Connectez-vous au système z/OS en tant qu'utilisateur ayant les privilèges d'administrateur système (SYSADM) ou de contrôle système (SYSCTRL) dans Db2 pour créer la base de données.
- Créez une instance de base de données, un groupe de stockage et un compte utilisateur pour le magasin de contenu.

  IBM Cognos Analytics utilise les données d'identification du compte utilisateur pour communiquer avec le serveur de bases de données.
- Réservez un groupe de mémoire tampon avec une taille de page de 32 Ko et un autre avec une taille de page de 4 Ko pour l'instance de base de données.
- Les administrateurs doivent exécuter un script pour créer des espaces de table contenant des objets LOB et d'autres données pour le magasin de contenu et octroyer des droits d'utilisation des espaces de table aux utilisateurs. Pour en savoir davantage sur l'exécution du script, reportez-vous à la section «Création d'espaces de table pour un magasin de contenu sur IBM Db2 for z/OS», à la page 70.
- L'administrateur des bases de données doit effectuer une sauvegarde régulière du magasin de contenu car il contient les informations sur l'application de données IBM Cognos et la sécurité. Pour garantir la sécurité et l'intégrité de la base de données du magasin de contenu, protégez-la contre tout accès non autorisé ou inapproprié.

## Paramètres suggérés pour la création du magasin de contenu dans Oracle

La base de données créée pour Content Store doit contenir les paramètres de configuration définis.

Pour que l'installation aboutisse, utilisez les instructions suivantes lors de la création du magasin de contenu. Utilisez les mêmes directives pour créer une base de données des messages de journal.

Utilisez la liste ci-dessous pour vous guider dans le processus de configuration du magasin de contenu sur Oracle.

- Vérifiez que le paramètre relatif au niveau de compatibilité de l'instance de base de données du magasin de contenu est défini sur 9.0.1 ou plus.

Par exemple, vous pouvez vérifier le paramètre d'initialisation COMPATIBLE en émettant l'instruction SQL suivante : `SELECT nom, valeur, description FROM v$parameter WHERE nom='compatible';`

Pour en savoir davantage sur la modification du paramètre de configuration d'une instance, reportez-vous à la documentation Oracle.

- Déterminez si la base de données utilise le format Unicode.

  **Conseil :** L'une des méthodes consiste à saisir l'instruction select suivante :

  `select * from NLS_DATABASE_PARAMETERS`

  Si l'ensemble de résultats renvoie un élément NLS_CHARACTERSET non Unicode, créez une base de données en définissant AL32UTF8 comme paramètres du jeu de caractères de base de données.

  Si vous utilisez le mode de requête compatible, il est recommandé de spécifier la variable d'environnement COGUDA_EXTENDEDCHAR_SUPPORT avec la valeur `T` ou `t`. Cette variable remplace les expressions substring par SUBSTRC pour qu'Oracle renvoie les résultats corrects lorsque la chaîne contient des caractères Unicode supplémentaires.
- Indiquez quel compte utilisateur sera utilisé pour accéder à la base de données.

  **Conseil :** Si vous voulez héberger plusieurs magasins de contenu sur votre instance Sybase et les utiliser simultanément, utilisez un compte utilisateur différent pour chacun, pour que chaque instance d'IBM Cognos Analytics soit parfaitement isolée des autres.
- Assurez-vous que le compte utilisateur qui accède à la base de données dispose des droits nécessaires pour effectuer les opérations suivantes :
  - Connexion à la base de données
  - Création, modification et suppression de déclencheurs, de vues, de procédures et de séquences
  - Création et modification de tables
  - Insertion, mise à jour et suppression de données dans les tables de la base de données
- L'administrateur des bases de données doit effectuer une sauvegarde régulière des bases de données IBM Cognos Analytics, car elles contiennent toutes les données Cognos. Pour garantir la sécurité et l'intégrité des bases de données, protégez-les contre tout accès non autorisé ou inapproprié.

## Paramètres suggérés pour la création du magasin de contenu sous Microsoft SQL Server

La base de données créée pour Content Store doit contenir les paramètres de configuration définis.

Pour que l'installation aboutisse, utilisez les instructions suivantes lors de la création du magasin de contenu. Utilisez les mêmes directives pour créer une base de données des messages de journal.

Utilisez la liste de contrôle ci-dessous pour vous guider dans le processus de configuration du magasin de contenu sur Microsoft SQL Server.

- Veillez à ce que la séquence de classement ne prenne pas en compte la distinction entre majuscules et minuscules.

  Dans le cadre d'une installation personnalisée, vous choisissez un classement, qui comprend des jeux de caractères et un ordre de tri, lors de la configuration de Microsoft SQL Server. Dans le cadre d'une installation standard, l'installation

utilise les paramètres régionaux identifiés par le programme d'installation pour le classement. Par la suite, ce paramètre ne pourra pas être modifié.

- Lorsque vous vous connectez à Microsoft SQL Server Management Studio pour créer la base de données, utilisez l'authentification de Microsoft SQL Server.

  Si vous vous connectez à l'aide de l'authentification Microsoft Windows, la base de données que vous allez créer utilisera également ce type d'authentification. Dans cette situation, vous devez configurer la connexion à la base de données via un type de **Base de données Microsoft SQL Server (Authentification Windows)** dans IBM Cognos Configuration.
- A partir du compte utilisateur qui sera utilisé pour accéder à la base de données, créez un nouvel identifiant sous **Security** et utilisez les paramètres suivants :
  - Sélectionnez **SQL Server authentication**.
  - Désélectionnez la case **Enforce password policy**.

  **Conseil :** Si vous voulez héberger plusieurs magasins de contenu sur votre instance Microsoft SQL Server et les utiliser simultanément, utilisez un compte utilisateur différent pour chacun, pour que chaque instance d'IBM Cognos Analytics soit parfaitement isolée des autres.
- Pour Microsoft SQL Server 2008, octroyez des droits d'exécution au compte utilisateur accédant à la base de données.
- Pour la base de données du magasin de contenu, créez une base de données sous **Databases**.
- Sous l'option **Security** associée à la nouvelle base de données, créez un schéma et affectez-lui un nom.
- Sous l'option **Security** associée à la nouvelle base de données, créez un utilisateur avec les paramètres ci-dessous :
  - Pour **Login name**, indiquez le nouvel identifiant créé pour le compte utilisateur.
  - Pour **Default schema**, indiquez le nouveau schéma.
  - Pour **Owned Schemas**, sélectionnez le nouveau schéma.
  - Pour **Role Members**, sélectionnez **db_datareader**, **db_datawriter** et **db_ddladmin**.

## Paramètres suggérés pour la création du magasin de contenu sur le serveur de base de données IBM Informix

La base de données que vous avez créée pour le magasin de contenu IBM Cognos Analytics doit contenir des paramètres de configuration spécifiques.

Utilisez les directives suivantes lors de la création du magasin de contenu. Utilisez les mêmes directives pour créer une base de données des messages de journal.

Utilisez la liste de contrôle ci-dessous pour vous guider dans le processus de configuration du magasin de données dans la base de données du serveur de base de données IBM Informix.

- Définissez les variables d'environnement suivantes :
  - Définissez **GL_USEGLU** sur 1 pour activer ICU (International Components for Unicode) dans le serveur de base de données Informix.
  - Définissez **DB_LOCALE** su `en_us.utf8` pour définir Unicode comme jeu de caractères de l'environnement local de la base de données.
- Créez une base de données au mode ANSI en activant la journalisation.

- Autorisez le privilège d'administration de la base de données pour le compte utilisateur utilisé afin d'accéder à la base de données.

  **Important :** Si vous hébergez plusieurs bases de données sur votre instance Informix et les utilisez simultanément, utilisez un compte utilisateur différent pour chaque base de données. Vous devez également définir le compte utilisateur de chaque instance de l'application IBM Cognos Configuration en créant un paramètre de propriété avancée et en spécifiant le compte utilisateur en tant que valeur. Dans le cas de bases de données de journalisation multiples, nommez la propriété **CMSCRIPT_CS_ID**. Dans le cas de bases de données de journalisation multiples, nommez la propriété **IPFSCRIPTIDX**.

## Configuration d'un compte utilisateur ou d'un compte de service réseau pour IBM Cognos Analytics

Vous pouvez configurer un compte utilisateur ou un compte de service réseau pour IBM Cognos Analytics.

Le compte utilisateur ou le compte de service réseau sous lequel IBM Cognos Analytics est exécuté doit :

- avoir accès à toutes les ressources requises, telles que les imprimantes,
- être autorisé à se connecter en tant que service et à agir en tant qu'élément du système d'exploitation.

En outre, le compte utilisateur doit appartenir au groupe d'administrateurs local.

Par exemple, pour imprimer des rapports à l'aide d'une imprimante réseau, il est nécessaire que le compte ait accès à celle-ci ou que vous affectiez un compte de connexion au service IBM Cognos.

### Configuration d'un compte utilisateur

Pour Microsoft Windows, affectez un nom de connexion au service IBM Cognos. Sous Windows, vous pouvez configurer le service IBM Cognos pour qu'il utilise un compte utilisateur spécial en sélectionnant le service IBM Cognos dans la liste de services affichée dans la fenêtre Services. Vous avez ensuite la possibilité de définir les propriétés du compte utilisateur.

Pour UNIX ou Linux, créez un groupe UNIX ou Linux, cognos, par exemple. Ce groupe doit contenir l'utilisateur qui est propriétaire des fichiers IBM Cognos. Définissez les droits de propriétaire des fichiers IBM Cognos pour le groupe cognos et définissez les droits d'accès à tous les fichiers IBM Cognos sur GROUP READABLE/WRITABLE/EXECUTABLE.

Vous devez configurer le serveur Web pour utiliser des alias. Pour en savoir davantage, reportez-vous à la rubrique concernant la configuration du serveur Web.

### Configuration d'un compte de service réseau

Le compte de service réseau est le compte intégré NT AUTHORITY\ NetworkService stocké dans le système d'exploitation. Les administrateurs n'ont pas besoin de gérer un mot de passe ou le compte.

Utilisez un compte ayant des privilèges d'administrateur si vous installez sur le serveur Windows 2008.

Vous devez configurer le serveur Web pour utiliser le groupe d'applications. Pour en savoir davantage, reportez-vous à la rubrique concernant la configuration du serveur Web. Vous devez aussi disposer de droits d'écriture pour faire des installations sur le répertoire.

# Configuration des navigateurs Web

Les composants IBM Cognos Analytics utilisent les configurations de navigateur par défaut. Les paramètres supplémentaires requis sont spécifiques au navigateur.

## Paramètres de navigateurs requis pour Cognos Analytics

Le tableau suivant indique les paramètres à activer.

*Tableau 7. Paramètres de navigateur activés*

| Navigateur | Paramètre |
|---|---|
| Internet Explorer | Autoriser les cookies de connexion<br>Script actif<br>META REFRESH autorisé<br>Exécuter les contrôles ActiveX et les plug-in<br>Contrôles ActiveX reconnus sûrs pour l'écriture de scripts<br>Comportements binaires et de script<br>Autoriser l'accès programmatique au Presse-papiers<br>Persistance des données utilisateur |
| Firefox | Autoriser les cookies de connexion<br>Activer Java<br>Activer JavaScript<br>Charger des images |
| Safari 5 | Activer Java<br>Activer JavaScript<br>Bloquer les cookies : Jamais |
| Google Chrome | Cookies: Autoriser la définition des données locales<br>Images : Afficher toutes les images<br>JavaScript : Autoriser tous les sites à exécuter JavaScript |

Reporting et Query Studio utilisent la norme native XML de Microsoft Internet Explorer, qui est un composant du navigateur. La prise en charge de la technologie ActiveX doit être activée, car les applications Microsoft l'utilisent pour implémenter

le langage XML. Cognos Analytics ne fournit ni ne télécharge de contrôles ActiveX. Seuls les contrôles ActiveX installés en même temps qu'Internet Explorer sont activés pour cette configuration.

Si vous utilisez Microsoft Internet Explorer, vous pouvez ajouter l'URL de vos passerelles à la liste des sites de confiance. Par exemple, `http://<nom_serveur>:<numéro_port>/ibmcognos`. Ceci active l'invite automatique pour les téléchargements de fichiers.

Autorisez les fenêtres en incrustation pour toutes les pages Cognos Analytics, pour tous les navigateurs.

## Cookies utilisés par les composants Cognos Analytics

Cognos Analytics utilise les cookies suivants pour stocker des informations utilisateur :

*Tableau 8. Cookies utilisés par les composants Cognos Analytics*

| Cookie | Type | Fonction |
|---|---|---|
| AS_TICKET | Session temporaire | Il est créé si Cognos Analytics est configuré pour utiliser un espace-noms IBM Cognos Series 7. |
| caf | Session temporaire | Contient des informations sur l'état de la sécurité. |
| Cam_passport | Session temporaire | Contient une référence à une session utilisateur stockée sur le serveur Content Manager.<br><br>Les administrateurs peuvent définir l'attribut HTTPOnly pour empêcher des scripts de lire ou de manipuler le cookie du passeport CAM lors d'une session utilisateur avec le navigateur Web.<br><br>Pour plus d'informations, voir le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*. |
| cc_session | Session temporaire | Conserve les informations de session |
| cc_state | Session temporaire | Conserve des informations pendant les opérations d'édition (par exemple, couper, copier, coller). |
| CRN | Session temporaire | Contient des informations régionales sur le produit et le contenu. Défini pour tous les utilisateurs d'IBM Cognos. |
| CRN_RS | Permanent | Enregistre le choix effectué par l'utilisateur pour l'option Afficher le dossier des membres dans Reporting. |

*Tableau 8. Cookies utilisés par les composants Cognos Analytics (suite)*

| Cookie | Type | Fonction |
|---|---|---|
| PAT_CURRENT_ FOLDER | Permanent | Contient le chemin du dossier en cours si l'accès au fichier local est utilisé. Mis à jour après utilisation de la boîte de dialogue Ouvrir ou Enregistrer. |
| qs | Permanent | Enregistre les paramètres sélectionnés par l'utilisateur pour les éléments d'interface utilisateur tels que les menus et les barres d'outils. |
| userCapabilities | Session temporaire | Contient toutes les fonctions et la signature de l'utilisateur en cours. |
| usersessionid | Session temporaire | Contient un identificateur de session utilisateur unique, valide uniquement pour la durée de la session de navigateur. |
| XSRF (Cross-Site Request Forgery) | Session temporaire | XSRF pousse un navigateur Web à exécuter une action malveillante sur un site de confiance auprès duquel l'utilisateur est actuellement authentifié. XSRF exploite la confiance qu'a un site dans le navigateur d'un utilisateur.<br><br>Empêche une page Web chargée à partir du domaine X d'envoyer des demandes au domaine Y, en supposant que l'utilisateur est déjà authentifié auprès du domaine Y.<br><br>Lors de votre première authentification auprès de Cognos Analytics, le cookie XSRF est défini. Dès cet instant, toutes les demandes nécessiteront le cookie XSRF-TOKEN et un en-tête HTTP appelé X-XSRF-TOKEN. |

Après avoir mis à niveau ou installé un nouveau logiciel, redémarrez le navigateur Web et demandez aux utilisateurs de vider le cache du navigateur.

# Chapitre 2. Options de répartition

Avant la mise en oeuvre de IBM Cognos Analytics, déterminez son mode d'installation dans votre environnement. Vous pouvez installer tous les composants serveur sur un ordinateur ou les répartir sur un réseau. Le choix du mode de répartition dépend de vos besoins en matière d'exécution de rapports, de vos ressources et de vos préférences. La configuration requise varie selon que vous installez tous les composants sur un ordinateur, ou que vous les répartissez sur plusieurs ordinateurs.

Cognos Analytics est compatible avec d'autres produits Cognos. Si votre environnement comprend d'autres produits Cognos, vous devez étudier la façon dontCognos Analytics va s'y intégrer.

Cognos Analytics ne peut pas être installé au même emplacement que d'autres produits Cognos, comme Cognos Framework Manager, Cognos Transformer, Cognos PowerPlay, etc.

## Composants Cognos Analytics

IBM Cognos Analytics est une solution Web d'information décisionnelle qui intègre entre autres des fonctionnalités de génération de rapport et de tableaux de bord, d'analyse, de gestion d'événements. Cognos Analytics comprend des composants de serveur et de modélisation.

Cognos Analytics s'intègre aisément dans votre infrastructure existante en exploitant les ressources qui se trouvent dans votre environnement. Certaines de ces ressources existantes sont indispensables, par exemple une base de données pour le magasin de contenu. D'autres ressources sont facultatives, par exemple un fournisseur de sécurité pour l'authentification.

**Conseil :** Lorsque Cognos Analytics est installé par le biais de l'option **Installation facile**, il ne vous est pas nécessaire de configurer une base de données de magasin de contenu ou un fournisseur de sécurité. Le produit est préconfiguré et prêt à être utilisé.

IBM Cognos Analytics utilise le serveur d'application WebSphere Application Server Liberty Profile.

### Composants serveur

Les composants serveur d'IBM Cognos Analytics forment trois groupes distincts : données, applications et passerelle facultative.

Les composants serveur offrent à l'utilisateur des interfaces pour la génération de rapports et de tableaux de bord, l'analyse, la gestion d'événements, etc., ainsi que la fonctionnalité permettant d'acheminer et de traiter les requêtes des utilisateurs.

Dans le programme d'installation, vous pouvez choisir d'installer les composants serveur suivants :

- «Couche de données : Content Manager», à la page 20
- «Groupe de serveurs d'applications : composants», à la page 20

- «Couche passerelle facultative : communication Web», à la page 22

  **Conseil :** La passerelle facultative n'est nécessaire que pour Kerberos.

En tant que composant serveur facultatif, vous pouvez également installer des exemples Cognos Analytics. A l'aide de données d'une société fictive, Vacances et Aventure, les exemples illustrent les fonctions du produit, ainsi que les meilleures pratiques en termes techniques et professionnels. Vous pouvez utiliser les exemples pour tester et partager des techniques de conception de rapports, ainsi que pour le traitement des incidents. Pour plus d'informations, voir le *%%Guide des exemples pour IBM Cognos Analytics*.

## Couche de données : Content Manager

Content Manager est le service d'IBM Cognos Analytics qui gère le stockage des données d'application, notamment la sécurité, les données de configuration, les modèles, ou encore les spécifications et les sorties de rapports, etc.

Content Manager est nécessaire pour publier des packs, extraire et stocker des spécifications de rapports, gérer des informations de planification ou encore gérer l'espace-noms de Cognos.

Content Manager stocke des informations dans une base de données de magasin de contenu.

## Groupe de serveurs d'applications : composants

Le groupe des serveurs d'applications IBM Cognos Analytics contient un ou plusieurs serveurs Cognos Analytics. Les serveurs exécutent des demandes, comme des rapports, des analyses et des requêtes transmises par la passerelle, puis affichent les interfaces.

### Configuration et gestion du produit - IBM Cognos Configuration

IBM Cognos Configuration permet de configurer Cognos Analytics, ainsi que de démarrer et d'arrêter ses services.

### Publication, gestion et affichage du contenu - Portail Cognos Analytics

Le portail Cognos Analytics offre un point d'accès unique aux données d'entreprise disponibles pour ses produits. Il offre un point d'entrée unique pour interroger, analyser et organiser les données, ainsi que pour créer des rapports, des scorecards et des événements. Les utilisateurs peuvent exécuter toutes leurs applications Web Cognos Analytics par l'intermédiaire du portail. Les autres applications, ainsi que les adresses URL vers d'autres applications, peuvent être intégrées au portail.

### Reporting professionnel

L'outil Reporting permet aux auteurs de créer, d'éditer et de distribuer une large gamme de rapports de qualité professionnelle.

### Dashboarding

Cognos Analytics fournit des tableaux de bord pour communiquer des informations et des analyses. Vous pouvez créer une vue qui contient des visualisations telles qu'un graphique, un diagramme, un tracé, un tableau, une carte ou toute autre représentation visuelle des données.

Un tableau de bord est un type de vue qui permet de surveiller des événements ou des activités d'un seul coup d'oeil. Il présente sur une ou plusieurs pages (ou un ou plusieurs écrans) des informations clés et des analyses sur les données.

### Administration centrale - Gestion et console d'administration

Cognos Analytics dispose d'une fonction **Gérer**, avec laquelle vous pouvez effectuer des tâches courantes d'administration au quotidien. Une option du menu **Gérer** ouvre la **Console d'administration**, une interface de gestion centrale qui contient les tâches d'administration d'IBM Cognos Analytics. Elle permet d'accéder facilement aux tâches de gestion globale de l'environnement IBM Cognos. L'accès aux tâches d'administration dépend des droits de l'utilisateur.

### IBM Cognos Mobile

IBM Cognos Mobile étend Cognos Analytics et la gestion des performances aux périphériques mobiles. Avec son client enrichi, Cognos Mobile permet aux utilisateurs d'afficher sur leur périphérique des rapports, des tableaux de bord et des analyses Cognos Analytics générés par des outils tels que Reporting, Query Studio, Analysis Studio et Cognos Workspace. Cognos Mobile fournit en temps utile des informations riches et interactives destinées à aider les utilisateurs nomades dans leurs processus décisionnels, quel que soit leur emplacement.

Cognos Mobile traite chaque rapport Cognos Analytics qu'il reçoit et l'affiche dans un format adapté aux périphériques mobiles.

Cognos Mobile utilise les fonctionnalités d'invite et de mécanismes de planification de Cognos Analytics pour fournir des rapports personnalisés de façon opportune. Pour plus d'informations sur les invites, voir le manuel *IBM Cognos Analytics - Reporting - Guide d'utilisation*. Pour plus d'informations sur les plannings, reportez-vous au manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Cognos Mobile utilise la sécurité Cognos Analytics, implémente des mesures de sécurité supplémentaires spécifiques aux applications mobiles, optimise diverses architectures de sécurité spécifiques à des tiers, et tire parti des mesures de sécurité du périphérique et du serveur.

De nombreux serveurs de gestion spécifiques aux périphériques et de nombreux outils d'administration utilisés par Cognos Mobile offrent la possibilité de supprimer à distance un contenu sur un périphérique ou de désactiver celui-ci complètement. Ainsi, par exemple, lorsqu'un périphérique est perdu ou volé, l'administrateur Cognos Analytics peut utiliser cette fonctionnalité pour protéger le contenu sensible sur le périphérique. L'administrateur Cognos Analytics dispose également de la possibilité de définir une date d'expiration pour un rapport, après laquelle le rapport devient inaccessible jusqu'à ce que l'utilisateur s'authentifie à nouveau. Pour plus d'informations sur la sécurité Cognos Analytics, reportez-vous au manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*. Pour plus d'informations sur la gestion et la sécurité des périphériques, consultez leur documentation.

Cognos Mobile prend également en charge les requêtes entre le périphérique mobile et l'environnement de serveur pour les fonctions produit de recherche, d'exploration et d'exécution :

Vous devez installer et exécuter des versions identiques pour Cognos Mobile et le serveur Cognos Analytics.

### Requête ad hoc et génération de rapports libre-service - Query Studio

Query Studio permet aux utilisateurs disposant de connaissances limitées de concevoir, de créer et d'enregistrer des rapports qui répondent aux besoins non couverts par les rapports standard de qualité professionnelle créés dans Reporting.

### Repérage des conditions exceptionnelles par contrôle des données - Event Studio

Dans Event Studio, vous définissez des agents pour suivre vos données et exécuter des tâches lorsque vous devez faire face à des conditions exceptionnelles ou des événements qui s'y rapportent. Lorsqu'un événement survient, les utilisateurs sont alertés afin qu'ils puissent réagir. Les agents peuvent publier des informations détaillées sur le portail, envoyer des alertes par courrier électronique, exécuter et distribuer des rapports basés sur les événements, ainsi que surveiller l'évolution de ces derniers. Par exemple, la demande d'assistance d'un client important ou l'annulation d'une grosse commande peut déclencher un événement, par exemple l'envoi d'un courrier électronique aux personnes concernées.

### Facilitation de la prise de décision - IBM Cognos Workspace

Vous pouvez créer des espaces de travail interactifs élaborés à l'aide de contenus IBM Cognos et de sources de données externes, telles que des feuilles Web ou des cubes TM1 en fonction de vos besoins d'informations spécifiques. Vous pouvez afficher et ouvrir des espaces de travail ou des rapports favoris, manipuler le contenu et transmettre par courrier électronique le résultat de vos recherches. Vous pouvez également utiliser des commentaires et des activités pour faciliter les prises de décision collaboratives.

Vous pouvez également utiliser des logiciels de communication tels que IBM Connections pour faciliter les prises de décision collaboratives.

### Compatibilité Microsoft Office - IBM Cognos for Microsoft Office

IBM Cognos for Microsoft Office permet aux utilisateurs de Microsoft Office d'accéder aux données et aux visualisations des rapports IBM Cognos au sein des applications Microsoft Office, comme Excel, PowerPoint et Word.

Les composants Cognos for Microsoft Office sont inclus avec Cognos Analytics et doivent être installés séparément.

### Couche passerelle facultative : communication Web

Les passerelles sont souvent des programmes CGI mais elles peuvent suivre d'autres normes, telles que ISAPI (Internet Server Application Program Interface) et Apache Modules (apache_mod). IBM Cognos Analytics utilise exclusivement CGI, ISAPI ou Apache module pour Kerberos. Sinon, il ne vous est pas nécessaire de configurer une passerelle.

Dans IBM Cognos Analytics, le groupe de serveurs d'application fournit les fonctions d'une passerelle.

## Composants de modélisation

Les composants de modélisation modélisent des données dans des sources de données afin de structurer et de présenter ces données de façon à ce qu'elles puissent être appréhendées par l'utilisateur. Les composants de modélisation incluent les outils suivants :

## Modélisation Web avec IBM Cognos Analytics

IBM Cognos Analytics est doté d'un outil de modélisation ultra-économique qui permet de créer simplement et rapidement des modules de données à partir de différentes sources. Les sources utilisées pour créer des modules de données peuvent être des serveurs de données, des fichiers téléchargés et des modules déjà enregistrés. Cognos Analytics utilise la modélisation intentionnelle des données pour générer un module à partir des termes que vous avez définis. Pour plus de détails sur toutes les fonctions disponibles, reportez-vous au manuel *IBM Cognos Analytics - Guide de modélisation des données*.

Les fonctions de modélisation des données de Cognos Analytics ne remplacent pas les fonctions de modélisation plus complexes d'IBM Cognos Framework Manager ou d'IBM Cognos Cube Designer. Ces outils restent disponibles dans Cognos Analytics.

## Création d'une vue métier de vos données - Framework Manager

IBM Cognos Framework Manager est l'outil de modélisation permettant de créer et de gérer des métadonnées d'entreprise utilisées dans IBM Cognos Analytics. Les métadonnées sont publiées de façon à être utilisées par des outils de génération de rapports sous forme de pack, offrant ainsi une vue métier intégrée unique d'un éventail de sources de données.

Framework Manager doit être installé à un emplacement différent de Cognos Analytics.

## Modélisation ROLAP - Cube Designer

IBM Cognos Cube Designer est l'outil de modélisation fourni avec IBM Cognos Dynamic Cubes. Il permet de créer des cubes dynamiques et de les publier pour être utilisés dans IBM Cognos Analytics.

Pour commencer, importez des métadonnées à partir d'une base de données relationnelle. A l'aide des métadonnées, modélisez des cubes dynamiques et enregistrez leurs définitions dans un projet. Les cubes publiés sont répertoriés en tant que sources de données dans Content Manager et les packs associés sont disponibles pour les auteurs de rapport.

Cube Designer doit être installé à un emplacement différent de Cognos Analytics.

## Création de modèles multidimensionnels - IBM Cognos Transformer

IBM Cognos Transformer est l'outil de modélisation d'IBM Cognos Analytics utilisé pour créer des PowerCubes à utiliser dans IBM Cognos Analytics. Les PowerCubes IBM Cognos Analytics sécurisés ne sont pas compatibles avec IBM Cognos Series 7.

Transformer doit être installé à un emplacement différent de Cognos Analytics.

**Conseil :** Pour en savoir davantage sur l'installation et la configuration de versions de Transformer antérieures à la 8.4, reportez-vous à la documentation fournie avec votre édition de Transformer.

### Importation et gestion des cartes (cartes Map Manager existantes uniquement)

IBM Cognos Map Manager est un utilitaire Windows permettant aux administrateurs et aux modélisateurs d'importer des cartes et de mettre à jour leur libellé dans Reporting. Pour les éléments de cartes, tels que les noms de pays et de villes, les administrateurs et les modélisateurs peuvent définir d'autres noms afin de fournir des versions multilingues du texte apparaissant sur la carte.

Map Manager doit être installé à un emplacement différent de Cognos Analytics.

Pour plus d'informations, reportez-vous au *Guide d'installation et d'utilisation d'IBM Cognos Map Manager*.

## Composants de base de données requis

Outre les outils fournis, IBM Cognos Analytics requiert les composants suivants créés à l'aide d'autres ressources.

### Magasin de contenu

Le magasin de contenu est une base de données relationnelle qui contient des données dont Cognos Analytics a besoin pour fonctionner. Il s'agit de spécifications de rapports, de modèles publiés et des packs qui les contiennent, ainsi que des informations de connexion pour les sources de données, des informations sur les espace-noms externes et celui de Cognos, ou encore des informations sur la planification et la diffusion de rapports en rafale, etc.

Lors de la configuration de votre environnement Cognos Analytics, configurez le magasin de contenu de manière à utiliser une base de données prise en charge qui soit sécurisée et calibrée dans un objectif de performances et de stabilité. Pour en savoir davantage, reportez-vous à la rubrique traitant du déploiement complet de la base de données du magasin de contenu dans le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Les modèles de conception et les fichiers journaux ne sont pas stockés dans le magasin de contenu.

Le service IBM Cognos  qui utilise la base de données du magasin de contenu s'appelle Content Manager.

### Sources de données

Les sources de données, également appelées bases de données de requêtes, sont des bases de données relationnelles, des cubes dimensionnels ou OLAP, des fichiers ou d'autres types de magasins de données physiques accessibles par l'intermédiaire d'Cognos Analytics. Les composants du groupe de serveurs d'applications utilisent des connexions spécifiques pour accéder aux sources de données.

## Composants Cognos Mobile

IBM Cognos Mobile inclut le service Cognos Mobile et l'application Cognos Mobile. Ces composants sont installés avec IBM Cognos Analytics.

Une fois le service Cognos Mobile configuré, les utilisateurs peuvent installer l'application Cognos Mobile sur leur unité mobile pour accéder au contenu d'Cognos Analytics, notamment des rapports et des tableaux de bord. Pour utiliser l'application, les utilisateurs téléchargent la version iOS depuis l'Apple App Store ou la version Android depuis le Google Play Store.

Le service Cognos Mobile gère les opérations suivantes :

- Il envoie par commande push le contenu des rapports et des analyses vers les périphériques mobiles.
- Il facilite les demandes entrantes et sortantes liées aux rapports et aux analyses entre le périphérique mobile et l'environnement dans lequel s'effectue la recherche, la navigation et l'exécution des rapports.
- Il synchronise le magasin de contenu Mobile sur le serveur avec la base de données Mobile sur le périphérique mobile.
- Il communique avec le périphérique mobile.

L'unité mobile contient l'application Cognos Mobile et le magasin de contenu Mobile compressé et chiffré. Ces composants fournissent les fonctions dont l'utilisateur du périphérique mobile a besoin pour utiliser les rapports, les tableaux de bord et les analyses Cognos Analytics.

Le diagramme ci-dessous illustre la façon dont les composants interagissent dans l'environnement Cognos Analytics. Les périphériques mobiles se connectent au serveur IBM Cognos par Internet et le réseau de télécommunication sans fil avec HTTP.

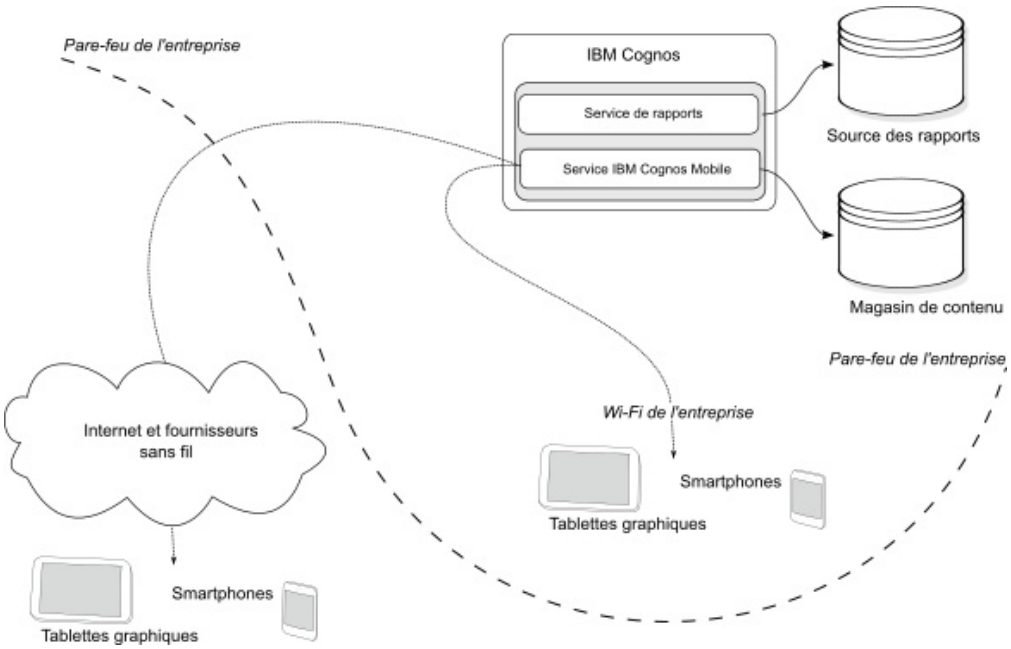



*Figure 1. Composants Cognos Mobile dans l'environnement Cognos Analytics*

## Répartition des composants

Lors de l'installation des composants serveur IBM Cognos Analytics, vous devez préciser l'emplacement des composants de groupe de serveurs d'application, de la couche données (Content Manager) et de la couche passerelle facultative.

Vous pouvez utiliser les scénarios d'installation suivants :

- Installer tous les composants sur un ordinateur.

  Cette option est habituellement utilisée pour un déploiement dans un service, sur un système de démonstration ou dans un environnement de banc d'essai.
- Installer les composants du groupe de serveurs d'applications et Content Manager sur des ordinateurs distincts.

  Choisissez cette option pour optimiser les performances, la disponibilité, la capacité ou la sécurité en fonction des caractéristiques de traitement de votre organisation.
- Installer la passerelle facultative sur un ordinateur distinct.

  Si vous choisissez cette option, la passerelle et le serveur web se trouvent sur le même ordinateur, et les composants de Cognos restants figurent sur d'autres ordinateurs. Vous pouvez choisir cette option si vous disposez de serveurs Web existants qui sont disponibles pour gérer les demandes des composants Cognos Analytics.
- Regrouper plusieurs serveurs en effectuant l'installation sur System z.

  IBM Cognos Analytics est pris en charge sous Linux on System z. Ce type d'installation est approprié lorsque vous configurez ou personnalisez une installation dans votre environnement en vue de répondre aux exigences de vos systèmes et infrastructures informatiques.

Après avoir installé les composants serveur, vous devez les configurer afin qu'ils puissent communiquer entre eux.

Outre les composants de la couche données (Content Manager), du groupe de serveurs d'application, et de la couche passerelle facultative, vous pouvez également installer Cognos Framework Manager, l'outil de modélisation de métadonnées, ainsi que Cognos Transformer, l'outil de modélisation permettant de créer des PowerCubes. Quel que soit le scénario d'installation d'IBM Cognos choisi, installez les composants de modélisation dans des emplacements différents.

## Installation des composants du groupe de serveurs d'applications et des applications Content Manager des ordinateurs distincts

Les composants du groupe de serveurs d'applications équilibrent les charges, accèdent aux données, effectuent les requêtes, programment les travaux et affichent les rapports. Content Manager conserve l'ensemble des spécifications de rapports, des résultats, des packs, des dossiers et des travaux dans le magasin de contenu.

Vous pouvez installer les composants du groupe de serveurs d'applications et Content Manager sur un ou plusieurs ordinateurs. L'installation sur plusieurs ordinateurs peut améliorer les performances, la disponibilité et la capacité.

### Installation de plusieurs applications Content Manager

Vous pouvez installer un nombre quelconque d'installations de Content Manager, mais une seule est activée à tout instant. Chacune des autres installations agit en tant que Content Manager en veille. Il devient uniquement actif si une panne

survient et affecte l'ordinateur Content Manager actif. Pour prendre en charge la reprise, il est recommandé d'installer Content Manager sur au moins deux ordinateurs.

### Installation de plusieurs gestionnaires de contenu

La base de données Content Manager stocke les données nécessaires au fonctionnement d'IBM Cognos Analytics, notamment les spécifications de rapports, les modèles publiés et les packs les utilisant, les informations de connexion pour les sources de données, les informations relatives à l'espace-noms externe, l'espace-noms de Cognos lui-même et les informations concernant la programmation de rapports et leur diffusion en rafale. Le magasin de contenu est un système de gestion de bases de données relationnelles (RDBMS). A chaque installation d'IBM Cognos n'est associée qu'un seul magasin de contenu.

Vous pouvez choisir d'installer Content Manager séparément des composants du groupe de serveurs d'applications. Par exemple, vous pouvez installer Content Manager au niveau des données plutôt que de l'application.

Lorsqu'un Content Manager actif échoue, toutes les données de session non enregistrées sont perdues. Lorsque le nouveau Content Manager actif prend le relais, les utilisateurs peuvent être invités à se connecter.

Dans le diagramme suivant, la passerelle transmet la requête au répartiteur (non indiqué), qui la transmet à son tour à l'ordinateur Content Manager actif par défaut. L'ordinateur ayant échoué, la demande est redirigée vers l'ordinateur Content Manager de secours, qui s'est activé quand l'ordinateur Content Manager actif par défaut a échoué.

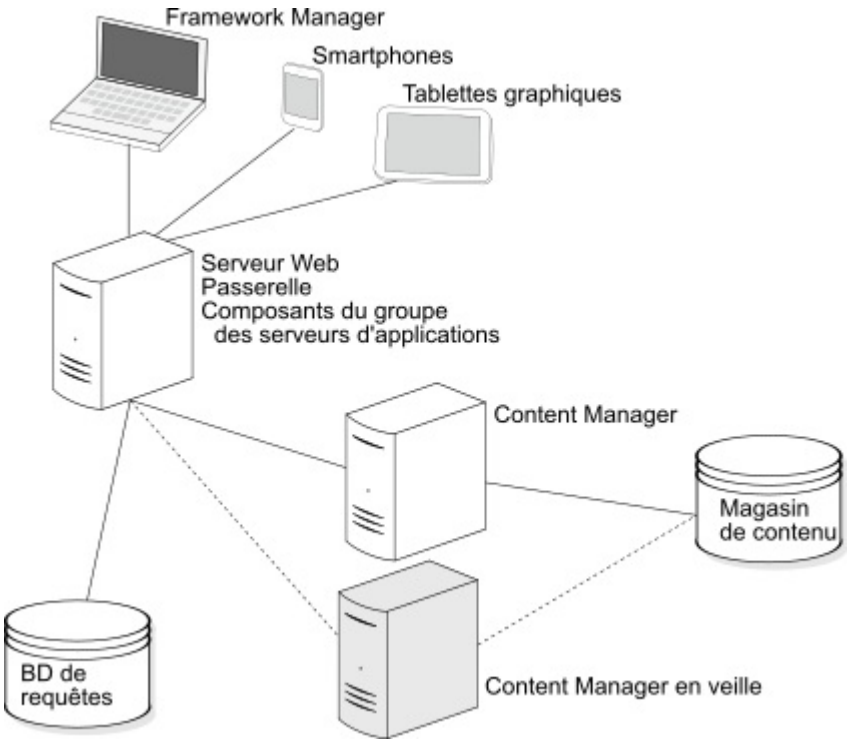



*Figure 2. Installation avec un ordinateur Content Manager actif et un ordinateur Content Manager de secours*

### Configuration requise

Sur chaque ordinateur sur lequel vous avez installé Content Manager, vous devez :

- définir les informations de connexion au magasin de contenu,
- définir les URI du répartiteur,
- définir tous les URI de Content Manager,
- définir l'URI du répartiteur des applications externes,
- configurer une connexion à un serveur de messagerie (si vous souhaitez envoyer des rapports par courrier électronique ou des notifications).

## Ordinateur hébergeant plusieurs composants du groupe de serveurs d'applications

Dans un souci d'amélioration de la modularité dans un environnement où le volume de demandes de rapports à traiter est généralement important, vous pouvez installer les composants du groupe de serveurs d'applications sur plusieurs ordinateurs réservés au traitement des demandes entrantes. En installant les composants du groupe de serveurs d'applications sur plusieurs ordinateurs, vous répartissez et équilibrez les charges entre ordinateurs. Vous bénéficiez également d'une accessibilité et d'un débit accrus par rapport à une installation sur un seul ordinateur, de même que d'une prise en charge des reprises.

### Configuration requise

Pour vous assurer qu'un ou que plusieurs composants du groupe de serveurs d'applications installés sur un ordinateur séparé peuvent communiquer avec les autres composants IBM Cognos Analytics, vous devez :

- définir tous les URI de Content Manager,
- définir les URI du répartiteur,
- définir l'URI du répartiteur des applications externes.

# Regroupement de serveurs pour Linux on System z

Linux on System z est une implémentation native du système d'exploitation Linux. Les options d'hébergement incluent l'exécution de Linux dans une ou plusieurs partitions logiques (LPAR).

## Integrated Facility for Linux (IFL)

Les IFL sont des processeurs System z dédiés à l'exécution de charges de travail Linux soit de façon native ou par l'intermédiaire d'un logiciel de virtualisation, en fonction de vos besoins. Ils permettent de consolider et de gérer centralement les ressources Linux on System z.

## Mode LPAR (Logical partition)

Linux peut s'exécuter en LPAR et communiquer avec d'autres partitions Linux via des connexions TCP/IP.

L'évolutivité horizontale dans un environnement Linux important est limitée par le nombre de LPAR pouvant être créées. L'exécution de Linux en LPAR peut être préférable si vous exécutez un petit nombre d'images Linux, qui utiliseront chacune une grande quantité de puissance de traitement ou vont nécessiter une très grande quantité de mémoire dédiée. Cela garantit que des ressources sous-utilisées ne seront pas allouées aux images.

## Installation des composants de modélisation facultatifs

Installez les outils de modélisation tels que Framework Manager et Transformer sur des ordinateurs Microsoft Windows.

Pour publier les packs et les mettre à la disposition des utilisateurs, vous devez configurer les outils de modélisation facultatifs de manière qu'ils utilisent un répartiteur, directement ou par l'intermédiaire d'une passerelle. Si le portail est sécurisé, vous devez disposer de privilèges pour y créer des sources de données et y publier des packs.

### Remarques sur le pare-feu

Lorsque l'outil de modélisation est situé en dehors du pare-feu réseau qui protège les composants du groupe de serveurs d'applications, des problèmes de communication peuvent se poser au niveau du répartiteur. Pour des raisons de sécurité, la configuration par défaut d'IBM Cognos Analytics empêche le répartiteur d'accepter les requêtes de l'outil de modélisation lorsque ce dernier se situe en dehors du pare-feu réseau.

Un outil de modélisation situé en dehors d'un pare-feu réseau, tel que Framework Manager, ne peut pas traverser le pare-feu réseau pour envoyer des demandes au répartiteur situé sur le serveur d'applications IBM Cognos Analytics. Pour éviter tout problème lors d'une communication via un pare-feu de réseau, installez l'outil de modélisation dans le même niveau architectural que les composants du groupe de serveurs d'applications. Le diagramme suivant illustre l'installation de l'ordinateur Framework Manager sur le pare-feu de réseau et l'établissement réussi de communications avec le répartiteur situé sur le serveur d'applications IBM Cognos Analytics.

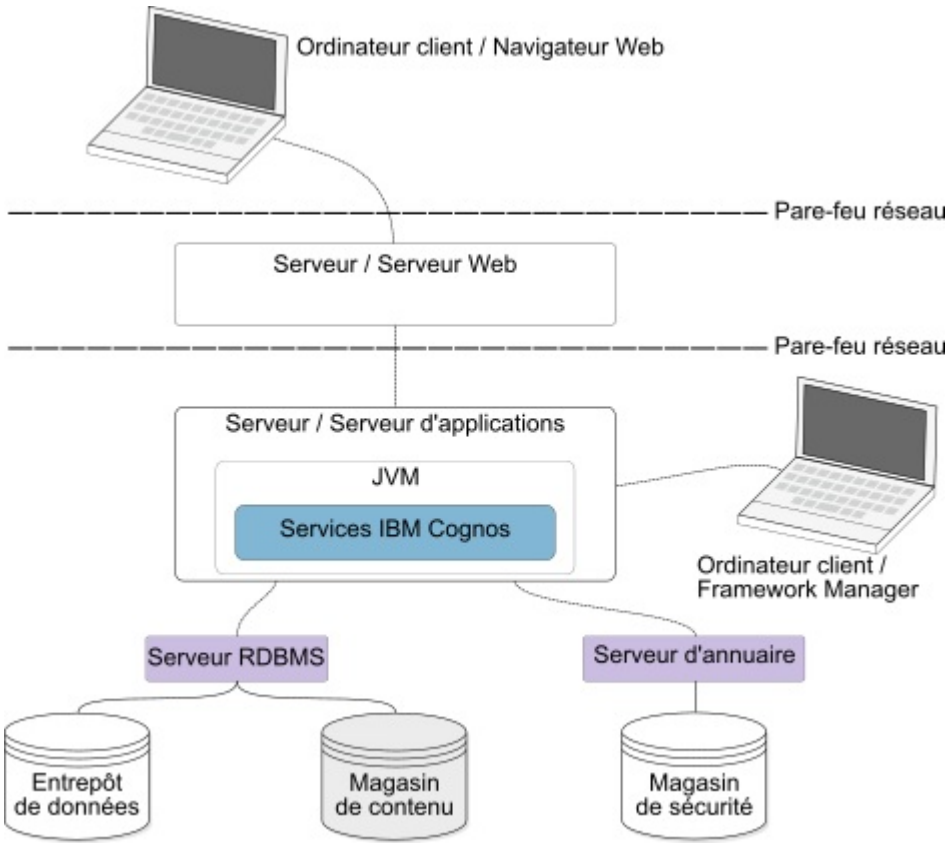



*Figure 3. Ordinateur client à l'extérieur du pare-feu*

Vous pouvez également installer une passerelle supplémentaire dédiée à la communication avec l'outil de modélisation, tel qu'indiqué dans le diagramme ci-après. Vous configurez alors l'outil de modélisation et sa passerelle de façon à ce que le répartiteur accepte les demandes de l'outil de modélisation.

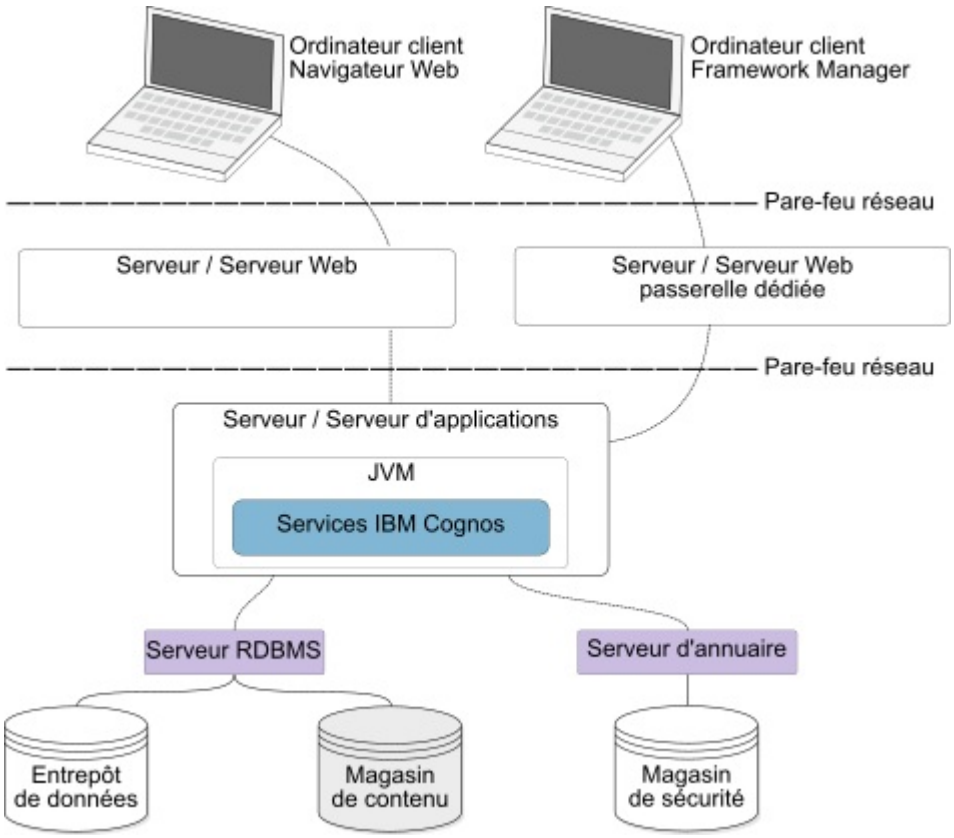



*Figure 4. Ordinateur client à l'extérieur du pare-feu*

## Répartition des composants de Framework Manager

Framework Manager communique avec les composants du groupe de serveurs d'applications, que vous pouvez installer sur un ou plusieurs serveurs d'applications. Pour publier des packs, vous devez configurer Framework Manager pour qu'il communique avec le répartiteur, soit directement, soit par le biais d'une passerelle dédiée.

### Configuration requise

Sur l'ordinateur où Framework Manager est installé, configurez les propriétés d'environnement suivantes :

- **URI de la passerelle**
- **URI du répartiteur pour des applications externes**

Si l'outil de modélisation utilise une passerelle dédiée au lieu de communiquer directement avec le répartiteur, vous devez également configurer la propriété **URI du répartiteur pour la passerelle** sur l'ordinateur de la passerelle dédiée.

## Répartition des composants de Transformer

Transformer peut être installé sur un ordinateur contenant d'autres composants IBM Cognos Analytics ou sur un ordinateur distinct. Lorsque Transformer est installé séparément, il peut être utilisé en tant que produit autonome ou configuré pour communiquer avec d'autres composants IBM Cognos Analytics.

Transformer est constitué des composants ci-dessous. Vous pouvez disposer de l'un de ces composants ou des deux selon votre environnement.

- Transformer sous Windows

  Il s'agit de l'outil de modélisation pour Microsoft Windows qui permet de concevoir des PowerCubes utilisés dans IBM Cognos Analytics. Il permet également de créer et de publier des PowerCubes.

- Transformer sous UNIX or Linux

  Il s'agit d'un utilitaire de ligne de commande permettant de créer des PowerCubes sous UNIX et Linux. Vous concevez d'abord les modèles à l'aide de scripts Transformer Windows ou MDL, puis vous utilisez ces modèles pour créer les PowerCubes.

  Installez les composants de création d'un PowerCube Transformer Linux sur System z.

## Fonctions prises en charge

Lorsque vous utilisez Transformer en tant que produit autonome, vous pouvez employer des sources de données externes à IBM Cognos Analytics et vous ne pouvez pas créer des vues sécurisées à l'aide de filtres dimensionnels. Si vous employez Transformer avec d'autres composants IBM Cognos Analytics, vous pouvez tirer parti des fonctions suivantes d'IBM Cognos Analytics :

- Fournisseurs d'authentification IBM Cognos Analytics
- Sources de données IBM Cognos Analytics, telles que des packs publiés ou des rapports Query Studio et Reporting.

  Les fichiers à plat ne peuvent pas être utilisés en tant que sources de données.
- Portail pour la publication du pack et de la source de données PowerCube
- Création de PowerCubes

## Considérations relatives aux serveurs basés sur des rôles

Vous souhaitez peut-être configurer des serveurs Transformer dédiés pour bénéficier de performances de création de cubes optimales et d'une accessibilité maximale pour les utilisateurs d'IBM Cognos Analytics. Si tel est le cas, tenez compte des exigences suivantes :

- Le logiciel du client de base de données est installé sur un ordinateur où Transformer sera utilisé pour la création de PowerCubes ou le test de sources de données.
- Pour la connectivité des sources de données, configurez les variables d'environnement appropriées pour les serveurs UNIX et Linux.
- Les serveurs IBM Cognos Analytics ont accès à l'emplacement de stockage des PowerCubes, de sorte que le serveur de rapports peut accéder à ces derniers.

La création et la mise à jour de PowerCubes de production peuvent être exécutées par le biais d'un script et effectuées à distance lorsque les privilèges d'accès et les privilèges utilisateur configurés sont suffisants. Pour en savoir davantage sur la création et la mise à jour de PowerCube de production, reportez-vous au *Guide d'utilisation* de Transformer.

## Spécialistes et analystes en informatique de gestion

Certains de vos utilisateurs avancés ou spécialisés souhaitent peut-être créer des PowerCubes modélisés selon des sources de données à la fois personnelles et professionnelles. Ces utilisateurs voudront sûrement effectuer leur propre analyse

des données pour leur domaine professionnel précis ou pour un petit groupe d'utilisateurs. Grâce à l'infrastructure informatique et de sécurité de l'entreprise, vous pouvez permettre à ces utilisateurs d'être autonomes ; il suffit pour cela que les conditions suivantes soient remplies :

- Le logiciel du client de base de données est installé (ou à la disposition des modélisateurs en vue d'une installation) sur les ordinateurs Transformer utilisés pour accéder aux sources de données IBM Cognos Analytics ou IBM Cognos Series 7 IQD.
- Les modélisateurs doivent disposer de privilèges pour créer une source de données dans IBM Cognos Administration.

  Ils n'ont pas besoin d'un accès direct à cette application. Ils peuvent créer et mettre à jour des sources de données à l'aide de Transformer ou d'outils de ligne de commande. Vous pouvez fournir aux modélisateurs un dossier sécurisé sur le portail, dans lequel ils pourront publier les packs de PowerCubes.
- Les modélisateurs doivent avoir accès à un emplacement dans lequel stocker les PowerCubes créés.

  Cet emplacement doit également être accessible pour le service IBM Cognos. Il peut s'agir d'un dossier de partage sécurisé sur un réseau local.
- Pour créer des PowerCubes sur un serveur Transformer spécifique, les modélisateurs doivent disposer de privilèges FTP pour transférer les modèles et de privilèges d'exécution pour créer les cubes sur ce serveur.

  Ils peuvent transférer les modèles et créer les cubes à l'aide de scripts. Ils peuvent également utiliser des méthodes automatisées pour créer les PowerCubes. Pour plus d'informations, voir le *Guide d'administration et de sécurité*.

### Configuration requise

Pour publier des packs de PowerCubes, vous devez configurer Transformer de façon à ce qu'il communique avec le répartiteur, soit directement, soit au moyen d'une passerelle dédiée. Si IBM Cognos Connection est sécurisé, vous devez disposer de privilèges pour créer des sources de données et publier des packs sur le portail.

Sur l'ordinateur où Transformer est installé, configurez les propriétés d'environnement suivantes :

- **URI de la passerelle**
- **URI du répartiteur pour des applications externes**

Si l'outil de modélisation utilise une passerelle dédiée au lieu de communiquer directement avec le répartiteur, vous devez également configurer la propriété **URI du répartiteur pour la passerelle** sur l'ordinateur de la passerelle dédiée.

## Options de répartition pour Cognos Mobile

IBM Cognos Mobile est un composant intégré à l'architecture IBM Cognos Analytics. Vous pouvez installer tous les composants IBM Cognos Mobile sur le même ordinateur, ou les répartir sur un réseau.

Cognos Mobile est composé des éléments suivants :

- Les composants du groupe de serveurs d'applications.
- L'app Cognos Mobile.

Vous devez installer les composants du groupe de serveurs d'application Cognos Mobile avec les composants du groupe de serveurs d'application Cognos Analytics.

Tous les composants obligatoires sont installés et activés par défaut.

## Composants Cognos Mobile installés sur un seul ordinateur

Vous pouvez installer et configurer IBM Cognos Mobile sur un seul ordinateur.

Dans le diagramme ci-dessous, tous les composants serveur sont installés sur le même ordinateur.

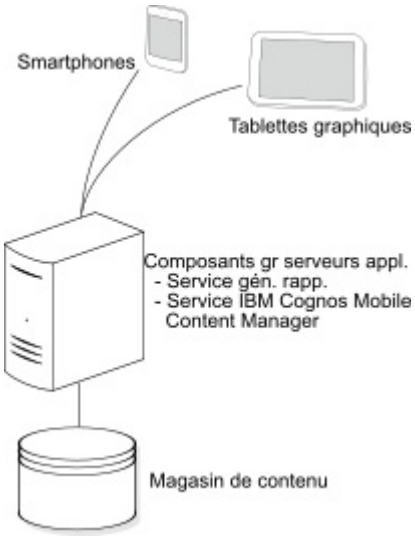



*Figure 5. Composants serveur Cognos Mobile installés sur un seul ordinateur*

## Installation de Cognos Mobile sur plusieurs ordinateurs

Vous utilisez la même méthode d'installation et de configuration pour répartir les composants d'IBM Cognos Mobile et ceux d'IBM Cognos Analytics.

Vous devez installer les composants sur chaque ordinateur, puis les configurer en indiquant l'emplacement des composants répartis d'IBM Cognos Analytics.

Dans une installation répartie, vous installez les composants du groupe de serveurs d'application Cognos Mobile sur les systèmes qui exécuteront le service Cognos Mobile.

Toutes les instances du service d'IBM Cognos Mobile doivent pouvoir accéder à la base de données dans laquelle les tables IBM Cognos Mobile sont stockées. Si une instance de serveur IBM Cognos Analytics n'est pas configurée avec les détails de base de données du magasin de contenu IBM Cognos, ou si vous voulez qu'IBM Cognos Mobile utilise une instance de base de données différente de celle du magasin de contenu IBM Cognos, ajoutez une base de données à l'aide d'IBM Cognos Configuration.

# IBM Cognos Analytics avec d'autres produits IBM Cognos

Vous pouvez installer IBM Cognos Analytics dans un environnement comprenant d'autres produits d'IBM Cognos.

L'assistant d'installation d'IBM Cognos Analytics reconnaît les répertoires compatibles et affiche un avertissement en cas de conflits. Une fois IBM Cognos Analytics installé, vous pouvez accéder aux objets créés dans un autre produit IBM Cognos dans IBM Cognos Analytics. Les conditions requises pour l'accès dépendent du mode d'exécution choisi pour les deux produits.

### Services en double en cas d'utilisation de plusieurs produits

De nombreux produits IBM Cognos utilisent des services similaires, tels que le service de génération de rapports et le service de présentation. Si vous utilisez plusieurs produits, tels qu'IBM Cognos Analytics avec IBM Cognos PowerPlay, vous devez désactiver certains services en double pour vous assurer que vos produits fonctionnent correctement.

Par exemple, vous disposez d'IBM Cognos Analytics et d'IBM Cognos PowerPlay. Les deux produits disposent d'un service de génération de rapports et d'un service de présentation. Si ces deux produits sont accessibles par la même passerelle, les rapports devant être exécutés sur les services IBM Cognos Analytics peuvent être routés vers les services IBM Cognos PowerPlay. Dans ce cas, vos rapports peuvent présenter une erreur.

## Produits IBM Cognos qui interagissent avec IBM Cognos Analytics

Certains produits IBM Cognos offrent des fonctionnalités non disponibles dans IBM Cognos Analytics. Vous pouvez utiliser ces produits dans le même environnement qu'IBM Cognos Analytics. Avec certains produits, vous pouvez accéder aux différents types de cubes ou rapports sur le portail IBM Cognos Analytics. Avec d'autres, vous pouvez uniquement accéder aux fonctionnalités du portail IBM Cognos Analytics.

### Cognos Planning - Analyst

Vous pouvez accéder aux données des plans publiés dans IBM Cognos Analytics à l'aide de l'assistant Generate Framework Manager Model, qui requiert IBM Cognos Planning - Analyst 7.3 MR1 ou version ultérieure.

Si vous souhaitez utiliser ce produit avec le serveur IBM Cognos Analytics, vous devez vous assurer que les deux produits sont issus de la même version.

Pour plus d'informations, voir le document *IBM Cognos Analyst - Guide d'utilisation.*

### Cognos Planning - Contributor

Vous pouvez accéder aux cubes Contributor (en temps réel) dans IBM Cognos Analytics en procédant à une installation personnalisée du composant IBM Cognos Analytics - Contributor Data Server qui est fourni avec IBM Cognos Planning - Contributor édition 7.3 MR1 ou ultérieure. Vous pouvez accéder aux données des plans publiés dans IBM Cognos Analytics à l'aide de l'extension d'administration Generate Framework Manager Model, qui requiert IBM Cognos Planning - Contributor 7.3 MR1 ou version ultérieure.

Si vous souhaitez utiliser ce produit avec le serveur IBM Cognos Analytics, vous devez vous assurer que les deux produits sont issus de la même version. Vous ne pouvez pas installer IBM Cognos Planning dans le même chemin qu'une instance 64 bits d'IBM Cognos Analytics.

Pour plus d'informations, voir le document *IBM Cognos Contributor Administration Guide*.

## Cognos Controller

Vous pouvez accéder à IBM Cognos Analytics pour créer des rapports standard IBM Cognos Controller au moyen d'un modèle Framework Manager prédéfini, créé lors de l'installation d'IBM Cognos Controller. Vous avez également la possibilité d'accéder à des structures et des données Controller publiées dans Framework Manager pour générer des analyses et des rapports personnalisés.

## Cognos Transformer

Vous pouvez utiliser directement dans IBM Cognos Analytics les PowerCubes IBM Cognos et les modèles Transformer créés par Transformer version 7.3 ou ultérieure. Les cubes et modèles sont compatibles avec les versions ultérieures et ne requièrent pas d'outil de migration ou de mise à niveau. Vous pouvez exécuter des rapports et des analyses dans IBM Cognos Analytics par rapport aux PowerCubes IBM Cognos.

Si vous voulez utiliser les nouvelles fonctions d'intégration de Transformer avec IBM Cognos Analytics, vous pouvez mettre à niveau les modèles IBM Cognos Series 7.x Transformer vers IBM Cognos Analytics Transformer 8.4 ou une version ultérieure. Vous pouvez ainsi utiliser les sources de données IBM Cognos Analytics (telles que les packs publiés), dresser la liste des rapports créés dans Query Studio ou Reporting, procéder à l'authentification via la sécurité IBM Cognos Analytics et publier directement les données sur le portail.

Avant de charger le modèle, vous devez avoir configuré l'espace-noms IBM Cognos Series 7 dans IBM Cognos Analytics et l'identificateur de nom utilisé pour le configurer doit correspondre au nom utilisé dans IBM Cognos Series 7.

Pour plus d'informations sur la mise à niveau de PowerCubes sécurisés IBM Cognos Series 7, voir le manuel *IBM Cognos Analytics Transformer - Guide d'utilisation*.

Pour que les PowerCubes IBM Cognos Series 7 puissent être utilisés dans IBM Cognos Analytics, optimisez-les pour cette utilisation à l'aide de l'utilitaire pcoptimizer, fourni avec IBM Cognos Analytics. Si vous n'effectuez pas cette opération, les PowerCubes créés avec les versions antérieures de Transformer risquent de mettre beaucoup de temps à s'ouvrir dans les studios Web d'IBM Cognos Analytics. Cet utilitaire d'optimisation convient aux PowerCubes plus anciens, créés avant Transformer 8.4. Il ne requiert aucun accès au modèle ni aux sources de données. Il n'est pas nécessaire d'exécuter cet utilitaire pour les cubes créés dans Transformer 8.4 ou une version ultérieure. Pour en savoir davantage sur l'optimisation des PowerCubes, reportez-vous au *Guide d'utilisation* de Transformer.

Vous pouvez publier des PowerCubes à l'aide de Transformer 8.4, de Framework Manager ou directement sur le portail IBM Cognos Analytics. Vous pouvez publier des sources de données PowerCube et des packs individuels sur le portail, de manière interactive dans Transformer ou à partir de la ligne de commande. Vous pouvez également procéder à une publication silencieuse à l'aide de scripts de traitement par lots, après avoir créé un PowerCube. Un utilisateur habilité à créer des sources de données et des packs sur le portail peut également y publier des PowerCubes. Le fichier MDC doit se trouver dans un emplacement sécurisé

auquel le répartiteur IBM Cognos Analytics et le serveur de rapports doivent pouvoir accéder. Les packs qui utilisent plusieurs PowerCubes depuis différentes définitions de cubes ou des cubes combinés avec d'autres sources de données doivent être publiés à l'aide de Framework Manager.

Si vous utilisez un PowerCube IBM Cognos Series 7 comme source de données, IBM Cognos Analytics convertit ses données en fonction du codage utilisé sur le système où le cube a été créé. Pour garantir la réussite de la conversion, les PowerCubes IBM Cognos Series 7 doivent être créés avec des paramètres régionaux définis pour s'adapter aux données du cube.

## Cognos Lifecycle Manager

Lifecycle Manager est une application Windows d'audit des mises à niveau de Cognos versions 8 et supérieures vers les nouvelles versions d'IBM Cognos Analytics. Il offre une fonction de vérification qui a pour but de valider, d'exécuter et de comparer les résultats de rapports obtenus à partir de deux éditions différentes d'IBM Cognos Analytics. Ainsi, les problèmes de mise à niveau et de compatibilité entre éditions sont plus facilement identifiés. La conception de l'interface utilisateur et la fonctionnalité de génération de rapports de statut constituent toutes deux un processus éprouvé et une bonne prise en charge pour la planification des projets de mise à niveau et la génération de rapports de statut.

Pour en savoir davantage, reportez-vous au guide d'utilisation d'*IBM Cognos Lifecycle Manager*.

## Planning Analytics

IBM Planning Analytics intègre la planification commerciale, la mesure des performances et les données opérationnelles pour permettre aux sociétés d'optimiser leur efficacité commerciale et leur interaction avec le client, quelle que soit la géographie ou la structure impliquée. Planning Analytics offre la visibilité immédiate sur les données, la responsabilité dans un processus collaboratif et une vue cohérente des informations, ce qui permet aux cadres de stabiliser rapidement les fluctuations opérationnelles et de profiter des nouvelles opportunités.

Pour plus d'informations, voir la documentation d'*IBM Planning Analytics*.

# Chapitre 3. Mise à niveau d'IBM Cognos Analytics

Les améliorations apportées aux nouvelles versions d'IBM Cognos Analytics peuvent avoir une incidence sur une grande partie de l'environnement d'information décisionnelle. Il est donc conseillé de réaliser la mise à niveau en plusieurs phases. Pour un succès garanti, considérez la mise à niveau comme un projet informatique nécessitant une planification soigneuse, un délai adéquat et des ressources.

### Site Web de Cognos Upgrade Central

Le site Web Cognos Upgrade Central (www-01.ibm.com/support/docview.wss?uid=swg22011664) fournit des informations supplémentaires destinées à vous aider à effectuer la mise à niveau. Par exemple, les questions fréquemment posées, les vidéos de démonstration et les liens vers des ressources supplémentaires sont disponibles sur ce site Web.

## Processus de mise à niveau

Chaque mise à niveau requiert un plan et chaque plan suit le même processus de mise à niveau de base.

Vous devez planifier votre mise à niveau de façon à savoir ce qui doit se passer à chaque étape du processus. Lors de l'étape de planification, vous pouvez consulter la documentation relative à la mise à niveau pour en savoir davantage sur le comportement attendu du système, les nouvelles fonctions, les fonctions obsolètes, la compatibilité entre les versions et les conditions requises pour la préparation de l'environnement de production. Une fois que vous avez passé en revue ces informations, vous pouvez procéder à une étude du site pour identifier l'infrastructure BI, les applications, les rapports et les paramètres de configuration personnalisés. Vous pouvez enfin tester la mise à niveau sur un sous-ensemble de données de façon à optimiser vos rapports et vos données avant d'entreprendre la mise à niveau complète.

Lors de la planification de votre mise à niveau, veillez à :

- Rassembler les informations nécessaires telles que les saisies nécessaires et les résultats attendus pour chaque phase.
- Evaluer les applications de votre environnement de génération de rapports et regrouper les rapports de même nature.
- Installer le nouveau logiciel dans un environnement de test et y déployer le contenu.
- Tester les applications mises à niveau pour vérifier que les rapports s'exécutent correctement.

  Vous pouvez utiliser Lifecycle Manager pour comparer les rapports émanant d'une version différente d'IBM Cognos Analytics. Pour en savoir davantage, reportez-vous à la documentation sur Lifecycle Manager.

Le déploiement et le test constituent généralement un processus itératif. Identifiez les différences potentielles entre les environnements source et cible. Effectuez le déplacement vers l'environnement de production lorsque vous considérez que les applications déployées répondent à vos besoins métier.

Le diagramme suivant présente un flux de travaux de mise à niveau général et les différentes phases du processus. Le processus inclut les phases suivantes :

- Création d'un plan de mise à niveau, qui comprend les activités suivantes :
  - Consultation des ressources, telles que la documentation, le site Web Upgrade Central (www.ibm.com/support/docview.wss?uid=swg22011664) et les étapes de mise à niveau suivantes : http://www-01.ibm.com/support/docview.wss?uid=swg21994915
  - Vérification des environnements pris en charge pour s'assurer de la compatibilité avec vos autres logiciels en accédant aux IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186). Vous pouvez également vérifier cette page si vous songez à mettre à niveau votre système d'exploitation.
  - Evaluation du système existant afin d'identifier les éléments à déplacer vers la nouvelle version du produit.
  - Création d'un plan détaillé de mise en oeuvre de la stratégie de mise à niveau.
- Création d'un système de développement ou de test avec la nouvelle version du produit.
- Utilisation des informations tirées du système de développement ou de test et application de celles-ci lors de la création des systèmes d'assurance qualité ou de production.

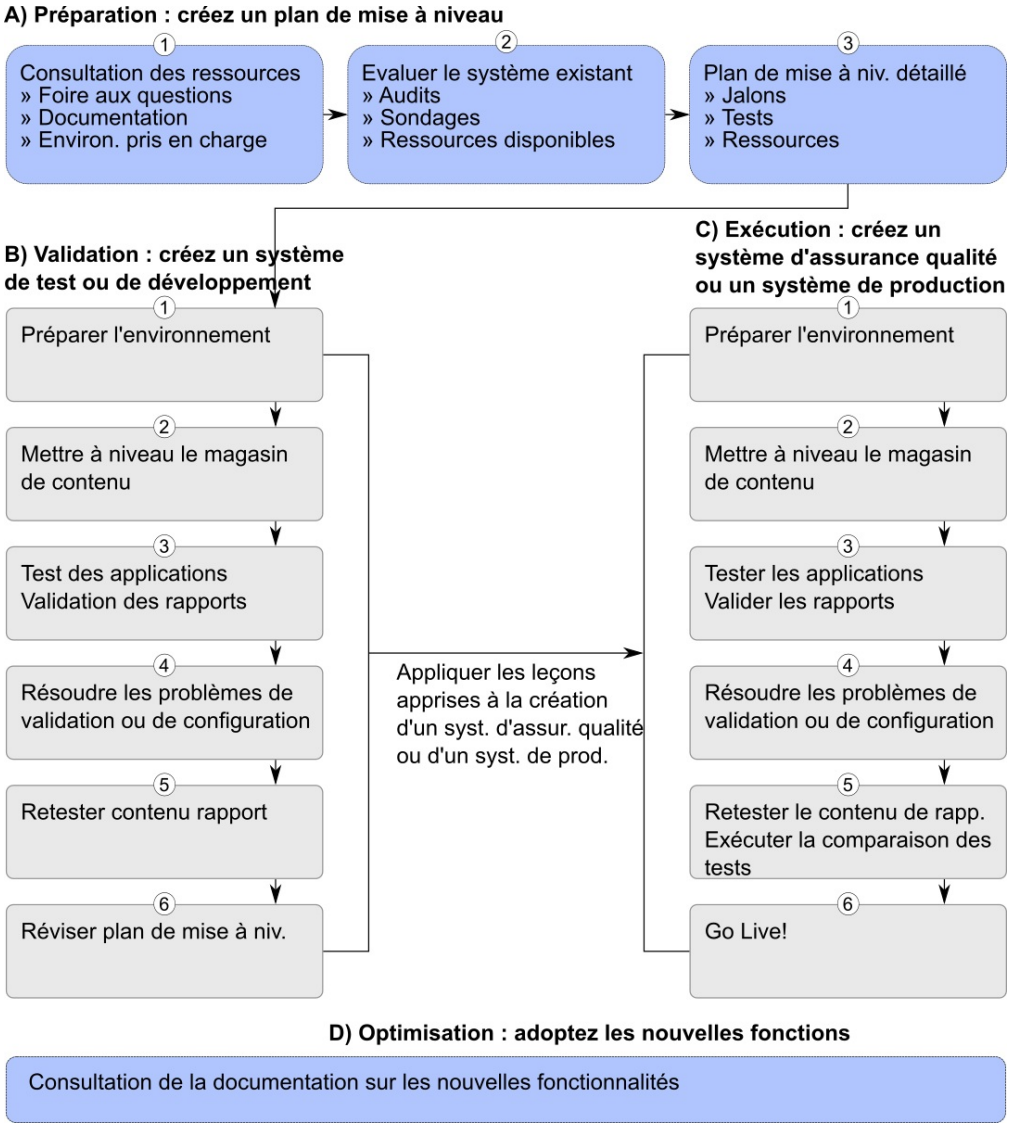



*Figure 6. Processus de mise à niveau*

## Consultation de la documentation

La documentation fournie est établie à partir de diverses sources pour vous aider à mener à bien la mise à niveau.

L'ensemble de la documentation est disponible en ligne sur l'IBM Cognos Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html).

## Evaluation des applications dans l'environnement avant la mise à niveau

La préparation de la mise à niveau est l'occasion de passer en revue vos applications existantes et d'assainir votre environnement source.

Par exemple, votre environnement compte peut-être un grand nombre d'applications. Cependant, il n'est pas inhabituel de constater qu'un certain nombre d'applications ne sont pas utilisées, ne répondent plus à vos besoins.

L'évaluation de vos applications est un exercice utile car il permet de réduire le nombre d'applications à prendre en compte au cours d'une mise à niveau.

Un audit de vos applications existantes peut inclure les tâches suivantes :

- Procédez à une étude de site pour évaluer l'environnement de production actuel et identifier les points auxquels vous devez prêter attention au cours de la mise à niveau. Cette étude fournit des informations sur l'infrastructure, les applications, les utilisateurs et les paramètres de configuration.
- Evaluez les logiciels que vous utilisez dans votre environnement et créez une liste des logiciels, comme les systèmes d'exploitation, les serveurs Web, les fournisseurs de sécurité et les bases de données.

  Pour consulter la liste actualisée des environnements pris en charge par les produits IBM Cognos Analytics, y compris des informations sur les systèmes d'exploitation, les correctifs, les navigateurs, les serveurs Web, les serveurs d'annuaire, les serveurs de base de données et les serveurs d'applications, consultez la page IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).
- Effectuez une évaluation détaillée de vos applications. L'utilisation, l'ancienneté, la taille et la complexité de vos applications sont des facteurs importants à prendre en compte lors de la planification de la mise à niveau. La taille totale des applications peut avoir une incidence sur le délai nécessaire à la réalisation de la mise à niveau.
- Répertoriez les informations suivantes concernant votre configuration :
  - Les paramètres de configuration activés dans IBM Cognos Configuration.

    L'installation de la nouvelle version du produit à un emplacement différent de celui où se trouve la version existante permet de comparer les paramètres entre les deux versions. Pour exécuter les deux versions, vous devez utiliser des numéros de port, des alias de serveur Web et des bases de données de magasin de contenu uniques.
  - Les modifications apportées aux autres fichiers de configuration.

    Vous devez modifier manuellement les autres fichiers de configuration au cours de la mise à niveau. Si vous avez modifié d'autres fichiers de configuration, vous devez évaluer les changements que vous souhaitez conserver dans l'environnement mis à niveau. Cela peut inclure les fichiers `.xml`, `.txt` et `.css` dans les répertoires `configuration`, `templates`, `webapps` et `webcontent`.

    **Remarque :** Si vous avez modifié les fichiers `.ini`, contactez le support client pour déterminer si les changements sont pris en charge dans la nouvelle version du logiciel.
- Sauvegardez votre base de données de magasin de contenu.

Un fois l'audit terminé, vous pouvez créer un plan de mise à niveau.

## Instructions de mise à niveau de votre système d'exploitation

Il est recommandé de prendre connaissance des instructions suivantes avant de migrer vers une version ultérieure du système d'exploitation sur les ordinateurs où IBM Cognos Analytics est installé :

- Consultez la page IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) pour vous assurer que votre version d'IBM Cognos Analytics prend en charge la version du système d'exploitation vers lequel vous souhaitez migrer.
- Assurez-vous que les logiciels tiers utilisés par IBM Cognos Analytics sont pris en charge sur la version de système d'exploitation proposée. Les logiciels tiers incluent des composants, tels que la base de données et les pilotes de base de données, les serveurs d'applications, les serveurs Web et les navigateurs.
- Déterminez si vous devez recompiler les application SDK d'IBM Cognos Analytics.
- Déterminez si vous devez recréer les déploiements Web, qui incluent les fichiers d'archive Web (.war) et les fichiers d'archive d'entreprise (.ear).

## Fichiers et dossiers conservés lors de la mise à niveau de Cognos Analytics

Vous pouvez installer une nouvelle version d'IBM Cognos Analytics sur votre version en cours du produit sans écraser les paramètres de configuration de la version précédente.

Les fichiers à conserver lors d'une mise à niveau sont répertoriés dans le fichier *emplacement_installation*\configuration\preserve\.ca_base_preserve.txt. Ne modifiez pas ce fichier. Modifiez plutôt le fichier *emplacement_installation*\configuration\preserve\preserve.txt si vous voulez supprimer ou conserver certains fichiers ou répertoires lors de la mise à niveau. Les instructions d'utilisation du fichier preserve.txt sont incluses dans le fichier lui-même.

**Conseil :** Les liens fixes ou lointains créés par les clients dans la structure de fichier de Cognos Analytics ne sont pas pris en charge.

Par défaut, les dossiers et fichiers suivants sont conservés lors de la mise à niveau de Cognos Analytics :

**Dossiers**

*emplacement_installation*\data

*emplacement_installation*\deployment

*emplacement_installation*\drivers

*emplacement_installation*\ldapschema

*emplacement_installation*\informix

*emplacement_installation*\configuration\certs

*emplacement_installation*\configuration\csk

*emplacement_installation*\configuration\data

*emplacement_installation*\webcontent\bi\alp\images

*emplacement_installation*\webapps\p2pd\WEB-INF\AAA\lib

**Fichiers de configuration**

*emplacement_installation*\configuration\cogconfig.prefs

*emplacement_installation*\configuration\cogconfig_reg.txt

*emplacement_installation*\configuration\coglocale.xml

*emplacement_installation*\configuration\cogstartup.xml

*emplacement_installation*\configuration\dispatcher.properties

*emplacement_installation*\configuration\install_gatewayurl.xml

*emplacement_installation*\configuration\installData.properties

*emplacement_installation*\configuration\ipfclientconfig.xml

*emplacement_installation*\configuration\configuration\caSerial

*emplacement_installation*\configuration\xqe.diagnosticlogging.xml

**Fichiers divers**

*emplacement_installation*\webapps\p2pd\WEB-INF\web.xml

*emplacement_installation*\wlp\usr\servers\cognosserver\
bootstrap.properties

*emplacement_installation*\wlp\usr\servers\cognosserver\jvm.options

*emplacement_installation*\wlp\usr\servers\cognosserver\server.xml

*emplacement_installation*\cgi-bin\web.config

*emplacement_installation*\webcontent\web.config

*emplacement_installation*\webcontent\default.htm

*emplacement_installation*\webcontent\index.html

*emplacement_installation*\webcontent\bi\web.config

**Fichiers TM1**

*emplacement_installationn*\templates\ps\portal\variables_TM1.xml

*emplacement_installation*\templates\ps\portal\variables_plan.xml

*emplacement_installation*\templates\ps\portal\
icon_active_application.gif

*emplacement_installation*\webcontent\planning.html

*emplacement_installation*\webcontent\tm1\web\tm1web.html

*emplacement_installation*\templates\ps\system.xml

*emplacement_installation*\templates\ps\portal\system.xml

**Fichiers PowerPlay**

*emplacement_installation*\webcontent\skins\series7\ppwb

*emplacement_installation*\webcontent\skins\presentation\ppwb

*emplacement_installation*\webcontent\skins\modern\ppwb

*emplacement_installation*\webcontent\skins\corporate\ppwb

*emplacement_installation*\webcontent\skins\contemporary\ppwb

*emplacement_installation*\webcontent\skins\classic\ppwb

*emplacement_installation*\webcontent\skins\business\ppwb

*emplacement_installation*\webcontent\bi\skins\series7\ppwb

*emplacement_installation*\webcontent\bi\skins\presentation\ppwb

*emplacement_installation*\webcontent\bi\skins\modern\ppwb

*emplacement_installation*\webcontent\bi\skins\corporate\ppwb

*emplacement_installation*\webcontent\bi\skins\contemporary\ppwb

*emplacement_installation*\webcontent\bi\skins\classic\ppwb

*emplacement_installation*\webcontent\bi\skins\business\ppwb

*emplacement_installation*\webcontent\bi\ppwb

*emplacement_installation*\webcontent\ps\powerplaystudio

*emplacement_installation*\webcontent\fragments\ppesAdmin

*emplacement_installation*\webcontent\ppwb

*emplacement_installation*\webapps\p2pd\WEB-INF\fragments\
applications\cogadmin\pages\ppesAdminPage.xml

*emplacement_installation*\webapps\p2pd\WEB-INF\fragments\
applications\cogadmin\fragments\ppesAdmin.xml

*emplacement_installation*\msgsdk\ppesAdminStrings_en.xml

*emplacement_installation*\msgsdk\ppesAdminStrings_ldkspec.xml

*emplacement_installation*\eclipse\plugins\
org.eclipse.equinox.cm_1.0.400.v20120522-1841.jar

*emplacement_installation*\eclipse\plugins\
org.eclipse.equinox.ds_1.4.1.v20120926-201320.jar

*emplacement_installation*\eclipse\plugins\
org.eclipse.equinox.event_1.2.200.v20120522-2049.jar

*emplacement_installation*\eclipse\plugins\
org.eclipse.equinox.util_1.0.400.v20120917-192807.jar

*emplacement_installation*\eclipse\plugins\
org.eclipse.osgi.services_3.3.100.v20120522-1822.jar

*emplacement_installation*\eclipse\plugins\
org.eclipse.osgi.util_3.2.300.v20120913-144807.jar

**Fichiers LCM**

*emplacement_installation*\wlp\usr\servers\lcm\server.xml

*emplacement_installation*\project

*emplacement_installation*\benchmarks

*emplacement_installation*\configuration

Vous devez migrer ces fichiers manuellement dans les cas suivants uniquement :

- Vous installez la nouvelle version dans un nouveau répertoire.
- Vous désinstallez la version actuelle, puis installez la nouvelle version.

  La désinstallation de la version actuelle supprime intégralement le répertoire *emplacement_installation*.

## Tâches de mise à niveau

Lorsque vous réalisez une mise à niveau, vous effectuez les opérations suivantes :

1. Installation et configuration de la nouvelle version du produit.
2. Déplacement du contenu vers la nouvelle version du produit.
3. Mise à niveau des spécifications de rapport.
4. Comparaison du contenu mis à niveau au contenu existant pour vérifier la cohérence.

## Installation et configuration d'une nouvelle version du produit

Installez la nouvelle version du produit vers un nouvel emplacement. L'emplacement peut se trouver sur le même ordinateur que la version existante du produit ou sur un autre ordinateur.

L'installation à un nouvel emplacement permet de conserver la version existante du produit et de l'exécuter en plus de la version plus récente du produit. Cela peut vous aider à tester la nouvelle version sans affecter la version existante. Vous pouvez comparer les paramètres de configuration entre les versions et comparer l'aspect et le fonctionnement des rapports dans les deux environnements afin de vérifier l'équivalence.

**Exécution de plusieurs versions ou instances d'IBM Cognos Analytics sur le même ordinateur :**

Pour installer plusieurs versions ou instances d'IBM Cognos Analytics sur le même ordinateur, vous devez modifier la configuration pour vous assurer que les versions ne partagent pas les numéros de port ou d'autres ressources.

**Modifications de configuration requises pour l'exécution de plusieurs versions sur le même ordinateur**

Pour exécuter plusieurs versions d'IBM Cognos Analytics sur le même ordinateur, vérifiez que chaque installation est distincte. Les versions ou instances doivent être installées dans des répertoires différents. Les paramètres de configuration de chaque version doivent utiliser des paramètres différents pour les propriétés de configuration ci-dessous.

**Paramètres de port et d'URI**

Si vous utilisez le serveur d'applications par défaut, vous devez utiliser des numéros de port différents de 9300 pour éviter les conflits de ports. IBM Cognos Analytics réserve une plage de numéros de port. Vous devez donc veiller à utiliser un décalage d'au moins 100 pour le numéro de port. Par exemple, si vous utilisez le numéro de port par défaut, 9300, pour une instance d'IBM Cognos Analytics, pour une deuxième installation sur le même ordinateur, remplacez le numéro de port par 9400 ou une valeur supérieure. N'utilisez pas le même numéro de port pour les deux installations.

Modifiez les ports ci-dessous.

- URI du répartiteur pour la passerelle
- URI de répartiteur externe
- URI de répartiteur interne
- URI du répartiteur des applications externes
- URI de Content Manager
- Numéro de port du serveur de journalisation local

Si vous installez le produit sur un serveur d'applications autre que celui fourni avec IBM Cognos Analytics, veillez à installer la nouvelle version sur un nouveau profil de serveur d'applications ou une instance distincte de celle la version existante.

**Magasin de contenu**

Utilisez un magasin de contenu ou un schéma différent pour chaque installation. Vous ne pouvez pas rétablir le contenu après sa mise à niveau. Vous pouvez utiliser une copie restaurée du magasin de contenu existant

comme magasin de contenu pour la version plus récente d'IBM Cognos Analytics. La version plus récente du produit met à niveau le magasin de contenu lorsque vous démarrez les services.

**Répertoires virtuels facultatifs du serveur Web**

Pour afficher le contenu statique d'IBM Cognos Analytics, les répertoires virtuels du serveur web doivent être différents pour chaque version. Veillez à mettre à jour l'URI de passerelle dans Cognos Configuration afin de refléter les noms des répertoires virtuels.

Par exemple, le répertoire virtuel par défaut est `http://nom_serveur/ibmcognos`. Si deux passerelles sont installées sur le même ordinateur, vous devez modifier le répertoire virtuel `ibmcognos` de l'une d'elles.

**Pools d'applications (Microsoft IIS Web Server)**

Si vous utilisez `cognosisap.dll`, chaque passerelle doit utiliser un pool d'applications séparé.

**Compte utilisateur qui démarre le service (facultatif)**

La modification du compte utilisateur peut être utile lors du traitement des incidents. Par exemple, vous pouvez traiter les problèmes des processus Java par propriétaire.

### Paramètres de configuration identiques pour plusieurs versions sur le même serveur

Plusieurs instances ou versions d'IBM Cognos Analytics qui s'exécutent sur le même ordinateur utilisent les mêmes ressources, comme la mémoire, le réseau et l'espace disque.

Plusieurs versions d'IBM Cognos peuvent utiliser la même source d'authentification pour les deux versions. Vous pouvez configurer des propriétés identiques pour l'espace-noms.

### Fichiers de configuration personnalisés

Si vous avez édité manuellement des fichiers de configuration, vous devez réappliquer les modifications. Conservez un enregistrement de toutes les personnalisations afin de garantir qu'elles pourront être appliquées à nouveau après la mise à niveau. Enregistrez également ces fichiers afin de pouvoir restaurer la version d'origine en cas de besoin.

Le service de présentation d'IBM Cognos Analytics prend en charge la mise à niveau automatique de certains fichiers `system.xml`. Si vous avez effectué de nombreuses modifications de personnalisation sur des fichiers `system.xml`, vous pouvez utiliser cette fonction de mise à niveau automatique au lieu d'intégrer manuellement les modifications après la mise à niveau. En remplaçant les fichiers `system.xml` par ceux de la version antérieure du produit, vous pouvez les mettre à niveau par la nouvelle version du produit. La mise à niveau automatique s'exécute lorsque vous démarrerez le service IBM Cognos.

Les fichiers `system.xml` concernés par la mise à niveau automatique se trouvent dans les répertoires suivants :

- *emplacement_installation*`/templates/ps`
- *emplacement_installation*`/templates/ps/portal`
- *emplacement_installation*`/templates/ps/qs`

**Configuration d'une seconde instance d'IBM Cognos Analytics sur un ordinateur :**

Pour disposer de plusieurs instances d'IBM Cognos Analytics sur un ordinateur, vous devez configurer chacune d'elles avec des valeurs uniques pour les ports, le répertoire virtuel du serveur web et la base de données du magasin de contenu.

**Avant de commencer**

Pour la nouvelle version du produit, un nouveau magasin de contenu est requis. Si vous effectuez une mise à niveau à partir d'une sauvegarde du magasin de contenu existant, créez un magasin de contenu à partir d'une sauvegarde du magasin de contenu existant. Si vous déplacez le contenu avec les archives de déploiement, vous pouvez créer une base de données de magasin de contenu vierge.

Veillez à ce que cette dernière soit en place avant de configurer la nouvelle version du produit.

**Important :** Si vous vous connectez à une sauvegarde du magasin de contenu, vous êtes invité à mettre à niveau vos rapports lors du premier démarrage des services IBM Cognos. La mise à niveau des rapports peut prendre du temps et il est préférable de le faire une fois la nouvelle version en cours d'exécution. Vous pouvez mettre à niveau des rapports après coup à l'aide d'IBM Cognos Administration.

**Procédure**

1. Pour la nouvelle instance d'IBM Cognos Analytics, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Vérifiez que les numéros de port des paramètres suivants n'entrent pas en conflit avec votre autre instance ou version d'IBM Cognos Analytics :
   - **URI du répartiteur pour la passerelle**
   - **URI de répartiteur externe**
   - **URI de répartiteur interne**
   - **URI du répartiteur des applications externes**
   - **URI de Content Manager**
4. Vérifiez que l'**URI de la passerelle** utilise un répertoire virtuel ou un alias différent de celui de votre autre instance ou version d'IBM Cognos Analytics.
5. Cliquez sur **Journalisation** et vérifiez que le numéro indiqué dans **Numéro de port du serveur de journalisation local** est unique.
6. Si vous utilisez Portal Services, mettez à jour l'emplacement du fichier `applications.xml` :
   - Dans la fenêtre **Explorateur**, cliquez sur **Environnement** > **Portal Services**.
   - Dans la fenêtre **Propriétés**, vérifiez que le numéro de port associé à la propriété **Emplacement du fichier applications.xml** correspond à celui des propriétés des autres URI.
7. Dans la fenêtre **Explorateur**, dans la section **Accès aux données** > **Content Manager**, vous ne devez pas utiliser le magasin de données qui est utilisé pour votre autre instance ou version d'IBM Cognos Analytics.
8. Enregistrez la configuration et démarrez IBM Cognos Analytics.

## Déplacement du contenu vers la nouvelle version du produit

Il existe deux méthodes pour déplacer le contenu. Vous pouvez déplacer la totalité du magasin de contenu, ou déplacer le contenu en créant des archives de déploiement.

### Déplacer le magasin de contenu dans son ensemble

Cette méthode exige la création d'une copie de sauvegarde du magasin de contenu existant et la restauration de celle-ci dans un nouveau magasin de contenu. Vous connectez ensuite la nouvelle version du produit dans le magasin de contenu restauré et le produit met à niveau le magasin de contenu vers la nouvelle version.

Cette méthode conserve toutes vos préférences d'utilisateur et de sécurité, mais elle requiert une nouvelle base de données de magasin de contenu.

Lors de la configuration de la sécurité assurez-vous de définir un identificateur unique sur la même valeur que celle de l'édition que vous mettez à niveau. Dans le cas contraire, les paramètres de sécurité seront perdus.

Lancez un test de cohérence sur votre magasin de contenu avant de mettre à niveau afin de vous assurer qu'il n'existe aucune incohérence. Pour plus d'informations, consultez la rubrique "Créer une tâche de maintenance du magasin de contenu" dans le document *IBM Cognos Business Intelligence - Guide d'administration et de sécurité*.

**Important :** Lorsque vous utilisez cette méthode, vous êtes invité à mettre à niveau vos rapports lors du premier démarrage des services IBM Cognos. La mise à niveau des rapports peut prendre du temps et il est préférable de le faire une fois la nouvelle version en cours d'exécution. De plus, si vous disposez d'applications SDK (Software Development Kit) qui créent, modifient ou enregistrent des spécifications de rapport, ne sélectionnez pas cette option pour mettre à niveau vos spécifications de rapport. Vous pouvez mettre à niveau des rapports après coup à l'aide d'IBM Cognos Administration.

Veillez également à désenregistrer les répartiteurs de la version précédente du produit. Pour cela, utilisez IBM Cognos Administration après avoir démarré les services.

**Avertissement :**

Les fichiers téléchargés et les modules de données en mode instantané (avant la version 11.0.4) sont enregistrés sur le système de fichiers. Ces fichiers de données **ne sont pas stockés dans le magasin de contenu**, ni dans une autre base de données. L'emplacement par défaut de ces fichiers de données est *emplacement_installation*\data\datafiles. Vous devez vous assurer que vous pouvez enregistrer ces fichiers avant de désinstaller ou de mettre à niveau l'installation existante, puis les restaurer dans le nouvel emplacement.

### Déplacer le contenu en créant les archives de déploiement

Vous pouvez déplacer le contenu en créant les archives de déploiement.

Cette méthode permet de déplacer le contenu spécifique, mais cela peut prendre du temps dans le cas d'un magasin de contenu de grande taille.

Si vous modifiez les fournisseurs de base de données de magasin de contenu, vous devez créer des déploiements pour déplacer le contenu. Par exemple, si vous modifiez le magasin de contenu à partir de Microsoft SQL Server vers IBM Db2, vous devez le faire par le biais d'archives de déploiement.

### Considérations sur les deux méthodes

Il n'est pas nécessaire de transférer les tables NC existantes lors d'une mise à niveau, car le système les resynchronise. En revanche, les tables de file d'attente doivent impérativement être vides et il est donc recommandé de ne pas utiliser les tables NC existantes lors de la réalisation d'une mise à niveau.

Les tables NC doivent être complètement vides avant la mise à niveau.Avant d'effectuer celle-ci, lancez le fichier `NC_DROP_`*`type_base_de_données`*`.sql` approprié.

Dans le cadre du processus de mise à niveau, vérifiez que vos applications fonctionnent correctement dans la nouvelle version. Parfois, les modifications apportées entraînent des résultats inattendus. Il est important de tester vos applications avec la nouvelle version du produit avant de les déplacer vers votre environnement de production.

## Mise à niveau du magasin de contenu

IBM Cognos Analytics met à niveau le contenu de la base de données du magasin de contenu vers la nouvelle version du produit lorsque vous démarrez les services pour la première fois.

Le processus de mise à niveau du magasin de contenu vers la nouvelle version du produit inclut les étapes suivantes :

1. Création d'une copie de sauvegarde de la base de données de magasin de contenu existante.
2. Création d'une base de données à partir de la sauvegarde.
3. Connexion de la nouvelle version du produit au magasin du contenu que vous avez créé à partir de la sauvegarde dans IBM Cognos Configuration.
4. Démarrage des services.

   Le magasin du contenu est mis à niveau au cours du processus de démarrage.

   **Conseil :** Lors d'un redémarrage manuel des services (si applicable), le service **`ApacheDS - cognos`** doit être démarré avant le service **`IBM Cognos`**.

Ce processus permet d'utiliser simultanément l'ancienne version et la nouvelle version du produit, où chaque version a son propre magasin de contenu.

Lorsque vous utilisez cette méthode, vous êtes invité à mettre à niveau vos rapports lors du premier démarrage des services IBM Cognos. La mise à niveau des rapports peut prendre du temps et il est préférable de le faire une fois la nouvelle version en cours d'exécution. Vous pouvez mettre à niveau des rapports à l'aide d'IBM Cognos Administration. De plus, si vous disposez d'applications SDK (Software Development Kit) qui créent, modifient ou enregistrent des spécifications de rapport, ne sélectionnez pas cette option pour mettre à niveau vos spécifications de rapport.

Lorsque vous connectez la nouvelle version du produit au magasin de contenu que vous avez créé à partir de la sauvegarde, la base de données du magasin de contenu est mise à niveau et ne peut plus être utilisée avec l'ancienne version du produit.

**Désenregistrement des répartiteurs d'un niveau de version antérieur du magasin de contenu :**

Si vous utilisez une sauvegarde du magasin de contenu existant avec une nouvelle version du produit, vous devez désenregistrer les répartiteurs appartenant au niveau de version antérieur.

**Procédure**

1. Depuis **Gérer** > **Console d'administration**, ouvrez IBM Cognos Administration.
2. Cliquez sur **Configuration**, puis sur **Répartiteurs et services**.
3. Cliquez sur **Plus** pour les répartiteurs appartenant à la version précédente.
4. Cliquez sur **Désenregistrer**, puis sur **OK**.

   Les informations sur le répartiteur sont supprimées du magasin de contenu.

## Déplacement du contenu par le biais de l'archive de déploiement

Pour déplacer un contenu spécifique depuis le magasin de contenu, vous pouvez utiliser les archives de déploiement. Ces dernières sont des fichiers compressés qu'il est possible d'importer dans la nouvelle version du produit.

**Important :** Si vous avez déplacé le contenu en restaurant le magasin de contenu existant, il n'est pas nécessaire de déplacer le contenu par le biais des archives de déploiement.

Le déplacement du contenu avec les archives de déploiement se déroule comme suit :

1. Création de l'archive.
2. Copie de l'archive vers la nouvelle version du produit.
3. Importation du contenu.

**Création d'une archive de déploiement :**

Procédez comme suit pour créer une archive de déploiement.

**Procédure**

1. Dans **IBM Cognos Administration**, dans l'onglet **Configuration**, cliquez sur **Administration du contenu**.
2. Dans la barre d'outils, cliquez sur l'icône **Nouvelle exportation**  .
3. Renseignez la zone **Nom** de l'archive.
4. Sélectionnez le contenu à inclure dans l'archive :
   - Pour exporter des dossiers et un contenu d'annuaire spécifiques, cliquez sur l'option **Sélectionner des dossiers publics et le contenu de l'annuaire**.
   - Pour exporter l'intégralité du magasin de contenu, cliquez sur l'option **Sélectionner Content Store dans son ensemble**. Si vous sélectionnez l'ensemble du magasin de contenu, vous pouvez également sélectionner **Inclure les informations de compte utilisateur**.
5. Cliquez sur **Suivant**.
6. Si vous avez cliqué sur **Sélectionner Content Store dans son ensemble**, saisissez un mot de passe à utiliser lors de l'importation du contenu et cliquez ensuite sur **OK**.
7. Si vous avez cliqué sur **Sélectionner des dossiers publics et le contenu de l'annuaire**:

a. Sur le panneau **Sélection du contenu des dossiers publics**, cliquez sur **Ajouter**.
b. Sur le panneau **Sélection des entrées**, dans la zone **Entrées disponibles**, sélectionnez les packs et les dossiers que vous souhaitez importer.

   Vous pouvez accéder à la hiérarchie des Dossiers publics et choisir des packs et dossiers. Cliquez sur l'icône **Ajouter**  pour transférer les éléments sélectionnés vers la zone **Entrées sélectionnées** et cliquez sur **OK**.
c. Pour chaque pack et dossier que vous exportez, exécutez les opérations suivantes et cliquez ensuite sur **Suivant** :
   - Si vous voulez apporter des changements au pack ou au dossier dans l'environnement cible, cliquez sur l'icône **Editer**  , effectuez vos modifications, puis cliquez sur **OK**.
   - Pour restreindre l'accès au pack ou au dossier et à leurs entrées, cochez la case dans la colonne **Désactiver après l'importation**. Cela permet de tester les rapports avant de les rendre disponibles dans l'environnement cible.
   - Sous **Options**, indiquez si vous souhaitez inclure les versions de sortie du rapport, l'historique d'exécution et les plannings, ainsi que ce qu'il convient de faire des entrées en cas de conflit.
d. Sur le panneau **Sélection du contenu de l'annuaire**, sélectionnez les options de votre choix et cliquez sur **Suivant**.
e. Sur le panneau **Définition des options générales**, sélectionnez les options de votre choix et cliquez sur **Suivant**.
f. Sur le panneau **Sélection d'une archive de déploiement**, sélectionnez une archive de développement existante dans la liste ou créez-en une.

   Si vous saisissez un nouveau nom d'archive de déploiement, n'utilisez pas d'espaces dans ce nom. Si le nom de la nouvelle archive de déploiement correspond au nom d'une archive de déploiement existante, cette dernière est remplacée.

8. Examinez les informations récapitulatives et cliquez sur **Suivant**.
9. Sous **Actions**, sélectionnez **Enregistrer et exécuter une fois**.
10. Sur le panneau **Options d'exécution**, sélectionnez **Maintenant** et cliquez sur **Exécuter**.

**Résultats**

Une archive de déploiement est créée dans le répertoire de `déploiement` dans lequel vous avez installé IBM Cognos Analytics.

**Copie de l'archive de déploiement vers la nouvelle version :**

Vous devez copier manuellement les archives de déploiement depuis l'instance où elles ont été créées vers la nouvelle instance.

**Procédure**

Copiez les archives de déploiement que vous avez créées à partir du répertoire *emplacement_installation_ancienne_version*`/deployment` vers le répertoire *emplacement_installation_nouvelle_version*`/deployment`.

**Remarque :** Le répertoire `deployment` est configurable dans IBM Cognos Configuration. L'emplacement par défaut est *`emplacement_installation`*`/deployment`. Si vous utilisez un emplacement différent, veillez à copier les archives de développement dans le répertoire approprié.

**Inclusion des objets de configuration lors de l'importation d'une archive de déploiement de l'ensemble du magasin de contenu :**

Vous pouvez inclure des objets de configuration lors de l'importation de l'intégralité du magasin de contenu. Par exemple, vous pouvez importer la configuration si vous disposez d'un ensemble de paramètres avancés pour vos services que vous souhaitez importer de l'environnement source.

Par défaut, les objets de configuration sont exclus lorsque vous importez l'intégralité du magasin de contenu, même s'ils sont inclus dans l'exportation. Ces objets comprennent des répartiteurs et les dossiers de configuration utilisés pour regrouper ces répartiteurs.

**Procédure**

1. Dans **IBM Cognos Administration**, dans l'onglet **Configuration**, cliquez sur **Répartiteurs et services**.
2. Cliquez sur le répartiteur souhaité.
3. En regard de **ContentManagerService**, cliquez sur l'icône Définir les propriétés.
4. Cliquez sur l'onglet **Paramètres**.
5. Dans la colonne **Valeur**, cliquez sur l'option **Editer**.
6. Cochez la case **Remplacer les paramètres hérités de l'entrée parent**.
7. Dans la colonne **Paramètre**, saisissez le texte suivant en majuscules :
   `CM.DEPLOYMENTINCLUDECONFIGURATION`
8. Dans la colonne **Valeur**, saisissez `true`.
9. Cliquez sur le bouton **OK** pour terminer la procédure.

**Importation d'une archive de déploiement :**

Pour importer les entrées, vous devez créer une spécification de déploiement d'importation.

Lorsque vous importez, vous devez opérer une sélection dans les entrées exportées. Vous pouvez accepter les options par défaut définies durant l'exportation ou bien les modifier. Vous pouvez sélectionner les options qui sont incluses dans l'archive de déploiement durant l'exportation.

Si vous procédez au déploiement partiel d'un contenu d'annuaire et de dossiers publics spécifiques, l'Assistant d'importation indique si les packs et les dossiers existent dans l'environnement cible, ainsi que la date et l'heure de leur dernière modification. Vous pouvez utiliser ces informations pour décider de la manière de résoudre des conflits. Lorsque vous redéployez, l'Assistant indique également si les packs et les dossiers figuraient dans le déploiement original.

**Avant de commencer**

Vérifiez que vous avez copié l'archive de déploiement dans le répertoire *`emplacement_installation`*`/deployment` de la nouvelle version du produit.

**Procédure**

1. Pour la nouvelle version du produit, dans **IBM Cognos Administration**, dans l'onglet **Configuration**, cliquez sur **Administration du contenu**.
2. Dans la barre d'outils, cliquez sur l'icône Nouvelle importation. 
3. Dans la zone **Archive de déploiement**, sélectionnez l'archive de déploiement à importer et cliquez sur **Suivant**.
4. Si l'archive de déploiement concerne l'ensemble du magasin de contenu, saisissez le mot de passe que vous avez entré lors de l'exportation et cliquez sur **OK**.
5. Saisissez un nom pour l'importation et sélectionnez le dossier dans lequel vous souhaitez l'enregistrer et cliquez ensuite sur **Suivant**.
6. Sélectionnez le contenu à inclure dans l'importation, sélectionnez les options et cliquez sur **Suivant**.

   **Conseil :** Cliquez sur l'icône d'édition  en regard du pack si vous souhaitez modifier l'emplacement cible pour le contenu importé.
7. Sur le panneau **Définition des options générales**, sélectionnez les options de votre choix et cliquez sur **Suivant**.
8. Examinez les informations récapitulatives et cliquez sur **Suivant**.
9. Sous **Actions**, sélectionnez **Enregistrer et exécuter une fois**, puis cliquez sur **Terminer**.
10. Sur le panneau **Options d'exécution**, effectuez les opérations suivantes :
    a. Sélectionnez **Mettre à niveau toutes les spécifications de rapports à la version la plus récente** si vous souhaitez mettre à niveau les spécifications de rapport au cours de l'importation. Vous pouvez également exécuter cette tâche après avoir importé le contenu.
    b. Cliquez sur **Exécuter**.

## Utilisation de Lifecycle Manager pour comparer les rapports entre les versions du produit

Lifecycle Manager permet de vérifier le contenu mis à niveau en comparant des rapports dans l'ancien environnement aux rapports dans la nouvelle version du produit.

Pour plus d'informations, voir la documentation d'IBM Cognos Lifecycle Manager.

**Mise à niveau des spécifications de rapport :**

Les spécifications de rapport sont passé d'une version d'IBM Cognos Analytics à une autre. Vous devez mettre à niveau les spécifications de rapport créées dans les versions précédentes du produit.

Si vous effectuez une mise à niveau à partir d'une sauvegarde du magasin de contenu existant, vous devez mettre à niveau les spécifications de rapport après avoir démarré les services.

Si vous déplacez le contenu vers une nouvelle version par le biais des archives de déploiement, vous pouvez choisir de mettre à niveau les spécifications d'importation au cours de l'importation.

Si vous avez déplacé le contenu à l'aide d'une archive de déploiement, vous avez peut-être sélectionné l'option de mise à niveau des spécifications de rapport. Si vous avez mis à niveau les spécifications de rapport au cours de l'importation, il n'est pas nécessaire de répéter l'opération.

**Avant de commencer**

**Important :** Ne mettez pas à niveau vos spécifications de rapports si vous disposez d'applications SDK (Software Development Kit) permettant de créer, de modifier ou d'enregistrer des spécifications de rapports. Vous devez d'abord mettre à jour vos applications SDK (Software Development Kit) pour qu'elles soient conformes au schéma de spécification de rapports d'IBM Cognos BI. Sinon, il se peut que vos applications SDK (Software Development Kit) ne puissent pas accéder aux spécifications de rapport mises à niveau. Pour plus d'informations sur la mise à niveau des spécifications de rapports, reportez-vous au manuel *IBM Cognos Software Development Kit Developer Guide*.

**Procédure**

1. Ouvrez **IBM Cognos Administration**.
2. Dans l'onglet **Configuration**, cliquez sur **Administration du contenu**.
3. Cliquez sur la flèche du bouton Nouvelle maintenance du contenu  dans la barre d'outils, puis sur **Nouvelle mise à niveau d'un rapport**.
4. Saisissez un nom pour la tâche de mise à niveau et éventuellement une description et une infobulle. Cliquez sur **Suivant**.
5. Sélectionnez les packs et les emplacements correspondant à la spécification de rapport à mettre à niveau. Cliquez sur **Suivant**.

   Si vous mettez à niveau les spécifications de rapport par pack, tous les rapports du magasin de contenu basés sur le modèle du pack seront mis à niveau. Si vous mettez à niveau les spécifications de rapport par dossier, tous les rapports du dossier seront mis à niveau.
6. Choisissez l'une des options suivantes :
   - L'option **Enregistrer et exécuter une fois** ouvre la page Options d'exécution.
   - L'option **Enregistrer et planifier** ouvre l'outil de planification.
   - L'option **Enregistrer seulement** vous permet de sauvegarder la mise à niveau pour l'exécuter ultérieurement.

## Configuration d'IIS et de Cognos Analytics lors de la mise à niveau de la version 11.0.3 vers la version 11.0.4 ou ultérieure

11.0.4

### Avant de commencer

Cette rubrique suppose que votre environnement version 11.0.3 fonctionne, qu'IIS est configuré et que le code d'accès unique fonctionne.

### Pourquoi et quand exécuter cette tâche

Cette rubrique utilise les hypothèses suivantes :

- Nom du serveur IIS : **`hôte-iis`**
- Numéro de port IIS : **`80`**
- Nom du répertoire virtuel IIS : **`ibmcognos`**
- Nom du serveur Cognos Analytics : **`hôte-ca`**

- Numéro de port de Cognos Analytics : **9300**

## Procédure

1. Effectuez une sauvegarde de votre magasin de contenu 11.0.3.
2. Installez la version 11.0.4 par dessus votre installation version 11.0.3. Si nécessaire, faites-le sur vos machines de niveau données, application et passerelle.
3. Avant de démarrer les services Cognos Analytics, apportez les modifications suivantes à l'environnement.
   a. Supprimez cette entrée du fichier *emplacement_installation*\wlp\usr\servers\cognosserver\server.xml (au niveau données et application) : `<jndiEntry jndiName="glass/sso/login" value="/ibmcognos/cgi-bin/cognosisapi.dll"/>`
   b. Examinez les fichiers `default.htm` et `index.html` dans le dossier *emplacement_installation_passerelle*/webcontent. A la ligne `<meta http-equiv="refresh" content="0; URL=bi/">`, vérifiez que la barre oblique (/) figure dans l'attribut `URL=bi/`.
   c. Lancez Cognos Configuration sur la couche passerelle. Modifiez **Environnement** > **Paramètres de passerelle** > **URI du répartiteur pour la passerelle** pour utiliser le format suivant : `http://<hôte_niveauapp>:<port_niveauapp>/bi/v1/disp`
   d. Lancez Cognos Configuration sur les niveaux données et application. Modifiez ce qui suit dans **Environnement** > **Paramètres de passerelle**, selon les cas :
      - **URI de la passerelle**: `http(s)://iis-host:80/ibmcognos/bi/v1/disp`

        Il s'agit de l'URL des contenus déconnectés, tels que les liens dans des PDF, dans Excel et dans les rapports actifs. Elle est également utilisée dans les liens envoyés par courrier électronique.
      - **URI du répartiteur pour la passerelle** : `http(s)://ca-host:9300/bi/v1/disp`

        Il s'agit de la liste des URI auxquels le code Cognos ISAPI se connecte lorsqu'il transmet des demandes. Plusieurs entrées sont utilisées pour la reprise en ligne. Incluez tous les serveurs d'applications Cognos Analytics appropriés.
      - **URI du répartiteur pour des applications externes** : `http(s)://ca-host:9300/bi/v1/disp`

        Les applications externes telles que Framework Manager se connecte sur cette URL pour effectuer des opérations SDK.
   e. Suivez les procédures décrites dans «Configuration d'IIS dans Cognos Analytics 11.0.3», à la page 123 pour reconfigurer IIS.
4. Démarrez les services dans l'ordre suivant : 1) Couche de données, 2) Groupe de serveurs d'applications, 3) Couche passerelle et IIS.

# Chapitre 4. Installation et configuration des composants du serveur

Vous pouvez installer tous les composants d'IBM Cognos Analytics sur le même ordinateur, sur plusieurs serveurs pour une installation distribuée, ou vous pouvez étendre une installation mono-ordinateur existante sur un autre serveur pour améliorer les performances.

Les options ci-après sont disponibles lors de l'installation d'IBM Cognos Analytics à partir de l'assistant d'installation.

- Choisissez l'option **Installation facile** pour obtenir sans délai une installation IBM Cognos Analytics opérationnelle, sans avoir à réaliser d'autres opérations de configuration ni à installer des logiciels complémentaires.

  **Important :** L'**Installation facile** n'est disponible que pour les systèmes d'exploitation Windows. Si vous mettez à niveau une **Installation facile** (installation par dessus une installation existante), arrêtez manuellement tous les services au préalable et notamment les services Informix et ApacheDS.

  Cette option d'installation comprend les éléments suivants, déjà entièrement configurés :

  – Une version complète d'IBM Cognos Analytics avec toutes ses nouvelles fonctions.
  – Informix 12.10 installé et configuré en tant que base de données du magasin de contenu.
  – Apache Directory Server pour créer et gérer les utilisateurs.
- Choisissez l'option **Personnalisé** si vous souhaitez de la souplesse pour sélectionner les composants IBM Cognos Analytics à installer. Souhaitez-vous personnaliser IBM Cognos Analytics, ou réaliser une intégration avec un logiciel tiers ? C'est l'option à sélectionner.

Si vous envisagez d'installer plusieurs composants sur un même ordinateur, installez-les au même endroit afin d'éviter tout conflit entre ports ou autres paramètres par défaut.

Lorsque vous effectuez une installation personnalisée, les composants serveur sont rassemblés dans les groupes suivants :

- Référentiel de contenu (Content Manager)
- Services d'application
- Couche passerelle facultative

Vous pouvez installer chaque composant sur un ordinateur distinct ou bien sur le même ordinateur. La passerelle doit être installée sur un ordinateur exécutant également un serveur Web.

## Séquence de l'arrêt de services

La séquence d'arrêt des services est importante dans un environnement réparti. Commencez par arrêter le service IBM Cognos des composants du groupe de serveurs d'applications, puis le Content Manager en veille et enfin le Content Manager actif.

Vous devez également arrêter :

- Les Applications liées au service IBM Cognos, telles que Framework Manager, Cognos Transformer ou IBM Cognos Administration.
- Toutes les applications SDK (Software Development Kit) en cours d'exécution.

## Mise à niveau de l'installation

Si vous effectuez une mise à niveau à partir d'une édition précédente des produits IBM Cognos, voir Chapitre 3, «Mise à niveau d'IBM Cognos Analytics», à la page 39.

Si vous procédez à une mise à niveau depuis une version antérieure d'IBM Cognos Analytics, tous les composants répartis doivent correspondre à la version d'IBM Cognos Analytics. Si vous installez IBM Cognos Analytics sur des hôtes supplémentaires ou alternatifs, vous devez mettre à jour les propriétés spécifiques de chaque emplacement dans IBM Cognos Configuration.

## Installations 64 bits

La passerelle d'IBM Cognos Analytics fournit des bibliothèques 32 bits, que vous effectuiez l'installation sur un serveur 32 ou 64 bits. Certains serveurs Web tels qu'Apache Web Server ne permettent pas de charger une bibliothèque compilée en 32 bits sur un serveur compilé en 64 bits. Dans ce cas, installez la version 32 bits de la passerelle IBM Cognos sur un serveur IBM Cognos 32 bits.

Le composant serveur de rapports, inclus dans les composants du groupe de serveurs d'applications, est fourni dans les versions 32 et 64 bits. La sélection de la version à utiliser est effectuée à l'aide d'IBM Cognos Configuration après l'installation. Par défaut, le composant serveur de rapports est défini pour utiliser le mode 32 bits, même sur un ordinateur 64 bits. Le mode 32 bits permet d'exécuter tous les rapports alors que le mode 64 bits permet d'exécuter uniquement les rapports créés pour le mode de requête dynamique.

Si vous mettez à niveau IBM Cognos Analytics dans un environnement qui comprend des versions antérieures d'autres produits IBM Cognos Analytics, tels qu'IBM Cognos Business Intelligence Controller version 8.x, IBM Cognos Analytics Planning version 8.x ou IBM Cognos Business Intelligence Analysis *for Microsoft Excel* version 8.x, installez la nouvelle version d'IBM Cognos Analytics dans un emplacement distinct de celui de l'autre produit IBM Cognos Analytics et configurez la nouvelle version d'IBM Cognos Analytics de manière qu'elle fonctionne indépendamment de ce produit. Lorsque l'autre produit aura été mis à niveau vers une version compatible avec IBM Cognos Analytics, vous pourrez configurer les deux produits pour qu'ils fonctionnent ensemble.

## Installations Windows

Sous Microsoft Windows, assurez-vous que vous disposez des privilèges d'administration sur l'ordinateur Windows où vous souhaitez effectuer l'installation. Assurez-vous également que l'ordinateur dispose d'une variable système TEMP pointant vers le répertoire où vous voulez stocker les fichiers temporaires. Durant l'installation, les fichiers du disque sont copiés temporairement dans ce répertoire.

### Installations UNIX

Pour les installations sous UNIX, vous pouvez installer les composants serveur à l'aide d'une interface graphique utilisateur ou en exécutant une installation silencieuse. Pour une installation en mode graphique, la console connectée à votre ordinateur UNIX doit prendre en charge l'interface graphique utilisateur de type Java.

En outre, IBM Cognos Analytics utilise les droits 755. Cela n'a une incidence que sur les répertoires d'installation, et non sur les droits d'accès aux fichiers à l'intérieur de ces répertoires.

### Conditions requises pour l'impression

Pour vous assurer que les rapports s'impriment correctement sous Windows, Adobe Reader requiert la configuration d'au moins une imprimante sur le système d'exploitation sous lequel les composants du groupe des serveurs d'applications sont installés. Tous les rapports, quel que soit le format d'impression choisi, sont envoyés en tant que fichiers PDF temporaires vers Adobe Reader pour impression.

### Désinstallation

Pour les instructions de désinstallation, voir Chapitre 12, «Désinstallation d'IBM Cognos Analytics», à la page 307.

## Séquence d'installation des composants serveur

Dans une installation répartie, l'ordre dans lequel vous configurez les composants est important. Configurez, puis démarrez les services dans au moins un emplacement où Content Manager est installé avant de configurer d'autres composants serveur.

Vous devez configurer le composant passerelle en dernier pour que les clés cryptographiques soient partagées et que la communication sécurisée s'effectue entre les trois composants. Le serveur indiqué pour la propriété URI externe du répartiteur sur l'ordinateur passerelle doit correspondre au dernier composant serveur que vous démarrez.

Le diagramme ci-dessous indique l'ordre d'installation des composants répartis. Après avoir planifié et préparé votre environnement, installez et configurez les composants Content Manager, puis les composants du groupe de serveurs d'applications et les passerelles. Une fois les composants serveur installés, vous pouvez installer et configurer Framework Manager.

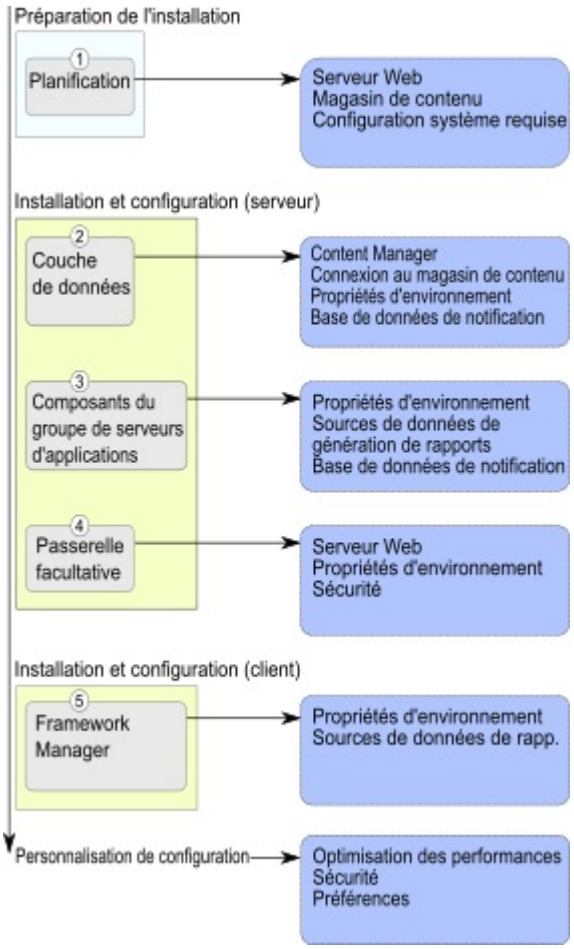



*Figure 7. Flux de travaux du processus d'installation répartie*

## Recommandation - Mise en place et configuration de l'installation de base dans le cadre d'installations réparties

Lorsque vous mettez en place une installation répartie, vous disposez de nombreuses options d'installation et de configuration pour personnaliser IBM Cognos Analytics afin qu'il s'intègre à votre infrastructure d'entreprise.

Effectuez d'abord une installation de base, qui implique la mise en place d'une ou de plusieurs instances de chaque composant serveur requis : couche données (Content Manager), composants du groupe de serveurs d'applications et couche passerelle. Effectuez uniquement les tâches de configuration requises, telles que la configuration des composants répartis en vue de permettre à ces derniers de communiquer, pour mettre en service votre environnement réparti avant de personnaliser vos paramètres.

Vous pourrez ultérieurement ajouter des composants facultatifs et personnaliser vos paramètres de configuration pour qu'ils répondent davantage à vos besoins en matière d'informations décisionnelles.

L'ordre de configuration des ordinateurs est important. Vous devez configurer, puis démarrer les services sur au moins un ordinateur où Content Manager est installé

avant de configurer les autres composants serveur ou Framework Manager. Pour en savoir davantage, reportez-vous à la section «Séquence d'installation des composants serveur», à la page 59.

La méthode la plus simple et la plus rapide pour mettre IBM Cognos Analytics en service dans votre environnement consiste à s'assurer qu'une installation de base est opérationnelle dans ce dernier.

## Modes d'installation

Pour réaliser une installation intégrale, vous devez installer les composants sur votre serveur, puis les configurer afin qu'ils fonctionnent dans votre environnement.

### Mode interactif

En règle générale, les programmes d'installation et de configuration d'IBM Cognos sont exécutés en mode interactif. Cela signifie que l'assistant d'installation vous invite à fournir des informations, et que l'outil de configuration vous permet de modifier les paramètres par défaut. L'assistant d'installation est `ca_srv_<plateforme>_<génération>.exe` (Windows) ou `ca_srv_<plateforme>_<génération>.bin` (UNIX, Linux).

### Mode silencieux

Vous pouvez automatiser l'installation des composants à l'aide de fichiers de réponses et en exécutant le programme d'installation en mode silencieux.

Vous pouvez automatiser la configuration de composants en exportant les paramètres de configuration d'un ordinateur vers un autre pourvu que les composants installés soient identiques. Exécutez IBM Cognos Configuration en mode interactif lors de la première utilisation.

L'autre option consiste à éditer le fichier cogstartup.xml, en utilisant des paramètres qui s'appliquent à votre environnement, puis à exécuter l'outil de configuration en mode silencieux.

### Mode interactif sur les systèmes UNIX

Sauf si vous avez l'intention d'effectuer une installation en mode silencieux, installez le logiciel depuis un poste de travail XWindow System, un terminal X ou un PC ou un autre système sur lequel le logiciel serveur X est installé.

Pour une installation en mode interactif, la console connectée à votre ordinateur doit prendre en charge les interfaces graphiques utilisateur Java.

## Installation des composants serveur sous UNIX ou Linux

Utilisez l'Assistant d'installation pour sélectionner les composants serveur que vous souhaitez installer, ainsi que l'emplacement approprié sur votre ordinateur.

### Avant de commencer

Accédez à la page IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) pour vérifier que les correctifs requis sont installés sur votre ordinateur.

## Procédure

1. Définissez la variable d'environnement JAVA_HOME de sorte qu'elle pointe vers l'emplacement d'installation de votre JRE (Java Runtime Environment), comme */répertoire*/java/*version_java*/jre.

   Pour fonctionner sur un système d'exploitation Linux, IBM Cognos Analytics requiert une machine JVM, comme celle qui est fournie IBM.
2. Sous HP-UX, définissez la variable d'environnement _M_ARENA_OPTS comme suit : _M_ARENA_OPTS 1:4.

   Cette opération augmente l'allocation de mémoire pour HP-UX afin qu'elle corresponde mieux à celle des autres plateformes UNIX.
3. Accédez à l'emplacement dans lequel les fichiers d'installation ont été téléchargés et décompressés.

   **Conseil :** Utilisez de nouvelles versions du logiciel de compression de fichier pour extraire les fichiers. Les versions antérieures de ces logiciels peuvent ne pas parvenir à extraire les fichiers.
4. Pour démarrer l'assistant d'installation, accédez au répertoire du système d'exploitation, puis entrez la commande suivante :

   ./ca_srv_<*plateforme*>_<*génération*>.bin

   Où <*génération*> désigne le numéro de génération, et<*plateforme*> vaut win (Windows), i386 (Linux i386), ppcle (Linux pl E), ppc (Linux Power PC), s390x (Linux z), sol (Solaris), aix (AIX), ou zos (z/OS).

   **Conseil :** Lorsque vous utilisez la commande ./ca_srv_<*plateforme*>_<*génération*>.bin avec XWindows, les caractères japonais figurant dans les messages et les fichiers journaux peuvent être altérés. Lors d'une installation en japonais sous UNIX ou Linux, commencez par définir les variables d'environnement LANG=C et LC_ALL=C (où C est le code de langue, par exemple ja_JP.PCK sous Solaris), puis démarrez l'assistant d'installation.

   Si vous n'utilisez pas XWindows, exécutez une installation automatique. Pour en savoir davantage, voir Chapitre 11, «Installation sans surveillance, désinstallation et configuration», à la page 299.
5. Suivez les instructions fournies par l'assistant d'installation pour copier les fichiers sur votre ordinateur.

   Procédez à l'installation dans un répertoire dont le nom de chemin ne contient que des caractères ASCII. Certains serveurs Web UNIX et Linux ne prennent pas en charge les caractères non ASCII dans les noms de répertoires.

   **Conseil :** Les exemples ne sont pas disponibles avec le kit d'installation Cognos Analytics AIX, version 11.0.7 et ultérieures. Pour plus d'informations, voir cet article.
6. Sur la page **Terminer** de l'assistant d'installation, vous pouvez cliquer sur **Afficher** pour accéder aux fichiers journaux. Ne configurez pas IBM Cognos Analytics immédiatement, car il convient d'abord d'effectuer d'autres tâches pour s'assurer que l'environnement est correctement installé.
7. Ajoutez le répertoire *emplacement_installation*/bin à la variable d'environnement de chemin de bibliothèque appropriée.
   - Pour Solaris ou Linux, LD_LIBRARY_PATH
   - Pour AIX, LIBPATH
   - Pour HP-UX, SHLIB_PATH

### Que faire ensuite

Vous pouvez configurer IBM Cognos Analytics à l'aide de l'outil IBM Cognos Configuration. Saisissez `cogconfig.sh` dans le répertoire *`emplacement_installation`*`/bin` pour démarrer Cognos Configuration.

## Installation des composants serveur sous Windows

Utilisez l'Assistant d'installation pour sélectionner les composants serveur que vous souhaitez installer, ainsi que l'emplacement approprié sur votre ordinateur.

Pour les ordinateurs Windows, l'emplacement d'installation par défaut utilise le répertoire **Program Files**. Si vous effectuez l'installation à cet emplacement, veillez à exécuter IBM Cognos Configuration comme administrateur. Vous pouvez également installer le produit dans un répertoire différent de **Program Files**, comme `C:\IBM\cognos\analytics`.

L'installation requiert au moins 5 Go dans le répertoire temp. Vous définissez ce répertoire temp à l'aide de la variable d'environnement TMP.

### Procédure

1. Accédez au répertoire dans lequel les fichiers d'installation ont été téléchargés et décompressés, puis cliquez deux fois sur `ca_srv_<plateforme>_<génération>.exe`.

   **Conseil :** Utilisez de nouvelles versions du logiciel de compression de fichier pour extraire les fichiers. Les versions antérieures de ces logiciels peuvent ne pas parvenir à extraire les fichiers.
2. Sélectionnez la langue d'installation.

   La langue sélectionnée détermine la langue de l'interface utilisateur. Toutes les langues prises en charge sont installées. Vous pouvez redéfinir l'interface utilisateur sur l'une des langues installées après l'installation.
3. Suivez les instructions fournies par l'assistant d'installation pour copier les fichiers sur votre ordinateur.

   Vous pouvez utiliser l'une des options d'installation suivantes :

   - Utilisez l'option **Installation facile** pour installer les composants sur le même ordinateur, installer une instance de la base de données Informix pour le magasin de contenu, et configurer le système.

     **Important :** Si vous mettez à niveau (c'est-à-dire que vous remplacez une installation existante) une **Installation facile**, arrêtez manuellement tous les services au préalable, y compris les services Informix et ApacheDS.
   - Utilisez l'option **Personnalisée** pour une répartition de l'installation sur plusieurs serveurs.

   Installez les composants IBM Cognos Analytics dans un répertoire dont le nom du chemin d'accès contient uniquement des caractères ASCII. Certains serveurs Web Windows ne prennent pas en charge les noms de répertoire comportant des caractères autres que des caractères ASCII.
4. S'il s'agit de la première installation, sélectionnez l'option **Première installation**. Pour étendre la capacité d'une installation en cours d'exécution, sélectionnez l'option **Connexion et installation**. Vous êtes invité à indiquer les composants à installer, ainsi que l'URL et les données d'identification du système en cours d'exécution. L'espace-noms et les données d'identification doivent être ceux d'un administrateur système.

- Vous pouvez rechercher la valeur de l'URL de l'installation en cours dans IBM Cognos Configuration, dans la catégorie **Environnement** > **Paramètres du répartiteur**. La valeur d'URL dont vous avez besoin est **URI externe du répartiteur**.
- Vous pouvez rechercher l'espace-noms de l'installation en cours dans IBM Cognos Configuration, dans la catégorie **Sécurité** > **Authentification**.

# Installation et configuration de Content Manager pour le référentiel de contenu

Vous pouvez installer plusieurs instances de Content Manager pour assurer la reprise et placer ce dernier dans un emplacement séparé de celui des autres composants afin d'améliorer les performances.

Les ordinateurs Content Manager doivent connaître l'emplacement du magasin de contenu et des autres composants Content Manager, ainsi que la base de données utilisée pour la notification.

Dans une installation répartie, au moins un des ordinateurs sur lequel vous installez Content Manager doit être configuré, actif et accessible avant que vous ne configuriez d'autres ordinateurs dans votre environnement IBM Cognos. Cela garantit que le service de l'autorité de certification installé avec Content Manager est disponible pour émettre des certificats pour d'autres ordinateurs.

Il est possible que votre installation comprenne plusieurs applications Content Manager, chacune sur un ordinateur différent. Un ordinateur Content Manager peut être activé et un ou plusieurs autres en veille.

## Droits

Vous pouvez effectuer l'installation avec des droits racine ou non racine.

En outre, IBM Cognos Analytics respecte le masque de création de mode fichier (umask) du compte exécutant le programme d'installation. Cela n'a une incidence que sur les répertoires d'installation, et non sur les droits d'accès aux fichiers à l'intérieur de ces répertoires. Toutefois, les fichiers créés en cours d'exécution, tels que les journaux, respectent le masque. Nous recommandons umask 022 pour le répertoire d'installation.

## Règles de configuration

Dans une installation qui comporte plusieurs composants Content Manager ou pour laquelle Content Manager a été placé dans un emplacement séparé, un composant Content Manager au moins doit être configuré, en cours d'exécution et accessible avant que vous ne configuriez les autres composants dans votre environnement. Cela garantit que le service de l'autorité de certification installé avec Content Manager est disponible pour émettre des certificats pour d'autres ordinateurs IBM Cognos.

Pour en savoir davantage sur l'ordre d'installation des composants répartis, reportez-vous à la section «Séquence d'installation des composants serveur», à la page 59.

### Règles pour le composant Content Manager actif

Si vous installez plusieurs composants Content Manager, le premier ordinateur Content Manager que vous démarrez devient celui actif par défaut. A l'aide d'IBM Cognos Administration, vous pouvez définir un autre ordinateur Content Manager comme ordinateur actif par défaut.

Les ordinateurs Content Manager en veille sont destinés à la protection par reprise automatique. Si l'ordinateur Content Manager actif n'est pas disponible à cause d'une panne logicielle ou matérielle, un ordinateur Content Manager en veille est activé et les demandes sont dirigées vers ce dernier.

En cas de défaillance du service Content Manager actif, les données de session non enregistrées sont perdues. Lorsqu'un autre service Content Manager devient actif, les utilisateurs peuvent être invités à se connecter.

Pour en savoir davantage sur l'activation d'un service Content Manager, reportez-vous au *Guide d'administration et de sécurité*. Pour en savoir davantage sur les composants Content Manager actifs et en veille, reportez-vous à la section «Composants Content Manager actifs et en veille».

Dans les installations comportant plusieurs composants Content Manager, configurez IBM Cognos Analytics pour qu'il utilise des passerelles compilées au lieu de la passerelle CGI par défaut. Par exemple, utilisez Apache Module pour Apache Server ou IBM HTTP Server, ou utilisez ISAPI pour IIS. Si vous ne procédez pas ainsi, les performances risquent de diminuer après une opération de reprise.

### Mise à niveau

Si vous procédez à une mise à niveau à partir de ReportNet ou d'une version antérieure d'IBM Cognos Business Intelligence, vous pouvez continuer à utiliser les données de configuration existantes. Cependant, certaines nouvelles fonctionnalités d'IBM Cognos Analytics nécessitent une configuration.

### PowerCubes

Si vous prévoyez d'installer IBM Cognos Transformer et d'utiliser des PowerCubes sécurisés à partir d'un espace-noms IBM Cognos Series 7, vous devez installer Content Manager sur un ordinateur prenant en charge IBM Cognos Series 7.

## Composants Content Manager actifs et en veille

Vous pouvez installer un nombre quelconque d'installations de Content Manager, mais une seule est activée à tout instant. Chacune des autres installations agit en tant que Content Manager en veille.

Les composants Content Manager en veille sont destinés à la protection par reprise automatique. Si le service Content Manager actif n'est pas disponible à cause d'une panne logicielle ou matérielle, un service Content Manager en veille est activé et les demandes sont dirigées vers ce dernier.

En cas de défaillance du service Content Manager actif, les données de session non enregistrées sont perdues. Lorsqu'un autre service Content Manager devient actif, les utilisateurs peuvent être invités à se connecter.

Par défaut, la première instance Content Manager installée avec IBM Cognos Analytics est l'instance active. Un administrateur du serveur IBM Cognos Analytics peut redéfinir l'instance Content Manager par défaut et l'instance Content Manager active à tout moment. Lors du démarrage d'IBM Cognos Analytics, l'instance Content Manager par défaut verrouille la base de données du magasin de contenu pour qu'elle ne soit plus accessible aux autres installations de Content Manager. Ces autres installations passent en mode veille.

Ce mécanisme de reprise fonctionne car les répartiteurs et le service Content Manager actif communiquent régulièrement. Si un répartiteur ne parvient plus à contacter Content Manager, il signale une instance Content Manager en veille, qui devient l'instance Content Manager active. Les autres installations de Content Manager restent en mode veille pour assurer une prise en charge permanente des reprises. Les instances Content Manager en veille extraient les paramètres cryptographiques, tels que la clé symétrique commune (utilisée pour chiffrer et déchiffrer les données) de l'instance Content Manager active.

Si vous installez plusieurs instances de Content Manager, vous **devez** vous assurer que les horloges système des ordinateurs Content Manager sont synchronisées, afin de garantir le bon fonctionnement des reprises entre chaque instance.

# Installation de Content Manager sous UNIX ou Linux

Procédez comme suit pour installer Content Manager sous UNIX ou Linux.

## Avant de commencer

Accédez à la page IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) pour vérifier que les correctifs requis sont installés sur votre ordinateur.

## Procédure

1. Définissez la variable d'environnement JAVA_HOME de sorte qu'elle pointe vers l'emplacement d'installation de votre JRE (Java Runtime Environment), comme `/répertoire/java/version_java/jre`.

   Pour fonctionner sur un système d'exploitation Linux, IBM Cognos Analytics requiert une machine JVM, comme celle qui est fournie IBM.
2. Accédez à l'emplacement dans lequel les fichiers d'installation ont été téléchargés et décompressés.

   **Conseil :** Utilisez de nouvelles versions du logiciel de compression de fichier pour extraire les fichiers. Les versions antérieures de ces logiciels peuvent ne pas parvenir à extraire les fichiers.
3. Pour démarrer un assistant d'installation, accédez au répertoire du système d'exploitation, puis tapez `./ca_srv_<plateforme>_<version>.bin`

   **Conseil :** Lorsque vous utilisez la commande `ca_srv_<plateforme>_<génération>.bin` avec XWindows, les caractères japonais figurant dans les messages et les fichiers journaux peuvent être altérés. Lors d'une installation en japonais sous UNIX ou Linux, commencez par définir les variables d'environnement LANG=C et LC_ALL=C (où C est le code de langue, par exemple ja_JP.PCK sous Solaris), puis démarrez l'assistant d'installation.

   Si vous n'utilisez pas XWindows, exécutez une installation automatique. Pour en savoir davantage, voir Chapitre 11, «Installation sans surveillance, désinstallation et configuration», à la page 299.

4. Suivez les instructions fournies par l'assistant d'installation pour copier les fichiers sur votre ordinateur et implémenter une configuration de base.
   - Lors du choix du répertoire, tenez compte des points suivants :

     Installez Content Manager dans un répertoire dont le nom du chemin d'accès contient uniquement des caractères ASCII. Certains serveurs Web UNIX et Linux ne prennent pas en charge les caractères non ASCII dans les noms de répertoires.

     Si vous installez IBM Cognos Analytics sur un ordinateur disposant d'une version antérieure du produit que vous souhaitez conserver, vous devez installer la nouvelle version dans un autre répertoire.
   - Lors du choix des composants, désélectionnez-les tous à l'exception de **Référentiel de contenu**.
5. Cliquez sur **Terminer**.
6. Ajoutez le répertoire *emplacement_installation*/bin à la variable d'environnement de chemin de bibliothèque appropriée.
   - Pour Solaris ou Linux, LD_LIBRARY_PATH
   - Pour AIX, LIBPATH
   - Pour HP-UX, SHLIB_PATH

### Que faire ensuite

Ne configurez pas IBM Cognos Analytics immédiatement, car il convient d'abord d'effectuer d'autres tâches pour s'assurer que l'environnement est correctement installé.

Vous pourrez configurer IBM Cognos Analytics ultérieurement à l'aide d'IBM Cognos Configuration en saisissant cogconfig.sh dans le répertoire *emplacement_installation*/bin.

## Installation de Content Manager sous Windows

Procédez comme suit pour installer Content Manager sur Microsoft Windows.

Pour les ordinateurs Windows, l'emplacement d'installation par défaut utilise le répertoire **Program Files**. Si vous effectuez l'installation à cet emplacement, veillez à exécuter IBM Cognos Configuration comme administrateur. Vous pouvez également installer le produit dans un répertoire différent de **Program Files**, comme C:\IBM\cognos\analytics.

L'installation requiert au moins 5 Go dans le répertoire temp. Vous définissez ce répertoire temp à l'aide de la variable d'environnement TMP.

### Avant de commencer

Accédez à la page IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) pour vérifier que les correctifs requis sont installés sur votre ordinateur.

### Procédure

1. Accédez au répertoire dans lequel les fichiers d'installation ont été téléchargés et décompressés, puis cliquez deux fois sur ca_srv_<plateforme>_<génération>.exe.

**Conseil :** Utilisez de nouvelles versions du logiciel de compression de fichier pour extraire les fichiers. Les versions antérieures de ces logiciels peuvent ne pas parvenir à extraire les fichiers.

2. Sélectionnez la langue d'installation.

   La langue sélectionnée détermine la langue de l'interface utilisateur. Toutes les langues prises en charge sont installées. Vous pouvez redéfinir l'interface utilisateur sur l'une des langues installées après l'installation.

3. Sélectionnez l'option d'installation **personnalisée** et suivez les instructions fournies par l'assistant d'installation pour copier les fichiers sur votre ordinateur.

   - Lors du choix du répertoire, tenez compte des points suivants :

     Installez Content Manager dans un répertoire dont le nom du chemin d'accès contient uniquement des caractères ASCII. Certains serveurs Web de Microsoft Windows ne prennent pas en charge les caractères non ASCII dans les noms de répertoires.

     Si vous installez IBM Cognos Analytics sur un ordinateur disposant d'une version antérieure du produit que vous souhaitez conserver, vous devez l'installer dans un autre répertoire.

   - Lors du choix des composants, désélectionnez-les tous à l'exception de **Référentiel de contenu** dans l'option d'installation **Personnalisée**.

4. Cliquez sur **Terminer**.

### Que faire ensuite

Si vous démarrez IBM Cognos Configuration depuis l'assistant d'installation, veillez à exécuter les tâches supplémentaires de cette section pour vous assurer que l'environnement est correctement configuré avant de démarrer les services.

Vous pouvez démarrer IBM Cognos Configuration à l'aide du raccourci **IBM Cognos Configuration** depuis le menu **Démarrer**.

## Configuration de la connectivité de base de données du magasin de contenu

Vous devrez peut-être installer un logiciel client de base de données et/ou des pilotes Java Database Connectivity (JDBC) sur chaque ordinateur sur lequel est installé Content Manager. De cette façon, Content Manager pourra accéder à la base de données Content Store.

### Configuration de la connectivité à la base de données pour le magasin de contenu Microsoft SQL Server

11.0.5

Le pilote JDBC Microsoft remplace le pilote JSQLConnect pour SQL Server. A partir de la version 11.0.5 et suivantes, vous devez télécharger le nouveau pilote de type 4 depuis Microsoft et le placer dans le dossier *emplacement_installation*/drivers.

Il vous faut le fichier pilote JAR `sqljdbc42.jar` pour prendre en charge la version Java fournie avec IBM Cognos Analytics.

**Important :** Pour le code d'accès unique (SSO) et l'authentification Windows, vous devez placer `sqljdbc_auth.dll` dans le répertoire `bin64`. L'authentification Windows est une configuration de code d'accès unique. La sélection dans

Configuration Manager pour Content Manager est appelée **Base de données Microsoft SQL Server (Authentification Windows)**.

## Configuration de la connectivité à une base de données de magasin de contenu IBM Db2

Cette procédure indique comment configurer la connectivité à un magasin de contenu Db2. Vous devez appliquer cette procédure à chaque ordinateur sur lequel vous avez installé Content Manager.

Vous devez utiliser un pilote JDBC (Java Database Connectivity) de type 4 pour vous connecter à votre magasin de contenu.

Le pilote de type 4 est considéré comme un produit indépendant. Il ne nécessite pas l'installation du client Db2.

### Procédure

Copiez les fichiers suivants du répertoire *installation_DB2*\sqllib\java dans le répertoire *emplacement_installation*\drivers :

- Le fichier de pilote universel, db2jcc4.jar
- Le fichier de licence :

  Pour Db2 on Linux, UNIX ou Windows, utilisez db2jcc_license_cu.jar.

  Pour Db2 on z/OS, utilisez db2jcc_license_cisuz.jar.

  Si vous vous connectez à Db2 on z/OS, utilisez la version de pilote de Linux, UNIX ou le kit de mise à jour version 5 de Windows version 9.1, ou encore le kit de mise à jour version 2 de la version 9.5.

  **Conseil :** Pour vérifier la version du pilote, exécutez la commande suivante :

  ```
  java -cp chemin\db2jcc4.jar com.ibm.db2.jcc.DB2Jcc -version
  ```

**Génération d'un fichier script pour créer une base de données pour un magasin de contenu IBM Db2 :**

Vous pouvez générer un fichier script pour créer automatiquement la base de données dans Db2 sur toutes les plateformes. Ce fichier script est un fichier DDL.

**Procédure**

1. Démarrez **IBM Cognos Configuration**.
2. Dans la fenêtre **Explorateur**, sous **Accès aux données** > **Content Manager**, cliquez sur **Content Store**.

   La configuration par défaut est conçue pour une base de données Db2. Assurez-vous que le **Type** est **DB2 database**.
3. Dans la zone **Serveur de base de données et numéro de port**, saisissez le nom de l'ordinateur et le numéro de port sur lequel s'exécute Db2. Par exemple, localhost:50000. Où 50000 est le numéro de port par défaut utilisé par Db2. Si vous utilisez un autre numéro de port, veillez à l'utiliser.
4. Cliquez sur la zone **Valeur** en regard de la propriété **ID utilisateur et mot de passe**, puis cliquez sur l'icône d'édition. Saisissez les valeurs appropriées et cliquez sur **OK**.
5. Dans la fenêtre **Propriétés**, pour la propriété **Nom de la base de données**, saisissez le nom de la base de données du magasin de contenu.

**Important :** Le nom ne doit pas comporter plus de huit caractères, et doit être composé exclusivement de caractères alphanumériques, de traits de soulignement et de traits d'union.

6. Cliquez avec le bouton droit sur **Content Store**, puis cliquez sur **Générer les données DDL**.
7. Cliquez sur **Détails** pour enregistrer l'emplacement du fichier DDL généré.

   Le fichier DDL appelé `createDB.sql` est créé. Le script est créé dans le répertoire *emplacement_installation*`\configuration\schemas\content\db2`.

**Que faire ensuite**

Utilisez ce script pour créer une base de données dans Db2. Pour plus d'informations sur l'utilisation d'un fichier DDL, consultez votre documentation Db2.

Si vous utilisez l'interface de ligne de commande Db2, vous pouvez exécuter le script en saisissant la commande suivante :

```
db2 -tvf createDB.sql
```

**Création d'espaces de table pour un magasin de contenu sur IBM Db2 for z/OS :**

Un administrateur de base de données doit exécuter des scripts pour créer un ensemble d'espaces de table requis pour la base de données du magasin de contenu. Modifiez les scripts pour remplacer les paramètres génériques par ceux convenant à votre environnement.

Par défaut, le magasin de contenu est utilisé pour les notifications, les tâches manuelles et les annotations. Vous pouvez créer des bases de données distinctes pour chacune.

**Pourquoi et quand exécuter cette tâche**

Utilisez les conventions d'attribution de nom pour Db2 on z/OS. Par exemple, tous les noms de paramètres doivent commencer par une lettre et ne pas dépasser huit caractères. Il existe deux exceptions à la limite de longueur des caractères :

- CMSCRIPT_CS_ID ne doit pas dépasser 2 caractères.
- CMSCRIPT_TABLESPACE ne doit pas dépasser 6 caractères.

L'exception se produit lorsque deux paramètres sont regroupés et que la longueur ne peut pas dépasser 8 caractères.

Pour plus d'informations, consultez le site IBM Db2 for z/OS Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEPEK/db2z_prodhome.html).

**Procédure**

1. Connectez-vous à la base de données en tant qu'utilisateur disposant de privilèges afin de créer et d'insérer des espaces de table, ainsi qu'autoriser l'exécution d'instructions SQL.
2. Accédez au répertoire contenant les scripts :

   *emplacement_installation*`/configuration/schemas/content/db2z0S`
3. Faites une copie de sauvegarde du fichier script `tablespace_db2z0S.sql` et enregistrez le fichier à un autre emplacement.
4. Ouvrez le fichier script `tablespace_db2z0S.sql` d'origine.

a. Ajoutez une instruction de connexion au début du script.

   Par exemple :

   ```
   connect to databasename;
   ```

b. Utilisez le tableau suivant pour vous aider à remplacer les paramètres génériques par des paramètres appropriés à votre environnement.

   Tous les paramètres listés ne figurent pas dans le script, mais pourront être ajoutés ultérieurement.

*Tableau 9. Noms et description des paramètres du script d'espace de table du magasin de contenu*

| Nom du paramètre | Description |
|---|---|
| **CMSCRIPT_STOGROUP** | Indique le nom du groupe de stockage. |
| **CMSCRIPT_DATABASE** | Indique le nom de la base de données du magasin de contenu. |
| **CMSCRIPT_CS_ID** | Indique l'identification du sous-système pour la base de données du magasin de contenu.<br><br>L'ID ne doit pas dépasser deux caractères. |
| **CMSCRIPT_TABLESPACE** | Spécifie le nom de l'espace de table dans lequel se trouvent toutes les tables de base du magasin de contenu.<br><br>Les tables auxiliaires ne sont pas incluses.<br><br>Le nom ne doit pas dépasser six caractères. |
| **CMSCRIPT_LARGE_BP** | Spécifie le nom du groupe de mémoire tampon alloué pour les objets LOB particulièrement importants.<br><br>Ce pool de mémoire tampon correspond au pool de mémoire tampon de 32 ko créé lorsque l'administrateur de base de données a créé la base de données du magasin de contenu sur le système z/OS. |
| **CMSCRIPT_REGULAR_BP** | Spécifie le nom du groupe de mémoire tampon de taille normale alloué pour les objets normaux ou importants.<br><br>Ce pool de mémoire tampon correspond au pool de mémoire tampon de 16 ko créé lorsque l'administrateur de base de données a créé la base de données du magasin de contenu sur le système z/OS. |
| **CMSCRIPT_USERNAME** | Spécifie le compte utilisateur qui accède à la base de données du magasin de contenu. |

5. Enregistrez et exécutez le script.

   Par exemple, si vous configurez votre fichier `clp.properties` et votre alias Db2 dans votre profil ou fichier script `tcshrc`, entrez la commande suivante pour exécuter le script :

   ```
   db2 -tvf tablespace_db2zOS.sql
   ```

6. Octroyez les droits d'utilisateur IBM Cognos pour les espaces de table créés lorsque vous avez exécuté le fichier script `tablespace_db2zOS.sql` :

a. Faites une copie du fichier script `rightsGrant_db2zOS.sql` et stockez-la dans un autre emplacement.
b. Dans l'outil d'accès distant, ouvrez le fichier script `rightsGrant_db2zOS.sql` d'origine et remplacez les paramètres génériques par des valeurs appropriées à votre environnement.

   Veillez à utiliser les mêmes valeurs que celles utilisées lors de l'allocation de ressources aux pools de mémoire tampon et au compte utilisateur..
c. Ajoutez une instruction de connexion au début du script.

   Par exemple :

   ```
   connect to databasename user username using password;
   ```
d. Enregistrez puis exécutez le script.

   Par exemple :

   ```
   db2 -tvf rightsGrant_db2zOS.sql
   ```

7. Pour créer les espaces de table de notifications, accédez au répertoire *emplacement_installation*/configuration/schemas/delivery/zosdb2.
   a. Faites une copie de sauvegarde du fichier script `NC_TABLESPACES.sql` et enregistrez le fichier sur un autre emplacement.
   b. Ouvrez le fichier script `NC_TABLESPACES.sql` d'origine et utilisez le tableau ci-après pour vous aider à remplacer les paramètres fictifs par ceux convenant à votre environnement.

*Tableau 10. Descriptions et noms des paramètres de l'espace de table pour la base de données de notification Db2 on z/OS*

| Nom du paramètre | Description |
|---|---|
| NCCOG | Indique le nom de la base de données de notification. |
| DSN8G810 | Indique le nom du groupe de stockage. |
| BP32K | Indique le nom du groupe de mémoire tampon. |

   Tous les paramètres répertoriés ne figurent pas dans le script, mais peuvent être ajoutés ultérieurement.
   c. Enregistrez et exécutez le script.

      Par exemple :

      ```
      db2 -tvf NC_TABLESPACES.sql
      ```
   d. Ouvrez le fichier de script `NC_CREATE_DB2.sql` et remplacez le paramètre fictif NCCOG par le nom de la base de données de notification.
   e. Enregistrez le script.

      Les services de surveillance des travaux et de planification exécutent automatiquement le script. Toutefois, vous pouvez l'exécuter vous-même.
8. Pour créer les espaces de table de tâches utilisateur, accédez au répertoire *emplacement_installation*/configuration/schemas/hts/zosdb2.
   a. Faites une copie de sauvegarde du fichier script `HTS_tablespaces.sql` et enregistrez le fichier à un autre emplacement.
   b. Ouvrez le fichier script `HTS_TABLESPACES.sql` d'origine et utilisez le tableau ci-après pour vous aider à remplacer les paramètres fictifs par ceux convenant à votre environnement.

*Tableau 11. Noms et descriptions des paramètres d'espace de table de tâches utilisateur dans Db2 on z/OS*

| Nom du paramètre | Description |
|---|---|
| NCCOG | Indique le nom de la base de données. |
| DSN8G810 | Indique le nom du groupe de stockage. |
| BP32K | Indique le nom du pool de mémoire tampon de 32 k. |

Pour une liste complète des paramètres requis, voir le script.

c. Enregistrez et exécutez le script.

d. Ouvrez le fichier de script `HTS2_CREATE_Db2zos.sql` et utilisez le tableau ci-après pour vous aider à remplacer les paramètres génériques par ceux convenant à votre environnement.

*Tableau 12. Noms et descriptions des paramètres d'espace de table de tâches utilisateur dans Db2 on z/OS*

| Nom du paramètre | Description |
|---|---|
| NCCOG | Nom de la base de données. |

Pour une liste complète des paramètres requis, voir le script.

e. Enregistrez et exécutez le script.

9. Pour créer les espaces de table d'annotations, accédez au répertoire *emplacement_installation*`/configuration/schemas/ans/zosdb2`.

a. Faites une copie de sauvegarde du fichier script `ANN_TABLESPACES.sql` et enregistrez le fichier à un autre emplacement.

b. Ouvrez le fichier script `ANN_TABLESPACES.sql` d'origine et utilisez le tableau ci-après pour vous aider à remplacer les paramètres fictifs par ceux convenant à votre environnement.

*Tableau 13. Noms et descriptions des paramètres d'espace de table pour les annotations dans Db2 on z/OS*

| Nom du paramètre | Description |
|---|---|
| NCCOG | Nom de la base de données. |
| DSN8G810 | Nom du groupe de stockage. |
| BP32K | Nom du pool de mémoire tampon de 32 k. |

Pour une liste complète des paramètres requis, voir le script.

c. Enregistrez et exécutez le script.

d. Ouvrez le fichier de script `ANS2_CREATE_Db2zos.sql` et utilisez le tableau ci-après pour vous aider à remplacer les paramètres génériques par ceux convenant à votre environnement.

*Tableau 14. Noms et descriptions des paramètres d'espace de table pour les annotations dans Db2 on z/OS*

| Nom du paramètre | Description |
|---|---|
| NCCOG | Nom de la base de données. |

Pour une liste complète des paramètres requis, voir le script.

e. Enregistrez et exécutez le script.

### Configuration de la connectivité à la base de données d'un magasin de contenu Oracle

Cette procédure indique comment configurer la connectivité à un magasin de contenu Oracle. Vous devez appliquer cette procédure à chaque ordinateur sur lequel vous avez installé Content Manager.

#### Procédure

1. Sur l'ordinateur où le client Oracle est installé, accédez au répertoire *ORACLE_HOME*/jdbc/lib.
2. Copiez le fichier de bibliothèque correspondant à votre version du client Oracle dans le répertoire *emplacement_installation*\drivers de l'ordinateur sur lequel Content Manager est installé et sur lequel la notification est envoyée à une base de données Oracle.

   Si vous utilisez Oracle 12c, vous devez disposer du fichier ojdbc7.jar.

   Si vous utilisez Oracle 11g, vous devez disposer du fichier ojdbc5.jar.

   Les fichiers sont disponibles dans le répertoire d'installation du client ou serveur Oracle ; ils peuvent également être téléchargés à partir du site Web Oracle Technology Network.

### Configuration de la connectivité à la base de données d'un magasin de contenu Informix

Cette procédure indique comment configurer la connectivité à la base de données pour un magasin de contenu Informix. Vous devez appliquer cette procédure à chaque ordinateur sur lequel vous avez installé Content Manager.

#### Procédure

1. Sur l'ordinateur sur lequel Informix est installé, accédez au répertoire *emplacement_Informix*/sqllib/java.
2. Copiez les fichiers suivants dans le répertoire *emplacement_installation*\drivers de chaque ordinateur sur lequel Content Manager est installé.
   - le fichier de pilote universel, db2jcc4.jar
   - Le fichier de licence, db2jcc4_license_cisuz.jar

## Opérations de configuration critiques à réaliser en premier

Ces opérations de configuration sont indispensables au succès de votre installation. Réalisez les opérations suivantes une fois les composants installés.

### Vérifiez que les pilotes JDBC se trouvent au bon emplacement

Pour la version 11.0.x d'IBM Cognos Analytics, les pilotes JDBC doivent être copiés dans le répertoire *emplacement_installation*\drivers.

L'utilisation du répertoire *emplacement_installation*\webapps\p2pd\WEB-INF\lib pour les pilotes JDBC n'est pas prise en charge.

### Remplacez le pilote JSQL pour Microsoft SQL Server par le pilote JDBC de Microsoft

A partir de la version 11.0.5 d'IBM Cognos Analytics, le pilote JSQL pour Microsoft SQL Server est remplacé par le pilote JDBC de Microsoft. Vous devez télécharger et placer le fichier JAR requis dans le répertoire *emplacement_installation*\drivers. Pour plus d'informations, voir Configuration pour le magasin de contenu Microsoft SQL Server.

### Spécifiez la propriété Groupe de configuration

Si vous avez installé IBM Cognos Analytics par le biais d'une installation de type **Personnalisé**, ouvrez IBM Cognos Configuration et définissez la propriété **Groupe de configuration**. Pour plus d'informations, voir Gestion du groupe de configuration.

### Activez ou désactivez la modélisation Web

Par défaut, les connexions de source de données JDBC qui ont été créées dans IBM Cognos Administration ne sont pas disponibles pour les modules de données dans l'interface d'administration **Gérer** > **Serveurs de données**. Si vous voulez utiliser vos connexions de source de données existantes (mises à niveau) pour créer des modules de données, vous devez activer la modélisation Web sur ces connexions.

Certaines sources de données ne sont pas aptes à être utilisées comme sources pour la création de modules de données. Dans ce cas, vous pouvez interdire l'utilisation de la modélisation Web sur les connexions de la source de données.

Pour activer ou désactiver la modélisation Web pour vos connexions de source de données, procédez comme suit :

1. Dans IBM Cognos Analytics, accédez à **Gérer** > **Console d'administration**.
2. Dans IBM Cognos Administration, dans l'onglet **Configuration**, sélectionnez **Connexions de source de données**.
3. Localisez la source de données et cliquez sur **Définir les propriétés**.
4. Dans l'onglet **Connexion**, sélectionnez ou désélectionnez la case **Autoriser la modélisation Web**.

## Démarrage d'IBM Cognos Configuration

Utilisez IBM Cognos Configuration pour configurer les composants IBM Cognos Analytics et pour démarrer et arrêter les services IBM Cognos.

### Avant de commencer

Avant de démarrer IBM Cognos Configuration, vérifiez que l'environnement d'exploitation est configuré correctement. Ainsi, assurez-vous que toutes les variables d'environnement ont été définies.

Sous Microsoft Windows, vous ne pouvez démarrer IBM Cognos Configuration à la dernière page de l'Assistant d'installation que si aucune configuration complémentaire n'est requise. Si, par exemple, vous utilisez un serveur de base de données autre que Microsoft SQL pour le magasin de contenu, copiez les pilotes JDBC (Java Database Connectivity) dans le dossier *emplacement_installation*/drivers avant de démarrer l'outil de configuration.

Sous UNIX ou Linux, ne démarrez pas IBM Cognos Configuration à la dernière page de l'assistant d'installation. Une configuration complémentaire est requise avant la configuration d'IBM Cognos Analytics. Par exemple, vous devez mettre à jour votre environnement Java.

Assurez-vous qu'un compte utilisateur ou un service a été configuré pour l'exécution d'IBM Cognos.

Lisez «Opérations de configuration critiques à réaliser en premier», à la page 1.

### Procédure

1. Sous Microsoft Windows, cliquez sur **Démarrer** > **IBM Cognos Configuration**.

   Si vous utilisez un ordinateur avec Windows, et si vous avez installé le produit dans le répertoire `Program Files (x86)`, lancez IBM Cognos Configuration en tant qu'administrateur.
2. Sous UNIX ou Linux, accédez au répertoire *emplacement_installation*`/bin64` et saisissez la commande suivante :

   `./cogconfig.sh`

   Si IBM Cognos Configuration ne s'ouvre pas, vérifiez que la variable d'environnement DISPLAY est définie.

   Si le message `JAVA.Lang.unsatisfied link` apparaît, assurez-vous que vous utilisez une version prise en charge de Java.

   Si le message `Java.lang.unsupportedClassVersionError` apparaît, vérifiez que vous utilisez une version 64 bits de Java.

## Définition des propriétés de connexion à la base de données du magasin de contenu

Vous devez fournir des informations sur le serveur de base de données pour permettre à Content Manager de se connecter à la base de données du magasin de contenu. Content Manager utilise la connexion à la base de données pour accéder au magasin de contenu. Après avoir défini les propriétés de connexion à la base de données, vous pouvez tester la connexion entre Content Manager et le magasin de contenu.

Dans un environnement de production, vous devez utiliser une base de données de niveau entreprise pour votre magasin de contenu. Pour en savoir davantage, reportez-vous à la rubrique traitant du déploiement complet du magasin de contenu dans le Guide d'administration et de sécurité.

Si vous effectuez une mise à niveau à partir de IBM Cognos Business Intelligence ou d'une version antérieure d'IBM Cognos Analytics, configurez IBM Cognos Analytics de manière qu'il pointe vers une copie de la base de données du magasin de contenu existante. Après avoir enregistré la configuration et démarré le service IBM Cognos, les données du magasin de contenu sont automatiquement mises à niveau et ne peuvent plus être utilisées par l'ancienne version. En utilisant une copie de la base de données d'origine avec la nouvelle version, vous pouvez conserver l'exécution des données d'origine avec IBM Cognos Analytics ou la version antérieure.

Assurez-vous que vous avez utilisé l'un des serveurs de base de données pris en charge pour créer le magasin de contenu.

### Configuration des propriétés de connexion à la base de données d'un magasin de contenu IBM Db2

Vous devez fournir des informations sur le serveur de base de données pour permettre à Content Manager de se connecter à la base de données du magasin de contenu.

#### Procédure

1. Dans l'emplacement où vous avez installé Content Manager, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Accès aux données**, **Content Manager**, cliquez sur **Content Store**.

3. Dans la fenêtre **Propriétés**, pour la propriété **Nom de la base de données**, saisissez le nom de la base de données ou son alias.
4. Modifiez les données d'identification de connexion pour spécifier un ID utilisateur et un mot de passe valides :
   - Cliquez sur la zone **Valeur** en regard de la propriété **ID utilisateur et mot de passe**, puis sur le bouton d'édition lorsqu'il s'affiche.
   - Saisissez les valeurs appropriées et cliquez sur **OK**.
5. Dans la zone **Serveur de base de données et numéro de port**, saisissez le nom de l'ordinateur et le numéro de port sur lequel s'exécute Db2. Par exemple,`localhost:50000`. 50000 est le numéro de port par défaut utilisé par Db2. Si vous utilisez un autre numéro de port, veillez à l'utiliser.
6. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
7. Pour tester la connexion entre Content Manager et la base de données du magasin de contenu, cliquez sur **Tester** dans le menu **Actions**.

   Content Manager se connecte à la base de données, vérifie les droits d'accès de celle-ci, puis crée une table et la complète. La table n'est pas supprimée et est utilisée à chaque exécution du test.

## Configuration des propriétés de connexion à la base de données d'un magasin de contenu sur IBM Db2 for z/OS

Vous devez fournir des informations sur le serveur de base de données pour permettre à Content Manager de se connecter à la base de données du magasin de contenu.

### Procédure

1. Dans l'emplacement où vous avez installé Content Manager, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Accès aux données** > **Content Manager**, cliquez sur **Content Store**.
3. Dans la fenêtre **Propriétés**, pour la propriété **Nom de la base de données**, saisissez le nom de la base de données ou son alias.
4. Modifiez les données d'identification de connexion pour spécifier un ID utilisateur et un mot de passe valides :
   - Cliquez sur la zone **Valeur** en regard de la propriété **ID utilisateur et mot de passe**, puis sur l'icône Editer lorsqu'elle s'affiche. Veillez à employer l'ID utilisateur spécifié pour **`CMSCRIPT_USERNAME`** lors de la création des espaces de table.
   - Saisissez les valeurs appropriées et cliquez sur **OK**.
5. Pour la propriété **Serveur de base de données et numéro de port**, entrez les informations relatives à la base de données sous la forme *`nom_d'hôte:port`*.
6. Dans la fenêtre **Explorateur**, cliquez sur **Configuration locale**.
7. Cliquez dans la zone **Valeur** des **Propriétés avancées**, puis cliquez sur l'icône d'édition.

   La boîte de dialogue **Valeur - Propriétés avancées** s'affiche.
8. Cliquez sur **Ajouter** pour ajouter les paramètres de la connexion de base de données.

   Les valeurs du tableau sont des exemples. Vous devez saisir des valeurs qui correspondent à votre environnement.

*Tableau 15. Paramètres de connexion au magasin de contenu pour Db2 for z/OS*

| Nom du paramètre | Exemple de valeur |
|---|---|
| CMSCRIPT_CREATE_IN | COGUCS.T1TSCS |
| CMSCRIPT_STOGROUP | DBOIUSR |
| CMSCRIPT_DATABASE | COGUCS |
| CMSCRIPT_CS_ID | T1 |
| CMSCRIPT_TABLESPACE | TSCS |
| CMSCRIPT_LARGE_BP | BP32K |
| CMSCRIPT_REGULAR_BP | BP16K0 |

9. Cliquez sur **Fichier** > **Enregistrer**.
10. Pour tester la connexion entre Content Manager et la base de données du magasin de contenu, cliquez sur **Tester** dans le menu **Actions**.

## Définition des propriétés de connexion de base de données d'un magasin de contenu Microsoft SQL Server, Oracle ou Informix

Vous devez fournir des informations sur le serveur de base de données pour vous assurer que Content Manager peut se connecter à la base de données du magasin de contenu.

### Procédure

1. Sur l'ordinateur où vous avez installé Content Manager, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Accès aux données**, **Content Manager**, cliquez avec le bouton droit sur **Content Store**, puis sélectionnez **Supprimer**.

   Cette étape supprime la connexion à la ressource par défaut. Content Manager ne peut accéder qu'à une seule instance du magasin de contenu.
3. Cliquez avec le bouton droit de la souris sur **Content Manager**, puis sélectionnez **Nouvelle ressource** et **Base de données**.
4. Dans la zone **Nom**, saisissez un nom pour la ressource.
5. Dans la zone **Type**, sélectionnez le type de base de données, puis cliquez sur **OK**.

   **Conseil :** Si vous souhaitez utiliser une base de données enfichable Oracle ( 11.0.4) ou une fonctionnalité Oracle RAC, sélectionnez **Base de données Oracle (options avancées)**.
6. Dans la fenêtre **Propriétés**, indiquez les valeurs du type de base de données :
   - Si vous utilisez une base de données Microsoft SQL Server saisissez les valeurs appropriées pour les propriétés **Serveur de base de données comportant un numéro de port ou un nom d'instance** et **Nom de la base de données**.

     Pour une base de données Microsoft SQL Server, vous pouvez utiliser un numéro de port, tel que 1433, ou une instance nommée comme valeur de la propriété **Serveur de base de données comportant un numéro de port ou un nom d'instance**.

     Pour la propriété **Serveur de base de données comportant un numéro de port ou un nom d'instance**, incluez le nom de l'instance s'il existe plusieurs instances de Microsoft SQL Server.

     Pour vous connecter à une instance nommée, vous devez indiquer son nom en tant que propriété URL JDBC (Java Database Connectivity) ou source de

données. Par exemple, vous pouvez taper `localhost\instance1`. Si aucune propriété de nom d'instance n'est indiquée, une connexion à l'instance par défaut est créée.

Les propriétés indiquées pour l'instance nommée, ainsi que l'ID utilisateur, le mot de passe et le nom de la base de données, servent à créer une adresse URL JDBC. Voici un exemple :

`jdbc:JSQLConnect://localhost\\instance1/user=sa/`*`plus de propriétés en fonction des besoins`*

- Si vous utilisez une base de données Oracle, saisissez les valeurs appropriées pour les propriétés **Serveur de base de données et numéro de port** et **SID**.
- `11.0.4` Si vous utilisez une base de données enfichable Oracle, pour la propriété **Identificateur de base de données**, entrez `//<serveur>/<nomservice>`. Par exemple, `//corpserv1:1522/PDB1`
- Si vous utilisez une base de données Oracle Net 8 avancée, saisissez la paire Net8 de type mot clé et valeur d'Oracle pour la connexion dans la propriété **Identificateur de base de données**.

  Voici un exemple de paire mot clé / valeur Oracle Net8 :

  ```
  (description=(address=(host=myhost)(protocol=tcp)(port=1521)
  (connect_data=(sid=(orcl)))))
  ```

  Quand vous sélectionnez la base de données Oracle avancée, IBM Cognos Analytics utilise les fonctions orientées entreprise d'Oracle pour sélectionner un écouteur, passer à un autre écouteur si le premier échoue, se reconnecter automatiquement à la base de données si la connexion échoue ou encore équilibrer les demandes de connexion entre les écouteurs et entre les répartiteurs.
- Si vous utilisez une base de données Informix, tapez les valeurs appropriées pour les propriétés **Serveur de base de données comportant un numéro de port ou un nom d'instance** et **Nom de la base de données**.

7. Pour configurer les données d'identification de connexion, indiquez un ID utilisateur et un mot de passe :
   - Cliquez sur la zone **Valeur** en regard de la propriété **ID utilisateur et mot de passe**, puis sur l'icône Editer lorsqu'elle s'affiche.
   - Saisissez les valeurs appropriées et cliquez sur **OK**.
8. Si vous hébergez plusieurs bases de données de magasin de contenu sur une instance Informix, créez la propriété avancée CMSCRIPT_CS_ID et indiquez le compte sous lequel cette instance est exécutée :
   - Dans la fenêtre **Explorateur**, cliquez sur **Configuration locale**.
   - Dans la fenêtre **Propriétés**, cliquez sur la colonne **Valeur** correspondant à **Propriétés avancées**, puis sur l'icône Editer.
   - Dans la boîte de dialogue **Valeur - Propriétés avancées**, cliquez sur l'option **Ajouter**.
   - Dans la colonne **Nom**, tapez `CMSCRIPT_CS_ID`.
   - Dans la colonne **Valeur**, saisissez l'ID utilisateur correspondant au compte sous lequel l'instance du magasin de contenu est exécutée.

     Utilisez un compte utilisateur différent pour chaque instance de la base de données Informix du magasin de contenu.
9. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

   Les données d'identification pour la connexion sont immédiatement chiffrées.
10. Pour tester la connexion entre Content Manager et la base de données du magasin de contenu, cliquez sur **Tester** dans le menu **Actions**.

Content Manager se connecte à la base de données, vérifie les droits d'accès de celle-ci, puis crée une table et la complète. La table n'est pas supprimée et est utilisée à chaque exécution du test.

### Résultats

Content Manager peut désormais créer les tables requises dans le magasin de contenu lors du premier démarrage du service IBM Cognos. Si les propriétés de connexion ne sont pas définies correctement, vous ne pouvez pas démarrer les services d'IBM Cognos.

## Configuration des propriétés d'environnement pour les ordinateurs Content Manager

Les ordinateurs Content Manager doivent connaître l'emplacement du magasin de contenu, des autres ordinateurs Content Manager et de la base de données utilisée pour la notification.

Après avoir installé Content Manager sur les ordinateurs que vous utilisez pour la protection par reprise automatique, vous devez configurer Content Manager sur ces ordinateurs. Si vous avez installé plusieurs ordinateurs Content Manager, vous devez répertorier tous les URI de Content Manager sur chaque ordinateur Content Manager.

Une fois les tâches de configuration requises effectuées et le service IBM Cognos Analytics démarré, le service de l'autorité de certification est disponible pour l'émission de certificats à l'attention d'autres ordinateurs. Vous pouvez ensuite exécuter les tâches de configuration requises sur d'autres ordinateurs, tels que l'ordinateur des composants du groupe de serveurs d'applications et les ordinateurs passerelle. Vous pouvez par ailleurs continuer à configurer les ordinateurs Content Manager en modifiant les paramètres de propriété par défaut (voir «Modification des paramètres de configuration par défaut», à la page 151) afin de mieux les adapter à votre environnement. Par exemple, vous pouvez configurer les composants d'IBM Cognos Analytics pour qu'ils utilisent un fournisseur d'authentification (voir Chapitre 8, «Configuration des fournisseurs d'authentification», à la page 239), activer et désactiver des services (voir «Activation et désactivation des services», à la page 165) sur les ordinateurs Content Manager ou modifier les paramètres globaux (voir «Modification des paramètres globaux», à la page 217).

Il est à noter que si vous modifiez les paramètres globaux sur l'un des ordinateurs Content Manager, vous devez effectuer les mêmes modifications sur les autres ordinateurs Content Manager.

### Configuration du Content Manager actif

Les ordinateurs Content Manager doivent connaître l'emplacement du magasin de contenu, des autres ordinateurs Content Manager et de la base de données utilisée pour la notification.

#### Procédure

1. Sur l'ordinateur Content Manager que vous désignez comme ordinateur actif par défaut, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, cliquez sur la valeur de l'option **URI de Content Manager**, puis cliquez sur le bouton d'édition.

4. Indiquez les URI pour les autres ordinateurs Content Manager :
   - Dans la boîte de dialogue **Valeur - URI de Content Manager**, cliquez sur **Ajouter**.
   - Dans la ligne vide de la table, cliquez et saisissez l'URI complet de l'ordinateur Content Manager.

     Ne supprimez pas la première valeur de la table. Cette valeur est nécessaire et identifie l'ordinateur Content Manager local.

     Remplacez la chaîne localhost de l'URI par un nom d'hôte ou une adresse IP. Toutes les propriétés d'URI doivent adopter le même format : tous les noms d'hôte, ou toutes les adresses IP.
   - Répétez les deux étapes précédentes (indiquées par des puces) pour chaque URI à ajouter.

     Vous devez inclure tous les URI de Content Manager dans la liste.
   - Cliquez sur le bouton **OK**.
5. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Configuration des gestionnaires de contenu en veille

Les ordinateurs Content Manager doivent connaître l'emplacement du magasin de contenu, des autres ordinateurs Content Manager et de la base de données utilisée pour la notification.

### Procédure

1. Assurez-vous que les propriétés d'environnement soient déjà configurées sur au moins un ordinateur Content Manager et que les composants IBM Cognos Analytics y soient actifs.
2. Démarrez IBM Cognos Configuration sur l'ordinateur Content Manager en veille.
3. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
4. Dans la fenêtre **Propriétés**, cliquez sur la valeur de l'option **URI de Content Manager**, puis cliquez sur le bouton d'édition.
5. Indiquez les URI pour les autres ordinateurs Content Manager :
   - Dans la boîte de dialogue **Valeur - URI de Content Manager**, cliquez sur **Ajouter**.
   - Dans la ligne vide de la table, cliquez et saisissez l'URI complet de l'ordinateur Content Manager.

     Ne supprimez pas la première valeur de la table. Cette valeur est nécessaire et identifie l'ordinateur Content Manager local.

     Remplacez la chaîne localhost de l'URI par un nom d'hôte ou une adresse IP. Toutes les propriétés d'URI doivent adopter le même format : tous les noms d'hôte, ou toutes les adresses IP.
   - Répétez les deux étapes précédentes (indiquées par des puces) pour chaque URI à ajouter.

     Vous devez inclure tous les URI de Content Manager dans la liste.
   - Cliquez sur le bouton **OK**.
6. Dans la fenêtre **Explorateur**, sous **Sécurité** > **Cryptographie**, cliquez sur **Cognos**, le fournisseur cryptographique par défaut.
7. Assurez-vous que tous les paramètres cryptographiques correspondent à ceux que vous avez configurés sur l'ordinateur Content Manager actif par défaut.
8. Dans la fenêtre **Explorateur**, dans la section **Accès aux données** > **Gestionnaire de contenu**, cliquez sur l'option **Content Store**.

9. Assurez-vous que toutes les autres propriétés correspondent à celles que vous avez configurées dans l'ordinateur Content Manager actif par défaut.
10. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Définition d'une connexion à un serveur de messagerie

Si vous désirez envoyer des rapports par courrier électronique, vous devez configurer une connexion à un serveur de messagerie.

### Procédure

1. Dans la section **Accès aux données** de la fenêtre **Explorateur**, cliquez sur **Notification**.
2. Dans la fenêtre **Propriétés**, pour la propriété **Serveur de messagerie et numéro de port**, saisissez le nom d'hôte et le port du serveur de messagerie SMTP (sortant).

   Pour être en mesure d'ouvrir des rapports envoyés par courrier électronique, vous devez remplacer la partie correspondant au nom d'hôte localhost dans l'**URI de la passerelle** par l'adresse IP ou par le nom de l'ordinateur. Sinon, l'adresse URL du courrier électronique contiendra la chaîne localhost, ce qui empêchera les utilisateurs distants d'ouvrir le rapport.

   Pour pouvoir ouvrir les rapports adressés sous forme de liens, assurez-vous que l'**URI de passerelle** définie sur les serveurs de rapports et de notifications correspond à un serveur web accessible et hébergeant le contenu IBM Cognos. Si des utilisateurs nomades accèdent aux liens à distance, envisagez d'utiliser un URI externe.
3. Cliquez sur la zone **Valeur** en regard de la propriété **Code d'utilisateur et mot de passe**, puis sur le bouton d'édition lorsqu'il s'affiche.
4. Saisissez les valeurs dans la boîte de dialogue **Valeur - Code d'utilisateur et mot de passe**, puis cliquez sur **OK**.

   Si les données d'identification de connexion ne sont pas requises pour le serveur SMTP, supprimez les informations par défaut pour la propriété **Compte et mode de passe**. Lorsque vous êtes invité à confirmer que cette propriété reste vide, cliquez sur **OK**. Assurez-vous que le nom d'utilisateur par défaut est supprimé. Dans le cas contraire, le compte par défaut est utilisé et les notifications ne fonctionnent pas correctement.
5. Dans la fenêtre **Propriétés**, saisissez la valeur appropriée pour le compte de l'expéditeur par défaut.
6. Dans la fenêtre **Explorateur**, cliquez avec le bouton droit sur **Notification**, puis sélectionnez **Tester**.

   IBM Cognos Analytics teste la connexion au serveur de messagerie.

### Activation d'une connexion TLS sécurisée à votre serveur de messagerie

Activer une connexion TLS sécurisée à votre serveur de messagerie pour autoriser la communication TLS chiffrée.

**Remarque :** Si le chiffrement SSL est configuré mais qu'aucune connexion TLS sécurisée n'est activée, la connexion échoue et le message suivant s'affiche :

502 Commande inconnue

### Avant de commencer

Vous devez disposer d'un certificat, généralement au format .crt, qui est commun au serveur de messagerie.

### Procédure

1. Importez le certificat pour activer une relation de confiance entre Cognos Analytics et le serveur de messagerie.
   a. Si vous utilisez HTTP sur l'URI du répartiteur, vous devez importer le certificat dans le magasin de clés JRE :
      - Sous Windows, tapez *emplacement_installation*\bin\DLS_SSL_CertImportTool.bat *emplacement_certificat**certificat_messagerie*.crt -p *mot_de_passe_magasin_de_clés*
      - Sous Unix ou Linux, tapez *emplacement_installation*/bin/DLS_SSL_CertImportTool.sh *emplacement_certificat*/*certificat_messagerie*.crt -p *mot_de_passe_magasin_clés*
   b. Si vous utilisez HTTPS sur l'URI du répartiteur, vous devez importer le certificat dans le magasin de clés Cognos :
      - Sous Windows, tapez *emplacement_installation*\bin\ThirdPartyCertificateTool.bat -T -i -r *emplacement_certificat**certificat_messagerie*.crt -p *mot_de_passe_magasin_de_clés*
      - Sous Unix ou Linux, tapez *emplacement_installation*/bin/ThirdPartyCertificateTool.sh -T -i -r *emplacement_certificat*/*certificat_messagerie*.crt -p *mot_de_passe_magasin_clés*
2. Dans Cognos Configuration, sélectionnez **Accès aux données** > **Notification** et éditez les propriétés comme suit :

| Nom | valeur |
|---|---|
| Serveur de messagerie SMTP | *nom_serveur_messagerie*:*numéro_port*, où *numéro_port* désigne un port activé pour TLS/SSL ou STARTTLS |
| Compte et mot de passe | ID utilisateur et mot de passe lorsque l'authentification sur le serveur de messagerie est requise. |
| Emetteur par défaut | Compte de messagerie qui envoie des courriers électroniques à partir du serveur de messagerie. |
| Chiffrement SSL activé | Vrai |

3. Dans Cognos Configuration, sélectionnez **Configuration locale**.
   a. Cliquez sur la zone **Valeur** pour **Propriétés avancées**.
   b. Cliquez sur l'icône en forme de crayon .
   c. Cliquez sur **Ajouter**.
   d. Dans la zone **Nom**, tapez `emf.mail.tls.enabled`
   e. Dans la zone **Valeur**, tapez `true`
   f. Cliquez sur le bouton **OK**.
4. Dans Cognos Administration, configurez le paramètre avancé `emf.mail.tls.enabled` avec la valeur `true`. Pour plus d'informations, voir *Configuration des paramètres avancés pour des services spécifiques*.

   **Remarque :** Vous devez redémarrer le service de diffusion après avoir apporté cette modification.

## Activation de la sécurité

Par défaut, IBM Cognos Analytics autorise l'accès anonyme. Si vous souhaitez appliquer un système de sécurité à votre environnement IBM Cognos Analytics, vous devez désactiver l'accès anonyme et configurer IBM Cognos Analytics de manière qu'il utilise un fournisseur d'authentification.

### Procédure

1. Dans la fenêtre **Explorateur** d'IBM Cognos Configuration, cliquez sur **Sécurité** >**Authentification** > **Cognos**.
2. Cliquez sur la zone **Valeur** associée à l'option **Voulez-vous autoriser les connexions anonymes ?**, puis sélectionnez **Faux**.
3. Cliquez avec le bouton droit de la souris sur **Authentification**, puis cliquez sur **Nouvelle ressource** > **Espace-noms**.
4. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
5. Dans la liste **Type**, cliquez sur le type d'espace-noms approprié, puis sur **OK**.

   Le nouveau fournisseur d'authentification s'affiche dans la fenêtre **Explorateur**, sous le composant **Authentification**.
6. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.
7. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Démarrage de Content Manager

Après avoir défini les propriétés de connexion à la base de données Content Store et configuré l'espace-noms de sécurité, vous pouvez démarrer l'ordinateur Content Manager.

### Avant de commencer

Assurez-vous qu'un compte utilisateur ou service est défini. Pour en savoir davantage, reportez-vous à la section «Configuration d'un compte utilisateur ou d'un compte de service réseau pour IBM Cognos Analytics», à la page 15.

### Procédure

1. Démarrez IBM Cognos Configuration.

   Lorsque vous procédez à une mise à niveau, un message indiquant la détection de fichiers de configuration et leur mise à niveau s'affiche.
2. Veillez à enregistrer la configuration pour pouvoir démarrer le service IBM Cognos.
3. Dans le menu **Actions**, cliquez sur **Tester**.

   IBM Cognos Configuration vérifie la disponibilité des clés symétriques communes (CSK), teste la configuration de l'espace-noms et contrôle les connexions au magasin de contenu et aux autres ressources.

   **Conseil :** Si l'option **Tester** ne peut pas être sélectionnée, dans la fenêtre **Explorateur**, cliquez sur **Configuration locale**.
4. Si le test échoue, reconfigurez les propriétés concernées, puis exécutez à nouveau le test.

   Vous pouvez tester certains composants individuellement en cliquant avec le bouton droit sur le composant souhaité dans le panneau **Explorateur** et en sélectionnant l'option **Tester**.

Démarrez le service uniquement lorsque tous les tests n'aboutissent à aucune erreur.

5. Dans le menu **Actions**, cliquez sur l'option **Démarrer**.

   Le démarrage du service IBM Cognos peut prendre quelques minutes.

   Cette action démarre tous les services installés qui ne sont pas en cours d'exécution et enregistre le service IBM Cognos sur Windows.

## Test de l'installation de Content Manager.

Vous pouvez tester l'installation via un navigateur Web.

### Procédure

1. Ouvrez un navigateur Web.
2. Vérifiez que Content Manager est en cours d'exécution en saisissant l'URI du gestionnaire de contenu actif. Par exemple, `http://nom_hôte:port/p2pd/servlet`

   La valeur par défaut de *nom_hôte:port* est localhost:9300.

   Content Manager est disponible si la valeur d'**Etat** est **En cours d'exécution** ou **En veille**.

# Installation et configuration des services d'application

Vous pouvez installer les composants des services d'application sur un ou plusieurs ordinateurs.

## Installation des composants des services d'application

Assurez-vous que l'ordinateur sur lequel vous avez installé le service Content Manager actif est configuré et disponible avant de configurer les ordinateurs hébergeant les composants des services d'application.

Si vous effectuez une mise à niveau, IBM Cognos Analytics utilise les données de configuration existantes pour les ordinateurs hébergeant les composants des services d'application. Toutefois, si vous avez installé les composants des services d'application dans un nouvel emplacement, vous devez configurer les propriétés d'environnement.

### Installations 64 bits

Le composant serveur de rapports, inclus dans les composants des services d'application, est fourni dans les versions 32 et 64 bits. La sélection de la version à utiliser est effectuée à l'aide d'IBM Cognos Configuration après l'installation. Par défaut, le composant serveur de rapports est défini pour utiliser le mode 32 bits, même sur un ordinateur 64 bits. Le mode 32 bits permet d'exécuter tous les rapports alors que le mode 64 bits permet d'exécuter uniquement les rapports créés pour le mode de requête dynamique.

### Conditions requises pour l'imprimante

Pour vous assurer que les rapports s'impriment correctement sous Microsoft Windows, Adobe Reader requiert la configuration d'au moins une imprimante sur le système d'exploitation dans lequel vous installez les composants des services d'application. Tous les rapports, quel que soit le format d'impression choisi, sont envoyés en tant que fichiers PDF temporaires vers Adobe Reader pour impression.

## Installation des composants des services d'application sur les systèmes d'exploitation UNIX ou Linux

Vous pouvez installer les composants des services d'application sur un ou plusieurs ordinateurs, en fonction de votre environnement.

### Avant de commencer

Accédez à la page IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) pour vérifier que les correctifs requis sont installés sur votre ordinateur.

### Procédure

1. Accédez à l'emplacement dans lequel les fichiers d'installation ont été téléchargés et décompressés.

   **Conseil :** Utilisez de nouvelles versions du logiciel de compression de fichier pour extraire les fichiers. Les versions antérieures de ces logiciels peuvent ne pas parvenir à extraire les fichiers.
2. Pour démarrer un assistant d'installation, accédez au répertoire du système d'exploitation, puis tapez `./ca_srv_<plateforme>_<génération>.bin`

   **Conseil :** Lorsque vous utilisez la commande `ca_srv_<plateforme>_<génération>.bin` avec XWindows, les caractères japonais figurant dans les messages et les fichiers journaux peuvent être altérés. Lors d'une installation en japonais sous UNIX ou Linux, commencez par définir les variables d'environnement LANG=C et LC_ALL=C (C étant le code de langue, par exemple ja_JP.PCK sous Solaris), puis démarrez l'Assistant d'installation.

   Si vous n'utilisez pas XWindows, exécutez une installation automatique. Pour en savoir davantage, voir «Utilisation d'une installation sans surveillance», à la page 299.
3. Suivez les instructions fournies par l'assistant d'installation pour copier les fichiers sur votre ordinateur.
   - Lors du choix du répertoire, tenez compte des points suivants :

     Installez les composants des services d'application dans un répertoire dont le nom du chemin d'accès contient uniquement des caractères ASCII. Certains serveurs Web UNIX et Linux ne prennent pas en charge les caractères non ASCII dans les noms de répertoires.
   - Lors du choix des composants, désélectionnez-les tous à l'exception des **services d'application**.
4. Cliquez sur **Terminer**. Ne configurez pas IBM Cognos Analytics immédiatement, car il convient d'abord d'effectuer d'autres tâches pour s'assurer que l'environnement est correctement installé.
5. Ajoutez le répertoire *emplacement_installation*`/bin` à la variable d'environnement de chemin de bibliothèque appropriée.
   - Pour Solaris ou Linux, LD_LIBRARY_PATH
   - Pour AIX, LIBPATH
   - Pour HP-UX, SHLIB_PATH

### Que faire ensuite

Pour configurer IBM Cognos Analytics, utilisez IBM Cognos Configuration. Ouvrez cet outil en saisissant `cogconfig.sh` dans le répertoire *emplacement_installation*`/bin64`.

### Installation des composants des services d'application sous Windows

Vous pouvez installer les composants des services d'application sur un ou plusieurs ordinateurs, en fonction de votre environnement.

Pour les ordinateurs Windows, l'emplacement d'installation par défaut utilise le répertoire **Program Files**. Si vous effectuez l'installation à cet emplacement, veillez à exécuter IBM Cognos Configuration comme administrateur. Vous pouvez également installer le produit dans un répertoire différent de **Program Files**, comme `C:\IBM\cognos\analytics`.

#### Procédure

1. Accédez au répertoire dans lequel les fichiers d'installation ont été téléchargés et décompressés, puis cliquez deux fois sur `ca_srv_<plateforme>_<génération>.exe`.

   **Conseil :** Utilisez de nouvelles versions du logiciel de compression de fichier pour extraire les fichiers. Les versions antérieures de ces logiciels peuvent ne pas parvenir à extraire les fichiers.
2. Sélectionnez la langue d'installation.

   La langue sélectionnée détermine la langue de l'interface utilisateur. Toutes les langues prises en charge sont installées. Vous pouvez redéfinir l'interface utilisateur sur l'une des langues installées après l'installation.
3. Sélectionnez l'option d'installation **personnalisée** et suivez les instructions fournies par l'assistant d'installation pour copier les fichiers sur votre ordinateur.
   - Lors du choix du répertoire, tenez compte des points suivants :

     Installez les composants des services d'application dans un répertoire dont le nom du chemin d'accès contient uniquement des caractères ASCII. Certains serveurs Web ne prennent pas en charge les caractères non ASCII dans les noms de répertoires.
   - Lors du choix des composants, désélectionnez-les tous à l'exception des **services d'application**.
4. Cliquez sur **Terminer**.

#### Que faire ensuite

Vous pouvez démarrer IBM Cognos Configuration à l'aide du raccourci **IBM Cognos Configuration** depuis le menu **Démarrer**.

## Configuration de la connectivité aux bases de données de génération de rapports

Pour assurer la prise en charge des communications entre IBM Cognos Analytics et les sources de données, vous devez installer les logiciels complémentaires de vos sources de données sur le même ordinateur que celui qui héberge le serveur de rapports. Selon la source de données et le mode de requête, le logiciel requis peut inclure des clients de base de données, des fichiers de pilotes JDBC (Java Database Connectivity), ou les deux.

Pour IBM Cognos Analytics, la base de données de requêtes (également appelée base de données de génération de rapports) est accessible uniquement par le moteur de génération de rapports. Le moteur de génération de rapports est installé

avec les composants du groupe de serveurs d'applications. Il est également utilisé par Framework Manager et IBM Cognos Transformer.

### Mode de requête compatible

Pour exécuter des rapports qui utilisent le mode de requête compatible, vous devez utiliser les bibliothèques client de source de données 32 bits et configurer le serveur de rapports comme étant 32 bits. Le mode de requête compatible utilise les connexions client et ODBC pour communiquer avec les sources de données.

### Mode de requête dynamique

Le mode de requête dynamique établit des communications avec les sources de données à l'aide d'une connexion Java ou XMLA.

Pour les bases de données relationnelles prises en charge, une connexion JDBC de type 4 est requise. Un pilote JDBC de type 4 convertit directement les appels JDBC dans le protocole de base de données spécifique au fournisseur. Il s'agit d'une pure syntaxe Java indépendante de la plateforme.

Pour les sources de données OLAP prises en charge, les connectivités Java/XMLA optimisent l'accès en fournissant une configuration MDX personnalisée et améliorée en fonction de la source et de la version spécifiques de votre technologie OLAP, et en reprenant les points intelligents de la source de données OLAP.

Pour consulter la liste actualisée des environnements pris en charge par les produits IBM Cognos Analytics, y compris des informations sur les systèmes d'exploitation, les correctifs, les navigateurs, les serveurs Web, les serveurs d'annuaire, les serveurs de base de données et les serveurs d'applications, consultez la page IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

## Accès aux sources de données OLAP sous Windows

Pour accéder aux bases de données relationnelles et aux sources de données OLAP pour la génération de rapports, vous devez installer le logiciel d'API client délivré par le fournisseur de votre source de données. Ce produit doit être installé sur le même ordinateur que celui où se trouvent les composants du groupe de serveurs d'applications.

### Procédure

1. Installez l'API de base de données de vos bases de données relationnelles et de vos sources de données OLAP sur chaque ordinateur qui héberge le serveur de rapports (où les composants du groupe de serveurs d'applications sont installés).

   Sur les systèmes d'exploitation Microsoft Windows, le moteur de génération de rapports pend en charge la connectivité à la base de données native ou ODBC.
2. Si Framework Manager est installé à un emplacement différent des composants du groupe de serveurs d'applications, vous devez également installer le logiciel d'API client sur l'ordinateur sur lequel Framework Manager est installé. Pour plus d'informations, voir «Définition des variables pour les connexions de source de données de Framework Manager», à la page 135.

## Accès aux sources de données ODBC sous UNIX ou Linux

Pour utiliser une source de données ODBC sous UNIX ou Linux pour vous connecter à une source de données prise en charge, vous devez configurer

l'environnement pour localiser le fichier `.odbc.ini` contenant les références à la source de données, aux bibliothèques de connectivité et à leurs bibliothèques de gestionnaire de pilotes.

Pour consulter les sources de données ODBC prises en charge, voir IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

Après avoir configuré les connexions ODBC, vous devez créer les connexions aux sources de données dans IBM Cognos Administration. Pour obtenir des informations, voir le document *IBM Cognos - Guide d'administration et de sécurité*.

Si votre fournisseur de base de données ne fournit pas de gestionnaire de pilotes, vous pouvez utiliser unixODBC ou iODBC, en fonction de votre système d'exploitation.

Sous Linux, le pack unixODBC livré avec le système d'exploitation fournit le gestionnaire de pilotes ODBC. Vous devez installer unixODBC version 2.2.11, ou une version ultérieure, pour pouvoir configurer des connexions de source de données. Pour vérifier quelle est la version installée, utilisez la commande suivante :`odbcinst --version`. Trouvez la version d'unixODBC requise pour votre base de données, et vérifiez que vous utilisez cette version.

Sous UNIX, le gestionnaire de pilotes iODBC de la source ouverte est fourni comme partie intégrante de l'installation IBM Cognos.

## Procédure

1. Créez une variable d'environnement pour indiquez l'emplacement du fichier `.odbc.ini`.

   Par exemple :

   ```
   export ODBCINI=/usr/local/etc/.odbc.ini
   ```

2. Définissez la variable d'environnement de chemin d'accès aux bibliothèques appropriée pour indiquer l'emplacement des bibliothèques de connectivité 32 bits et du gestionnaire de pilotes pour votre base de données.

   Le tableau suivant répertorie les variables d'environnement devant indiquer l'emplacement des bibliothèques du gestionnaire de pilotes pour chaque système d'exploitation.

*Tableau 16. Variables d'environnement pour votre système d'exploitation*

| Système d'exploitation | Variable d'environnement |
|---|---|
| AIX | LIBPATH |
| Solaris et Linux | LD_LIBRARY_PATH |

3. Si votre fournisseur de base de données ne fournit pas de gestionnaire de pilotes, définissez le chemin d'accès à la bibliothèque pour inclure le chemin du gestionnaire de pilotes local.
   - Sous UNIX, iODBC est fourni comme partie intégrante de l'installation d'IBM Cognos. Les fichiers de bibliothèque se trouvent dans le répertoire *`emplacement_installation`*`/bin`. Le chemin d'accès à la bibliothèque doit déjà contenir le répertoire *`emplacement_installation`*`/bin`.

     Par exemple :

     ```
     LIBPATH=/usr/IBM/cognos/bin:$LIBPATH
     ```

- Sous Linux, le pack unixODBC fournit les bibliothèques de gestionnaire de pilotes requises.

  Par exemple :

  ```
  LD_LIBRARY_PATH=/usr/lib:$LD_LIBRARY_PATH
  ```

### Que faire ensuite

Si vous utilisez plusieurs sources ODBC sous UNIX ou Linux, il peut y avoir des dépendances des fichiers de bibliothèque avec des noms communs mais des implémentations différentes pour la connectivité et le gestionnaire de pilotes. Dans un scénario dans lequel une source ODBC est approuvée alors qu'une autre échoue en raison d'une dépendance, contactez le support technique client. L'utilisation d'un fichier `.odbc.ini` commun peut aboutir à des entrées incompatibles pour divers gestionnaires de pilotes. Pour résoudre le problème, revoyez les exigences de structure entre les gestionnaires de pilotes que vous utilisez et tentez d'utiliser la syntaxe commune entre les gestionnaires de pilotes en conflit.

## Configuration d'IBM Cognos Analytics en vue de l'utilisation d'Oracle Essbase

Si vous utilisez IBM Cognos Analytics avec une source de données Oracle Essbase version 11.1.1, vous devez éditer un fichier de configuration pour informer le serveur IBM Cognos Analytics de votre version.

Par défaut, IBM Cognos Analytics est configuré pour utiliser Oracle Essbase version 11.1.2. Par conséquent, si vous utilisez cette version, aucune configuration n'est requise. Si vous utilisez une autre version d'Oracle Essbase prise en charge, vous devez éditer le fichier qfs.config.xml pour votre version.

En outre, si vous utilisez Oracle Essbase version 11.1.2, vous devez installer Oracle Foundation Services ainsi que le client Oracle Essbase.

### Procédure

1. Accédez au répertoire *emplacement_installation*/configuration.
2. Ouvrez le fichier qfs_config.xml dans un éditeur xml ou un éditeur de texte.
3. Recherchez les lignes suivantes :

   ```
   <!--provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO"-->
   <provider name="DB2OlapODP" libraryName="essodp1112" connectionCode="DO">
   ```

4. Pour Oracle Essbase 11.1.1, modifiez-les comme suit :

   ```
   <provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO">
   <!--provider name="DB2OlapODP" libraryName="essodp1112"
   connectionCode="DO"-->
   ```

5. Pour Oracle Essbase 11.1.2, vérifiez que les lignes apparaissent comme suit :

   ```
   <!--provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO"-->
   <provider name="DB2OlapODP" libraryName="essodp1112" connectionCode="DO">
   ```

6. Enregistrez le fichier et redémarrez le service IBM Cognos.

## Configuration d'Oracle Essbase sur un système d'exploitation UNIX ou Microsoft Windows 64 bits

Si vous utilisez une source de données Oracle Essbase version 11.1.2 avec IBM Cognos Analytics sur un système d'exploitation UNIX ou Microsoft Windows 64 bits, vous devez configurer manuellement les variables d'environnement **ARBORPATH** et **ESSBASEPATH**.

Les variables d'environnement **ARBORPATH** et **ESSBASEPATH** sont créées lors de l'installation du client Oracle Essbase. IBM Cognos Analytics utilise ces variables pour trouver l'emplacement du client Oracle Essbase.

Pour utiliser Oracle Essbase version 11.1.2 avec IBM Cognos Analytics sur un système d'exploitation UNIX ou Microsoft Windows 64 bits, vous devez installer le client Oracle Essbase 64 bits. Ce client 64 bits inclut un client 32 bits utilisé par IBM Cognos Analytics. Pour pointer vers ce client 32 bits, vous devez modifier manuellement les variables d'environnement **ARBORPATH** et **ESSBASEPATH** en remplaçant `EssbaseClient` par `EssbaseClient-32`. L'exemple suivant suppose que le client est installé sur l'unité C. Votre emplacement d'installation peut être différent.

```
ARBORPATH=C:\Hyperion\EPMSystem11R1\products\Essbase\EssbaseClient-32
ESSBASEPATH=C:\Hyperion\EPMSystem11R1\products\Essbase\EssbaseClient-32
```

Si vous utilisez un système d'exploitation Microsoft Windows 32 bits avec un client Oracle Essbase 32 bits, vous n'avez pas besoin de modifier ces variables d'environnement.

# Démarrage d'IBM Cognos Configuration

Utilisez IBM Cognos Configuration pour configurer les composants IBM Cognos Analytics et pour démarrer et arrêter les services IBM Cognos.

## Avant de commencer

Avant de démarrer IBM Cognos Configuration, vérifiez que l'environnement d'exploitation est configuré correctement. Ainsi, assurez-vous que toutes les variables d'environnement ont été définies.

Sous Microsoft Windows, vous ne pouvez démarrer IBM Cognos Configuration à la dernière page de l'Assistant d'installation que si aucune configuration complémentaire n'est requise. Si, par exemple, vous utilisez un serveur de base de données autre que Microsoft SQL pour le magasin de contenu, copiez les pilotes JDBC (Java Database Connectivity) dans le dossier *emplacement_installation*`/drivers` avant de démarrer l'outil de configuration.

Sous UNIX ou Linux, ne démarrez pas IBM Cognos Configuration à la dernière page de l'assistant d'installation. Une configuration complémentaire est requise avant la configuration d'IBM Cognos Analytics. Par exemple, vous devez mettre à jour votre environnement Java.

Assurez-vous qu'un compte utilisateur ou un service a été configuré pour l'exécution d'IBM Cognos.

Lisez «Opérations de configuration critiques à réaliser en premier», à la page 1.

## Procédure

1. Sous Microsoft Windows, cliquez sur **Démarrer** > **IBM Cognos Configuration**.

   Si vous utilisez un ordinateur avec Windows, et si vous avez installé le produit dans le répertoire `Program Files (x86)`, lancez IBM Cognos Configuration en tant qu'administrateur.
2. Sous UNIX ou Linux, accédez au répertoire *emplacement_installation*`/bin64` et saisissez la commande suivante :

   ```
   ./cogconfig.sh
   ```

Si IBM Cognos Configuration ne s'ouvre pas, vérifiez que la variable d'environnement DISPLAY est définie.

Si le message `JAVA.Lang.unsatisfied link` apparaît, assurez-vous que vous utilisez une version prise en charge de Java.

Si le message `Java.lang.unsupportedClassVersionError` apparaît, vérifiez que vous utilisez une version 64 bits de Java.

## Configuration des propriétés d'environnement pour les ordinateurs hébergeant les composants des services d'application

Si vous installez les composants des services d'application sur un ordinateur autre que Content Manager, vous devez configurer l'ordinateur des composants des services d'application de sorte qu'il connaisse l'emplacement de Content Manager. Les composants répartis peuvent ainsi communiquer entre eux.

L'ordinateur des composants des services d'application doit connaître l'emplacement des ordinateurs Content Manager et de la base de données de notification à utiliser pour les données relatives aux travaux et aux plannings. Les composants des services d'application doivent utiliser la même base de données de notification que celle utilisée par les ordinateurs équipés de Content Manager. Pour en savoir davantage, reportez-vous à la section «Modification de la base de données de notification», à la page 178.

Si vous avez installé plusieurs ordinateurs Content Manager, vous devez répertorier tous les URI de Content Manager sur chaque ordinateur des composants des services d'application.

### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, modifiez la portion **localhost** de la propriété **URI de Content Manager** et attribuez-lui le nom d'un ordinateur de Content Manager.
4. Indiquez les URI pour les ordinateurs Content Manager restants :
   - Dans la boîte de dialogue **Valeur - URI de Content Manager**, cliquez sur **Ajouter**.
   - Dans la ligne vide de la table, cliquez et saisissez l'URI complet de l'ordinateur Content Manager.

     Remplacez la chaîne localhost de l'URI par un nom d'hôte ou une adresse IP. Toutes les propriétés d'URI doivent adopter le même format : tous les noms d'hôte, ou toutes les adresses IP.
   - Répétez les deux étapes précédentes (indiquées par des puces) pour chaque URI à ajouter.

     Vous devez inclure tous les URI de Content Manager dans la liste.
   - Cliquez sur le bouton **OK**.
5. Remplacez la partie **localhost** de la propriété **URI de la passerelle** par le nom de l'ordinateur sur lequel vous prévoyez d'installer le composant de la passerelle.

   Ceci permet de s'assurer que les utilisateurs situés dans différents endroits peuvent se connecter aux rapports et aux espaces de travail envoyés par courrier électronique.

6. Remplacez la portion **localhost** des propriétés restantes de l'URI par le nom ou l'adresse IP de votre serveur IBM Cognos Analytics.
7. Dans la fenêtre **Explorateur**, sous **Sécurité** > **Cryptographie**, cliquez sur **Cognos**, le fournisseur cryptographique par défaut.
8. Dans le groupe de propriétés **Paramètres de l'autorité de certification**, définissez la propriété **Mot de passe** de façon à ce qu'elle corresponde à celle configurée sur l'ordinateur Content Manager actif par défaut.
9. Assurez-vous que tous les autres paramètres cryptographiques correspondent à ceux que vous avez configurés dans l'ordinateur Content Manager actif par défaut.
10. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Activation de la version 64 bits du serveur de rapports

Vous pouvez choisir d'utiliser une version 32 bits ou 64 bits du composant serveur de rapports. Pour utiliser la version 64 bits, vous devez l'activer avec IBM Cognos Configuration. L'option par défaut est 32 bits.

Un serveur de rapports 32 bits peut être utilisé avec des packs de mode de requête dynamique et des packs de mode de requête compatible. Un serveur de rapports 64 bits ne peut être utilisé qu'avec des packs de mode de requête dynamique.

Le serveur de rapports fonctionne avec le service de requête. Le service de requête est le moteur qui active le mode de requête dynamique et les cubes dynamiques. Dans une installation 64 bits, le service de requête est 64 bits, que le composant serveur de rapports soit configuré pour la version 32 bits ou 64 bits.

L'utilisation de la version 64 bits du serveur de rapports autorise plus de mémoire adressable pour le rendu des sorties de rapport. Par exemple, des conditions d'insuffisance de mémoire lors de l'étape de rendu de l'exécution d'un rapport peuvent être évitées. Seules les sorties de rapport volumineuses, par exemple des rapports PDF avec plus de mille pages, ont besoin de la version 64 bits du composant serveur de rapports.

Vous devez faire appel à la version 32 bits du serveur de rapports pour les modules qui n'utilisent pas le mode de requête dynamique. Par exemple, si votre module est basé sur des IBM Cognos PowerCubes, vous devez utiliser la version 32 bits du serveur de rapports.

Si vous disposez de plusieurs instances des composants du groupe de serveurs d'application dans votre environnement, vous pouvez en dédier une au serveur de rapports 32 bits. Vous pouvez ensuite utiliser des règles de routage pour que les demandes de rapport pour les modules en mode de requête non dynamique soient routés vers l'instance qui exécute la version 32 bits du serveur de rapports Pour plus d'informations sur les règles de routage, reportez-vous au *Guide d'administration et de sécurité*.

Pour activer la version 64 bits, vous devez installer la version 64 bits des composants du groupe de serveurs d'application sur un ordinateur 64 bits. Si vous installez la version 32 bits des composants du groupe de serveurs d'applications ou si vous utilisez un ordinateur 32 bits, n'activez pas le serveur de rapports 64 bits.

### Procédure

1. Dans la fenêtre **Explorateur** d'IBM Cognos Configuration, cliquez sur **Environnement**.

2. Cliquez sur la zone **Valeur** associée à l'option **Mode d'exécution du serveur de rapports**, puis sélectionnez **64 bits**.
3. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
4. Redémarrez les services IBM Cognos s'ils s'exécutent.

# Démarrage des composants des services d'application

Une fois que vous avez configuré les propriétés de l'environnement, vous pouvez démarrer les services sur l'ordinateur hébergeant les composants des services d'application.

## Avant de commencer

Afin d'utiliser IBM Cognos Analytics pour la génération de rapports, vous devez installer et configurer les composants serveur, démarrer le service IBM Cognos et disposer d'un pack qui référence une source de données disponible. Remarquez que si vous procédez à la mise à niveau, vous pouvez continuer à utiliser les mêmes sources de données.

Assurez-vous qu'un compte utilisateur ou service est défini. Pour en savoir davantage, reportez-vous à la section «Configuration d'un compte utilisateur ou d'un compte de service réseau pour IBM Cognos Analytics», à la page 15.

## Procédure

1. Démarrez IBM Cognos Configuration.

   Lorsque vous procédez à une mise à niveau, un message indiquant la détection de fichiers de configuration et leur mise à niveau s'affiche.
2. Veillez à enregistrer la configuration pour pouvoir démarrer le service IBM Cognos.
3. Dans le menu **Actions**, cliquez sur **Tester**.

   IBM Cognos Configuration vérifie la disponibilité des clés symétriques communes (CSK), teste la configuration de l'espace-noms et contrôle les connexions au magasin de contenu et aux autres ressources.

   **Conseil :** Si l'option **Tester** ne peut pas être sélectionnée, dans la fenêtre **Explorateur**, cliquez sur **Configuration locale**.
4. Si le test échoue, reconfigurez les propriétés concernées, puis exécutez à nouveau le test.

   Vous pouvez tester certains composants individuellement en cliquant avec le bouton droit sur le composant souhaité dans le panneau **Explorateur** et en sélectionnant l'option **Tester**.

   Démarrez le service uniquement lorsque tous les tests n'aboutissent à aucune erreur.
5. Dans le menu **Actions**, cliquez sur l'option **Démarrer**.

   Le démarrage du service IBM Cognos peut prendre quelques minutes.

   Cette action démarre tous les services installés qui ne sont pas en cours d'exécution et enregistre le service IBM Cognos sur Windows.

# Test des composants des services de l'application

Vous pouvez tester l'installation à l'aide d'un navigateur Web.

### Procédure

1. Ouvrez un navigateur Web.
2. Testez la disponibilité du répartiteur en saisissant la valeur **URI externe de répartiteur** d'IBM Cognos Configuration. Par exemple :

   `http://nom_hote:port/bi`

   La valeur par défaut de *nom_hôte:port* est localhost:9300.

   Le répartiteur est disponible lorsque le portail apparaît.

## Configuration d'une base de données Cognos Mobile

Par défaut, les tables Cognos Mobile sont créées dans la base de données Content Store d'IBM Cognos Analytics. Si Cognos Analytics Content Manager et les composants du groupe de serveurs d'applications ne sont pas installés au même emplacement, vous pouvez configurer une autre base de données Cognos Mobile.

Pour configurer la base de données Cognos Mobile, vous devez d'abord la créer, puis créer un compte utilisateur de cette dernière. Vous devez également configurer Cognos Analytics afin qu'il puisse utiliser la base de données.

### Procédure

1. Créez une base de données en utilisant les mêmes instructions que pour la création d'une base de données Content Store. Pour en savoir davantage, voir «Instructions pour la création du magasin de contenu», à la page 8.
2. Créez un compte utilisateur destiné à être utilisé avec la base de données.
3. Sur l'ordinateur sur lequel sont installés les composants du groupe de serveurs d'applications, démarrez IBM Cognos Configuration.
4. Dans le panneau **Explorateur**, sous **Accès aux données**, cliquez avec le bouton droit de la souris sur **Mobile**, puis sélectionnez **Nouvelle ressource** > **Base de données**.
5. Dans la zone **Type**, sélectionnez le type de base de données.
6. Entrez le nom de la base de données et cliquez sur **OK**.
7. Dans la fenêtre **Base de données - Propriétés des ressources**, spécifiez le nom du serveur de base de données et le numéro de port, ainsi que l'ID utilisateur et le mot de passe spécifiés à l'étape 2.
8. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

   Les données d'identification pour la connexion sont immédiatement chiffrées.
9. Pour tester la connexion à la nouvelle base de données, cliquez sur l'option **Tester** dans le menu **Actions**.
10. Dans le menu **Actions**, **démarrez** ou **redémarrez** le service **IBM Cognos**.

    Les tables Cognos Mobile sont créées automatiquement après le premier démarrage du service Mobile.

    **Conseil :** Si les tables ne sont pas créées, en raison des droits d'accès de sécurité de Cognos Analytics qui ne l'autorisent peut-être pas, vous pouvez les créer manuellement. Les scripts de création sont disponibles dans le répertoire *emplacement_installation*`\configuration\schemas\mobile`.

### Que faire ensuite

Les utilisateurs peuvent installer l'application IBM Cognos Mobile sur leurs périphériques mobiles pour accéder aux rapports ou aux analyses d'IBM Cognos Analytics. La version iOS de l'application peut être téléchargée à partir de l'App

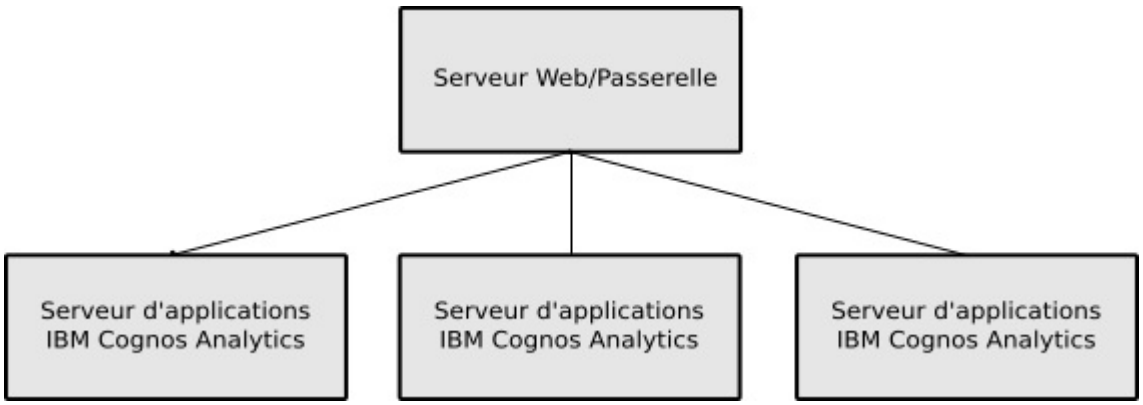
Store d'Apple et la version Android à partir du Play Store de Google.

# Chapitre 5. Installation et configuration de la passerelle

Vous pouvez installer la passerelle facultative sur un ou plusieurs ordinateurs. Installez la passerelle uniquement si vous prévoyez de configurer des options avancées, telles qu'une connexion unique dotée de la sécurité Kerberos avec IIS ou une architecture dans laquelle le serveur Web est publiquement disponible en dehors du pare-feu. IBM Cognos Analytics utilise le serveur Web pour équilibrer les charges de certaines demandes, ainsi que pour héberger et fournir du contenu statique, comme des icônes et des fichiers image.

Assurez-vous que l'ordinateur sur lequel vous avez installé les services d'application actifs est configuré et disponible avant de configurer les ordinateurs passerelle.

Le diagramme suivant montre le serveur de passerelle et plusieurs serveurs Cognos Analytics. Lorsque l'équilibrage de charge est activé, la charge de travail est répartie sur les serveurs.




Cette configuration est également recommandée dans un environnement comportant un seul serveur de groupe de serveurs d'application car le routage serait dirigé vers le serveur ; elle permet également d'ajouter des groupes de serveurs d'applications si nécessaire.

Effectuez les opérations suivantes pour installer et configurer la passerelle :

- Installez les composants de passerelle. Voir «Installation de la passerelle deCognos Analytics», à la page 98.
- Configurez IBM Cognos Analytics. Voir «Configuration de Cognos Analytics avec votre serveur Web», à la page 99.
- Si votre serveur Web est Apache HTTP Server ou IBM HTTP Server, effectuez les procédures de la section «Configuration d'Apache HTTP Server ou IBM HTTP Server», à la page 102.
- Si votre serveur Web est Microsoft Internet Information Services, effectuez les procédures de la section «Configuration de Microsoft Internet Information Services», à la page 116.
- Testez l'installation de la passerelle .

# Installation de la passerelle deCognos Analytics

Vous pouvez installer la passerelle de IBM Cognos Analytics sur un ou plusieurs ordinateurs. Si vous disposez d'une ferme web, vous pouvez installer une passerelle IBM Cognos Analytics sur chaque serveur Web.

## Avant de commencer

Accédez à la page IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186) pour vérifier que les correctifs requis sont installés sur votre ordinateur.

Assurez-vous que le répertoire temporaire dispose d'au moins 5 Go de mémoire.

**Conseil :** Le répertoire temporaire est défini via la variable d'environnement *IATEMPDIR* pour les systèmes d'exploitation UNIX ou Linux, ou via *TMP* pour les systèmes d'exploitation Microsoft Windows.

## Procédure

1. Démarrez l'Assistant d'installation.
   a. Pour UNIX ou Linux, accédez au répertoire du système d'exploitation et tapez : `./ca_srv_version_plateforme.bin`

      **Conseil :** Lorsque vous utilisez la commande `ca_srv_<plateforme>_<génération>.bin` avec XWindows, les caractères japonais figurant dans les messages et les fichiers journaux peuvent être altérés. Lors d'une installation en japonais sous UNIX ou Linux, commencez par définir les variables d'environnement LANG=C et LC_ALL=C (où C est le code de langue, par exemple ja_JP.PCK sous Solaris), puis démarrez l'assistant d'installation.

      Si vous n'utilisez pas XWindows, exécutez une installation automatique. Pour en savoir davantage, voir Chapitre 11, «Installation sans surveillance, désinstallation et configuration», à la page 299.
   b. Pour Microsoft Windows, accédez au répertoire du système d'exploitation, ou bien à l'emplacement de téléchargement des fichiers d'installation, puis faites un double clic sur `ca_srv_version_plateforme.exe`.
2. Sélectionnez la langue d'installation.

   La langue sélectionnée détermine la langue de l'interface utilisateur. Toutes les langues prises en charge sont installées. Vous pouvez redéfinir l'interface utilisateur sur l'une des langues installées après l'installation.
3. Sélectionnez l'option d'installation **personnalisée** et suivez les instructions fournies par l'assistant d'installation pour copier les fichiers nécessaires sur votre ordinateur.
   - Lors du choix du répertoire, tenez compte des points suivants :

     Installez les composants de passerelle dans un répertoire dont le nom du chemin d'accès contient uniquement des caractères ASCII. Certains serveurs Web UNIX et Linux ne prennent pas en charge les caractères non ASCII dans les noms de répertoires.
   - Lors du choix des composants, désélectionnez-les tous à l'exception de **Passerelle**.
4. Cliquez sur **Terminer**.

# Configuration de Cognos Analytics avec votre serveur Web

Vous devez configurer votre serveur Web pour que les utilisateurs puissent se connecter au portail IBM Cognos Analytics.

Pour la génération de rapports avec IBM Cognos Analytics, vous devez également définir la date d'expiration applicable au contenu du répertoire d'images de votre serveur Web, pour que le navigateur Web ne contrôle pas le statut de ces dernières après le premier accès.

## Droits d'accès au fichier

Le compte sous lequel le serveur s'exécute doit bénéficier des droits en lecture, écriture et exécution sur l'emplacement d'installation Cognos. L'accès en lecture est requis pour le répertoire `./configuration` du fichier `cogstartup.xml`. L'accès en écriture est requis pour `./logs`, si le suivi pour débogage est nécessaire. L'accès en exécution est requis pour le répertoire `./cgi-bin`, de sorte que les modules SSO pour Apache HTTP Server, IBM HTTP Server, ou Microsoft Internet Information Services puissent être exécutés par le serveur Web.

## Valeurs de référence pour les procédures de configuration

Référez-vous aux valeurs suivantes lorsque nécessaire :

- Nom de serveur : nom d'hôte du serveur Web
- Numéro de port : 80 (non-SSL) ou 443 (SSL)
- Nom de répertoire virtuel : ibmcognos
- Nom de serveur Cognos Analytics : nom d'hôte du serveur IBM Cognos Analytics

  **Important :** Si votre environnement contient plusieurs serveurs Cognos Analytics, n'incluez pas le serveur qui exécute le service Content Manager dans les étapes ci-dessous. N'incluez que les serveurs Cognos Analytics dont les composants de serveur d'applications sont installés et configurés.
- Numéro de port de Cognos Analytics : `9300`

Tous ces paramètres, ou certains d'entre eux, se trouvent dans Cognos Configuration, en fonction du type d'installation utilisé :

- **URI de la passerelle** : Si vous n'utilisez pas SSL, accédez à `http://`*`nom_hôte_serveur_web`*`:80/ibmcognos/bi/v1/disp`. Si vous utilisez SSL, accédez à `https://`*`nom_hôte_serveur_web`*`:443/ibmcognos/bi/v1/disp`

  Il s'agit de l'URL des contenus déconnectés, tels que les liens dans des PDF, dans Excel et dans les rapports actifs. Elle est également utilisée dans les liens envoyés par courrier électronique.
- **URI du répartiteur pour la passerelle** : `http(s)://`*`nom_hôte_serveur_IBM_Cognos_Analytics`*`:9300/bi/v1/disp`

  Il s'agit de la liste des URI auxquels le module Cognos Apache ou le code ISAPI se connecte lors d'un transfert de demandes. Plusieurs entrées sont utilisées pour la reprise en ligne. Incluez tous les serveurs d'applications IBM Cognos Analytics appropriés.
- **URI du répartiteur des applications externes** : `http(s)://`*`nom_hôte_serveur_IBM_Cognos_Analytics`*`:9300/bi/v1/disp`

  Les applications externes telles que Framework Manager se connectent sur cette URL pour effectuer des opérations SDK.

### Microsoft Internet Information Services

Si vous souhaitez configurer la connexion unique (SSO), assurez-vous qu'IsapiModule et WindowsAuthenticationModule sont installés et activés.

Installez l'extension Application Request Routing for IIS. Pour savoir comment procéder, voir https://www.iis.net/downloads/microsoft/application-request-routing. L'extension URL Rewrite est installée par la même occasion.

URL Rewrite permet aux administrateurs Web de créer des règles puissantes dans le but d'implémenter des URL plus simples à mémoriser pour les utilisateurs et plus faciles à trouver par les moteurs de recherche. Application Request Routing permet aux administrateurs de serveur web d'accroître l'évolutivité et la fiabilité des applications Web par le biais du routage basé sur des règles, l'affinité de nom d'hôte et client, l'équilibrage de charge des demandes de serveur HTTP et le cache-disque distribué.

Si vous effectuez la mise à niveau à partir de Cognos Analytics 11.0.3 vers Cognos Analytics 11.0.4 (ou version ultérieure) et si vous avez modifié le fichier `server.xml` pour configurer un chemin `sso/login` pointant vers `/ibmcognos/cgi-bin/cognosisapi.dll`, supprimez l'entrée suivante de *`emplacement_installation`*`/wlp/usr/servers/cognosserver/server.xml` :

```
<jndiEntry jndiName="glass/sso/login" value="/ibmcognos/cgi-bin/cognosisapi.dll"/>
```

Pour plus de détails sur la configuration d'Active Directory Server, voir «Activation du code d'accès unique entre Active Directory Server et les composants IBM Cognos», à la page 253

## Activation de la passerelle Web 32 bits

Pour un serveur Web 32 bits, vous devez déplacer manuellement les fichiers de passerelle 32 bits vers votre répertoire d'installation.

### Procédure

1. Accédez au répertoire *`emplacement_installation`*`/cgi-bin`.
2. Saisissez la commande suivante :
   - Sur les systèmes d'exploitation UNIX ou Linux, entrez `./copyGateMod.sh 32bit`
   - Sur les systèmes d'exploitation Windows, entrez `copyGateMod.bat 32bit`

### Résultats

Les fichiers de la passerelle 32 bits sont copiés du répertoire `cgi-bin/lib` vers le répertoire `cgi-bin`.

**Remarque :** Si vous devez restaurer les fichiers de passerelle 64 bits par défaut, suivez la procédure et entrez `./copyGateMod.sh 64bit` ou `copyGateMod.bat 64bit`. Les fichiers de passerelle 64 bits sont copiés du répertoire `cgi-bin/lib64` vers le répertoire `cgi-bin`.

## Configuration des URI du répartiteur

Si vous installez la passerelle sur un ordinateur autre que Content Manager ou que celui des composants du groupe de serveurs d'applications, vous devez configurer la passerelle afin qu'elle connaisse l'emplacement d'un répartiteur. Un répartiteur est installé sur chaque ordinateur Content Manager et des composants du groupe

de serveurs d'applications. Configurez la passerelle afin qu'elle utilise le répartiteur sur un ordinateur des composants du groupe de serveurs d'applications.

Pour la protection par reprise automatique, vous pouvez configurer plusieurs répartiteurs pour un même ordinateur passerelle. Lorsque plusieurs répartiteurs sont configurés, les demandes sont normalement acheminées vers le premier répartiteur de la liste. Si le répartiteur devient indisponible, la passerelle identifie le prochain répartiteur opérationnel de la liste et lui adresse les demandes. Le statut du répartiteur principal est contrôlé par la passerelle et les demandes sont réacheminées vers ce composant lorsqu'il est remis en service.

Une fois les tâches de configuration effectuées, la passerelle peut fonctionner dans votre environnement.

## Avant de commencer

Assurez-vous que les ordinateurs sur lesquels vous avez installé Content Manager sont configurés et que l'ordinateur Content Manager actif par défaut est disponible avant de configurer les ordinateurs passerelle.

## Procédure

1. Démarrez IBM Cognos Configuration.
   a. Sous Microsoft Windows, cliquez sur **Démarrer** > **IBM Cognos Configuration**.

      Si vous utilisez un ordinateur avec Windows 7 ou Windows 2008, et si vous avez installé le produit dans le répertoire `Program Files (x86)`, lancez IBM Cognos Configuration en tant qu'administrateur.
   b. Sous UNIX ou Linux, accédez au répertoire *`emplacement_installation`*`/bin64` et saisissez la commande suivante :

      ```
      ./cogconfig.sh
      ```

      Si IBM Cognos Configuration ne s'ouvre pas, vérifiez que la variable d'environnement *DISPLAY* est définie.

      Si le message `JAVA.Lang.unsatisfied link` apparaît, assurez-vous que vous utilisez une version prise en charge de Java.

      Si le message `Java.lang.unsupportedClassVersionError` apparaît, vérifiez que vous utilisez une version 64 bits de Java.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, sous **Paramètres de la passerelle**, définissez les valeurs de l'option **URI du répartiteur pour la passerelle** :
   - Cliquez dans la colonne **Valeur**.
   - Cliquez sur le bouton **Editer**.
   - Remplacez la chaîne *localhost* de l'URI par le nom ou l'adresse IP d'un ordinateur des composants du groupe de serveurs d'applications.

     Ceci permet de s'assurer que les utilisateurs situés dans différents endroits peuvent se connecter aux rapports et aux espaces de travail envoyés par courrier électronique.

     **Conseil :** Si vous souhaitez envoyer des requêtes au répartiteur depuis une application SDK (Software Development Kit) ou un outil de modélisation IBM Cognos Analytics situé en dehors d'un pare-feu réseau, connectez-vous à une passerelle dédiée configurée de manière à se connecter au répartiteur à l'aide de l'URI interne du répartiteur correspondant à votre environnement

(par exemple, http://localhost:9300/p2pd/servlet/dispatch). Pour des raisons de sécurité, le paramètre par défaut de l'URI du répartiteur pour la propriété de la passerelle empêche le répartiteur d'accepter des requêtes pour une application SDK (Software Development Kit) ou un outil de modélisation situé en dehors du pare-feu. Veillez à configurer un niveau de sécurité approprié pour cette passerelle dédiée, tel que SSL (voir «Configuration du protocole SSL pour les composants d'IBM Cognos», à la page 188). Ne modifiez pas votre passerelle principale de manière à utiliser l'URI interne du répartiteur. Une telle opération réduit le niveau de sécurité des studios et du portail IBM Cognos Analytics.

- Pour ajouter un autre URI, cliquez sur **Ajouter** et remplacez la chaîne *localhost* du nouvel URI par le nom ou l'adresse IP d'un autre ordinateur de composants d'application.

  **Conseil :** Pour utiliser le répartiteur sur un ordinateur Content Manager en veille, veillez à l'ajouter après avoir ajouté les ordinateurs des composants du groupe de serveurs d'applications. Si vous ajoutez le répartiteur à partir de l'ordinateur Content Manager actif, vérifiez qu'il figure en dernier dans la liste.
- Une fois tous les URI définis, cliquez sur **OK**.

4. Dans la fenêtre **Explorateur**, sous **Sécurité** > **Cryptographie**, cliquez sur **Cognos**, le fournisseur cryptographique par défaut.
5. Dans le groupe de propriétés **Paramètres de l'autorité de certification**, définissez la propriété **Mot de passe** de façon à ce qu'elle corresponde à celle configurée sur l'ordinateur Content Manager actif par défaut.
6. Assurez-vous que tous les autres paramètres cryptographiques correspondent à ceux que vous avez configurés dans l'ordinateur Content Manager actif par défaut.
7. Testez l'extraction de la clé symétrique. Dans la fenêtre **Explorateur**, cliquez avec le bouton droit sur **Cryptographie**, puis sélectionnez **Tester**.

   Les composants d'IBM Cognos Analytics vérifient la disponibilité des clés symétriques communes (CSK).
8. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

# Configuration d'Apache HTTP Server ou IBM HTTP Server

Cette section vous explique comment configurer Apache HTTP Server ou IBM HTTP Server en tant que votre serveur Web dans IBM Cognos Analytics.

## Configuration d'IBM HTTP Server V9 dans Cognos Analytics 11.0.10+

11.0.10

Le serveur Web IBM HTTP Server (IHS) V9 vous permet de prendre en charge l'équilibrage de charge et le basculement sur plusieurs serveurs d'application IBM Cognos Analytics.

Pour ce faire, vous devez installer IHS V9 ainsi que les modules de serveur Web pour IBM WebSphere Application Server V9, puis configurer IHS V9 de manière à utiliser le fichier `cognos.conf`.

Pour plus d'informations sur l'installation des modules de serveur Web pour IBM WebSphere Application Server V9, voir cet article (www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/rins_plugins_info.html).

## Procédure

1. Installez IBM Installation Manager (IIM), de préférence la version 1.8.5 ou une version ultérieure, si elle n'est pas déjà installée.

   Vous pouvez télécharger IIM depuis cet emplacement (www.ibm.com/support/docview.wss?uid=swg24041188).
2. Via IIM, installez IBM HTTP Server (IHS) V9 ainsi que les modules de serveur Web pour IBM WebSphere Application Server V9 depuis les référentiels de produit en ligne pour les offres Liberty (www.ibm.com/support/knowledgecenter/SSEQTP_liberty/com.ibm.websphere.wlp.nd.multiplatform.doc/ae/cwlp_ins_repositories.html).

   Assurez-vous d'utiliser les chemins d'installation suivants :
   - `/opt/IHS90` en tant que répertoire racine d'installation d'IHS V9
   - `/opt/IHS90Plugin` en tant que répertoire racine d'installation des modules de serveur Web pour IBM WebSphere Application Server

     Vous ne pouvez pas installer les modules dans le répertoire racine d'IHS V9.
3. Associez les modules de serveur Web WAS V9 à IHS V9 en exécutant les commandes suivantes :

   ```
   . cd /opt/IHS90
   . bin/simplepct.sh /opt/IHS90Plugin
   ```

   **Conseil :** Sous UNIX, consultez le fichier `httpd.conf` de votre installation IHS V9 une fois la commande exécutée. Si vous voyez `$PLG_ROOT`, remplacez-le par le dossier racine d'installation des modules de serveur Web WAS V9, typiquement `/opt/IHS90Plugin`.
4. Générez le fichier `plugin-cfg.xml` pour les modules de serveur Web WAS. Pour en savoir davantage, voir «Génération de plugin-cfg.xml pour les serveurs Cognos Analytics», à la page 105.
5. Copiez le fichier `plugin-cfg.xml` généré à l'étape 4 dans le répertoire *rep_racine_installation_modules_serveur_Web_WAS*`/config/webserver1`, typiquement `/opt/IHS90Plugin/config/webserver1`.

   **Conseil :** Sous UNIX, assurez-vous que le fichier `plugin-cfg.xml` est associé à des droits en lecture et en exécution une fois le fichier copié.
6. Configurez IHS V9 en procédant comme suit :
   a. Accédez au fichier modèle `cognos_IHS9_SSO.conf` ou `cognos_IHS9.conf` dans le répertoire *emplacement_installation_composant_passerelle_cognos_analytics*`/cgi-bin/templates`.
   b. Copiez le fichier modèle dans le répertoire *rép_racine_IHS9*`/conf`, typiquement `/opt/IHS90/conf`, et renommez-le `cognos.conf`. Modifiez le fichier `cognos.conf` de sorte qu'il pointe vers l'emplacement d'installation adéquat.
   c. Configurez `httpd.conf`, comme indiqué dans l'article Configuration de Cognos Analytics avec Apache HTTP Server ou IBM HTTP Server.
   d. Redémarrez le serveur Web IHS V9.

## Configuration d'IBM HTTP Server V9 avec SSL

Si vous utilisez SSL (Secure Sockets Layer) avecIBM Cognos Analytics et IBM HTTP Server V9 comme serveur Web, vous devez configurer SSL entre les modules de serveur Web WAS et le serveur d'application Cognos Analytics en récupérant le certificat IBM Cognos et en l'ajoutant au magasin de clés de confiance des modules de serveur Web WAS.

Si vous utilisez SSL sur IBM HTTP Server V9, configurez votre environnement selon les indications de l'article «Configuration d'IBM HTTP Server avec SSL», à la page 107.

### Procédure

1. Démarrez le serveur d'application IBM Cognos Analytics configuré pour utiliser SSL.
2. Copiez la section `Server` du fichier *racine_installation_serveur_application_Cognos_Analytics*`/wlp/usr/servers/cognosserver/logs/state/plugin-cfg.xml` dans le fichier `plug-in/config/webserver1/plugin-cfg.xml`. Assurez-vous que le point d'entrée `https` Cognos Analytics est indiqué, comme le montre l'exemple suivant :

   ```
   <Server CloneID="a4949c5e-cb36-40dd-9f43-58702daf7b1a" ConnectTimeout="5"
   ExtendedHandshake="false" LoadBalanceWeight="20" MaxConnections="-1"
   Name="default_node_cognosserver" ServerIOTimeout="900" WaitForContinue="false">
      <Transport Hostname="hostname" Port="xxx" Protocol="https">
      <Property Name="keyring" Value="D:\install\IBM\WebSphere\Plugins\config\
            webserver1\plugin-key.kdb"/>
      <Property Name="stashfile" Value="D:\install\IBM\WebSphere\Plugins\config\
            webserver1\plugin-key.sth"/>
      </Transport>
   </Server>
   ```

3. Dans le fichier `Plug-in/config/webserver1/plugin-cfg.xml` ajoutez l'attribut suivant à la section `Config` :

   ```
   AutoSecurity="false"
   ```

4. Obtenez le certificat IBM Cognos par l'un des moyens suivants :
   a. Accédez au répertoire Cognos Analytics *racine_installation_serveur_application*`/bin`.
   b. Récupérez le certificat en saisissant une commande qui correspond à votre système d'exploitation.

      Sous UNIX ou Linux, saisissez :

      ```
      ThirdPartyCertificateTool.sh -E -T -r destination file -p NoPassWordSet
      ```

      Sous Windows, saisissez :

      ```
      ThirdPartyCertificateTool.bat -E -T -r destination file -p NoPassWordSet
      ```

5. Copiez le fichier `.cert`, par exemple `ca-host1.cert`, généré à l'étape 4, dans l'hôte des modules de serveur Web WAS.
6. Ajoutez le fichier Cognos Analytics `.cert` dans le magasin de clés de confiance des modules de serveur Web WAS `plugin-key.kdb`. Si le fichier `plugin-key.kdb` n'existe pas, créez-en un comme décrit à l'étape 7.

   Vous pouvez utilisez différentes méthodes pour ajouter le fichier `.cert` au magasin de clés. Les étapes suivantes décrivent comment procéder par le biais de l'outil `gskcapicmd`, livré avec IHS V9.
   a. Accédez au dossier racine IHS9.
   b. Saisissez une commande correspondant à votre système d'exploitation.

      Sous UNIX ou Linux, saisissez :

```
bin/gskcapicmd -cert -add -db WAS_Plugin_root/config/webserver1/plugin-key.kdb
-stashed -label ca-host1 -file ca-host1.cert
```

Sous Windows, saisissez :

```
bin\gskcapicmd.bat -cert -add -db WAS_Plugin_root\config\webserver1\plugin-key.kdb
-stashed -label ca-host1 -file ca-host1.cert
```

Vous trouverez des informations sur les autres méthodes d'ajout de fichiers certificats au magasin de clés dans l'IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0).

7. Créez un magasin de clés vide pour les modules de serveur Web WAS :
   a. Accédez au dossier racine IHS9.
   b. Saisissez une commande correspondant à votre système d'exploitation.

      Sous UNIX ou Linux, saisissez :

      ```
      bin/gskcapicmd -keydb -create -db WAS_Plugin_root/config/webserver1
        /plugin-key.kdb -pw xxx -stash
      ```

      Sous Windows, saisissez :

      ```
      bin\gskcapicmd.bat -keydb -create -db WAS_Plugin_root\config\webserver1
         \plugin-key.kdb -pw xxx -stash
      ```

## Génération de plugin-cfg.xml pour les serveurs Cognos Analytics

Dans un environnement WebSphere Application Server, le fichier `plugin-cfg.xml` contient des informations de configuration, qui déterminent la façon dont le module de serveur Web transfère les requêtes.

**Conseil :** La procédure suivante ne s'applique pas aux serveurs IBM Cognos Analytics qui exécutent le service Content Manager.

### Procédure

1. Accédez à l'emplacement d'installation du serveur d'application Cognos Analytics.
2. Ouvrez le fichier *racine_installation_serveur_applicaton_ca*`/wlp/usr/servers/cognosserver/server.xml`, puis ajoutez-y le paramètre suivant :

   ```
   <pluginConfiguration pluginInstallRoot="racine_installation_module_serveur_Web_WAS"
   webserverPort="port_IHS9"/>
   ```

   Par exemple :

   ```
   <pluginConfiguration pluginInstallRoot="/opt/IHS90Plugin" webserverPort="8080"/>
   ```

3. Configurez et démarrez le serveur d'application Cognos Analytics.

   Une fois le serveur démarré, un fichier nommé `plugin-cfg.xml` est généré dans le répertoire *racine_installation_serveur_applicaton*`/wlp/usr/servers/cognosserver/logs/state` de Cognos Analytics.
4. Ouvrez le fichier `plugin-cfg.xml`, puis modifiez la section `UriGroup` en supprimant tout sauf les deux éléments suivants :

   ```
   <UriGroup Name="default_host_cognosserver_default_node_Cluster_URIs">
       <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
           Name="/bi/*"/>
       <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
           Name="/bi/v1/*"/>
   </UriGroup>
   ```

   **Conseil :** La deuxième entrée d'URL n'existe pas dans le fichier. Il vous faut l'ajouter.
5. Sauvegardez le fichier `plugin-cfg.xml`.

Vous venez de configurer un serveur d'application Cognos Analytics pour le cluster de serveurs (ServerCluster).

6. Pour ajouter un nouveau serveur d'application Cognos Analytics au cluster de serveurs (ServerCluster), procédez comme suit :
   a. Depuis le répertoire *racine_installation_serveur_application*/wlp/usr/servers/cognosserver/logs/state de Cognos Analytics, ouvrez le fichier plugin-cfg.xml. Copiez l'élément Server de la section ServerCluster. Par exemple, copiez l'élément Server suivant :

      ```
      <Server CloneID="081cd7c5-bb6c-4a93-a074-33fa07e587f3" ConnectTimeout="5"
      ExtendedHandshake="false" LoadBalanceWeight="20" MaxConnections="-1"
      Name="default_node_cognosserver" ServerIOTimeout="900" WaitForContinue="false">
      <Transport Hostname="caserverhost" Port="9300" Protocol="http"/>
      </Server>
      ```

   b. Collez l'élément Server dans la section ServerCluster du fichier plugin-cfg.xml généré à l'étape 4. Assurez-vous que le noeud final indiqué dans l'élément Server est accessible depuis votre hôte de serveur Web.
   c. Changez le nom du serveur en modifiant la valeur de l'attribut Name. Assurez-vous que le nom diffère des autres serveurs du cluster ServerCluster. Par exemple, remplacez la valeur default_node_cognosserver par default_node_cognosserver_1.
   d. Ajoutez le nouveau serveur à la section PrimaryServers, comme indiqué ci-dessous :

      ```
      <PrimaryServers>
          <Server Name="default_node_cognosserver"/>
          <Server Name="default_node_cognosserver_1"/>
      </PrimaryServers>
      ```

   e. Sauvegardez le fichier plugin-cfg.xml. Le nouveau serveur est ajouté à ServerCluster.
7. Pour ajouter plus de serveurs, reprenez l'étape 6.

### Que faire ensuite

Pour plus d'informations sur la fusion de fichiers plugin-cfg.xml de plusieurs serveurs autonomes WebSphere Liberty Profile, voir cet article (www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/twsv_merge_configfiles.html).

## Configuration de WebDAV sur IBM HTTP Server ou Apache HTTP Server

Pour afficher et parcourir les images dans Reporting, configurez WebDAV (Web Distributed Authoring and Versioning) sur le serveur Web. Les auteurs du rapport peuvent parcourir les images à inclure dans les rapports comme ils parcourent un système de fichiers. Sur IBM HTTP Server ou Apache HTTP Server, vous devez ajouter des directives au fichier de configuration du serveur, puis configurer l'accès au répertoire.

### Procédure

1. Dans le répertoire *emplacement_serveur_web*/conf, ouvrez le fichier httpd.conf dans un éditeur de texte.
2. Supprimez la mise en commentaire des directives qui chargent modules/mod_dav.so et modules/mod_dav_fs.so.

   ```
   LoadModule dav_module modules/mod_dav.so
   LoadModule dav_fs_module modules/mod_dav_fs.so
   ```

3. Indiquez un emplacement pour la directive DAVLockDB.
   Par exemple :
   DAVLockDB "*emplacement_serveur_Web*/var/DavLock"
   Vérifiez que le répertoire existe.
4. Créez un alias pour le répertoire dans lequel les images sont stockées.
5. Ajoutez Dav On aux informations <Directory> de l'alias.
   Par exemple :

```
Alias /images "chemin/shared_images"

<Directory "chemin/shared_images">
   Dav On
   Options Indexes MultiViews
   AllowOverride None
   Order allow,deny
   Allow from all
</Directory>
```

6. Enregistrez le fichier.
7. Redémarrez votre serveur Web.

### Résultats

Une fois WebDAV activé, les utilisateurs de Reporting peuvent ajouter des images à leurs rapports. Lorsque les utilisateurs cliquent sur **Parcourir** dans le navigateur d'images, l'emplacement d'exploration par défaut est http://*nom_serveur*/ibmcognos/bi/samples/images. Si vous avez créé un autre emplacement, les utilisateurs peuvent indiquer cet emplacement.

## Configuration d'IBM HTTP Server avec SSL

Si vous utilisez SSL (Secure Sockets Layer) sur IBM HTTP Server, vous devez modifier les valeurs de l'**URI de la passerelle** dans IBM Cognos Configuration pour pouvoir accéder au portail.

Pour activer le protocole SSL sur votre serveur Web, vous devez obtenir un certificat du serveur Web signé par une autorité de certification, puis l'installer sur le serveur Web. Pour en savoir davantage sur l'utilisation des certificats dans votre serveur Web, reportez-vous à sa documentation. Ces certificats ne sont pas fournis avec les produits IBM Cognos.

Pour permettre aux utilisateurs d'accéder au portail IBM Cognos à l'aide de SSL, vous devez modifier les valeurs de l'**URI de la passerelle** dans IBM Cognos Configuration pour tous les ordinateurs sur lesquels les composants du groupe des serveurs d'application et Framework Manager sont installés.

### Avant de commencer

IBM HTTP Server nécessite qu'IBM Global Security Kit (GSKit) soit installé. Pour plus d'informations sur les versions prises en charge de GSKit sur IBM HTTP Server, voir Global Security Kit (GSKit) supported versions for releases of IBM HTTP Server (www.ibm.com/support/docview.wss?rs=177&context=SSEQTJ&uid=swg21173214) sur le portail de support IBM.

## Procédure

1. Sur chaque ordinateur sur lequel les composants du groupe des serveurs d'applications ou Framework Manager sont installés, démarrez IBM Cognos Configuration.
2. Sous **Configuration locale**, cliquez sur **Environnement**, puis remplacez la valeur `http` de l'**URI de la passerelle** par `https`.
3. Dans la valeur de l'**URI de la passerelle**, remplacez le numéro du port par celui du port SSL défini pour le serveur Web. Par exemple, le numéro de port par défaut pour les connexions SSL est habituellement 443.
4. Sur chaque ordinateur où les composants du groupe de serveurs d'applications ou Framework Manager sont installés, accédez au répertoire *emplacement_installation*/bin, et importez tous les certificats composant la chaîne d'approbation, en commençant par le certificat racine de l'autorité de certification, dans le fichier de clés certifiées d'IBM Cognos.

   Importez les certificats en saisissant la commande suivante :

   Sur UNIX ou LINUX, tapez :

   `ThirdPartyCertificateTool.sh -T -i -r chemin/nom_fichier_certificat -p mot_de_passe`

   Sur Windows, tapez :

   `ThirdPartyCertificateTool.bat -T -i -r chemin\nom_fichier_certificat -D emplacement_installation\configuration\certs -p mot_de_passe`

   **Remarque :** Si le mot de passe n'est pas défini, le mot de passe par défaut est NoPassWordSet.
5. Saisissez la commande suivante depuis le répertoire de serveur Web *racine_installation_ihs*/bin : *racine_installation_ihs*/bin/*nom_script*

   Où *racine_installation_ihs* désigne le répertoire dans lequel IBM HTTP Server est installé, et *nom_script* désigne `gskver.bat` pour Microsoft Windows ou `gskver.sh` pour UNIX ou Linux. Les bibliothèques partagées GSKit et les informations de version s'affichent. Vérifiez que la version affichée est la version minimale prise en charge, comme indiqué dans le document de support mentionné dans la section *Avant de commencer* de cette procédure.
6. Démarrez l'utilitaire iKeyman, en saisissant la commande suivante : *racine_installation_ihs*/bin/*nom_script*

   Où *racine_installation_ihs* désigne le répertoire dans lequel IBM HTTP Server est installé, et *nom_script* désigne `ikeyman.bat` pour Microsoft Windows ou `ikeyman.sh` pour UNIX ou Linux.
7. Dans le menu, sélectionnez **Fichier de base de données de clés** > **Nouveau**.
8. Entrez les valeurs suivantes et cliquez sur le bouton **OK** :

   **Nom du fichier**
   Nom du fichier de la base de données de clés. La valeur par défaut est `key.kdb`.

   **Emplacement**
   Emplacement où enregistrer le fichier `key.kdb`. La valeur par défaut est *racine_installation_ihs*/bin.
9. Dans le fenêtre Password Prompt, saisissez un mot de passe, cochez la case **Stash a password to a file**, puis cliquez sur **OK**. Lorsque vous cochez la case **Stash a password to a file**, le mot de passe est chiffré et enregistré en tant que fichier `.sth` dans le même répertoire que le fichier de la base de données de clés.

**Remarque :** Pour savoir comment créer une demande de certificat à envoyer à une autorité de certification, voir Using iKeyman to create a key database file (www.ibm.com/support/docview.wss?rs=177&context=SSEQTJ &uid=swg21006430).
Un message apparaît pour indiquer la réussite de la procédure.

10. Ouvrez le fichier *racine_installation_ihs*/conf/httpd.conf dans un éditeur de texte.
11. Ajoutez la directive Keyfile avec le chemin d'accès à votre fichier de la base de données de clés. Insérez-la après la section VirtualHost du fichier. Par exemple :

    ```
    <VirtualHost *:443>
    ...
    </VirtualHost>
    KeyFile racine_installation_ihs/key.kdb
    ```
12. Sauvegardez et fermez le fichier httpd.conf.
13. Extrayez le certificat Cognos Analytics vers un fichier. Exécutez la commande suivante depuis le serveur IBM Cognos Analytics dans *installation_ac*/bin.

    *nom_script* -E -T -r *fichier_cert_ca* -p NoPassWordSet

    Où *nom_script* désigne ThirdPartyCertificateTool.bat pour Microsoft Windows ou ThirdPartyCertificateTool.sh pour UNIX ou Linux, et *fichier_cert_ca* est le nom du fichier certificat.
14. Copiez le fichier certificat dans *racine_installation_ihs*/*rép_fichier_bdd_clés* où *racine_installation_ihs* désigne le répertoire où IBM HTTP Server est installé et *rép_fichier_bdd_clés* désigne le répertoire où le fichier de la base de données de clés est enregistré.
15. Dans *racine_installation_ihs*/bin, saisissez la commande suivante :

    *nom_script* -cert -import -db *fichier_cert_ca*
    -pw NoPassWordSet -target key.kdb -target_pw *mdp_fichier_bdd_clés*

    Où *nom_script* désigne gskcapicmd.bat pour Microsoft Windows ou gskcapicmd.sh pour UNIX ou Linux et *mdp_fichier_bdd_clés* désigne le mot de passe pour le fichier de base de données de clés.
16. Démarrez IBM HTTP Server. Saisissez la commande suivante dans racine_installation_ihs/bin :

    *nom_script* -k start

    Où *nom_script* désigne apchectl.bat pour Microsoft Windows ou ./apachectl pour UNIX ou Linux. Sous Microsoft Windows, vous pouvez également démarrer le script en tant que service.
17. Vérifiez qu'IBM HTTP Server s'exécute en saisissant l'URI suivante dans la barre d'adresse d'un navigateur Web :

    https://*nom_hôte_serveur_web*:*port*

    Où *nom_hôte_serveur_web* désigne le nom d'hôte d'IBM HTTP Server et *port* désigne le numéro de port d'IBM HTTP Server.
18. Enregistrez la configuration et redémarrez les services.

## Résultats

Lorsque vous accédez au portail en indiquant https://**nom_serveur**:443/ibmcognos, vous êtes invité à installer un certificat. Pour ne pas recevoir une alerte de sécurité à chaque nouvelle session, installez le certificat dans l'un des magasins de certificats de votre navigateur Web.

# Configuration d'Apache HTTP Server ou d'IBM HTTP Server dans Cognos Analytics 11.0.5+

11.0.5+

Une fois cette procédure effectuée, le serveur peut gérer des demandes pour les fichiers statiques (comme `.js`, `.html` et `.css`), des demandes d'équilibrage de charge à IBM Cognos Analytics, et transférer les demandes SSO par le biais du code passerelle d'IBM Cognos Analytics.

## Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'un des exemples de fichiers de configuration fournis avec IBM Cognos Analytics. Ces fichiers se trouvent dans *emplacement_installation_composant_passerelle*`/cgi-bin/templates`, où *emplacement_installation_composant_passerelle* est le répertoire dans lequel le composant de passerelle est installé. Le tableau suivant décrit les fichiers exemples. Choisissez le fichier qui correspond à votre environnement :

| Environnement | Nom du fichier exemple |
|---|---|
| Apache 2.2 non SSO | cognos_apache22_loadbalance.conf |
| Apache 2.2 SSO | cognos_apache22_loadbalance_SSO.conf |
| Apache 2.4 non SSO | cognos_apache24_loadbalance.conf |
| Apache 2.4 SSO | cognos_apache24_loadbalance_SSO.conf |
| IBM HTTP Server 8.5 non SSO | cognos_IHS85_loadbalance.conf |
| IBM HTTP Server 8.5 SSO | cognos_IHS85_loadbalance_SSO.conf |

## Procédure

1. Copiez l'exemple de fichier de configuration dans *racine_installation_apache_ou_ihs*`/conf` et renommez-le `cognos.conf`.
2. Ouvrez `cognos.conf` dans un éditeur de texte et modifiez la directive `BalancerMember` pour utiliser HTTPS et un nom de domaine complet. Par exemple :

   ```
   <Proxy balancer://mycluster>
    BalancerMember https://ica-host1.domain:9300 route=1
    BalancerMember https://ica-host2.domain:9300 route=2
   </Proxy>
   ```

3. Vérifiez que la section suivante figure dans l'exemple de fichier.

   ```
   # Rewrite Saved-Output and Viewer static references
   RewriteRule ^/ibmcognos/bi/rv/(.*)$ /ibmcognos/rv/$1 [PT,L]
   ```

   Si cette section est absente, ajoutez-la après la section `# Rewrite Event Studio static references`.
4. Trouvez la section `Directory` et assurez-vous qu'elle pointe vers l'emplacement d'installation d'IBM Cognos Analytics.
5. Enregistrez le fichier `cognos.conf`.

# Configuration d'Apache HTTP Server ou d'IBM HTTP Server dans Cognos Analytics 11.0.4

11.0.4

Une fois cette procédure effectuée, le serveur peut gérer des demandes pour les fichiers statiques (comme .js, .html et .css), des demandes d'équilibrage de charge à IBM Cognos Analytics, et transférer les demandes SSO par le biais du code passerelle d'IBM Cognos Analytics.

## Avant de commencer

Une instance de serveur Cognos Analytics au moins doit être configurée et en cours d'exécution. Elle doit être accessible depuis le serveur Web avec une URL similaire à : http://*nom d'hôte du serveur IBM Cognos Analytics*1:9300/bi. Utilisez mod_proxy_balancer pour équilibrer la charge des demandes entre plusieurs instances Cognos Analytics. Pour connaître les options d'équilibrage de charge, voir la documentation Apache.

## Pourquoi et quand exécuter cette tâche

La configuration dans cette tâche configure l'équilibrage de charge des sessions permanentes. Vous pouvez surveiller et configurer l'équilibreur de charge à http://*nom_hôte_serveur_web*/ibmcognos/balancer-manager

L'instruction expires_module ajoute les en-têtes de réponse aux demandes qui indiquent au navigateur la durée pendant laquelle il peut conserver la ressource renvoyée avant de vérifier s'il existe de nouvelles versions. L'instruction deflate_module procède à la compression des ressources avant leur envoi, ce qui économise la bande passante.

Les différences en fonction des plateformes sont indiquées ci-dessous dans comments. Les références à cognos_module dans la configuration ci-après sont requises uniquement si vous configurez le code d'accès unique (SSO). Si SSO n'est pas requis, le module cognos_module n'est pas nécessaire.

## Procédure

1. Dans le répertoire apache/conf, créez un fichier vide nommé cognos.conf.
2. Ouvrez le fichier cognos.conf dans un éditeur de texte.

   Le contenu ci-après s'applique à Apache 2.2 et Cognos Analytics, versions 11.0.4 Apportez les modifications au code, telles qu'indiquées dans les exemples suivants, en fonctions des besoins de votre environnement. Certaines valeurs du code ne sont données qu'à titre d'exemple. Pour plus d'informations sur les directives Apache qui peuvent être utilisées, voir http://httpd.apache.org/docs/2.2/mod/mod_authnz_ldap.html.

```
# cognos.conf for Apache 2.2 and IHS 8
LoadModule headers_module modules/mod_headers.so
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule expires_module modules/mod_expires.so
LoadModule filter_module modules/mod_filter.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule deflate_module modules/mod_deflate.so

# Apache 2.2 UNIX
 LoadModule cognos_module "/opt/IBM/cognos/analytics/cgi-bin/mod2_2_cognos.so"

# Apache 2.2 Windows
 LoadModule cognos_module "c:/IBM/cognos/analytics/cgi-bin/mod2_2_cognos.dll"
```

```
<IfModule mod_expires.c>
    <FilesMatch "\.(jpe?g|png|gif|js|css|json|html|woff2?|template)$">
        ExpiresActive On
        ExpiresDefault "access plus 1 day"
    </FilesMatch>
</IfModule>

 <IfModule mod2_2_cognos.c>
    CGIBinDir "/opt/IBM/cognos/analytics/cgi-bin"
 </IfModule>

<Directory /opt/IBM/cognos/analytics>
    <IfModule mod_deflate>
        AddOutputFilterByType DEFLATE text/html application/json text/css application/javascript
    </IfModule>
    Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

#Set up a cluster for load-balancing
# Include all Cognos Analytics servers that have the Application server components
# installed and configured.
# Important: do not include Cognos Analytics servers that are used to run the
# Content Manager service.
<Proxy balancer://mycluster>
    BalancerMember http://ca-host1:9300 route=1
    BalancerMember http://ca-host2:9300 route=2
    BalancerMember http://ca-host3:9300 route=3
</Proxy>

# UI to monitor/configure load balancer
<Location /ibmcognos/balancer-manager>
    SetHandler balancer-manager
</Location>


# Use ScriptAlias if you plan to use cognos.cgi instead of mod_cognos for SSO
ScriptAlias /ibmcognos/cgi-bin /opt/IBM/cognos/analytics/cgi-bin

Alias /ibmcognos /opt/IBM/cognos/analytics/webcontent

RewriteEngine On

# Send default URL to service
RewriteRule ^/ibmcognos/bi/$ balancer://mycluster/bi/ [P]

# Send login requests and legacy UI's through cognos_module for SSO
RewriteRule ^/ibmcognos/bi/v1/(login|disp)(/.*)?
    /ibmcognos/sso/bi/v1/$1$2 [PT,L]

#Or Send login requests and legacy UI's through cognos.cgi for SSO
RewriteRule ^/ibmcognos/bi/v1/(login|disp)(/.*)?
    /ibmcognos/bi/v1/disp/bi/v1/$1$2 [PT,L]


# Rewrite Event Studio static references
RewriteCond %{HTTP_REFERER} v1/disp [NC]
RewriteRule ^/ibmcognos/bi/(ags|cr1|prompting|ccl|common|skins|ps)/(.*) /ibmcognos/$1/$2 [PT,L]

# Rewrite Saved-Output and Viewer static references
RewriteRule ^/ibmcognos/bi/rv/(.*)$ /ibmcognos/rv/$1 [PT,L]

# Define cognos location
<Location /ibmcognos>
    RequestHeader set X-BI-PATH /ibmcognos/bi/v1
</Location>
```

```
# Route CA REST service requests through proxy with load balancing
<Location /ibmcognos/bi/v1>
    Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e;
    path=/ibmcognos/bi/v1"
    env=BALANCER_ROUTE_CHANGED
    ProxyPass balancer://mycluster/bi/v1 stickysession=ROUTEID
</Location>

# Route login and legacy UI requests through mod_cognos
<Location /ibmcognos/sso>
    SetHandler cognos-handler
    # Add SSO Directives here, for example...
    AuthType basic
    AuthName "LDAP"
    AuthBasicProvider ldap
    AuthLDAPURL "ldap://ldap:389/ou=people, o=example.com?uid?sub?(objectClass=*)"

    Require valid-user
</Location>


# Il ne s'agit que d'un exemple.
# Pour plus d'informations sur les directives Apache qui peuvent être utilisées,
# voir http://httpd.apache.org/docs/2.2/mod/mod_authnz_ldap.html
# Route login and legacy UI requests through cognos.cgi
<Location /ibmcognos/cgi-bin>
    # Add SSO Directives here, for example...
    AuthType basic
    AuthName "LDAP"
    AuthBasicProvider ldap
    AuthLDAPURL "ldap://ldap:389/ou=people, o=example.com?uid?sub?(objectClass=*)"

    Require valid-user
</Location>
```

3. Si vous utilisez IBM HTTP Server 8.5, modifiez la ligne suivante dans `cognos.conf` :

   ```
   LoadModule proxy_balancer_module modules/WebSphereCE/mod_proxy_balancer.so
   ```

4. Enregistrez le fichier `cognos.conf`.
5. Redémarrez le serveur.

## Configuration d'Apache HTTP Server ou IBM HTTP Server dans Cognos Analytics 11.0.3

11.0.0+ 11.0.3

Vous ne pouvez pas utiliser les modules Apache avec la version d'Apache Server 2.2 qui est fournie avec Red Hat Enterprise Linux version 5.3 et ultérieure.

### Avant de commencer

Cette rubrique suppose que vous avez installé un composant de passerelle facultatif, que vous disposez d'un serveur Apache HTTP Server installé et en cours d'exécution, et que vous pouvez administrer des environnements Linux et UNIX.

Lorsque vous utilisez Apache HTTP Server, sachez que les fonctions suivantes sont disponibles dans des versions différentes.

| Fonction | Apache 2.2 | Apache 2.4 |
|---|---|---|
| Equilibrage de charge | Non pris en charge | Oui |
| Module de passerelle | Oui | Non |

| Fonction | Apache 2.2 | Apache 2.4 |
|---|---|---|
| Proxy | Oui | Oui |

Configurez le serveur Web Apache de sorte qu'il accepte un nouveau fichier de configuration qui contiendra tous les paramètres requis par IBM Cognos Analytics.

## Apache 2.2

### Procédure

1. Editez le fichier `cognos.conf` et ajoutez les lignes suivantes :

```
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule cognos_module "<gateway_location>/cgi-bin/mod2_2_cognos.<xx>"

<Location /<alias>/bi>
RequestHeader set X-BI-PATH /alias/bi/v1
 ProxyPass http(s)://<app_server:port>/bi
 ProxyPassReverse http(s)://<app_server:port>/bi
 ProxyPassReverseCookieDomain "." "<domain>"
</Location>

# Aliases for the CA web content
ScriptAlias /<alias>/cgi-bin "<gateway_location>/cgi-bin"
<Directory "<gateway_location>/cgi-bin">
AllowOverride None
Options None
Order allow,deny
Allow from all
</Directory>

Alias /<alias> "<gateway_location>/webcontent"
<Directory "<gateway_location>/webcontent">
Options Indexes MultiViews
AllowOverride None
Order allow,deny
Allow from all
</Directory>

<Location /<alias>/cgi-bin/mod2_2_cognos.<xx>>
       SetHandler cognos-handler
 CGIBinDir "<gateway_location>/cgi-bin/"
       Order allow,deny
       Allow from all
</Location>
```

2. Dans la section ajoutée ci-dessus, remplacez les indicateurs d'emplacement par les valeurs appropriées :
   - *<alias>* : indiquez le nom de votre alias Web. Par exemple, `ibmcognos`
   - *<app_server:port>* : indiquez le nom et le numéro de port d'un serveur d'applications Cognos Analytics. Par exemple, `appserver.ibm.com:9300`
   - *<domain>* : indiquez le domaine dans lequel se trouvent les serveurs. Par exemple, `ibm.com`
   - *<gateway_location>* : indiquez l'emplacement physique d'installation de la passerelle Cognos Analytics. Par exemple, `/opt/ibm/cognos/analytics`
   - *<xx>* : indiquez le suffixe de l'extension en fonction du système d'exploitation sur lequel Apache est installé. Par exemple, `Windows = dll, Unix/Linux = so`
3. Enregistrez le fichier `cognos.conf`.

4. Si vous avez configuré la connexion unique pour IBM Cognos Analytics, appelez-la au moyen de l'URL suivante :

```
http://ICA_Web_Server:80/ibmcognos/cgi-bin/mod2_2_cognos.so?
      b_action=xts.run&m=portal/main.xts&m_redirect=/ibmcognos/bi/
```

## Apache 2.4

### Procédure

1. Editez le fichier cognos.conf et ajoutez les lignes suivantes :

```
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule slotmem_plain_module modules/mod_slotmem_plain.so
LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so

# Header to add a cookie for sticky sessions
Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e; path=/"
    env=BALANCER_ROUTE_CHANGED

# Send everything which goes to BI Services through balanced proxy
#
# Add/Remove the number of BalanceMember lines depending on the server in your # environment
<Proxy balancer://mycluster>
 BalancerMember http://<app_server_x:port> route=1
 BalancerMember http://<app_server_x:port> route=2
 ProxySet stickysession=ROUTEID
</Proxy>

<LocationMatch ^/<alias>/bi/(.*)$>
 RequestHeader set X-BI-PATH /<alias>/bi/v1
 ProxyPass balancer://mycluster/bi/$1
 ProxyPassReverseCookieDomain "." "<domain>"
</LocationMatch>
ProxyRequests off

# Aliases for the CA web content
ScriptAlias /<alias>/cgi-bin "<gateway_location>/cgi-bin"
<Directory "<gateway_location>/webcontent/cgi-bin">
AllowOverride None
Options None
Require all granted
</Directory>

Alias /<alias> "<gateway_location>/webcontent"
<Directory "<gateway_location>/webcontent">
Options Indexes MultiViews
AllowOverride None
Require all granted
</Directory>
```

2. Modifiez les informations suivantes en fonction de votre environnement :
   - *<alias>* : indiquez le nom de votre alias Web. Par exemple, ibmcognos
   - *<app_server_x:port>* - indiquez le nom et le numéro de port d'un serveur d'applications ICA. Par exemple, appserver.ibm.com:9300
   - *<domain>* : indiquez le domaine dans lequel se trouvent les serveurs. Par exemple, ibm.com
   - *<gateway_location>* - indiquez l'emplacement physique d'installation de la passerelle ICA. Par exemple, /opt/ibm/cognos/analytics
3. Pour ajouter ou supprimer des serveurs du groupe de serveurs d'application à partir de la configuration de proxy, ajustez le nombre de lignes BalancerMember de manière appropriée dans la section Proxy.

Ainsi, si vous disposez d'un serveur d'application, il ne doit y avoir qu'une seule entrée.

```
<Proxy balancer://mycluster>
 BalancerMember http://app_server_1:port route=1
 ProxySet stickysession=ROUTEID
</Proxy>
```

Si vous disposez de 4 serveurs d'application, il doit y avoir 4 entrées.

```
<Proxy balancer://mycluster>
 BalancerMember http://app_server_1:port route=1
 BalancerMember http://app_server_2:port route=2
 BalancerMember http://app_server_3:port route=3
 BalancerMember http://app_server_4:port route=4
 ProxySet stickysession=ROUTEID
</Proxy>
```

Le paramètre `route=` détermine l'ordre dans lequel la demande est envoyée.

4. Enregistrez le fichier `cognos.conf`.
5. Redémarrez Apache HTTP Server.
6. En supposant que la connexion unique a été configurée pour IBM Cognos Analytics, vous pouvez appeler cette dernière avec l'URL suivante : `http://ICA_Web_Server:80/ibmcognos/bi/v1/disp?b_action=xts.run&m=portal/main.xts&m_redirect=/ibmcognos/bi/`
7. Sinon, si vous souhaitez retirer la section de redirection de l'URL, procédez comme suit :
   a. Accédez au répertoire analytics/webcontent.
   b. Editez le fichier `default.htm` en modifiant la ligne suivante.

      Modifiez `<meta http-equiv="refresh" content="0; URL=/bi">` en `<meta http-equiv="refresh" content="0; URL=/<alias>/bi">`
   c. Enregistrez `default.htm`.
   d. Faites de même avec `index.htm`.
   e. Testez la connexion avec `http:// ICA_Web_Server:80/ibmcognos/bi/v1/disp` ou `http:// ICA_Web_Server:80/ibmcognos/cgi-bin/mod2_2_cognos.so`

# Configuration de Microsoft Internet Information Services

Cette section vous explique comment configurer Microsoft Internet Information Services (IIS) en tant que votre serveur Web dans IBM Cognos Analytics.

## Configuration de WebDAV sur IIS

Pour afficher et parcourir les images dans Reporting, configurez WebDAV (Web Distributed Authoring and Versioning) sur le serveur Web. Les auteurs du rapport peuvent parcourir les images à inclure dans les rapports comme ils parcourent un système de fichiers. Sur des serveurs Web Microsoft Internet Information Services (IIS), vous devez d'abord activer la fonction WebDAV, puis configurer votre serveur Web pour qu'il accède à l'emplacement de l'image.

### Procédure

1. Dans le **Panneau de configuration** Microsoft Windows, cliquez sur **Programmes** > **Programmes et fonctionnalités**.

   Si vous utilisez Microsoft Windows 8 ou 2012 Server, **Programmes et fonctionnalités** est disponible directement dans le **Panneau de configuration**.
2. Cliquez sur **Activer ou désactiver des fonctionnalités Windows**.
3. Si vous utilisez Microsoft Windows 2008 Server, procédez comme suit :

a. Cliquez sur **Gestionnaire de serveur** > **Rôles** > **Serveur Web (IIS)**.
b. Dans la section **Services de rôle**, sélectionnez **Ajouter des services de rôle**.
c. Sous **Serveur Web** > **Fonctionnalités HTTP communes**, sélectionnez **Publication WebDAV**.
d. Cliquez sur **Suivant**, puis sur **Installer**.

4. Si vous utilisez Microsoft Windows 2012 Server, procédez comme suit :
   a. Dans **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis sur **Suivant**.
   b. Sélectionnez votre serveur et cliquez sur **Suivant**.
   c. Développez **Serveur Web (IIS)** > **Serveur Web** > **Fonctionnalités HTTP communes**, puis sélectionnez **Publication WebDAV**.
   d. Cliquez sur **Suivant** > **Suivant**, puis sur **Installer**.
5. Si vous utilisez Microsoft Windows 7 ou 8, procédez comme suit :
   a. Développez **Internet Information Services** > **Services World Wide Web** > **Fonctionnalités HTTP communes**.
   b. Sélectionnez **Publication WebDAV** et cliquez sur **OK**.
6. Dans la console **Gestionnaire des services Internet (IIS)**, sous **Connexions**, sélectionnez le nom du serveur.
   - Si vous utilisez Microsoft Windows 2012 Server, dans **Gestionnaire de serveur**, sélectionnez **IIS**, cliquez avec le bouton droit de la souris sur le nom de votre serveur, puis cliquez sur **Gestionnaire des services Internet (IIS)**.
   - Si vous utilisez Microsoft Windows 2008 Server, dans **Gestionnaire de serveur**, développez **Rôles** > **Serveur Web (IIS)**, puis cliquez sur **Gestionnaire des services Internet (IIS)**.
   - Si vous utilisez Microsoft Windows 8, dans le **Panneau de configuration**, cliquez sur **Outils d'administration** pour accéder à la console **Gestionnaire des services Internet (IIS)**.
   - Si vous utilisez Microsoft Windows 7, dans le **Panneau de configuration**, cliquez sur **Système et sécurité** > **Outils d'administration** pour accéder à la console **Gestionnaire des services Internet (IIS)**.
7. Sous **Connexions**, développez votre serveur Web, puis **Sites** et sélectionnez votre site Web. Par exemple, sélectionnez **Site Web par défaut**.
8. Cliquez deux fois sur **Règles de création WebDAV**.
9. Cliquez sur **Activer WebDAV**.
10. Cliquez sur **Paramètres WebDAV**.
11. Si l'accès anonyme est activé, sélectionnez **True** pour **Autoriser les requêtes de propriété anonymes** et cliquez sur **Appliquer**.
12. Sélectionnez le répertoire ou le répertoire virtuel auquel vous souhaitez autoriser l'accès à WebDAV.
13. Cliquez deux fois sur **Règles de création WebDAV**.
14. Cliquez sur **Ajouter une règle de création** et ajoutez les règles appropriées pour votre environnement. Si, par exemple, vous avez installé les exemples et que vous souhaitez utiliser le chemin par défaut sous le répertoire virtuel `ibmcognos`, développez `bi/samples`, sélectionnez `images` et ajoutez une règle de création pour les fichiers d'image.
15. Cliquez avec le bouton droit de la souris sur le répertoire ou le répertoire virtuel dans lequel vous avez ajouté des règles de création et cliquez sur **Editer les droits**.

16. Cliquez sur **Sécurité** et ajoutez les droits d'accès appropriés. Par exemple, si vous autorisez l'accès anonyme à votre serveur Web, ajoutez des droits d'accès pour l'utilisateur à accès anonyme. Vous pouvez trouver cet utilisateur en sélectionnant le site Web, en cliquant deux fois sur **Authentification** et en affichant les propriétés pour les utilisateurs affichés.

### Résultats

Une fois WebDAV activé, les utilisateurs de Reporting peuvent ajouter des images à leurs rapports. Lorsque les utilisateurs cliquent sur **Parcourir** dans le navigateur d'images, l'emplacement d'exploration par défaut est `http://nom_serveur/ibmcognos/bi/samples/images`. Si vous avez créé un autre emplacement, les utilisateurs peuvent indiquer cet emplacement.

## Configuration d'IIS avec SSL

Pour configurer Microsoft Internet Information Services (IIS) avec SSL (Secure Sockets Layer), vous extrayez le certificat IBM Cognos, puis vous l'ajoutez au magasin de clés de confiance sur IIS.

### Procédure

1. Accédez au répertoire *emplacement_installation*/bin.
2. Extrayez le certificat IBM Cognos en saisissant la commande suivante :

   Sur les systèmes d'exploitation UNIX ou Linux, saisissez
   `ThirdPartyCertificateTool.sh -E -T -r destination_file -p NoPassWordSet`

   Sur les systèmes d'exploitation Microsoft, saisissez
   `ThirdPartyCertificateTool.bat -E -T -r destination_file -p NoPassWordSet`
3. Effectuez la procédure de Copie du certificat de l'autorité de certification vers les serveurs IBM Cognos.
4. Importez le certificat dans le magasin de clés de confiance sur IIS. Pour plus d'informations sur la façon d'importer le certificat dans le magasin de clés de confiance sur IIS, voir Ajout de certificats au magasin d'autorités de certification racine digne de confiance pour un ordinateur local.

## Configuration d'IIS dans Cognos Analytics 11.0.4 et les versions ultérieures

**Remarque :**

Il s'agit d'un document évolutif qui sera mis à jour si besoin.

**Remarque :**

Le script IIS automatisé est disponible ici.

Cette rubrique décrit la configuration d'ISS (Microsoft Internet Information Services) nécessaire à la prise en charge d'IBM Cognos Analytics. IIS est alors configuré pour servir le contenu statique (tel que `.js`, `.html` et `.css`) directement à partir d'IIS tout en transmettant les demandes REST et d'autres serveurs aux serveurs Cognos Analytics d'arrière-plan.

### Procédure

1. Installez l'extension IIS Application Request Routing.

a. Installez l'extension ARR (Application Request Routing) pour IIS en accédant à l'URL suivante : http://www.iis.net/downloads/microsoft/application-request-routing
b. Lorsque vous arrivez sur la page Web Microsoft, cliquez sur le bouton vert "Install this extension". Suivez les instructions pour télécharger et exécuter l'extension ARR.
c. Pour vérifier que l'extension ARR a été installée avec succès, lancez IIS Manager à partir du menu Windows **Démarrer\Administrative Tools**. Une fois IIS Manager lancé, cliquez sur le nom du serveur situé en haut à gauche de l'écran pour afficher les fonctions disponibles. Dans le panneau IIS du milieu, la fonction **URL Rewrite** doit maintenant être visible ; elle est installée avec ARR.

2. Créez un pool d'applications dédié. Par exemple, `CAPool`.
   a. Cliquez avec le bouton droit de la souris sur **Pools d'applications**. Cliquez sur **Ajouter un pool d'applications**.
3. Le cas échéant, créez un parc de serveurs pour assurer l'équilibrage de charge et la reprise des demandes de service Cognos Analytics. Incluez tous les serveurs Cognos Analytics dont les composants de serveur d'applications sont installés et configurés.
   a. Cliquez sur **Server Farms** à l'aide du bouton droit de la souris dans l'arborescence de gauche et sélectionnez **Create Server Farm**.
   b. Attribuez un nom au nouveau parc de serveurs. Par exemple, `ca_servers`.
   c. Pour chaque serveur Cognos Analytics, procédez comme suit :
      - Entrez l'adresse de serveur. Par exemple, `ca-host1`.
      - Cliquez sur **Paramètres avancés** et développez **applicationRequestRouting**. Définissez `httpPort` ou `httpsPort` (si vous utilisez HTTPS). Par exemple, `9300`.
   d. Cliquez sur **Terminer**.
   e. Cliquez sur **Non** lorsque vous y êtes invité pour autoriser IIS Manager à créer une règle de réécriture.
   f. Sélectionnez votre parc de serveurs dans l'arborescence située à gauche et cliquez deux fois sur **Server Affinity**.
   g. Cochez la case **Client Affinity**.
   h. Cliquez sur **Appliquer**.
   i. Sélectionnez votre parc de serveurs dans l'arborescence située à gauche et cliquez deux fois sur **Caching Affinity**.
   j. Remplacez **Query String Support** par **Include Query String**.
   k. Cliquez sur **Appliquer**.
   l. Sélectionnez votre parc de serveurs dans l'arborescence située à gauche et cliquez deux fois sur **Health Test**.
   m. Dans la section **URL Test**, entrez l'URL suivante : `http://ca_servers/bi/v1/ping`
   n. Cliquez sur **Appliquer**.
   o. Sélectionnez votre parc de serveurs dans l'arborescence située à gauche et cliquez deux fois sur **Proxy**.
   p. Dans la zone **Time-out (seconds)**, remplacez la valeur par `120`.
   q. Cliquez sur **Appliquer**.
4. Cliquez avec le bouton droit de la souris sur **Site Web par défaut**, puis cliquez sur **Add Application**.

- L'alias est ibmcognos.
- Le pool d'applications est celui qui a été créé à l'étape 1.
- Le chemin physique est *emplacement_installation*\webcontent

a. Activez l'expiration du contenu Web
   1) Sélectionnez ibmcognos et cliquez deux fois sur **HTTP Response Headers**.
   2) Cliquez sur **Set Common Headers**.
   3) Cochez la case **Expire Web Content** et définissez l'expiration appropriée.

b. Sélectionnez ibmcognos et cliquez deux fois sur **Types MIME**.

   **Important :** Ajoutez les types mime ci-après à votre configuration IIS s'ils ne sont pas déjà présents.
   - .svg : image/svg+xml
   - .woff : application/x-font-woff
   - .json : application/json
   - .woff2 : font/woff2
   - .template : text/html
   - .txt : text/plain

5. Si vous configurez le code d'accès unique entre IIS et Cognos, cliquez avec le bouton droit de la souris sur ibmcognos et sélectionnez **Add Application**.
   - Pour **Alias** spécifiez sso.
   - Le **pool d'applications** est celui que vous avez créé à l'étape 1.
   - Le **chemin physique** est *emplacement_installation*\cgi-bin

   a. Sélectionnez **sso** et cliquez deux fois sur **Handler Mappings**.
   b. Cliquez sur **Add Module Mapping** dans la sous-fenêtre **Actions** de droite.
      - Le chemin des demandes est cisapi.
      - Le module est **IsapiModule**.
      - L'exécutable est emplacement_installation\cgi-bin\cognosisapi.dll
      - Le nom est Connexion unique Cognos.
      - Cliquez sur **Request Restrictions** et assurez-vous que la case **Invoke Handler** est désélectionnée.
      - Cliquez à deux reprises sur **OK**.
      - Dans la boîte de dialogue **Edit Script Map**, cliquez sur **Yes**.
      - Sélectionnez **sso** et cliquez deux fois sur **Modules**. Si WebDAVModule apparaît dans la liste, supprimez-le.
6. Créez des règles d'URL de réécriture pour mapper les demandes aux gestionnaires corrects.
   a. Cliquez sur le répertoire bi, sous **ibmcognos**.
   b. Cliquez deux fois sur **URL Rewrite**.
   c. Ajoutez une variable de serveur pour identifier l'emplacement de Cognos Analytics en cliquant sur **View Server Variables**.
      - Cliquez sur le bouton **Ajouter**.
      - Attribuez le nom HTTP_X_BI_PATH à la variable.
      - Cliquez sur **Back to Rules**.
      - Cliquez sur le bouton **Ajouter**.
      - Attribuez le nom HTTP_X_WEBCONTENTROOT à la variable
      - Cliquez sur **Back to Rules**.

- Cliquez sur le bouton **Ajouter**.
- Attribuez le nom `HTTP_X_FORWARDED_HOST` à la variable.
- Cliquez sur **Back to Rules**.

d. Ajoutez une règle pour transmettre l'emplacement de Cognos Analytics aux machines `ca-host` en cliquant sur **Add Rules** > **Inbound Rules** > **Blank Rule**.
   - Le nom est `En-tête`se.
   - Le modèle est `(.*)`
   - Le type d'action est **none**.
   - Développez **Server variables** et
     – Cliquez sur **Ajouter**. Sélectionnez `HTTP_X_BI_PATH` et affectez-lui la valeur `/ibmcognos/bi/v1`.
     – Cliquez sur **Ajouter**. Sélectionnez `HTTP_X_FORWARDED_HOST` et affectez-lui la valeur `{HTTP_HOST}`.
     – Cliquez sur **Ajouter**. Sélectionnez `HTTP_X_WEBCONTENTROOT` et affectez-lui la valeur `/ibmcognos`.
   - Désélectionnez **Stop processing of subsequent rules**.
   - Cliquez sur **Apply** et **Back to Rules**.

e. Si vous avez configuré l'application SSO à une étape précédente, ajoutez des règles pour mapper les demandes de service d'interface utilisateur existante et de connexion au gestionnaire SSO.
   1) Cliquez sur **Add Rules** > **Inbound Rules** > **Blank Rule**.
      - Le nom est `Connexion unique`.
      - Le modèle est `v1/login$`
      - Le type d'action est **Rewrite**.
      - L'URL de réécriture est `/ibmcognos/sso/cisapi/bi/v1/login`
      - Sélectionnez **Stop processing of subsequent rules**.
      - Cliquez sur **Apply** et **Back to Rules**.
   2) Cliquez sur **Add Rules** > **Inbound Rules** > **Blank Rule**.
      - Le nom est `Connexion unique existante`.
      - Le modèle est `(v1/disp(/.*)?)`
      - Le type d'action est **Rewrite**.
      - L'URL de réécriture est `/ibmcognos/sso/cisapi/bi/{R:1}`
      - Sélectionnez **Stop processing of subsequent rules**.
      - Cliquez sur **Apply** et **Back to Rules**.

f. Ajoutez une règle pour mapper les demandes de service REST de Cognos Analytics aux serveurs Cognos Analytics d'arrière-plan.
   1) Cliquez sur **Add Rules** > **Inbound and Outbound Rules** > **Reverse Proxy**.
      - Si les proxys ne sont pas déjà activés, vous êtes invité à le faire. Cliquez sur **OK**.
      - Le nom du serveur est `ca-host:9300/bi`

        ou si vous avez configuré un parc de serveurs, `http://ca_servers/bi`

      Sélectionnez la nouvelle règle et cliquez sur **Editer**.
      - Le modèle est `(^$)|(^v1(/.*)?)|(^[^/]+\.jsp)`
      - Le type d'action est **Rewrite**.
      - L'URL de réécriture est `http://ca-host:9300/bi/{R:0}`

ou, si vous avez configuré un parc de serveurs, `http://ca_servers/bi/{R:0}`
- Sélectionnez **Stop processing of subsequent rules**.
- Cliquez sur **Apply** et **Back to Rules**.

2) Cliquez sur **Add Rules** > **Inbound Rules** > **Blank Rule**.
   - Le nom est `Event Studio`.
   - Le modèle est `^(ags|cr1|prompting|ccl|common|skins|ps)/(.*)`
   - Ouvrez la section **Conditions**.
   - Modifiez le **Logical Grouping** en **Match Any**
   - Cliquez sur le bouton **Add**.
     - **Condition input** est `{HTTP_REFERER}`
     - **Check if input string** est `Matches the Pattern`
     - Le modèle est `v1/disp`
     - Cochez la case **Ignore case**.
   - Cliquez sur **Add**
     - **Condition input** est `{HTTP_REFERER}`
     - **Check if input string** est `Matches the Pattern`
     - Le modèle est `(ags|cr1|prompting|ccl|common|skins|ps)/(.*)\.css`
     - Cochez la case **Ignore case**.
   - Cliquez sur le bouton **Add**.
     - **Condition input** est `{HTTP_REFERER}`
     - **Check if input string** est `Matches the Pattern`
     - Le modèle est `pat/rsapp.htm`
     - Cochez la case **Ignore case**.
   - Le type d'action est **Rewrite**.
   - L'URL de réécriture est `/ibmcognos/{R:0}`
   - Sélectionnez **Stop processing of subsequent rules**.
   - Cliquez sur **Apply** et **Back to Rules**.

3) Cliquez sur **Add Rules** > **Inbound Rules** > **Blank Rule**
   - Le nom est `Visualiseur de rapports`
   - Le modèle est `^rv/(.*)`
   - Le type d'action est **Rewrite**.
   - L'URL de réécriture est `/ibmcognos/{R:0}`
   - Sélectionnez **Stop processing of subsequent rules**.
   - Cliquez sur **Apply** et **Back to Rules**.

7. Ajustez les limites de taille des demandes.
   a. Sélectionnez le répertoire `bi` sous l'application **ibmcognos** créée précédemment.
   b. Cliquez deux fois sur **Filtrage des demandes**.
   c. Cliquez sur **Modifier les paramètres de fonction** dans le panneau de droite.
      - Définissez **Maximum URL length (bytes)** sur `8192`.
      - Définissez **Maximum query string (bytes)** sur `8192`.
      - Cliquez sur le bouton **OK**.
   d. Cliquez deux fois sur **Filtrage des demandes**.

e. Sélectionnez l'onglet **En-têtes** et cliquez sur **Ajouter un en-tête**.
f. Dans l'**encadré d'en-tête**, entrez le nom de zone d'en-tête comme `Référent`.
g. Dans l'encadré **Limite de taille**, entrez `8192`.
h. Cliquez sur le bouton **OK**.
i. Répétez le processus pour une zone d'en-tête nommée `Cookie` avec la **Limite de taille** de `4096`.
j. Cliquez sur le bouton **OK**.
k. Cliquez sur le répertoire virtuel **ibmcognos**.
l. Sur l'écran d'**accueil**, dans la section **Gestion**, cliquez deux fois sur **Editeur de configuration**.
m. Dans la liste déroulante **Section**, développez **system.web** et sélectionnez **httpRuntime**.
n. Définissez la propriété **maxQueryStringLength** sur 8192.
o. Appliquez le changement de configuration.

8. Configurez IIS pour autoriser la transmission des 441 erreurs personnalisées qui sont utilisées pour les exceptions récupérables dans CAM. Autrement, IIS peut bloquer ces erreurs et le client verra l'erreur "Réponse non valide de la connexion" en essayant de se connecter.
   a. Cliquez sur le répertoire virtuel `ibmcognos`.
   b. Sur l'écran d'accueil, dans la section **Gestion**, faites un double-clic sur **Editeur de configuration**.
   c. Dans la liste déroulante **Section**, développez **system.webServer** et sélectionnez **httpErrors**.
   d. Définissez la propriété **existingResponse** sur **PassThrough**.
   e. Appliquez le changement de configuration.
9. Si vous avez configuré l'application SSO à une étape précédente, activez l'**Authentification Windows**.
   a. Sélectionnez l'application SSO. Pour le navigateur Microsoft Edge, sélectionnez l'application `ibmcognos`.
   b. Cliquez deux fois sur **Authentification**. Désactivez l'**Authentification anonyme** et activez l'**Authentification Windows**.

   Cognos Analytics devrait maintenant disponible à l'adresse suivante : `http://iis-host/ibmcognos`.

   **Remarque :** Si vous avez configuré un dossier virtuel à plusieurs niveaux au-dessus de l'application ibmcognos, par exemple Site Web par défaut > MonDossierRépertoireVirtuel > ibmcognos, utilisez /MyVirtualDirectoryFolder/ibmcognos au lieu de /ibmcognos dans les règles de réécriture d'URL que vous avez créées à l'étape 6.

## Configuration d'IIS dans Cognos Analytics 11.0.3

Si vous utilisez Microsoft Internet Information Services (IIS) version 7 ou 8, configurez IBM Cognos de sorte que celui-ci utilise la passerelle ISAPI, plutôt que la passerelle CGI par défaut. Cette opération est nécessaire si vous implémentez la connexion unique.

**Remarque :** Cette rubrique est utile dans les versions 11.0.0 - 11.0.3 Pour une méthode plus simple dans la version 11.0.4, voir «Configuration d'IIS dans Cognos Analytics 11.0.4 et les versions ultérieures», à la page 118.

## Avant de commencer

Vous avez installé un composant de passerelle facultatif pour Cognos Analytics.

## Pourquoi et quand exécuter cette tâche

Si vous utilisez Microsoft IIS comme serveur Web et si vous avez l'intention d'exécuter plusieurs produits IBM Cognos Analytics ou plusieurs instances du même produit sur un même ordinateur, vous devez effectuer les étapes suivantes :

1. Installer l'extension IIS Application Request Routing (ARR)
2. Configurer le pool d'applications IIS
3. Configurer l'application et les répertoires virtuels IIS
4. Configurer ISAPI
5. Configurez le proxy inverse

**Important :** Si vous utilisez la version 32 bits de la passerelle ISAPI, vous devez activer l'application 32 bits pour le pool d'applications utilisé pour la passerelle IBM Cognos. Depuis le gestionnaire Internet Information Services (IIS), sélectionnez le pool d'applications utilisé pour IBM Cognos et cliquez sur **Paramètres avancés**. Remplacez la valeur définie pour **Enable 32-Bit Applications** par **True**.

## Procédure

1. Installez l'extension IIS Application Request Routing.
   a. Installez l'extension ARR (Application Request Routing) pour IIS en accédant à l'URL suivante : http://www.iis.net/downloads/microsoft/application-request-routing
   b. Lorsque vous arrivez sur la page Web Microsoft, cliquez sur le bouton vert "Install this extension". Suivez les instructions pour télécharger et exécuter l'extension ARR.
   c. Pour vérifier que l'extension ARR a été installée avec succès, lancez IIS Manager à partir du menu Windows **Démarrer\Administrative Tools**. Une fois IIS Manager lancé, cliquez sur le nom du serveur situé en haut à gauche de l'écran pour afficher les fonctions disponibles. Dans le panneau IIS du milieu, la fonction **URL Rewrite** doit maintenant être visible ; elle est installée avec ARR.
2. Configurez le pool d'applications IIS.
   a. Ouvrez Internet Information Services Manager en cliquant sur **Démarrer\Administrative Tools\Internet Information Services (IIS) Manager**.
   b. Développez le serveur **<nom du serveur>** situé sous la page de démarrage, puis cliquez sur **Application Pools**.
   c. Cliquez sur **Add Application Pool...** dans le panneau **Actions**.
   d. Fournissez les détails requis dans la boîte de dialogue **New Application Pool**. Dans la zone **Name**, indiquez un nom comme IBM Cognos Analytics pour le nouveau pool d'applications. Laissez les zones **.Net Framework version** et **Managed pipeline mode** définies sur leurs valeurs par défaut. Cliquez sur **OK** pour créer le pool d'applications.
3. Configurez l'application et les répertoires virtuels IIS.

   IIS sert son contenu aux clients en exposant une arborescence virtuelle. Ce répertoire virtuel détermine l'élément de chemin (ou alias) à employer dans l'URL juste après le nom d'hôte ou l'adresse du serveur Web. Dans cet exemple,

l'alias est ibmcognos. L'application IIS pour cgi-bin mappe les modules de passerelle d'IBM Cognos Analytics au pool d'applications créé précédemment.

a. Dans le panneau de gauche de l'explorateur IIS Manager, développez **Sites** et **Default Web Site**.
b. Cliquez à l'aide du bouton droit de la souris sur **Default Web Site** et sélectionnez **Add Virtual Directory**.
c. Indiquez les détails demandés dans la boîte de dialogue **Add Virtual Directory**, puis cliquez sur **OK**.

   Dans la zone **Alias**, indiquez un nom pour le répertoire virtuel, comme ibmcognos. Le nom de répertoire virtuel ibmcognos est utilisé dans le reste de cette rubrique.

   Dans la zone **Physical path**, indiquez l'emplacement du sous-répertoire webcontent dans l'installation de la passerelle IBM Cognos Analytics. Si nécessaire, accédez au répertoire.
d. Dans le panneau de gauche de l'explorateur IIS Manager, repérez le répertoire virtuel créé précédemment.
e. Cliquez à l'aide du bouton droit de la souris sur le répertoire virtuel et sélectionnez **Add Application...**
f. Indiquez les détails demandés dans la boîte de dialogue **Add Application**, puis cliquez sur **OK**.
   - Dans la zone **Alias**, indiquez la valeur cgi-bin.
   - Dans la zone **Physical path**, indiquez l'emplacement du sous-répertoire cgi-bin dans l'installation de la passerelle IBM Cognos Analytics. Si nécessaire, accédez au répertoire.
   - Dans la zone **Application pool**, sélectionnez le pool d'applications créé à l'étape 3, Configurez le pool d'applications IIS, en cliquant sur le bouton **Select...**

4. Configurer ISAPI

   IBM Cognos Analytics propose deux implémentations de modules de passerelle à utiliser avec IIS : l'interface ISAPI (Internet Server Application Programming Interface) et l'interface CGI (Common Gateway Interface). Etant donné qu'il est recommandé d'employer ISAPI avec IIS en raison de meilleures performances et allocation des ressources via l'interface CGI, cette section décrit uniquement la configuration du module ISAPI.

   Deux étapes sont nécessaires au fonctionnement du module ISAPI. Vous devez tout d'abord configurer un mappage de module qui achemine les demandes appelant cognosisapi.dll à l'exécutable. Vous devez ensuite ajouter le module en tant qu'extension autorisée pour qu'IIS ne bloque pas son exécution.

   a. Sélectionnez l'application **cgi-bin** dans l'arborescence **Default Web Site\ibmcognos** dans le panneau de gauche d'IIS Manager, puis sélectionnez **Features View** dans la barre inférieure du panneau du milieu.
   b. Cliquez deux fois sur **Handler Mappings** dans le panneau du milieu. La liste des mappages des gestionnaires pour cette application s'affiche.
   c. Dans le panneau **Actions** situé en haut à droite, cliquez sur **Add Module Mapping...** pour ajouter le mappage ISAPI.
   d. Indiquez les détails demandés dans la boîte de dialogue **Add Module Mapping**, puis cliquez sur **OK**.
      - Dans la zone **Request path**, indiquez la valeur cognosisapi.dll. Il s'agit d'une valeur obligatoire qui ne peut pas être modifiée.
      - Dans la zone **Module**, sélectionnez **IsapiModule** dans la liste déroulante.

- Dans la zone **Executable (optional)**, indiquez le chemin de `cognosisapi.dll` dans l'installation d'IBM Cognos Gateway. Il s'agit du fichier *`emplacement_installation`*`/cgi-bin`, où *emplacement_installation* représente le répertoire d'installation d'IBM Cognos BI. Dans cet exemple, le répertoire est : `D:\Apps\IBM\Cognos\Analytics\cgi-bin`.
- Dans la zone **Name**, indiquez le nom de ce module. Par exemple, `IBMCOGNOS-ISAPI`

e. Lorsque la boîte de dialogue apparaît pour confirmer que cette nouvelle extension ISAPI doit être autorisée, cliquez sur **Yes**.

   De retour sur l'écran Handler Mappings, le gestionnaire nouvellement ajouté apparaît dans la section **Enabled**. Dans cet exemple, le gestionnaire est nommé `IBMCOGNOS-ISAPI`.

5. Configurez le proxy inverse

   Cette procédure indique les étapes requises pour configurer le proxy inverse afin d'autoriser IIS à réécrire les demandes de passerelle et à les transmettre au groupe de serveurs d'application. Ces étapes supposent l'existence d'une architecture à deux serveurs, dans laquelle la passerelle IBM Cognos Analytics est installée dans `Server1_Gateway` et l'application IBM Cognos Analytics est installée dans `Server2_Application`.

   a. Sur le serveur `Server1_Gateway`, lancez IIS Manager et sélectionnez le dossier "**bi**" dans le répertoire virtuel `ibmcognos` configuré précédemment.

   b. Dans la vue des fonctions, démarrez la fonction **URL Rewrite**.

   c. Dans le panneau **Actions**, cliquez sur **Add Rule(s)**, puis sélectionnez **Reverse Proxy**. Cliquez sur le bouton **OK**.

   d. Dans la boîte de dialogue **Add Reverse Proxy Rule**, dans la section **Inbound Rules**, renseignez la zone **Enter the server name or the IP address...** au format suivant : *`<Server2_Application:Port>`*`/bi`. Par exemple, `Server2_Application:9300/bi`

   e. Vérifiez que la case **Enable SSL Offloading** est cochée, puis cliquez sur **OK**.

   f. Dans la page **Rules**, dans le panneau **Action**, cliquez sur **View Server Variables**.

   g. Cliquez sur **Ajouter** et ajoutez à `Server1_Gateway` une variable intitulée `HTTP_X_BI_PATH`. Lorsque vous avez terminé, cliquez sur **OK** pour créer la variable.

   h. Dans le panneau **Actions**, cliquez sur **Back to Rules**.

   i. Sélectionnez la règle précédemment créée, puis, dans le panneau **Inbound rules** situé à droite, cliquez sur **Edit...**

   j. Développez la section **Server Variables**.

   k. Dans la section **Server Variables**, cliquez sur le bouton **Add**.

   l. Dans la boîte de dialogue **Set Server Variable**, sélectionnez la variable de serveur **HTTP_X_BI_PATH** et définissez la zone **Value** sur `/ibmcognos/bi/v1`.

   m. Assurez-vous que la case **Replace existing value** est cochée.

   n. Cliquez sur **OK** pour enregistrer, puis, dans le panneau **Action**, cliquez sur **Apply**.

   o. Dans le panneau **Action** situé en haut à droite, cliquez sur **Back to Rules** pour terminer la définition de la règle.

   p. Testez la configuration en entrant le format d'URL suivant dans un navigateur : `http(s)://`*`<serveur_web>`*`:`*`<port_serveur_web>`*`/`*`<alias>`*`/bi/`. Dans cet exemple, l'URL est : `http://Server1_Gateway:80/ibmcognos/bi/`

### Résultats

**Accès direct à la passerelle IBM Cognos Analytics**

En supposant que la connexion unique pour le fournisseur d'authentification d'IBM Cognos Analytics ait été configurée, il est possible d'appeler cette dernière en accédant à l'environnement IBM Cognos Analytics en indiquant l'URL complète de la passerelle ISAP en respectant le format suivant : `HTTP(S)://<serveur_web>:<port_serveur_web>/<alias>/cgibin/cognosisapi.dll?b_action=xts.run&m=portal/main.xts&m_redirect=/<alias>/bi/`

Pour que l'URL soit correctement résolue, vous devez configurer IBM Cognos Configuration sur le serveur `Server1_Gateway` de telle sorte que les URI de répartiteur de l'entrée de la passerelle soient configurés pour pointer vers `Server2_Application server`.

Testez l'URL complète en la saisissant au format `HTTP(S)://<serveur_web>:<port_serveur_web>/<alias>/cgibin/cognosisapi.dll?b_action=xts.run&m=portal/main.xts&m_redirect=/<alias>/bi/`

Dans cet exemple, l'URL est : `http://Server1_Gateway:80/ibmcognos/cgibin/cognosisapi.dll?b_action=xts.run&m=portal/main.xts&m_redirect=/IBMCognos/bi/`

## Configuration de la passerelle CGI sur IIS version 7 ou 8

Si vous utilisez Microsoft Internet Information Services (IIS) version 7 ou ultérieure, configurez la passerelle CGI. Cette procédure est obligatoire pour la connexion unique.

La passerelle CGI est disponible pour les serveurs Web 32 bits et 64 bits.

### Pourquoi et quand exécuter cette tâche

Si vous utilisez Microsoft IIS comme serveur Web et si vous avez l'intention d'exécuter plusieurs produits IBM Cognos Analytics ou plusieurs instances du même produit sur un même ordinateur, vous devez créer un groupe d'applications distinct pour chaque produit ou instance auquel vous associerez ensuite les alias de ce produit ou de cette instance.

Pour en savoir davantage sur la création d'un groupe d'applications, reportez-vous à la documentation sur le serveur Web.

### Procédure

1. Dans le **Panneau de configuration** Microsoft Windows, cliquez sur **Programmes** > **Programmes et fonctionnalités**.

   Si vous utilisez Microsoft Windows 8 ou 2012 Server, **Programmes et fonctionnalités** est disponible directement dans le **Panneau de configuration**.
2. Cliquez sur **Activer ou désactiver des fonctionnalités Windows**.
3. Si vous utilisez Microsoft Windows 2008 Server, procédez comme suit :
   a. Cliquez sur **Gestionnaire de serveur** > **Rôles** > **Serveur Web (IIS)**.
   b. Vérifiez que **Fonctionnalités HTTP communes** ou les fonctions dont vous avez besoin sont activées.
   c. Si l'option **CGI** a la valeur **Non installé**, sélectionnez-la et cliquez sur **Ajouter des services de rôle**.

4. Si vous utilisez Microsoft Windows 2012 Server, procédez comme suit :
   a. Dans Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis sur **Suivant**.
   b. Sélectionnez votre serveur et cliquez sur **Suivant**.
   c. Sélectionnez **Serveur Web (IIS)**, si celui-ci n'est pas encore installé, vérifiez que **Fonctionnalités HTTP communes** est sélectionné et cliquez sur **Suivant** jusqu'à ce que vous accédiez la section **Services de rôle** de l'assistant.
   d. Développez **Développement d'applications**.
   e. Sélectionnez **CGI** si ce n'est pas déjà fait et cliquez sur **Suivant**.
   f. Cliquez sur **Installer**.
5. Si vous utilisez Microsoft Windows 7 ou 8, procédez comme suit :
   a. Sélectionnez **Services Internet (IIS)** si ce n'est pas déjà fait.
   b. Développez **Services Internet (IIS)** > **Services World Wide Web**.
   c. Vérifiez que **Fonctionnalités HTTP communes** ou les fonctions dont vous avez besoin sont activées.
   d. Développez **Fonctionnalités de développement d'applications**.
   e. Si l'option **CGI** n'est pas sélectionnée, sélectionnez-la.
   f. Cliquez sur le bouton **OK**.
6. Dans la console **Gestionnaire des services Internet (IIS)**, sous **Connexions**, sélectionnez le nom du serveur.
   - Si vous utilisez Microsoft Windows 2012 Server, dans **Gestionnaire de serveur**, sélectionnez **IIS**, cliquez avec le bouton droit de la souris sur le nom de votre serveur, puis cliquez sur **Gestionnaire des services Internet (IIS)**.
   - Si vous utilisez Microsoft Windows 2008 Server, dans **Gestionnaire de serveur**, développez **Rôles** > **Serveur Web (IIS)**, puis cliquez sur **Gestionnaire des services Internet (IIS)**.
   - Si vous utilisez Microsoft Windows 8, dans le **Panneau de configuration**, cliquez sur **Outils d'administration** pour accéder à la console **Gestionnaire des services Internet (IIS)**.
   - Si vous utilisez Microsoft Windows 7, dans le **Panneau de configuration**, cliquez sur **Système et sécurité** > **Outils d'administration** pour accéder à la console **Gestionnaire des services Internet (IIS)**.
7. Cliquez deux fois sur **Restrictions ISAPI et CGI**.
8. Sous **Actions**, cliquez sur **Ajouter**.
9. Entrez le chemin du fichier `cognos.cgi`. Le fichier se trouve dans le répertoire *`emplacement_installation`*`\cgi-bin`.

   Vous devez entrer le chemin d'accès complet, nom de fichier inclus. Si le chemin contient des espaces, encadrez-le par des guillemets. Saisissez par exemple :

   «`C:\Program Files\ibm\cognos\analytics\cgi-bin\cognos.cgi`»
10. Entrez une **Description**, par exemple, `CognosCGI`.
11. Sélectionnez **Autoriser l'exécution du chemin de l'extension**, puis cliquez sur **OK**.
12. Sous **Connexions**, développez **Sites**, et sous votre site Web, ajoutez les répertoires virtuels indiqués dans le tableau suivant :

*Tableau 17. Répertoires virtuels requis*

| Alias | Emplacement |
|---|---|
| ibmcognos | *emplacement_installation*/webcontent |
| ibmcognos/cgi-bin | *emplacement_installation*/cgi-bin |

**Important :** bi est la valeur par défaut des paramètres **URI de la passerelle** et **URI de Controller pour la passerelle** dans IBM Cognos Configuration. Si vous n'utilisez pas bi pour les valeurs Alias, veillez à modifier les valeurs de l'**URI de la passerelle** et l'**URI de Controller pour la passerelle** pour les faire correspondre avec les valeurs que vous utilisez.

13. Sélectionnez le répertoire virtuel cgi-bin que vous avez créé.
14. Cliquez deux fois sur **Mappages de gestionnaires**.
15. Sous **Actions**, cliquez sur **Add Module Mapping**.
    a. Dans **Request Path**, saisissez cognos.cgi.
    b. Dans **Module**, sélectionnez CgiModule.
    c. Laissez la zone **Executable (optional)** à blanc.
    d. Dans **Nom**, attribuez un nom à l'entrée comme CognosCGI.
    e. Cliquez sur le bouton **OK**.
16. Configurez le proxy inverse

    Cette procédure indique les étapes requises pour configurer le proxy inverse afin d'autoriser IIS à réécrire les demandes de passerelle et à les transmettre au groupe de serveurs d'application. Ces étapes supposent l'existence d'une architecture à deux serveurs, dans laquelle la passerelle IBM Cognos Analytics est installée dans Server1_Gateway et l'application IBM Cognos Analytics est installée dans Server2_Application.
    a. Sur le serveur Server1_Gateway, lancez IIS Manager et sélectionnez le dossier "**bi**" dans le répertoire virtuel ibmcognos configuré précédemment.
    b. Dans la vue des fonctions, démarrez la fonction **URL Rewrite**.
    c. Dans le panneau **Actions**, cliquez sur **Add Rule(s)**, puis sélectionnez **Reverse Proxy**. Cliquez sur le bouton **OK**.
    d. Dans la boîte de dialogue **Add Reverse Proxy Rule**, dans la section **Inbound Rules**, renseignez la zone **Enter the server name or the IP address...** au format suivant : *<Server2_Application:Port>*/bi. Par exemple, Server2_Application:9300/bi
    e. Vérifiez que la case **Enable SSL Offloading** est cochée, puis cliquez sur **OK**.
    f. Dans la page **Rules**, dans le panneau **Action**, cliquez sur **View Server Variables**.
    g. Cliquez sur **Add** et ajoutez une variable nommée HTTP_X_BI_PATH. Lorsque vous avez terminé, cliquez sur **OK** pour créer la variable.
    h. Dans le panneau **Actions**, cliquez sur **Back to Rules**.
    i. Sélectionnez la règle précédemment créée, puis, dans le panneau **Inbound rules** situé à droite, cliquez sur **Edit...**
    j. Développez la section **Server Variables**.
    k. Dans la section **Server Variables**, cliquez sur le bouton **Add**.
    l. Dans la boîte de dialogue **Set Server Variable**, sélectionnez la variable de serveur **HTTP_X_BI_PATH** et définissez la zone **Value** sur /ibmcognos/bi/v1.

m. Assurez-vous que la case **Replace existing value** est cochée.
n. Cliquez sur **OK** pour enregistrer, puis, dans le panneau **Action**, cliquez sur **Apply**.
o. Dans le panneau **Action** situé en haut à droite, cliquez sur **Back to Rules** pour terminer la définition de la règle.
p. Testez la configuration en entrant le format d'URL suivant dans un navigateur : `http(s)://<serveur_web>:<port_serveur_web>/<alias>/bi/`. Dans cet exemple, l'URL est : `http://Server1_Gateway:80/ibmcognos/bi/`.

### Résultats

Les utilisateurs peuvent accéder à la passerelle CGI en saisissant `http://nom_serveur/ibmcognos/bi/` dans leur navigateur Web.

## Test de la passerelle

Vous pouvez tester l'installation via un navigateur Web.

### Procédure

1. Vérifiez que votre serveur Web est en cours d'exécution.
2. Ouvrez un navigateur Web.
3. Dans la barre d'adresse, tapez l'**URI de passerelle** depuis IBM Cognos Configuration. Par exemple :

   `http://host_name:port/ibmcognos`

   La page d'**accueil** du portail IBM Cognos Analytics s'affiche.

# Chapitre 6. Installation et configuration des composants de modélisation facultatifs

Après l'installation et la configuration des composants de serveur IBM Cognos Analytics, vous pouvez installer et configurer IBM Cognos Framework Manager, le composant de modélisation destiné à la production de rapports, ainsi qu'IBM Cognos Transformer, l'outil de modélisation qui permet de créer des PowerCubes.

Installez Framework Manager et Transformer à un emplacement différent de Cognos Analytics.

## IBM Cognos Framework Manager

IBM Cognos Framework Manager est l'outil de modélisation de métadonnées d'IBM Cognos Analytics.

Vous pouvez l'installer sur le même ordinateur que les autres composants d'IBM Cognos Analytics, ou sur un autre ordinateur.

Si vous procédez à une mise à niveau depuis une version précédente de Framework Manager, vous pouvez utiliser les mêmes modèles et projets que vous avez utilisés avec la version précédente. Pour mettre à niveau des projets existants, vous devez les ouvrir dans la nouvelle version de Framework Manager.

Si vous effectuez une mise à niveau de Framework Manager à partir d'une version précédente, vous devez d'abord désinstaller la version précédente de Framework Manager. Pour en savoir davantage, reportez-vous à la section Chapitre 12, «Désinstallation d'IBM Cognos Analytics», à la page 307.

Avant d'installer Framework Manager, fermez tous les programmes en cours d'exécution pour vous assurer que le programme d'installation copie tous les fichiers requis sur l'ordinateur.

Assurez-vous que vous disposez de privilèges d'administration sur l'ordinateur Windows où vous souhaitez faire l'installation. Si vous n'êtes pas administrateur, demandez à votre administrateur système de vous ajouter au groupe Administrateurs sur votre ordinateur. Les privilèges d'administration sont également requis pour le compte qui est utilisé pour l'exécution de Framework Manager.

Installez et configurez tous les composants serveur d'IBM Cognos Analytics avant d'installer Framework Manager.

Procédez à l'installation dans un répertoire dont le nom de chemin ne contient que des caractères ASCII. Certains serveurs ne prennent pas en charge les caractères non ASCII dans les noms de répertoires. L'installation de Framework Manager dans un répertoire dont le nom de chemin contient une apostrophe peut entraîner une ouverture incorrecte de l'aide.

Pour faciliter la gestion, le partage et la sécurisation des différentes versions de vos métadonnées, vous pouvez configurer Framework Manager de façon à ce qu'il utilise un système de contrôle source externe. Pour en savoir davantage,

reportez-vous à la section relative à l'utilisation des systèmes de contrôle de référentiel externe dans le manuel *IBM Cognos Framework Manager - Guide d'utilisation*.

## Configuration système requise pour IBM Cognos Framework Manager

Avant d'installer IBM Cognos Framework Manager, assurez-vous que l'ordinateur Windows satisfait les configurations matérielle et logicielle requises pour IBM Cognos Analytics. La taille de vos modèles détermine la configuration matérielle requise, telle que l'espace disque nécessaire.

Le tableau ci-dessous répertorie les configurations matérielle et logicielle minimales requises pour exécuter Framework Manager.

*Tableau 18. Configuration système requise pour Framework Manager*

| Configuration requise | Spécification |
|---|---|
| Système d'exploitation | Windows |
| RAM | Minimum : 512 Mo<br><br>Optimum : 1 Go |
| Espace disque | Minimum : 500 Mo d'espace libre sur l'unité contenant le répertoire temporaire utilisé par IBM Cognos Analytics |
| Base de données | Le logiciel de client de base de données doit être installé sur le même ordinateur que Framework Manager si vous utilisez le mode de requête compatible.<br><br>Connectivité aux bases de données |
| Autre | Microsoft Data Access Component (MDAC), version 2.6 ou ultérieure, à utiliser avec les exemples de produits. |

Pour faciliter la gestion, le partage et la sécurisation des différentes versions de vos métadonnées, vous pouvez configurer Framework Manager de façon à ce qu'il utilise un système de contrôle source externe. Pour en savoir davantage, reportez-vous à la section relative à l'utilisation des systèmes de contrôle de référentiel externe dans le manuel Framework Manager *User Guide*.

## Installation d'IBM Cognos Framework Manager

Pour une installation complète d'IBM Cognos Analytics, vous devez installer Cognos Framework Manager sur un ordinateur Windows.

L'emplacement d'installation doit être différent de celui d'IBM Cognos Analytics.

### Procédure

1. Accédez au répertoire dans lequel les fichiers d'installation ont été téléchargés et décompressés, puis cliquez deux fois sur le fichier `ca_model_<plateforme>_<génération>.exe`.
2. Sélectionnez la langue d'installation.

   La langue sélectionnée détermine la langue de l'interface utilisateur. Toutes les langues prises en charge sont installées. Vous pouvez redéfinir l'interface utilisateur sur l'une des langues installées après l'installation.
3. Suivez les instructions fournies par l'assistant d'installation pour copier les fichiers nécessaires sur votre ordinateur.

4. Protégez le répertoire d'installation des accès non autorisés.

### Que faire ensuite

Les paramètres par défaut sont utilisés pour la configuration. Vous pouvez modifier ces paramètres par défaut au cours de l'installation ou ultérieurement afin qu'ils soient mieux adaptés à votre environnement.

## Configuration d'IBM Cognos Framework Manager

Vous devez configurer IBM Cognos Framework Manager pour la communication avec IBM Cognos Analytics et ses composants.

### Avant de commencer

Installez et configurez IBM Cognos Analytics avant de configurer Framework Manager. Vous devez d'abord installer et configurer Content Manager, puis démarrer le service **IBM Cognos** sur au moins un ordinateur Content Manager. Cela garantit que le service d'autorité de certification émet un certificat pour l'ordinateur Framework Manager.

Il vous faut également configurer les sources de données que vous prévoyez d'utiliser dans vos projets Framework Manager.

### Pourquoi et quand exécuter cette tâche

Si vous installez Framework Manager sur le même ordinateur qu'IBM Cognos Analytics (dans un répertoire différent), la configuration n'est pas nécessaire si les conditions suivantes sont respectées :

- Le serveur Web est configuré pour utiliser les répertoires virtuels par défaut.
- Les ports, les ressources et les paramètres cryptographiques par défaut sont utilisés.

Lorsque Framework Manager est installé en dehors du pare-feu réseau qui protège les composants du groupe de serveurs d'applications, des problèmes de communication peuvent se poser au niveau du répartiteur. Pour éviter ces problèmes, vous pouvez installer Framework Manager avec les composants du groupe de serveurs d'application, ou bien installer et configurer une passerelle dédiée aux communications entre Framework Manager et le répartiteur. Pour en savoir davantage, reportez-vous à la section«Configuration de Framework Manager à l'extérieur du pare-feu du réseau», à la page 134 ou «Configuration de Framework Manager à l'extérieur du pare-feu du réseau», à la page 134.

### Procédure

1. Sur l'ordinateur où vous avez installé Framework Manager, démarrez IBM Cognos Configuration.
2. Dans la sous-fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Indiquez des valeurs appropriées pour les paramètres suivants :

   **URI de la passerelle**

   Valeur par défaut : `http://`*`serveur_ca`*`:`*`port`*`/bi/v1/disp`

   Exemple : `http://mon_serveur_ca:`*`9300`*`/bi/v1/disp`

   Il doit toujours être identique à l'URI de Cognos Analytics.

Si l'URI contient **localhost**, remplacez **localhost** par un nom d'hôte qualifié complet ou une adresse IP.

**URI du répartiteur des applications externes**
Valeur par défaut : `http://serveur_ca:port/p2pd/servlet/dispatch`

Exemple : `http://mon_serveur_ca:9300/p2pd/servlet/dispatch`

Si l'URI contient **localhost**, remplacez **localhost** par un nom d'hôte qualifié complet ou une adresse IP.

4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Résultats

Framework Manager est configuré pour communiquer avec IBM Cognos Analytics.

## Configuration de Framework Manager à l'extérieur du pare-feu du réseau

Procédez comme suit pour configurer les communications entre Framework Manager et IBM Cognos Analytics lorsque Framework Manager est à l'intérieur d'un pare-feu du réseau.

### Procédure

1. Sur l'ordinateur où vous avez installé Framework Manager, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, saisissez la valeur adéquate pour la zone **URI de la passerelle**. Utilisez le protocole HTTPS ou HTTP pour sélectionner les communications SSL ou non SMS.
4. Remplacez la chaîne de nom d'hôte localhost de l'**URI de la passerelle** par l'adresse IP ou le nom d'hôte de l'ordinateur sur lequel le composant de la passerelle est installé.
5. Définissez la valeur de l'**URI du répartiteur pour des applications externes** en saisissant l'URI du serveur sur lequel les composants du groupe de serveurs d'applications sont installés.

   Cette valeur est identique à celle de la propriété **URI interne du répartiteur** sur l'ordinateur des composants du groupe de serveurs d'applications.
6. Dans la fenêtre **Explorateur**, sous **Cryptographie**, cliquez sur **Cognos**, le fournisseur cryptographique par défaut.
7. Dans le groupe de propriétés **Paramètres de l'autorité de certification**, définissez la propriété **Mot de passe** de telle sorte qu'elle corresponde à celle que vous avez configurée sur l'ordinateur Content Manager actif par défaut.
8. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Configuration de Framework Manager à l'extérieur du pare-feu du réseau

Lorsque Framework Manager est installé à l'extérieur du pare-feu réseau, vous pouvez installer et configurer une passerelle dédiée aux communications avec le répartiteur.

### Procédure

1. Configurez une passerelle dédiée pour Framework Manager.

2. Sur l'ordinateur passerelle, ouvrez IBM Cognos Configuration, puis attribuez à la propriété **URI du répartiteur pour la passerelle** l'URI indiqué pour **URI de répartiteur interne** sur l'ordinateur des composants du groupe de serveurs d'application.
3. Sur l'ordinateur Framework Manager, démarrez IBM Cognos Configuration.
4. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
5. Dans la fenêtre **Propriétés**, attribuez à la zone **URI de la passerelle** la valeur qui correspond au serveur servant de passerelle dédiée.
   - Si le serveur Web est configuré pour la passerelle ISAPI, remplacez `cognos.cgi` par `cognosisapi.dll`.
   - S'il est configuré pour utiliser des modules Apache, utilisez la syntaxe suivante :

     `http://`*`nom_hôte:port`*`/ibmcognos/cgi-bin/`*`alias_module`*
6. Remplacez la chaîne de nom d'hôte localhost de l'**URI de la passerelle** par l'adresse IP ou par le nom d'hôte du serveur de la passerelle dédiée.
7. Dans la zone **URI du répartiteur des applications externes**, saisissez l'URI spécifiée pour **URI de répartiteur interne** sur le serveur où les composants du groupe de serveurs d'application sont installés.
8. Dans la fenêtre **Explorateur**, sous **Cryptographie**, cliquez sur **Cognos**, le fournisseur cryptographique par défaut.
9. Dans le groupe de propriétés **Paramètres de l'autorité de certification**, définissez la propriété **Mot de passe** de telle sorte qu'elle corresponde à celle que vous avez configurée sur l'ordinateur Content Manager actif par défaut.
10. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

### Résultats

Framework Manager est configuré pour communiquer avec IBM Cognos Analytics et ses composants.

## Définition des variables pour les connexions de source de données de Framework Manager

Les outils de modélisation d'IBM Cognos Analytics BI permettent de créer et de gérer des métadonnées. Framework Manager crée et gère les métadonnées associées aux fonctions de génération de rapports. Etant donné que les métadonnées sont dérivées de sources de données d'environnements multilingues ou multiplateformes, vous devez prendre en compte plusieurs points ou effectuer différentes opérations lorsque vous configurez l'environnement de sources de données de Framework Manager. Généralement, ces opérations dépendent de l'autre technologie utilisée pour votre source de données ou d'importation.

Si vous avez procédé à une mise à niveau à partir d'une version antérieure de Framework Manager, aucun élément n'a besoin d'être configuré dans l'environnement de sources de données. Vous devez configurer l'environnement de sources de données uniquement si vous avez installé Framework Manager dans un emplacement différent de celui de la version précédente.

Les utilisateurs qui travaillent avec des langues différentes peuvent se connecter à une source de données MSAS 2005 depuis la même instance d'IBM Cognos Analytics. Les modélisateurs doivent créer un pack distinct pour chaque langue. Les utilisateurs peuvent exécuter les rapports dans n'importe quelle langue.

Pour plus d'informations sur les connexions de source de données, voir le *Guide d'administration et de sécurité* IBM Cognos.

Veillez à installer les polices appropriées pour la prise en charge des jeux de caractères et des symboles monétaires que vous utilisez. Pour que les symboles monétaires japonais et coréens s'affichent correctement, vous devez installer les polices supplémentaires depuis le CD-ROM Supplementary Language Documentation.

Procédez comme suit dans l'emplacement où vous avez installé Framework Manager.

## Procédure

1. Paramétrez la variable d'environnement pour une prise en charge multilingue :
   - Pour Oracle, définissez la variable d'environnement **NLS_LANG** (prise en charge de la langue nationale) sur chaque ordinateur sur lequel Framework Manager et le serveur IBM Cognos Analytics sont installés en saisissant la commande suivante :

     ```
     NLS_LANG = language_territory.character_set
     ```

     Quelques exemples :

     ```
     NLS_LANG = AMERICAN_AMERICA.UTF8
     ```

     ```
     NLS_LANG = JAPANESE_JAPAN.UTF8
     ```

     La valeur de la variable détermine le comportement d'IBM Cognos Analytics par rapport aux paramètres régionaux. Les messages d'erreur, l'ordre de tri, la date, l'heure, la devise, les données numériques et les conventions de calendrier peuvent en effet s'adapter automatiquement à la langue et aux paramètres régionaux.
   - Pour IBM Db2, affectez à la variable d'environnement **DB2CODEPAGE** la valeur 1252.

     Pour en savoir davantage sur l'usage de cette variable d'environnement facultative, reportez-vous à la documentation sur Db2.

   Aucun paramètre n'est requis pour SAP BW. SAP prend en charge une seule page de codes sur les systèmes SAP BW non-Unicode.
2. Pour Oracle, ajoutez `$ORACLE_HOME/lib` à la variable **LD_LIBRARY_PATH**.

   Lors de la définition des chemins d'accès à la bibliothèque de chargement, assurez-vous que les bibliothèques Oracle 32 bits se trouvent sur le chemin d'accès à la bibliothèque (généralement le répertoire `$ORACLE_HOME/lib` ou `$ORACLE_HOME/lib32` si vous installez un client Oracle 64 bits).
3. Pour SAP BW, configurez les objets d'autorisation ci-dessous de façon à ce que l'outil de modélisation puisse extraire les métadonnées.

   Lorsque des valeurs par défaut sont définies, il peut être souhaitable de modifier les valeurs sur le système SAP.
   - **S_RFC**

     Attribuez à la zone **Activité** la valeur **16**.

     Définissez la zone **Nom de RFC à protéger** sur la valeur **SYST, RSOB, SUGU, RFC1, RS_UNIFICATION, RSAB, SDTX, SU_USER**.

     Définissez l'objet **Type de RFC** en vue de désigner la zone protégée sur la valeur **FUGR**.
   - **S_TABU_DIS**

     Attribuez à la zone **Activité** la valeur **03**.

     Attribuez à la zone **Groupe d'autorisation** la valeur **&NC&**.

**Remarque :** **&NC&** une table n'ayant pas de groupe d'autorisation. Pour des raisons de sécurité, créez un groupe d'autorisation et affectez-lui la table **RSHIEDIR**. Le nouveau groupe d'autorisation limite l'accès de l'utilisateur à la table uniquement, ce qui est nécessaire à l'outil de modélisation. Créez le groupe d'autorisation en tant que personnalisation dans le système SAP.

- **S_USER_GRP**

  Attribuez à la zone **Activité** la valeur **03, 05**.

  Définissez la zone **Groupe d'utilisateurs pour maintenance principale des utilisateurs** sur la valeur par défaut.

- **S_RS_COMP**

  Définissez la zone **Activité** sur la valeur par défaut.

  Attribuez à la zone **InfoArea** la valeur *Nom technique InfoArea*.

  Attribuez à la zone **InfoCube** la valeur : *Nom technique InfoCube*.

  Définissez la zone **Nom (identificateur) des composants de génération de rapports** sur la valeur par défaut.

  Définissez la zone **Type de composants de génération de rapports** sur la valeur par défaut.

- **S_RS_COMP1**

  Définissez la zone **Activité** sur la valeur par défaut.

  Définissez la zone **Nom (identificateur) des composants de génération de rapports** sur la valeur par défaut.

  Définissez la zone **Type de composants de génération de rapports** sur la valeur par défaut.

  Définissez la zone **Propriétaire (personne responsable)** sur la valeur par défaut.

- **S_RS_HIER**

  Attribuez à la zone **Activité** la valeur **71**.

  Attribuez à la zone **Nom de hiérarchie** la valeur *Nom de hiérarchie*.

  Attribuez à la zone **InfoObject** la valeur *Nom technique InfoObject*.

  Attribuez à la zone **Version** la valeur *Version de hiérarchie*.

- **S_RS_ICUBE**

  Attribuez à la zone **Activité** la valeur **03**.

  Attribuez à la zone **Sous-objet InfoCube** les valeurs **DATA** et **DEFINITION**.

  Attribuez à la zone **InfoArea** la valeur *Nom technique InfoArea*.

  Attribuez à la zone **InfoCube** la valeur *Nom technique InfoCube*.

Pour en savoir davantage sur les objets d'autorisation SAP BW, reportez-vous à Transaction SU03.

## Test de l'installation de Framework Manager

Pour tester votre configuration, démarrez l'application et créez un projet.

### Procédure

Pour démarrer Framework Manager, dans le menu **Démarrer**, cliquez sur **Tous les programmes** > **IBM Cognos Framework Manager**.
Sous Microsoft Windows 8 ou Windows 2012 Server, cliquez deux fois sur l'icône **Framework Manager** dans le panneau **Démarrer**.
Si la version du schéma de modèle est antérieure à celle actuellement prise en

charge, vous serez probablement invité à effectuer une mise à niveau.
Si la page **Bienvenue** de Framework Manager s'affiche, cela signifie que l'installation fonctionne.

# IBM Cognos Transformer

IBM Cognos Transformer est un outil de modélisation de métadonnées qui vous permet de créer des PowerCubes à utiliser avec les produits IBM Cognos.

Transformer peut désormais être mis plus facilement à la disposition des spécialistes métier qui souhaitent concevoir des modèles et créer des PowerCubes pour leur usage personnel. Ainsi, les départements informatiques peuvent fournir aux spécialistes métier ou aux modélisateurs Transformer un programme d'installation Web téléchargeable à partir d'un portail professionnel ou sécurisé, de façon à faciliter la distribution des fichiers d'installation.

Transformer est constitué des composants ci-dessous :

- Utilitaire UNIX et Linux pour la création de PowerCubes
- Client IBM Cognos Transformer

  Ce composant doit être installé sur un ordinateur Windows.

Chaque composant doit être installé à un emplacement différent de IBM Cognos Analytics.

Les paramètres par défaut sont utilisés pour la configuration. Vous pouvez modifier ces paramètres par défaut si nécessaire. Toutefois, ils doivent toujours être identiques à ceux d'IBM Cognos Analytics.

## Configuration système requise pour IBM Cognos Transformer

Avant d'installer IBM Cognos Transformer, assurez-vous que l'ordinateur satisfait la configuration logicielle et matérielle requise. La taille de vos PowerCubes détermine la configuration matérielle requise, telle que l'espace disque nécessaire.

Le tableau ci-dessous présente les configurations matérielle et logicielle minimales requises pour exécuter IBM Cognos Transformer.

*Tableau 19. Configuration système requise pour Transformer*

| **Configuration requise** | **Spécification** |
|---|---|
| Système d'exploitation | Windows<br><br>UNIX : Oracle Solaris, IBM AIX<br><br>Linux |
| RAM | Minimum : 512 Mo<br><br>Optimum : 4 Go |
| Espace disque | Minimum : 500 Mo d'espace libre sur l'unité contenant le répertoire temporaire |
| Source de données | Logiciel client de base de données installé sur le même ordinateur qu'IBM Cognos Transformer<br><br>Configuration de la connectivité à la base de données |

*Tableau 19. Configuration système requise pour Transformer (suite)*

| Configuration requise | Spécification |
|---|---|
| Autre | Microsoft Data Access Component (MDAC), version 2.6 ou ultérieure, à utiliser avec les exemples de produits. |

# Installation d'IBM Cognos Transformer

L'installation d'IBM Cognos Transformer vous permet de créer des PowerCubes à utiliser avec les produits IBM Cognos.

L'emplacement d'installation de Transformer doit être différent de celui d'IBM Cognos Analytics.

Avant l'installation de Transformer, les composants de serveur Cognos Analytics doivent être installés et configurés.

La langue que vous sélectionnez dans l'assistant d'installation détermine la langue de l'interface utilisateur à la fois pour l'assistant d'installation pour IBM Cognos Transformer. Toutes les langues disponibles sont installées.

Dans le cas d'un système d'exploitation UNIX ou Linux, l'installation d'IBM Cognos Transformer n'est complète que si vous installez également IBM Cognos Transformer sur un ordinateur équipé de Microsoft Windows. Tous les composants sont installés dans ces deux environnements et vous devez utiliser les fonctions et les outils qui conviennent pour chaque environnement. Par exemple, le client IBM Cognos Transformer fournit une interface graphique utilisateur pour la conception de modèles sur des ordinateurs Windows. Vous pouvez ensuite créer des cubes sur votre ordinateur UNIX ou Linux. Les modèles contenant une source de données IQD ne sont pas pris en charge sous Linux.

Installez les composants dans un répertoire dont le nom du chemin d'accès contient uniquement des caractères ASCII. Certains serveurs ne prennent pas en charge les caractères non ASCII dans les noms de répertoires.

Avant d'installer IBM Cognos Transformer, fermez tous les programmes en cours d'exécution pour s'assurer que le programme d'installation copie tous les fichiers requis sur l'ordinateur.

Dans le cas d'une installation sous Windows, assurez-vous que vous disposez de privilèges d'administration sur l'ordinateur Windows où vous effectuez l'installation. Si vous n'êtes pas administrateur, demandez à votre administrateur système de vous ajouter au groupe Administrateurs sur votre ordinateur.

## Installation d'IBM Cognos Transformer sous UNIX ou Linux

Procédez comme suit pour installer IBM Cognos Transformer sur UNIX ou Linux.

### Procédure

1. Accédez à l'emplacement dans lequel les fichiers d'installation ont été téléchargés et décompressés.
2. Pour démarrer l'assistant d'installation, accédez au répertoire du système d'exploitation, puis saisissez :

   ```
   ./issetup
   ```
3. Sélectionnez la langue d'installation.

La langue que vous sélectionnez dans l'assistant d'installation détermine la langue de l'interface utilisateur à la fois pour l'assistant d'installation pour IBM Cognos Transformer. Toutes les langues disponibles sont installées.

4. Suivez les instructions de l'Assistant d'installation et copiez les fichiers requis sur votre ordinateur.

   **Conseil :** Le composant Series 7 IQD Bridge n'est pas pris en charge sous Linux.

5. Dans la page **Terminer** de l'Assistant d'installation, procédez comme suit :
   - Si vous souhaitez consulter les fichiers journaux, cliquez sur **Afficher** en sélectionnant le fichier journal approprié.
   - Ne démarrez pas IBM Cognos Configuration maintenant car vous devez d'abord vérifier que votre environnement est configuré correctement.

     Vous pouvez configurer Transformer ultérieurement à l'aide d'IBM Cognos Configuration en saisissant `cogconfig.sh` dans le répertoire *`emplacement_installation`*`/bin64`.
   - Cliquez sur **Terminer**.

### Que faire ensuite

Pour des informations sur la syntaxe pour les options de ligne de commande UNIX qui sont prises en charge par IBM Cognos Transformer, voir le *guide des commandes UNIX d'IBM Cognos Transformer* dans le Knowledge Center d'IBM Cognos Analytics (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html).

Vous pouvez accéder à la page d'aide d'IBM Cognos Transformer sous UNIX en saisissant `cogtr man` depuis le répertoire *`emplacement_installation`*`/bin64`.

## Installation d'IBM Cognos Transformer sous Windows

Procédez comme suit pour installer IBM Cognos Transformer sur Microsoft Windows.

### Procédure

1. Accédez à l'emplacement dans lequel les fichiers d'installation ont été téléchargés et décompressés, puis cliquez deux fois sur `issetup.ex`.
2. Sélectionnez la langue d'installation.

   La langue que vous sélectionnez dans l'assistant d'installation détermine la langue de l'interface utilisateur à la fois pour l'assistant d'installation pour IBM Cognos Transformer. Toutes les langues disponibles sont installées.
3. Suivez les instructions fournies par l'assistant d'installation pour copier les fichiers nécessaires sur votre ordinateur.
4. Dans la page **Terminer** de l'Assistant d'installation, procédez comme suit :
   - Si vous souhaitez consulter les fichiers journaux, cliquez sur **Afficher** en sélectionnant le fichier journal approprié.
   - Ne démarrez pas IBM Cognos Configuration maintenant car vous devez d'abord vérifier que votre environnement est configuré correctement.

     Vous pouvez démarrer IBM Cognos Configuration à l'aide du raccourci **IBM Cognos Configuration** depuis le menu **Démarrer**.
   - Cliquez sur **Terminer**.

# Configuration d'IBM Cognos Transformer

Vous devez configurer IBM Cognos Transformer pour communiquer avec IBM Cognos Analytics.

## Avant de commencer

Installez et configurez les composants IBM Cognos Analytics avant de configurer IBM Cognos Transformer. Vous devez d'abord installer et configurer Content Manager, puis démarrer le service **IBM Cognos** sur au moins un ordinateur Content Manager avant de configurer IBM Cognos Transformer. Ainsi, vous garantissez que le service d'autorité de certification émettra un certificat pour l'ordinateur IBM Cognos Transformer.

Pour prendre en charge l'utilisation des sources de données IBM Cognos Analytics (y compris les packs et rapports) dans Transformer, veillez à ce que le client de base de données soit installé sur l'ordinateur où Transformer est installé.

## Procédure

1. Sur l'ordinateur où vous avez installé IBM Cognos Transformer, démarrez IBM Cognos Configuration.
2. Dans la sous-fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Indiquez des valeurs appropriées pour les paramètres suivants :

   **URI de la passerelle**
   Valeur par défaut : `http://serveur_ca:port/bi/v1/disp`

   Exemple : `http://mon_serveur_ca:9300/bi/v1/disp`

   Il doit toujours être identique à l'URI de Cognos Analytics.

   Si l'URI contient **localhost**, remplacez **localhost** par un nom d'hôte qualifié complet ou une adresse IP.

   **URI du répartiteur des applications externes**
   Valeur par défaut : `http://serveur_ca:port/p2pd/servlet/dispatch`

   Exemple : `http://mon_serveur_ca:9300/p2pd/servlet/dispatch`

   Si l'URI contient **localhost**, remplacez **localhost** par un nom d'hôte qualifié complet ou une adresse IP.
4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Résultats

IBM Cognos Transformer est configuré pour communiquer avec IBM Cognos Analytics.

# Communication entre Transformer et Cognos Analytics

Vous devez configurer IBM Cognos Transformer pour la communication avec IBM Cognos Analytics et ses composants.

Les instructions de cette rubrique sont destinées à l'installateur ou l'administrateur. Si vous êtes le spécialiste métier ou un modélisateur Transformer et souhaitez télécharger et utiliser Transformer, reportez-vous à «Déploiement d'IBM Cognos Transformer pour les modélisateurs», à la page 147

Si IBM Cognos Analytics est installé dans plusieurs emplacements, vérifiez que tous les URI pointent vers la version correcte de ce produit.

### Installations avec un pare-feu

Lorsque Transformer est situé en dehors du pare-feu réseau qui protège les composants du groupe de serveurs d'applications, des problèmes de communication peuvent se poser au niveau du répartiteur. Pour éviter ces problèmes, vous pouvez installer l'outil de modélisation dans le même niveau architectural que les composants du groupe de serveurs d'applications ou bien installer et configurer une passerelle dédiée aux communications de Transformer. Pour en savoir davantage, voir «Remarques sur le pare-feu», à la page 29.

Si vous utilisez une passerelle dédiée, vous devez également configurer l'ordinateur de cette passerelle. Pour en savoir davantage, voir Chapitre 5, «Installation et configuration de la passerelle», à la page 97.

## Sources de données et Transformer

IBM Cognos Transformer crée et gère les métadonnées associées aux PowerCubes. Etant donné que les métadonnées sont dérivées de sources de données d'environnements multilingues ou à plusieurs plateformes, vous devez prendre en compte plusieurs points ou effectuer différentes opérations lorsque vous configurez l'environnement de sources de données pour IBM Cognos Transformer. Généralement, ces opérations dépendent des technologies utilisées pour votre source de données ou d'importation.

Si des utilisateurs travaillant dans différentes langues se connectent à une source de données Microsoft Analysis Services (MSAS) 2000, vous devez créer une instance distincte d'IBM Cognos Analytics pour chaque langue.

Les utilisateurs qui travaillent avec des langues différentes peuvent se connecter à une source de données MSAS 2005 depuis la même instance d'IBM Cognos Analytics. Les modélisateurs doivent créer un pack distinct pour chaque langue. Les utilisateurs peuvent exécuter les rapports dans n'importe quelle langue.

Pour en savoir davantage sur les connexions de sources de données, reportez-vous au *IBM Cognos AnalyticsGuide d'administration et de sécurité*.

Veillez à installer les polices appropriées pour la prise en charge des jeux de caractères et des symboles monétaires que vous utilisez. Pour que les symboles monétaires japonais et coréens s'affichent correctement, vous devez installer les polices supplémentaires depuis le CD-ROM Supplementary Language Documentation.

### Configuration des sources de données pour Transformer

Procédez comme suit pour configurer des sources de données Oracle ou SAP BW pour IBM Cognos Transformer.

#### Procédure

1. Paramétrez la variable d'environnement pour une prise en charge multilingue :
   - Pour Oracle, définissez la variable d'environnement **NLS_LANG** (prise en charge de la langue nationale) sur chaque ordinateur sur lequel Framework Manager et le serveur IBM Cognos Analytics sont installés en saisissant la commande suivante :

     ```
     NLS_LANG = language_territory.character_set
     ```

Quelques exemples :

```
NLS_LANG = AMERICAN_AMERICA.UTF8
NLS_LANG = JAPANESE_JAPAN.UTF8
```

La valeur de la variable détermine le comportement d'IBM Cognos Analytics par rapport aux paramètres régionaux. Les messages d'erreur, l'ordre de tri, la date, l'heure, la devise, les données numériques et les conventions de calendrier peuvent en effet s'adapter automatiquement à la langue et aux paramètres régionaux.

- Pour IBM Db2, affectez à la variable d'environnement **DB2CODEPAGE** la valeur 1252.

  Pour en savoir davantage sur l'usage de cette variable d'environnement facultative, reportez-vous à la documentation sur Db2.

Aucun paramètre n'est requis pour SAP BW. SAP prend en charge une seule page de codes sur les systèmes SAP BW non-Unicode.

2. Pour Oracle, ajoutez $ORACLE_HOME/lib au chemin d'accès aux bibliothèques.

   Lors de la définition des chemins d'accès à la bibliothèque de chargement, assurez-vous que les bibliothèques Oracle 32 bits se trouvent sur le chemin d'accès à la bibliothèque (généralement le répertoire $ORACLE_HOME/lib ou $ORACLE_HOME/lib32 si vous installez un client Oracle 64 bits).

3. Pour SAP BW, configurez les objets d'autorisation ci-dessous de façon à ce que l'outil de modélisation puisse extraire les métadonnées.

   Lorsque des valeurs par défaut sont définies, il peut être souhaitable de modifier les valeurs sur le système SAP.

   - **S_RFC**

     Attribuez à la zone **Activité** la valeur **16**.

     Définissez la zone **Nom de RFC à protéger** sur la valeur **SYST, RSOB, SUGU, RFC1, RS_UNIFICATION, RSAB, SDTX, SU_USER**.

     Définissez l'objet **Type de RFC** en vue de désigner la zone protégée sur la valeur **FUGR**.

   - **S_TABU_DIS**

     Attribuez à la zone **Activité** la valeur **03**.

     Attribuez à la zone **Groupe d'autorisation** la valeur **&NC&**.

     **Remarque : &NC&** une table n'ayant pas de groupe d'autorisation. Pour des raisons de sécurité, créez un groupe d'autorisation et affectez-lui la table **RSHIEDIR**. Le nouveau groupe d'autorisation limite l'accès de l'utilisateur à la table uniquement, ce qui est nécessaire à l'outil de modélisation. Créez le groupe d'autorisation en tant que personnalisation dans le système SAP.

   - **S_USER_GRP**

     Attribuez à la zone **Activité** la valeur **03, 05**.

     Définissez la zone **Groupe d'utilisateurs pour maintenance principale des utilisateurs** sur la valeur par défaut.

   - **S_RS_COMP**

     Définissez la zone **Activité** sur la valeur par défaut.

     Attribuez à la zone **InfoArea** la valeur *Nom technique InfoArea*.

     Attribuez à la zone **InfoCube** la valeur : *Nom technique InfoCube*.

     Définissez la zone **Nom (identificateur) des composants de génération de rapports** sur la valeur par défaut.

Définissez la zone **Type de composants de génération de rapports** sur la valeur par défaut.

- **S_RS_COMP1**

  Définissez la zone **Activité** sur la valeur par défaut.

  Définissez la zone **Nom (identificateur) des composants de génération de rapports** sur la valeur par défaut.

  Définissez la zone **Type de composants de génération de rapports** sur la valeur par défaut.

  Définissez la zone **Propriétaire (personne responsable)** sur la valeur par défaut.

- **S_RS_HIER**

  Attribuez à la zone **Activité** la valeur **71**.

  Attribuez à la zone **Nom de hiérarchie** la valeur *Nom de hiérarchie*.

  Attribuez à la zone **InfoObject** la valeur *Nom technique InfoObject*.

  Attribuez à la zone **Version** la valeur *Version de hiérarchie*.

- **S_RS_ICUBE**

  Attribuez à la zone **Activité** la valeur **03**.

  Attribuez à la zone **Sous-objet InfoCube** les valeurs **DATA** et **DEFINITION**.

  Attribuez à la zone **InfoArea** la valeur *Nom technique InfoArea*.

  Attribuez à la zone **InfoCube** la valeur *Nom technique InfoCube*.

Pour en savoir davantage sur les objets d'autorisation SAP BW, reportez-vous à Transaction SU03.

## Test de l'installation de Transformer

Pour tester votre configuration, démarrez l'application et créez un modèle.

### Procédure

Pour démarrer IBM Cognos Transformer, depuis le menu **Démarrer**, accédez à Programmes et cliquez sur **IBM Cognos Transformer**.
Sous Microsoft Windows 8 ou Windows 2012 Server, cliquez deux fois sur l'icône **IBM Cognos Transformer** dans le panneau **Démarrer**.
Pour démarrer manuellement IBM Cognos Transformer, cliquez deux fois sur le fichier `cogtr.exe` dans le répertoire *emplacement_installation*`\bin`.
Si la fenêtre **Transformer** s'affiche, votre installation fonctionne.

## Tâches de configuration supplémentaires d'IBM Cognos Transformer

Une fois l'installation de Transformer effectuée, vous pouvez effectuer les tâches suivantes :

- Si vous souhaitez utiliser les modèles Transformer depuis IBM Cognos Series 7 et continuer d'utiliser les sources de données IQD, vous devez ajouter les sources de données IBM Cognos Series 7 dans Transformer

Pour mettre Transformer à la disposition des modélisateurs afin que ceux-ci puissent l'installer et l'utiliser, vous pouvez effectuer les opérations suivantes :

- Créer un emplacement d'installation réseau pour les modélisateurs Transformer
- Exporter les données de configuration pour les modélisateurs qui travaillent avec Transformer
- Déployer des instances d'IBM Cognos Analytics pour les modélisateurs

## Ajout de sources de données IBM Cognos Series 7 à Transformer

Si vous prévoyez d'utiliser des modèles Transformer et des sources de données IBM Cognos Series 7, vous devez ajouter l'emplacement de vos sources de données IBM Cognos Series 7 au fichier de passerelle Transformer.

Les instructions de cette rubrique sont destinées à l'installateur ou l'administrateur. Si vous êtes le spécialiste métier ou un modélisateur Transformer et souhaitez télécharger et utiliser Transformer, reportez-vous à «Déploiement d'IBM Cognos Transformer pour les modélisateurs», à la page 147

### Procédure

1. Connectez-vous en tant qu'administrateur.
2. Dans le répertoire *emplacement_installation*/CS7Gateways/bin, ouvrez le fichier cs7g.ini dans un éditeur de texte.
3. Ajoutez les emplacements de vos sources de données IBM Cognos Series 7 dans le fichier.
4. Enregistrez le fichier.

   Les changements sont appliqués à la prochaine ouverture de Transformer.

## Création d'un emplacement d'installation réseau pour les modélisateurs Transformer

Certains utilisateurs avancés ou spécialisés de votre entreprise souhaitent peut-être créer des PowerCubes modélisés selon des sources de données à la fois personnelles et professionnelles. Ces utilisateurs voudront sûrement effectuer leur propre analyse des données pour leur domaine professionnel précis ou pour un petit groupe d'utilisateurs. Un installateur ou un administrateur a la possibilité de télécharger un fichier exécutable dans un emplacement Web ou de réseau local (LAN), où les modélisateurs pourront l'exécuter pour lancer l'Assistant d'installation d'IBM Cognos Transformer.

Les instructions de cette rubrique sont destinées à l'installateur ou l'administrateur. Si vous êtes le spécialiste métier ou un modélisateur Transformer et souhaitez télécharger et utiliser Transformer, reportez-vous à «Déploiement d'IBM Cognos Transformer pour les modélisateurs», à la page 147

### Avant de commencer

Avant de mettre le fichier d'installation à la disposition des modélisateurs Transformer, vous devez configurer d'autres ressources et droits d'accès :

- Le logiciel du client de base de données est installé (ou à la disposition des modélisateurs en vue d'une installation) sur les ordinateurs Transformer utilisés pour accéder aux sources de données IBM Cognos Analytics ou IBM Cognos Series 7 IQD.
- Les modélisateurs doivent disposer de privilèges pour créer une source de données dans IBM Cognos Administration.

  Ils n'ont pas besoin d'un accès direct à cette application. Ils peuvent créer et mettre à jour des sources de données à l'aide de Transformer ou d'outils de ligne de commande. Vous pouvez fournir aux modélisateurs un dossier sécurisé sur le portail, dans lequel ils pourront publier les packs de PowerCubes.
- Les modélisateurs doivent avoir accès à un emplacement dans lequel stocker les PowerCubes créés.

Cet emplacement doit également être accessible pour le service IBM Cognos. Il peut s'agir d'un dossier de partage sécurisé sur un réseau local.

- Pour créer des PowerCubes sur un serveur Transformer spécifique, les modélisateurs doivent disposer de privilèges FTP pour transférer les modèles et de privilèges d'exécution pour créer les cubes sur ce serveur.

  Ils peuvent transférer les modèles et créer les cubes à l'aide de scripts. Ils peuvent également utiliser des méthodes automatisées pour créer les PowerCubes. Pour plus d'informations, voir le *Guide d'administration et de sécurité*.

### Procédure

1. Insérez le CD du produit de modélisation IBM Cognos Transformer.
2. Si la page **Accueil** de l'Assistant d'installation s'affiche, quittez l'assistant.
3. Sur le CD, recherchez le fichier C8transformerinstall.exe.
4. Copiez le fichier dans un emplacement sécurisé auquel les modélisateurs Transformer ont accès.

## Données de configuration pour les modélisateurs Transformer

Si vous souhaitez que le fichier d'installation de Transformer soit accessible aux modélisateurs Transformer, ces derniers doivent disposer des paramètres de répartiteurs et de chiffrement pour configurer Transformer sur leur ordinateur local. Vous pouvez exporter la configuration d'un ordinateur Transformer afin de l'utiliser avec tous les autres ordinateurs Transformer. Les modélisateurs peuvent copier le fichier de configuration exporté dans leur répertoire d'installation Transformer, puis exécuter la commande permettant de configurer l'ordinateur Transformer en mode silencieux.

Les instructions de cette rubrique sont destinées à l'installateur ou l'administrateur. Si vous êtes le spécialiste métier ou un modélisateur Transformer et souhaitez télécharger et utiliser Transformer, reportez-vous à «Déploiement d'IBM Cognos Transformer pour les modélisateurs», à la page 147

Si vous avez mis à jour les fichiers coglocale, cogtr.xml ou cs7g.ini sur l'ordinateur Transformer, vous devez les copier dans l'emplacement Web ou de réseau local (LAN) pour que les modélisateurs Transformer puissent les télécharger sur leur ordinateur.

Pour que la configuration puisse être exportée, l'ordinateur source doit disposer des mêmes composants IBM Cognos Analytics que les ordinateurs des modélisateurs qui travaillent avec Transformer «Communication entre Transformer et Cognos Analytics», à la page 141.

**Exportation de la configuration de Transformer :**

Utilisez IBM Cognos Configuration pour exporter la configuration d'un ordinateur Transformer afin de l'utiliser avec tous les autres ordinateurs Transformer.

**Procédure**

1. Dans IBM Cognos Configuration, dans le menu **Fichier**, cliquez sur **Exporter en tant que**.
2. Si vous voulez exporter la configuration actuelle vers un autre dossier, dans la zone **Rechercher dans**, localisez et ouvrez le dossier.

   Veillez à ce que le dossier soit protégé contre tout accès non autorisé ou inapproprié.

3. Dans la zone **Nom de fichier**, saisissez un nom pour le fichier de configuration.
4. Cliquez sur **Enregistrer**.
5. Renommez le fichier exporté en cogstartup.xml.
6. Copiez le fichier cogstartup.xml exporté depuis l'ordinateur source vers l'emplacement Web ou LAN où réside le fichier d'installation de Transformer.
7. Si vous avez modifié la configuration globale sur l'ordinateur source, copiez le fichier coglocale.xml depuis l'ordinateur source vers l'emplacement Web ou LAN où réside le fichier d'installation de Transformer.

   L'emplacement par défaut du fichier coglocale.xml est *emplacement_installation*/configuration.

**Copie des fichiers de configuration de Transformer mis à jour :**

Si vous avez mis à jour des fichiers de configuration, vous devez les copier au même emplacement que le fichier d'installation de Transformer.

**Procédure**

1. Si vous avez mis à jour le fichier cogtr.xml, copiez-le depuis le répertoire `emplacement_installation/configuration`, dans le même emplacement Web ou de réseau local que le fichier d'installation de Transformer.
2. Si vous avez mis à jour le fichier cs7g.ini, copiez-le depuis le répertoire `emplacement_installation/CS7Gateways/bin`, dans le même emplacement Web ou de réseau local que le fichier d'installation de Transformer.

## Déploiement d'IBM Cognos Transformer pour les modélisateurs

Si vous êtes un spécialiste métier ou un modélisateur Transformer, vous devez maintenant déployer Transformer de façon à pouvoir créer des PowerCubes et les publier à l'intention des utilisateurs ou groupes sélectionnés.

Si vous n'avez pas effectué l'installation, suivez la procédure d'installation de Transformer. Pour configurer Transformer de façon qu'il puisse communiquer avec le répartiteur IBM Cognos Analytics, suivez la procédure de configuration de Transformer.

Pour prendre en charge l'utilisation des sources de données IBM Cognos Analytics (y compris les packs et rapports) dans Transformer, veillez à ce que le client de base de données soit installé sur l'ordinateur Transformer.

**Installation de Transformer :**

En tant que spécialiste métier ou un modélisateur Transformer, procédez comme suit pour installer Transformer depuis l'emplacement Web ou LAN fourni par l'administrateur.

**Procédure**

1. Dans l'emplacement Web ou de réseau local (LAN) indiqué par l'administrateur, exécutez le fichier c8transformerinstall.exe.
2. Suivez les instructions de l'Assistant d'installation et copiez les fichiers requis sur votre ordinateur.

   **Conseil :** Le composant Series 7 IQD Bridge n'est pas pris en charge sous Linux.
3. Sur la page **Terminer** de l'assistant, cliquez sur **Terminer**.

**Que faire ensuite**

Le *Guide des commandes UNIX d'IBM Cognos Transformer* vous fournit la syntaxe des options de ligne de commande UNIX prises en charge par Cognos Transformer. Vous pouvez accéder à ce document dans IBM Cognos Analytics Knowledge Center (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0).

**Configuration de Transformer :**

En tant que spécialiste métier ou un modélisateur Transformer, procédez comme suit pour configurer Transformer.

**Procédure**

1. Accédez à l'emplacement Web ou LAN où réside le fichier d'installation de Transformer.
2. Si des fichiers .xml sont présents, copiez-les vers le répertoire *emplacement_Transformer*\configuration, où *emplacement_Transformer* est le répertoire d'installation de Transformer.
3. Si un fichier .ini est présent, copiez-le dans le répertoire *emplacement_Transformer*\CS7Gateways\bin.
4. Accédez au répertoire *emplacement_Transformer*\bin.
5. Saisissez la commande de configuration :

   ```
   ./cogconfig.bat -s
   ```

   IBM Cognos Configuration applique les paramètres de configuration spécifiés dans la copie locale du fichier cogstartup.xml, chiffre les données d'identification, crée des certificats numériques et démarre les services IBM Cognos.
6. Pour tester IBM Cognos Transformer, depuis le menu **Démarrer**, accédez à Programmes et cliquez sur **IBM Cognos Transformer**.

   Si la fenêtre **Transformer** s'affiche, votre installation fonctionne.
7. Une fois que Transformer est installé et s'exécute correctement, supprimez les fichiers d'installation extraits du fichier d'installation.

# Chapitre 7. Options de configuration

Après avoir installé et configuré les composants d'IBM Cognos, vous pouvez modifier la configuration en fonction de votre environnement. Initialement, les paramètres par défaut servent à configurer les composants. Toutefois, vous pouvez modifier ces paramètres par défaut si les conditions rendent les choix par défaut inadéquats ou si vous souhaitez qu'ils soient plus adaptés à votre environnement.

Vous pouvez, par exemple, configurer les fonctions d'IBM Cognos Application Firewall ou indiquer la quantité de ressources utilisées par les composants d'IBM Cognos. Vous pouvez également afficher le contenu d'IBM Cognos à l'aide d'un autre portail en configurant Portal Services.

Les composants d'IBM Cognos peuvent être configurés pour l'utilisation d'autres ressources, telles que l'emploi d'un fournisseur d'authentification et l'activation du code d'accès unique pour les utilisateurs et la connexion à la base de données.

Si vous utilisez un système d'équilibrage de charge dans votre environnement, vous pouvez modifier les paramètres pour améliorer les performances. Par exemple, vous pouvez équilibrer des demandes parmi les répartiteurs en modifiant leur capacité de traitement ou en définissant le nombre maximal et minimal de processus et de connexions. Pour en savoir davantage sur l'optimisation des performances des serveurs, reportez-vous au *Guide d'administration et de sécurité*.

Pour toutes les installations sous Microsoft Windows et la plupart des installations sous UNIX et Linux, utilisez IBM Cognos Configuration pour configurer les paramètres. Cependant, si la console attachée à l'ordinateur UNIX ou Linux sur lequel vous installez les composants d'IBM Cognos ne prend pas en charge une interface utilisateur graphique Java, vous devez éditer manuellement le fichier `cogstartup.xml` dans le répertoire *`emplacement_installation`*`/configuration` et exécuter ensuite IBM Cognos Configuration en mode silencieux.

Utilisez ces tâches facultatives pour personnaliser votre configuration afin que les composants d'IBM Cognos s'intègrent aisément à l'environnement existant.

## Changement de la version de Java utilisée par les composants IBM Cognos Analytics

Pour pouvoir fonctionner, les composants IBM Cognos Analytics ont besoin d'un JRE (Java Runtime Environment).

Vous pouvez changer la version Java lorsque vous voulez utiliser les composants d'IBM Cognos Analytics avec un serveur d'applications qui nécessite une version de JRE spécifique ou lorsque vous utilisez déjà une version JRE avec d'autres applications. Vous changez de version Java en définissant la variable d'environnement JAVA_HOME.

### JAVA_HOME

Définissez une variable d'environnement JAVA_HOME si vous souhaitez utiliser votre propre environnement Java.

Assurez-vous que la version JRE est prise en charge par les produits IBM Cognos.

Sous Microsoft Windows, si vous ne disposez pas d'une variable JAVA_HOME, les fichiers JRE fournis avec l'installation sont utilisés.

Pour vérifier que votre JRE est pris en charge, consultez le site IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047186).

## Fichier de règles JCE à accès illimité

Les environnements JRE incluent un fichier de règles à accès limité qui vous cantonne à certains algorithmes de cryptographie et à certaines suites de chiffrement. Si vous avez besoin d'algorithmes de cryptographie et de suites de chiffrement plus nombreux que ceux indiqués dans IBM Cognos Configuration, vous pouvez télécharger et installer le fichier de règles JCE à accès illimité.

Pour Java fourni par IBM, le fichier de règles JCE à accès non limité est disponible sur le site Web d'IBM (www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).

## Procédure

1. Lancez Cognos Configuration.
2. Cliquez sur **Fichier** > **Exporter en tant que...** et exportez la configuration dans un fichier texte tel que `export_cogstartup.xml` dans le dossier `configuration`. Quittez Cognos Configuration.
3. Sauvegardez les dossiers et les fichiers suivants :
   - **Fichiers**
   - *emplacement_installation/configuration/cogstartup.xml*
   - *emplacement_installation/configuration/caSerial*
   - **Dossiers**
   - *emplacement_installation/configuration/csk*
   - *emplacement_installation/configuration/certs*
4. Supprimez les dossiers et les fichiers que vous avez sauvegardés, **sauf** le dossier *emplacement_installation*`/configuration/certs/mobile`. Supprimez tous les autres fichiers dans le dossier *emplacement_installation*`/configuration/certs`.
5. Renommez le fichier de configuration de sauvegarde que vous avez créé à l'**étape 2** en lui donnant le nom `cogstartup.xml`.
6. Définissez la variable d'environnement système JAVA_HOME sur l'environnement d'exécution Java que vous voulez utiliser. Vérifiez que le fichier bcprov est prêt pour ce JRE dans le dossier `jre/lib/ext`.
7. Lancez Cognos Configuration, enregistrez la configuration et redémarrez le serveur. Vous pouvez aussi lancer la commande suivante sur la ligne de commande depuis le dossier *emplacement_installation*`/bin64` : `cogconfig.bat -s`.

   Cette opération recréera les clés pour le nouveau JRE.

## Modification des paramètres de configuration par défaut

Lorsque vous installez des composants d'IBM Cognos, l'installation utilise des paramètres de configuration par défaut. Si vous devez rejeter ces valeurs par défaut, par exemple, si un port est également utilisé par un autre processus, utilisez IBM Cognos Configuration pour changer la valeur.

Si vous modifiez la valeur d'une propriété, vous devez enregistrer la configuration et redémarrer le service IBM Cognos pour appliquer les nouveaux paramètres à votre ordinateur.

Pour les installations réparties, assurez-vous d'avoir configuré tous les ordinateurs sur lesquels vous avez installé Content Manager avant de modifier les paramètres de configuration par défaut sur les autres ordinateurs IBM Cognos. Vous pouvez par exemple :

- modifier un URI
- gérer le groupe de configuration
- gérer le serveur de configuration
- définir les paramètres cryptographiques
- configurer les composants IBM Cognos pour utiliser IBM Cognos Application Firewall
- définir les propriétés des fichiers temporaires
- configurer la passerelle pour utiliser un espace-noms
- activer et désactiver des services
- configurer des polices
- changer la police par défaut des rapports
- enregistrer la sortie de rapport dans un fichier système
- modifier l'emplacement des graphiques de type Carte pour Reporting
- modifier la base de données de notification,

Après avoir modifié le comportement par défaut des composants d'IBM Cognos afin qu'il s'adapte mieux à votre environnement IBM Cognos, vous pouvez configurer un fournisseur d'authentification, puis installer et configurer Framework Manager.

## Paramètres de port et d'URI

Vous pouvez modifier certains éléments d'un URI selon votre environnement. Un URI d'IBM Cognos contient les éléments suivants :

Des informations supplémentaires sur les ports sont disponibles dans la rubrique suivante : «Vérification des paramètres de port par défaut», à la page 7

- Pour un URI de Content Manager, un URI du répartiteur destiné aux applications externes ou un URI du répartiteur

  ```
  protocole://nom_hôte_ou_adresse_IP:port/racine_contexte/chemin_alias
  ```

- Pour un URI de passerelle ou un URI de contenu Web

  ```
  protocole://nom_hôte_ou_adresse_IP:port/répertoire_virtuel/
  application_passerelle
  ```

  ou

  ```
  protocole://nom_hôte_ou_adresse_IP:port/racine_contexte/chemin_alias
  ```

**Important :** Pour les configurations HTTPS/SSL, veillez à bien utiliser des noms d'hôte complets pour les URI.

Les éléments sont décrits dans le tableau suivant.

*Tableau 20. Descriptions et éléments de l'identificateur URI IBM Cognos*

| Elément | Description |
|---|---|
| protocole | Indique le protocole utilisé pour demander et transmettre les informations ; il s'agit de HTTP (Hyper Text Transfer Protocol) ou de HTTPS (Hyper Text Transfer Protocol Sécurisé).<br><br>**Exemple :** http ou https |
| nom d'hôte ou adresse IP | Indique l'identité de l'hôte sur le réseau. Vous pouvez utiliser une adresse IP, un nom d'ordinateur ou un nom de domaine qualifié complet.<br><br>Dans le cadre d'une installation répartie, vous devez modifier l'élément localhost d'un URI.<br><br>Dans un environnement mixte de serveurs UNIX et Microsoft Windows, assurez-vous que les noms d'hôtes peuvent être convertis en adresses IP par tous les serveurs présents dans l'environnement.<br><br>**Exemple :** localhost ou 192.168.0.1 ou [2001:0db8:0000:0000:0000:148:57ab]:80 |
| port | Indique le port sur lequel le système hôte écoute les demandes.<br><br>Le port par défaut pour les services IBM Cognos Analytics est 9300. Le port par défaut d'un serveur Web est 80.<br><br>**Exemple :** 9300 ou 80 |
| racine de contexte | Utilisée par le serveur d'applications pour déterminer le contexte de l'application afin que la demande puisse être acheminée vers l'application Web appropriée en vue de son traitement.<br><br>**Exemple :** p2pd |
| chemin d'alias | Utilisé par le serveur d'applications pour acheminer une demande vers le composant approprié dans une application Web.<br><br>Le chemin d'alias ne doit pas être modifié, sinon les composants d'IBM Cognos ne fonctionneront pas correctement.<br><br>**Exemple :** servlet/dispatch |
| répertoire virtuel | Utilisé par le serveur Web pour mapper un répertoire virtuel ou un alias avec un emplacement physique.<br><br>Par exemple, dans l'URI de passerelle par défaut http://localhost:80/ibmcognos/cgi-bin/cognos.cgi, le répertoire virtuel est ibmcognos/cgi-bin.<br><br>**Exemple :** ibmcognos/ |

*Tableau 20. Descriptions et éléments de l'identificateur URI IBM Cognos (suite)*

| Elément | Description |
|---|---|
| application passerelle | Indique le nom de l'application passerelle Cognos utilisée.<br><br>Par exemple, si vous accédez aux composants d'IBM Cognos à l'aide d'une interface CGI (Common Gateway Interface), l'application passerelle par défaut correspondra à cognos.cgi.<br><br>**Exemple :** cognos.cgi |

Si vous utilisez la collaboration avec IBM Connections, assurez-vous d'inclure le domaine complet pour toutes les entrées de noms d'hôte dans IBM Cognos Configuration. Si, par exemple, votre ordinateur porte le nom MonOrdinateur et que votre domaine est intitulé **MaSociété.com**, pour la valeur de nom_hôte_ou_adresse_IP, utilisez **MonOrdinateur.MaSociété.com**. Le nom de domaine doit être inclus pour que IBM Connections puisse autoriser l'accès.

## Modification d'un port ou d'un paramètre URI

Procédez comme suit pour changer les propriétés URI dans IBM Cognos Configuration.

### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur le groupe ou composant approprié :
   - Pour changer un élément du répartiteur, cliquez sur l'option **Environnement**.
   - Pour changer un élément du serveur de journalisation local, dans la section **Environnement**, cliquez sur l'option **Journalisation**.
3. Dans la fenêtre **Propriétés**, cliquez sur la zone **Valeur** à côté de la propriété d'URI que vous voulez modifier.
4. Sélectionnez l'élément et saisissez les nouvelles informations.
   - Pour changer le port utilisé par le répartiteur local, vous devez modifier la valeur de la propriété URI interne du répartiteur. Etant donné que le changement a une incidence sur tous les URI définis en fonction du répartiteur local, vous devez modifier ceux de tous les composants locaux.
   - Si vous changez le port du répartiteur dans son URI, veillez à indiquer le nouveau numéro de port lorsque vous configurez des ordinateurs distants utilisant les services du répartiteur, de Content Manager et du kit SDK (Software Development Kit) sur ce système.
   - Pour les configurations HTTPS/SSL, veillez à bien utiliser des noms d'hôte complets pour les URI.
5. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Modification du port de service des jeux de données dans Cognos Analytics 11.0.6 à 11.0.8

Le port de service des jeux de données IBM Cognos Analytics est saisi dynamiquement lors du premier démarrage Cognos Analytics.

Le port est stocké et peut être référencé dans le fichier *emplacement_installation*`/wlp/usr/servers/dataset-service/bootstrap.properties`.

Le numéro de port vaut le numéro de port du répartiteur Cognos Analytics plus 1. Par exemple, 9300 +1 = 9301 (par défaut).

Une fois le port de service des jeux de données affecté et stocké, il ne peut plus être mis à jour ou modifié, même si vous modifiez le port du répartiteur. Cependant, vous pouvez forcer le service de jeux de données à ressaisir le port, ou bien coder en dur le port dans le fichier `bootstrap.properties` de manière à imposer un port spécifique au service de requête.

Comme le port de service des jeux de données est affecté lors du premier démarrage deCognos Analytics, nous vous recommandons de démarrer tous les logiciels avant de démarrer Cognos Analytics. Ainsi, le service de jeux de données n'occupe pas un port déjà utilisé par un autre produit.

Procédez comme suit pour forcer le service de jeux de données à occuper un nouveau port dynamiquement :

1. Arrêtez l'instance Cognos Analytics que vous souhaitez mettre à jour.
2. Ouvrez le fichier *emplacement_d'installation*`/wlp/usr/servers/dataset-service/bootstrap.properties` dans un éditeur de texte.
3. Affectez au paramètre `http.port` la valeur 0, de la manière suivante : `http.port=0`
4. Démarrez Cognos Analytics. Le paramètre `http.port` est ressaisi lors du démarrage du produit.
5. Consultez le fichier `bootstrap.properties` pour voir le numéro de port affecté.

Procédez comme suit pour imposer un port spécifique au service de jeux de données :

1. Arrêtez l'instance Cognos Analytics que vous souhaitez mettre à jour.
2. Ouvrez le fichier *emplacement_d'installation*`/wlp/usr/servers/dataset-service/bootstrap.properties` dans un éditeur de texte.
3. Affectez la valeur souhaitée au paramètre `http.port`. Par exemple, `http.port=9876`.
4. Démarrez Cognos Analytics. Le paramètre `http.port` prend sa valeur lors du démarrage du produit.
5. Consultez le fichier `bootstrap.properties` pour vérifier que le numéro de port souhaité est affecté.

Une fois Cognos Analytics démarré, vérifiez via netstat que le service de jeux de données écoute le port correspondant au paramètre `http.port`.

**Conseil :** A partir de Cognos Analytics 11.0.9, le port de service des jeux de données peut être configuré dans IBM Cognos Configuration.

## Gestion du groupe de configuration

11.0.4

Le groupe de configuration définit un groupe de serveurs qui partagent une configuration. Cette étape est essentielle dans les installations multiserveurs, pour que les valeurs de configuration restent disponibles et cohérentes sur tous les noeuds, même après les partitions du réseau. L'hôte de contact du groupe de configuration s'exécute sur la même instance que le gestionnaire de contenu actif.

### Pourquoi et quand exécuter cette tâche

- Dans une installation **simple**, si vous augmentez la capacité d'un système en cours d'exécution en sélectionnant l'option **Connexion et installation**, ces valeurs sont définies automatiquement.

- Pour une **première installation personnalisée** où la machine est configurée en tant que Content Manager actif, ces valeurs sont définies automatiquement.
- Pour une installation avec l'option **Connexion et installation**, si vous parvenez à vous connecter au noeud Content Manager à l'aide de l'URL Cognos Analytics au cours de l'installation, ces valeurs sont définies automatiquement.
- Pour une installation de type **Première installation personnalisée**, dans laquelle la machine Content Manager est configurée comme étant en veille, ou si vous choisissez de continuer malgré l'échec de la validation de l'URL de la passerelle au cours de l'installation, vous devez configurer ces propriétés en suivant la procédure ci-après.

## Procédure

1. Démarrez Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Configuration locale**, cliquez sur **Environnement**.
3. Cliquez sur **Groupe de configuration**.
4. Pour définir les valeurs correctes :
   - S'il s'agit de l'installation du serveur Content Manager active, vous pouvez définir les valeurs du serveur local en cliquant à l'aide du bouton droit de la souris sur **Redéfinir aux valeurs par défaut**.
   - S'il s'agit de l'installation du serveur Content Manager en veille, ou d'une installation de groupe de serveurs d'application, vous devez définir les valeurs.
     a. Cliquez sur **Groupe de configuration** à l'aide du bouton droit de la souris, puis cliquez sur le bouton **Extraire** pour lancer la boîte de dialogue **Extraction des serveurs de configuration**.

        11.0.6 Si l'instance active de Content Manager est compatible SSL, vous pourrez extraire les propriétés du groupe de configuration **une fois que** l'URL et les autres propriétés de Content Manager ont été correctement configurées et sauvegardées.

     b. Entrez les informations correctes pour accéder au serveur Content Manager actif, puis cliquez sur **OK**.

        **ID utilisateur** : ID doté des privilèges d'administration sur le serveur.

        **Mot de passe** : mot de passe associé à l'ID utilisateur.

        **ID espace-noms** : cette valeur se trouve dans la ressource **Sécurité**, **Authentification**. Par exemple, `CognosEx`

        **URL Cognos Analytics** : URL utilisée pour exécuter Cognos Analytics. Par exemple, `http://myserver:9300/bi`
   - Si vous ne parvenez pas à extraire les valeurs à l'aide de l'option **Extraire**, vous pouvez définir les valeurs manuellement. Suivez les instructions dans la partie inférieure de la fenêtre des propriétés pour chacune des propriétés.

     Assurez-vous que les deux ports sous **Paramètres du membre local** sont des ports locaux distincts non utilisés. Si toutes les applications sur la machine étaient actives au cours de l'installation, ces ports doivent déjà être définis avec des ports disponibles.

     **Important :** Ces ports doivent être ouverts pour le trafic entrant et sortant.

     – Le **port de synchronisation de membre** est le port local utilisé pour la communication réseau qui transfère et synchronise les informations de configuration d'un serveur à l'autre. Chaque installation doit pouvoir communiquer avec le noeud `MutualAuthSSLHttpEndpoint` des autres

installations. Par exemple, tout pare-feu installé entre les composants d'application et de données doit être ouvert sur ce port. Le noeud httpEndpoint est utilisé exclusivement pour la communication interne entre une instance Cognos Analytics et une autre. Le port par défaut est 4300.

- Le **port de coordination de membre** est le port local utilisé pour la communication réseau pour la coordination de groupe. Ce port est utilisé pour détecter et rejoindre un groupe, ainsi que pour conserver une liste à jour des membres du groupe de configuration. Dans l'installation de Content Manager principale, le port de contact du groupe est le même. Chaque installation doit pouvoir communiquer avec les autres installations sur le port de coordination de groupe, ce qui exige que tout pare-feu entre les éléments de l'installation soit ouvert pour ce port. Le port par défaut est 5701.

5. Enregistrez la configuration.

# Gestion du serveur de configuration

11.0.3

Le serveur de configuration identifie le serveur qui gère les valeurs de configuration. Cette étape est essentielle dans les installations multiserveurs, pour que les valeurs de configuration restent disponibles et cohérentes sur tous les noeuds, même après les partitions du réseau. Le serveur de configuration s'exécute sur la même instance que le gestionnaire de contenu actif.

Applicable à la version 11.0.3 (remplacé dans la version 11.0.4 par Groupe de configuration).

## Pourquoi et quand exécuter cette tâche

Dans les installations faciles, si vous augmentez la capacité d'un système en cours d'exécution en sélectionnant l'option de connexion et d'installation, cette valeur est définie automatiquement.

## Procédure

1. Démarrez Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Configuration locale**, cliquez sur **Environnement**.
3. Faites défiler la fenêtre **Environnement - Propriétés du groupe** jusqu'à la catégorie **Autres paramètres de l'URI**, et cliquez sur **Serveur de configuration**.
4. Pour définir la valeur correcte :
   - S'il s'agit de l'installation du serveur Content Manager active, vous pouvez définir la valeur vers le serveur local en cliquant à l'aide du bouton droit de la souris sur **Redéfinir aux valeurs par défaut**.
   - S'il s'agit de l'installation du serveur Content Manager en veille, ou d'une installation de groupe de serveurs d'application, vous devez définir la valeur en cliquant sur l'icône Editer  pour lancer la boîte de dialogue.
     a. Dans la boîte de dialogue **Valeur - Serveur de configuration**, cliquez sur le bouton **Extraire** pour lancer la boîte de dialogue **Extraction des serveurs de configuration**. Entrez les informations correctes pour accéder au serveur Content Manager actif, puis cliquez sur **OK**.

        **ID utilisateur** : ID doté des privilèges d'administration sur le serveur.

**Mot de passe** : mot de passe associé à l'ID utilisateur.

**ID espace-noms** : cette valeur se trouve dans la ressource **Sécurité**, **Authentification**. Par exemple, `CognosEx`

**URL Cognos Analytics** : URL utilisée pour exécuter Cognos Analytics. Par exemple, `http://myserver:9300/bi`

b. La valeur **Serveur de configuration** est extraite. Cliquez sur **OK** pour définir la valeur.

- Si vous ne parvenez pas à extraire la valeur à l'aide du bouton **Extraire**, vous pouvez la définir manuellement.
  a. Sur le serveur Content Manager actif, ouvrez *emplacement_installation*`/zookeeper/conf/zoo.cfg`
  b. Recherchez les deux paramètres suivants :

     ```
     server.1=Myhost.ibm.com:2888:3888
     clientPort=2181
     ```

  c. Concaténez les deux valeurs avec un point-virgule comme suit :

     ```
     Myhost.ibm.com:2888:3888;2181
     ```

  d. Entrez cette valeur dans la propriété.

5. Enregistrez la configuration.

## Configuration des paramètres cryptographiques

Les composants d'IBM Cognos ont besoin d'un fournisseur cryptographique, sans lequel ils ne peuvent pas fonctionner. Si vous supprimez le fournisseur cryptographique par défaut, vous devez en configurer un autre pour le remplacer.

Vous pouvez configurer les paramètres cryptographiques suivants :

- paramètres cryptographiques généraux
- paramètres du fournisseur cryptographique par défaut
- paramètres d'un fournisseur cryptographique au sein d'une de sécurité Entrust

### Configuration des paramètres cryptographiques généraux

Dans une installation répartie, les ordinateurs IBM Cognos communiquent avec Content Manager pour établir l'approbation et obtenir certaines clés cryptographiques de Content Manager.

Si vous modifiez les clés cryptographiques dans Content Manager, en modifiant par exemple des serveurs d'applications ou en installant de nouveau Content Manager, vous devez supprimer les clés cryptographiques des autres ordinateurs IBM Cognos. Enregistrez ensuite la configuration de tous les ordinateurs afin qu'ils obtiennent les nouvelles clés cryptographiques de Content Manager. Par ailleurs, tous les composants d'IBM Cognos dans une installation répartie doivent être configurés avec les mêmes paramètres de fournisseur cryptographique.

En outre, dans une installation répartie, la clé symétrique ne doit être stockée que sur les ordinateurs sur lesquels Content Manager a été installé.

Vous pouvez configurer les paramètres cryptographiques généraux suivants :

- Conformité aux standards

  Définit les standards cryptographiques à utiliser, IBM Cognos ou NIST SP 800-131A.
- Propriétés du magasin de clés symétriques communes (CSK).

  IBM Cognos utilise la CSK pour chiffrer et déchiffrer les données.

- Paramètres SSL (Secure Sockets Layer)

  Ils incluent les paramètres d'authentification mutuelle, de confidentialité et de protocole TLS (Transport Layer Security) SSL.

  **Remarque :** Le protocole TLS est un ensemble de règles de chiffrement qui s'appuie sur des certificats vérifiés et des clés de chiffrement pour sécuriser les communications sur Internet. TLS est une mise à jour du protocole SSL. Sélectionnez 1.1, 1.2 ou le paramètre de combinaison.
- Paramètres d'algorithme avancés

  Il s'agit d'algorithmes de signature et de prétraitement.

## Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, dans la section **Sécurité**, cliquez sur **Cryptographie**.
3. Dans la fenêtre **Propriétés**, modifiez les valeurs par défaut en cliquant sur la zone **Valeur**, puis en sélectionnant la valeur appropriée :
   - Les options de la conformité aux standards sont IBM Cognos et NIST SP 800-131A. Cette valeur peut provoquer l'échec de l'enregistrement si d'autres paramètres ne sont pas autorisés dans le standard sélectionné. Vous devez sélectionner un autre algorithme ou modifier les choix de conformité aux standards. Il peut être nécessaire d'installer les fichiers Unlimited Jurisdiction Policy correspondant à votre JRE pour activer tous les algorithmes pris en charge. Vous pouvez vous les procurer auprès d'IBM.
   - Sur des ordinateurs ne disposant pas de Content Manager, si vous ne voulez pas conserver les clés symétriques communes (CSK) localement, dans la section **Paramètres CSK**, définissez l'option **Voulez-vous stocker la clé symétrique localement ?** sur **Faux**.

     Lorsque l'option **Voulez-vous stocker la clé symétrique localement ?** est définie sur **Faux**, la clé est obtenue auprès de Content Manager, le cas échéant. La propriété **Emplacement du magasin de clés symétriques communes** est ignorée.
   - Si vous souhaitez que les ordinateurs situés à chaque extrémité d'une transmission prouvent leur identité, dans la section **Paramètres SSL**, définissez l'option **Voulez-vous utiliser une authentification mutuelle ?** sur **Vrai**.

     Ne modifiez pas le paramètre **Utilisation de la confidentialité**.
   - Si vous souhaitez modifier l'algorithme de prétraitement, sélectionnez une autre valeur pour la propriété **Algorithme de prétraitement**.
4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
5. Le test du fournisseur cryptographique doit être effectué sur une passerelle uniquement. Dans la fenêtre **Explorateur**, cliquez avec le bouton droit sur **Cryptographie**, puis sélectionnez **Tester**.

   Les composants d'IBM Cognos BI vérifient la disponibilité de la clé symétrique.

## Résultats

Après avoir configuré les paramètres cryptographiques, les mots de passe de votre configuration et toutes les données que vous créez sont chiffrés.

## Configuration du fournisseur cryptographique par défaut

Vous pouvez configurer des paramètres cryptographiques pour le fournisseur cryptographique par défaut.

Les paramètres suivants peuvent être configurés :

- Algorithmes et suites de chiffrement
- Paramètres de nom d'identité
- Paramètres du magasin de clés de chiffrement

  La paire de clés de chiffrement comprend la clé privée utilisée pour chiffrer les données et la clé publique utilisée pour les déchiffrer.
- Paramètres de l'autorité de certification

  L'autorité de certification est l'autorité de certification par défaut ou une autre autorité de certification.
- Paramètres de la propriété Autre nom de sujet

  La propriété Autre nom de sujet (Subject Alternative Name) sert à valider l'origine d'un certificat SSL.

### Procédure

1. Si vous utilisez un environnement d'exécution Java différent de celui fourni avec le serveur IBM Cognos, accédez au répertoire *emplacement_installation*/jre/lib/ext.
2. Copiez bcprov-jdk*version*.jar vers *emplacement_JRE*/lib/ext.
3. Si vous utilisez un environnement d'exécution Java autre que ceux fournis par IBM, vous devez également télécharger et installer le fichier de règles JCE (Java Cryptograph Extension) à accès illimité pour votre environnement d'exécution Java afin de vous assurer que tous les algorithmes et toutes les suites de chiffrement apparaissent dans IBM Cognos Configuration.
4. Démarrez IBM Cognos Configuration.
5. Dans la fenêtre **Explorateur**, dans la section **Sécurité**, **Cryptographie**, cliquez sur l'option **Cognos**.
6. Dans la fenêtre **Propriétés**, modifiez les propriétés selon les besoins.

   **Conseil :** Pour plus d'informations sur chaque propriété, voir la description de propriété dans IBM Cognos Configuration lorsque vous cliquez sur une propriété.

   - Pour configurer l'algorithme de confidentialité, sous la propriété appropriée, **Algorithme de confidentialité** ou **Algorithme de confidentialité PDF**, cliquez sur la colonne **Valeur** et sélectionnez l'algorithme dans la liste déroulante.

     La valeur d'un algorithme de confidentialité détermine le mode de chiffrement des données qui est employé par les composants d'IBM Cognos. Par exemple, les mots de passe de base de données saisis dans IBM Cognos Configuration sont chiffrés lors de l'enregistrement de la configuration. L'algorithme sélectionné lors du chiffrement des données doit également être disponible pour que ces mêmes données puissent par la suite être déchiffrées.

     La disponibilité des algorithmes de confidentialité peut varier en cas de modifications apportées à votre environnement. C'est, par exemple, le cas si votre environnement d'exécution Java (Java Runtime Environment) a changé ou si vous avez installé un autre logiciel cryptographique sur l'ordinateur.

Vous devez vous assurer que le paramètre **Algorithme de confidentialité** sélectionné lors du chiffrement des données est également disponible lorsque vous souhaitez accéder à ces données.

Si vous avez apporté des modifications à un ordinateur, telles qu'une mise à niveau de l'environnement d'exécution Java ou l'installation d'un logiciel ayant entraîné la mise à niveau de l'environnement d'exécution Java, cela peut avoir une incidence sur les algorithmes de confidentialité. Pour que les algorithmes et les suites de chiffrement disponibles s'affichent dans IBM Cognos Configuration, téléchargez et installez le fichier de règles JCE (Java Cryptograph Extension) à accès illimité. Pour Java fourni par IBM, le fichier de règles JCE à accès illimité peut être téléchargé depuis le site Unrestricted JCE policy files (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).

- Pour ajuster les suites de chiffrement, sous **Algorithmes de cryptage pris en charge**, cliquez sur la colonne **Valeur** et sur l'icône Editer  .

  Supprimez les suites de chiffrement non pertinentes et déplacez les suites restantes vers le haut ou le bas de la liste de sorte que celles dont le niveau est le plus élevé se retrouvent en haut de la liste.

  Ne mélangez pas les suites de chiffrement comprises dans la plage de 40 à 56 bits avec celles de la plage de 128 à 168 bits.
- Pour modifier l'emplacement des clés de chiffrement, dans la section **Paramètres de clés de chiffrement**, définissez l'option **Emplacement du magasin de clés de chiffrement** sur le nouvel emplacement.
- Pour utiliser une autre autorité de certification, dans la section **Paramètres de l'autorité de certification**, définissez l'option **Voulez-vous utiliser une autorité de certification tierce ?** sur **Vrai**.

  Pour en savoir davantage, reportez-vous à la section «Configuration des composants IBM Cognos pour l'utilisation d'une autre autorité de certification», à la page 182.
- Si la configuration concerne HTTPS/SSL, remplacez le **nom usuel du serveur** (CAMUSER) par son nom de domaine complet.
- Pour configurer la propriété **Autre nom de sujet**, indiquez les **Noms DNS**, les **Adresses IP** et les **Adresses de courrier électronique** (facultatif) associées au certificat du serveur. Les valeurs sont ajoutées aux extensions Autre nom de sujet dans le certificat du serveur. Vous pouvez indiquer plusieurs valeurs pour chaque propriété. Séparez les valeurs à l'aide du caractère espace.

7. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

### Résultats

Si vous utilisez un autre serveur d'autorité de certification, configurez les composants d'IBM Cognos en conséquence. Pour en savoir davantage, reportez-vous à la section «Configuration des composants IBM Cognos pour l'utilisation d'une autre autorité de certification», à la page 182.

## Configuration des paramètres du fournisseur cryptographique au sein d'une infrastructure de sécurité Entrust

Pour configurer le chiffrement dans une infrastructure de sécurité Entrust, remplacez le fournisseur cryptographique par défaut dans IBM Cognos Configuration par un fournisseur configuré pour Entrust, puis mettez à jour les fichiers de sécurité dans votre environnement IBM Cognos.

## Avant de commencer

Vérifiez que les mots de passe du magasin de clés correspondent à celui de votre profil Entrust (EPF).

Pour éviter toute erreur au niveau de la passerelle, assurez-vous que le compte invité Internet dispose de droits de lecture et d'écriture sur le fichier Entrust `.epf` et de droits de lecture sur le fichier Entrust `.ual`.

## Procédure

1. Si vous utilisez un environnement d'exécution Java différent de celui fourni avec le serveur IBM Cognos, accédez au répertoire *emplacement_installation*/jre/lib/ext.
2. Copiez bcprov-jdk*version*.jar vers *emplacement_JRE*/lib/ext.
3. Assurez-vous que les fichiers IBM Cognos et Entrust ci-après figurent à l'emplacement où le JRE est installé :
   - Copiez le fichier `.jar` (par exemple `enttoolkit.jar`) issu du composant Entrust Authority Security Toolkit téléchargé depuis Entrust, vers le répertoire *emplacement_JRE*.
4. Pour que tous les algorithmes et les suites de chiffrement disponibles s'affichent dans IBM Cognos Configuration, téléchargez et installez le fichier de règles JCE (Java Cryptography Extension) à accès illimité. Pour Java fourni par IBM, le fichier de règles JCE à accès illimité peut être téléchargé depuis le site Unrestricted JCE policy files (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).
5. Démarrez IBM Cognos Configuration.
6. Dans la fenêtre **Explorateur**, sous le groupe **Sécurité**, cliquez sur l'option **Cryptographie**.
7. Dans la fenêtre **Propriétés**, dans la section **Paramètres d'algorithme avancés**, modifiez la valeur de l'**Algorithme de prétraitement** pour lui attribuer une valeur d'algorithme de prétraitement de message ou de hachage sécurisé des données correspondant à votre règle de sécurité.
8. Dans la fenêtre **Explorateur**, sous le groupe **Sécurité** et le composant **Cryptographie**, cliquez avec le bouton droit de la souris sur la ressource **IBM Cognos**, puis cliquez sur **Supprimer**.
9. Dans le groupe **Sécurité**, cliquez avec le bouton droit de la souris sur l'option **Cryptographie**, puis cliquez sur **Nouvelle ressource** > **Fournisseur**.
10. Dans la zone **Nom**, saisissez un nom pour le service de chiffrement que vous êtes en train de créer.
11. Dans la zone **Type**, cliquez sur la flèche, puis sur **Entrust** et cliquez sur **OK**.

    Une branche portant le nom que vous avez indiqué s'affiche sous l'option **Cryptographie**.
12. Cliquez sur la branche que vous avez créée.

    Les propriétés des ressources s'affichent dans la fenêtre des propriétés.
13. Dans la fenêtre **Propriétés des ressources**, saisissez les valeurs du tableau suivant :

*Tableau 21. Descriptions et valeurs de propriété de la cryptographie*

| Propriété | Description |
|---|---|
| Emplacement du fichier INI | Emplacement du fichier d'initialisation Entrust (.ini). |

*Tableau 21. Descriptions et valeurs de propriété de la cryptographie (suite)*

| Propriété | Description |
|---|---|
| Nom distinctif (DN) du fichier d'identité | Nom distinctif associé au profil de l'identité Entrust. |
| Emplacement du fichier d'identité | Emplacement du fichier de profil d'identification Entrust (.epf). |
| Utiliser la connexion du serveur Entrust | Paramètre qui vérifie si les utilisateurs doivent saisir un mot de passe pour se connecter à la PKI Entrust. |
| Mot de passe du fichier d'identité | Le mot de passe du profil Entrust doit correspondre à celui indiqué dans votre profil Entrust (EPF). |
| algorithme de confidentialité | Niveau de chiffrement requis pour respecter votre règle de sécurité. |
| Algorithme de confidentialité PDF | Algorithme de chiffrement appliqué lors du chiffrement des données PDF. |
| Suites de chiffrement prises en charge | Suites de chiffrement prises en charge dans votre environnement de sécurité. Supprimez les suites non pertinentes et réorganisez les suites restantes de la plus complexe à la plus simple. L'utilisation de la suite de chiffrement la plus sécurisée en premier est ainsi garantie. |
| Emplacement du magasin de clés de signature | Emplacement du magasin de clés qui contient les paires de clés de signature. |
| Emplacement du magasin de clés de chiffrement | Emplacement du magasin de clés qui contient les paires de clés de chiffrement. |

**Important :** Enregistrez le mot de passe dans un emplacement sécurisé.

14. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
15. Effectuez une mise à jour vers Entrust Java Toolkit 7.2 SP2 correctif 170072.

## IBM Cognos Application Firewall

IBM Cognos Application Firewall (CAF) analyse et valide les demandes HTTP et XML avant qu'elles ne soient traitées par les serveurs IBM Cognos. Il est possible qu'IBM Cognos Application Firewall modifie ces demandes.

IBM Cognos Application Firewall protège les produits IBM Cognos Web contre les données malveillantes. Les formes les plus courantes de données malveillantes sont les dépassements de tampon et les attaques de scripts intersites (XSS), par insertion de script dans des pages valides ou réacheminement vers un autre site Web.

Vous pouvez effectuer un suivi des activités du pare-feu en consultant le fichier journal, qui contient les demandes rejetées. Par défaut, les messages de journal sont stockés dans le fichier *emplacement_installation*/logs/cogaudit.log.

Si vous utilisez les fonctions de collaboration d'IBM Connections, vous devez ajouter le nom d'hôte, le domaine et le numéro de port sur lesquels IBM Connections s'exécute à la propriété **Domaines et hôtes valides** de Cognos Application Firewall.

Tous les paramètres de Cognos Application Firewall doivent être identiques sur tous les ordinateurs sur lesquels les composants du groupe de serveurs d'applications d'IBM Cognos sont installés dans un environnement distribué. Par exemple, si Cognos Application Firewall est désactivé sur certains ordinateurs et activé sur d'autres, un comportement inattendu et des erreurs peuvent se produire.

Les types d'URL suivants sont acceptés par la validation Cognos Application Firewall :

- Adresses URL complètes (absolues)

  Format : *protocole*://*hôte*:*port*/*chemin_accès*, où *protocole* est http ou https et où l'élément *hôte* est vérifié par rapport à la liste de domaines valides.
- Adresses URL relatives au répertoire d'installation Web

  Format : /*racine_installation_Web*/.*, où *racine_installation_Web* correspond au répertoire Web de la passerelle basé sur l'alias ibmcognos configuré sur votre serveur Web.

  Par exemple :

  /ibmcognos/ps/portal/images/action_delete.gif
- Adresses URL autorisées spécifiques, telles que (toutes sont sensibles à la casse) :

  about:blank

  JavaScript:window.close( )

  JavaScript:parent.close( )

  JavaScript:history.back( )

  parent.cancelErrorPage( )

  doCancel( )

## Configuration des composants IBM Cognos en vue de l'utilisation d'IBM Cognos Application Firewall

IBM Cognos Configuration vous permet également de modifier les paramètres de prise en charge des autres outils XSS et d'ajouter des noms d'hôte et de domaine à la liste des noms valides d'IBM Cognos.

### Procédure

1. Démarrez IBM Cognos Configuration à chaque emplacement où des composants du groupe de serveurs d'application sont installés.
2. Dans la fenêtre **Explorateur**, dans la section **Sécurité**, cliquez sur l'option **IBM Cognos Application Firewall**.
3. Dans la fenêtre **Propriétés**, définissez les valeurs adéquates pour la propriété **Activer l'option de validation du module CAF**.

   IBM Cognos Application Firewall est actif par défaut.

   **Important :** IBM Cognos Application Firewall est un composant essentiel de la sécurité IBM Cognos qui protège les données contre les intrusions. La désactivation d'IBM Cognos Application Firewall supprime cette protection. Dans des circonstances normales, ne désactivez pas IBM Cognos Application Firewall.
4. Si vous utilisez un autre outil XSS qui vérifie la présence de caractères spécifiques dans les paramètres de requête GET, ouvrez la fenêtre **Propriétés** (pour la propriété **Vérification XSS tierce activée**) et remplacez la valeur par **Vrai**.

   Les caractères par défaut interdits sont >, < et '.

5. Ajoutez les noms d'hôte et de domaine à la liste de noms valides d'IBM Cognos :
   - Pour la propriété **Domaines ou hôtes valides**, cliquez sur la valeur, puis sur l'icône Editer  .
   - Dans la boîte de dialogue **Valeur - Domaines ou hôtes valides**, cliquez sur **Ajouter**.

     Vous devez inclure les domaines de tous les liens hypertextes ajoutés sur le portail. Pour en savoir davantage, reportez-vous à la rubrique relative à la création d'une URL dans le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

     **Conseil :** Si vous accédez au détail depuis IBM Cognos Series 7 dans des rapports dans IBM Cognos Analytics, ajoutez les noms d'hôte des serveurs passerelles IBM Cognos Series 7 à la liste.
   - Dans la ligne blanche de la table, cliquez et saisissez le nom d'hôte ou de domaine.

     Pour autoriser un domaine et tous ses sous-domaines, insérez un caractère générique au début du nom de domaine.

     Par exemple, ***.masociété.com**

     Si vous utilisez les fonctions de collaboration avec IBM Connections, vous devez ajouter le nom d'hôte, le domaine et le numéro de port du profil IBM WebSphere sous lequel vous avez installé IBM Connections. A titre d'exemple, si vous avez installé IBM Connections sur un ordinateur appelé **monserveur** et que votre domaine se nomme **masociété.com**, vous devez ajouter **monserveur.masociété.com:9080**, où 9080 est le numéro de port d'IBM WebSphere sur lequel IBM Connections est exécuté.
   - Répétez les deux étapes précédentes (indiquées par des puces) pour chaque nom à ajouter.
   - Cliquez sur le bouton **OK**.

   IBM Cognos Application Firewall valide des noms d'hôte et de domaine pour protéger les adresses URL créées. Par défaut, IBM Cognos Application Firewall considère les noms de domaine issus des propriétés de configuration de l'environnement comme étant sécurisés. Il est utile d'ajouter des noms à la liste des noms et hôtes valides si vous devez rediriger des demandes vers des ordinateurs non-IBM Cognos à l'aide des fonctions Précédent ou Annuler ou bien lorsque vous accédez au détail dans d'autres installations de produits IBM Cognos.
6. Enregistrez la configuration.
7. Redémarrez les services.

## Chiffrement des propriétés des fichiers temporaires

Les fichiers temporaires sont utilisés dans IBM Cognos Analytics pour stocker les rapports récemment affichés et les données utilisées par les services pendant le traitement. Vous pouvez modifier l'emplacement des fichiers temporaires et chiffrer leur contenu.

Par défaut, les composants d'IBM Cognos stockent les fichiers temporaires dans le répertoire *emplacement_installation*\temp sans les chiffrer.

Pour un maximum de sécurité, refusez tout accès au répertoire temp, sauf pour le compte du service pour le démarrage des services IBM Cognos. Des droits en lecture et en écriture sont requis pour le compte du service.

### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, pour la propriété **Emplacement des fichiers temporaires**, indiquez le nouvel emplacement.
4. Si vous souhaitez que le contenu des fichiers temporaires soit chiffré, définissez la propriété **Voulez-vous chiffrer les fichiers temporaires ?** sur **Vrai**.
5. Assurez-vous que le compte utilisateur sous lequel les composants d'IBM Cognos Analytics fonctionnent dispose des privilèges appropriés sur l'emplacement des fichiers temporaires. Par exemple :
   - sous Microsoft Windows, privilèges de contrôle intégral
   - sous UNIX ou Linux, les privilèges de lecture et d'écriture

## Configuration de la passerelle pour l'utilisation d'un espace-noms

Si les composants d'IBM Cognos utilisent plusieurs espaces-noms ou si l'accès anonyme est activé et que les composants d'IBM Cognos n'utilisent qu'un seul espace-noms, vous pouvez configurer la passerelle pour qu'elle se connecte à un seul espace-noms. Les utilisateurs connectés au serveur Web sur lequel se trouve la passerelle ne sont pas invités à sélectionner une source d'authentification. Par exemple, si vous disposez de deux serveurs Web, vous pouvez les configurer Web afin qu'ils utilisent un espace-noms différent.

### Procédure

1. Sur l'ordinateur où se trouve la passerelle, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, dans la zone **Valeur** située en regard de la propriété **Espace noms de la passerelle**, saisissez l'identificateur de l'espace-noms que vous souhaitez utiliser.
4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
5. Redémarrez votre serveur Web.

## Activation et désactivation des services

Dans une installation répartie, vous pouvez envoyer certains types de demande à des ordinateurs spécifiques en activant ou en désactivant les services installés.

Par exemple, pour dédier un ordinateur à l'exécution et à la diffusion de rapports, vous pouvez désactiver le service de présentation sur un ordinateur hébergeant les composants du groupe de serveurs d'applications.

**Remarque :** Les valeurs par défaut des services de répartition et de présentation sont définies sur false sur les ordinateurs où seul Content Manager est installé. Pour tous les autres types d'installations, les valeurs par défaut sont définies sur " vrai ".

Si vous avez installé tous les composants sur plusieurs ordinateurs, vous pouvez désactiver les services appropriés sur chacun d'eux afin d'obtenir la configuration répartie requise. Les demandes sont envoyées uniquement aux répartiteurs sur lesquels un service donné est activé.

La désactivation d'un service empêche son chargement en mémoire. Une fois désactivés, les services ne démarrent plus et ne consomment donc plus de ressources. Le service ne s'exécute pas tant que vous ne l'activez pas.

Si vous désactivez le service du répartiteur, les services associés sont également désactivés. Seuls les services de répartiteur activés peuvent traiter des demandes.

**Restriction :** Lors d'un redémarrage manuel des services (si applicable), le service **ApacheDS - cognos** doit être démarré avant le service **IBM Cognos**.

### Activation et désactivation des services

Utilisez la procédure suivante pour désactiver les services sélectionnés dans les composants d'une installation répartie.

#### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Environnement**, cliquez sur l'option **Services IBM Cognos**.
3. Dans la fenêtre **Propriétés**, cliquez sur l'option **Valeur** en regard du service que vous souhaitez activer ou désactiver.

   Par défaut, tous les services sont activés.
4. Cliquez sur l'état approprié pour les services :
   - Pour désactiver le service, cliquez sur **Faux**.
   - Pour l'activer, cliquez sur **Vrai**.

   Lors d'un redémarrage manuel des services (si applicable), le service **ApacheDS - cognos** doit être démarré avant le service **IBM Cognos**.
5. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Configuration des polices

Les produits IBM Cognos utilisent des polices pour afficher des rapports au format PDF sur le serveur IBM Cognos. Ils utilisent également des polices pour afficher les graphiques utilisés dans les rapports aux formats PDF et HTML.

Pour afficher correctement une version de rapport, les polices doivent être disponibles à l'endroit où le rapport ou le graphique est affiché. Dans le cas des graphiques et des rapports au format PDF, les polices doivent être installées sur le serveur IBM Cognos. Si la police demandée n'est pas disponible, les composants d'IBM Cognos la remplacent par une autre.

Etant donné que les rapports au format HTML s'affichent dans un navigateur, les polices requises doivent être installées sur l'ordinateur de chaque utilisateur d'IBM Cognos appelé à visualiser le rapport. Si une police n'est pas disponible, le navigateur la remplace par une autre.

Utilisez la liste de contrôle ci-dessous si vous voulez employer une nouvelle police dans vos rapports.

__ • Ajouter la police à la liste de celles prises en charge.

__ • Indiquer l'emplacement du fichier de la nouvelle police.

__ • Faire correspondre la nouvelle police avec le nom de police physique, le cas échéant.

## Considérations relatives à la prise en charge du chinois simplifié

Les produits IBM Cognos prennent en charge le jeu de caractères GB18030-2000, qui est utilisé dans le codage des environnements locaux en chinois simplifié.

Si vous effectuez l'installation sous Microsoft Windows, le jeu de caractères GB18030-2000 est pris en charge dans la police SimSun-18030 qui est fournie par Microsoft.

Sur les systèmes d'exploitation autres que Windows, vous devez installer une police prenant en charge le jeu de caractères GB18030-2000.

## Ajout de polices à l'environnement IBM Cognos

Si vous souhaitez créer des rapports utilisant des polices indisponibles, vous pouvez ajouter ces polices à la liste de celles prises en charge dans votre environnement IBM Cognos. Vous pouvez également supprimer des polices. Par défaut, les composants d'IBM Cognos utilisent un jeu de polices globales disponibles sur tous les serveurs IBM Cognos.

### Procédure

1. Démarrez IBM Cognos Configuration sur chaque ordinateur Content Manager.
2. Dans le menu **Actions**, cliquez sur l'option **Editer la configuration globale**.
3. Cliquez sur l'onglet **Polices**.
4. Cliquez sur **Ajouter**.

   **Conseil :** Pour supprimer une police de la liste des polices prises en charge, cliquez sur la zone en regard du nom de la police, puis sur **Supprimer**.
5. Dans la zone **Nom de la police prise en charge**, saisissez le nom de la police, puis cliquez sur **OK**.
6. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

   Toutes les polices universelles, y compris les nouvelles polices ajoutées, doivent être installées sur tous les ordinateurs IBM Cognos présents dans votre environnement.

### Résultats

Si une police universelle n'est pas installée sur tous les ordinateurs IBM Cognos, vous devez mettre en correspondance la police universelle avec une police physique installée.

## Spécification de l'emplacement des polices disponibles

Vous devez indiquer l'emplacement d'installation de toutes les polices, y compris celles que vous ajoutez à la liste des polices prises en charge.

La liste des polices contient par défaut les polices installées dans le répertoire *emplacement_installation*\bin\fonts de l'ordinateur IBM Cognos. Si les composants d'IBM Cognos sont installés sur un ordinateur Microsoft Windows, ils utilisent également les polices installées dans le répertoire des polices (fonts) de Windows.

Vous devez indiquer l'emplacement des polices sur tous les ordinateurs sur lesquels les composants du groupe de serveurs d'applications sont installés.

### Procédure

1. Sur chaque ordinateur des composants du groupe de serveurs d'applications, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, pour la propriété **Emplacements des polices physiques**, indiquez l'emplacement des polices.

   S'il existe plusieurs chemins d'accès aux polices, séparez-les par un point-virgule (;).

   Si vous utilisez un serveur d'application autre que celui fourni avec IBM Cognos Analytics, entrez le chemin d'accès complet de l'emplacement des polices. Par exemple : *emplacement_installation*\bin\fonts.
4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Mise en correspondance des polices prises en charge avec les polices installées

Vous pouvez remplacer des polices universelles qui ne sont pas installées sur l'ordinateur par des polices physiques.

Vous pouvez mettre en correspondance les polices sur tous les ordinateurs où sont installés les composants du groupe de serveurs d'applications.

Par exemple, vous ajoutez à la liste des polices prises en charge une police qui n'est pas installée sur l'ordinateur IBM Cognos. Vous pouvez indiquer la police à utiliser pour la remplacer.

Pour imprimer des rapports plus rapidement à l'aide des polices PDF intégrées, vous pouvez mettre en correspondance l'une des polices globales (Arial, par exemple) avec l'une des polices PDF intégrées (Helvetica-PDF, par exemple), en suivant la procédure ci-après. Vous pouvez également sélectionner l'une des polices PDF intégrées pour un objet texte dans Reporting ou Query Studio. Pour plus d'informations, voir le manuel *Query Studio - Guide d'utilisation* ou *Reporting - Guide d'utilisation*.

Aucun mappage n'est requis si vous ajoutez une police à la liste des polices prises en charge installées sur les ordinateurs IBM Cognos. En revanche, vous devez indiquer l'emplacement de la police.

### Procédure

1. Sur chaque ordinateur des composants du groupe de serveurs d'applications, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, cliquez sur la zone **Valeur** à côté de la propriété **Mappage des polices physiques**, puis cliquez sur l'icône Editer  .

   La boîte de dialogue **Valeur - Correspondance des polices physiques** s'affiche.
4. Cliquez sur **Ajouter**.

   **Conseil :** Pour supprimer une police, cochez sa case, puis cliquez sur **Supprimer**.

5. Dans la zone **Nom de police universelle**, saisissez le nom de la police que vous avez ajoutée à la liste des polices prises en charge.
6. Cochez la case **Nom de police physique**.
7. Si vous connaissez le nom de la police physique, saisissez-le. Autrement, cliquez sur l'icône Editer  .

   Dans la boîte de dialogue **Nom de police physique**, cliquez sur le bouton **Rechercher maintenant**, puis sur le nom d'une police dans les résultats.
8. Répétez les étapes 4 à 7 pour chaque police universelle nécessitant un mappage.
9. Cliquez sur le bouton **OK**.
10. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

### Résultats

A présent, vous devez, le cas échéant, indiquer l'emplacement d'installation des polices.

## Utilisation des polices système dans IBM Cognos Configuration

Vous pouvez définir IBM Cognos Configuration pour utiliser vos polices système sur les systèmes d'exploitation Microsoft Windows.

**Remarque :** Si vous activez les paramètres des polices système, vous ne pouvez pas modifier les paramètres des polices dans IBM Cognos Configuration.

### Procédure

1. Accédez au répertoire *emplacement_installation*/configuration.
2. Ouvrez le fichier `cogconfig.prefs` dans un éditeur de texte.
3. Ajoutez la ligne suivante :

   ```
   UseSystemDisplaySetting=true
   ```
4. Sauvegardez et fermez le fichier.
5. Redémarrez IBM Cognos Configuration.

# Modification de la police par défaut des rapports PDF

Vous pouvez modifier la police par défaut que les composants d'IBM Cognos Analytics utilisent pour les rapports PDF. La police par défaut est celle que vous voyez lorsque vous ouvrez un rapport.

Vous pouvez modifier la police par défaut sur l'ordinateur où Content Manager est installé. La police devient la police par défaut de tous les ordinateurs de votre installation. Vous modifiez la police utilisée pour les rapports PDF à l'aide d'IBM Cognos Configuration.

Veillez à ce que la police par défaut soit installée sur tous les ordinateurs de l'installation d'IBM Cognos.

Pour que les caractères GB18030 s'affichent correctement dans les rapports PDF, définissez la police par défaut comme étant SimSun-GB18030.

### Procédure

1. Démarrez IBM Cognos Configuration sur chaque ordinateur Content Manager.
2. Dans le menu **Actions**, cliquez sur l'option **Editer la configuration globale**.

3. Cliquez sur l'onglet **Général**.
4. Dans la zone **Valeur**, saisissez la police que vous voulez utiliser par défaut pour les rapports dans **Police par défaut**.
5. Cliquez sur le bouton **OK**.
6. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
7. Sur tous les ordinateurs des composants du groupe de serveurs d'applications, assurez-vous que l'emplacement d'installation de la police par défaut est précisé dans la propriété **Emplacements des polices physiques** (dans la section **Environnement** de la fenêtre **Explorateur**) ou que la police se trouve dans le répertoire des polices de Windows.

## Configuration des polices incorporées des rapports PDF

Lors de l'ouverture d'un rapport PDF dans Adobe Reader, toutes les polices utilisées dans ce rapport doivent être disponibles. Les polices doivent être soit incorporées dans le rapport, soit installées sur l'ordinateur de l'utilisateur. Si une police ne se trouve ni dans le rapport, ni sur l'ordinateur, Adobe Reader tente de la remplacer par une autre. Ce remplacement peut engendrer des modifications de la présentation du rapport ou empêcher l'affichage de certains caractères.

Pour garantir un affichage correct des rapports au format PDF dans Adobe Reader, IBM Cognos Analytics comprend par défaut les polices requises. Afin de réduire la taille des fichiers, IBM Cognos Analytics n'inclut que les caractères (également appelés glyphes) utilisés dans le rapport, et non l'intégralité des caractères du jeu de polices. IBM Cognos Analytics n'intègre que les polices disposant d'une licence à cet effet. Les informations relatives à cette licence se trouvent dans la police elle-même et sont lues par IBM Cognos Analytics.

Si vous êtes sûr que les polices employées dans les rapports sont disponibles sur les ordinateurs des utilisateurs, vous pouvez limiter ou éliminer les polices incorporées ou restreindre leur nombre afin de réduire la taille des rapports PDF. Si vous optez pour la restriction du nombre de polices, vous devez indiquer si une police est systématiquement incorporée ou si au contraire elle ne l'est jamais, à l'aide d'une liste des polices incorporées établie dans IBM Cognos Configuration.

### Procédure

1. Démarrez IBM Cognos Configuration sur l'ordinateur Content Manager.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, sous **Paramètres des polices**, cliquez sur la valeur **Polices à imbriquer (Service de génération de rapports par lots)** ou **Polices à imbriquer (Service de génération de rapports)**, puis cliquez sur l'icône Editer  .
4. Si vous n'utilisez pas le répertoire de polices par défaut ou souhaitez ajouter un chemin d'accès à un autre répertoire, indiquez le nouveau chemin dans la zone des chemins d'accès aux polices de la boîte de dialogue **Polices à incorporer dans les rapports PDF**.

   **Astuce :** Cliquez sur **Rechercher maintenant** pour obtenir la liste des polices disponibles dans le ou les chemins d'accès indiqués.
5. Pour une police devant être toujours disponible sur les ordinateurs des utilisateurs, faites défiler la liste jusqu'au nom de la police, puis cochez la case **Jamais**.

IBM Cognos Analytics n'intègre cette police dans aucun rapport. Adobe Reader la sélectionne sur l'ordinateur de l'utilisateur lorsque celui-ci ouvre le rapport.

6. Pour une police qui ne sera peut-être pas toujours disponible sur les ordinateurs des utilisateurs, faites défiler la liste jusqu'au nom de la police, puis cochez la case **Toujours**.

   IBM Cognos Analytics intègre la police dans tous les rapports qui l'utilisent. Adobe Reader utilise la police incorporée à l'ouverture du rapport.
7. Cliquez sur le bouton **OK**.

# Enregistrement d'une sortie de rapport

Par défaut, les fichiers de sortie de rapport sont enregistrés dans le magasin de contenu. Vous avez la possibilité d'enregistrer une copie de la sortie de rapport dans un autre emplacement, dans IBM Cognos Analytics ou en dehors. Si vous utilisez cette option, un fichier descripteur doté de l'extension _descr est également enregistré. Les fichiers enregistrés ne sont pas gérés par IBM Cognos Analytics.

## Enregistrement de la sortie des rapports en dehors d'IBM Cognos Analytics

Si vous configurez un emplacement de système de fichiers situé en dehors d'IBM Cognos Analytics, vous pouvez partager vos sorties de rapport avec des applications externes ou des personnes ne possédant pas IBM Cognos Analytics. C'est de cette façon que la plupart des fichiers de sortie de rapport sont enregistrés.

Pour utiliser cette fonctionnalité, vous devez d'abord configurer un répertoire racine dans IBM Cognos Configuration. Un administrateur doit ensuite définir l'emplacement des fichiers dans l'outil Administration d'IBM Cognos. Pour plus d'informations, consultez la rubrique relative à la définition d'un répertoire de stockage pour les sorties de rapport enregistrées en dehors d'IBM Cognos Analytics, dans le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Les sorties de rapport sont toujours enregistrées dans le répertoire configuré pour chaque instance du service de diffusion. Pour éviter de disperser les sorties de rapport dans différents répertoires, vous devez exécuter une seule instance du service de diffusion, ou configurer toutes les instances du service de manière qu'elle utilisent un même répertoire partagé sur le réseau. Les répartiteurs qui exécutent le service de diffusion doivent avoir accès au système de fichiers, ou être désactivés sur les systèmes sur lesquels ils ne sont pas censés enregistrer des sorties de rapport.

### Procédure

1. Créez un répertoire pour votre système de fichiers.

   **Astuce :** Assurez-vous que le répertoire est accessible pour les utilisateurs et qu'il est distinct du répertoire d'installation. Par exemple, dans une installation répartie configurée sous Microsoft Windows, un fichier d'archive tel que *\\nom_serveur\répertoire* peut être utilisé.
2. Démarrez IBM Cognos Configuration sur l'ordinateur Content Manager.
3. Dans le menu **Actions**, cliquez sur l'option **Editer la configuration globale**.
4. Dans la boîte de dialogue **Configuration globale**, cliquez sur l'onglet **Général**.
5. Pour **Racine du système de fichiers d'emplacements d'archives**, indiquez un URI au format approprié

   `file://directory`

   où *répertoire* est le répertoire créé à l'étape 1.

La section file:// de l'URI est requise. Les noms UNC Windows, tels que *nom_serveur**répertoire* peuvent être utilisés. Dans ce cas, l'URI doit avoir le format suivant :

```
file://\\nom_serveur\répertoire
```

**Conseil :** Veillez à ne pas utiliser une unité mise en correspondance lors de l'exécution de Cognos en tant que service Microsoft Windows.

6. Pour vérifier que l'emplacement approprié va être utilisé, cliquez sur **Tester**.
7. Cliquez sur le bouton **OK**.
8. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

### Résultats

L'administrateur doit maintenant configurer l'emplacement des fichiers. Pour plus d'informations, consultez la rubrique relative à la définition d'un répertoire de stockage pour les sorties de rapport enregistrées en dehors d'IBM Cognos Analytics, dans le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

## Enregistrement de la sortie des rapports dans IBM Cognos Analytics

La configuration d'un emplacement sur le système de fichiers dans IBM Cognos Analytics vous permet de réutiliser la sortie du rapport. Cela peut également s'avérer utile à des fins d'archivage, étant donné que les fichiers enregistrés dans le magasin de contenu peuvent être régulièrement supprimés en raison des règles de rétention.

Pour utiliser cette fonctionnalité, vous devez d'abord activer la propriété **Enregistrer les sorties de rapport dans un système de fichiers ?** dans IBM Cognos Configuration. Un administrateur doit ensuite configurer l'emplacement de fichiers à l'aide du paramètre CM.OutPutLocation dans IBM Cognos Administration. Pour plus d'informations, consultez la rubrique relative à la définition d'un répertoire de stockage pour les sorties de rapport enregistrées dans IBM Cognos Analytics, dans le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Les sorties de rapport sont toujours enregistrées dans le répertoire configuré pour chaque instance du service de diffusion. Pour éviter de disperser les sorties de rapport dans différents répertoires, vous devez exécuter une seule instance du service de diffusion, ou configurer toutes les instances du service de manière qu'elle utilisent un même répertoire partagé sur le réseau. Les répartiteurs qui exécutent le service de diffusion doivent avoir accès au système de fichiers, ou être désactivés sur les systèmes sur lesquels ils ne sont pas censés enregistrer des sorties de rapport.

Afin de protéger la sécurité des données de sorties de rapport émises lors de l'utilisation de cette fonctionnalité, le système de fichiers doit être doté d'un chiffrement tiers.

### Procédure

1. Créez un répertoire pour votre système de fichiers.

   **Conseil :** Assurez-vous que le répertoire n'est accessible que pour les utilisateurs autorisés.
2. Démarrez IBM Cognos Configuration sur l'ordinateur Content Manager.

3. Dans la fenêtre **Explorateur**, cliquez sur **Accès aux données** > **Content Manager**.
4. Pour la propriété **Enregistrer les sorties de rapport dans un système de fichiers ?**, cliquez sur **Vrai**.
5. Pour tester la connexion au répertoire des sorties de rapports, cliquez sur **Tester** dans le menu **Actions**.
6. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

### Résultats

L'administrateur doit maintenant configurer l'emplacement des fichiers à l'aide du paramètre CM.OutPutLocation. Pour plus d'informations, consultez la rubrique relative à la définition d'un répertoire de stockage pour les sorties de rapport enregistrées dans IBM Cognos Analytics, dans le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

## Changement de l'emplacement de la sortie de rapport temporaire

Lorsque les utilisateurs exécutent des rapports interactifs, la sortie du rapport est stockée dans Content Manager ou dans un cache de session temporaire situé dans le système de fichiers du rapport local. Vous pouvez modifier l'emplacement du cache de session temporaire sur un ordinateur distant, par exemple pour un répertoire partagé sous Microsoft Windows ou un répertoire monté commun sous UNIX ou Linux.

Par défaut, l'emplacement du cache de session temporaire dans le système de fichiers du rapport est `emplacement_installation/temp/session`. Le répertoire `session` est créé par le serveur de rapports lors de la réception de la première demande émise par une session utilisateur.

### Procédure

1. Démarrez IBM Cognos Configuration sur les ordinateurs sur lesquels des composants du groupe de serveurs d'application sont installés.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, cliquez sur la valeur de la zone **Emplacement des fichiers temporaires**, puis cliquez sur l'icône Editer  .
4. Dans la boîte de dialogue **Sélection de dossier**, utilisez la case **Enregistrer sous** pour localiser l'ordinateur et le répertoire, puis cliquez sur **Sélectionner**.
5. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

   Lorsqu'un utilisateur exécutera une session de rapport interactive, la sortie de rapport temporaire sera désormais stockée dans le nouvel emplacement.

## Modification de l'emplacement des cartes existantes de Map Manager pour Reporting

IBM Cognos Analytics est livré avec un ensemble de graphiques de type Carte que vous pouvez utiliser comme exemples dans Reporting. Vous pouvez modifier l'emplacement des graphiques de type Carte à l'aide d'IBM Cognos Configuration.

**Remarque :** Ces informations ne s'appliquent qu'aux cartes existantes de Map Manager que vous pouvez utiliser dans des rapports.

Par défaut, les graphiques de type Carte sont stockés dans le répertoire `emplacement_installation/maps` sur l'ordinateur des composants du groupe de serveurs d'applications.

Pour plus d'informations sur l'utilisation des graphiques de type Carte, voir le manuel Reporting - *Guide d'utilisation*.

Pour en savoir davantage sur l'utilisation des graphiques de type Carte personnalisés provenant d'autres sources, reportez-vous au manuel *Map Manager Installation and User Guide*.

### Procédure

1. Sur l'ordinateur hébergeant les composants du groupe de serveurs d'applications, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, cliquez sur la valeur relative à l'élément **Emplacement des fichiers de carte**.
4. Cliquez sur le bouton Editer  .
5. Dans la fenêtre **Sélection de dossier**, accédez au répertoire de votre choix, puis cliquez sur **Sélectionner**.
6. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Réglage de WebSphere Liberty Profile

Dans les environnements de production, réglez WebSphere Liberty Profile pour autoriser le nombre maximal d'utilisateurs simultanés que vous prévoyez en ajustant les valeurs de **coreThreads** et de **maxThreads** dans les propriétés avancées des ressources. Ces valeurs définissent le nombre d'unités d'exécution de coeur et de programme d'exécution.

### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Environnement** et sous **Services IBM Cognos**, cliquez sur le nom de ressource (**IBM Cognos** par défaut).
3. Dans la fenêtre **Propriétés**, en regard de **Propriétés avancées**, cliquez dans la zone **Valeur**, puis sur l'icône Editer  .
4. Ajustez les valeurs de paramètre en fonction de vos besoins.

*Tableau 22. Noms et valeurs des paramètres de ressource de service*

| Nom du paramètre | Valeur |
|---|---|
| **coreThreads** | Nombre d'unités d'exécution de coeur avec lesquelles le serveur WebSphere Liberty Profile démarre. Si cette valeur est inférieure à 0, une valeur par défaut est utilisée. Cette valeur par défaut est calculée en fonction du nombre d'unités d'exécution matérielles dans le système. |
| **maxThreads** | Nombre maximal d'unités d'exécution qui peuvent être associées au serveur WebSphere Liberty Profile. |

Pour plus d'informations, reportez-vous à la rubrique du Knowledge Center WebSphere Liberty Profile Tuning the Liberty profile (http://www.ibm.com/

support/knowledgecenter/?lang=en#!/SSEQTP_8.5.5/com.ibm.websphere.wlp.doc/ae/twlp_tun.html?cp=SSEQTP_8.5.5%2F1-3-11-0-7).

5. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Activation de la réplication de session pour les services Content Manager en veille

La fonction de réplication de session permet une reprise d'IBM Cognos Content Manager transparente entre un service Content Manager actif et un service Content Manager en veille.

Avec la réplication de session activée, les données de session utilisateur sont répliquées sur toutes les instances de Content Manager. Si le service Content Manager actif est défaillant, les données de session utilisateur sont conservées et les utilisateurs peuvent continuer à utiliser l'application sans interruption.

La réplication de session utilise deux ports pour communiquer en toute sécurité avec les différentes instances d'IBM Cognos Content Manager configurées dans un environnement unique.

### Procédure

1. Sur un ordinateur sur lequel IBM Cognos Content Manager est installé, démarrez IBM Cognos Configuration.
2. Dans le panneau **Explorateur**, sous **Sécurité**, cliquez sur **Réplication**.
3. Définissez les propriétés suivantes :
   a. Définissez la propriété **Activer la réplication** sur **Vrai**.
   b. Dans la zone de valeur **Numéro de port du programme d'écoute des homologues**, entrez un numéro de port.

      La valeur 0 sélectionne le premier port dynamique disponible lors du démarrage du service IBM Cognos.
   c. Dans la zone de valeur **Numéro de port de la réplication RMI**, entrez un numéro de port.

   **Remarque :** Les **Propriétés avancées** ne doivent être utilisées que sous la supervision du support technique IBM.
4. Enregistrez la configuration et redémarrez le service IBM Cognos.
5. Répétez les étapes pour chaque instance de Content Manager de votre environnement.

   Les numéros de port que vous indiquez ne doivent pas nécessairement être identiques pour chaque instance de Content Manager.

## Utilisation d'un conteneur d'objets externe pour les sorties de rapport et les ensembles de données

Vous pouvez configurer Content Manager pour stocker les sorties de rapport et les ensembles de données sur une unité locale ou dans un partage de réseau en définissant un conteneur d'objets externe. Les sorties de rapport sont disponibles sur le portail et IBM Cognos SDK, mais elles ne sont pas stockées dans la base de données du magasin de contenu.

L'utilisation d'un conteneur d'objets externe pour les sorties de rapport permet de réduire la taille du magasin de contenu et d'améliorer les performances pour Content Manager.

### Avant de commencer

Veillez à exécuter les opérations ci-dessous avant de créer une connexion de conteneur d'objets externe.

- Donnez aux ordinateurs Content Manager accès à l'emplacement de fichier du conteneur d'objets externe.
- Accordez au compte utilisateur qui exécute le service IBM Cognos un accès en lecture et en écriture à l'emplacement de fichier.
- Créez le magasin de contenu.

### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Accès aux données** > **Content Manager**, cliquez avec le bouton droit sur le nom de votre **magasin de contenu**, puis cliquez sur **Nouvelle ressource** > **Conteneur d'objets externe**.
3. Dans la fenêtre **Nouvelle ressource - Conteneur d'objets externe**, saisissez un nom unique pour votre référentiel de système de fichiers et cliquez sur **OK**.

   Vous ne pouvez disposer que d'un seul conteneur d'objets externe.
4. Cliquez sur le nom de ce référentiel.
5. Dans la fenêtre **Conteneur d'objets externe - Propriétés des ressources**, cliquez dans la zone de valeur, cliquez sur Editer. Puis, lorsque la fenêtre **Valeurs URI** s'ouvre, entrez le chemin d'accès à l'emplacement de votre système de fichiers en indiquant le chemin d'accès complet à un emplacement de fichier existant.

*Tableau 23. Exemples de valeurs d'URI*

| Système de fichiers | Valeur de l'URI |
|---|---|
| Windows | `file:///c:/chemin_système_fichiers`<br><br>`file://host/share/chemin_système_fichiers` |
| UNIX ou Linux | `file:///chemin_système_fichiers` |

   **Remarque :** Les chemins relatifs, tels que `file:///../chemin_système_fichiers` et les mappages d'unité ne sont pas pris en charge.

   Dans une installation répartie, tous les gestionnaires Content Manager doivent disposer d'un accès en lecture et en écriture à l'emplacement du système de fichiers. Pour améliorer les performances de lecture des sorties, les composants du groupe de serveurs d'application, en particulier le service de référentiel, doivent disposer d'un accès en lecture à l'emplacement du système de fichiers. Si vous ne détenez pas un accès en lecture, les demandes sont routées vers le gestionnaire Content Manager actif.
6. Redémarrez le service IBM Cognos.

## Vérification de l'accès au conteneur d'objets externe

Utilisez IBM Cognos Configuration pour vérifier que les composants IBM Cognos peuvent se connecter au conteneur d'objets externe.

### Procédure

1. Démarrez IBM Cognos Configuration.
2. Depuis **Explorateur** > **Accès aux données**, cliquez avec le bouton droit de la souris sur le nom de la connexion de votre conteneur d'objets externe.
3. Cliquez sur l'option **Test**.

   IBM Cognos Configuration vérifie l'accès à l'emplacement de fichier du conteneur d'objets externe.

   Vous pouvez également tester cette connexion en cliquant avec le bouton droit de la souris sur **Configuration locale** et en sélectionnant **Tester**.

## Personnalisation de l'impression côté serveur sur les plateformes UNIX et Linux

La façon dont le portail de connexion d'IBM Cognos Analytics gère l'impression sur les serveurs peut varier en fonction de votre plateforme.

Pour cette raison, vous pouvez personnaliser la manière dont le portail gère l'impression des rapports au format PDF pour les plateformes UNIX et Linux en configurant le fichier *rsprintpdf.sh*.

Le fichier *rsprintpdf.sh* ne doit pas être configuré pour les serveurs d'impression Microsoft Windows.

Quand un utilisateur sélectionne **Options d'exécution**, choisit PDF comme **Format**, sélectionne **Imprimer le rapport** dans la section **Diffusion**, puis indique d'autres formats avec les **Options avancées**, par exemple l'orientation Paysage, la taille de papier A4 ou une option **Heure et Mode** pour exécuter le rapport, des problèmes peuvent survenir en cas d'impression sur un serveur d'impressions UNIX ou Linux. Il se peut que la sortie ne soit pas générée, ou qu'elle apparaisse tronquée ou avec une orientation incorrecte.

### Procédure

1. Ouvrez le fichier *rsprintpdf.sh* situé dans le répertoire *emplacement_installation/bin*.
2. Dans un éditeur de texte, personnalisez la section spécifique à la plateforme de votre serveur d'impression, par exemple AIX ou Linux.
3. Utilisez les informations suivantes pour la personnalisation. Les informations sont transmises au script *rsprintpdf.sh* par le processus du serveur en tant qu'options de ligne de commande.

*Tableau 24. Options de personnalisation pour l'impression des rapports au format PDF*

| Option | Nom | Description |
|---|---|---|
| -p | imprimante | Définit la file d'attente. Si aucune file d'attente n'est indiquée, la file par défaut est utilisée. |
| -o | orientation | Spécifie l'orientation des pages dans un fichier (portrait ou paysage). Si aucune orientation n'est indiquée, l'orientation Portrait est utilisée. |
| -m | support | Définit la taille du support pour la sortie générée (par exemple, le format Lettre ou A4). Si aucun support ou aucune taille ni largeur ne sont spécifiés, le bac à papier par défaut est utilisé. |

*Tableau 24. Options de personnalisation pour l'impression des rapports au format PDF (suite)*

| Option | Nom | Description |
|---|---|---|
| -h | hauteur | Pour les tailles de pages personnalisées. Indique la hauteur de la page, en points. Cette option est valable uniquement si elle est spécifiée avec l'option -w et sans l'option -m. |
| -w | largeur | Pour les tailles de pages personnalisées. Indique la largeur de la page, en points. Cette option est valable uniquement si elle est spécifiée avec l'option -h et sans l'option -m. |
| -L | fichier journal | Spécifie le chemin d'accès à un fichier défini par l'utilisateur destiné à journaliser les messages d'erreur. Le nom par défaut du fichier journal est *rsprintpdf.errors.log*. |

4. **Astuce** : Conservez une copie du fichier *rsprintpdf.sh* en cas de remplacement de celui-ci par une mise à jour ultérieure du logiciel.

## Modification de la base de données de notification

Par défaut, le serveur de notification utilise la même base de données que celle utilisée par Content Manager comme magasin de contenu. Vous pouvez utiliser une base de données séparée pour la notification lorsque vous exécutez des volumes importants de production de rapports par lots et de courriers électroniques.

Utilisation d'une base de données séparée pour la notification implique les tâches suivantes :

- Création d'une base de données de notification.

  Pour IBM Db2, Oracle ou Microsoft SQL Server, utilisez la procédure ayant servi à la création de la base de données du magasin de contenu. Suivez les instructions présentées dans «Instructions pour la création du magasin de contenu», à la page 8.

  **Remarque :** Si vous utilisez Db2, vous ne pouvez pas générer un script pour créer la base de données de notification de la même manière que le magasin de contenu.

  Pour Db2 on z/OS, utilisez les instructions dans «Paramètres suggérés pour la création d'une base de données de notification sous IBM Db2 on z/OS», à la page 179.
- Configuration de la connectivité de la base de données.

  Vous pouvez utiliser la même procédure que pour configurer la connectivité de la base de données du magasin de contenu «Configuration de la connectivité de base de données du magasin de contenu», à la page 68.
- Modification des propriétés de connexion de la base de données de notification.

  Suivez les instructions présentées dans «Modification des propriétés de la connexion au niveau de la base de données de notification», à la page 180.

## Paramètres suggérés pour la création d'une base de données de notification sous IBM Db2 on z/OS

La base de données créée pour la base de données de notification doit contenir les paramètres de configuration précisés.

Pour que l'installation aboutisse, utilisez les instructions suivantes lors de la création de la base de données de notification.

Utilisez la liste de contrôle ci-dessous pour configurer la base de données des notifications dans Db2 on z/OS.

__ • Créez une instance de base de données, un groupe de stockage et un compte utilisateur pour la base de données de notification.

Un utilisateur doit disposer du droit de créer et de supprimer les tables de la base de données.

IBM Cognos Analytics utilise les données d'identification du compte utilisateur pour communiquer avec le serveur de bases de données.

__ • Réservez un groupe de mémoire tampon avec une taille de page de 32 ko et un autre avec une taille de page de 4 ko pour l'instance de base de données.

__ • Les administrateurs doivent exécuter un script pour créer des espaces de table contenant des objets LOB et d'autres données pour que la base de données de notification utilise ces espaces de table.

Pour en savoir davantage sur l'exécution du script, voir «Création d'espaces de table pour une base de données de notification sur IBM Db2 for z/OS».

__ • L'administrateur des bases de données doit effectuer une sauvegarde régulière des bases de données IBM Cognos Analytics, car elles contiennent toutes les données IBM Cognos.

Pour garantir la sécurité et l'intégrité des bases de données, protégez-les contre tout accès non autorisé ou inapproprié.

## Création d'espaces de table pour une base de données de notification sur IBM Db2 for z/OS

Si vous utilisez Db2 for z/OS, un administrateur de base de données doit exécuter des scripts pour créer un ensemble d'espaces de table requis pour la base de données de notification. Les scripts doivent être modifiés pour remplacer les paramètres génériques par ceux convenant à votre environnement.

Utilisez les conventions d'attribution de nom pour Db2 for z/OS. Par exemple, tous les noms de paramètres doivent commencer par une lettre et ne pas dépasser 6 caractères. Pour plus d'informations, voir le Knowledge Center d'Db2.

### Procédure

1. Connectez-vous à la base de données en tant qu'utilisateur disposant de privilèges afin de créer et d'insérer des espaces de table, ainsi qu'autoriser l'exécution d'instructions SQL.
2. Pour créer les espaces de table de notifications, accédez au répertoire *emplacement_installation*/configuration/schemas/delivery/zosdb2.
   a. Faites une copie de sauvegarde du fichier script NC_TABLESPACES.sql et enregistrez le fichier sur un autre emplacement.
   b. Ouvrez le fichier script NC_TABLESPACES.sql d'origine et utilisez le tableau ci-après pour vous aider à remplacer les paramètres fictifs par ceux convenant à votre environnement.

*Tableau 25. Descriptions et noms des paramètres de l'espace de table pour la base de données de notification Db2 on z/OS*

| Nom du paramètre | Description |
|---|---|
| NCCOG | Indique le nom de la base de données de notification. |
| DSN8G810 | Indique le nom du groupe de stockage. |
| BP32K | Indique le nom du groupe de mémoire tampon. |

Tous les paramètres répertoriés ne figurent pas dans le script, mais peuvent être ajoutés ultérieurement.

c. Enregistrez et exécutez le script.

Par exemple :

```
db2 -tvf NC_TABLESPACES.sql
```

d. Ouvrez le fichier de script `NC_CREATE_DB2.sql` et remplacez le paramètre fictif NCCOG par le nom de la base de données de notification.

e. Enregistrez le script.

Les services de surveillance des travaux et de planification exécutent automatiquement le script. Toutefois, vous pouvez l'exécuter vous-même.

## Modification des propriétés de la connexion au niveau de la base de données de notification

Après avoir créé une base de données séparée pour la notification, vous devez configurer IBM Cognos pour qu'il utilise cette nouvelle base de données.

Vous devez configurer l'ensemble des composants Content Manager et des composants du groupe de serveurs d'applications pour qu'ils utilisent la même base de données de notification.

### Procédure

1. Démarrez IBM Cognos Configuration dans chaque emplacement où Content Manager ou les composants du groupe de serveurs d'applications sont installés.
2. Dans la section **Accès aux données** de la fenêtre **Explorateur**, cliquez sur **Notification**.
3. Identifiez la base de données utilisée pour la notification :
   - Dans la fenêtre Explorateur, cliquez avec le bouton droit de la souris sur l'option **Notification**, puis sélectionnez **Nouvelle ressource** > et **Base de données**.
   - Saisissez un nom pour la ressource de base de données.
   - Sélectionnez le type de base de données dans le menu déroulant.
   - Cliquez sur le bouton **OK**.
4. Dans la fenêtre **Propriétés**, saisissez les valeurs pour la ressource de base de données de notification.
5. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
6. Testez la notification. Dans la fenêtre **Explorateur**, cliquez avec le bouton droit sur **Notification**, puis sélectionnez **Tester**.

   Cette opération teste la connexion à la base de données et la connexion au serveur de messagerie.

Si vous avez l'habitude d'utiliser la base de données du magasin de contenu pour la notification, les plannings sont répliqués dans les tables de la nouvelle base de données de notification.

### Résultats

Veillez à ce que les valeurs utilisées pour identifier la ressource de base de données de notification soient les mêmes sur tous les ordinateurs équipés de Content Manager et des composants du groupe de serveurs d'applications. Pour utiliser la base de données de notification par défaut, vous n'avez pas besoin d'éditer les valeurs de la fenêtre **Propriétés**.

## Changement de la conformité aux normes de sécurité pour les magasins de clés certifiées IBM Cognos

Par défaut, les magasins de clés certifiées IBM Cognos qui sont utilisés pour les communications SSL contiennent uniquement des certificats conformes au standard NIST SP800-131a. Vous pouvez modifier les certificats disponibles à l'aide de l'outil ThirdPartyCertificateTool.

Vous pouvez ajouter des normes non-NIST SP800-131a et également supprimer les normes non-NIST SP800-131a que vous avez ajoutées.

## Restauration de certificats non-NIST SP800-131a dans des magasins de clés certifiées IBM Cognos

Par défaut, les magasins de clés certifiées IBM Cognos contiennent uniquement des certificats d'autorité de certification (CA) conformes au standard NIST SP800-131a. Si vous utilisez d'autres certificats, par exemple, des certificats SHA1 ou des certificats d'autorité de certification 1024 bits, vous devez les ajouter individuellement au magasin de clés certifiées. Vous pouvez également ajouter ces certificats depuis le magasin de clés certifiées du JRE que vous utilisez à l'aide de la commande de restauration de ThirdPartyCertificateTool.

**Conseil :** Les exemples de cette rubrique utilisent le mot de passe par défaut **NoPassWordSet**. Si vous modifiez le **Mot de passe du fichier de clés**, ainsi que le mot de passe des **Paramètres de l'autorité de certification** dans IBM Cognos Configuration, veillez à utiliser le mot de passe que vous avez défini.

### Avant de commencer

Sous UNIX ou Linux, vous devez définir une variable d'environnement JAVA_HOME avant d'utiliser l'outil `ThirdPartyCertificateTool`.

Sur des installations Microsoft Windows, vous pouvez exécuter l'outil `-java:local` pour utiliser le JRE fourni avec l'installation. Par exemple :

```
ThirdPartyCertificateTool.bat -java:local -R
```

### Procédure

1. Accédez au répertoire `emplacement_installation/bin`.
2. Restaurez les certificats non-NIST SP800-131a en saisissant la commande suivante :

   Sous UNIX ou Linux, saisissez :

   ```
   ThirdPartyCertificateTool.sh -R -p NoPassWordSet
   ```

Sous Windows, saisissez :

```
ThirdPartyCertificateTool.bat -R -p NoPassWordSet
```

## Suppression de certificats non-NIST SP800-131a des magasins de clés certifiées IBM Cognos

Si vous avez ajouté des certificats non-NIST SP800-131a aux magasins de clés certifiées IBM Cognos, par exemple, des certificats SHA1 ou des certificats d'autorité de certification 1024 bits, vous pouvez les supprimer avec l'outil ThirdPartyCertificateTool.

**Conseil :** Les exemples de cette rubrique utilisent le mot de passe par défaut **NoPassWordSet**. Si vous modifiez le **Mot de passe du fichier de clés**, ainsi que le mot de passe des **Paramètres de l'autorité de certification** dans IBM Cognos Configuration, veillez à utiliser le mot de passe que vous avez défini.

### Avant de commencer

Sous UNIX ou Linux, vous devez définir une variable d'environnement JAVA_HOME avant d'utiliser l'outil `ThirdPartyCertificateTool`.

Sur des installations Microsoft Windows, vous pouvez exécuter l'outil `-java:local` pour utiliser le JRE fourni avec l'installation. Par exemple :

```
ThirdPartyCertificateTool.bat -java:local -N
```

### Procédure

1. Accédez au répertoire `emplacement_installation/bin`.
2. Saisissez la commande suivante :

   Sous UNIX ou Linux, saisissez :

   ```
   ThirdPartyCertificateTool.sh -N -p NoPassWordSet
   ```

   Sous Windows, saisissez :

   ```
   ThirdPartyCertificateTool.bat -N -p NoPassWordSet
   ```

# Configuration des composants IBM Cognos pour l'utilisation d'une autre autorité de certification

Les composants IBM Cognos Analytics utilisent, par défaut, leur propre service d'autorité de certification (CA) pour établir la racine d'approbation dans l'infrastructure de sécurité d'IBM Cognos. Vous pouvez néanmoins configurer les composants IBM Cognos de façon qu'ils utilisent le certificat d'une autre autorité de certification, par exemple iPlanet ou Microsoft.

Pour utiliser le certificat d'une autre autorité de certification, procédez de la manière suivante :

1. «Création de fichiers de demande de signature de certificat (CSR)», à la page 185.

   Une partie de cette tâche exige que vous soumettiez les demandes de signature de certificat (CSR) à votre autorité de certification, et génériez les certificats. Pour en savoir davantage sur ce processus, reportez-vous à la documentation de votre autorité de certification.
2. «Importation des certificats de l'autorité de certification dans les composants IBM Cognos», à la page 186

3. «Configuration de composants IBM Cognos pour l'utilisation de certificats générés par votre autorité de certification», à la page 187.

# Commandes ThirdPartyCertificateTool et exemples

Certaines tâches utilisent un outil de ligne de commande nommé `ThirdPartyCertificateTool`. Les tableaux qui suivent répertorient les options de cet outil de ligne de commande.

## Commandes ThirdPartyCertificateTool

*Tableau 26. Mode de fonctionnement principal*

| Commande | Description |
|---|---|
| **-c** | Crée une demande de signature de certificat (CSR). |
| **-i** | Importe un certificat. |
| **-E** | Exporte un certificat. |

*Tableau 27. Modificateurs de fonctionnement*

| Commande | Description |
|---|---|
| **-e** | Utiliser l'identité de chiffrement. |
| **-T** | Utiliser le magasin de clés de confiance (utilisé uniquement avec **-i** et **-E**). |

*Tableau 28. Indicateurs d'informations*

| Commande | Description |
|---|---|
| **-d** | Nom distinctif (DN) à utiliser pour le certificat. |
| **-r** | Emplacement de la demande de signature de certificat ou du fichier de certificat (selon le mode) |
| **-t** | Fichier de chaîne d'autorité de certification. Peut être de type PEM, une chaîne de certificats d'autorité de certification PKCS#7 binaire ou un certificat d'autorité de certification unique au format DER. |
| **-p** | Mot de passe du fichier de clés. Si **-p** n'est pas inclus, **NoPassWordSet** est utilisé comme mot de passe par défaut. |
| **-a** | Algorithme de paire de clés : **RSA**. **RSA** est la valeur par défaut. |
| **-P** | Crée un fichier de clés d'autorité de certification incluant les autorités de certification approuvées par l'environnement d'exécution Java (JRE) en cours. |
| **-N** | Définit le magasin de clés de confiance pour utiliser la norme NIST SP800-131a. |
| **-R** | Restaure des certificats non-NIST SP800-131a dans le magasin de clés de confiance. |

Les exemples de valeurs du tableau suivant sont utilisés :

*Tableau 29. Exemples de valeurs*

| Propriété | Valeur |
|---|---|
| Nom distinctif du certificat de chiffrement | Valeur unique, formatée de la façon suivante :<br><br>`CN=EncryptCert,O=MaSociété,C=CA` |
| Mot de passe du fichier de clés | Mot de passe par défaut : NoPassWordSet<br><br>Cette valeur doit correspondre aux mots de passe dans IBM Cognos Configuration sous **Sécurité** > **Cryptographie** > **Cognos**. Si vous modifiez les valeurs par défaut pour **Mot de passe du magasin de clés de signature**, **Mot de passe du magasin de clés de chiffrement** et **Mot de passe du magasin de clés de l'autorité de certification**, veillez à utiliser les mots de passe que vous définissez. |

## Exemples de commandes ThirdPartyCertificateTool

*Tableau 30. Exemples de commandes ThirdPartyCertificateTool*

| Exemple | Commande |
|---|---|
| Pour créer une paire de clés de chiffrement et une demande de signature de certificat PKCS#10 | `ThirdPartyCertificateTool.bat -c -e -d cn=Me,o=MyCompany,c=CA -r crypto.csr -a RSA -p password` |
| Pour importer le certificat de chiffrement généré par l'autorité de certification tierce et la chaîne de certificats d'autorité de certification PKCS#7 | `ThirdPartyCertificateTool.bat -i -e -r crypto.cer -p password -t cacert.p7b` |
| Pour importer le certificat de chiffrement généré par l'autorité de certification tierce et la chaîne de certificats d'autorité de certification PEM | `ThirdPartyCertificateTool.bat -i -e -r crypto.cer -p password -t cacert.pem` |
| Pour ajouter `ca.cer` comme certificat digne de confiance | `ThirdPartyCertificateTool.bat -i -T -r ca.cer -p password -t cacert.cer` |
| Pour exporter le certificat de chiffrement vers `crypto.cer` | `ThirdPartyCertificateTool.bat -E -e -r crypto.cer -p password` |
| Pour exporter le certificat de l'autorité de certification IBM Cognos vers `ca.cer` (si vous N'UTILISEZ PAS d'autorité de certification tierce) | `ThirdPartyCertificateTool.bat -E -T -r ca.cer -p password` |
| Pour retirer tous les certificats d'autorité de certification non conformes au standard NIST SP800-131a et définir le magasin de clés de confiance de l'autorité de certification selon ce standard | `ThirdPartyCertificateTool.bat -N -p password` |
| Pour restaurer les certificats JRE non conformes au standard NIST SP800-131a dans le magasin de clés de confiance | `ThirdPartyCertificateTool.bat -R -p password` |

# Création de fichiers de demande de signature de certificat (CSR)

Pour obtenir un certificat d'une autorité de certification (CA), vous devez au préalable générer des fichiers de demande de signature de certificat (CSR) pour la clé de chiffrement du magasin de clés d'IBM Cognos. L'autorité de certification utilise ce fichier pour produire un certificat de chiffrement et un certificat d'autorité de certification que vous importez dans votre magasin de clés.

**Conseil :** Les exemples de cette rubrique utilisent le mot de passe par défaut **NoPassWordSet**. Si vous modifiez le **Mot de passe du fichier de clés**, ainsi que le mot de passe des **Paramètres de l'autorité de certification** dans IBM Cognos Configuration, veillez à utiliser le mot de passe que vous avez défini.

## Avant de commencer

Sous UNIX ou Linux, vous devez définir une variable d'environnement JAVA_HOME avant d'utiliser l'outil ThirdPartyCertificateTool.

Sur des installations Microsoft Windows, vous pouvez exécuter l'outil -java:local pour utiliser le JRE fourni avec l'installation. Par exemple :

```
ThirdPartyCertificateTool.bat -java:local -c -d ...
```

## Procédure

1. Effectuez une copie de sauvegarde de vos données de clé :
   a. Accédez au répertoire *emplacement_installation*\configuration.
   b. Effectuez une copie de sauvegarde du fichier cogstartup.xml dans un emplacement sécurisé.
   c. Sauvegardez le contenu du répertoire suivant à un emplacement sécurisé : *emplacement_installation*\configuration\certs
2. Accédez au répertoire *emplacement_installation*\bin.
3. Créez la demande de signature de certificat pour la clé de chiffrement en saisissant la commande suivante :

   Sous UNIX ou Linux, saisissez

   ```
   ThirdPartyCertificateTool.sh -c -e -d "CN=EncryptCert,O=MyCompany,C=CA"
   -r encryptRequest.csr -p NoPassWordSet
   ```

   Sur Windows, tapez :

   ```
   ThirdPartyCertificateTool.bat -c -e -d "CN=EncryptCert,O=MyCompany,C=CA"
   -r encryptRequest.csr -p NoPassWordSet
   ```

   a valeur de nom distinctif (DN) dans la commande ("CN=SignCert,O=**MyCompany**,C=CA") identifie de manière unique l'installation IBM Cognos. Les attributs utilisés reflètent une structure hiérarchique de votre organisation.

   Le mot de passe que vous entrez pour cette clé sera réutilisé lors de l'importation du certificat, et à nouveau dans IBM Cognos Configuration.

   Vous pouvez ignorer les avertissements relatifs à la journalisation.

   La commande crée le fichier CAMKeystore dans le répertoire certs, définit le mot de passe spécifié, crée une paire de clés et la stocke dans le magasin de clés, puis exporte le fichier encryptRequest.csr dans le répertoire *emplacement_installation*\bin.
4. Copiez le fichier dans un répertoire encryptRequest.csr accessible par votre autorité de certification.

5. Entrez le fichier `encryptRequest.csr` dans l'autorité de certification et générez le certificat.

   L'autorité de certification produit un certificat de clé de chiffrement et un certificat de l'autorité de certification.

   **Important :** Les fichiers générés par l'autorité de certification doivent être au format PEM (ASCII codé en base 64).

### Résultats

Vous pouvez maintenant importer les certificats générés dans les composants IBM Cognos.

## Importation des certificats de l'autorité de certification dans les composants IBM Cognos

Après avoir obtenu les certificats de l'autorité de certification, vous devez les importer dans les composants IBM Cognos.

Vous devez importer les certificats sur tous les postes sur lesquels les composants IBM Cognos sont installés, y compris Content Manager, les composants du groupe des serveurs d'applications, la passerelle et les composants de modélisation.

**Conseil :** Les exemples de cette rubrique utilisent le mot de passe par défaut **`NoPassWordSet`**. Si vous modifiez le **Mot de passe du fichier de clés**, ainsi que le mot de passe des **Paramètres de l'autorité de certification** dans IBM Cognos Configuration, veillez à utiliser le mot de passe que vous avez défini.

### Avant de commencer

Sous UNIX ou Linux, vous devez définir une variable d'environnement JAVA_HOME avant d'utiliser l'outil `ThirdPartyCertificateTool`.

Sur des installations Microsoft Windows, vous pouvez exécuter l'outil `-java:local` pour utiliser le JRE fourni avec l'installation. Par exemple :

```
ThirdPartyCertificateTool.bat -java:local -c -d ...
```

### Procédure

1. Créez une copie du certificat de chiffrement, et renommez-la `encryptCertificate.cer`.
2. Créez une copie du certificat racine de l'autorité de certification, et renommez-la `ca.cer`.
3. Copiez les fichiers `encryptCertificate.cer` et `ca.cer` dans le répertoire *`emplacement_installation`*`/bin`.
4. Importez le certificat de chiffrement dans le magasin de clés de chiffrement d'IBM Cognos à l'aide de la commande suivante :

   Sous UNIX ou Linux, saisissez :

   ```
   ThirdPartyCertificateTool.sh -i -e -r encryptCertificate.cer -p
   NoPassWordSet -t ca.cer
   ```

   Sous Windows, saisissez :

   ```
   ThirdPartyCertificateTool.bat -i -e -r encryptCertificate.cer -p
   NoPassWordSet -t ca.cer
   ```

**Important :** Vous devez utiliser le mot de passe que vous avez entré lors de l'exportation de la clé de chiffrement, à la tâche précédente.

Vous pouvez ignorer les avertissements relatifs à la journalisation.

La commande lit les fichiers `encryptCertificate.cer` et `ca.cer` dans le répertoire *`emplacement_installation`*`\bin` et importe les certificats depuis les deux fichiers dans le fichier `CAMKeystore` dans le répertoire `certs` en utilisant le mot de passe spécifié.

5. Importez le certificat de l'autorité de certification dans le magasin de clés certifiées d'IBM Cognos en saisissant la commande suivante :

   Sous UNIX ou Linux, saisissez :

   ```
   ThirdPartyCertificateTool.sh -i -T -r ca.cer -p NoPassWordSet
   ```

   Sous Windows, saisissez :

   ```
   ThirdPartyCertificateTool.bat -i -T -r ca.cer -p NoPassWordSet
   ```

   La commande lit le fichier `ca.cer` et importe le contenu dans le fichier `CAMKeystore` dans le répertoire `certs` en utilisant le mot de passe spécifié.

### Résultats

Vous pouvez maintenant configurer les composants IBM Cognos en vue de l'utilisation des certificats de l'autorité de certification.

## Configuration de composants IBM Cognos pour l'utilisation de certificats générés par votre autorité de certification

Après avoir importé les certificats de l'autorité de certification, vous utilisez IBM Cognos Configuration pour configurer leur utilisation sur chaque poste sur lequel est installé un composant IBMCognos.

**Remarque :** Assurez-vous que les emplacements de magasin de clés et le mot de passe dans IBM Cognos Configuration correspondent à ceux saisis dans l'outil de ligne de commande. Par exemple, si vous modifiez le **Mot de passe du fichier de clés cryptographiques** et le **Mot de passe du magasin de clés de l'autorité de certification** dans IBM Cognos Configuration, veillez à utiliser le mot de passe que vous définissez.

### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, dans la section **Sécurité** > **Cryptographie**, cliquez sur **Cognos**.
3. Cliquez sur la zone **Valeur** en regard de **Voulez-vous utiliser une autorité de certification tierce ?**, et sélectionnez **Vrai**.

   Lorsque vous définissez cette propriété sur Vrai, toutes les propriétés relatives à l'autorité de certification et au nom d'identité sont ignorées.
4. Entrez le mot de passe que vous avez utilisé pour la clé de chiffrement dans **Mot de passe du magasin de clés de chiffrement** et indiquez le chemin pour **Emplacement du magasin de clés de chiffrement**. Si vous avez utilisé les valeurs des exemples des tâches précédentes, le chemin n'a pas à être modifié.
5. Entrez le **Mot de passe du magasin de clés de l'autorité de certification**.
6. Cliquez sur **Fichier** > **Enregistrer**.
7. Redémarrez les services IBM Cognos.

# Configuration du protocole SSL pour les composants d'IBM Cognos

Vous pouvez utiliser le protocole SSL (Secure Sockets Layer) pour les communications entre les composants IBM Cognos dans des installations monoserveur et réparties.

### Connecteurs IBM WebSphere Liberty Profile

Si l'URI interne du répartiteur porte le préfixe http, alors que l'URI externe porte le préfixe https, ou l'inverse, les deux connecteurs, Liberty HTTP/1.1 non-SSL et Liberty HTTP/1.1 SSL, sont activés dans le fichier `server.xml`.

Si les URI des répartiteurs interne et externe utilisent des protocoles ou des ports différents, le port du répartiteur interne n'est accessible que pour les composants situés sur l'ordinateur local. L'URI interne du répartiteur doit également préciser le nom d'hôte localhost.

### Installations sur un seul ordinateur

Dans une installation monoposte dans laquelle SSL n'est pas encore utilisé, vous devez arrêter le service avant de remplacer le protocole en cours par https. Une fois que vous aurez enregistré la configuration avec les paramètres SSL, vous pourrez redémarrer les services.

### Installations réparties

Dans une installation répartie, vous devez commencer par configurer l'utilisation du protocole SSL sur l'ordinateur actif Content Manager par défaut, et démarrer les services sur cet ordinateur, avant de configurer l'utilisation de SSL dans les composants du groupe des serveurs d'applications et dans la passerelle.

### Ajout d'un ordinateur à une installation

Si vous ajoutez un ordinateur à un environnement compatible SSL, vous êtes invité à accepter provisoirement un certificat lorsque vous enregistrez la configuration. L'acceptation de ce certificat provisoire permet la mise en place d'une approbation permanente pour les composants existants.

### Ajout d'un composant à un ordinateur

Si vous ajoutez un composant à une installation déjà configurée pour SSL, l'approbation des certificats SSL est héritée des composants existants. Si vous ajoutez ce composant dans un emplacement de l'ordinateur différent, mais dans un environnement déjà configuré pour SSL, vous êtes invité à accepter provisoirement un certificat lorsque vous enregistrez la configuration. L'acceptation de ce certificat provisoire permet la mise en place d'une approbation permanente pour les composants existants.

# Configuration de SSL pour les composants IBM Cognos

Pour les composants IBM Cognos, vous pouvez utiliser SSL pour les connexions internes, les connexions externes, ou toutes les connexions.

Si vous configurez le protocole SSL uniquement pour les connexions internes, les composants d'IBM Cognos sur l'ordinateur local communiquent à l'aide de ce

protocole. Le répartiteur écoute les connexions sécurisées sur un port distinct de celui utilisé pour les demandes HTTP distantes. Vous devez donc configurer deux URI de répartiteur.

Si vous configurez le protocole SSL uniquement pour les connexions externes, les communications entre des composants d'IBM Cognos distants et l'ordinateur local utilisent ce protocole. Vous devez configurer le répartiteur afin qu'il écoute les demandes sécurisées distantes sur un port distinct de celui utilisé pour les demandes HTTP locales. Vous devez également configurer les URI de Content Manager et l'URI du répartiteur pour les applications externes de façon à ce qu'ils utilisent le même protocole et le même port que le répartiteur externe.

Si vous configurez le protocole SSL pour toutes les connexions, le répartiteur peut utiliser le même port pour les connexions internes et externes. Si vous n'utilisez pas le protocole SSL pour les communications locales ou distantes, le répartiteur peut utiliser le même port pour toutes les communications.

Les composants IBM Cognos Analytics utilisent, par défaut, un service d'autorité de certification (CA) interne pour établir la racine d'approbation dans l'infrastructure de sécurité d'IBM Cognos. Ce fonctionnement est appliqué aux connexions SSL et non-SSL. Pour utiliser des certificats gérés par un autre service, voir «Configuration des composants IBM Cognos pour l'utilisation d'une autre autorité de certification», à la page 182.

Dans une installation répartie, vous devez commencer par configurer l'utilisation du protocole SSL sur l'ordinateur actif Content Manager par défaut, et démarrer les services sur cet ordinateur, avant de configurer l'ordinateur des composants du groupe des serveurs d'applications.

## Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, entrez les valeurs de l'URI :

   **Important :** pour les configurations HTTPS/SSL, veillez à utiliser un nom d'hôte complet pour les URI. De plus, dans la fenêtre de l'explorateur, sous **Sécurité** > **Cryptographie** > **Cognos** > **Nom d'identité**, remplacez le **nom usuel du serveur** CAMUSER par son nom de domaine complet.

   - Afin de configurer le protocole SSL uniquement pour les connexions internes, entrez `https` et un numéro de port pour les communications SSL dans la propriété **URI interne du répartiteur**.

     Pour les propriétés **URI externe du répartiteur** et **URI du répartiteur des applications externes**, entrez le protocole `http` et utilisez le port par défaut ou tout autre port disponible.

     Si vous utilisez le serveur d'application fourni avec IBM Cognos Analytics, la propriété **URI interne du répartiteur** doit avoir la valeur `localhost`.

     Les ports des deux URI du répartiteur doivent être différents.
   - Afin de configurer le protocole SSL uniquement pour les connexions externes, entrez `https` et un numéro de port pour les communications SSL dans les propriétés **URI externe du répartiteur** et **URI du répartiteur des applications externes**.

     Pour la propriété **URI interne du répartiteur**, conservez le protocole `http` et utilisez le port par défaut ou tout autre port disponible.

Si vous utilisez le serveur d'application fourni avec IBM Cognos Analytics, la propriété **URI interne du répartiteur** doit avoir la valeur `localhost`.

Les ports des deux URI du répartiteur doivent être différents.

- Pour configurer le protocole SSL pour toutes les connexions, saisissez le même URI pour les propriétés **URI interne du répartiteur**, **URI externe du répartiteur** et **URI du répartiteur des applications externes**. Entrez `https` et un numéro de port pour les communications SSL.
- En outre, vous pouvez entrer `https` et un numéro de port pour les communications SSL dans la propriété **URI de Content Manager**.
- Si vous avez installé la passerelle sur un ordinateur distinct, et si vous utilisez SSL pour les connexions externes, dans IBM Cognos Configuration sur le poste passerelle, entrez `https` et le numéro de port des communications SSL dans la propriété **URI du répartiteur pour la passerelle**.

4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
5. Redémarrez les services.

   Dans un environnement réparti, démarrez les services sur l'ordinateur Content Manager puis sur les ordinateurs hébergeant les composants du groupe de serveurs d'applications.

# Configuration de la sécurité partagée entre les serveurs IBM Cognos et d'autres serveurs

Si vous souhaitez utiliser l'autorité de certification par défaut d'IBM Cognos et employer le protocole SSL pour des connexions entre d'autres serveurs et des serveurs IBM Cognos, vous devez ajouter le certificat d'IBM Cognos au magasin de clés certifiées des autres serveurs.

**Remarque :** Si vous utilisez des navigateurs pour vous connecter aux composants IBM Cognos, ils invitent automatiquement les utilisateurs à mettre à jour leurs magasins de clés certifiées.

Si vous souhaitez que la connexion entre les serveurs IBM Cognos et l'autre serveur soit mutuellement authentifiée, vous devez également copier le certificat de votre autorité de certification dans le magasin de clés certifiées pour les serveurs IBM Cognos.

Lorsque vous avez configuré les composants d'IBM Cognos pour l'utilisation d'une autre autorité de certification (CA), il n'est pas nécessaire de configurer de sécurité partagée entre le serveur IBM Cognos et les autres serveurs.

## Copie du certificat IBM Cognos vers un autre serveur

La première tâche de l'ajout du certificat IBM Cognos au magasin de clés certifiées sur d'autres serveurs consiste à copier le certificat vers le serveur.

### Procédure

1. Accédez au répertoire *emplacement_installation*`/bin`.
2. Procédez à l'extraction du certificat d'IBM Cognos en saisissant la commande suivante :
   - Sur UNIX ou Linux, tapez

     `ThirdPartyCertificateTool.sh -E -T -r` *destination_file* `-p` **`NoPassWordSet`**
   - Sous Microsoft Windows, tapez

```
ThirdPartyCertificateTool.bat -E -T -r destination_file -p
NoPassWordSet
```

3. Importez le certificat dans le magasin de clés certifiées de votre serveur.

   Pour en savoir davantage sur la mise à jour du magasin de clés certifiées du serveur, reportez-vous à la documentation du serveur.

### Copie du certificat de l'autorité de certification vers les serveurs IBM Cognos

Après avoir copié le certificat IBM Cognos vers les autres serveurs, copiez le certificat de l'autorité de certification vers le serveur IBM Cognos.

#### Procédure

1. Copiez le certificat de l'autorité de certification dans un emplacement sécurisé sur le serveur IBM Cognos.

   Assurez-vous que le certificat de l'autorité de certification utilise l'encodage Base-64, format X.509.

2. Importez le certificat de l'autorité de certification en saisissant la commande suivante :
   - Sous UNIX ou Linux, entrez la commande suivante :

     ```
     ThirdPartyCertificateTool.sh -T -i -r CA_certificate_file -p
     NoPassWordSet
     ```

   - Sous Microsoft Windows, tapez

     ```
     ThirdPartyCertificateTool.bat -T -i -r CA_certificate_file -p
     NoPassWordSet
     ```

## Sélection et classement des suites de chiffrement pour SSL

Une connexion SSL commence par une négociation au cours de laquelle le client et le serveur présentent une liste des suites de chiffrement prises en charge, par ordre de priorité. Une suite de chiffrement garantit la qualité de la protection pour la connexion. Elle contient des algorithmes de cryptographie, d'authentification, de hachage et d'échange de clés. Le protocole SSL sélectionne la suite de priorités les plus élevées que le client et le serveur prennent en charge.

Une liste des suites de chiffrement prises en charge pour SSL est fournie. Vous pouvez éliminer les suites qui ne correspondent pas à vos exigences, puis affecter une priorité ou une préférence à celles qui restent. Les suites de chiffrement sélectionnées sont présentées par ordre de priorité pour les côtés client et serveur de la négociation. Au moins l'une des suites de chiffrement entre les plateformes client et serveur doit correspondre.

La liste des suites de chiffrement prises en charge est créée de façon dynamique sur chaque ordinateur et dépend du JRE (Java Runtime Environment) ou de la présence d'autres logiciels cryptographiques installés sur l'ordinateur. Si vous avez apporté des modifications à un ordinateur, telles qu'une mise à niveau du JRE ou l'installation d'un logiciel ayant entraîné la mise à niveau du JRE, cela peut avoir une incidence sur les suites de chiffrement prises en charge sur l'ordinateur en question. Si vous ne disposez plus d'aucune suite de chiffrement correspondant aux autres ordinateurs de votre environnement, vous devrez peut-être changer de JRE sur votre ordinateur afin qu'il corresponde à celui des autres ordinateurs de l'environnement.

### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Cryptographie** > **Cognos**.
3. Dans la fenêtre **Propriétés**, cliquez sur la colonne **Valeur** correspondant à la propriété **Algorithmes de chiffrement (ciphersuites) pris en charge**.
4. Cliquez sur l'icône Editer  .
   - Pour déplacer une suite de chiffrement dans la liste **Valeurs actuelles**, cochez la case dans la liste **Valeurs disponibles**, puis cliquez sur **Ajouter**.
   - Pour déplacer une suite de chiffrement vers le haut ou vers le bas dans la liste **Valeurs actuelles**, cochez la case correspondante, puis cliquez sur les flèches de déplacement vers le haut et vers le bas.
   - Pour supprimer une suite de chiffrement de la liste **Valeurs actuelles**, cochez la case correspondante, puis cliquez sur **Supprimer**.
5. Cliquez sur le bouton **OK**.
6. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Utilisation de SSL pour les connexions de base de données dans IBM Cognos Configuration

Vous pouvez configurer IBM Cognos Analytics de manière qu'il utilise le protocole SSL (Secure Sockets Layer) pour les communications avec les bases de données utilisées par IBM Cognos Analytics, y compris le magasin de contenu, la base de données de notification et la base de données de journalisation.

Le protocole SSL doit être activé sur le serveur de base de données et l'utilisation de SSL pour les connexions au serveur doit être configurée sur les clients avant l'activation de SSL dans IBM Cognos Configuration.

Le support SSL est disponible pour toutes les bases de données prises en charge, à l'exception d'IBM Db2 for z/OS.

### Db2

Vous pouvez utiliser SSL pour Db2 version 9.1 Fix Pack 2 et les versions ultérieures.

Pour obtenir des informations sur la configuration de Db2 en vue des connexions SSL, consultez la documentation relative à votre version de Db2.

Par exemple, pour la version 10.5, consultez la documentation d'IBM Db2 version 10.5 (pic.dhe.ibm.com/infocenter/db2luw/v10r5/index.jsp?topic=%2Fcom.ibm.db2.luw.admin.sec.doc%2Fdoc%2Fc0053514.html).

### IBM Informix

Pour obtenir des informations sur la configuration d'IBM Informix en vue des connexions SSL, consultez la documentation relative à votre version d'IBM Informix.

Par exemple, pour la version 12.10, consultez la documentation d'IBM Informix version 12.10 (pic.dhe.ibm.com/infocenter/informix/v121/index.jsp?topic=%2Fcom.ibm.sec.doc%2Fids_ssl_001.htm).

### Oracle

Pour obtenir des informations sur la configuration d'Oracle en vue des connexions SSL, consultez la documentation relative à votre version d'Oracle.

Le livre blanc SSL With Oracle JDBC Thin Driver (www.oracle.com/technetwork/database/enterprise-edition/wp-oracle-jdbc-thin-ssl-130128.pdf) publié par Oracle fournit des informations sur la configuration de SSL pour le serveur et le client de base de données.

### Microsoft SQL Server

Pour obtenir des informations sur la configuration de Microsoft SQL Server en vue des connexions SSL, consultez la documentation relative à votre version de Microsoft SQL Server.

Par exemple, pour la version 2012, consultez la documentation de Microsoft SQL Server version 2012 (technet.microsoft.com/en-us/library/bb879949.aspx).

**Remarque :** Après avoir activé SSL sur le serveur de base de données, vous pouvez définir **SSL Encryption Enabled** sur **True** dans IBM Cognos Configuration.

## Utilisation de SSL pour les connexions de base de données dans IBM Cognos Configuration for Microsoft SQL Server

11.0.5

Pour utiliser Secure Sockets Layer (SSL) pour les connexions de base de données dans IBM Cognos Configuration, vous devez importer le certificat SSL dans le magasin de clés Java, puis modifier certains fichiers de configuration IBM Cognos. Pour obtenir des informations sur la configuration de Microsoft SQL Server pour les connexions SSL, consultez la documentation relative à votre version de Microsoft SQL Server.

Vous pouvez utiliser SSL pour les connexions de base de données dans IBM Cognos Configuration, y compris les bases de données Content Store, de notification et de journalisation, ainsi que les services de gestion des tâches humaines et d'annotation, et Cognos Mobile.

Le pilote JDBC Microsoft **remplace** le pilote JSQLConnect pour SQL Server. A partir de la version 11.0.5 et suivantes, vous devez télécharger le nouveau pilote de type 4 depuis Microsoft et le placer dans le dossier *emplacement_installation*/drivers.

**Remarque :** Il existe plusieurs noms de fichier JAR de pilote différents, tels que sqljdbc4.jar, sqljdbc41.jar et sqljdbc42.jar. Officiellement, le fichier sqljdbc42.jar prend en charge JRE8 qui est la version livrée avec Cognos Analytics.

### Avant de commencer

Vous devez activer SSL sur votre serveur de base de données avant de configurer IBM Cognos en vue de l'utilisation de SSL pour les connexions de base de données.

Le certificat SSL doit avoir été exporté de votre serveur de base de données et être disponible sur l'ordinateur sur lequel vous configurez la connexion de base de données dans IBM Cognos Configuration.

## Procédure

1. Si vous utilisez un serveur SQL qui est configuré pour SSL comme base de données de votre magasin de contenu, procédez comme suit :
   a. Obtenez le certificat racine de l'autorité de certification qui a émis le certificat de votre serveur SQL Server (ou le certificat de serveur auto-signé s'il n'a pas été émis par une autorité de certification), et copiez-le sur l'ordinateur sur lequel Cognos Analytics est installé. Par exemple, copiez le fichier `sqlcert.cer` dans le répertoire racine, `c:\sqlcert.cer`
   b. Entrez `cd C:\Program Files\ibm\cognos\analytics\jre\lib\security`
   c. Entrez, par exemple, `C:\Progra~1\ibm\cognos\analytics\jre\bin\keytool -import -trustcacerts -file "c:\sqlcert.cer" -keystore cacerts -alias SQLCert`
2. Editez *emplacement_installation*`\bin64\startwlp.bat` (Windows) ou *emplacement_installation*`\bin64\startwlp.sh` (Linux, UNIX) pour ajouter les lignes suivantes après la ligne `set JVM_ARGS=-Xmx4096m -XX:MaxNewSize=2048m -XX:NewSize=1024m %DEBUG_OPTS%` :

   Windows :

   ```
   set JVM_ARGS="-Dcom.ibm.jsse2.overrideDefaultTLS=true" %JVM_ARGS%
   set JVM_ARGS="-Dcom.ibm.jsse2.sp800-131=strict" %JVM_ARGS%
   ```

   Linux, UNIX :

   ```
   JVM_ARGS=-Dcom.ibm.jsse2.overrideDefaultTLS=true $JVM_ARGS
   JVM_ARGS=-Dcom.ibm.jsse2.sp800-131=strict $JVM_ARGS
   ```
3. Editez *emplacement_installation*`\bin64\bootstrap_wlp_`*version_système_exploitation*`.xml` pour ajouter les lignes suivantes après la ligne `<param condName="${java_vendor}" condValue="IBM">-Xscmaxaot4m</param>`:

   Windows :

   ```
   <param>"-Dcom.ibm.jsse2.overrideDefaultTLS=true"</param>
   <param>"-Dcom.ibm.jsse2.sp800-131=strict"</param>
   ```

   Linux, UNIX :

   ```
   <param>-Dcom.ibm.jsse2.overrideDefaultTLS=true</param>
   <param>-Dcom.ibm.jsse2.sp800-131=strict</param>
   ```
4. Editez *emplacement_installation*`\bin64\cogconfig.bat` (Windows) ou *emplacement_installation*`\bin64\cogconfig.sh` (Linux, UNIX) pour ajouter les lignes suivantes après la ligne `set J_OPTS=%DD_OPTS% %J_OPTS%` :

   Windows :

   ```
   set J_OPTS="-Dcom.ibm.jsse2.overrideDefaultTLS=true" %J_OPTS%
   set J_OPTS="-Dcom.ibm.jsse2.sp800-131=strict" %J_OPTS%
   ```

   Linux, UNIX :

   ```
   JAVA_OPTS=$JAVA_OPTS -Dcom.ibm.jsse2.overrideDefaultTLS=true
   JAVA_OPTS=$JAVA_OPTS -Dcom.ibm.jsse2.sp800-131=strict
   ```
5. Démarrez Cognos Configuration à l'aide de `cogconfig.bat` ou de `cogconfig.sh` que vous avez modifié à l'étape précédente.

   **Important :** Vous devez démarrer IBM Cognos Configuration en utilisant `cogconfig.bat` (que vous avez modifié pour inclure le magasin de clés et le mot de passe) et non pas l'exécutable habituel (cogconfigw.exe) ou le raccourci du menu Démarrer.

6. Sous **Accès aux données**, sous le type de connexion de base de données, sélectionnez la connexion.
7. Sélectionnez **True** pour **SSL Encryption Enabled**.
8. Testez la connexion et enregistrez votre configuration.
9. Démarrez Cognos Analytics. Vous devrez faire en sorte que le nom de serveur complet dans SQL Server Configuration Manager corresponde à celui indiqué dans le certificat (par exemple `mymachine.canlab.ibm.com` au lieu de `localhost`).

### Résultats

**Important :** Pour le code d'accès unique (SSO) et l'authentification Windows, vous devez placer `sqljdbc_auth.dll` dans le répertoire `bin64`. L'authentification Windows est une configuration de code d'accès unique. La sélection dans Configuration Manager pour Content Manager est appelée **Base de données Microsoft SQL Server (Authentification Windows)**.

## Utilisation de SSL pour les connexions de base de données dans IBM Cognos Configuration pour une base de données IBM Db2 ou Informix

Pour utiliser Secure Sockets Layer (SSL) pour les connexions de base de données dans IBM Cognos Configuration, vous devez importer le certificat SSL dans le magasin de clés Java, puis modifier certains fichiers de configuration IBM Cognos.

Vous pouvez utiliser SSL pour les connexions de base de données dans IBM Cognos Configuration, y compris les bases de données du magasin de contenu, de notification et de journalisation.

### Avant de commencer

Vous devez activer SSL sur votre serveur de base de données avant de configurer IBM Cognos en vue de l'utilisation de SSL pour les connexions de base de données.

Le certificat SSL doit avoir été exporté de votre serveur de base de données et être disponible sur l'ordinateur sur lequel vous configurez la connexion de base de données dans IBM Cognos Configuration.

### Procédure

1. Suivez les instructions de la documentation correspondant à votre version de base de données pour activer SSL sur le serveur de base de données et exporter le certificat SSL.
2. Téléchargez les fichiers JAR des règles de force illimitée.

   Pour IBM JRE, accédez au site https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk) et téléchargez `unrestrictedpolicyfiles.zip`. Décompressez les fichiers de règles dans le répertoire *`emplacement_installation`*`/jre/lib/security`.
3. Sur l'ordinateur sur lequel vous configurez la connexion à la base de données, importez le certificat SSL avec l'utilitaire keytool du JRE utilisé pour IBM Cognos Analytics. Par exemple, si vous utilisez le JRE fourni avec les installations IBM Cognos Analytics sous Microsoft Windows, procédez ainsi :
   a. Accédez au répertoire *`emplacement_installation`*`/jre/bin`.
   b. Exécutez la commande suivante.

```
keytool -import -file chemin/nom_fichier -keystore
nom_magasin_clés -alias nom_alias
```

Où *nom_magasin_clés* est le nom d'un nouveau magasin de clés et *nom_alias* est l'alias de votre choix pour le certificat.

c. Entrez le mot de passe du magasin de clés. Si vous ajoutez le certificat à un magasin de clés existant, entrez son mot de passe. Si vous créez un nouveau magasin de clés, entrez un mot de passe pour celui-ci.

**Important :** Le certificat SSL doit être importé dans le magasin de clés de l'environnement d'exécution Java que vous utilisez pour IBM Cognos Analytics.

4. Editez le fichier `java.security` pour y inclure le fournisseur SSL.
   a. Si vous utilisez le JRE fourni avec les installations IBM Cognos Analytics sous Microsoft Windows, accédez au répertoire *emplacement_installation*`/jre/lib/security`. Sinon, accédez au répertoire `lib/security` de l'environnement d'exécution Java que vous utilisez pour IBM Cognos Analytics.
   b. Ouvrez `java.security` dans un éditeur de texte.
   c. Recherchez les lignes suivantes dans le fichier :

      ```
      ssl.KeyManagerFactory.algorithm=IbmX509
      ssl.TrustManagerFactory.algorithm=PKIX
      ```

   d. Ajoutez lignes ci-dessous après les lignes précédentes.

      ```
      ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
      ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
      ```

   e. Sauvegardez et fermez le fichier.
5. Editez le fichier IBM Cognos `startwlp`. Ce fichier est utilisé lors du démarrage d'IBM Cognos Analytics.
   a. Accédez au répertoire *emplacement_installation*`/bin64`.
   b. Ouvrez le fichier `startwlp.bat` dans un éditeur de texte. Sous UNIX ou Linux, ouvrez le fichier `startwlp.sh`.
   c. Recherchez la ligne suivante dans le fichier.

      Windows :

      ```
      set JVM_ARGS=-Dcom.ibm.cognos.disp.useDaemonThreads=true %JVM_ARGS%
      ```

      Linux, UNIX :

      ```
      DISP_OPTS="-Dcom.ibm.cognos.disp.useDaemonThreads=true"
      ```

   d. Ajoutez lignes ci-dessous après les lignes précédentes.

      Windows :

      ```
      set JVM_ARGS=-Dcom.ibm.jsse2.usefipsprovider=true %JVM_ARGS%
      set JVM_ARGS=-Djavax.net.ssl.trustStore=chemin/nom_magasin_clés %JVM_ARGS%
      ```

      Linux, UNIX :

      ```
      DISP_OPTS="-Dcom.ibm.jsse2.usefipsprovider=true %DISP_OPTS%"
      DISP_OPTS="-Djavax.net.ssl.trustStore=path/keystorename"
      ```

      Où *chemin* est le chemin du magasin de clés et *nom_magasin_clés* est son nom.

   e. Sauvegardez et fermez le fichier.
6. Editez le fichier `bootstrap_wlp_`*version_se*`.xml`. Ce fichier est utilisé lors du démarrage d'IBM Cognos Analytics en tant que service à partir d'IBM Cognos Configuration.
   a. Accédez au répertoire *emplacement_installation*`/bin64`.
   b. Ouvrez le fichier `bootstrap_wlp_`*version_se*`.xml` dans un éditeur de texte.

c. Ajoutez les lignes suivantes au fichier.

```
<param>"-Dcom.ibm.jsse2.usefipsprovider=true"</param>
<param>"-Djavax.net.ssl.trustStore=chemin/nom_magasin_clés"</param>
```

Où *chemin* est le chemin du magasin de clés et *nom_magasin_clés* est son nom.

d. Sauvegardez et fermez le fichier.

7. Editez le fichier IBM Cognos `cogconfig`.
   a. Accédez au répertoire *emplacement_installation*/`bin64`.
   b. Ouvrez le fichier `cogconfig.bat` dans un éditeur de texte. Sous UNIX ou Linux, ouvrez le fichier `cogconfig.sh`.
   c. Recherchez la ligne suivante dans le fichier.

      Windows :

      ```
      J_OPTS=%DD_OPTS% %J_OPTS% %DEBUG_OPTS%
      ```

      Linux, UNIX :

      ```
      $JAVA_CMD $JAVA_OPTS CRConfig $*
      ```

   d. Ajoutez lignes ci-dessous après les lignes précédentes.

      Windows :

      ```
      set J_OPTS=-Dcom.ibm.jsse2.usefipsprovider=true %J_OPTS%
      set J_OPTS=-Djavax.net.ssl.trustStore=chemin/nom_magasin_clés %J_OPTS%
      ```

      Linux, UNIX :

      ```
      JAVA_OPTS="$JAVA_OPTS -Dcom.ibm.jsse2.usefipsprovider=true %JAVA_OPTS%"
      JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore=chemin/nom_magasin_clés"
      ```

      Où *chemin* est le chemin du magasin de clés et *nom_magasin_clés* est son nom.

   e. Sauvegardez et fermez le fichier.
8. Démarrez IBM Cognos Configuration à l'aide du fichier `cogconfig` que vous avez modifié.
   - Sur les systèmes d'exploitation Microsoft Windows, cliquez deux fois sur le fichier `cogconfig.bat` que vous avez modifié.
   - Sous UNIX ou Linux, exécutez le fichier `cogconfig.sh` que vous avez modifié.
9. Sous **Accès aux données**, sous le type de connexion de base de données, sélectionnez la connexion.

   Vous pouvez utiliser SSL pour les connexions à la base de données du magasin de contenu, aux bases de données de notification et de journalisation, et à celles des tâches manuelles et des annotations.
10. Sélectionnez **Vrai** pour **Chiffrement SSL activé**.
11. Testez la connexion.
12. Enregistrez la configuration et redémarrez les services.

## Utilisation de SSL pour les connexions de base de données dans IBM Cognos Configuration pour une base de données Oracle

Pour utiliser Secure Sockets Layer (SSL) pour les connexions de base de données dans IBM Cognos Configuration, vous devez importer le certificat SSL dans le magasin de clés Java, puis modifier certains fichiers de configuration IBM Cognos.

Vous pouvez utiliser SSL pour les connexions de base de données dans IBM Cognos Configuration, y compris les bases de données du magasin de contenu, de notification et de journalisation.

## Avant de commencer

Vous devez activer SSL sur votre serveur de base de données avant de configurer IBM Cognos en vue de l'utilisation de SSL pour les connexions de base de données.

## Procédure

1. Editez le fichier IBM Cognos `startwlp`.
   a. Accédez au répertoire *emplacement_installation*/bin64.
   b. Ouvrez le fichier `startwlp.bat` dans un éditeur de texte. Sous UNIX ou Linux, ouvrez le fichier `startwlp.sh`.
   c. Ajoutez les lignes suivantes au fichier.

      ```
      set JVM_ARGS=-Doracle.net.ssl_version=3 %JVM_ARGS%
      set JVM_ARGS=-Doracle.net.ssl_client_authentication=false %JVM_ARGS%
      set JVM_ARGS=-Doracle.net.wallet_location=(SOURCE=(METHOD=file)
      (METHOD_DATA=(DIRECTORY=path/client_wallet))) %JVM_ARGS%
      ```

      Le paramètre *path* est le chemin d'accès au répertoire du portefeuille Oracle du client et *client_wallet* est son nom.
   d. Enregistrez et fermez le fichier.
2. Editez le fichier `bootstrap_wlp_version_se.xml`.

   Ce fichier est utilisé lors du démarrage d'IBM Cognos Analytics en tant que service à partir d'IBM Cognos Configuration.
   a. Accédez au répertoire *emplacement_installation*/bin64.
   b. Ouvrez le fichier `bootstrap_wlp_version_se.xml` dans un éditeur de texte.
   c. Ajoutez les lignes suivantes au fichier.

      ```
      <param>-Doracle.net.ssl_version=3</param>
      <param>-Doracle.net.ssl_client_authentication=false</param>
      <param>-Doracle.net.wallet_location=(SOURCE=(METHOD=file)(METHOD_DATA=(DIRECTORY=path/client_w
      ```

      Les paramètres Java de ce fichier doivent être les mêmes qu'à l'étape 1.

      **Conseil :** L'utilisation de guillemets dans le fichier `bootstrap_wlp_linux38664.xml` empêche IBM Java de démarrer et entraîne le blocage et l'échec du démarrage de Cognos.
   d. Enregistrez et fermez le fichier.
3. Editez le fichier IBM Cognos `cogconfig`.
   a. Accédez au répertoire *emplacement_installation*/bin64.
   b. Ouvrez le fichier `cogconfig.bat` dans un éditeur de texte. Sous UNIX ou Linux, ouvrez le fichier `cogconfig.sh`.
   c. Ajoutez les lignes suivantes au fichier.

      ```
      set J_OPTS=-Doracle.net.ssl_version=3 %J_OPTS%
      set J_OPTS=-Doracle.net.wallet_location=(SOURCE=(METHOD=file)
      (METHOD_DATA=(DIRECTORY=path/client_wallet))) %J_OPTS%
      set J_OPTS=-Doracle.net.ssl_client_authentication=false %J_OPTS%
      ```
   d. Enregistrez et fermez le fichier.
4. Copiez les fichiers des pilotes Oracle suivants dans le répertoire *emplacement_installation*/drivers.
   - `jssl-1_1.jar`
   - `oraclepki.jar`

- `osdt_cert.jar`
- `osdt_core.jar`

5. Démarrez IBM Cognos Configuration.
6. Sous **Accès aux données**, pour le type de connexion de base de données, sélectionnez la connexion.

   Vous pouvez utiliser SSL pour les connexions à la base de données du magasin de contenu, aux bases de données de notification et de journalisation, et à celles des tâches manuelles et des annotations.

   **Conseil :** Vérifiez que la connexion utilise le type **Base de données Oracle (options avancées)**. Si vous n'avez pas sélectionné le type **Base de données Oracle (options avancées)**, supprimez la connexion à la base de données et créez-en une qui l'utilise.
7. Sélectionnez **True** pour **SSL Encryption Enabled**.
8. Testez la connexion.
9. Enregistrez la configuration et redémarrez les services.

## Sécurisation des sources de données JDBC avec SSL

Sécurisation des sources de données JDBC avec SSL

### Procédure

1. Vérifiez que le serveur de données est configuré pour SSL en dehors de l'environnement IBM Cognos Analytics.
2. Dans Cognos Analytics, vérifiez que l'URL JDBC et/ou les propriétés de connexion au serveur de données ont été mises à jour pour inclure tous les paramètres requis, conformément à la documentation du fournisseur pour l'activation de SSL via JDBC. Voici un exemple de paramètre d'URL JDBC requis lorsque Db2 est le serveur de données : Exemple de connexion au serveur de données DB2
3. Importez le(s) certificat(s) SSL dans le magasin de clés certifiées JRE IBM Cognos d'après la documentation suivante (les certificats doivent être importés dans `jre/lib/security/cacerts` et le mot de passe par défaut est `changeit`) : Importation des certificats de CA dans les composants IBM Cognos

# Configuration de connexions de source de données JDBC pour un code d'accès unique à l'aide de Kerberos

Vous pouvez configurer un code d'accès unique à l'aide du protocole Kerberos pour les connexions de sources de données JDBC utilisées pour le mode de requête dynamique (DQM).

Sauf pour Microsoft SQL Server, l'authentification de source de données avec un code d'accès unique n'est prise en charge que pour le mode de requête dynamique.

`11.0.6` La prise en charge de la délégation contrainte (extension Microsoft à Kerberos) permet à un service d'obtenir un ticket pour un autre service pour le compte de l'utilisateur en présentant le ticket de service de l'utilisateur à lui-même. Le ticket de service est délégué par l'utilisateur (Service for User to Proxy - S4U2Proxy) ou généré par le service lui-même si l'utilisateur est authentifié par d'autres moyens.

Pour configurer une source de données en vue de l'autentification unique à la connexion avec Kerberos, vous devez :

- Créer un fichier d'initialisation Kerberos.
- Configurer un nom principal de service (SPN) pour la source de données du mode de requête dynamique.
- Créer un fichier de clés.
- Configurer le module de connexion Kerberos. Il existe une nouvelle autre procédure pour la version 11.0.6
- Configurer les connexions de source de données.

Avant de commencer, vous devez vous assurer que les critères suivants sont satisfaits :

1. Le service IBM Cognos est configuré pour un code d'accès unique à l'aide d'un espace-noms Microsoft Active Directory.
2. La base de données est configurée pour utiliser le protocole Kerberos.
3. Les utilisateurs Active Directory sont également configurés sur le serveur de base de données.
4. 11.0.6 Si le code d'accès unique est configuré avec une délégation contrainte, vérifiez la documentation du pilote pour vous assurer que ce dernier prend en charge la délégation contrainte. Les pilotes qui prennent en charge l'authentification Kerberos ne prennent pas tous en charge également la délégation contrainte.

   La requête dynamique prend en charge la délégation contrainte de Kerberos avec les pilotes JDBC pour Netezza et Cloudera Impala. Cette fonctionnalité requiert des pilotes JDBC de versions suivantes (ou ultérieures) étendus pour recevoir les données d'identification GSS : Netezza 7.2.0.9-P3 et 7.2.1.3-P3 (pour plus d'informations, voir http://www-01.ibm.com/support/docview.wss?uid=swg21997658) et Cloudera Impala 2.5.36

   IBM Cognos Analytics peut être utilisé avec un environnement d'exécution Java ORACLE ou IBM. Vous trouverez les versions requises par IBM dans la page des environnements pris en charge. Les personnes qui tentent d'utiliser Cognos Analytics avec un environnement d'exécution Java IBM et une connectivité JDBC Cloudera Impala doivent utiliser l'environnement d'exécution Java IBM 8.0.3.12 (ou une version ultérieure). Voir https://developer.ibm.com/javasdk/downloads/sdk8/.

## Utilisation de l'authentification Kerberos sans code d'accès unique

Si vous ne configurez pas l'espace-noms Active Directory, vous pouvez néanmoins configurer votre source de données en vue de l'authentification Kerberos. Le service de requête dynamique interprète les données d'identification que vous fournissez (nom d'utilisateur et mot de passe) en tant que données d'identification pour l'obtention d'un ticket d'octroi d'autorisations (TGT) auprès du centre de distribution Kerberos (Active Directory ou une autre implémentation Kerberos). Ces données d'identification peuvent être fournies par un code d'accès, ou saisies par l'utilisateur lorsqu'il est invité à le faire pour la base de données. Dans ce cas, la configuration est différente :

- Il n'est pas nécessaire d'enregistrer un nom principal de service (SPN).
- Il n'est pas nécessaire de créer un fichier de clés.
- 11.0.6 Vous n'avez **pas** besoin de configurer le module de connexion Kerberos.

11.0.0- 11.0.5 Vous devez configurer le module de connexion Kerberos, mais vous n'avez pas besoin de spécifier le nom principal de service et la spécification de fichier de clés.

- Vous devez fournir un fichier d'initialisation Kerberos.

## Création de fichiers d'initialisation Kerberos

Vous devez créer un fichier d'initialisation Kerberos et le placer à un endroit spécifique sur tous les ordinateurs sur lesquels les composants du groupe de serveurs d'applications sont installés. Le fichier d'initialisation Kerberos, `krb5.conf`, est utilisé par l'implémentation du protocole Kerberos du JRE.

Pour plus d'informations sur les fichiers d'initialisation Kerberos, consultez le site MIT Kerberos Documentation (web.mit.edu/kerberos/krb5-devel/doc/admin/conf_files/krb5_conf.html).

### Procédure

Sur tous les ordinateurs sur lesquels les composants du groupe de serveurs d'applications sont installés, copiez le fichier `krb5.conf` dans le répertoire `JAVA_HOME/lib/security`.
Sur les ordinateurs UNIX, copiez le fichier `krb5.conf` dans le répertoire `/etc/krb5`.
Sur les ordinateurs Linux, copiez le fichier `krb5.conf` dans le répertoire `/etc`.
Sur les ordinateurs Microsoft Windows, copiez le fichier `krb5.conf` dans le répertoire `C:\winnt` et renommez-le `krb5.ini`.

## Création d'un nom principal de service pour le service de requête

Vous devez créer un nom principal de service (SPN) pour le service de requête à utiliser. Le nom principal de service doit être configuré avec un utilisateur de domaine Active Directory approuvé pour la délégation.

Le nom principal de service doit avoir le format `spn@DOMAINE`. La valeur `spn` a le format *`nom de service/nom de domaine complet`* et `DOMAINE` représente le nom de domaine configuré dans le fichier d'initialisation Kerberos. Par exemple, si dqm est le nom de service, `dqm/monserveur.mondomaine.com@MONDOMAINEWINDOWS.COM`.

Si l'utilisateur de domaine Active Directory a pour nom dqmuser, vous devez enregistrer le nom principal de service à l'aide de la commande suivante :

```
setspn -s dqm/myserver.mydomain.com mywindowsdomain\dqmuser
```

Vous pouvez utiliser les paramètres **`-L`** et **`-Q`** pour vérifier que le nom principal de service a été créé correctement. Par exemple :

```
setspn -L mywindowsdomain\dqmuser
```

```
setspn -Q dqm/myserver.mydomain.com
```

## Création d'un fichier de clés

Après avoir créé le nom principal de service, vous devez créer un fichier de clés pour le service. Le fichier de clés permet au service de se connecter sans mot de passe. Le fichier de clés doit être recréé si le mot de passe du compte de service change.

### Procédure

Utilisez la commande suivante pour créer un fichier de clés :
`ktpass -out krb5.keytab -princ` *`SPN`* `-mapUser` *`username`* `-mapOp set -pass` *`password`* `-pType KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT`
Par exemple :
`ktpass -out krb5.keytab -princ` *`dqm/myserver.mydomain.com@mywindowsdomain.com`* `-mapUser` *`dqmuser@mywindowsdomain`* `-mapOp set -pass` *`password`* `-pType KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT`

## Configuration du module de connexion Kerberos

Vous devez configurer le module de connexion Kerberos pour permettre au service de requête IBM Cognos de se connecter au domaine Active Directory. Pour autoriser la connexion, le pack JAAS (Java Authentication and Authorization Service) a besoin d'un fichier de configuration.

Il existe deux procédures possibles, en fonction de votre version de Cognos Analytics.

11.0.6+

Pour configurer le module de connexion de Kerberos avec le code d'accès unique (Active Directory) :

1. Dans Cognos Configuration, sélectionnez l'espace-noms Active Directory dans **Sécurité** > **Authentification**.
2. Dans la propriété **Nom du principal du service DQM**, entrez la valeur exactement tel qu'elle est répertoriée dans le fichier de clés.

   Utilisez la commande **`klist -k <fichier de clés>`** pour rechercher le nom principal.
3. Renommez le fichier de clés en `ibmcognosba.keytab` et placez-le dans le dossier *`emplacement_installation`*`/configuration`.

Cognos Analytics crée dynamiquement la configuration de connexion nécessaire.

11.0.0+ 11.0.5 Cette procédure peut toujours être utilisée dans la version 11.0.6+

Un fichier de configuration doit être inclus dans le fichier `java.security` du répertoire *`JRE_HOME`*`/lib/security`. Vous devez inclure une ligne telle que la ligne suivante dans le fichier `java.security`.

```
login.config.url.1=file:///${java.home}/lib/security/jaas.conf
```

Des exemples de configuration JAAS sont fournis dans l'installation IBM Cognos. Les exemples de fichiers sont nommés `jaas-ibm.config` et `jaas-oracle.config`, et figurent dans *`emplacement_installation`*`\configuration`.

Dans les exemples de fichiers, vous devez remplacer les valeurs suivantes :

- *`<principal name>`* est le nom principal de service que vous avez créé.
- *`<keytab file specification>`* est le chemin d'accès et le nom du fichier de clés que vous avez créé.

Si vous n'utilisez pas une connexion de base de données configurée pour l'authentification Kerberos pour la modélisation, au lieu de modifier le fichier

java.security, vous pouvez indiquer le fichier de configuration JAAS comme un paramètre de démarrage supplémentaire pour le service de requête dans IBM Cognos Administration. Dans IBM Cognos Administration, sous **Système**, développez le serveur, sélectionnez **Service de requête** > **Définir les propriétés** > **Paramètres** et entrez la valeur dans **Autres arguments JVM pour le service de requête** au format `-Djava.security.auth.login.config=<fichier de configuration>`.

## Vérification de la configuration Kerebos

Pour vérifier la configuration JAAS (Java Authentication and Authorization Service) et le fichier, vous pouvez lancer une commande **java** depuis le JRE utilisé par Cognos Analytics.

### Procédure

Exécutez la commande suivante depuis *emplacement_installation*/webapps/p2pd/WEB-INF/lib **java -cp xqeService.jar -Dcom.ibm.security.krb5.Krb5Debug=all -Dcom.ibm.security.jgss.debug=all com.cognos.xqe.util.KerberosSSOLoginHelper**
L'utilitaire tente de se connecter à l'aide du fichier de clés et affiche la trace de débogage Kerberos. Ensuite, il affiche `Helper login successful (La connexion de l'assistant a abouti)` ou `Helper Login failed (La connexion de l'assistant a échoué) <message d'erreur>`.

## Vérification du fonctionnement du pilote JDBC

Que le code d'accès unique soit configuré ou non, DQM nécessite que le pilote de base de données puisse créer des connexions à l'aide d'un sujet pré-autorisé. Un utilitaire fourni avec l'installation IBM Cognos Analytics permet de tester le pilote.

### Avant de commencer

L'utilitaire accepte les paramètres **url**, **uid** et **password**. Le pilote doit être installé dans le dossier *répertoire_installation*/webapps/p2pd/WEB-INF/lib.

### Procédure

Dans le dossier *emplacement_installation*/webapps/p2pd/WEB-INF/lib, sur la ligne de commande du JRE utilisé par Cognos, lancez la commande suivante : **java -cp xqeService.jar;<pilote.jar> com.cognos.xqe.util.KerberosConnectionHelper <nom de classe du pilote> <url jdbc> <utilisateur> <mot de passe>**
où :

- *<pilote.jar>* est le fichier jar contenant le pilote. Si le pilote a un trop grand nombre de fichiers jar, vous pouvez entrer "*" pour le paramètre de chemin d'accès aux classes.
- *<nom de classe du pilote>* est le nom de classe utilisé pour charger le pilote.
- *<url jdbc>* est l'URL de la connexion JDBC à la source de données, contenant les propriétés spécifiques au pilote pour l'authentification Kerberos.
- *<utilisateur>* est le principal Kerberos.
- *<mot de passe>* est le mot de passe du principal Kerberos.

L'utilitaire tente d'établir la connexion à la base de données à l'aide des paramètres fournis et affiche la trace de débogage Kerberos.

## Configuration des connexions de source de données à l'aide de Kerberos

Utilisez les instructions de cette rubrique lorsque vous configurez les chaînes de connexion des connexions de source de données à l'aide d'un code d'accès unique Kerberos.

### Procédure

1. A la section Code d'accès, sélectionnez **Espace-noms externe** et sélectionnez l'espace-noms Active Directory dans la liste. Pour les chaînes de connexion sur deux onglets (Mode natif et JDBC), la section Code d'accès est dans l'onglet Mode natif.
2. Dans la zone **Propriétés de connexion**, entrez `ibmcognos.authentication=java_krb5`, puis ajoutez les propriétés requises par le pilote JDBC pour l'authentification Kerberos, le cas échéant. Pour les connexions de source de données à deux onglets (Mode natif et JDBC), cette zone se trouve dans l'onglet **JDBC** et porte le nom **Paramètres de connexion JDBC**.

   Si IBM Cognos Analytics est installé sur un ordinateur exécutant un système d'exploitation Microsoft Windows, vous n'avez pas besoin d'indiquer `ibmcognos.authentication=java_krb5` pour des connexions de source de données Microsoft SQL Server et Teradata.
3. Testez la connexion de source de données.

### Exemple

Voici des exemples de propriétés de connexion de source de données pour certaines sources de données :

- Pour des connexions de source de données Teradata :

  `ibmcognos.authentication=java_krb5;LOGMECH=KRB5;`
- Pour des connexions de source de données SAP-HANA :

  `ibmcognos.authentication=java_krb5;`
- Pour des connexions de source de données Microsoft SQL Server :

  `ibmcognos.authentication=java_krb5;authenticationScheme=JavaKerberos;`

## Configuration d'un référentiel pour les messages de journal

Le protocole BI Bus inclut le traitement des messages des journaux, un outil de diagnostic important pour analyser le comportement d'IBM Cognos Analytics.

Outre les messages d'erreur, les messages de journal fournissent des informations sur le statut des composants et une vue de niveau supérieur des événements essentiels. Par exemple, les messages de journal peuvent donner des informations sur les tentatives de démarrage et d'arrêt des services, la fin du traitement des requêtes et les indicateurs d'erreurs fatales. Les journaux d'audit, disponibles depuis une base de données de journalisation, fournissent des informations sur l'activité des utilisateurs et des rapports.

Les services IBM Cognos de chaque ordinateur envoient des informations sur les erreurs et les événements vers un serveur de journalisation local. Un serveur de journalisation local est installé dans le dossier *emplacement_installation*`/logs` de tous les ordinateurs IBM Cognos Analytics sur lesquels Content Manager ou les composants du groupe de serveurs d'applications sont installés. Comme le serveur de journalisation utilise un port différent de celui des autres composants d'IBM

Cognos Analytics, il continue à traiter les événements même si d'autres services de l'ordinateur local, tels que le répartiteur, sont désactivés.

Le flux de travaux ci-dessous indique les tâches requises pour préparer la journalisation.

- Lors de la planification, déterminez la configuration de journalisation adaptée à votre environnement. Par exemple, évaluez différents référentiels de messages de journal, tels que les fichiers journaux et les serveurs de journalisation distants (exemple : le journal système UNIX ou Linux ou le journal des événements Windows NT), en plus du fichier journal local. Vous pouvez également envoyer uniquement les informations des messages d'audit à une base de données. Tenez compte de la sécurité, notamment des méthodes disponibles pour protéger les fichiers journaux contre les pannes système ou l'altération par les utilisateurs.
- Lors de la configuration, définissez les propriétés de démarrage pour la journalisation et notamment les paramètres de connexion des bases de données. Vous devez aussi créer une base de données de journalisation si vous prévoyez de conserver les journaux d'audit. Si la communication entre un serveur de journalisation local et un serveur de journalisation distant doit être sécurisée, modifiez la configuration de façon appropriée sur les deux ordinateurs IBM Cognos Analytics. Vous pouvez également activer certaines fonctions de journalisation, par exemple la journalisation pour des utilisateurs particuliers.
- Lors de la configuration de la journalisation, définissez le niveau de détail à enregistrer dans le journal pour cibler les messages sur les informations pertinentes par rapport à votre entreprise. Les rapports d'audit peuvent également être configurés de manière à effectuer le suivi de l'activité des utilisateurs et des rapports.

  Pour en savoir davantage sur la configuration de la journalisation, reportez-vous au manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Pour plus d'informations sur l'utilisation des messages de journal pour le traitement des incidents liés à la journalisation, voir le manuel *IBM Cognos Analytics - Guide de traitement des incidents*.

## Instructions pour la création d'une base de données de journalisation

Vous pouvez créer une base de données pour stocker des messages de journal. La création d'une base de données de journalisation comprend les tâches suivantes :

- Création d'une base de données de journalisation.

  Pour IBM Db2, Oracle ou Microsoft SQL Server, utilisez la procédure ayant servi à la création de la base de données du magasin de contenu. Suivez les instructions présentées dans «Instructions pour la création du magasin de contenu», à la page 8.

  **Remarque :** Si vous utilisez Db2, vous ne pouvez pas générer un script pour créer la base de données de notification de la même manière que le magasin de contenu.

  Pour Db2 on z/OS, utilisez les instructions dans «Paramètres suggérés pour la création d'une base de données de journalisation sous Db2 on z/OS», à la page 206.
- Configurez la connectivité de la base de données.

  Suivez les instructions présentées dans «Connectivité à la base de données de journalisation», à la page 207.
- Indiquez le référentiel des messages de journal.

Suivez les instructions présentées dans «Référentiels de messages de journal», à la page 209.

## Paramètres suggérés pour la création d'une base de données de journalisation sous Db2 on z/OS

La base de données créée doit contenir certains des paramètres de configuration spécifiés.

Utilisez la liste de contrôle ci-dessous pour vous guider dans le processus de configuration de la base de données de journalisation dans Db2 on z/OS.

__ • Connectez-vous au système z/OS en tant qu'utilisateur ayant les privilèges d'administrateur dans Db2 on z/OS.

__ • Créez une instance de base de données, un groupe de stockage et un compte utilisateur pour le magasin de contenu. IBM Cognos utilise les données d'identification du compte utilisateur pour communiquer avec le serveur de bases de données.

__ • Allouez à un groupe de mémoire tampon une taille de page de 8 ko pour l'instance de base de données.

__ • Pour une base de données de journalisation dans Db2 on z/OS, les administrateurs doivent exécuter un script d'espace de table afin de créer des espaces de table destinés à contenir des objets importants et d'autres données pour la base de données de journalisation, puis octroyer des droits d'utilisateur sur la table. Pour en savoir davantage sur l'exécution du script d'espace de table, voir «Création d'espaces de table pour une base de données de journalisation dans Db2 on z/OS».

## Création d'espaces de table pour une base de données de journalisation dans Db2 on z/OS

Si vous utilisez IBM Db2 on z/OS, un administrateur de base de données doit exécuter un script pour créer un ensemble d'espaces de table requis pour la base de données de journalisation. Le script doit être modifié pour remplacer les paramètres génériques par ceux convenant à votre environnement.

Utilisez les convention de dénomination pour Db2 on z/OS. Par exemple, tous les noms de paramètres doivent commencer par une lettre et ne pas dépasser 6 caractères. Pour plus d'informations, voir le Knowledge Center d'Db2.

### Procédure

1. Connectez-vous à la base de données en tant qu'utilisateur disposant de privilèges afin de créer et d'insérer des espaces de table, ainsi qu'autoriser l'exécution d'instructions SQL.
2. Accédez au répertoire *emplacement_installation*`/configuration/schemas/logging/db2zos`.
3. Ouvrez le fichier de script `LS_tablespace_db2zOS.sql` et utilisez le tableau ci-après pour vous aider à remplacer les paramètres génériques par ceux convenant à votre environnement.

*Tableau 31. Noms et descriptions des paramètres d'espace de table pour une base de données de journalisation dans Db2 on z/OS*

| Nom du paramètre | Description |
|---|---|
| IPFSCRIPT_DATABASE | Nom de la base de données de journalisation. |

*Tableau 31. Noms et descriptions des paramètres d'espace de table pour une base de données de journalisation dans Db2 on z/OS (suite)*

| Nom du paramètre | Description |
|---|---|
| IPFSCRIPT_STOGROUP | Nom du groupe de stockage. |
| IPFSCRIPT_TABLESPACE | Nom de l'espace de table qui contient les tables de base dans la base de données de journalisation.<br><br>Cet espace de table n'est pas destiné aux tables auxiliaires. |
| IPFSCRIPT_LS_ID | Identificateur d'instance pour la base de données d'audit. Cette valeur ne doit pas dépasser deux caractères. |
| IPFSCRIPT_BP | Nom du groupe de mémoire tampon de 8 k alloué pour les objets normaux. |
| IPFSCRIPT_USERNAME | Compte utilisateur qui accède à la base de données de journalisation. |

Tous les paramètres listés ne figurent pas dans le script, mais pourront être ajoutés ultérieurement.

4. Enregistrez et exécutez le script.
5. Octroyez les droits d'utilisateur IBM Cognos pour les espaces de table créés lorsque vous avez exécuté le fichier script :
   - Ouvrez le fichier script `LS_rightsGrant_db2zOS.sql`.
   - Remplacez les valeurs des paramètres afin de les adapter à votre environnement.

     **Astuce :** utilisez les mêmes valeurs que celles utilisées lors de la création de groupes de mémoire tampon et du compte utilisateur.
   - Enregistrez et exécutez le script `LS_rightsGrant_db2zOS.sql`.

### Résultats

La base de données de journalisation est créée.

## Connectivité à la base de données de journalisation

Après la création d'une base de données pour les journaux d'audit, la configuration du client de base de données requiert des étapes supplémentaires si vous utilisez Oracle, IBM Db2 ou Informix Dynamic Server comme serveur de base de données.

Dans un environnement réparti, le serveur de journalisation local d'un ordinateur de composants du groupe de serveurs d'applications peut envoyer des messages de journal vers un serveur de journalisation distant, lequel envoie ensuite des messages à la base de données de journalisation. Pour Oracle et Db2, le pilote JDBC approprié et/ou le logiciel de client de base de données est requis uniquement sur l'ordinateur des composants du groupe de serveurs d'applications avec le serveur de journalisation distant qui se connecte à la base de données de journalisation.

### Microsoft SQL Server

Si vous utilisez une base de données Microsoft SQL Server, le fichier `JSQLConnect.jar` est installé par défaut à l'emplacement approprié. La seule autre

procédure consiste à s'assurer que Microsoft SQL Server utilise la connectivité TCP/IP.

## Configuration de la connectivité à une base de données de journalisation IBM Db2

Vous devez configurer le logiciel du client de base de données et le pilote JDBC sur tous les ordinateurs des composants du groupe de serveurs d'applications avec une connexion à la base de données de journalisation. Vous devez configurer le pilote JDBC sur l'ordinateur Content Manager, sauf si vous utilisez le même type de base de données que le magasin de contenu pour les messages de journal.

La version du pilote doit être au moins JCC 3.7 pour un système d'exploitation Linux ou UNIX, ou un système d'exploitation Microsoft Windows version 9.1 avec groupe de correctifs, ou JCC 3.42 pour un système d'exploitation Linux ou UNIX, ou un système d'exploitation Microsoft Windows version 9.5 groupe de correctifs 2.

### Procédure

Copiez les fichiers suivants du répertoire *installation_DB2*\sqllib\java dans le répertoire *emplacement_installation*\drivers :

- Le fichier de pilote universel, db2jcc4.jar
- Le fichier de licence :

  Pour Db2 on Linux, UNIX ou Windows, utilisez db2jcc_license_cu.jar.

  Pour Db2 on z/OS, utilisez db2jcc_license_cisuz.jar.

  Si vous vous connectez à Db2 on z/OS, utilisez la version de pilote de Linux, UNIX ou le kit de mise à jour version 5 de Windows version 9.1, ou encore le kit de mise à jour version 2 de la version 9.5.

  **Conseil :** Pour vérifier la version du pilote, exécutez la commande suivante :

  ```
  java -cp chemin\db2jcc4.jar com.ibm.db2.jcc.DB2Jcc -version
  ```

## Configuration de la connectivité à une base de données de journalisation Oracle

Vous devez configurer le pilote JDBC sur tous les ordinateurs des composants du groupe de serveurs d'applications avec une connexion à la base de données de journalisation. Vous devez aussi configurer le pilote JDBC sur l'ordinateur Content Manager, sauf si vous utilisez le même type de base de données que le magasin de contenu pour les messages de journal.

### Procédure

1. Sur l'ordinateur où le client Oracle est installé, accédez au répertoire *ORACLE_HOME*/jdbc/lib.
2. Copiez le fichier de bibliothèque correspondant à votre version du client Oracle dans le répertoire *emplacement_installation*\drivers de l'ordinateur sur lequel Content Manager est installé et sur lequel la notification est envoyée à une base de données Oracle.

   Si vous utilisez Oracle 12c, vous devez disposer du fichier ojdbc7.jar.

   Si vous utilisez Oracle 11g, vous devez disposer du fichier ojdbc5.jar.

   Les fichiers sont disponibles dans le répertoire d'installation du client ou serveur Oracle ; ils peuvent également être téléchargés à partir du site Web Oracle Technology Network.

### Configuration de la connectivité à une base de données de journalisation Informix

Vous devez configurer le pilote JDBC sur tous les ordinateurs des composants du groupe de serveurs d'applications avec une connexion à la base de données de journalisation. Vous devez aussi configurer le pilote JDBC sur l'ordinateur Content Manager, sauf si vous utilisez le même type de base de données que le magasin de contenu pour les messages de journal.

#### Procédure

1. Sur l'ordinateur sur lequel Informix est installé, accédez au répertoire *emplacement_Informix*/sqllib/java.
2. Copiez les fichiers suivants dans le répertoire *emplacement_installation*\drivers de chaque ordinateur sur lequel Content Manager est installé.
   - le fichier de pilote universel, db2jcc4.jar
   - Le fichier de licence, db2jcc4_license_cisuz.jar

## Référentiels de messages de journal

Un serveur de journalisation local est automatiquement installé lors de l'installation de Content Manager ou des composants du groupe de serveurs d'applications. Vous pouvez définir un ou plusieurs référentiels vers lesquels le serveur de journal local envoie les messages de journal.

### Envoi de messages de journal à un serveur de journalisation distant

Dans une installation répartie, vous pouvez configurer le serveur de journalisation de chaque ordinateur IBM Cognos de façon à envoyer des messages de journal vers un seul serveur de journalisation distant, lequel agit tel un serveur de journal partagé. Vous pouvez ensuite configurer le serveur de journal partagé pour envoyer les messages de journal vers un fichier ou une base de données en local sur un même ordinateur ou un ordinateur différent.

Si le serveur de journalisation distant devient indisponible, les messages de journal sont redirigés vers les fichiers de récupération de l'ordinateur local situés dans le répertoire *emplacement_installation*/logs/recovery/remote. Les noms de ces fichiers de récupération contiennent des informations d'horodatage. Ces fichiers ne sont pas lisibles comme des fichiers de journalisation ordinaires. Lorsque le serveur de journalisation est disponible, un processus de récupération automatique transfère toutes les informations de journalisation vers le serveur de journalisation distant et supprime les fichiers de journalisation locaux.

### Enregistrement des messages de journal dans un fichier

Le serveur de journalisation est configuré par défaut pour envoyer les messages de journal vers le fichier *emplacement_installation*/logs/cogaudit.log. Le fichier journal par défaut est automatiquement créé s'il n'existe pas au démarrage du service IBM Cognos.

Vous pouvez configurer le serveur de journal de façon à envoyer les messages de journal vers un autre fichier. Si vous configurez un fichier journal différent, IBM Cognos tente automatiquement de créer ce fichier au démarrage, en plus du fichier journal par défaut. Si l'emplacement du fichier journal configuré est différent du répertoire *emplacement_installation*/logs, vous devez vous assurer que le chemin d'accès au fichier journal existe avant de démarrer le service IBM Cognos. Par

exemple, si vous configurez le serveur de journalisation de façon à envoyer les messages vers le fichier /usr/lpp/logfiles/cognos.log, IBM Cognos tente automatiquement de créer le fichier `cognos.log` dans le dossier `/usr/lpp/logfiles`. Si ce dossier n'existe pas, IBM Cognos ne crée pas le fichier `cognos.log` et aucun message de journal ne peut y être consigné. Notez que ces messages de journal ne sont pas consignés dans le fichier journal par défaut. Bien qu'IBM Cognos crée automatiquement le fichier journal par défaut même si un autre fichier journal est configuré, le fichier journal par défaut n'est pas utilisé comme sauvegarde.

## Enregistrement des messages de journal dans une base de données

Le serveur de journalisation peut également envoyer des journaux d'audit vers le même ordinateur ou sur un ordinateur différent. Les journaux d'audit fournissent des informations sur l'activité des utilisateurs et des rapports.

La base de données de journalisation présente les mêmes exigences de configuration et de compte utilisateur que la base de données du magasin de contenu. Après avoir configuré les composants d'IBM Cognos pour qu'ils envoient des messages à une base de données de journalisation, puis redémarré le service IBM Cognos, les composants d'IBM Cognos créent les tables et les zones de table requises. Vous pouvez tester la connexion à la base de données de journalisation avant de redémarrer le service IBM Cognos.

## Définition du référentiel des messages de journal pour IBM Db2 on UNIX, Linux ou Windows

Vous pouvez configurer un type de référentiel pour les messages de journal et configurer ensuite les propriétés pour le référentiel spécifique. Vous pouvez également configurer plusieurs référentiels pour des messages de journal.

### Avant de commencer

Avant de spécifier une base de données en tant que référentiel, vérifiez que

__ • vous avez créé la base de données de journalisation

__ • avez configuré le client de base de données

### Procédure

1. Sur l'ordinateur où vous avez installé Content Manager ou les composants du groupe de serveurs d'applications, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, dans la section **Environnement**, cliquez sur **Journalisation**.
3. Dans la fenêtre **Propriétés**, consultez le tableau suivant pour définir les propriétés du serveur de journalisation.

*Tableau 32. Propriétés du serveur de journalisation*

| Tâche | Action |
|---|---|
| Utilisation de TCP entre les composants d'IBM Cognos sur un ordinateur et son serveur de journalisation local | Définissez la propriété **Voulez-vous activer le protocole TCP** sur **Vrai**.<br><br>UDP offre une communication plus rapide avec un risque moindre de perte de connexion que le protocole TCP. Cependant, le risque de perte d'une connexion locale via TCP est faible. Le protocole TCP est toujours utilisé pour la communication entre un serveur de journalisation local et un serveur de journalisation distant. |
| Modification du nombre d'unités d'exécution disponibles pour le serveur de journalisation local | Tapez la valeur de la propriété **Nombre maximal d'unités d'exécution du serveur de journalisation local**.<br><br>Conservez la valeur par défaut de 10. La plage est comprise entre 1 et 20.<br><br>Cependant, si vous disposez d'un nombre élevé de messages de journal, vous pouvez allouer davantage d'unités d'exécution pour améliorer les performances. |

4. Dans la fenêtre **Explorateur**, sous **Environnement**, cliquez avec le bouton droit sur **Journalisation**, puis sélectionnez **Nouvelle ressource** > > **Destination**.
5. Dans la zone **Nom**, saisissez le nom du référentiel.
6. Dans la liste **Type**, cliquez sur le type de référentiel, puis sur **OK**.
7. Si le référentiel est un fichier, dans la fenêtre **Propriétés**, saisissez les valeurs appropriées pour les propriétés obligatoires et facultatives.
8. Si le référentiel est un serveur de journalisation distant, saisissez les valeurs appropriées pour les propriétés obligatoires et facultatives dans la fenêtre **Propriétés**.

   Si l'**URI interne du répartiteur** de l'ordinateur contenant le référentiel est configuré de manière à utiliser le protocole SSL, dans la fenêtre **Propriétés**, définissez la propriété **Activation du protocole SSL** sur **Vrai**.

   Vous devez ensuite définir le référentiel des messages de journal lorsque vous configurez le serveur de journalisation distant.
9. Si le référentiel est une base de données, dans la fenêtre **Explorateur**, sous **Journalisation**, définissez le type de base de données et ses propriétés de la façon suivante :
   - Cliquez avec le bouton droit de la souris sur le nom de la base de données, puis cliquez sur **Nouvelle ressource**, et sur **Base de données**.
   - Dans la zone **Nom**, saisissez le nom du référentiel.
   - Dans la liste **Type**, cliquez sur le type de base de données approprié, puis sur le bouton **OK**.
   - Dans la fenêtre **Propriétés**, saisissez les valeurs appropriées pour les propriétés facultatives et obligatoires.

     Pour une base de données Microsoft SQL Server, vous pouvez utiliser un numéro de port, tel que 1433, ou une instance nommée en tant que valeur de la propriété **Serveur de base de données comportant un numéro de**

**port ou un nom d'instance**. Incluez le numéro du port si vous utilisez des ports non définis par défaut. Incluez le nom de l'instance de Microsoft SQL Server s'il en existe plusieurs.

Pour vous connecter à une instance nommée, vous devez indiquer son nom en tant que propriété URL JDBC ou source de données. Par exemple, vous pouvez taper **localhost\instance1**. Si aucune propriété de nom d'instance n'est indiquée, une connexion à l'instance par défaut est créée.

Notez que les propriétés indiquées pour l'instance nommée, ainsi que l'ID utilisateur, le mot de passe et le nom de la base de données, servent à créer une adresse URL JDBC. Voici un exemple :

jdbc:JSQLConnect://localhost\\instance1/user=sa/*plus de propriétés en fonction des besoins*

- Testez la connexion à la nouvelle base de données. Dans la fenêtre **Explorateur**, sous **Environnement**, cliquez avec le bouton droit sur **Journalisation**, puis sélectionnez **Tester**.

  Les composants d'IBM Cognos se connectent à la base de données. Si vous avez configuré plusieurs bases de données pour la journalisation des messages, les composants d'IBM Cognos testent l'ensemble des bases de données.

10. Répétez les étapes 5 à 10 pour chacun des référentiels auxquels le serveur de journalisation doit envoyer des messages.
11. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
12. Dans la fenêtre **Explorateur**, cliquez sur **Services IBM Cognos** > **IBM Cognos**.
13. Dans le menu **Fichier**, cliquez sur **Redémarrer**.

    Si vous avez sélectionné une base de données comme référentiel, les composants d'IBM Cognos créent les tables et les zones requises dans la base de données que vous avez créée.

### Résultats

Si le référentiel était un serveur de journalisation distant, configurez le serveur de journalisation distant et démarrez-le. Redémarrez ensuite le service IBM Cognos sur l'ordinateur local.

Si le référentiel est une base de données, vous pouvez utiliser les composants d'IBM Cognos pour exécuter les rapports de journalisation à partir de la base de données.

Vous pouvez également définir le niveau de journalisation qui contrôle la quantité de détails et le type de messages qui sont envoyés vers un fichier ou une base de données de journalisation. Pour obtenir des instructions, voir le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

## Définition du référentiel des messages de journal pour IBM Db2 on z/OS

Vous pouvez configurer un type de référentiel pour les messages de journal et configurer ensuite les propriétés pour le référentiel spécifique. Vous pouvez également configurer plusieurs référentiels pour des messages de journal.

### Procédure

1. Sur l'ordinateur où vous avez installé Content Manager ou les composants du groupe de serveurs d'applications, démarrez IBM Cognos Configuration.

2. Dans la fenêtre **Explorateur**, dans la section **Environnement**, cliquez sur **Journalisation**.
3. Dans la fenêtre **Propriétés**, consultez le tableau suivant pour définir les propriétés du serveur de journalisation.

*Tableau 33. Propriétés du serveur de journalisation*

| Tâche | Action |
|---|---|
| Utilisation de TCP entre les composants d'IBM Cognos sur un ordinateur et son serveur de journalisation local | Définissez la propriété **Voulez-vous activer le protocole TCP** sur **Vrai**.<br><br>UDP offre une communication plus rapide avec un risque moindre de perte de connexion que le protocole TCP.<br><br>Le protocole TCP est utilisé pour la communication entre un serveur de journalisation local et un serveur de journalisation distant. |
| Modification du nombre d'unités d'exécution disponibles pour le serveur de journalisation local | Tapez la valeur de la propriété **Nombre maximal d'unités d'exécution du serveur de journalisation local**.<br><br>Conservez la valeur par défaut de 10. La plage est comprise entre 1 et 20. Cependant, si vous disposez d'un nombre élevé de messages de journal, vous pouvez allouer davantage d'unités d'exécution pour améliorer les performances. |

4. Dans la fenêtre **Explorateur**, sous **Environnement**, cliquez avec le bouton droit sur **Journalisation**, puis sélectionnez **Nouvelle ressource** > > **Destination**.
5. Dans la zone **Nom**, saisissez le nom du référentiel.
6. Dans la liste **Type**, cliquez sur **Base de données**, puis sur le bouton **OK**.
7. Dans la fenêtre **Explorateur**, sous **Journalisation**, cliquez avec le bouton droit sur le nom de la base de données, puis sélectionnez **Nouvelle ressource** > > **Base de données**.
8. Dans la zone **Nom**, saisissez le nom du référentiel.
9. Dans la liste **Type**, cliquez sur **Base de données DB2**, puis sur le bouton **OK**.
10. Dans la fenêtre **Propriétés**, tapez le **Serveur de base de données et numéro de port**, **ID utilisateur et mot de passe** et le **Nom de base de données** z/OS.

    Vérifiez que l'ID utilisateur correspond à la valeur indiquée pour le paramètre IPFSCRIPT_USERNAME dans le fichier script LS_tablespace_db2zOS.sql «Création d'espaces de table pour une base de données de journalisation dans Db2 on z/OS», à la page 206.
11. Dans la fenêtre **Explorateur**, cliquez sur **Configuration locale**.
12. Dans la fenêtre **Propriétés**, en regard de **Propriétés avancées**, cliquez dans la zone **Valeur**, puis sur l'icône Editer  .
13. Cliquez sur **Ajouter**, puis ajoutez les noms et les valeurs de paramètres de configuration d'après le tableau suivant :

*Tableau 34. Noms et valeurs des paramètres de configuration*

| Nom du paramètre | Valeur |
|---|---|
| IPFSCRIPT_CREATE_IN | Emplacement des tables de base.<br><br>Par exemple, Nombasededonnées.NomEspacetablebase |
| IPFSCRIPT_STOGROUP | Nom du groupe de stockage. |
| IPFSCRIPT_DATABASE | Nom de la base de données de journalisation. |
| IPFSCRIPT_LS_ID | Identificateur d'instance pour la base de données d'audit. Cette valeur ne doit pas dépasser deux caractères. |

14. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
15. Testez la connexion à la nouvelle base de données. Dans la fenêtre **Explorateur**, sous **Environnement**, cliquez avec le bouton droit sur **Journalisation**, puis sélectionnez **Tester**.

    Les composants d'IBM Cognos se connectent à la base de données. Si vous avez configuré plusieurs bases de données pour la journalisation des messages, les composants d'IBM Cognos testent l'ensemble des bases de données.

## Définition du référentiel des messages de journal pour Informix

Vous pouvez configurer un type de référentiel pour les messages de journal et configurer ensuite les propriétés pour le référentiel spécifique. Vous pouvez également configurer plusieurs référentiels pour des messages de journal.

### Procédure

1. Dans la fenêtre **Explorateur**, dans la section **Environnement**, cliquez sur **Journalisation**.
2. Dans la fenêtre **Propriétés**, consultez le tableau suivant pour définir les propriétés du serveur de journalisation.

*Tableau 35. Propriétés du serveur de journalisation*

| Tâche | Action |
|---|---|
| Utilisation de TCP entre les composants d'IBM Cognos sur un ordinateur et son serveur de journalisation local | Définissez la propriété **Voulez-vous activer le protocole TCP** sur **Vrai**.<br><br>UDP offre une communication plus rapide avec un risque moindre de perte de connexion que le protocole TCP.<br><br>Le protocole TCP est utilisé pour la communication entre un serveur de journalisation local et un serveur de journalisation distant. |

*Tableau 35. Propriétés du serveur de journalisation (suite)*

| Tâche | Action |
|---|---|
| Modification du nombre d'unités d'exécution disponibles pour le serveur de journalisation local | Tapez la valeur de la propriété **Nombre maximal d'unités d'exécution du serveur de journalisation local**.<br><br>Conservez la valeur par défaut de 10. La plage est comprise entre 1 et 20. Cependant, si vous disposez d'un nombre élevé de messages de journal, vous pouvez allouer davantage d'unités d'exécution pour améliorer les performances. |

3. Dans la fenêtre **Explorateur**, sous **Environnement**, cliquez avec le bouton droit sur **Journalisation**, puis sélectionnez **Nouvelle ressource** > > **Destination**.
4. Dans la zone **Nom**, saisissez le nom du référentiel.
5. Dans la liste **Type**, cliquez sur **Base de données**, puis sur le bouton **OK**.
6. Dans la fenêtre **Explorateur**, sous **Journalisation**, cliquez avec le bouton droit sur le nom de la base de données, puis sélectionnez **Nouvelle ressource** > > **Base de données**.
7. Dans la zone **Nom**, saisissez le nom du référentiel.
8. Dans la liste **Type**, cliquez sur **Base de données Informix Dynamic Server**, puis sur le bouton **OK**.
9. Dans la fenêtre **Propriétés**, indiquez les valeurs de **Serveur de base de données et numéro de port**, **ID utilisateur et mot de passe** et **Nom de base de données**.
10. Si vous possédez plusieurs instances d'une base de données de journalisation Informix, créez la propriété avancée IPFSCRIPTIDX et indiquez le compte sous lequel cette instance est exécutée :
    - Dans la fenêtre **Explorateur**, cliquez sur **Configuration locale**.
    - Dans la fenêtre **Propriétés**, cliquez sur la colonne **Valeur** de **Propriétés avancées**, puis sur l'icône Editer  .
    - Dans la boîte de dialogue **Valeur - Propriétés avancées**, cliquez sur l'option **Ajouter**.
    - Dans la colonne **Nom**, saisissez **IPFSCRIPTIDX**.
    - Dans la colonne **Valeur**, saisissez l'ID utilisateur correspondant au compte sous lequel l'instance de la base de données de journalisation est exécutée.

      Utilisez un compte utilisateur différent pour chaque instance de la base de données de journalisation Informix.
    - Répétez cette procédure pour chaque instance d'IBM Cognos Configuration qui utilise une instance de base de données de journalisation Informix.
11. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
12. Testez la connexion à la nouvelle base de données. Dans la fenêtre **Explorateur**, sous **Environnement**, cliquez avec le bouton droit sur **Journalisation**, puis sélectionnez **Tester**.

    Les composants d'IBM Cognos se connectent à la base de données. Si vous avez configuré plusieurs bases de données pour la journalisation des messages, les composants d'IBM Cognos testent l'ensemble des bases de données.

# Activation de la journalisation pour des utilisateurs particuliers

Lorsque vous diagnostiquez des problèmes, vous pouvez définir une journalisation temporaire afin de suivre un ou plusieurs utilisateurs particuliers et non tous les utilisateurs à la fois. Une fois le diagnostic effectué, vous pouvez reprendre la journalisation normale. Pour activer la journalisation pour les utilisateurs, utilisez IBM Cognos Configuration pour configurer les informations de connexion pour une technologie Java Management Extensions (JMX) qui fournit les outils qui gèrent et contrôlent les applications et les réseaux orientés service. Puis, configurez les informations de connexion JMX dans un fichier de propriétés de déploiement.

Une fois que la journalisation pour des utilisateurs particuliers a été activée pour les composants d'IBM Cognos, activez la journalisation pour un utilisateur particulier à l'aide du service de processus à distance pour JMX. Pour en savoir davantage, reportez-vous à la rubrique traitant de l'utilisation de la journalisation pour le diagnostic d'un problème propre à un utilisateur dans le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Vous devez installer Oracle Java SE Development Kit ou Java Software Development Kit pour IBM pour pouvoir activer la journalisation pour des utilisateurs particuliers.

## Configuration des informations de connexion JMX à l'aide d'IBM Cognos Configuration

La configuration des informations de connexion JMX (Java Management Extensions) dans IBM Cognos Configuration s'effectue en spécifiant un cookie et en définissant le port JMX et les données d'identification.

### Procédure

1. Démarrez IBM Cognos Configuration sur l'ordinateur où est installé Content Manager.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Dans la fenêtre **Propriétés**, configurez les propriétés JMX sous **Paramètres du répartiteur** :
   - Pour le **Port JMX externe**, saisissez un numéro de port disponible.
   - Pour **Donnée d'identification JMX externe**, cliquez sur l'icône Editer  dans la colonne **Value**, tapez un ID utilisateur et un mot de passe et cliquez sur **OK**.

     Grâce à l'ID utilisateur et au mot de passe, seul un utilisateur autorisé peut se connecter à l'environnement Java par le biais du **Port JMX externe** et indiquer le ou les utilisateurs à journaliser.
4. Enregistrez la configuration.

## Configuration des informations de connexion JMX dans un fichier de propriétés de déploiement

Pour que les paramètres JMX (Java Management Extensions) soient pris en charge sur le serveur d'applications, indiquez le port JMX dans le fichier des propriétés de déploiement p2pd.

### Procédure

1. Dans un éditeur de texte, ouvrez le fichier `p2pd.deploy_defaults.properties` situé dans le répertoire *`emplacement_installation`*`/webapps/p2pd/WEB-INF`.

2. Supprimez la mise en commentaire de la ligne `rmiregistryport` et définissez la valeur du **Port JMX externe** que vous avez configurée dans IBM Cognos Configuration.
3. Enregistrez le fichier `p2pd.deploy_defaults.properties`.
4. Redémarrez les services pour IBM Cognos.

### Résultats

IBM Cognos prend désormais en charge la journalisation pour un ou plusieurs utilisateurs. Pour en savoir davantage, reportez-vous à la rubrique traitant de l'utilisation de la journalisation pour le diagnostic d'un problème propre à un utilisateur dans le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

## Modification des paramètres globaux

Par défaut, les composants d'IBM Cognos appliquent une forme normalisée à tous les paramètres régionaux, qui peuvent provenir de différentes sources et se présenter sous divers formats. Cela signifie que tous les paramètres régionaux étendus sont conformes à une définition de langue et de code régional. Chaque ordinateur a des paramètres système régionaux par défaut et des paramètres régionaux par utilisateur. Les paramètres régionaux de l'utilisateur peuvent différer de ceux du système. Si vous modifiez les paramètres globaux sur l'un des ordinateurs Content Manager, vous devez effectuer les mêmes modifications sur les autres ordinateurs Content Manager.

Vous pouvez modifier les paramètres globaux pour :

- personnaliser la prise en charge linguistique de l'interface utilisateur
- personnaliser la prise en charge des devises
- personnaliser le support des paramètres régionaux
- associer la langue utilisée dans l'interface utilisateur du produit
- associer les paramètres régionaux de contenu
- ajouter des polices à l'environnement IBM Cognos
- personnaliser le fuseau horaire par défaut
- changer le codage des messages électroniques
- personnaliser les paramètres de cookie

## Personnalisation du support de langue de l'interface utilisateur

Utilisez la table Paramètres régionaux du produit pour ajouter ou supprimer des langues prises en charge par l'interface utilisateur. Par exemple, si vous n'avez pas besoin d'une interface utilisateur en allemand, vous pouvez supprimer cette langue de la liste.

La modification de la langue de l'interface utilisateur du produit n'affecte pas les données.

### Avant de commencer

Veillez à installer les polices appropriées pour la prise en charge des jeux de caractères et des symboles monétaires que vous utilisez. Pour que les symboles monétaires japonais et coréens s'affichent correctement, vous devez installer les

polices supplémentaires depuis le CD-ROM Supplementary Language Documentation.

### Procédure

1. Démarrez IBM Cognos Configuration sur chaque ordinateur Content Manager.
2. Dans le menu **Actions**, cliquez sur l'option **Editer la configuration globale**.
3. Cliquez sur l'onglet **Langues du produit**.

   Tous les environnements régionaux pris en charge sont affichés.
4. Cliquez sur **Ajouter**.

   **Conseil :** Pour supprimer un élément pris en charge, cochez la case située en regard de l'option **Paramètres régionaux pris en charge**, puis cliquez sur **Supprimer**.
5. Dans la deuxième colonne, saisissez la portion linguistique des paramètres régionaux.
6. Répétez les étapes 3 à 5 pour les autres langues prises en charge à ajouter.
7. Cliquez sur le bouton **OK**.
8. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Personnalisation de la prise en charge des devises

Si vous souhaitez disposer de devises supplémentaires ou en supprimer certaines de l'interface utilisateur, vous pouvez mettre à jour la liste des devises prises en charge dans la table Devises. Si vous utilisez des devises japonaises ou coréennes, vous devez configurer la prise en charge pour que les caractères du yen japonais et du won coréen s'affichent correctement.

Les composants d'IBM Cognos présentent, par défaut, uniquement un sous-ensemble des devises prises en charge dans l'interface utilisateur. Les devises sont identifiées par leur code ISO 4217. La liste complète des devises prises en charge que vous pouvez ajouter figure dans le fichier i18n_res.xml du répertoire *emplacement_installation*/bin.

L'ajout de devises à l'environnement d'IBM Cognos ne garantit pas que l'ordinateur dispose de la police nécessaire pour en afficher les symboles. Veillez à installer les polices appropriées pour la prise en charge des symboles des devises que vous utilisez. Par exemple, pour afficher correctement le symbole de la devise indienne (roupie), vous devez installer une police contenant ce caractère. En outre, pour que les symboles monétaires japonais et coréens s'affichent correctement, vous devez installer les polices supplémentaires depuis le CD de documentation du composant Supplementary Languages.

### Ajout de devises à l'interface utilisateur

Vous pouvez ajouter des devises (prises en charge ou non) dans l'interface utilisateur. Les devises prises en charge sont ajoutées dans IBM Cognos Configuration. Vous ajoutez des devises non prises en charge au fichier i18n_res.xml fourni dans IBM Cognos.

Si vous ajoutez un code de devise qui n'est pas pris en charge par IBM Cognos, vous devez l'ajouter manuellement au fichier i18n_res.xml dans le répertoire *emplacement_installation*/bin. Copiez ce fichier sur chaque ordinateur IBM Cognos de votre installation.

### Procédure

1. Démarrez IBM Cognos Configuration sur chaque ordinateur Content Manager.
2. Dans le menu **Actions**, cliquez sur l'option **Editer la configuration globale**.
3. Cliquez sur l'onglet **Devises**.
4. Cliquez sur **Ajouter**.

   **Conseil :** Pour supprimer un élément pris en charge, cochez la case située en regard de l'élément, puis cliquez sur **Supprimer**.
5. Dans la deuxième colonne, saisissez une valeur appropriée.

   La valeur que vous ajoutez doit être conforme aux codes ISO 4217 relatifs à la représentation des devises et des formats. Généralement, la valeur que vous ajoutez doit être un code alphabétique de trois lettres. Les deux premiers caractères sont les lettres représentant le code de pays ou de région ISO 3166 de la devise. La lettre supplémentaire correspond à l'initiale de la devise.
6. Répétez les étapes 3 à 5 pour les autres types d'éléments pris en charge à ajouter.
7. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Personnalisation du support des paramètres régionaux du contenu

Pour s'assurer que les utilisateurs visualisent les rapports, les données ou les métadonnées dans leur langue favorite ou avec des spécificités propres à leur région, vous pouvez ajouter des paramètres régionaux partiels (langues) ou complets (langue-région) à la table Paramètres régionaux (contenu). De cette façon, si le contenu est disponible dans plusieurs langues ou avec plusieurs spécificités régionales, il s'affiche pour les utilisateurs en fonction de leurs paramètres régionaux. Pour une partie du contenu du portail, les paramètres régionaux de contenu prévalent sur ceux du produit.

Lorsque vous affichez les rapports en langue thaïe, les chiffres ne sont pas pris en charge.

### Avant de commencer

Si des paramètres régionaux ne sont pas obligatoires, vous pouvez les supprimer de la liste. Vous devez laisser au moins un paramètre régional de contenu dans la liste pour que les composants du groupe de serveurs d'applications puissent fonctionner.

L'ajout de paramètres régionaux incomplets (langages) à l'environnement IBM Cognos ne garantit pas que l'ordinateur dispose de la police nécessaire pour afficher les pages Web dans vos langues favorites. Veillez à installer les polices appropriées pour la prise en charge des jeux de caractères et des symboles monétaires que vous utilisez. Pour que les symboles monétaires japonais et coréens s'affichent correctement, vous devez installer les polices supplémentaires depuis le CD-ROM Supplementary Language Documentation.

### Procédure

1. Démarrez IBM Cognos Configuration sur chaque ordinateur Content Manager.
2. Dans le menu **Actions**, cliquez sur l'option **Editer la configuration globale**.
3. Cliquez sur l'onglet **Langues du contenu**.

   Tous les environnements régionaux pris en charge sont affichés.

4. Cliquez sur **Ajouter**.

   **Conseil :** Pour supprimer un élément pris en charge, cochez la case située en regard de l'élément, puis cliquez sur **Supprimer**.
5. Dans la deuxième colonne, saisissez une valeur appropriée.
   - Pour ajouter la prise en charge d'une langue pour les données et métadonnées de rapport, saisissez un paramètre local partiel (langue).
   - Pour ajouter une prise en charge spécifique à une région, saisissez des paramètres régionaux complets (langue-région).
6. Répétez les tâches 3 à 5 pour chaque paramètre régional supplémentaire que vous voulez prendre en charge.
7. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Paramètres régionaux de contenu

Utilisez la table Mappages des paramètres régionaux (contenu) pour mapper les paramètres régionaux de l'utilisateur avec des paramètres régionaux complets (langue-région) ou partiels (langue). Vous pouvez également faire correspondre la langue favorite d'un utilisateur avec une autre langue si le contenu n'est pas disponible dans la langue préférentielle de l'utilisateur.

Par exemple, si un rapport ou un scorecard n'est pas disponible dans la langue d'un utilisateur, comme le vietnamien, mais est disponible en français et en allemand, vous pouvez utiliser la table pour mapper la langue favorite de l'utilisateur (vietnamien) avec une autre langue (français ou allemand). Le rapport ou scorecard s'affiche alors dans cette langue.

Par défaut, la table Mappages des paramètres régionaux (contenu) contient des paramètres régionaux n'incluant pas la région. Cela permet de n'utiliser que la partie linguistique des paramètres régionaux et garantit que vous voyez toujours les informations appropriées. Par exemple, dans une base de données multilingue, les données sont généralement disponibles dans différentes langues, telles que le français (fr), l'espagnol (es) et l'anglais (en), plutôt que dans des langues régionales, telles que l'anglais du Canada (en-ca), l'anglais des Etats-Unis (en-us) ou le français de France (fr-fr).

Les exemples ci-dessous montrent comment les composants d'IBM Cognos déterminent le rapport ou le scorecard que l'utilisateur visualise si des versions en différentes langues sont disponibles.

### Exemple 1

Un rapport est disponible dans Content Manager dans deux langues régionales, telles que en-us (anglais des Etats-Unis) et fr-fr (français de France), mais les paramètres régionaux de l'utilisateur sont définis sur fr-ca (français du Canada). IBM Cognos utilise les mappages de paramètres régionaux pour déterminer le rapport à afficher pour l'utilisateur.

Tout d'abord, IBM Cognos vérifie dans Content Manager si le rapport est disponible dans le paramètre régional de l'utilisateur. Si tel n'est pas le cas, IBM Cognos associe les paramètres régionaux de l'utilisateur à un paramètre régional normalisé configuré dans l'onglet Correspondances des paramètres régionaux (contenu). Comme le paramètre régional de l'utilisateur est fr-ca, il est mappé à fr. IBM Cognos utilise la valeur mappée pour vérifier si le rapport est disponible en français. Dans ce cas, le rapport est disponible en en-us et fr-fr, mais pas en fr.

IBM Cognos met ensuite en correspondance les rapports disponibles avec des paramètres régionaux normalisés. Ainsi, en-us devient en, et fr-fr devient fr.

Du fait que tant le rapport que les paramètres régionaux de l'utilisateur sont mis en correspondance avec fr, l'utilisateur dont les paramètres régionaux indiquent la langue fr-ca voit s'afficher le rapport en fr-fr.

### Exemple 2

Le paramètre régional de l'utilisateur et les paramètres régionaux de rapport sont tous associés à la même langue. IBM Cognos sélectionne les paramètres régionaux à utiliser. Par exemple, si le paramètre régional de l'utilisateur est en-ca (English-Canada) et que les rapports sont disponibles en anglais des Etats-Unis (en-us) et en anglais du Royaume-uni (en-gb), IBM Cognos associe chaque paramètre régional à en. L'utilisateur visualise le rapport conformément aux paramètres régionaux choisis par IBM Cognos.

### Exemple 3

Les paramètres régionaux du rapport et ceux de l'utilisateur ne sont pas mis en correspondance avec une langue commune. IBM Cognos sélectionne la langue. Dans ce cas, il peut s'avérer nécessaire de configurer le mappage. Par exemple, si un rapport est disponible en anglais des Etats-Unis (en-us) et français de France (fr-fr) et que le paramètre régional de l'utilisateur indique la langue espagnol d'Espagne (es-es), IBM Cognos sélectionne la langue.

## Mise en correspondance des paramètres régionaux (contenu)

Utilisez la table Mappages des paramètres régionaux (contenu) pour mapper les paramètres régionaux de l'utilisateur avec des paramètres régionaux complets (langue-région) ou partiels (langue). Vous pouvez également faire correspondre la langue favorite d'un utilisateur avec une autre langue si le contenu n'est pas disponible dans la langue préférentielle de l'utilisateur.

### Procédure

1. Démarrez IBM Cognos Configuration sur chaque ordinateur Content Manager.
2. Dans le menu **Actions**, cliquez sur l'option **Editer la configuration globale**.
3. Cliquez sur l'onglet **Mappages des paramètres régionaux (contenu)**.
4. Cliquez sur **Ajouter**.
5. Dans la zone **Clé**, saisissez les paramètres régionaux de l'utilisateur.
   - Pour faire en sorte que toutes les régions correspondant à une langue voient le contenu dans cette langue spécifique, saisissez la portion linguistique des paramètres régionaux, suivie d'un tiret (-) et d'un astérisque (*).

     Par exemple, saisissez **fr-***.
   - Pour faire en sorte qu'un utilisateur voie le contenu correspondant à ses paramètres régionaux spécifiques (langue-région), saisissez les paramètres régionaux complets.

     Par exemple, tapez **fr-ch**
   - Pour mapper une langue favorite avec une autre, saisissez la portion de langue favorite des paramètres régionaux.

     Par exemple, tapez type **zh**

   **Conseil :** Pour indiquer les paramètres régionaux à employer pour plusieurs clés, utilisez le caractère générique (*) avec la valeur **Clé** puis dans la zone

**Mappage local**, tapez le paramètre régional. Si vous souhaitez par exemple que toutes les clés allemandes utilisent des paramètres régionaux allemands, tapez **de*** dans la zone **Clé** et dans la zone **Mappage de paramètre régional**.

6. Dans la zone **Mappage des langues** saisissez la portion linguistique des paramètres régionaux.

   Les paramètres régionaux de l'utilisateur spécifiés dans la zone **Clé** appelleront le contenu dans cette langue.
7. Répétez les étapes 3 à 5 pour les autres mappages à établir.
8. Cliquez sur le bouton **OK**.
9. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Mise en correspondance des langues du produit

Utilisez la table Mappage des langues du produit pour indiquer la langue utilisée dans l'interface utilisateur lorsque celle précisée dans les paramètres régionaux de l'utilisateur n'est pas disponible.

Vous pouvez faire en sorte que toutes les régions correspondant à des paramètres régionaux utilisent la même langue ou que des paramètres régionaux complets spécifiques (langue-région) utilisent une langue particulière.

Par défaut, l'utilisateur voit l'interface du produit s'afficher dans la langue correspondant à celle de ses paramètres régionaux.

### Procédure

1. Démarrez IBM Cognos Configuration sur chaque ordinateur Content Manager.
2. Dans le menu **Actions**, cliquez sur l'option **Editer la configuration globale**.
3. Cliquez sur l'onglet **Mappage des langues du produit**.
4. Cliquez sur **Ajouter**.
5. Dans la zone **Clé**, saisissez les paramètres régionaux de l'utilisateur.
   - Pour faire en sorte que toutes les régions correspondant à une langue voient l'interface utilisateur dans cette langue spécifique, saisissez la portion linguistique des paramètres régionaux, suivie d'un tiret (-) et d'un astérisque (*).

     Par exemple, saisissez **es-***.
   - Pour faire en sorte que les paramètres régionaux complets (langue-région) entraînent l'affichage de l'interface utilisateur dans une langue spécifique, saisissez les paramètres régionaux complets.

     Par exemple, **es-es**
   - Pour mapper une langue favorite avec une autre, saisissez la portion de langue favorite des paramètres régionaux.

     Par exemple, tapez**zh**

   **Conseil :** Pour indiquer le paramètre régional à utiliser par défaut, utilisez le caractère générique (*) pour la valeur **Clé**puis dans la zone **Mappage local**, tapez le paramètre régional.
6. Dans la zone **Mappage des langues** saisissez la portion linguistique des paramètres régionaux.

   Les paramètres régionaux de l'utilisateur spécifiés dans la zone **Clé** appelleront le contenu dans cette langue.
7. Répétez les étapes 3 à 5 pour les autres mappages à établir.

8. Cliquez sur le bouton **OK**.
9. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Personnalisation du fuseau horaire du serveur

Vous pouvez modifier le fuseau horaire utilisé par Content Manager en sélectionnant un autre fuseau horaire dans IBM Cognos Configuration.

Pour les installations UNIX ne prenant pas en charge les interfaces graphiques utilisateur Java, vous pouvez consulter la liste des fuseaux horaires acceptables en ouvrant IBM Cognos Configuration sur l'ordinateur Windows où Framework Manager est installé.

Par défaut, Content Manager est configuré pour utiliser le fuseau horaire de votre système d'exploitation. Toutes les activités programmées dans IBM Cognos sont définies à l'aide de ce fuseau horaire. En outre, les utilisateurs du portail utilisent ce fuseau horaire lorsque leurs préférences sont définies avec le fuseau horaire par défaut. Pour en savoir davantage sur la définition des préférences utilisateur sur le portail, reportez-vous au manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans le menu **Actions**, cliquez sur l'option **Editer la configuration globale**.
3. Dans la boîte de dialogue **Configuration globale**, cliquez sur l'onglet **Général**.
4. Cliquez sur la colonne **Valeur** correspondant à **Fuseau horaire du serveur** et sélectionnez un autre fuseau horaire dans la liste.
5. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Codage des courriers électroniques

Les composants d'IBM Cognos utilisent, par défaut, l'encodage UTF-8 dans les courriers électroniques. Cette valeur définit l'encodage par défaut utilisé par le service de diffusion dans cette instance pour tous les messages électroniques. Il est possible que vous disposiez de clients de courrier électronique plus anciens ou que vous envoyiez des courriers électroniques depuis IBM Cognos à des téléphones portables et des assistants électroniques ne reconnaissant pas le format UTF-8. Si tel est le cas, vous pouvez redéfinir l'encodage des courriers électroniques sur une valeur applicable à tous vos clients de courrier électronique (par exemple, ISO-8859-1, Shift-JIS). Chaque instance d'IBM Cognos disposant d'un service de diffusion disponible doit être modifiée.

L'encodage défini a une incidence sur la totalité du message, notamment l'objet, les pièces jointes, les noms de pièces jointes et le texte du corps du message au format brut ou HTML.

Les valeurs d'encodage sont indiquées dans le tableau suivant :

*Tableau 36. Valeurs d'encodage prises en charge*

| Jeu de caractères | Valeur d'encodage prise en charge |
|---|---|
| UTF-8 | utf-8 |
| Europe de l'Ouest ( ISO 8859-1 ) | iso-8859-1 |
| Europe de l'Ouest (ISO 8859-15) | iso-8859-15 |
| Europe de l'Ouest (Windows-1252) | windows-1252 |

*Tableau 36. Valeurs d'encodage prises en charge (suite)*

| Jeu de caractères | Valeur d'encodage prise en charge |
|---|---|
| Europe centrale et continentale (ISO 8859-2) | iso-8859-2 |
| Europe centrale et continentale (Windows-1250) | windows-1250 |
| Cyrillique (ISO 8859-5) | iso-8859-5 |
| Cyrillique (Windows-1251) | windows-1251 |
| Turc (ISO 8859-9) | iso-8859-9 |
| Turc (Windows-1254) | windows-1254 |
| Grec (ISO 8859-7) | iso-8859-7 |
| Grec (Windows-1253) | windows-1253 |
| Japonais (EUC-JP) | euc-jp |
| Japonais (ISO-2022-JP) | iso-2202-jp |
| Japonais (Shift-JIS) | shift_jis |
| Chinois traditionnel (Big5) | big5 |
| Chinois simplifié (GB-2312) | gb2312 |
| Coréen (EUC-KR) | euc-kr |
| Coréen (ISO 2022-KR) | ISO 2022-KR |
| Coréen (KSC-5601) | ksc_5601 |
| Thaï (Windows-874) | windows-874 |
| Thaï (TIS-620) | tis-620 |

### Modification de l'encodage pour les courriers électroniques

Vous pouvez remplacer le codage des courriers électroniques par une valeur applicable à tous vos clients de courrier électronique.

#### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans le menu **Actions**, cliquez sur l'option **Editer la configuration globale**.
3. Dans la boîte de dialogue **Configuration globale**, cliquez sur l'onglet **Général**.
4. Cliquez sur la colonne **Valeur** correspondant à la propriété **Encodage des courriers électroniques**.
5. Défilez jusqu'au paramètre souhaité et sélectionnez-le.
6. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Personnalisation des paramètres de cookie

Selon les exigences de votre environnement IBM Cognos vous pouvez être amené à modifier les paramètres utilisés par les composants d'IBM Cognos pour créer les cookies. Vous pouvez utiliser IBM Cognos Configuration pour personnaliser le domaine, le chemin d'accès et l'indicateur de sécurité des cookies.

Les composants d'IBM Cognos déterminent le domaine des cookies à partir de la demande HTTP transmise par le client, qui correspond généralement à un navigateur Web. Dans la plupart des configurations réseau, les demandes HTTP passent par des intermédiaires tels que des serveurs proxy et des pare-feu pendant leur transfert depuis le navigateur vers les composants d'IBM Cognos. Certains intermédiaires modifient les informations que les composants d'IBM

Cognos utilisent pour calculer le domaine de cookies ; ces composants ne parviennent alors pas à définir de cookies. Le symptôme principal de ce problème est l'apparition répétée de l'invite de connexion. Pour éviter ce problème, configurez le domaine des cookies.

Pour définir la valeur adéquate pour le domaine de cookies, utilisez le format et la valeur qui représentent la couverture la plus importante pour l'hôte, en vous aidant des indications ci-dessous :

- Pour la valeur de domaine, utilisez simplement le nom de l'ordinateur ou du serveur. Entrez le nom sans points. Par exemple, `mycompany`
- Le domaine peut aussi comporter un suffixe. Les suffixes sont .com, .edu, .gov, .int, .mil, .net ou .org. Incluez un point comme préfixe. Par exemple, `.mycompany.com`
- D'autres niveaux peuvent être utilisés dans la valeur de domaine. Ajoutez un point comme préfixe. Par exemple `.accounts.mycompany.com`
- Vous pouvez limiter encore les cookies à l'aide d'un chemin. Le chemin `/` est le plus général. Le chemin `/payables` limite les cookies à tous les chemins commençant par "payable" (et tous ses sous-répertoires). Le chemin `/payables/` limite les cookies au répertoire "payables" (et à ses sous-répertoires).

De plus, pour la sécurité, les administrateurs peuvent définir l'attribut HTTPOnly pour empêcher des scripts de lire ou de manipuler le cookie du passeport CAM lors d'une session utilisateur avec le navigateur Web. Pour plus d'informations sur cet attribut, reportez-vous au manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

### Procédure

1. Démarrez IBM Cognos Configuration sur chaque ordinateur Content Manager.
2. Dans le menu **Actions**, cliquez sur l'option **Editer la configuration globale**.
3. Cliquez sur l'onglet **Général**.
4. Cliquez sur la colonne **Valeur** dans la section **Paramètres de cookie** de chaque propriété que vous souhaitez modifier et indiquez la nouvelle valeur.

   Si vous laissez la propriété **Domaine** vide, le répartiteur déduit le domaine du nom d'hôte de la demande.
5. Cliquez sur le bouton **OK**.

## Modification de la version de l'adresse IP

Les produits IBM Cognos prennent en charge deux versions d'adresse IP : IPv4 et IPv6. IPv4 utilise des adresses IP 32 bits et IPv6 des adresses IP 128 bits.

Par exemple :

- IPv4 : 192.168.0.1:80
- IPv6 : [2001:0db8:0000:0000:0000:148:57ab]:80

Dans IBM Cognos Configuration, vous pouvez sélectionner IPv4 ou IPv6 pour la communication IBM Cognos en utilisant la propriété **Version IP pour la résolution du nom d'hôte**. La valeur par défaut est IPv4.

Le paramètre s'applique uniquement à l'ordinateur sur lequel il est défini. Si vous sélectionnez l'option **Utiliser les adresses IPv4**, toutes les connexions IBM Cognos sortantes de cet ordinateur sont établies à l'aide du protocole IPv4 et le répartiteur accepte uniquement les connexions IPv4 entrantes. Si vous sélectionnez

l'option **Utiliser les adresses IPv6**, toutes les connexions IBM Cognos sortantes de cet ordinateur sont établies à l'aide du protocole IPv6 et le répartiteur accepte les connexions IPv4 et IPv6 entrantes.

Les ordinateurs client IPv4 peuvent communiquer avec les ordinateurs répartiteurs configurés pour IPv6.

Les noms d'hôtes spécifiés dans un URI sont résolus en fonction de la valeur de la propriété **Configuration Version IP pour la résolution du nom d'hôte**. Cependant, si un URI a été spécifié avec une adresse numérique, il prévaut sur ce paramètre et la communication est établie à l'aide du protocole IPv4.

Pour qu'IBM Cognos Configuration accepte des adresses IPv6 dans les propriétés URI locales, vous devez démarrer IBM Cognos Configuration avec l'option -ipv6. Vous pouvez indiquer l'option à chaque ouverture IBM Cognos Configuration depuis la ligne de commande.

Vous pouvez définir l'option de façon permanente en ajoutant l'option au raccourci vers le menu Démarrer sous Windows.

## Définition de la version IP

Utilisez IBM Cognos Configuration pour sélectionner la version IP.

### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
3. Cliquez sur la zone **Valeur** pour **Version IP pour la résolution du nom d'hôte** et cliquez sur **Utiliser les adresses IPv4** ou sur **Utiliser les adresses IPv6**.
4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
5. Fermez IBM Cognos Configuration.

## Configuration manuelle d'IBM Cognos Configuration pour démarrer l'option IPv6

Vous pouvez configurer IBM Cognos Configuration pour qu'il utilise l'option IPv6 en définissant l'option dans la commande Démarrer.

### Procédure

1. Accédez au répertoire *emplacement_installation*/bin ou *emplacement_installation*/bin64.
2. Lancez IBM Cognos Configuration en incluant l'option IPv6 dans la commande, comme suit :
   - Sur Windows, tapez :

     ```
     cogconfig.bat -ipv6
     ```
   - Sur UNIX ou Linux, tapez

     ```
     ./cogconfig.sh -ipv6
     ```
3. Editez les propriétés d'URI qui utilisent le format IPv6, indiquez les valeurs, puis depuis le menu**Fichier**, cliquez sur **Enregistrer**.

## Configuration d'IBM Cognos Configuration pour qu'il démarre toujours avec l'option IPv6 sous Windows

Vous pouvez configurer IBM Cognos Configuration pour qu'il utilise toujours l'option IPv6 sur Microsoft Windows en définissant l'option dans le raccourci du menu Démarrer.

### Procédure

1. Dans le menu **Démarrer**, cliquez avec le bouton droits sur **IBM Cognos Configuration** et sélectionnez **Propriétés**.
2. Sur l'onglet **Raccourci**, dans la zone **Cible**, saisissez `"emplacement_installation\bin\cogconfigw.exe -ipv6"`
3. Cliquez sur le bouton **OK**.

# Configuration de l'URI de recherche de collaboration

Vous pouvez configurer IBM Cognos Analytics et IBM Cognos Workspace de manière à utiliser IBM Connections pour l'aide à la décision collaborative. L'intégration à IBM Connections permet aux utilisateurs professionnels de collaborer tout en créant ou en visualisant les rapports, en effectuant les analyses ou en contrôlant les espaces de travail. Les utilisateurs ont accès aux activités d'IBM Connections depuis IBM Cognos Workspace et à la page d'accueil d'IBM Connections depuis IBM Cognos Analytics et IBM Cognos Workspace.

L'URI de recherche de collaboration définit le serveur IBM Connections à utiliser en tant que fournisseur de collaboration. Lorsqu'un URI est défini, la prise en charge liée à la collaboration est ajoutée à IBM Cognos Analytics de la façon suivante :

- un lien est ajouté à la page d'accueil du portail IBM Cognos Analytics. Si l'utilisateur a accès à la page d'accueil d'IBM Connections, le lien, intitulé **Accéder à mon réseau social**, permet à l'utilisateur d'accéder à cette page. Si l'utilisateur a accès aux activités d'IBM Connections, mais pas à la page d'accueil, le lien, intitulé **Mes activités**, permet à l'utilisateur d'accéder à la page des activités.
- un lien à la page d'accueil d'IBM Connections est ajouté au menu Lancer sur le portail
- un lien à la page d'accueil d'IBM Connections est ajouté au menu Actions d'IBM Cognos Workspace
- le bouton du menu **Collaborer** est ajouté sur la barre d'applications de l'espace de travail dans IBM Cognos Workspace. L'utilisateur peut créer ou afficher une activité d'espace de travail dans IBM Connections.

### Procédure

1. Dans **IBM Cognos Administration**, dans l'onglet **Configuration**, cliquez sur **Répartiteurs et services** pour afficher la liste des répartiteurs.
2. Dans la barre d'outils, cliquez sur le bouton Définir les propriétés - Configuration.
3. Cliquez sur l'onglet **Paramètres**.
4. Dans la catégorie **Environnement**, pour **URI de recherche de collaboration**, indiquez l'URI comme suit :

   `http://`*`nom_serveur`*`:`*`numéro_port`*`/activities/serviceconfigs`

   Par exemple, `http://`*`nom_serveur`*`:9080/activities/serviceconfigs`

   où *`nom_serveur`* désigne le serveur sur lequel IBM Connections est installé.

5. Cliquez sur le bouton **OK**.

# Configuration d'IBM Cognos Workspace

IBM Cognos Workspace est fourni avec le serveur IBM Cognos Analytics. Il propose des fonctionnalités dynamiques et personnalisables qui vous permettent d'assembler rapidement et facilement des espaces de travail interactifs en utilisant du contenu IBM Cognos, ainsi que des sources de données externes. Après avoir vérifié qu'IBM Cognos Workspace est en cours d'exécution, configurez l'accès aux fonctions et fonctionnalités protégées.

Exécutez les tâches de configuration suivantes.

__ • Configurez l'accès à IBM Cognos Workspace.

__ • Configurez les types MIME pris en charge dans Microsoft Internet Information Services.

Après avoir effectué les tâches de configuration, vous pouvez exécuter les tâches suivantes, le cas échéant :

__ • Configurez une base de données pour les annotations.

__ • Configurez IBM Cognos Workspace en vue de l'utilisation du contenu provenant de TM1 Data Server.

__ • Configurez IBM Cognos Workspace pour l'accès à IBM Cognos TM1 Applications.

__ • Modifiez les styles dans les rapports.

__ • Utilisez les exemples.

## Configuration de l'accès à IBM Cognos Workspace ou à ses fonctions

Configurez l'accès à IBM Cognos Workspace en octroyant les droits d'exécution du tableau de bord informatif requis pour des espaces-noms, des utilisateurs, des groupes ou des rôles précis.

Vous pouvez octroyer un accès intégral à IBM Cognos Workspace, ou un accès limité à la fonction de publication.

IBM Cognos Analytics BI doit être configuré et opérationnel avant que vous ne configuriez l'accès pour IBM Cognos Workspace.

### Octroi de l'accès intégral à IBM Cognos Workspace

Pour octroyer l'accès à IBM Cognos Workspace et à toutes ses fonctionnalités, vous devez attribuer des droits d'exécution et de passage pour la fonction Tableau de bord informatif.

Des informations supplémentaires sur la configuration des droits pour les utilisateurs sont disponibles dans une note technique (www.ibm.com/support/docview.wss?uid=swg21498402) sur le site Web IBM.

#### Procédure

1. Sur le portail IBM Cognos Analytics, lancez **IBM Cognos Administration**.
2. Dans l'onglet **Sécurité**, cliquez sur **Fonctions**.

3. Recherchez la fonction **Tableau de bord informatif**, cliquez sur le bouton Actions  situé en regard du nom de la fonction et sélectionnez **Définir les propriétés**.
4. Sélectionnez l'onglet **Droits**.
5. Attribuez les droits d'exécution à tous les groupes d'utilisateurs censés accéder à IBM Cognos Workspace, puis cliquez sur **OK**.

### Octroi de l'accès à la fonction de publication d'IBM Cognos Workspace

Pour octroyer l'accès uniquement à la fonction de publication d'IBM Cognos Workspace, accordez des droits de passage pour la fonction Tableau de bord informatif et des droits d'exécution pour la fonction protégée Publication de tableaux de bord dans les espaces de collaboration.

#### Procédure

1. Sur le portail IBM Cognos Analytics, lancez **IBM Cognos Administration**.
2. Dans l'onglet **Sécurité**, cliquez sur **Fonctions**.
3. Recherchez et sélectionnez la fonction **Tableau de bord informatif**.
4. Cliquez sur le bouton Actions  à côté de **Publication de tableaux de bord dans les espaces de collaboration**, puis cliquez sur **Définir les propriétés**.
5. Sélectionnez l'onglet **Droits**.
6. Si vous souhaitez définir des droits d'accès de façon explicite pour chaque entrée, sélectionnez **Remplacer les droits d'accès hérités de l'entrée parent**.
7. Pour chaque groupe d'utilisateurs, cochez la case correspondant à l'entrée puis, dans la zone en regard de la liste, cochez les cases appropriées pour attribuer les droits souhaités.
8. Pour ajouter des entrées à la liste, cliquez sur le bouton **Ajouter**, puis choisissez le mode de sélection des entrées :
   - Pour choisir une entrée disponible dans la liste, cliquez sur l'espace-noms correspondant, puis cochez une case en regard des utilisateurs, des groupes ou des rôles.
   - Pour rechercher une entrée, cliquez sur l'onglet **Rechercher** et saisissez la phrase à rechercher dans la zone Chaîne de recherche. Pour accéder aux options de recherche, cliquez sur le bouton **Editer**. Cliquez sur l'entrée recherchée.
   - Pour saisir le nom des entrées que vous voulez ajouter, cliquez sur **Saisir** et saisissez le nom des groupes, rôles ou utilisateurs au format suivant (en séparant chaque entrée par un point-virgule (;)) : *espace-noms/nom_groupe*;*namespace/nom_rôle*;*espace_noms/nom_utilisateur*;

   Vous pouvez ensuite attribuer les droits appropriés sur chaque nouvelle entrée.
9. Cliquez sur le bouton **OK**.

## Configuration des types MIME pris en charge dans Microsoft Internet Information Services

Si vous utilisez Microsoft Internet Information Services (IIS) 6.0, vous devez définir le type MIME utilisé par IBM Cognos Workspace pour que celui-ci puisse charger IBM Cognos Workspace correctement.

### Procédure

1. Ouvrez la console de gestion Microsoft IIS.
2. Cliquez avec le bouton droit de la souris sur le nom de l'ordinateur, puis cliquez sur l'option **Propriétés**.
3. Cliquez sur l'option **Types MIME**.
4. Cliquez sur **Nouveau**.
5. Dans la zone **Extension**, saisissez **.cfg**.
6. Dans la zone **Type MIME**, saisissez **texte/brut**.
7. Appliquez les nouveaux paramètres.

   Les modifications seront appliquées lors du recyclage du processus de travail. Pour éviter toute attente, vous pouvez redémarrer le service de publication World Wide Web. Pour plus d'informations, recherchez la rubrique *Gestion des types MIME dans Internet Explorer* dans la bibliothèque en ligne de Microsoft.

## Création d'espaces de table pour la base de données des tâches utilisateur et d'annotations dans IBM Db2 on z/OS

Si vous utilisez Db2, un administrateur de base de données doit exécuter des scripts pour créer les espaces de table requis pour la base de données des tâches utilisateur et d'annotations. Le script doit être modifié pour remplacer les paramètres génériques par ceux convenant à votre environnement.

Utilisez les convention de dénomination pour Db2 on z/OS. Par exemple, tous les noms de paramètres doivent commencer par une lettre et ne pas dépasser six caractères. Pour plus d'informations, voir le Knowledge Center d'Db2.

Vous pouvez utiliser votre base de données de magasin de contenu ou une base de données distincte pour la base de données de tâches utilisateur et d'annotations. Dans les deux cas, vous devez exécuter les scripts pour créer les espaces de table.

### Procédure

1. Connectez-vous à la base de données en tant qu'utilisateur disposant de privilèges afin de créer et d'insérer des espaces de table, ainsi qu'autoriser l'exécution d'instructions SQL.
2. Pour créer les espaces de table de tâches utilisateur, accédez au répertoire *emplacement_installation*/configuration/schemas/hts/zosdb2.
   a. Faites une copie de sauvegarde du fichier script HTS_tablespaces.sql et enregistrez le fichier à un autre emplacement.
   b. Ouvrez le fichier script HTS_TABLESPACES.sql d'origine et utilisez le tableau ci-après pour vous aider à remplacer les paramètres fictifs par ceux convenant à votre environnement.

*Tableau 37. Noms et descriptions des paramètres d'espace de table de tâches utilisateur dans Db2 on z/OS*

| Nom du paramètre | Description |
|---|---|
| NCCOG | Indique le nom de la base de données. |
| DSN8G810 | Indique le nom du groupe de stockage. |
| BP32K | Indique le nom du pool de mémoire tampon de 32 k. |

   Pour une liste complète des paramètres requis, voir le script.
   c. Enregistrez et exécutez le script.

d. Ouvrez le fichier de script HTS2_CREATE_Db2zos.sql et utilisez le tableau ci-après pour vous aider à remplacer les paramètres génériques par ceux convenant à votre environnement.

*Tableau 38. Noms et descriptions des paramètres d'espace de table de tâches utilisateur dans Db2 on z/OS*

| Nom du paramètre | Description |
|---|---|
| NCCOG | Nom de la base de données. |

Pour une liste complète des paramètres requis, voir le script.

e. Enregistrez et exécutez le script.

3. Pour créer les espaces de table d'annotations, accédez au répertoire *emplacement_installation*/configuration/schemas/ans/zosdb2.
   a. Faites une copie de sauvegarde du fichier script ANN_TABLESPACES.sql et enregistrez le fichier à un autre emplacement.
   b. Ouvrez le fichier script ANN_TABLESPACES.sql d'origine et utilisez le tableau ci-après pour vous aider à remplacer les paramètres fictifs par ceux convenant à votre environnement.

*Tableau 39. Noms et descriptions des paramètres d'espace de table pour les annotations dans Db2 on z/OS*

| Nom du paramètre | Description |
|---|---|
| NCCOG | Nom de la base de données. |
| DSN8G810 | Nom du groupe de stockage. |
| BP32K | Nom du pool de mémoire tampon de 32 k. |

Pour une liste complète des paramètres requis, voir le script.

c. Enregistrez et exécutez le script.

d. Ouvrez le fichier de script ANS2_CREATE_Db2zos.sql et utilisez le tableau ci-après pour vous aider à remplacer les paramètres génériques par ceux convenant à votre environnement.

*Tableau 40. Noms et descriptions des paramètres d'espace de table pour les annotations dans Db2 on z/OS*

| Nom du paramètre | Description |
|---|---|
| NCCOG | Nom de la base de données. |

Pour une liste complète des paramètres requis, voir le script.

e. Enregistrez et exécutez le script.

## Configuration d'une base de données pour les tâches utilisateur et les annotations

Par défaut, les données utilisées par la fonctionnalité Tâches utilisateur et annotations d'IBM Cognos Workspace sont stockées dans la même base de données que celle utilisée pour Content Store. Vous pouvez configurer une base de données distincte pour les tâches utilisateur et les annotations.

Pour configurer la base de données, vous devez d'abord la créer, puis créer un compte utilisateur de cette dernière. Vous devez également configurer la fonctionnalité Tâches utilisateur et annotations afin qu'elle puisse utiliser la nouvelle base de données.

### Procédure

1. Créez une base de données en utilisant les mêmes instructions que «Instructions pour la création du magasin de contenu», à la page 8.

   Si vous utilisez IBM Db2 on z/OS pour la base de données, vous devez créer les espaces de table requis en exécutant deux scripts. Pour en savoir davantage, reportez-vous à la section «Création d'espaces de table pour la base de données des tâches utilisateur et d'annotations dans IBM Db2 on z/OS», à la page 230.
2. Créez un compte utilisateur destiné à être utilisé avec la base de données.
3. En ce qui concerne l'instance dans laquelle sont installés les composants du groupe de serveurs d'applications, démarrez IBM Cognos Configuration.
4. Dans la fenêtre **Explorateur**, cliquez avec le bouton droit de la souris sur l'option **Services de gestion des tâches humaines et d'annotation** et sélectionnez l'option **Nouvelle ressource** > **Base de données**.
5. Dans la boîte de dialogue **Nouvelle ressource - Base de données**, saisissez un nom pour la base de données, sélectionnez le type, puis cliquez sur **OK**.
6. Dans la fenêtre des propriétés de ressource de base de données, appliquez les configurations suivantes :
   - Définissez les valeurs obligatoires pour toutes les propriétés marquées par un astérisque.
   - Définissez la propriété **ID utilisateur et mot de passe** du compte qui gère la base de données.
7. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

   Les données d'identification pour la connexion sont immédiatement chiffrées.
8. Pour tester la connexion à la nouvelle base de données, cliquez sur l'option **Test** dans le menu **Actions**.
9. Répétez cette étape pour chaque instance de composant du groupe de serveurs d'applications et Content Manager.

## Configuration d'IBM Cognos Workspace en vue de l'utilisation des données IBM Cognos TM1

Pour pouvoir utiliser les données IBM Cognos TM1 dans IBM Cognos Workspace, vous devez modifier les fichiers de configuration dans votre installation IBM Cognos Analytics.

Pour configurer le serveur de données TM1 pour IBM Cognos Workspace, effectuez les opérations suivantes :

__ • Définissez les informations de connexion au serveur TM1.

__ • Définissez les noms du serveur IBM Cognos TM1 qui doivent s'afficher dans IBM Cognos Workspace.

__ • Facultativement, changez le nom du dossier Vues.

### Définition des informations de connexion au serveur TM1

Pour définir les informations de connexion aux serveurs TM1, vous devez modifier un fichier de configuration.

Un exemple de fichier de contribution est fourni dans l'installation IBM Cognos Analytics. Si vous utilisez une installation répartie, le fichier de configuration est disponible sur les ordinateurs sur lesquels vous avez installée les composants du groupe de serveurs d'applications.

Si la passerelle IBM Cognos Analytics s'exécute sur un ordinateur différent de TM1 Web, assurez-vous d'utiliser les noms de domaines qualifiés complets pour les noms de serveur, tels que TM1WebHost. Par exemple, entrez http://*mycomputer*.*mydomain*.com/ibmcognos, plutôt que http://*mycomputer*/ibmcognos. Vous devez également utiliser les noms de domaines qualifiés complets pour les valeurs de nom de serveur dans la section **Environnement** d'IBM Cognos Configuration.

## Procédure

1. Sur l'ordinateur sur lequel vous avez installé les composants du groupe de serveurs d'applications d'IBM Cognos Analytics, accédez au répertoire *emplacement_installation*\configuration\icd\contributions\contrib, et renommez le fichier tm1_contribution.atom.sample en tm1_contribution.atom.
2. Ouvrez le fichier tm1_contribution.atom dans un éditeur de texte.

   Le fichier contient trois sections <atom:entry>. Vous devez modifier les valeurs de l'une des sections <atom:entry> pour chaque serveur TM1 auquel vous voulez accéder dans IBM Cognos Workspace. Ajoutez autant de sections <atom:entry> que de serveurs TM1 supplémentaires à ajouter. A contrario, vous devez mettre en commentaire les sections <atom:entry> non utilisées. La troisième section <atom:entry> du fichier d'exemple est déjà mise en commentaire.

   La première section <atom:entry> est destinée à un serveur TM1 n'utilisant pas l'authentification Cognos.

   La seconde section <atom:entry> est destinée à un serveur TM1 qui utilise l'authentification Cognos.
3. Dans la section <atom:entry> pour laquelle l'authentification est requise, remplacez les valeurs de **TM1WebHostName** et **TM1HostName** par le nom ou l'adresse IP du serveur TM1 Web et du serveur de données TM1.

   Par exemple, modifiez dans l'exemple les éléments mis en évidence.

   ```
   TM1WebHost=TM1WebHostName&amp;
   TM1WebVirtualDirectory=tm1web&amp;
   TM1Host=TM1HostName&amp;
   ```
4. Pour un serveur TM1 qui n'utilise pas l'authentification IBM Cognos, modifiez la valeur de TM1DataServer mise en évidence :

   ```
   TM1DataServer=TM1ServerHostWithoutCAM&amp;
   TM1username=admin&amp;TM1pass=apple
   ```

   Remplacez **admin** et **apple** par l'ID utilisateur et le mot de passe du compte administrateur utilisé pour le serveur TM1.
5. Pour un serveur TM1 utilisant l'authentification IBM Cognos, modifiez la valeur de TM1DataServer mise en évidence :

   ```
   TM1DataServer=CamAuthenticatedTM1ServerHost
   ```
6. Si vous n'utilisez pas les valeurs par défaut, modifiez les propriétés suivantes :
   - https

     Cette propriété décrit le protocole utilisé pour le serveur Web TM1. Si le serveur TM1 Web fonctionne avec le protocole HTTP sécurisé, remplacez **0** par **1**.
   - TM1WebVirtualDirectory

     Cette propriété est le nom du répertoire virtuel du serveur Web TM1. Si le nom du répertoire Web TM1 n'est pas tm1web, remplacez la valeur de la propriété TM1WebVirtualDirectory par le nom correct.

     Par exemple :

```
TM1WebVirtualDirectory=planningweb&amp;
```

- `TM1Toolbar`

  Cette propriété détermine si la barre d'outils interne est visible. Les versions de TM1Web antérieures à la version 9.5.2 ne permettent pas l'utilisation d'une barre d'outils externe. La valeur par défaut de `TM1Toolbar` est **0**. Pour afficher la barre d'outils interne, définissez la valeur sur **1**.

7. Si vous définissez plusieurs connexions à des serveurs TM1, créez une section `<atom:entry>` pour chaque serveur TM1.

   Toutes les valeurs `atom:id` de toutes les entrées `.atom` doivent être uniques. Par exemple :

   ```
   <atom:entry>
     <atom:id>tag:ibm.cognos.icd.com,2010-01-01:/tm1_rootfeed_2
   </atom:id>
   ```

   ```
   <atom:entry>
     <atom:id>tag:ibm.cognos.icd.com,2010-01-01:/tm1_rootfeed_2b
   </atom:id>
   ```

   Les sections de l'exemple sont uniques grâce à `tm1_rootfeed_2` et `tm1_rootfeed_2b`.

   Vérifiez que les noms des valeurs telles que **tm1_rootfeed_1**, **rootfeed_title_1** et **rootfeed_summary_1** sont bien uniques.
8. Vérifiez que les sections `<atom:entry>` non utilisées ont été mises en commentaire ou supprimées.
9. Sauvegardez et fermez le fichier.
10. Redémarrez les services IBM Cognos. Si vous souhaitez modifier les noms sous lesquels les serveurs TM1 doivent s'afficher dans IBM Cognos Workspace, redémarrez les services après la tâche suivante.

## Définition des noms des serveurs IBM Cognos TM1

Vous pouvez définir les noms sous lesquels s'affichent dans IBM Cognos Workspace les serveurs TM1.

Si vous utilisez des langues autres que l'anglais, vous pouvez créer des fichiers supplémentaires pour l'affichage des noms dans ces langues dans IBM Cognos Workspace.

### Procédure

1. Sur l'ordinateur sur lequel vous avez installé les composants du groupe de serveurs d'applications d'IBM Cognos Analytics, accédez au répertoire *emplacement_installation*`\configuration\icd\contributions\contrib`.
2. Ouvrez le fichier `tm1_en.properties` dans un éditeur de texte.
3. Remplacez le texte qui suit le signe (=) par un nom permettant d'identifier le serveur TM1 défini pour le titre.

   Par exemple, si vous avez défini à l'étape précédente une connexion au serveur TM1 dans la section `rootfeed_title_1` du fichier `tm1_contribution.atom`, remplacez le nom par :

   ```
   rootfeed_title_1 = MyTM1Server
   ```
4. Remplacez le texte de la propriété `rootfeed_summary_1` par une description du serveur TM1.

   Par exemple, si vous avez défini un nom pour la connexion au serveur TM1 dans `rootfeed_title_1`, remplacez la valeur de `rootfeed_summary_1` par :

   ```
   rootfeed_summary_1 = Detail about MyTM1Server
   ```

5. Remplacez les valeurs de chaque serveur TM1 ajouté au fichier `tm1_contribution.atom` à l'étape précédente. Vous devez faire correspondre les sections `rootfeed_title` et `rootfeed_summary` avec les valeurs définies dans le fichier `tm1_contribution.atom`.
6. Si votre environnement prend en charge plusieurs langues :
   - Faites une copie du fichier `tm1_en.properties`.
   - Renommez-le `tm1_`*`code de langue`*`.properties`, où *`code de langue`* est le code à deux caractères associé à la langue utilisée, par exemple ja ou es.

     Voici comment s'appellerait le fichier de propriétés français : `tm1_fr.properties`.
7. Redémarrez les services IBM Cognos pour que les modifications soient prises en compte.

### Modification du nom du dossier Vues

Si vous le souhaitez, vous pouvez modifier le nom qui s'affiche dans IBM Cognos Workspace pour le dossier **Vues**.

Par défaut, IBM Cognos Workspace affiche un dossier Applications et un dossier Vues pour chaque serveur TM1 identifié dans le fichier `tm1_contribution.atom`. Le nom du dossier Applications est renvoyé par le serveur TM1. Le nom du dossier Vues est déterminé par un fichier de messages fourni par IBM Cognos Workspace.

#### Procédure

1. Accédez au répertoire *`emplacement_installation`*`\templates\ps\messages`.
2. Créez une copie du fichier `tm1buxmsgs_en.xml` et renommez-la en utilisant le code de langue approprié.

   Voici comment s'appellerait le fichier pour la version française : `tm1buxmsgs_fr.xml`.
3. Ouvrez le nouveau fichier de conversion dans un éditeur XML.
4. Remplacez le mot `Views` de la section suivante par la valeur de votre choix :

   ```
   <string id="TM1_VIEWS" type="String" usage="TM1 views">Views</string>
   ```
5. Enregistrez et fermez le nouveau fichier.
6. Répétez cette procédure pour chaque langue utilisée.

## Configuration d'IBM Cognos Workspace pour l'accès à IBM Cognos TM1 Applications

Le serveur IBM Cognos Analytics peut accéder au client Web pour IBM Cognos TM1 Applications via un iwidget externe qui s'affiche dans la sous-fenêtre de contenu d'IBM Cognos Workspace. Pour pouvoir afficher l'iwidget, consultez la documentation TM1 Applications pour effectuer les tâches suivantes :

### Procédure

1. Installation d'IBM Cognos TM1 Applications.
2. Configuration d'IBM Cognos TM1 Applications pour l'interopérabilité avec le serveur IBM Cognos Analytics.

   Lors de la copie du fichier `icon_active_application.gif` dans le dossier d'images du portail du serveur Cognos Analytics, copiez également ce fichier dans le dossier *`emplacement_installation`*`/webcontent/icd/feeds/images`.
3. Déployez vos applications.

   IBM Cognos TM1 Applications génère une URL qui est détectée par le serveur IBM Cognos Analytics.

### Résultats

L'URL TM1 Contributor s'affiche sous **Dossiers publics** dans le panneau de contenu d'IBM Cognos Workspace.

## Modification du style des objets rapport dans IBM Cognos Workspace

Lorsque vous faites glisser un objet rapport dans un espace de travail, celui-ci s'affiche dans le style dégradé argent et bleu de votre produit. Vous pouvez configurer l'objet rapport pour l'afficher dans le style d'origine de l'auteur en modifiant une propriété globale dans le fichier de configuration d'IBM Cognos Viewer.

Les objets rapport affectés par le paramètre global incluent les requêtes, les analyses, les rapports et les portions de rapports créés à travers l'utilisation d'IBM Cognos version 1.x, version 8.x et de type état financier. Ces objets s'adaptent au paramètre global même si vous les avez enregistrés avant de modifier le paramètre. Une miniature d'espaces de travail est affectée par le paramètre global uniquement si vous l'exécutez à nouveau.

Certains objets rapport ne sont pas affectés par le paramètre global et s'affichent toujours dans le style dans lequel ils ont été créés, tels que les rapports PowerPlay et les miniatures des objets rapport.

### Procédure

1. Pour chaque instance de Content Manager et des composants du groupe de serveurs d'applications, accédez au répertoire *emplacement_installation*`/webapps/p2pd/WEB-INF/classes directory`.
2. Ouvrez le fichier `viewerconfig.properties` dans un éditeur de texte.
3. Pour que les objets de rapports s'affichent dans le style dans lequel ils ont été créés, modifiez la valeur de **`useAuthoredReportStyles`** en `true`.
4. Enregistrez le fichier et redémarrez les services.

## Accès aux exemples IBM Cognos Workspace

Les exemples IBM Cognos Workspace sont fournis avec les exemples IBM Cognos Analytics.

Les utilisateurs professionnels peuvent accéder aux exemples IBM Cognos Workspace en sélectionnant l'option qui permet d'ouvrir les espaces de travail existants, puis en sélectionnant **Exemples** > **Modèles** > **Exemples de Cognos Workspace**.

Pour en savoir davantage sur l'installation et la configuration des exemples, voir le manuel *IBM Cognos Analytics - Guide des exemples*. Pour plus d'informations sur l'utilisation des exemples, voir le document *IBM Cognos Workspace - Guide d'utilisation*.

# Configuration du routeur pour tester la disponibilité d'un répartiteur

Si vous utilisez un routeur pour distribuer des demandes aux répartiteurs d'IBM Cognos et si ce routeur peut tester la disponibilité d'un serveur à l'aide d'une adresse URL test, vous pouvez le configurer pour qu'il teste la disponibilité d'un répartiteur d'IBM Cognos.

### Procédure

Configurez le routeur pour utiliser une adresse URL avec le chemin d'accès `/p2pd/servlet/ping`.
Si le répartiteur n'est pas prêt, la réponse suivante est envoyée :
`503 Service non disponible`
Si le répartiteur est prêt, la réponse suivante est envoyée :
`200 OK`

## Configuration d'IBM Cognos Analytics en vue d'une utilisation avec d'autres produits IBM Cognos

Certains produits IBM Cognos offrent des fonctionnalités non disponibles dans IBM Cognos Analytics.

Vous pouvez continuer à utiliser ces produits dans le même environnement. D'autres tâches de configuration peuvent se révéler nécessaires pour permettre à IBM Cognos Analytics d'accéder aux objets créés à l'aide d'autres produits IBM Cognos. Les conditions supplémentaires requises pour l'accès dépendent du mode d'exécution choisi pour les deux produits.

### Activation des rapports et agents planifiés pour les sources de données d'IBM Cognos Planning Contributor

Pour exécuter des rapports et agents planifiés qui ont pour base des sources de données IBM Cognos Planning Contributor, vous devez définir un mot de passe secret partagé. Cela contribue à la sécurité des communications entre les serveurs IBM Cognos Analytics et Contributor Data Server.

#### Procédure

1. Sur l'ordinateur hébergeant les composants du groupe de serveurs d'applications, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, cliquez sur **Accès aux données**, **IBM Cognos Planning**, **Contributor Data Server**.
3. Dans la fenêtre **Propriétés**, cliquez sur la zone **Valeur** à côté de la propriété **Mot de passe de la signature**, puis cliquez sur le bouton Editer  lorsqu'il s'affiche.
4. Dans la boîte de dialogue **Valeur - Mot de passe de la signature**, saisissez le mot de passe qui sera l'objet d'une signature numérique.

   Le mot de passe est sensible à la casse et doit correspondre à la propriété **Mot de passe de la signature** que vous avez configurée dans les propriétés d'IBM Cognos Series 7, Configuration Manager, **Cognos Planning/Cognos BI - Contributor Data Server/Général**.
5. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

#### Résultats

Une signature numérique est créée à partir du mot de passe. La signature numérique est codée par IBM Cognos Analytics et décodée par Contributor Data Server.

# Chapitre 8. Configuration des fournisseurs d'authentification

Les composants d'IBM Cognos s'exécutent avec deux niveaux d'accès : anonyme et authentifié. Par défaut, l'accès anonyme est activé.

Vous pouvez utiliser deux types de connexion dans votre installation. Si vous souhaitez utiliser uniquement la connexion authentifiée, vous devez désactiver l'accès anonyme. Pour plus d'informations, voir Désactivation de l'accès anonyme.

Pour une connexion authentifiée, vous devez configurer les composants d'IBM Cognos Analytics avec un espace-noms approprié pour le type de fournisseur d'authentification de votre environnement. Vous pouvez configurer plusieurs espaces-noms pour l'authentification, puis sélectionner, en cours d'exécution, celui que vous voulez utiliser. Pour plus d'informations, voir le *Guide d'administration et de sécurité*.

Si vous procédez à une mise à niveau à partir de ReportNet et qu'IBM Cognos détecte un espace-noms auparavant configuré, mais qui ne l'est plus, cet espace-noms s'affiche dans la liste des fournisseurs d'authentification, sur le portail d'administration. Vous pouvez configurer l'espace-noms si vous avez toujours besoin des informations de compte utilisateur. Dans le cas contraire, vous pouvez supprimer l'espace-noms. Par ailleurs, lors de la mise à niveau d'une version vers une autre, vous devez utiliser le même espace-noms d'authentification pour les deux versions. Dans le cas contraire, l'ancien contenu sécurisé sera indisponible, car la nouvelle version peut ne pas contenir les mêmes règles, utilisateurs, rôles et groupes.

Les composants d'IBM Cognos prennent en charge les types de serveurs suivants en tant que sources d'authentification :

- Active Directory Server
- Fournisseur d'authentification personnalisé
- Espace-noms IBM Cognos Series 7
- LDAP
- OpenID Connect
- CA SiteMinder
- RACF
- SAP

Si vous utilisez plusieurs instances de Content Manager, vous devez configurer des fournisseurs d'authentification identiques sur chaque emplacement de Content Manager. De fait, le type de fournisseur d'authentification que vous sélectionnez et la manière dont vous le configurez doivent être les mêmes à tous les emplacements de toutes les plateformes. La configuration doit contenir des informations auxquelles toutes les instances de Content Manager ont accès.

Si IBM Cognos est installé sur un seul ordinateur Linux ou que Content Manager est installé sur un ordinateur Linux, IBM Cognos peut être configuré pour utiliser uniquement des serveurs d'annuaire V3 LDAP et des fournisseurs personnalisés comme sources d'authentification.

Certains fournisseurs d'authentification requièrent que des bibliothèques externes à l'environnement IBM Cognos soient disponibles. Si tel n'est pas le cas sous Linux, le fournisseur d'authentification ne peut être initialisé.

Pour configurer l'un des éléments suivants en tant que source d'authentification, vous devez installer Content Manager sur un système d'exploitation qu'il prend en charge :

- Espace-noms IBM Cognos Series 7 (Windows, Solaris, AIX)
- Active Directory Server (Windows uniquement)
- SAP BW (Tous, exceptés Power PC, z/OS, z/Linux)

Si vous activez la sécurité, vous devez configurer des paramètres de sécurité dès que vous avez terminé le processus d'installation et de configuration. Pour plus d'informations, voir le *Guide d'administration et de sécurité*.

**Important :** Une fois la sécurité activée, ne la désactivez pas. Les paramètres de droits existants continuent à faire référence à des utilisateurs, des groupes et des rôles qui n'existent plus. Si cela n'affecte pas le fonctionnement des droits, un utilisateur administrant les paramètres de droits risque de voir des entrées "inconnues". Etant donné que ces entrées font référence à des utilisateurs, des groupes et des rôles qui n'existent plus, vous pouvez les supprimer en toute sécurité. Toutefois, des entrées "inconnues" peuvent également être affichées si vous n'êtes pas authentifié dans tous les espaces-noms. Dans ce scénario, ne supprimez pas les entrées "inconnues".

Après avoir configuré un fournisseur d'authentification pour les composants d'IBM Cognos, vous pouvez activer le code d'accès unique entre votre environnement de fournisseur d'authentification et les composants d'IBM Cognos BI. Ainsi, un utilisateur se connecte une seule fois et peut passer d'une application à une autre sans se reconnecter.

Les utilisateurs peuvent sélectionner des espaces-noms lorsqu'ils se connectent au portail IBM Cognos Analytics. Vous pouvez masquer les espaces-noms Java personnalisés et les espaces-noms CA SiteMinder pour que les utilisateurs ne puissent pas les sélectionner. Pour en savoir davantage, reportez-vous à la section «Masquage de l'espace-noms de la vue des utilisateurs durant la connexion», à la page 263.

## Désactivation de l'accès anonyme

Si vous voulez configurer IBM Cognos Analytics de sorte qu'il utilise uniquement une connexion authentifiée, vous devez désactiver l'accès anonyme à l'application.

Par défaut, les composants d'IBM Cognos n'exigent pas d'authentification de l'utilisateur. Les utilisateurs peuvent ouvrir une session anonyme.

### Procédure

1. Démarrez IBM Cognos Configuration sur chaque ordinateur où est installé Content Manager.
2. Dans la fenêtre **Explorateur**, dans la section **Sécurité** > **Authentification**, cliquez sur l'option **Cognos**.

   L'espace-noms de Cognos stocke des informations sur les groupes et les rôles d'IBM Cognos, les contacts et les listes de distribution, ainsi que des références à des objets figurant dans d'autres espaces-noms de sécurité.

3. Dans la fenêtre **Propriétés**, cliquez sur la zone située en regard de la propriété **Voulez-vous autoriser les connexions anonymes ?**, puis sélectionnez **Faux**.
4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

### Résultats

Vous devez à présent configurer un espace-noms afin que les utilisateurs soient invités à fournir leurs données d'identification lorsqu'ils accèdent à IBM Cognos Analytics.

## Restriction de l'accès utilisateur à l'espace-noms Cognos

Vous pouvez configurer l'accès à IBM Cognos Analytics de sorte que seuls les utilisateurs membres d'un groupe ou d'un rôle dans l'espace-noms **Cognos** puissent accéder à l'application.

Vérifiez que vous êtes un membre du rôle **Administrateur système** intégré dans l'espace-noms **Cognos** avant d'activer cette configuration.

### Procédure

1. Démarrez IBM Cognos Configuration sur chaque ordinateur Content Manager.
2. Dans la fenêtre **Explorateur**, dans la section **Sécurité**, cliquez sur **Authentification**.
3. Dans la fenêtre **Propriétés**, remplacez la valeur de la propriété **Voulez-vous limiter l'accès aux membres de l'espace-noms prédéfini ?** par **True**.
4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

### Que faire ensuite

Vous devez à présent retirer le groupe **Tous** de certains groupes et rôles intégrés de Cognos et vérifier que les utilisateurs autorisés appartiennent à au moins un groupe ou rôle Cognos. Ces tâches sont effectuées par des administrateurs dans les interfaces d'administration de Cognos Analytics. Pour plus d'informations, voir le *Guide de gestion d'IBM Cognos Analytics* ou le *Guide d'administration et de sécurité d'IBM Cognos Analytics*.

## Configuration de l'authentification LTPA

Vous pouvez configurer des composants IBM Cognos Analytics de sorte à utiliser l'authentification IBM LTPA (Lightweight Third-Party Authentication). La procédure décrite dans la présente rubrique se base sur l'environnement distribué Cognos Analytics 11.0.7 avec IBM Tivoli Directory Server LDAP ou Microsoft Active Directory définis comme sources d'authentification.

Pour implémenter l'authentification LTPA, Cognos Analytics doit être configuré de sorte à utiliser une source d'authentification configurée dans le conteneur WebSphere Liberty dans lequel elle s'exécute. Vous pouvez configurer la connexion unique entre Cognos Analytics et WebSphere Liberty en utilisant la configuration de mappage des identités dans l'espace-noms Cognos. Par exemple, vous pouvez configurer WebSphere Liberty afin qu'il utilise un serveur LDAP ou Active Directory pour l'authentification, puis configurer Cognos Analytics afin qu'il utilise le même serveur LDAP ou Active Directory, et définir le mappage des identités en vue de l'utilisation de REMOTE_USER.

Pour Cognos Analytics, cela signifie qu'un utilisateur doit être authentifié avec une identité affectée à la session HTTP avant l'accès à Cognos Analytics dans la même session. L'authentification est effectuée en présentant les données d'identification à un système de sécurité externe à Cognos. Le système de sécurité peut fournir l'identité et un genre de données d'identification adaptées à la connexion unique à d'autres systèmes, généralement sous la forme d'un jeton SSO. Les candidats typiques pour de tels systèmes de sécurité sont les proxys d'authentification, tels qu'IBM Tivoli WebSEAL, Oracle Oblix, Computer Associates SiteMinder, ou d'autres solutions logicielles ou matérielles pouvant authentifier une session HTTP et la rendre persistante dans un jeton.

WebSphere Liberty dispose de plusieurs méthodes d'authentification des utilisateurs. Pour plus d'informations, voir la documentation de WebSphere Liberty : https://www.ibm.com/support/knowledgecenter/en/SSD28V_8.5.5/com.ibm.websphere.wlp.nd.iseries.doc/ae/twlp_sec.html

## Configuration de l'authentification LTPA à l'aide d'un espace-noms LDAP

La procédure qui suit décrit comment configurer l'authentification LTPA pour Cognos Analytics lorsqu'IBM Tivoli Directory Server LDAP est utilisé comme source d'authentification.

Pour des détails sur la configuration de LDAP, voir «Configuration des composants IBM Cognos en vue de l'utilisation de LDAP», à la page 264.

### Procédure

1. A chaque emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
2. Dans **Explorateur**, sous **Sécurité**, cliquez avec le bouton droit sur **Authentification** , puis cliquez sur **Nouvelle ressource** > > **Espace-noms**.
3. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
4. Dans la liste **Type**, sélectionnez **LDAP – Valeurs générales par défaut**.
5. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.
6. Définissez les propriétés suivantes :

   **Hôte et port**
   Hôte qualifié complet et port du serveur LDAP.

   **Nom distinctif de base**
   Par exemple, `o=nom_organisation.com`

   **Fichier de correspondance d'utilisateur**
   Par exemple, `uid=${IDutilisateur},ou=people`

   **Voulez-vous utiliser une identité externe ?**
   `Vrai`

   **Mappage des identités externes**
   Par exemple, `uid=${environment("REMOTE_USER")},ou=people`
7. Si, lors de recherches, le fournisseur d'authentification LDAP doit établir une liaison avec le serveur d'annuaire à l'aide d'un paramètre **Nom distinctif et mot de passe de l'utilisateur de liaison** spécifique, indiquez ces valeurs.

   Si aucune valeur n'est indiquée, le fournisseur d'authentification LDAP se lie en tant qu'anonyme.

Si le mappage des identités externes est activée, la propriété **Nom distinctif et mot de passe de l'utilisateur de liaison** est utilisée pour tous les accès LDAP. Si le mappage des identités externes n'est pas activée, les propriétés **Nom distinctif et mot de passe de l'utilisateur de liaison** sont uniquement utilisées lorsqu'un filtre de recherche est spécifié pour la propriété **Fichier de correspondance d'utilisateur**. Dans ce cas, lorsque le nom unique de l'utilisateur est défini, les demandes envoyées ultérieurement au serveur LDAP sont exécutées dans le contexte d'authentification de l'utilisateur.

8. Si vous n'utilisez pas le mappage des identités externes, faites appel aux données d'identification de liaison pour effectuer des recherches sur le serveur d'annuaire LDAP. Pour cela, procédez comme suit :
   - Vérifiez que l'option **Voulez-vous utiliser une identité externe ?** est définie sur **Faux**.
   - Définissez l'option **Voulez-vous utiliser des données d'identification de liaison pour la recherche ?** sur **Vrai**.
   - Indiquez l'ID utilisateur et le mot de passe correspondant à l'option **Nom distinctif et mot de passe de l'utilisateur de liaison**.

   Si vous n'indiquez pas d'ID utilisateur et de mot de passe, et si l'accès anonyme est activé, la recherche est effectuée de façon anonyme.
9. Vérifiez les paramètres de mappage des objets et des attributs requis.

   En fonction de la configuration LDAP, vous devrez peut-être modifier certaines valeurs par défaut pour garantir une communication correcte entre les composants d'IBM Cognos et le serveur LDAP.

   Les attributs LDAP qui sont mis en correspondance avec la propriété **Nom** dans **Mappage des dossiers**, **Mappage de groupes** et **Mappage de comptes** doivent être accessibles à tous les utilisateurs authentifiés. En outre, la propriété **Nom** doit obligatoirement être définie.
10. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
11. Créez un fichier XML appelé `local-server.xml` et placez-le dans le répertoire *emplacement_installation*`/configuration`.
12. Dans le fichier `local-server.xml`, saisissez les valeurs appropriées à votre environnement :

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
 <featureManager>
  <feature>ldapRegistry-3.0</feature>
  <feature>appSecurity-2.0</feature>
 </featureManager>
 <ldapRegistry id="id" realm="realm"
  host="host" port="port" ignoreCase="true"
  baseDN="o=basedn" ldapType="Custom" sslEnabled="false">
  <idsFilters
   userFilter="(uid=%v,ou=people)"
   userIdMap="*:uid"
   groupFilter='(objectclass=groupofnames)'
   groupIdMap="*:cn" />
 </ldapRegistry>
      <webAppSecurity allowFailOverToBasicAuth="true" displayAuthenticationRealm="true"/>
</server>
```

13. Si Cognos Analytics est configuré de sorte à utiliser SSL, voir «Configuration du protocole SSL pour les composants d'IBM Cognos», à la page 188 pour plus d'informations.
14. Pour vérifier la configuration, connectez-vous à `http://`*hôte*`:`*port*`/bi` ou `https://`*hôte*`:`*port*`/bi` pour les systèmes compatibles avec SSL, où hôte est le domaine d'hôte Cognos Analytics qualifié complet.

La page de connexion de Cognos Analytics ne devrait pas s'afficher. Vous devriez à la place être invité par le navigateur à vous connecter.

### Que faire ensuite

Pour configurer la connexion unique entre l'application Cognos Analytics qui a été configurée avec l'authentification LTPA et l'application qui a été déployée dans une instance de WebSphere, installez la clé WebSphere sur chaque répartiteur Cognos Analytics où l'authentification LTPA a été configurée, et mettez à jour le fichier `local-server.xml` avec l'élément `<ltpa>` suivant :

```
<ltpa keysFileName="yourLTPAKeysFileName.keys"
keysPassword="keysPassword" expiration="120" />
```

Pour plus d'informations, voir la documentation de WebSphere Liberty.

## Configuration de l'authentification LTPA à l'aide d'un espace-noms Active Directory

La procédure qui suit décrit comment configurer l'authentification LTPA pour Cognos Analytics lorsque Microsoft Active Directory est utilisé comme source d'authentification.

### Procédure

1. A chaque emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
2. Dans **Explorateur**, sous **Sécurité**, cliquez avec le bouton droit sur **Authentification** , puis cliquez sur **Nouvelle ressource** > > **Espace-noms**.
3. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
4. Dans la liste **Type**, sélectionnez **LDAP - Valeurs par défaut pour Active Directory**, puis cliquez sur le bouton **OK**.

   Le nouveau fournisseur d'authentification s'affiche dans la fenêtre **Explorateur**, sous le composant **Authentification**. Les valeurs par défaut sont générées automatiquement. Vérifiez-les et modifiez-les si nécessaire.
5. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.

   **Conseil :** La propriété Identificateur d'espace-noms ne doit pas contenir de signe deux-points (:).
6. Définissez les valeurs de toutes les propriétés requises pour vous assurer que les composants d'IBM Cognos pourront localiser et utiliser le fournisseur d'authentification existant.
   - Pour **Fichier de correspondance d'utilisateur**, entrez `(sAMAccountName=${userID})`
   - Si vous utilisez un code d'accès unique, pour **Voulez-vous utiliser une identité externe ?**, définissez la valeur sur **Vrai**.
   - Si vous utilisez un code d'accès unique, pour **Mappage des identités externes**, entrez `(sAMAccountName=$environment("REMOTE_USER"))`.

     Si vous souhaitez supprimer le nom de domaine de la variable REMOTE_USER, entrez `(sAMAccountName=${replace(${environment("REMOTE_USER")},"domain\\","")})`.

**Important :** Veillez à utiliser uniquement la variable REMOTE_USER. L'utilisation d'une autre variable peut entraîner une vulnérabilité en matière de sécurité.

- Pour **Nom distinctif et mot de passe de l'utilisateur de liaison**, entrez **user@domain**.
- Pour **Identificateur unique**, entrez objectGUID

7. Créez un fichier XML appelé local-server.xml et placez-le dans le répertoire *emplacement_installation*/configuration.
8. Dans le fichier local-server.xml, saisissez les valeurs appropriées à votre environnement :

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
 <featureManager>
  <feature>ldapRegistry-3.0</feature>
  <feature>appSecurity-2.0</feature>
 </featureManager>
 <ldapRegistry id="id" realm="realm"
 host="host" port="port" ignoreCase="true"
 baseDN="DC=dc,DC=dc,DC=dc" bindDN="CN=doejohn,
              OU=Users,DC=dc,DC=dc,DC=dc"
 bindPassword="password" ldapType="Microsoft Active Directory" sslEnabled="false">
  <actived Filters
   userFilter="(&amp;(sAMAccountName=%v)(objectcategory=user))"
   groupFilter="(&amp;(cn=%v)(objectcategory=group))"
   userIdMap="user:sAMAccountName"
   groupIdMap="*:cn"
   groupMemberIdMap="memberOf:member">
  </actived Filters>
 </ldapRegistry>
 <webAppSecurity allowFailOverToBasicAuth="true" displayAuthenticationRealm="true"/>
</server>
```

9. Si Cognos Analytics est configuré de sorte à utiliser SSL, voir «Configuration du protocole SSL pour les composants d'IBM Cognos», à la page 188 pour plus d'informations.
10. Pour vérifier la configuration, connectez-vous à http://*hôte*:*port*/bi ou https://*hôte*:*port*/bi pour les systèmes compatibles avec SSL, où hôte est le domaine d'hôte Cognos Analytics complet.

    La page de connexion de Cognos Analytics ne devrait pas s'afficher. Vous devriez à la place être invité par le navigateur à vous connecter.

## Que faire ensuite

Pour configurer la connexion unique entre l'application Cognos Analytics qui a été configurée avec l'authentification LTPA et l'application qui a été déployée dans une instance de WebSphere, installez la clé WebSphere sur chaque répartiteur Cognos Analytics où l'authentification LTPA a été configurée, et mettez à jour le fichier local-server.xml avec l'élément <ltpa> suivant :

```
<ltpa keysFileName="yourLTPAKeysFileName.keys"
keysPassword="keysPassword" expiration="120" />
```

Pour plus d'informations, voir la documentation de WebSphere Liberty.

# Fournisseur d'authentification OpenID Connect

OpenID Connect est une couche d'identité simple au-dessus du protocole OAuth 2.0. Il est utilisé pour l'identité fédérée et l'authentification sur plusieurs applications qui partagent le même fournisseur d'identité. OpenID Connect est le fournisseur d'authentification Web recommandé si vous voulez fédérer IBM Cognos Analytics avec d'autres applications.

OpenID Connect est une norme moderne qui intègre les normes OpenID et OAuth 2.0. Elle est prise en charge pour les installations sur site et sur le cloud d'Cognos Analytics.

Cognos Analytics prend en charge les types de fournisseur d'identité OpenID Connect suivants :

- ADFS (Active Directory Federation Services)
- Azure AD (Active Directory)
- Google
- IBMid (fournisseur d'identité d'IBM)
- OKTA
- Ping
- SalesForce
- SiteMinder

**Conseil :** Contactez l'administrateur du fournisseur d'identité de votre organisation ou le service de ventes et de support pour savoir quelle version du produit vous devez utiliser.

## Proxy d'authentification OpenID Connect S'applique à la version 11.0.10 et aux versions ultérieures, sauf indication contraire

Cognos Analytics propose désormais un autre type de fournisseur, "Proxy d'authentification OpenID Connect", dans Cognos Configuration. Ce menu vous permet d'utiliser le fournisseur TSP (Trusted Signon Provider) pour OpenID Connect. Comme pour les entrées OpenID Connect, la liste des fournisseurs d'identité actuellement pris en charge s'affiche.

Les entrées des paramètres de configuration supplémentaires sont désormais visibles sous Propriétés avancées. Vous devrez configurer la déclaration que vous voulez transmettre au fournisseur réel ainsi que l'ID d'espace-noms du fournisseur réel.

- Nom de la déclaration d'identité : indique le nom de la déclaration qui sera fournie à l'espace-noms cible (par exemple, John Doe)
- Nom de l'environnement sécurisé : indique le nom de la variable d'environnement qui sera utilisée pour transférer la déclaration vers l'espace-noms cible (par exemple, REMOTE_USER)
- ID d'espace-noms de redirection : indique l'ID d'espace-noms qui sera appelé avec la déclaration obtenue du fournisseur d'identité OpenID (par exemple, LDAP)

### Optimisation de la connexion unique du fournisseur d'identité

Si votre fournisseur d'identité OpenID prend en charge la connexion unique et l'authentification à deux facteurs, Cognos Analytics peut optimiser cette fonctionnalité.

Si le fournisseur d'identité ne prend pas en charge la connexion unique, l'utilisateur est redirigé vers la page de connexion du fournisseur d'identité OpenID Connect lorsqu'il émet une demande d'authentification à Cognos Analytics. Une fois les informations nécessaires fournies, l'utilisateur est de nouveau redirigé vers Cognos Analytics avec un code d'autorisation à échanger contre un jeton d'ID contenant l'identité de l'utilisateur. L'utilisateur peut alors accéder à Cognos Analytics.

Si le fournisseur d'identité prend en charge la connexion unique, l'utilisateur reçoit le jeton d'ID lorsqu'il émet la demande d'authentification à Cognos Analytics et peut immédiatement accéder à l'application.

### Fédération d'IBMid avec des fournisseurs d'identité SAML 2.0

IBMid n'est autre que le fournisseur d'identité IBM OpenID Connect. Si votre fournisseur d'identité (IdP) ne prend pas en charge OpenID Connect mais prend en charge SAML 2.0, vous pouvez utiliser IBMid pour configurer un espace-noms OpenID Connect comme fournisseur d'authentification dans Cognos Analytics. Sélectionnez simplement IBMid comme fournisseur d'identité lorsque vous configurez l'espace-noms OpenID Connect.

Avec cette configuration d'espace-noms, vous pouvez fédérer Cognos Analytics avec la plupart des fournisseurs d'identité SAML 2.0. Par conséquent, lorsque des utilisateurs se connectent à Cognos Analytics, ils sont redirigés vers la page de connexion d'IBMid pour y entrer leur adresse e-mail. Si l'adresse e-mail est reconnue par IBMid, les utilisateurs sont redirigés vers la page de connexion du fournisseur d'identité SAML 2.0 de leur organisation. Sur cette page, les utilisateurs terminent le processus d'authentification en fournissant leurs données d'identification. Ils peuvent ensuite accéder à Cognos Analytics.

## Configuration d'un espace-noms OpenID Connect

Pour utiliser un fournisseur d'identité OpenID Connect avec IBM Cognos Analytics, vous devez configurer un espace-noms OpenID Connect.

Si vous utilisez IBMid comme fournisseur d'identité OpenID Connect, voir Gestion des espace-noms OpenID Connect pour plus d'informations.

Si les utilisateurs rencontrent des problèmes d'authentification une fois l'espace-noms OpenID Connect configuré avec succès, utilisez la journalisation des diagnostics dans le composant **Gérer** de Cognos Analytics pour traiter les incidents. Vous devez créer une nouvelle rubrique de journalisation basée sur la rubrique prédéfinie **AAA**. Modifiez la rubrique de journalisation **AAA** en y ajoutant les lignes de code suivantes :

```
{
"loggerDefinitions": [
{
"loggerName": "com.ibm.cognos.camaaa.internal.OIDC",
"level": "DEBUG",
"additivity": true
```

```
}
],
"topicName": "OIDC"
}
```

Pour plus d'informations sur la journalisation des diagnostics, voir Types et fichiers de journalisation.

## Procédure

1. Ouvrez IBM Cognos Configuration sur votre ordinateur Content Manager.
2. Sous **Sécurité** > **Authentification**, sélectionnez à l'aide du bouton droit de la souris **Nouvelle ressource** > **Espace-noms**.
3. Pour **Type (Groupe)**, sélectionnez **OpenID Connect**.
4. Pour **Type**, sélectionnez l'un des fournisseurs d'identité de la liste déroulante qui inclut les fournisseurs d'identité pris en charge.
5. Entrez le nom de l'espace-noms dans la zone **Nom**, puis cliquez sur **OK**.

   Le nouvel espace-noms est ajouté dans la sous-fenêtre **Explorateur** sous **Sécurité** > **Authentification** et ses caractéristiques sont affichées dans la sous-fenêtre de propriétés.
6. Indiquez des valeurs pour les propriétés de l'espace-noms.

   **Conseil :** Des informations sur chaque propriété sont affichées dans l'interface utilisateur lorsque vous cliquez sur une propriété.

   - L'**ID d'espace-noms** est utilisé dans l'ID de Cognos Access Manager (CAMID).
   - Indiquez des valeurs pour **Noeud final de recherche**, **Identificateur de client** et **Secret client OpenID Connect**, comme suggéré par votre administrateur OpenID Connect.
   - Mettez à jour l'**Adresse URL de retour** à l'aide de votre URL de passerelle ou de répartiteur, comme indiqué dans l'exemple suivant :

     `http://masociété:9300/bi/completeAuth.jsp`

     Si vous utilisez un équilibreur de charge dans votre environnement, incluez l'entrée DNS de cet équilibreur de charge dans l'**Adresse URL de retour** en regard des noeuds de la passerelle ou du répartiteur, comme indiqué dans l'exemple suivant :

     `https://DNS_équilibreur_charge.masociété.com:443/ibmcognos/bi/completeAuth.jsp`

     Dans cet exemple, la passerelle Cognos Analytics est installée sur le serveur Web.

     Si vous utilisez un ensemble de noeuds de répartiteur derrière l'équilibreur de charge où la passerelle Cognos Analytics n'est pas installée sur le serveur Web, l'**Adresse URL de retour** peut avoir l'apparence suivante :

     `https://DNS_équilibreur_charge.masociété.com:9300/bi/completeAuth.jsp`

   **Conseil :** Il n'est pas nécessaire d'indiquer les propriétés de **Multilocation** pour le moment.
7. Importez le certificat racine OpenID Connect de l'autorité de certification dans le magasin de clés de Cognos Analytics à l'aide de l'outil de certificat tiers.
   - Sur les systèmes d'exploitation UNIX ou Linux, entrez `ThirdPartyCertificateTool.sh -i -T -r cert.cer -p` **`NoPassWordSet`**
   - Sur les systèmes d'exploitation Windows, entrez `ThirdPartyCertificateTool.bat -i -T -r cert.cer -p` **`NoPassWordSet`**

**Conseil :** Remplacez la variable *cert* par le nom du fichier certificat utilisé par votre fournisseur d'identité OpenID Connect. Pour IBMid, le nom du fichier est `blueid.cer`.
La commande importe le contenu dans le fichier `CAMKeystore` du répertoire `certs` à l'aide du mot de passe spécifié.

8. Effectuez la même procédure de configuration sur votre ordinateur Content Manager de secours.
9. Redémarrez le service IBM Cognos sur l'ordinateur Content Manager et l'ordinateur Content Manager de secours.

### Résultats

Tous les utilisateurs inscrits avec votre fournisseur d'identité OpenID Connect doivent désormais avoir accès à Cognos Analytics.

## Configuration des composants d'IBM Cognos pour Active Directory Server

Si vous installez Content Manager sur un ordinateur doté d'un système d'exploitation Microsoft Windows, vous pouvez configurer un espace-noms Active Directory comme source d'authentification.

Si vous installez Content Manager sur un ordinateur UNIX, vous devez utiliser un espace-noms LDAP pour configurer Active Directory comme source d'authentification. Si vous installez Content Manager sur des ordinateurs panachant UNIX et Windows, vous devez utiliser un espace-noms LDAP pour configurer Active Directory sur toutes les instances de Content Manager. Lorsque vous employez un espace-noms LDAP pour vous authentifier auprès d'Active Directory Server, vous avez uniquement accès aux fonctions LDAP. Vous n'avez pas accès aux fonctions Active Directory telles que les propriétés avancées des domaines et le code d'accès unique avec la délégation Kerberos.

Si vous installez Content Manager sur un ordinateur Linux, les restrictions qui s'appliquent sont les mêmes que pour UNIX. Vous devez utiliser un espace-noms LDAP pour configurer Active Directory comme source d'authentification.

Si vous souhaitez utiliser Microsoft SQL Server ou Microsoft Analysis Server en tant que source de données et utiliser un code d'accès unique pour l'authentification, vous devez utiliser Active Directory en tant que source d'authentification.

Vous ne pouvez pas vous connecter au catalogue global Active Directory, qui est un serveur de mise en cache pour Active Directory Server. Si la connexion utilise le port 3268, vous devez en définir un autre. Par défaut, Active Directory Server utilise le port 389.

### Procédure

1. Configurez les composants IBM Cognos pour qu'ils utilisent un espace-noms Active Directory Server
2. Activez la communication sécurisée pour Active Directory Server, le cas échéant.
3. Activez le code d'accès unique entre Active Directory et les composants IBM Cognos.

# Configuration d'un espace-noms Active Directory

Vous pouvez utiliser Active Directory Server en tant que fournisseur d'authentification.

Vous avez également la possibilité de rendre disponibles des propriétés d'utilisateur personnalisées d'Active Directory Server dans les composants d'IBM Cognos.

## Avant de commencer

Pour que IBM Cognos puisse fonctionner correctement avec Active Directory Server, assurez-vous que le groupe Utilisateurs authentifiés dispose de privilèges de lecture sur le dossier Active Directory où sont stockés ces utilisateurs.

Si vous configurez un espace-noms Active Directory pour prendre en charge un code d'accès unique avec une source de données Microsoft SQL Server ou Microsoft Analysis Server, vérifiez la configuration suivante :

- La passerelle IBM Cognos est installée sur un serveur Web IIS, configuré pour l'authentification intégrée sur Microsoft Windows.
- La passerelle est affectée au site Web intranet local dans votre navigateur Web.
- Content Manager est installé sur un serveur Windows 2008 ou Windows 2012.
- Content Manager, les composants du groupe de serveurs d'applications, le serveur Web IIS et le serveur de source de données (Microsoft SQL Server ou Microsoft Analysis Server) appartiennent au domaine Active Directory.
- La connexion de source de données pour Microsoft SQL Server ou Microsoft Analysis Server est configurée pour un **espace-noms externe** et celui-ci doit être un espace-noms Active Directory.

Pour en savoir davantage sur les sources de données, reportez-vous au manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

## Procédure

1. A chaque emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
2. Dans **Explorateur**, sous **Sécurité**, cliquez avec le bouton droit sur **Authentification** , puis cliquez sur **Nouvelle ressource** > > **Espace-noms**.
3. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
4. Dans la liste **Type**, cliquez sur l'espace-noms approprié, puis sur **OK**.

   La nouvelle ressource de fournisseur d'authentification s'affiche dans la fenêtre **Explorer** sous le composant Authentification.
5. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.
6. Définissez les valeurs de toutes les propriétés requises pour vous assurer que les composants d'IBM Cognos pourront localiser et utiliser le fournisseur d'authentification existant.
7. Définissez les valeurs de la propriété **Hôte et port**.

   Pour permettre la prise en charge de la reprise Active Directory Server, vous pouvez indiquer le nom de domaine au lieu d'un contrôleur de domaine spécifique. Par exemple, utilisez *mon_domaine*.com:389 au lieu de dc1.*mon_domaine*.com:389.

8. Pour rechercher des détails en cas d'échec de l'authentification, indiquez l'ID utilisateur et le mot de passe de la propriété **Données d'identification pour la liaison**.

   Utilisez les données d'identification pour l'utilisateur d'Active Directory Server qui possède des privilèges de recherche et de lecture pour ce serveur.
9. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
10. Testez la connexion à un nouvel espace-noms. Dans la fenêtre **Explorateur**, sous **Authentification**, cliquez avec le bouton droit de la souris sur la nouvelle ressource d'authentification, puis sélectionnez **Tester**.

    Vous êtes invité à saisir les données d'identification d'un utilisateur dans l'espace-noms pour réaliser le test.

    Selon la manière dont votre espace-noms est configuré, vous pouvez entrer l'ID et le mot de passe d'un utilisateur valide dans l'espace-noms, ou le nom distinctif et le mot de passe de l'utilisateur de liaison.

### Résultats

IBM Cognos charge, initialise et configure les bibliothèques du fournisseur de l'espace-noms concerné.

## Mise à disposition des propriétés d'utilisateur personnalisées d'Active Directory pour les composants d'IBM Cognos

Vous pouvez utiliser des attributs d'utilisateur arbitraires d'Active Directory Server dans les composants d'IBM Cognos. Pour procéder à cette configuration, vous devez ajouter ces attributs en tant que propriétés personnalisées pour l'espace-noms Active Directory.

Les propriétés personnalisées sont disponibles en tant que paramètres de session par le biais de Framework Manager. Pour en savoir davantage sur les paramètres de session, voir le document *Framework Manager User Guide*

Vous pouvez également utiliser les propriétés personnalisées à l'intérieur des blocs de commande pour configurer les sessions et les connexions Oracle. Les blocs de commande peuvent être utilisés avec les connexions Oracle légères et les bases de données privées virtuelles. Pour plus d'informations, voir le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

### Procédure

1. A chaque emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Sécurité** > > **Authentification**, cliquez sur l'espace-noms Active Directory.
3. Dans la fenêtre **Propriétés**, cliquez sur la colonne **Valeur** correspondant à **Propriétés personnalisées**, puis sur l'icône Editer.
4. Dans la fenêtre **Valeur - Propriétés personnalisées**, cliquez sur **Ajouter**.
5. Cliquez sur la colonne **Nom** et saisissez le nom que les composants d'IBM Cognos doivent utiliser pour le paramètre de session.
6. Cliquez sur la colonne **Valeur** et saisissez le nom du paramètre de compte dans Active Directory Server.
7. Répétez les étapes 4 à 6 pour chaque paramètre personnalisé.
8. Cliquez sur le bouton **OK**.
9. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Activation de la communication sécurisée pour Active Directory Server

Si vous utilisez une connexion SSL pour Active Directory Server, vous devez copier le certificat d'Active Directory Server sur l'instance de Content Manager.

### Procédure

1. Sur chaque emplacement de Content Manager, utilisez le navigateur Web pour vous connecter à Active Directory Server et copiez le certificat de la racine de l'autorité de certification à l'emplacement de Content Manager.
2. Ajoutez ce certificat au magasin de certificat du compte que vous utilisez pour la session d'IBM Cognos en cours :
   - Si vous exécutez la session d'IBM Cognos avec un compte utilisateur, utilisez le même navigateur Web que celui utilisé à l'étape 1 pour importer le certificat de racine de l'autorité de certification dans le magasin de certificats de votre compte utilisateur.

     Pour en savoir davantage, reportez-vous à la documentation de votre navigateur Web.
   - Si vous exécutez la session d'IBM Cognos avec un compte local, utilisez la console MMC (Microsoft Management Console) pour importer le certificat de racine de l'autorité de certification dans le magasin de certificats de l'ordinateur local.

     Pour en savoir davantage, reportez-vous à la documentation de MMC.
3. Dans IBM Cognos Configuration, redémarrez le service comme suit :
   - Dans la fenêtre **Explorateur**, cliquez sur **Services IBM Cognos**, **IBM Cognos**.
   - Dans le menu **Actions**, cliquez sur l'option **Redémarrer**.

## Inclusion ou exclusion de domaines à l'aide des propriétés avancées

Lorsque vous configurez un espace-noms d'authentification pour IBM Cognos, les utilisateurs d'un seul domaine peuvent se connecter. A l'aide des propriétés avancées d'Active Directory Server, les utilisateurs des domaines (parent-enfant) associés et des arborescences de domaines non connexes de la même forêt de serveurs ont également la possibilité de se connecter. Les topologies inter-forêts ne sont pas prises en charge. Un espace-noms est requis par forêt.

Si vous définissez le paramètre chaseReferrals sur true, les utilisateurs du domaine authentifié d'origine et tous les domaines enfants de l'arborescence de domaines peuvent se connecter à IBM Cognos. Les utilisateurs issus d'un domaine parent du domaine authentifié d'origine ou d'une arborescence de domaines différente ne peuvent pas se connecter.

Si vous définissez le paramètre MultiDomainTrees sur true, les utilisateurs de toutes les arborescences de domaines du groupe de serveurs peuvent se connecter à IBM Cognos.

### Procédure

1. A chaque emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Sécurité** > > **Authentification**, cliquez sur l'espace-noms Active Directory.
3. Dans la fenêtre **Propriétés**, spécifiez la propriété **Hôte et port**:

- Pour les utilisateurs d'un domaine, indiquez l'hôte et le port d'un contrôleur de ce domaine.
- Pour les utilisateurs d'une arborescence de domaines, indiquez l'hôte et le port du contrôleur de niveau supérieur de l'arborescence.
- Pour les utilisateurs de toutes les arborescences de domaines du groupe de serveurs, indiquez l'hôte et le port de n'importe quel contrôleur de domaine du groupe de serveurs.

4. Cliquez dans la colonne Valeur des **Propriétés avancées**, puis cliquez sur l'icône Editer.
5. Dans la fenêtre **Valeur - Propriétés avancées**, cliquez sur **Ajouter**.
6. Définissez deux nouvelles propriétés, **chaseReferrals** et **MultiDomainTrees**, avec les valeurs issues du tableau suivant :

*Tableau 41. Paramètres de propriétés avancés*

| **Authentification pour** | **chaseReferrals** | **MultiDomainTrees** |
|---|---|---|
| Un domaine | Faux | Faux |
| Une arborescence de domaines | Vrai | Faux |
| Toutes les arborescences de domaines du groupe de serveurs | Vrai | Vrai |

7. Cliquez sur le bouton **OK**.
8. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Activation du code d'accès unique entre Active Directory Server et les composants IBM Cognos

Par défaut, le fournisseur Active Directory utilise l'authentification Kerberos. Il s'intègre au serveur Web IIS (Microsoft Internet Information Services) pour le code d'accès unique si l'authentification Windows (auparavant appelée stimulation/réponse de Windows NT) est activée sur le serveur Web IIS.

Si l'authentification Windows est activée, vous n'êtes pas invité à saisir à nouveau les informations d'authentification lorsque vous accédez au contenu d'IBM Cognos sécurisé par l'espace-noms Active Directory.

Si vous utilisez l'authentification Kerberos, vous pouvez choisir d'utiliser Service for User (S4U). S4U permet aux utilisateurs d'accéder à IBM Cognos Analytics à partir d'ordinateurs qui ne se trouvent pas sur le domaine Active Directory. Pour activer S4U, vous devez activer la délégation sous contrainte.

Par exemple, certains de vos utilisateurs possèdent des ordinateurs qui n'appartiennent pas au domaine, mais ils possèdent un compte de domaine. Lorsqu'ils ouvrent leur navigateur Web, leur compte de domaine leur est demandé. Toutefois, ils reçoivent le ticket Kerberos avec des privilèges d'identité uniquement, ce qui les empêche d'être authentifié sur IBM Cognos Analytics. Pour résoudre ce problème, vous pouvez utiliser S4U.

Si vous ne souhaitez pas utiliser l'authentification Kerberos, vous pouvez configurer le fournisseur de façon à accéder à la variable d'environnement **REMOTE_USER** pour obtenir le code d'accès unique.

**Important :** Veillez à utiliser uniquement la variable **REMOTE_USER**. L'utilisation d'une autre variable peut entraîner une vulnérabilité en matière de sécurité.

Pour permettre au code d'accès unique d'utiliser l'authentification Kerberos, vous devez vous assurer de bien effectuer les tâches suivantes :

1. Configurez l'authentification Windows sur votre serveur Web Microsoft IIS pour l'application ibmcognos/cgi-bin.
2. Installez Content Manager sur un ordinateur qui fait partie du domaine Active Directory, pour les instances de Content Manager actives et en veille.
3. Configurez les ordinateurs ou le compte utilisateur sous lequel Content Manager opère, afin qu'il soit sécurisé.

Pour plus d'informations, voir les notes techniques suivantes :

- Enabling single sign-on to CRN or Cognos secured against Active Directory technote (www.ibm.com/support/docview.wss?uid=swg21341889)
- When using Kerberos Single Sign-on (SSO) with Active Directory in Cognos, user is prompted for credentials technote (www.ibm.com/support/docview.wss?uid=swg21659267)

## Activation du code d'accès unique entre Active Directory Server et les composants d'IBM Cognos pour utiliser REMOTE_USER

Si vous ne souhaitez pas utiliser l'authentification Kerberos, vous pouvez configurer le fournisseur de façon à accéder à la variable d'environnement **REMOTE_USER** pour obtenir le code d'accès unique.

Vous devez affecter à la propriété avancée **singleSignonOption** la valeur **IdentityMapping**. Vous devez également indiquer les données d'identification de liaison pour l'espace-noms Active Directory.

Microsoft IIS définit **REMOTE_USER** par défaut lorsque vous activez l'authentification Windows. Si l'authentification Kerberos n'est pas utilisée, le code d'accès unique aux sources de données Microsoft OLAP (MSAS) n'est pas possible.

Lorsque vous définissez la variable **REMOTE_USER**, vous pouvez également choisir de la sauvegarder comme données d'identification sécurisées. Sauvegarder cette variable comme données d'identification sécurisée signifie que les travaux planifiés authentifient la variable **REMOTE_USER** avec les privilèges **Données d'identification pour la liaison**.

**Important :** Veillez à utiliser uniquement la variable **REMOTE_USER**. L'utilisation d'une autre variable peut entraîner une vulnérabilité en matière de sécurité.

### Procédure

1. Sur l'ordinateur où vous avez installé Content Manager, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, accédez à **Sécurité** > **Authentification** et sélectionnez l'espace-noms Active Directory.
3. Cliquez dans la colonne **Valeur** des **Propriétés avancées**, puis cliquez sur l'icône d'édition.

4. Dans la boîte de dialogue **Valeur - Propriétés avancées**, cliquez sur l'option **Ajouter**.
5. Dans la colonne **Nom**, saisissez `singleSignonOption`
6. Dans la colonne **Valeur**, saisissez `IdentityMapping`
7. Si vous souhaitez sauvegarder la variable REMOTE_USER comme données d'identification sécurisées, dans la boîte de dialogue **Valeur - Propriétés avancées**, cliquez sur **Ajouter**.
8. Dans la colonne **Nom**, saisissez `trustedCredentialType`
9. Dans la colonne **Valeur**, saisissez `IdentityMappingForTC`.
10. Cliquez sur le bouton **OK**.
11. Cliquez dans la colonne **Valeur** des **Données d'identification pour la liaison**, puis cliquez sur l'icône d'édition.
12. Dans la boîte de dialogue **Valeur - Données d'identification pour la liaison**, indiquez un ID utilisateur et un mot de passe, puis cliquez sur **OK**.

## Activation du code d'accès unique pour utiliser l'authentification Kerberos

Si votre serveur Web IIS est configuré pour l'authentification Windows, vous n'avez pas besoin d'ajouter de paramètres supplémentaires. L'authentification Kerberos est utilisée par défaut.

## Activation du code d'accès unique pour utiliser l'authentification Kerberos avec une délégation sous contrainte

Pour pouvoir utiliser la délégation sous contrainte, vous devez définir les noms SPN (Service Principal Name) des utilisateurs configurés pour exécuter les composants IBMCognos et le pool d'applications de votre serveur Web Microsoft Internet Information Services (IIS) dans votre domaine Active Directory.

Si vous utilisez Kerberos avec la délégation sous contrainte, vous devez ajouter un utilisateur **`sAMAccountName`** pour Content Manager lorsque vous configurez votre passerelle. Tous les gestionnaires de contenu actifs et de secours doivent être configurés pour être exécutés sous le même compte.

Si vous configurez le code d'accès unique à vos serveurs de base de données, vous devez configurer **`sAMAccountName`** de l'utilisateur qui exécute les composants du groupe des serveurs d'applications lorsque vous ajoutez l'espace-noms Active Directory. Tous les composants du groupe des serveurs d'applications doivent être configurés pour être exécutés sous le même compte.

Les noms SPN correspondent aux utilisateurs que vous entrez dans les zones **`sAMAccountName`** d'IBM Cognos Configuration.

Par exemple, supposons qu'un utilisateur exécute le composant Content Manager, qu'un autre exécute les composants du groupe des serveurs d'applications et qu'un dernier exécute le pool d'applications de votre serveur Web. L'utilisateur Content Manager est `CognosCMUser`. L'utilisateur des composants du groupe des serveurs d'applications est `CognosATCUser`. L'utilisateur du pool d'applications est `IISUser`. Chaque utilisateur se trouve dans le domaine `MyDomain`.

1. Vous devez configurer IIS de sorte que votre ID `MyDomain\IISUser` corresponde à l'identité du pool d'applications.
2. Exécutez la commande `setspn` pour l'ordinateur sur lequel IIS est exécuté.

   Par exemple :

```
setspn -A http/IISServerName MyDomain\IISUser
setspn -A http/IISServerName.MyDomain.com MyDomain\IISUser
```

3. Exécutez la commande `setspn` pour vos utilisateurs IBM Cognos.

   Par exemple :

   ```
   setspn -A ibmcognosba/CognosCMUser MyDomain\CognosCMUser
   setspn -A ibmcognosba/CognosATCUser MyDomain\CognosATCUser
   ```

   Dans ces commandes, vous devez utiliser `ibmcognosba` comme illustré dans les exemples. Les noms d'utilisateur et les domaines doivent correspondre à ceux de votre environnement.

   **Remarque :** Dans cet exemple, les utilisateurs **`sAMAccountName`** que vous devez entrer sont `CognosCMUser` et `CognosATCUser`.

4. Si vous configurez le code d'accès unique à votre serveur de base de données Microsoft SQL Server ou Microsoft SQL Server Analysis Services, vous devez configurer le nom SPN du serveur de base de données. Pour en savoir davantage, reportez-vous à la documentation de votre serveur de base de données.
5. Enfin, vous devez configurer la délégation sous contrainte dans l'outil d'administration des utilisateurs et ordinateurs Active Directory. Dans l'onglet **Délégation** de tous les utilisateurs (`IISUser`, `CognosCMUser` et `CognosATCUser`), vous devez sélectionner **Approuver cet utilisateur pour la délégation à des services spécifiques uniquement** et **Utiliser uniquement Kerberos** pour utiliser Kerberos avec la délégation sous contrainte. Sélectionnez **Approuver cet utilisateur pour la délégation à des services spécifiques uniquement** et **Utiliser un protocole d'authentification** si vous utilisez l'extension Kerberos S4U.

   Vous devez ensuite ajouter les noms SPN requis. Par exemple, ajoutez `ibmcognosba` comme type de service. Ajoutez également `DomainController1` et `DomainController2` comme type de service `ldap`.

   Si vous configurez le code d'accès unique pour la source de données, ajoutez le service MSOLAPSvc3 ou MSQLSVC.

## Procédure

1. Sur l'ordinateur où vous avez installé Content Manager, démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, accédez à **Sécurité** > **Authentification** et sélectionnez l'espace-noms Active Directory.
3. Cliquez dans la colonne **Valeur** des **Propriétés avancées**, puis cliquez sur l'icône d'édition.
4. Dans la boîte de dialogue **Valeur - Propriétés avancées**, cliquez sur l'option **Ajouter**.
5. Dans la colonne **Nom**, saisissez `singleSignonOption`
6. Dans la colonne **Valeur**, entrez l'une des valeurs suivantes :
   - Entrez `KerberosS4UAuthentication` si vous souhaitez utiliser l'authentification Kerberos en premier. Si Kerberos échoue, l'authentification Service For User (S4U) est tentée. Si S4U échoue, l'utilisateur est invité à entrer ces données d'identification.
   - Entrez `S4UAuthentication` si vous souhaitez utiliser l'authentification S4U en premier. Si S4U échoue, l'utilisateur est invité à entrer ces données d'identification.
7. Dans la boîte de dialogue **Valeur - Propriétés avancées**, cliquez sur l'option **Ajouter**.

8. Dans la colonne **Nom**, saisissez `trustedCredentialType`
9. Dans la colonne **Valeur**, entrez l'une des valeurs suivantes :
   - Entrez `CredentialForTC` si vous souhaitez sauvegarder les données d'identification de l'utilisateur comme données d'identification sécurisées. Par exemple, si vous souhaitez utiliser les données d'identification pour exécuter des travaux planifiés.
   - Entrez `S4UForTC` si vous ne souhaitez sauvegarder que le nom d'utilisateur authentifié comme données d'identification sécurisées. Le nom d'utilisateur est sauvegardé au format UPN et les travaux planifiés peuvent être exécutés avec le nom UPN sans le mot de passe de l'utilisateur.
10. Cliquez sur le bouton **OK**.
11. Cliquez dans la colonne **Valeur** de **sAMAccountName des composants du groupe des serveurs d'applications** et entrez le **`sAMAccountName`** de l'utilisateur qui exécute les composants du groupe des serveurs d'applications.

    **Important :** Cette valeur n'est requise que si vous configurez le code d'accès unique à votre serveur de base de données Microsoft SQL Server ou Microsoft SQL Server Analysis Services. Si vous ne configurez pas le code d'accès unique au serveur de base de données, ne modifiez pas cette valeur.
12. Cliquez sur **Fichier** > **Enregistrer**.
13. Redémarrez le service IBM Cognos.
14. Sur l'ordinateur où vous avez installé les composants de passerelle, ouvrez IBM Cognos Configuration.
15. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.
16. Cliquez dans la colonne **Valeur** de **sAMAccountName de Content Manager** et entrez le **`sAMAccountName`** de l'utilisateur qui exécute Content Manager.
17. Cliquez sur **Fichier** > **Enregistrer**.

## Configuration d'IBM Cognos pour utiliser l'espace-noms IBM Cognos Series 7

Vous pouvez configurer les composants d'IBM Cognos de façon à ce qu'ils utilisent un espace-noms IBM Cognos Series 7 en tant que fournisseur d'authentification. Les utilisateurs sont authentifiés sur la base des paramètres d'authentification et d'accès paramétrés pour l'espace-noms IBM Cognos Series 7.

Un espace-noms IBM Cognos Series 7 est requis si vous souhaitez utiliser des PowerCubes IBM Cognos Series 7 et des modèles Transformer dans IBM Cognos Analytics. Vous devez configurer l'espace-noms avant que vous chargiez les modèles Transformer.

**Remarque :** Vous ne pouvez pas utiliser un fichier IBM Cognos Series 7 Local Authentication Export (LAE) pour l'authentification auprès des composants IBM Cognos.

Vous pouvez configurer les composants d'IBM Cognos de façon à ce qu'ils utilisent plusieurs fournisseurs d'authentification d'IBM Cognos Series 7. Tous les espaces-noms IBM Cognos Series 7 utilisent le même Ticket Server principal d'IBM Cognos Series 7. Dans le cas contraire, vous pouvez recevoir des messages d'erreur ou être invité à vous authentifier plusieurs fois. Pour maintenir les performances vérifiez aussi que Ticket Server est en cours d'exécution.

Si vous modifiez les informations de configuration stockées dans le serveur d'annuaire utilisé pour IBM Cognos Series 7, vous devez redémarrer le service IBM Cognos pour que les modifications soient prises en compte dans l'installation d'IBM Cognos.

L'utilisateur doit faire partie d'au moins une classe d'utilisateurs Access Manager pour pouvoir se connecter aux composants d'IBM Cognos.

### Procédure

1. Configurez un espace-noms Series 7
2. Activez la communication sécurisée pour le serveur d'annuaire utilisé par l'espace-noms IBM Cognos Series 7, le cas échéant.
3. Activez le code d'accès unique entre IBM Cognos Series 7 et IBM Cognos

## Configuration d'un espace-noms IBM Cognos Series 7

Vous pouvez configurer IBM Cognos de façon à ce qu'il utilise un ou plusieurs espaces-noms d'IBM Cognos Series 7 pour l'authentification.

### Procédure

1. A chaque emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
2. Dans **Explorateur**, sous **Sécurité**, cliquez avec le bouton droit sur **Authentification** , puis cliquez sur **Nouvelle ressource** > > **Espace-noms**.
3. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
4. Dans la liste **Type**, cliquez sur l'espace-noms approprié, puis sur **OK**.

   La nouvelle ressource de fournisseur d'authentification s'affiche dans la fenêtre **Explorer** sous le composant Authentification.
5. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.
6. Définissez les valeurs de toutes les propriétés requises pour vous assurer que les composants d'IBM Cognos pourront localiser et utiliser le fournisseur d'authentification existant.

   Si vous disposez d'un espace-noms IBM Cognos Series 7 version 16.0, assurez-vous que la propriété **Encodage des données** est définie sur **UTF-8**. En outre, les emplacements dans lesquels Content Manager est installé doivent utiliser les mêmes paramètres régionaux que les données de l'espace-noms IBM Cognos Series 7.

   La valeur de l'hôte peut être un nom de serveur ou une adresse IP. Si vous publiez depuis PowerPlay Enterprise Server sur IBM Cognos Analytics, vous devez utiliser le même format que celui qui est utilisé dans IBM Cognos Series 7 Configuration Manager pour l'emplacement du serveur d'annuaire. Par exemple, si le nom du serveur est utilisé dans IBM Cognos Series 7 Configuration Manager, vous devez également l'utiliser dans IBM Cognos Configuration pour IBM Cognos Analytics.
7. Si votre environnement d'espace-noms contient la version 15.2 de l'espace-noms d'IBM Cognos Series 7, vous devez désactiver le paramètre **Series7NamespacesAreUnicode**.
   - Dans la fenêtre **Propriétés**, dans la valeur **Propriétés avancées**, puis cliquez sur l'icône Editer.
   - Dans la fenêtre **Valeur - Propriétés avancées**, cliquez sur **Ajouter**.
   - Dans la zone **Nom**, saisissez **Series7NamespacesAreUnicode**.

- Dans la zone **Valeur**, saisissez **Faux**, puis cliquez sur **OK**.

8. Dans la section **Paramètres de cookie** de la fenêtre **Propriétés**, assurez-vous que les propriétés **Chemin d'accès**, **Domaine** et **Indicateur de sécurité activé ?** correspondent aux paramètres configurés pour IBM Cognos Series 7.
9. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
10. Testez la connexion à un nouvel espace-noms. Dans la fenêtre **Explorateur**, sous **Authentification**, cliquez avec le bouton droit de la souris sur la nouvelle ressource d'authentification, puis sélectionnez **Tester**.

    Vous êtes invité à saisir les données d'identification d'un utilisateur dans l'espace-noms pour réaliser le test.

    Selon la manière dont votre espace-noms est configuré, vous pouvez entrer l'ID et le mot de passe d'un utilisateur valide dans l'espace-noms, ou le nom distinctif et le mot de passe de l'utilisateur de liaison.

## Activation de la communication sécurisée pour le serveur d'annuaire utilisé par l'espace-noms IBM Cognos Series 7

Si vous utilisez une connexion SSL pour le serveur d'annuaire utilisé par l'espace-noms IBM Cognos Series 7, vous devez configurer le certificat de Directory Server à chaque emplacement de Content Manager.

Pour plus d'informations, voir le document IBM Cognos Access Manager *Administrator Guide* et la documentation du serveur d'annuaire.

## Activation du code d'accès unique entre IBM Cognos Series 7 et IBM Cognos

Si votre espace-noms IBM Cognos Series 7 a été configuré pour intégrer les mécanismes d'authentification externe associés au code d'accès unique, le fournisseur d'IBM Cognos Series 7 utilise automatiquement cette configuration.

En configurant le code d'accès unique, vous n'êtes pas invité à saisir à nouveau les informations d'authentification lorsque vous accédez au contenu d'IBM Cognos sécurisé par l'espace-noms IBM Cognos Series 7.

### Procédure

1. Veillez à configurer les composants d'IBM Cognos pour utiliser un espace-noms IBM Cognos Series 7 comme fournisseur d'authentification.
2. Pour IBM Cognos Series 7, démarrez Configuration Manager.
3. Cliquez sur **Ouvrir la configuration actuelle**.
4. Sous l'onglet **Composants**, dans la fenêtre **Explorateur**, développez **Services**, **Access Manager - Authentification Web** et cliquez sur **Paramètres de cookie**.
5. Dans la fenêtre **Propriétés**, assurez-vous que les propriétés **Chemin d'accès**, **Domaine** et **Indicateur de sécurité activé ?** correspondent aux paramètres configurés pour IBM Cognos Analytics.
6. Enregistrez et fermez Configuration Manager.
7. Si l'espace-noms IBM Cognos Series 7 utilise le plug-in Trusted Signon pour le code d'accès unique, vous devez dès maintenant définir la fonction SaferAPIGetTrustedSignonWithEnv.

### Résultats

Vous pouvez maintenant ajouter des classeurs d'IBM Cognos Upfront Series 7 à IBM Cognos Analytics.

## Espaces-noms IBM Cognos Series 7 et plug-in IBM Cognos Series 7 Trusted Signon

Si l'espace-noms IBM Cognos Series 7 utilise le plug-in Trusted Signon pour le code d'accès unique, vous devez dès maintenant définir la fonction SaferAPIGetTrustedSignonWithEnv dans le plug-in. Vous devez ensuite recompiler et redéployer la bibliothèque pour que le code d'accès unique prenne effet entre les composants IBM Cognos et votre mécanisme d'authentification.

La fonction SaferAPIGetTrustedSignonWithEnv est une version mise à jour de la fonction SaferAPIGetTrustedSignon. Cette mise à jour est requise car la connexion à IBM Cognos n'est pas effectuée sur le serveur Web, comme c'est le cas avec les applications IBM Cognos Series 7. Par conséquent, il n'est pas possible pour le plug-in d'effectuer un appel API getenv( ) pour extraire les variables de l'environnement du serveur Web. Le plug-in peut exiger que des variables d'environnement spécifiques soient supprimées du serveur Web à l'aide de la fonction SaferAPIGetTrustedSignonWithEnv.

Si vous exécutez les produits IBM Cognos Series 7 et IBM Cognos à l'aide du même plug-in, les fonctions SaferAPIGetTrustedSignonWithEnv et SaferAPIGetTrustedSignon sont requises. Pour en savoir davantage sur la fonction SaferAPIGetTrustedSignon, reportez-vous à la documentation d'IBM Cognos Series 7.

### Fonction SaferAPIGetTrustedSignonWithEnv

Pour que les utilisateurs soient authentifiés correctement par Access Manager, les codes d'accès au SE doivent exister et être activés dans l'espace-noms en cours.

La mémoire pour les noms trustedSignonName et trustedDomainName renvoyés est allouée dans cet API. Si la fonction renvoie SAFER_SUCCESS, Access Manager appelle la fonction SaferAIFreeTrustedSignon pour libérer la mémoire allouée.

La mémoire de la fonction reqEnvVarList renvoyée est allouée dans cet API. Si la fonction renvoie SAFER_INFO_REQUIRED, Access Manager appelle la fonction SaferAPIFreeBuffer() pour libérer la mémoire allouée.

Vous devez mettre en oeuvre les fonctions SaferAPIGetTrustedSignon et SaferAPIFreeBuffer pour enregistrer correctement la bibliothèque lorsque la fonction SaferAPIGetTrustedSignonWithEnv est mise en oeuvre. La fonction SaferAPIGetError est nécessaire uniquement si vous voulez que des messages d'erreur précis soient renvoyés à partir du plug-in.

### Syntaxe

```
SaferAPIGetTrustedSignonWithEnv(
   EnvVar             envVar[],                  /*[IN]*/
   char               **reqEnvVarList,           /*[OUT]*/
   void               **trustedSignonName,       /*[OUT]*/
   unsigned long      *trustedSignonNameLength,  /*[OUT]*/
   void               **trustedDomainName,       /*[OUT]*/
   unsigned long      *trustedDomainNameLength,  /*[OUT]*/
```

```
SAFER_USER_TYPE    *userType,                  /*[OUT]*/
void               **implementerData);         /*[IN/OUT]*/
```

## Paramètres de la fonction SaferAPIGetTrustedSignonWithEnv

*Tableau 42. Paramètres et description de la fonction SaferAPIGetTrustedSignonWithEnv*

| Paramètre | Description |
|---|---|
| [in] envVar | Tableau de noms de variable d'environnement et de valeurs extraits du serveur Web. La fin du tableau est représentée par une entrée dotée d'un nom envVarName nul et d'une valeur envVarValue nulle. Notez que la première fois que cet API est appelé, le groupe envVar contient uniquement la fin du repère de tableau. |
| [in] reqEnvVarList | Chaîne contenant une liste de noms de variable d'environnement séparés par une virgule et requis par la mise en oeuvre Safer. La fin de la liste doit se terminer par une valeur nulle. |
| [out] trustedSignonName | Séquence d'octets identifiant l'utilisateur actuellement authentifié. Cette valeur ne doit pas nécessairement être nulle. Cette valeur est obligatoire. |
| [out] trustedSignonNameLength | Valeur d'entier indiquant la longueur de la fonction trustedSignonName. Cette longueur doit exclure la marque de fin nulle, si elle est présente. Cette valeur est obligatoire. |
| [out] trustedDomainName | Séquence d'octets identifiant le domaine de l'utilisateur actuellement authentifié. Vous n'avez pas nécessairement besoin de définir cette valeur comme nulle. S'il n'y a pas de nom trustedDomainName, le renvoi est nul. Cette valeur est facultative. |
| [out] trustedDomainNameLength | Valeur d'entier indiquant la longueur du nom trustedDomainName. Cette longueur doit exclure la marque de fin nulle, si elle est présente. Cette valeur est obligatoire et doit être réglée sur zéro s'il n'existe pas de nom trustedDomainName. |

*Tableau 42. Paramètres et description de la fonction SaferAPIGetTrustedSignonWithEnv (suite)*

| Paramètre | Description |
|---|---|
| [out] userType | Valeur indiquant le type d'utilisateur qu'Access Manager doit authentifier. Cette valeur est obligatoire.<br><br>Les valeurs renvoyées suivantes sont nécessaires pour qu'Access Manager authentifie les utilisateurs correctement :<br><br>**SAFER_NORMAL_USER**<br>Utilisateur nommé. Les codes d'accès au SE doivent exister et être activés dans l'espace-noms actuel.<br><br>**SAFER_GUEST_USER**<br>Invité. Un compte d'invité doit exister et être activé dans l'espace-noms actuel.<br><br>**SAFER_ANONYMOUS_USER**<br>Utilisateur anonyme. Un compte utilisateur anonyme doit exister et être activé dans l'espace-noms actuel. |
| [in/out] implementerData | Pointeur utilisé pour conserver les données spécifiques à la mise en oeuvre entre les appels. Un appel se produit à chaque fois qu'Access Manager sollicite le plug-in Trusted Signon. Cette valeur est valide uniquement si le plug-in Trusted Signon est appelé et qu'une valeur lui est attribuée. |

## Configuration d'IBM Cognos pour l'utilisation d'un fournisseur d'authentification personnalisé

Si vous avez implémenté un fournisseur d'authentification Java personnalisé avec votre infrastructure de sécurité existante, vous pouvez configurer les composants IBM Cognos pour qu'ils l'utilisent.

Vous pouvez utiliser un fournisseur d'authentification personnalisé pour accéder à des utilisateurs d'une source d'authentification et les authentifier. Vous pouvez également l'utiliser comme méthode de code d'accès unique pour intégrer les composants d'IBM Cognos à votre infrastructure de sécurité. Vous pouvez masquer cet espace-noms de la vue des utilisateurs durant la connexion.

Pour en savoir davantage, reportez-vous au manuel *Custom Authentication Provider Developer Guide*.

## Configuration d'un espace-noms d'authentification personnalisé

Vous pouvez configurer les composants d'IBM Cognos de façon à ce qu'ils utilisent un espace-noms d'authentification personnalisé. Toute configuration supplémentaire pour l'accès à une source d'authentification, le code d'accès unique ou des attributs personnalisés dépend de l'implémentation du fournisseur d'authentification personnalisé.

Vérifiez que les versions de Java runtime environment (JRE) et Java SDK (Software Development Kit) que vous utilisez sont compatibles entre elles. Si vous utilisez des versions de JRE et de Java SDK (Software Development Kit) prises en charge mais qui ne sont pas compatibles entre elles, le fournisseur d'authentification Java personnalisé que vous configurez n'apparaîtra pas dans la liste des espaces-noms, dans IBM Cognos Configuration.

### Procédure

1. Ouvrez IBM Cognos Configuration à chaque emplacement où Content Manager est installé.
2. Dans la fenêtre **Explorateur**, sous **Sécurité**, cliquez avec le bouton droit sur **Authentification** , puis cliquez sur **Nouvelle ressource** > **Espace-noms**.
3. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
4. Dans la liste **Type**, sélectionnez **Fournisseur Java personnalisé**, puis cliquez sur **OK**.

   Le nouveau fournisseur d'authentification s'affiche dans la fenêtre **Explorateur**, sous le composant **Authentification**.
5. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.

   **Conseil :** La propriété Identificateur d'espace-noms ne doit pas contenir de signe deux-points (:).
6. Définissez les valeurs de toutes les autres propriétés requises pour vous assurer que IBM Cognos peut localiser et utiliser le fournisseur d'authentification existant.
7. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
8. Testez la connexion à un nouvel espace-noms. Dans la fenêtre **Explorateur**, sous **Authentification**, cliquez avec le bouton droit de la souris sur la nouvelle ressource d'authentification, puis sélectionnez **Tester**.

   Vous êtes invité à saisir les données d'identification d'un utilisateur dans l'espace-noms pour réaliser le test.

   Selon la manière dont votre espace-noms est configuré, vous pouvez entrer l'ID et le mot de passe d'un utilisateur valide dans l'espace-noms, ou le nom distinctif et le mot de passe de l'utilisateur de liaison.

### Résultats

IBM Cognos charge, initialise et configure les bibliothèques du fournisseur de l'espace-noms concerné.

## Masquage de l'espace-noms de la vue des utilisateurs durant la connexion

Vous pouvez masquer des espaces-noms de la vue des utilisateurs durant la connexion. Vous pouvez disposer d'espaces-noms de codes d'accès sécurisés sans qu'ils soient affichés dans la liste de sélection des espaces-noms présentée lorsque les utilisateurs se connectent.

Supposons, par exemple, que vous souhaitiez généraliser le code d'accès unique à l'ensemble des systèmes tout en permettant aux utilisateurs de s'authentifier directement sur IBM Cognos sans être invités à choisir un espace-noms.

### Procédure

1. A chaque emplacement où vous avez configuré un fournisseur d'authentification Java personnalisé, ouvrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Sécurité** > **Authentification**, cliquez sur le fournisseur d'authentification Java personnalisé.
3. Dans la fenêtre **Propriétés**, cliquez sur la zone située en regard de l'option **Sélectionnable pour authentification ?**, puis sélectionnez **False**.
4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

### Résultats

L'espace-noms n'est pas affiché sur la liste de sélection présentée durant la connexion.

## Configuration des composants IBM Cognos en vue de l'utilisation de LDAP

Vous pouvez configurer les composants d'IBM Cognos de façon à ce qu'ils utilisent un espace-noms LDAP en tant que fournisseur d'authentification. Vous pouvez utiliser un espace-noms LDAP pour les utilisateurs qui sont stockés dans un annuaire d'utilisateurs LDAP, sur Active Directory Server, sur IBM Directory Server, sur Novell Directory Server ou sur Oracle Directory Server.

Vous pouvez aussi utiliser l'authentification LDAP avec des sources de données OLAP IBM Db2 et Essbase en définissant l'espace-noms LDAP lorsque vous configurez la connexion de source de données. Pour plus d'informations, voir le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Vous avez également la possibilité de rendre disponibles des propriétés d'utilisateur personnalisées de l'espace-noms LDAP dans les composants d'IBM Cognos.

Si vous souhaitez lier les utilisateurs au serveur LDAP, voir «Mappage LDAP».

### Procédure

1. «Configuration d'un espace-noms LDAP», à la page 265
2. Mettez à la disposition des composants d'IBM Cognos les propriétés d'utilisateur personnalisées, le cas échéant.
3. Activez la communication sécurisée pour le serveur LDAP, le cas échéant.
4. Activez le code d'accès unique entre LDAP et les composants IBM Cognos, le cas échéant.

## Mappage LDAP

Pour lier un utilisateur au serveur LDAP, le fournisseur d'authentification LDAP doit construire le nom distinctif (DN). Si la propriété Voulez-vous utiliser une identité externe ? a la valeur Vrai, elle utilise la propriété Mappage des identités externes pour tenter de résoudre le nom unique de l'utilisateur. S'il ne trouve pas la variable d'environnement ou le nom unique dans le serveur LDAP, il essaie d'utiliser la propriété Fichier de correspondance d'utilisateur pour créer le DN.

Si les utilisateurs occupent différents niveaux hiérarchiques dans le serveur d'annuaire, vous pouvez configurer les propriétés Fichier de correspondance d'utilisateur et Mappage des identités externes de façon à ce qu'elles utilisent des

filtres de recherche. Lorsque le fournisseur d'authentification LDAP effectue des recherches, il utilise les filtres que vous spécifiez pour les propriétés Fichier de correspondance d'utilisateur et Mappage des identités externes. Par ailleurs, il établit une liaison avec le serveur d'annuaire au moyen de la valeur que vous indiquez pour la propriété Nom distinctif et mot de passe de l'utilisateur de liaison ou de façon anonyme si aucune valeur n'est précisée.

Si un espace-noms LDAP est configuré pour utiliser la propriété Mappage des identités externes pour l'authentification, le fournisseur LDAP se lie au serveur d'annuaire à l'aide de la propriété Nom distinctif et mot de passe de l'utilisateur de liaison ou de façon anonyme si aucune valeur n'est indiquée. Tous les utilisateurs qui se connectent à IBM Cognos à l'aide d'un mappage des identités externes voient les mêmes utilisateurs, groupes et dossiers que l'utilisateur de liaison.

Si vous n'utilisez pas le mappage des identités externes, vous pouvez indiquer si des données d'identification de liaison doivent être utilisées pour rechercher le serveur d'annuaire LDAP en configurant la propriété **Voulez-vous utiliser des données d'identification de liaison pour la recherche ?**. Lorsque cette propriété est activée, les recherches sont effectuées à l'aide des données d'identification de l'utilisateur de liaison ou d'un accès anonyme si aucune valeur n'est indiquée. Lorsque cette propriété est désactivée (ce qui correspond au paramètre par défaut), les recherches sont effectuées à l'aide des données d'identification de l'utilisateur connecté. L'utilisation de données d'identification de liaison présente l'avantage de pouvoir modifier uniquement les droits d'administration de l'utilisateur de liaison, au lieu de devoir modifier ces droits pour plusieurs utilisateurs.

**Remarque :** Si vous utilisez une syntaxe de non distinctif, telle que *uid*=${*userID*}, ou=*mycompany*.com, pour les propriétés **Recherche d'utilisateur**, **Mappage des identités externes** ou **Nom distinctif et mot de passe de l'utilisateur de liaison**, vous devez protéger par échappement tous les caractères spéciaux utilisés dans le nom distinctif. Si vous employez une syntaxe de recherche telle que (*ID_unique*=${*ID_utilisateur*}), pour les propriétés **Fichier de correspondance d'utilisateur**, **Mappage des identités externes**, vous ne devez pas protéger par échappement les caractères spéciaux utilisés dans le nom unique.

## Configuration d'un espace-noms LDAP

Vous pouvez configurer les composants d'IBM Cognos de façon à ce qu'ils utilisent un espace-noms LDAP lorsque les utilisateurs sont stockés dans un annuaire d'utilisateurs LDAP. Il est possible d'accéder à l'annuaire d'utilisateurs LDAP à partir d'un autre environnement serveur tel qu'Active Directory Server ou CA SiteMinder.

Si vous configurez un espace-noms LDAP pour un serveur d'annuaire non LDAP, reportez-vous à la section appropriée :

- Pour Active Directory Server, voir Configuration d'un espace-noms LDAP pour Active Directory Server.
- Pour IBM Directory Server, voir Configuration d'un espace-noms LDAP pourIBM Directory Server.
- Pour Novell Directory Server, voir Configuration d'un espace-noms LDAP pour Novell Directory Server.
- Pour Oracle Directory Server, voir Configuration d'un espace-noms LDAP pour Oracle Directory Server.

Vous pouvez aussi utiliser l'authentification LDAP avec des sources de données OLAP IBM Db2 et Essbase en définissant l'espace-noms LDAP lorsque vous configurez la connexion de source de données. Pour plus d'informations, voir le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

## Procédure

1. A chaque emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
2. Dans **Explorateur**, sous **Sécurité**, cliquez avec le bouton droit sur **Authentification** , puis cliquez sur **Nouvelle ressource** > > **Espace-noms**.
3. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
4. Dans la liste **Type**, cliquez sur l'espace-noms approprié, puis sur **OK**.

   La nouvelle ressource de fournisseur d'authentification s'affiche dans la fenêtre **Explorer** sous le composant Authentification.
5. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.
6. Définissez les valeurs de toutes les propriétés requises pour vous assurer que les composants d'IBM Cognos pourront localiser et utiliser le fournisseur d'authentification existant.
7. Si, lors de recherches, le fournisseur d'authentification LDAP doit établir une liaison avec le serveur d'annuaire à l'aide d'un paramètre **Nom distinctif et mot de passe de l'utilisateur de liaison** spécifique, indiquez ces valeurs.

   Si aucune valeur n'est indiquée, le fournisseur d'authentification LDAP se lie en tant qu'anonyme.

   Si le mappage des identités externes est activée, la propriété **Nom distinctif et mot de passe de l'utilisateur de liaison** est utilisée pour tous les accès LDAP. Si le mappage des identités externes n'est pas activée, les propriétés **Nom distinctif et mot de passe de l'utilisateur de liaison** sont uniquement utilisées lorsqu'un filtre de recherche est spécifié pour la propriété **Fichier de correspondance d'utilisateur**. Dans ce cas, lorsque le nom unique de l'utilisateur est défini, les demandes envoyées ultérieurement au serveur LDAP sont exécutées dans le contexte d'authentification de l'utilisateur.
8. Si vous n'utilisez pas le mappage des identités externes, utilisez les données d'identification de liaison pour effectuer des recherches sur le serveur d'annuaire LDAP. Pour cela, procédez comme suit :
   - Vérifiez que l'option **Voulez-vous utiliser une identité externe ?** est définie sur **Faux**.
   - Définissez l'option **Voulez-vous utiliser des données d'identification de liaison pour la recherche ?** sur **Vrai**.
   - Indiquez l'ID utilisateur et le mot de passe correspondant à l'option **Nom distinctif et mot de passe de l'utilisateur de liaison**.

   Si vous n'indiquez pas d'ID utilisateur et de mot de passe, et si l'accès anonyme est activé, la recherche est effectuée de façon anonyme.
9. Vérifiez les paramètres de mappage des objets et des attributs requis.

   En fonction de la configuration LDAP, vous devrez peut-être modifier certaines valeurs par défaut pour garantir une communication correcte entre les composants d'IBM Cognos et le serveur LDAP.

   Les attributs LDAP qui sont mis en correspondance avec la propriété **Nom** dans **Mappage des dossiers**, **Mappage de groupes** et **Mappage de comptes** doivent être accessibles à tous les utilisateurs authentifiés. En outre, la propriété **Nom** doit obligatoirement être définie.

10. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
11. Testez la connexion à un nouvel espace-noms. Dans la fenêtre **Explorateur**, sous **Authentification**, cliquez avec le bouton droit de la souris sur la nouvelle ressource d'authentification, puis sélectionnez **Tester**.

    Vous êtes invité à saisir les données d'identification d'un utilisateur dans l'espace-noms pour réaliser le test.

    Selon la manière dont votre espace-noms est configuré, vous pouvez entrer l'ID et le mot de passe d'un utilisateur valide dans l'espace-noms, ou le nom distinctif et le mot de passe de l'utilisateur de liaison.

### Résultats

IBM Cognos charge, initialise et configure les bibliothèques du fournisseur de l'espace-noms concerné.

## Configuration d'un espace-noms LDAP pour Active Directory Server

Si vous configurez un nouvel espace-noms LDAP pour l'utiliser avec Active Directory Server, les valeurs par défaut sont générées automatiquement.

### Procédure

1. A chaque emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Sécurité,** cliquez avec le bouton droit sur **Authentification**, puis cliquez sur **Nouvelle ressource** > **Espace-noms**.
3. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
4. Dans la liste **Type**, sélectionnez **LDAP - Valeurs par défaut pour Active Directory**, puis cliquez sur le bouton **OK**.

   Le nouveau fournisseur d'authentification s'affiche dans la fenêtre **Explorateur**, sous le composant **Authentification**. Les valeurs par défaut sont générées automatiquement. Vérifiez-les et modifiez-les si nécessaire.
5. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.

   **Conseil :** La propriété Identificateur d'espace-noms ne doit pas contenir de signe deux-points (:).
6. Définissez les valeurs de toutes les propriétés requises pour vous assurer que les composants d'IBM Cognos pourront localiser et utiliser le fournisseur d'authentification existant.

   Voici des exemples de paramètres :

   - Pour **Fichier de correspondance d'utilisateur**, entrez `(sAMAccountName=${userID})`
   - Si vous utilisez un code d'accès unique, pour **Voulez-vous utiliser une identité externe ?**, définissez la valeur sur **Vrai**.
   - Si vous utilisez un code d'accès unique, pour **Mappage des identités externes**, entrez `(sAMAccountName=$environment("REMOTE_USER"))`.

     Si vous souhaitez supprimer le nom de domaine de la variable REMOTE_USER, entrez `(sAMAccountName=${replace(${environment("REMOTE_USER")}, "domain\\","")})`.

**Important :** Veillez à utiliser uniquement la variable REMOTE_USER. L'utilisation d'une autre variable peut entraîner une vulnérabilité en matière de sécurité.

- Pour **Nom distinctif et mot de passe de l'utilisateur de liaison**, entrez **user@domain**.
- Pour **Identificateur unique**, entrez `objectGUID`

7. Si, lors de recherches, le fournisseur d'authentification LDAP doit établir une liaison avec le serveur d'annuaire à l'aide d'un paramètre **Nom distinctif et mot de passe de l'utilisateur de liaison** spécifique, indiquez ces valeurs.

   Si aucune valeur n'est indiquée, le fournisseur d'authentification LDAP se lie en tant qu'anonyme.
8. Si vous n'utilisez pas le mappage des identités externes, faites appel aux données d'identification de liaison pour effectuer des recherches sur le serveur d'annuaire LDAP. Pour cela, procédez comme suit :
   - Vérifiez que l'option **Voulez-vous utiliser une identité externe ?** est définie sur **Faux**.
   - Définissez l'option **Voulez-vous utiliser des données d'identification de liaison pour la recherche ?** sur **Vrai**.
   - Indiquez l'ID utilisateur et le mot de passe correspondant à l'option **Nom distinctif et mot de passe de l'utilisateur de liaison**.
9. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
10. Testez la connexion à un nouvel espace-noms. Dans la fenêtre **Explorateur**, sous **Authentification**, cliquez avec le bouton droit de la souris sur la nouvelle ressource d'authentification, puis sélectionnez **Tester**.

    Vous êtes invité à saisir les données d'identification d'un utilisateur dans l'espace-noms pour réaliser le test.

    Selon la manière dont votre espace-noms est configuré, vous pouvez entrer l'ID et le mot de passe d'un utilisateur valide dans l'espace-noms, ou le nom distinctif et le mot de passe de l'utilisateur de liaison.

### Résultats

IBM Cognos charge, initialise et configure les bibliothèques du fournisseur de l'espace-noms concerné.

## Configuration d'un espace-noms LDAP pour IBM Directory Server

Si vous configurez un nouvel espace-noms LDAP pour l'utiliser avec IBM Directory Server, les valeurs par défaut sont générées automatiquement.

### Procédure

1. A chaque emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Sécurité,** cliquez avec le bouton droit sur **Authentification**, puis cliquez sur **Nouvelle ressource** > **Espace-noms**.
3. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
4. Dans la liste **Type**, cliquez sur **LDAP - Valeurs par défaut pour IBM Tivoli**, puis sur le bouton **OK**.

   La nouvelle ressource d'espace-noms pour l'authentification s'affiche dans la fenêtre **Explorateur**, sous le composant **Authentification**. Vérifiez-la et modifiez-la si nécessaire.

5. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.

   **Conseil :** La propriété Identificateur d'espace-noms ne doit pas contenir de signe deux-points (:).
6. Définissez les valeurs de toutes les autres propriétés requises pour vous assurer qu'IBM Cognos pourra localiser et utiliser l'espace-noms d'authentification existant.
   - Pour **Fichier de correspondance d'utilisateur**, indiquez `(cn=${userID})`
   - Pour **Nom distinctif et mot de passe de l'utilisateur de liaison**, indiquez *`cn=root`*.
7. Si, lors de recherches, le fournisseur d'authentification LDAP doit établir une liaison avec le serveur d'annuaire à l'aide d'un paramètre **Nom distinctif et mot de passe de l'utilisateur de liaison** spécifique, indiquez ces valeurs.

   Si aucune valeur n'est indiquée, le fournisseur d'authentification LDAP se lie en tant qu'anonyme.
8. Si vous n'utilisez pas le mappage des identités externes, faites appel aux données d'identification de liaison pour effectuer des recherches sur le serveur d'annuaire LDAP. Pour cela, procédez comme suit :
   - Vérifiez que l'option **Voulez-vous utiliser une identité externe ?** est définie sur **Faux**.
   - Définissez l'option **Voulez-vous utiliser des données d'identification de liaison pour la recherche ?** sur **Vrai**.
   - Indiquez l'ID utilisateur et le mot de passe correspondant à l'option **Nom distinctif et mot de passe de l'utilisateur de liaison**.
9. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Configuration d'un espace-noms LDAP pour Novell Directory Server

Si vous configurez un nouvel espace-noms LDAP pour l'utiliser avec Novell Directory Server, vous devez modifier les paramètres nécessaires ainsi que les valeurs de toutes les propriétés des objets Novell Directory.

### Procédure

1. A chaque emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Sécurité,** cliquez avec le bouton droit sur **Authentification**, puis cliquez sur **Nouvelle ressource** > **Espace-noms**.
3. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
4. Dans la liste **Type (Groupe)**, cliquez sur **LDAP**, puis dans la liste **Type**, sélectionnez **LDAP - Valeurs générales par défaut**, puis cliquez sur **OK**.

   La nouvelle ressource d'espace-noms pour l'authentification s'affiche dans la fenêtre **Explorateur**, sous le composant **Authentification**.
5. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.

   **Conseil :** La propriété Identificateur d'espace-noms ne doit pas contenir de signe deux-points (:).
6. Définissez les valeurs de toutes les autres propriétés requises pour vous assurer qu'IBM Cognos pourra localiser et utiliser l'espace-noms d'authentification existant.

- Pour **Fichier de correspondance d'utilisateur**, indiquez `(cn=${userID})`
- Pour **Nom distinctif et mot de passe de l'utilisateur de liaison**, définissez le nom distinctif de base d'un utilisateur d'administration, par exemple `cn=Admin,o=COGNOS`

7. Si, lors de recherches, le fournisseur d'authentification LDAP doit établir une liaison avec le serveur d'annuaire à l'aide d'un paramètre **Nom distinctif et mot de passe de l'utilisateur de liaison** spécifique, indiquez ces valeurs.

   Si aucune valeur n'est indiquée, le fournisseur d'authentification LDAP se lie en tant qu'anonyme.
8. Si vous n'utilisez pas le mappage des identités externes, faites appel aux données d'identification de liaison pour effectuer des recherches sur le serveur d'annuaire LDAP. Pour cela, procédez comme suit :
   - Vérifiez que l'option **Voulez-vous utiliser une identité externe ?** est définie sur **Faux**.
   - Définissez l'option **Voulez-vous utiliser des données d'identification de liaison pour la recherche ?** sur **Vrai**.
   - Indiquez l'ID utilisateur et le mot de passe correspondant à l'option **Nom distinctif et mot de passe de l'utilisateur de liaison**.
9. Pour configurer les propriétés de mappage avancé LDAP à employer avec les objets Novell Directory Server, utilisez les valeurs indiquées dans le tableau ci-dessous.

*Tableau 43. Valeurs de mappage avancé LDAP pour une utilisation avec des objets Novell Directory Server*

| Mappages | Propriété LDAP | Valeur LDAP |
|---|---|---|
| Dossier | Classe d'objets | organizationalunit,organization,container |
| | Description | description |
| | Nom | ou,o,cn |
| Groupe | Classe d'objets | groupofnames |
| | Description | description |
| | Membre | membre |
| | Nom | cn |
| Compte | Classe d'objets | inetOrgPerson |
| | Téléphone professionnel | telephonenumber |
| | Paramètres régionaux de contenu | Language |
| | Description | description |
| | Courrier électronique | mail |
| | Télécopieur/téléphone | facsimiletelephonenumber |
| | Prénom | givenname |
| | Téléphone privé | homephone |
| | Téléphone mobile | mobile |
| | Nom | cn |
| | Récepteur d'appels | pager |
| | Mot de passe | (ne pas saisir de valeur) |
| | Adresse postale | postaladdress |
| | Langue du produit | Language |

*Tableau 43. Valeurs de mappage avancé LDAP pour une utilisation avec des objets Novell Directory Server (suite)*

| Mappages | Propriété LDAP | Valeur LDAP |
|---|---|---|
| | Nom de famille | sn |
| | Nom d'utilisateur | uid |

Ces propriétés de mappage représentent des modifications basées sur une installation par défaut de Novell Directory Server. Si vous modifiez le schéma, vous devrez peut-être faire d'autres modifications des mappages.

Les attributs LDAP qui sont mis en correspondance avec la propriété **Nom** dans **Mappage des dossiers**, **Mappage de groupes** et **Mappage de comptes** doivent être accessibles à tous les utilisateurs authentifiés. En outre, la propriété **Nom** doit obligatoirement être définie.

Pour pouvoir se connecter au portail, les utilisateurs doivent disposer de droits leur permettant de lire les attributs `ou` et `o`.

10. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Configuration d'un espace-noms LDAP pour Oracle Directory Server

Si vous configurez un nouvel espace-noms LDAP pour l'utiliser avec Oracle Directory Server, les valeurs par défaut sont générées automatiquement.

### Procédure

1. A chaque emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, sous **Sécurité,** cliquez avec le bouton droit sur **Authentification**, puis cliquez sur **Nouvelle ressource** > **Espace-noms**.
3. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
4. Dans la liste **Type**, cliquez sur **LDAP - Valeurs par défaut pour Oracle Directory Server**, puis sur le bouton **OK**.

   La nouvelle ressource d'espace-noms pour l'authentification s'affiche dans la fenêtre **Explorateur**, sous le composant **Authentification**. Vérifiez-la et modifiez-la si nécessaire.
5. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.

   **Conseil :** La propriété Identificateur d'espace-noms ne doit pas contenir de signe deux-points (:).
6. Définissez les valeurs de toutes les autres propriétés requises pour vous assurer qu'IBM Cognos pourra localiser et utiliser l'espace-noms d'authentification existant.

   Voici des exemples de paramètres :

   - Pour **Fichier de correspondance d'utilisateur**, indiquez `(uid=${userID})`
   - Si vous utilisez un code d'accès unique, pour **Voulez-vous utiliser une identité externe ?**, définissez la valeur sur **Vrai**.
   - Si vous utilisez un code d'accès unique, pour **Mappage des identités externes**, définissez un attribut, tel que l'identifiant de domaine utilisateur NT ou l'ID utilisateur :

     ```
     (ntuserdomainid=$environment("REMOTE_USER")})
     (uid=${environment("REMOTE_USER")})
     ```

**Important :** Veillez à utiliser uniquement la variable REMOTE_USER. L'utilisation d'une autre variable peut entraîner une vulnérabilité en matière de sécurité.

- Pour **Identificateur unique**, indiquez `nsuniqueid`

7. Si, lors de recherches, le fournisseur d'authentification LDAP doit établir une liaison avec le serveur d'annuaire à l'aide d'un paramètre **Nom distinctif et mot de passe de l'utilisateur de liaison** spécifique, indiquez ces valeurs.

   Si aucune valeur n'est indiquée, le fournisseur d'authentification LDAP se lie en tant qu'anonyme.
8. Si vous n'utilisez pas le mappage des identités externes, faites appel aux données d'identification de liaison pour effectuer des recherches sur le serveur d'annuaire LDAP. Pour cela, procédez comme suit :
   - Vérifiez que l'option **Voulez-vous utiliser une identité externe ?** est définie sur **Faux**.
   - Définissez l'option **Voulez-vous utiliser des données d'identification de liaison pour la recherche ?** sur **Vrai**.
   - Indiquez l'ID utilisateur et le mot de passe correspondant à l'option **Nom distinctif et mot de passe de l'utilisateur de liaison**.
9. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Mise à disposition des propriétés d'utilisateur personnalisées LDAP aux composants IBM Cognos

Vous pouvez utiliser des attributs d'utilisateur arbitraires de votre fournisseur d'authentification LDAP dans les composants d'IBM Cognos. Pour procéder à cette configuration, vous devez ajouter ces attributs en tant que propriétés personnalisées pour l'espace-noms LDAP. Les propriétés personnalisées sont disponibles en tant que paramètres de session par le biais de Framework Manager.

Vous pouvez également utiliser les propriétés personnalisées à l'intérieur des blocs de commande pour configurer les sessions et les connexions Oracle. Vous pouvez utiliser les blocs de commande avec les connexions Oracle légères et les bases de données privées virtuelles. Pour plus d'informations, voir le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Pour en savoir davantage sur les paramètres de session, voir le document *Framework Manager User Guide*.

### Procédure

1. Ouvrez Cognos Configuration dans chaque emplacement où Content Manager est installé.
2. Dans la fenêtre **Explorateur**, sous **Sécurité** > **Authentification**, sélectionnez l'espace-noms LDAP.
3. Dans la fenêtre **Propriétés**, cliquez sur la colonne **Valeur** correspondant à **Propriétés personnalisées**, puis sur l'icône Editer.
4. Dans la fenêtre **Valeur - Propriétés personnalisées**, cliquez sur **Ajouter**.
5. Cliquez sur la colonne **Nom** et saisissez le nom que les composants d'IBM Cognos doivent utiliser pour le paramètre de session.
6. Cliquez sur la colonne **Valeur** et saisissez le nom du paramètre de compte dans votre fournisseur d'authentification LDAP.
7. Répétez les deux étapes précédentes pour chaque paramètre personnalisé.
8. Cliquez sur le bouton **OK**.

9. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

# Activation de la communication sécurisée pour le serveur LDAP

Le protocole LDAP sécurisé (LDAPS) chiffre les communications entre le composant Access Manager de Content Manager et le serveur d'annuaire. LDAPS empêche l'envoi des informations confidentielles du serveur d'annuaire et des données d'identification LDAP sous forme de texte en clair.

Pour activer LDAPS, installez un certificat de serveur signé par une autorité de certification sur le serveur d'annuaire. Créez ensuite une base de données de certificats contenant les certificats. Configurez enfin le serveur d'annuaire et l'espace-noms LDAP IBM Cognos pour LDAPS.

Le certificat du serveur doit être une copie d'un des éléments suivants :

- Le certificat racine de confiance et tous les autres certificats composant la chaîne d'approbation du certificat du serveur d'annuaire.

  Le certificat racine de confiance est celui de l'autorité de certification racine qui a signé le certificat du serveur d'annuaire.
- Le certificat du serveur d'annuaire uniquement.

Ces certificats doivent être au format Base64 encodé en ASCII (PEM). Hormis le certificat racine approuvé, les certificats ne doivent pas être auto-signés.

## Avant de commencer

IBM Cognos fonctionne avec les versions `cert8.db` et `cert7.db` de la base de données de certificats client. Vous devez utiliser l'outil `certutil` de NSS (Netscape Security Services) pour créer les bases de données de certificats. IBM Cognos n'accepte pas les autres versions des fichiers `cert8.db`, y compris les fichiers de l'outil `certutil` fourni avec Microsoft Active Directory. IBM Cognos inclut désormais l'outil `certutil` sur les plateformes où NSS (Netscape Security Services) n'est plus requis par le système. Pour les plateformes où NSS est requis, veuillez utiliser cette version de l'outil `certutil`.

## Procédure

1. Créez un répertoire pour la base de données de certificats.
2. Créez la base de données de certificats en saisissant la commande suivante :

   `certutil -N -d` *`répertoire_certificats`*

   Où *`répertoire_certificats`* est le répertoire créé à l'étape 1.

   Cette commande crée un fichier `cert8.db` et un fichier `key3.db` dans le nouveau répertoire.
3. Ajoutez le certificat de l'autorité de certification ou le certificat du serveur d'annuaire à la base de données de certificats en saisissant la commande correspondant au type de certificat :
   - Pour un certificat d'autorité de certification :

     `certutil -A -n` *`nom_certificat`* `-d` *`répertoire_certificats`* `-i CA.cert -t C,C,C`
   - Pour un certificat de serveur d'annuaire :

     `certutil -A -n` *`nom_certificat`* `-d` *`répertoire_certificats`* `-i` *`certificat_serveur`*`.cert -t P`

Où *nom_certificat* est un alias que vous affectez, par exemple le nom d'hôte ou le nom de l'autorité de certification, et *certificat_serveur* est le préfixe du fichier de certificat du serveur d'annuaire.

4. Copiez le répertoire de la base de données de certificats dans le répertoire *emplacement_installation*/configuration à chaque emplacement où Content Manager est installé.
5. Configurez le serveur d'annuaire pour LDAPS et redémarrez-le.

   Pour en savoir davantage, reportez-vous à la documentation du serveur d'annuaire.
6. Démarrez IBM Cognos Configuration dans chaque emplacement de Content Manager où vous avez configuré l'espace-noms LDAP pour le serveur d'annuaire.
7. Dans la fenêtre **Explorateur**, sous **Sécurité** > **Authentification**, cliquez sur l'espace-noms LDAP.
8. Dans la fenêtre **Propriétés**, pour la propriété **Hôte et port**, remplacez le port en cours par le port LDAPS sécurisé.

   Pour la propriété **Base de données de certificats SSL**, spécifiez le chemin d'accès au fichier cert7.db.
9. Dans la fenêtre **Explorateur**, cliquez avec le bouton droit de la souris sur l'espace-noms LDAP, puis sélectionnez **Tester**.

   Si le test échoue, réexaminez les propriétés pour vérifier que le certificat approprié est utilisé.
10. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
11. Dans le menu **Actions**, cliquez sur l'option **Redémarrer**.
12. Répétez les étapes 6 à 11 pour tout autre emplacement où Content Manager est installé.

## Activation du code d'accès unique entre LDAP et les composants IBM Cognos

Pour bénéficier du code d'accès unique aux composants d'IBM Cognos, vous devez configurer la propriété Mappage des identités externes.

Le mappage des identités externes peut faire référence à une variable d'environnement CGI ou à un en-tête HTTP variable. Dans le cas d'une entrée de passerelle ou de répartiteur de serveur d'applications pointant vers les composants d'IBM Cognos, le Mappage des identités externes peut faire référence à la variable de session userPrincipalName. La valeur résolue de la propriété de mappage des identités externes en phase d'exécution doit être un nom de domaine d'utilisateur valide.

Si un espace-noms LDAP est configuré pour utiliser la propriété Mappage des identités externes pour l'authentification, le fournisseur LDAP se lie au serveur d'annuaire à l'aide de la propriété Nom distinctif et mot de passe de l'utilisateur de liaison, ou de façon anonyme si aucune valeur n'est indiquée. Tous les utilisateurs qui se connectent à IBM Cognos à l'aide d'un mappage des identités externes voient les mêmes utilisateurs, groupes et dossiers que l'utilisateur de liaison.

Si vous voulez que les composants IBM Cognos fonctionnent avec les applications qui utilisent Java ou la sécurité du serveur d'applications, vous pouvez configurer la propriété Mappage des identités externes pour obtenir l'ID utilisateur à partir du

principal de l'utilisateur Java. Ajoutez le jeton `${environment("USER_PRINCIPAL")}` à la valeur de la propriété. Pour en savoir davantage, reportez-vous à l'aide en ligne d'IBM Cognos Configuration.

Vous pouvez appliquer une édition limitée de l'expression à la propriété Mappage des identités externes à l'aide de l'opération de remplacement.

## Opération de remplacement

L'opération de remplacement renvoie une copie de la chaîne avec toutes les occurrences de la sous-chaîne précédente remplacée par la nouvelle sous-chaîne.

Les règles suivantes s'appliquent :

- Le caractère \ est utilisé comme caractère d'échappement dans les paramètres de la fonction. Les caractères \ et " doivent être précédés d'un caractère d'échappement.
- Les appels de fonction imbriquée ne sont pas pris en charge.
- Les caractères spéciaux ne sont pas pris en charge.

### Syntaxe

```
${replace(str , old , new)}
```

### Paramètres de l'opération Replace

*Tableau 44. Paramètres et description de l'opération Replace*

| Paramètre | Description |
|---|---|
| `chaîne` | Chaîne à rechercher. |
| `ancienne` | Sous-chaîne à remplacer par la nouvelle sous-chaîne. |
| `nouvelle` | Sous-chaîne remplaçant l'ancienne sous-chaîne. |

### Exemples

```
${replace(${environment("REMOTE_USER")},"NAMERICA\\",)}
```

```
${replace(${environment("REMOTE_USER")},"NAMERICA\\","")}
```

# Fournisseur d'authentification CA SiteMinder

Vous pouvez configurer IBM Cognos Analytics pour utiliser un espace-noms CA SiteMinder en tant que source d'authentification.

Le fournisseur d'authentification utilise le kit de développement de logiciels de CA SiteMinder pour implémenter un agent personnalisé. Le déploiement de cet agent personnalisé requiert que vous définissiez les propriétés de l'agent dans la console d'administration du serveur de règles CA SiteMinder pour la prise en charge des agents 4.x.

### Configuration requise pour CA SiteMinder

Configurez les éléments suivants dans le serveur de règles CA SiteMinder :

- Cognos Analytics doit utiliser des caractères spéciaux et des séquences de caractères particulières dans l'URL de Cognos Analytics Server 11.0.x. Pour éviter les erreurs, supprimez les séquences de caractères suivantes de la liste dans le paramètre **BadURLChars** de l'objet de configuration d'agent dans le serveur de règles CA SiteMinder :
  - tilde (~)
  - point (.)
  - point et barre oblique (./)
  - barre oblique et point (/.)
  - signe plus grand que (>)

  **Conseil :** Les clients qui incorporent des URL dans leurs rapports doivent vérifier les caractères figurant dans les paramètres d'URL et s'assurer que CA Siteminder ne traite pas ces caractères comme **BadURLChars** ou **BadCSSChars**. Pour plus d'informations, reportez-vous à la documentation sur CA SiteMinder.
- Cognos Analytics nécessite 4 instructions pour fonctionner. Activez les valeurs suivantes dans le serveur de règles CA SiteMinder : GET, POST, PUT, et DELETE.

## CA SiteMinder configuré pour plusieurs annuaires d'utilisateurs

Si votre environnement CA SiteMinder est configuré pour plusieurs annuaires d'utilisateurs, vous devez utiliser le type d'espace-noms **SiteMinder** dans IBM Cognos Configuration.

Une fois que vous avez configuré l'espace-noms SiteMinder dans IBM Cognos Configuration, vous devez également ajouter un espace-noms LDAP ou Active Directory Server correspondant à IBM Cognos Configuration pour chaque annuaire d'utilisateurs défini dans CA SiteMinder.

Lorsque vous configurez un espace-noms LDAP correspondant, vérifiez que la propriété **Mappage des identités externes** est activée et que vous incluez bien le jeton **REMOTE_USER** dans la valeur de la propriété. Cela ne signifie pas que vous devez configurer CA SiteMinder pour définir **REMOTE_USER**.

Lorsque vous configurez un espace-noms Active Directory correspondant, vérifiez que la propriété **singleSignonOption** est définie sur **IdentityMapping**.

L'espace-noms **SiteMinder** transmet les informations utilisateur en interne à l'espace-noms LDAP correspondant à l'aide de la variable d'environnement **REMOTE_USER** lorsqu'il reçoit une identification utilisateur correcte de l'environnement CA SiteMinder.

Pour en savoir davantage, reportez-vous à la section «Activation du code d'accès unique entre Active Directory Server et les composants d'IBM Cognos pour utiliser REMOTE_USER», à la page 254.

**Important :** Assurez-vous de n'utiliser que la variable **REMOTE_USER**. L'utilisation d'une autre variable peut entraîner une vulnérabilité en matière de sécurité.

### CA SiteMinder configuré avec un seul annuaire d'utilisateurs

Si votre environnement CA SiteMinder est configuré avec un seul annuaire d'utilisateurs, vous n'avez pas besoin d'utiliser le type d'espace-noms **SiteMinder** dans IBM Cognos Configuration.

Dans ce cas, vous pouvez utiliser l'annuaire d'utilisateurs en tant que source d'authentification en configurant l'espace-noms approprié ou configurer **SiteMinder** avec un annuaire d'utilisateurs. Par exemple, si l'annuaire d'utilisateurs CA SiteMinder est LDAP, vous pouvez configurer les composants d'IBM Cognos avec un espace-noms LDAP ou un espace-noms **SiteMinder**, en faisant référence à un annuaire d'utilisateurs constituant un espace-noms LDAP.

Si l'annuaire d'utilisateurs CA SiteMinder est Active Directory, vous pouvez utiliser un espace-noms Active Directory ou un espace-noms LDAP configuré pour une utilisation avec Active Directory.

Si vous souhaitez utiliser l'annuaire d'utilisateurs comme source d'authentification directement au lieu de configurer un espace-noms **SiteMinder**, vous pouvez configurer l'espace-noms LDAP ou Active Directory approprié. Dans ce cas, vérifiez les propriétés d'objet de configuration d'agent sur le serveur de règles CA SiteMinder. Vérifiez que **SetRemoteUser** est activé.

Lorsque vous configurez l'espace-noms Active Directory, vérifiez que la propriété **singleSignonOption** est définie sur **IdentityMapping**.

Lorsque vous configurez un espace-noms LDAP correspondant, vérifiez que la propriété **Mappage des identités externes** est activée et que vous incluez bien le jeton **REMOTE_USER** dans la valeur de la propriété.

Pour en savoir davantage, reportez-vous à la section «Activation du code d'accès unique entre Active Directory Server et les composants d'IBM Cognos pour utiliser REMOTE_USER», à la page 254.

**Important :** Assurez-vous de n'utiliser que la variable **REMOTE_USER**. L'utilisation d'une autre variable peut entraîner une vulnérabilité en matière de sécurité.

## Configuration de l'espace-noms SiteMinder

Si vous avez configuré CA SiteMinder pour plusieurs annuaires d'utilisateurs, vous devez utiliser le type d'espace-noms **SiteMinder** dans IBM Cognos Configuration. Après avoir ajouté l'espace-noms SiteMinder, vous devez également ajouter un espace-noms LDAP correspondant pour chaque annuaire d'utilisateurs de votre environnement CA SiteMinder.

Vous pouvez également utiliser le type d'espace-noms **SiteMinder** si des utilisateurs sont stockés sur un serveur LDAP ou un serveur Active Directory.

Vous pouvez masquer des espaces-noms de la vue des utilisateurs durant la connexion. Vous pouvez disposer d'espaces-noms de codes d'accès sécurisés sans qu'ils soient affichés dans la liste de sélection des espaces-noms présentée lorsque les utilisateurs se connectent. Supposons, par exemple, que vous souhaitiez généraliser le code d'accès unique à l'ensemble des systèmes tout en permettant aux utilisateurs de s'authentifier directement sur IBM Cognos sans être invités à choisir un espace-noms.

## Avant de commencer

Pour utiliser l'espace-noms **SiteMinder**, vous devez obtenir les fichiers de bibliothèque CA SiteMinder requis indiqués dans le tableau suivant et les ajouter dans le chemin d'accès de bibliothèque approprié pour votre système d'exploitation.

*Tableau 45. Fichiers de bibliothèque CA SiteMinder*

| Système d'exploitation | Fichier de bibliothèque CA SiteMinder |
|---|---|
| Solaris et AIX | `libsmagentapi.so` |
| Microsoft Windows 64 bits | `smagentapi.dll`<br><br>`smerrlog.dll` |

## Procédure

1. Sur l'ordinateur sur lequel Content Manager est installé, ajoutez le répertoire qui contient le fichier de bibliothèque CA SiteMinder dans la variable d'environnement de chemin d'accès de bibliothèque appropriée.
   - Pour les systèmes d'exploitation Solaris, **LD_LIBRARY_PATH**
   - Pour les systèmes d'exploitation AIX, **LIBPATH**
   - Pour les systèmes d'exploitation Microsoft Windows, **PATH**
2. Ouvrez IBM Cognos Configuration.
3. Dans la fenêtre **Explorateur**, sous **Sécurité,** cliquez avec le bouton droit sur **Authentification**, puis cliquez sur **Nouvelle ressource** > **Espace-noms**.
4. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
5. Dans la liste **Type**, cliquez sur **SiteMinder**, puis sur **OK**.
6. Sélectionnez l'espace-noms que vous avez ajouté.
7. Dans la propriété **ID d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.

   **Conseil :** N'utilisez pas le signe deux-points dans l'identificateur.
8. Indiquez des valeurs pour les autres propriétés requises.

   **Conseil :** Si vous ne voulez pas que les utilisateurs voient le nom de l'espace-noms lorsqu'ils se connectent, définissez la propriété **Sélectionnable pour authentification** sur **Faux**.
9. Dans la fenêtre **Explorateur**, sous **Sécurité** > **Authentification**, cliquez avec le bouton droit sur l'espace-noms que vous avez ajouté et cliquez sur **Nouvelle ressource** > **Serveur de stratégies SiteMinder**.
10. Dans la zone **Nom**, saisissez un nom pour le serveur de règles, puis cliquez sur le bouton **OK**.
11. Dans la fenêtre **Propriétés**, définissez la propriété **Hôte** et les autres valeurs de propriétés que vous souhaitez modifier.
12. Dans la fenêtre **Explorateur**, cliquez avec le bouton droit sur le nouveau serveur de stratégies SiteMinder, puis cliquez sur **Nouvelle ressource** > **Annuaire d'utilisateurs**.
13. Dans la zone **Nom**, saisissez un nom pour l'annuaire d'utilisateurs, puis cliquez sur **OK**.

    **Important :** Le nom doit correspondre au nom figurant dans l'annuaire d'utilisateurs qui se trouve sur le serveur de règles.

14. Dans la fenêtre **Propriétés**, indiquez une valeur pour la propriété **Référence d'identification de l'espace-noms**.
15. Configurez un annuaire d'utilisateurs pour chaque annuaire d'utilisateurs dans le serveur de règles SiteMinder.
16. Cliquez sur **Fichier** > **Enregistrer**.
17. Testez la connexion à un nouvel espace-noms. Dans la fenêtre **Explorateur**, sous **Authentification**, cliquez avec le bouton droit de la souris sur la nouvelle ressource d'authentification, puis sélectionnez **Tester**.

    Vous êtes invité à saisir les données d'identification d'un utilisateur dans l'espace-noms pour réaliser le test.

    Selon la manière dont votre espace-noms est configuré, vous pouvez entrer l'ID et le mot de passe d'un utilisateur valide dans l'espace-noms, ou le nom distinctif et le mot de passe de l'utilisateur de liaison.
18. Configurez un espace-noms LDAP ou Active Directory correspondant pour chaque annuaire d'utilisateurs.

    Veillez à utiliser la même valeur pour la propriété **ID espace-noms** et pour la propriété **ID espace-noms** de l'espace-noms SiteMinder.

# Configuration d'IBM Cognos pour utiliser SAP

Pour utiliser un serveur SAP en tant que fournisseur d'authentification, vous devez employer une version prise en charge de SAP BW.

Dans SAP BW, vous pouvez affecter des utilisateurs à des groupes d'utilisateurs, des rôles ou les deux. Le fournisseur d'authentification SAP n'utilise que des rôles.

Les droits d'autorisation requis par l'utilisateur SAP dépendent du statut de la personne qui emploie les composants IBM Cognos : utilisateur ou administrateur.

## Paramètres d'autorisation SAP pour les utilisateurs d'IBM Cognos

Les objets d'autorisation contenus dans le tableau suivant sont requis pour tous les utilisateurs d'IBM Cognos.

*Tableau 46. Paramètres d'autorisation SAP pour les utilisateurs d'IBM Cognos*

| Objet d'autorisation | Zone | Valeur |
|---|---|---|
| S_RFC<br><br>Contrôle d'autorisation pour l'accès RFC | Activité | |
| | Nom de RFC à protéger | RFC1 RS_UNIFICATION, SDTX, SH3A, SU_USER, SYST, SUSO |
| | Type de RFC à protéger | FUGR |
| S_USER_GRP<br><br>Maintenance principale des utilisateurs : Groupe d'utilisateurs | Activité | 03 |
| | Nom du groupe d'utilisateurs | * |

Certaines valeurs affichées, telles que *, sont les valeurs par défaut que vous pouvez modifier pour votre environnement.

### Paramètres d'autorisation SAP pour les administrateurs d'IBM Cognos

Si des utilisateurs effectuent des tâches d'administration et recherchent des utilisateurs ou des rôles, les valeurs contenues dans le tableau suivant doivent être ajoutées à l'objet d'autorisation S_RFC, en plus des valeurs pour les utilisateurs d'IBM Cognos.

*Tableau 47. Paramètres d'autorisation SAP pour les administrateurs d'IBM Cognos*

| Objet d'autorisation | Zone | Valeur |
|---|---|---|
| S_RFC<br><br>Contrôle d'autorisation pour l'accès RFC | Activité | 16 |
| | RFC_NAME | PRGN_J2EE, SHSS, SOA3 |
| | Type d'objet RFC à protéger | FUGR |

Certaines valeurs affichées, par exemple *, sont les valeurs par défaut que vous pouvez modifier pour votre environnement.

### Connectivité entre SAP BW et IBM Cognos sur UNIX

Pour configurer la connectivité entre SAP BW et les composants IBM Cognos sur un système d'exploitation UNIX, veillez à installer le fichier de bibliothèque partagée SAP (fourni par SAP) et à l'ajouter à la variable d'environnement de chemin d'accès aux bibliothèques, comme suit :

- Solaris

  LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<librfccm.so_directory>
- AIX

  LIBPATH=$LIBPATH:<librfc.a_directory>

## Configuration d'un espace-noms SAP

Vous pouvez configurer les composants d'IBM Cognos de façon à ce qu'ils utilisent un serveur SAP en tant que fournisseur d'authentification.

### Avant de commencer

Si vous avez installé votre produit IBM Cognos sur un serveur 64 bits, vous devez également copier manuellement les fichiers de bibliothèque SAP RFC vers le répertoire d'installation d'IBM Cognos.

### Procédure

1. Si l'exécution a lieu sur un serveur 64 bits, procédez comme suit :
   - Accédez au répertoire d'installation SAP sur le serveur 64 bits.
   - Copiez tous les fichiers de bibliothèque SAP RFC 64 bits dans *emplacement_installation*\bin64.
   - Copiez tous les fichiers de bibliothèque SAP RFC 32 bits vers *emplacement_installation*\bin.

2. Si vous exécutez un serveur 32 bits, copiez tous les fichiers de bibliothèque SAP 32 bits depuis le répertoire d'installation de SAP vers le répertoire *emplacement_installation*\bin64.
3. A l'emplacement où Content Manager est installé, ouvrez IBM Cognos Configuration.
4. Dans la fenêtre **Explorateur**, sous **Sécurité**, cliquez avec le bouton droit de la souris sur **Authentification**, puis sur **Nouvelle ressource** > **Espace-noms**.
5. Dans la zone **Nom**, saisissez le nom de votre espace-noms d'authentification.
6. Dans la liste **Type**, cliquez sur **SAP**, puis sur le bouton **OK**.

   La nouvelle ressource de fournisseur d'authentification s'affiche dans la fenêtre **Explorer** sous le composant Authentification.
7. Dans la fenêtre **Propriétés**, pour la propriété **Identificateur d'espace-noms**, indiquez un identificateur unique pour l'espace-noms.

   **Important :** La propriété Identificateur d'espace-noms ne doit pas contenir de signe deux-points (:).
8. Définissez les valeurs de toutes les propriétés requises pour vous assurer que les composants d'IBM Cognos pourront localiser et utiliser le fournisseur d'authentification existant.

   En fonction de votre environnement, pour la propriété **Hôte**, vous devrez peut-être ajouter la chaîne du routeur SAP au nom d'hôte SAP.
9. Si le système SAP code le contenu des paramètres de cookie, activez la fonction de décodage des permis :
   - Dans la fenêtre **Propriétés**, pour l'option **Propriétés avancées**, cliquez sur Valeur, puis sur l'icône Editer.
   - Cliquez sur **Ajouter**.
   - Entrez le nom `URLDecodeTickets` et la valeur `true`
   - Cliquez sur le bouton **OK**.

   Tous les permis de connexion SAP seront décodés par l'espace-noms SAP avant l'établissement de la connexion.
10. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
11. Testez la connexion à un nouvel espace-noms. Dans la fenêtre **Explorateur**, sous **Authentification**, cliquez avec le bouton droit de la souris sur la nouvelle ressource d'authentification, puis sélectionnez **Tester**.

    Vous êtes invité à saisir les données d'identification d'un utilisateur dans l'espace-noms pour réaliser le test.

    Selon la manière dont votre espace-noms est configuré, vous pouvez entrer l'ID et le mot de passe d'un utilisateur valide dans l'espace-noms, ou le nom distinctif et le mot de passe de l'utilisateur de liaison.

## Activation du code d'accès unique entre SAP et IBM Cognos

Vous pouvez activer le code d'accès unique entre SAP Enterprise Portal et les composants d'IBM Cognos, et utiliser la fonction d'espace-noms externe des connexions de sources de données SAP BW.

Pour ce faire, veillez à définir les paramètres système suivants sur le serveur SAP BW :

- **login/accept_sso2_ticket = 1**
- **login/create_sso2_ticket = 1**
- **login/ticket_expiration_time = 200**

# Suppression d'un fournisseur d'authentification

Vous pouvez supprimer des espaces-noms que vous avez ajoutés ou annuler la configuration des espaces-noms que les composants d'IBM Cognos ont détectés, si ceux-ci ne sont plus requis.

Vous ne devez pas supprimer l'espace-noms de Cognos. Il contient des données d'authentification qui appartiennent à tous les utilisateurs et il est nécessaire pour l'enregistrement de la configuration.

Lorsque vous supprimez un espace-noms, vous ne pouvez plus vous y connecter. Les données de sécurité de l'espace-noms sont conservées dans Content Manager jusqu'à ce que vous les supprimiez définitivement du portail. Pour plus d'informations, voir le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

## Procédure

1. Ouvrez Cognos Configuration dans chaque emplacement où Content Manager est installé.
2. Dans la fenêtre **Explorateur**, dans la section **Sécurité** > **Authentification**, cliquez sur l'option **Supprimer**.
3. Cliquez sur **Oui** pour confirmer.

   L'espace-noms disparaît de la fenêtre **Explorateur** et vous ne pouvez plus vous connecter à celui-ci à cet emplacement.
4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.
5. Répétez les étapes 1 à 4 pour chaque emplacement sur lequel vous avez installé Content Manager.

   Vous devez désormais vous connecter au portail et supprimer les données de l'espace-noms de manière permanente. Pour plus d'informations, voir le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

## Résultats

Une fois l'espace-noms supprimé, il apparaît comme inactif sur le portail.

# Chapitre 9. Gestion des performances

Cette section inclut des rubriques relatives à l'utilisation d'IBM Cognos Analytics et d'autres outils et indicateurs pour la gestion des performances de votre environnement IBM Cognos Analytics.

## Indicateurs des performances du système

IBM Cognos Analytics BI fournit des indicateurs système permettant de contrôler l'état du système global et de chaque serveur, répartiteur et service. Vous pouvez également définir les seuils des scores d'indicateurs. Les indicateurs de performance du système incluent, par exemple, le nombre de sessions de votre système, la durée pendant laquelle un rapport est resté en file d'attente, la durée d'exécution d'un composant JVM (Java Virtual Machine) et le nombre de demandes et de processus du système.

Les indicateurs de performance du système résident dans l'environnement Java, mais peuvent être surveillés dans IBM Cognos Administration par l'intermédiaire du portail. Pour en savoir davantage sur la surveillance des indicateurs de performance, reportez-vous au manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Vous pouvez effectuer un instantané des indicateurs système en cours, ce qui vous permet de suivre les tendances au fil du temps ou de consulter les détails relatifs à l'état du système à un moment précis. Pour en savoir davantage, reportez-vous à la rubrique traitant du fichier de vidage des indicateurs dans le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Vous pouvez également surveiller les indicateurs du système par voie externe vers IBM Cognos Administration en utilisant la technologie JMX (Java Management Extensions), qui fournit des outils de gestion et de surveillance des applications et des réseaux orientés services.

### Surveillance des indicateurs système par voie externe

Vous pouvez surveiller les indicateurs système en dehors d'IBM Cognos Administration en utilisant la technologie normalisée JMX (Java Management Extensions). Vous devez tout d'abord configurer deux propriétés JMX dans IBM Cognos Configuration afin de permettre l'accès sécurisé aux indicateurs dans l'environnement Java. Ensuite, vous utilisez un ID utilisateur et un mot de passe pour vous connecter aux indicateurs via un outil de connexion JMX.

#### Avant de commencer

Vous devez installer le kit Oracle Java SE Development Kit ou le kit de développement de logiciels Java Software d'IBM pour pouvoir utiliser la fonction de contrôle externe.

#### Procédure

1. Démarrez IBM Cognos Configuration depuis l'emplacement d'installation de Content Manager.
2. Dans la fenêtre **Explorateur**, cliquez sur **Environnement**.

3. Dans la fenêtre **Propriétés**, sous **Paramètres du répartiteur**, cliquez sur **Port JMX externe**.
4. Dans la colonne **Valeur**, saisissez un numéro de port disponible.
5. Cliquez sur **Donnée d'identification JMX externe**.
6. Dans la colonne **Valeur**, cliquez sur l'icône Editer, saisissez un ID utilisateur et un mot de passe, puis cliquez sur **OK**.

   L'ID utilisateur et le mot de passe permettent d'assurer que seul un utilisateur autorisé peut se connecter aux indicateurs du système dans l'environnement Java, à l'aide du port spécifié à la section **Port JMX externe**.
7. Enregistrez les modifications et redémarrez le service.
8. Pour accéder aux données des indicateurs système, spécifiez les informations suivantes dans l'outil de connexion JMX :
   - adresse URL de connexion aux données d'indicateur du système

     Par exemple :

     `service:jmx:rmi://`*`Content_Manager_server`*`/jndi/rmi://`*`monitoring_server`*`:<`*`JMXport`*`>/proxyserver`

     où *JMXport* est la valeur saisie pour **Port JMX externe**, et *serveur_Content_Manager* et *serveur_surveillance* désignent des noms de machines. Ne spécifiez pas le nom localhost, même si vous vous connectez localement.
   - l'ID utilisateur et le mot de passe d'accès sécurisé à la connexion

     Utilisez les mêmes valeurs que celles que vous avez configurées pour la **Donnée d'identification JMX externe**.

## Activation des services requis uniquement

Si certains services IBM Cognos Analytics ne sont pas nécessaires dans votre environnement, vous pouvez les désactiver afin d'optimiser les performances des autres services.

Par exemple, pour dédier un ordinateur à l'exécution et à la diffusion de rapports, vous pouvez désactiver le service de présentation sur un ordinateur hébergeant les composants du groupe de serveurs d'applications. Lorsque vous désactivez le service de présentation, les performances des composants du groupe de serveurs d'applications sont améliorées.

**Remarque :**

- Le service de présentation doit rester activé sur au moins un ordinateur de votre environnement IBM Cognos Analytics.
- Si vous souhaitez utiliser Query Studio, vous devez activer le service de présentation.
- Si vous souhaitez utiliser Analysis Studio, vous devez activer le service de génération de rapports.
- Si certains composants d'IBM Cognos Analytics ne sont pas installés sur un ordinateur, il est préférable de désactiver les services qui leur sont associés. Sinon, les composants d'IBM Cognos Analytics risquent de subir des interruptions aléatoires.

## Services IBM Cognos

Une fois IBM Cognos Analytics installé et configuré, un répartiteur est disponible par défaut sur chaque ordinateur. Chaque répartiteur est associé à un ensemble de services, présentés dans le tableau ci-dessous.

*Tableau 48. Services IBM Cognos*

| Service | Fonction |
|---|---|
| Service d'agent | Exécute des agents. Si les conditions d'un agent sont remplies lorsque l'agent est exécuté, le service d'agent demande au service de surveillance d'exécuter les tâches. |
| Service d'annotation | Permet d'ajouter des commentaires à des rapports via IBM Cognos Workspace. Ces commentaires sont persistants d'une version à l'autre du rapport. |
| Service de génération de rapports par lots | Gère les demandes en arrière-plan concernant l'exécution de rapports et fournit des versions de sortie des rapports pour le compte du service de surveillance. |
| Service cache de Content Manager | Améliore les performances du système en général ainsi que l'évolutivité de Content Manager en plaçant en cache les résultats des requêtes fréquemment exécutées dans chaque répartiteur. |
| Service Content Manager | • Exécute des fonctions de manipulation d'objets dans le magasin de contenu (par exemple, ajout, requête, mise à jour, suppression, déplacement et copie).<br>• Met également en oeuvre des fonctions de gestion du magasin de contenu, telles que l'importation et l'exportation |
| Service de diffusion | Envoie des courriers électroniques à un serveur SMTP externe pour le compte d'autres services, tels que le service de génération de rapports, le service de travail ou le service d'agent. |
| Service de gestion des événements | Crée, programme et gère des objets d'événements représentant des rapports, des travaux, des agents, la maintenance du magasin de contenu et des importations et exportations de déploiement |
| Service Graphics | Produit des graphiques pour le compte du service de génération de rapports. Les graphiques peuvent être générés sous quatre formats différents : Raster, Vector, Microsoft Excel XML ou PDF. |
| Service de gestion des tâches utilisateur | Permet la création et la gestion de tâches utilisateur. Une tâche utilisateur telle que l'approbation d'un rapport peut être affectée à des individus ou à des groupes sur la base de circonstances ad hoc ou par le biais de n'importe quel autre service. |

*Tableau 48. Services IBM Cognos (suite)*

| Service | Fonction |
|---|---|
| Service de visualisation de recherche interactive | Utilisé par Cognos Workspace pour fournir des recommandations de visualisation. |
| Service de travail | Exécute des travaux en indiquant au service de surveillance qu'il doit exécuter les étapes en arrière-plan. Les tâches incluent notamment des rapports, d'autres travaux, des importations et des exportations. |
| Service de journalisation | Enregistre les messages de journal générés par le répartiteur et par d'autres services. Le service de journalisation peut être configuré pour enregistrer les informations de journalisation dans un fichier, une base de données, un serveur de journalisation distant, le journal des événements Windows ou un journal système UNIX. Les informations de journalisation peuvent ensuite être analysées par les clients ou par Cognos Software Services. Elles incluent :<br>• les événements liés à la sécurité,<br>• les informations sur les erreurs des applications et du système,<br>• les informations de diagnostic sélectionnées. |
| Service de métadonnées | Fournit l'accès aux informations de lignée depuis Cognos Viewer, Reporting, Query Studio et Analysis Studio. Les informations de lignée concernent par exemple les sources de données ou les expressions de calcul. |
| Service de migration | Gère la migration depuis IBM Cognos Series 7 vers IBM Cognos Analytics. |

*Tableau 48. Services IBM Cognos (suite)*

| Service | Fonction |
| --- | --- |
| Service Mobile | Gère les activités associées au client IBM Cognos Mobile :<br>• Il transforme les rapports et les analyses en vue de leur consommation sur les mobiles.<br>• Il compresse le contenu des rapports et des analyses en vue d'une diffusion rapide aux périphériques mobiles et de l'accès à partir de ceux-ci.<br>• Il envoie par commande push le contenu des rapports et des analyses vers les périphériques mobiles.<br>• Il facilite les demandes entrantes et sortantes liées aux rapports et aux analyses entre le périphérique mobile et l'environnement dans lequel s'effectue la recherche, la navigation et l'exécution des rapports.<br>• Il synchronise le magasin de contenu Mobile sur le serveur avec la base de données Mobile sur le périphérique mobile.<br>• Il convertit les messages SOAP (Simple Object Access Protocol) en messages transmissibles par des communications sans fil.<br>• Il communique avec le périphérique mobile. |
| Service de surveillance | • Gère le suivi et l'exécution des tâches qui sont programmées, soumises pour une exécution ultérieure ou exécutées en arrière-plan.<br>• Affecte un service cible pour le traitement d'une tâche planifiée. Par exemple, le service de surveillance peut demander au service de génération de rapports par lots d'exécuter un rapport, au service de travail d'exécuter un travail ou au service d'agent d'exécuter un agent.<br>• Crée des objets d'historique dans Content Manager et gère les opérations de reprise et de récupération liées à l'exécution des entrées. |
| Service PowerPlay | Gère les requêtes permettant d'exécuter les rapports PowerPlay. |
| Service de présentation | • Convertit les réponses XML génériques provenant d'un autre service dans un format de sortie, tel que HTML ou PDF.<br>• Fournit des fonctions d'affichage, de navigation et d'administration. |

*Tableau 48. Services IBM Cognos (suite)*

| Service | Fonction |
|---|---|
| Service de requête | Gère les requêtes dynamiques et renvoie le résultat au service de traitement par lots ou de rapport ayant émis la requête. |
| Service de métadonnées relationnelles | Utilisé par Framework Manager et CubeDesigner pour importer des métadonnées à partir de bases de données relationnelles. Il arrive également que Dynamic Query Analyzer l'utilise au moment de l'exécution. |
| Service de génération de données de rapports | Gère le transfert des données de rapport entre IBM Cognos Analytics et les applications qui les exploitent, notamment IBM Cognos BI for Microsoft Office et IBM Cognos Mobile. |
| Service de génération de rapports | Gère les demandes interactives concernant l'exécution de rapports et fournit des versions de sortie des rapports pour un utilisateur. |
| Service de référentiel | Gère les demandes d'extraction de la sortie de rapport archivée à partir d'un référentiel d'archive ou d'un conteneur d'objets. |

## Optimisation d'un magasin de contenu IBM Db2

Si vous utilisez une base de données Db2 pour le magasin de contenu, vous pouvez effectuer la procédure permettant d'accélérer le traitement des requêtes.

Par défaut, Db2 affecte des tables qui contiennent des LOBS (large objects) à un espace de table géré par une base de données. Ainsi, les LOBS ne sont pas gérés par les groupes de mémoire tampon Db2. Ce qui entraîne des requêtes E/S directes sur les LOBS, ce qui a une incidence sur les performances. En réattribuant les tables qui contiennent des LOBS à un espace de table géré par une base de données, vous réduisez le nombre de requêtes E/S directes.

Avant de modifier un magasin de contenu Db2, allouez un espace de journalisation suffisant pour restructurer la base de données.

Pour reconfigurer le magasin de contenu Db2, procédez comme suit :

- Exportez les données à partir des tables qui contiennent au moins un LOB (large object).
- Créez les tables dans un espace de table géré par le système.
- Importez les données dans les tables.

## Ajustement des ressources de mémoire pour le service IBM Cognos

Pour améliorer les performances dans un environnement réparti, vous pouvez modifier la quantité de ressources utilisée par le service IBM Cognos.

Le service IBM Cognos est configuré par défaut pour utiliser un minimum de ressources mémoires afin d'optimiser le temps de démarrage.

Les paramètres du service IBM Cognos s'appliquent uniquement au serveur d'applications utilisé par défaut par IBM Cognos Analytics. Si vous souhaitez configurer IBM Cognos Analytics pour qu'il s'exécute sur un autre serveur d'applications, n'utilisez pas IBM Cognos Configuration pour configurer les ressources. Configurez-les directement au sein de l'environnement du serveur d'applications en question.

Le service IBM Cognos n'est disponible que sur les ordinateurs sur lesquels vous avez installé Content Manager ou les composants du groupe de serveurs d'applications.

### Procédure

1. Démarrez IBM Cognos Configuration.
2. Dans la fenêtre **Explorateur**, développez **Environnement** > **Services IBM Cognos**, puis cliquez sur **IBM Cognos**.
3. Dans la fenêtre **Propriétés**, modifiez la valeur du paramètre **Quantité maximale de mémoire (en Mo)**.
   - Pour réduire le temps de démarrage, ainsi que l'utilisation de la mémoire et des ressources, utilisez la valeur par défaut 4096.
   - Cette valeur peut être ajustée en fonction des ressources système disponibles.
4. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

## Performances de Cognos Mobile

Vous pouvez utiliser différentes méthodes pour évaluer et contrôler les performances de votre environnement IBM Cognos Mobile.

### Estimation de la bande passante requise par IBM Cognos Mobile

IBM Cognos Mobile envoie les versions compressées des rapports du serveur vers le périphérique mobile.

Chaque version d'un rapport est envoyée une seule fois. Elle est alors stockée dans une mémoire cache du périphérique mobile. L'utilisateur nomade peut ensuite afficher le rapport autant de fois qu'il le désire sur le périphérique sans consommation supplémentaire de bande passante.

D'autres opérations, telles que la navigation dans le magasin de contenu ou la réponse à des invites dans les tableaux de bord Cognos Workspace, consomment également de la bande passante. Pour la même action, la bande passante consommée est proportionnelle à celle utilisée par le navigateur d'un ordinateur de bureau.

Pour estimer la consommation de bande passante, l'administrateur peut se servir de la formule suivante comme guide :

```
(nb. d'utilisateurs) x (taille moyenne d'un rapport) x (nb. de rapp. planifiés envoyés à chaque ut
```

### Estimation du nombre de serveurs requis

La charge générée par un utilisateur d'IBM Cognos Mobile sur un serveur (répartiteur) est minime s'il ne consomme que des rapports actifs. Pour les utilisateurs de tableaux de bord Cognos Workspace, l'app ne fait pas peser de charge supplémentaire sur le serveur par rapport à un utilisateur sédentaire.

## Réduction du délai de diffusion pour les rapports sur un réseau

Les rapports diffusés globalement sont plus longs à ouvrir dans les emplacements distants qu'en local. En outre, les rapports HTML sont plus longs à ouvrir que les rapports PDF, car le nombre de requêtes à traiter est supérieur.

Il existe deux façons de réduire le délai d'ouverture des rapports dans les emplacements distants. Vous pouvez diminuer le nombre de requêtes entre le navigateur et le serveur en exécutant le rapport au format PDF. Si des rapports HTML sont requis, vous pouvez accélérer la livraison du rapport en configurant des passerelles supplémentaires dans certains emplacements distants. Le contenu statique tel que les images et les feuilles de style sera diffusé plus rapidement.

## Augmentation du délai d'attente asynchrone dans les environnements à forte charge utilisateur

Si vous disposez d'un environnement à forte charge utilisateur (plus de 165 utilisateurs) et que des rapports interactifs s'exécutent en continu dans une installation répartie, vous pouvez augmenter le paramètre de délai asynchrone afin de ne plus recevoir de messages d'erreur. La valeur par défaut est 30000.

Vous pouvez également définir le paramètre de délai maximal de la file d'attente sur 360. Pour obtenir des informations, voir le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Pour résoudre ce problème, augmentez la valeur du délai d'attente.

### Procédure

1. Ouvrez le répertoire suivant : *emplacement_installation*webapps/p2pd/WEB-INF/services/.
2. Ouvrez le fichier reportservice.xml dans un éditeur de texte.
3. Définissez le paramètre async_wait_timeout_ms sur 120000.
4. Enregistrez le fichier.
5. Redémarrez le service.

# Chapitre 10. Configuration manuelle d'IBM Cognos Analytics sous UNIX et Linux

La console connectée à l'ordinateur UNIX ou Linux sur lequel vous installez IBM Cognos Analytics ne prend pas forcément en charge les interfaces utilisateur graphiques de type Java.

Vous devez effectuer manuellement les tâches suivantes :

__ • Modifier manuellement les paramètres de configuration par défaut en éditant le fichier `cogstartup.xml` situé dans le répertoire *emplacement_installation*`/configuration`.

__ • Modifier le support de langue ou de devise ou le mappage des paramètres régionaux en éditant le fichier `coglocale.xml` situé dans le répertoire *emplacement_installation*`/configuration`.

__ • Appliquer la configuration et les paramètres régionaux à l'ordinateur en exécutant IBM Cognos Configuration en mode silencieux.

Pour toutes les installations, certaines tâches de configuration sont nécessaires pour qu'IBM Cognos Analytics puisse fonctionner dans votre environnement. Si vous répartissez des composants d'IBM Cognos Analytics sur plusieurs ordinateurs, l'ordre dans lequel vous configurez et démarrez les ordinateurs est important.

D'autres tâches de configuration sont facultatives et dépendent de votre environnement d'exécution de rapports. Vous pouvez changer le comportement par défaut d'IBM Cognos Analytics en éditant le fichier `cogstartup.xml` afin de changer la valeur des propriétés. Vous pouvez également utiliser des exemples de fichiers permettant à IBM Cognos Analytics d'utiliser des ressources existantes de votre environnement.

## Modification manuelle des paramètres de configuration par défaut

Si la console connectée à l'ordinateur UNIX ou Linux ne prend pas en charge les interfaces utilisateur graphiques de type Java, vous devez éditer le fichier `cogstartup.xml` pour configurer IBM Cognos Analytics pour le faire fonctionner dans votre environnement.

**Important :** Certains paramètres de configuration ne sont pas enregistrés dans le fichier `cogstartup.xml` si vous n'utilisez pas l'interface graphique. Par exemple, le fuseau horaire du serveur n'est pas défini pour vos composants d'IBM Cognos lorsque vous modifiez le fichier `cogstartup.xml` directement et que vous exécutez IBM Cognos Configuration en mode silencieux. Dans ce cas, les paramètres des autres utilisateurs qui utilisent le fuseau horaire du serveur peuvent ne pas fonctionner comme prévu.

Si vous souhaitez qu'IBM Cognos Analytics utilise une ressource, telle qu'un fournisseur d'authentification existant dans votre environnement, vous pouvez ajouter un composant à votre configuration. Pour ce faire, copiez le code XML requis des exemples de fichiers vers le fichier `cogstartup.xml`, puis éditez les valeurs en fonction de l'environnement.

Par défaut, le fichier `cogstartup.xml` est encodé au format UTF-8. Lorsque vous enregistrez le fichier `cogstartup.xml`, veillez à modifier l'encodage des paramètres

régionaux de l'utilisateur afin qu'ils correspondent à l'encodage utilisé. L'encodage des paramètres régionaux de l'utilisateur est défini par les variables d'environnement.

Avant d'éditer le fichier cogstartup.xml, n'oubliez pas que le code XML est sensible à la casse. La casse est importante dans toutes les sections de texte, notamment les libellés d'éléments et d'attributs, les éléments et les valeurs.

Avant d'éditer le fichier cogstartup.xml, veillez à :

- faire une copie de sauvegarde,
- créer le magasin de contenu sur un ordinateur disponible de votre réseau,
- passer en revue la configuration requise pour votre type d'installation.

### Procédure

1. Accédez au répertoire *emplacement_installation*/configuration.
2. Ouvrez le fichier cogstartup.xml dans un éditeur.
3. Identifiez le paramètre de configuration que vous voulez modifier en consultant l'aide et les commentaires de descriptifs qui se trouvent devant la balise de début des éléments <crn:parameter>.
4. Modifiez la valeur de l'élément <crn:value> pour qu'il soit conforme à votre environnement.

   **Conseil :** Utilisez l'attribut type pour déterminer le type de données de la propriété de configuration.
5. Répétez les tâches 3 et 4 jusqu'à ce que les valeurs de configuration soient adaptées à votre environnement.
6. Sauvegardez et fermez le fichier.

### Résultats

Vous devez à présent utiliser un éditeur XML de validation afin de valider les modifications par rapport aux règles inscrites dans le fichier cogstartup.xsd, situé dans le répertoire *emplacement_installation*/configuration.

## Ajout d'un composant à la configuration

Le fichier cogstartup.xml contient les paramètres de configuration utilisés par IBM Cognos Analytics et par les composants par défaut. Vous pouvez changer les composants qu'utilise IBM Cognos Analytics en copiant les éléments XML des exemples de fichiers vers le fichier cogstartup.xml. Vous pouvez ensuite éditer les valeurs de configuration afin de les adapter à votre environnement.

Par exemple, pour utiliser une base de données Oracle pour le magasin de contenu, vous pouvez utiliser l'exemple de fichier ContentManager_*code_de_langue*.xml afin de remplacer les informations par défaut de connexion à la base de données.

IBM Cognos Analytics ne peut utiliser qu'une seule instance à la fois des éléments ci-dessous :

- la base de données du magasin de contenu,
- un fournisseur cryptographique,
- un modèle de configuration pour le service IBM Cognos.

Avant de commencer à éditer des fichiers XML, vous devez en connaître la structure.

## Procédure

1. Accédez au répertoire *emplacement_installation*/configuration/samples.
2. Choisissez un exemple de fichier et ouvrez-le dans un éditeur :
   - Si vous souhaitez utiliser Oracle ou IBM Db2 pour le magasin de contenu, ouvrez le fichier ContentManager_*code_de_langue*.xml.
   - Si vous souhaitez utiliser un fournisseur d'authentification, ouvrez le fichier Authentication_*code_de_langue*.xml.
   - Si vous souhaitez utiliser un fournisseur cryptographique, ouvrez le fichier Cryptography_*code_de_langue*.xml.
   - Si vous souhaitez consigner les messages de journal ailleurs que dans un fichier, ouvrez le fichier Logging_*code_de_langue*.xml.
   - Si vous souhaitez utiliser un modèle de taille moyenne ou grande pour la quantité de ressources utilisée par le processus IBM Cognos Analytics, ouvrez le fichier CognosService_*code_de_langue*.xml.
3. Copiez les éléments dont vous avez besoin.

   **Conseil :** Veillez à copier le code en incluant les balises de début et de fin de l'élément <crn:instance>.

   Par exemple, recherchez les commentaires (Begin of) et (End of) :

   ```
   <!--
   (Begin of) Db2 template
   -->
   <crn:instance ...>
   ...
   </crn:instance>
   <!--
   End of) Db2 template
   -->
   ```
4. Accédez au répertoire *emplacement_installation*/configuration.
5. Ouvrez le fichier cogstartup.xml dans un éditeur.
6. Collez le code du fichier exemple vers le fichier cogstartup.xml en remplaçant l'élément <crn:instance> approprié.
7. Modifiez les valeurs de ces nouveaux éléments afin de les adapter à votre environnement.

   Pour l'élément <crn:instance>, ne changez pas l'attribut class. Vous pouvez modifier l'attribut name afin de l'adapter à votre environnement.

   Par exemple, si vous utilisez une base de données Oracle pour le magasin de contenu, modifiez uniquement l'attribut name pour l'adapter à votre environnement.

   ```
   <crn:instance class="Oracle" name="MyContentStore">
   ```
8. Sauvegardez et fermez le fichier.
9. Exécutez IBM Cognos Configuration en mode silencieux en saisissant la commande suivante :

   ```
   ./cogconfig.sh -s
   ```

   Cela garantit la validité du fichier et le chiffrement des mots de passe.

## Modification manuelle des paramètres chiffrés

Il est possible de modifier manuellement les paramètres chiffrés, tels que les mots de passe ou les références de l'utilisateur, dans le fichier `cogstartup.xml`.

Pour demander à IBM Cognos Configuration d'enregistrer un paramètre chiffré, vous devez modifier la valeur, puis définir l'indicateur de chiffrement sur Faux.

### Procédure

1. Accédez au répertoire *emplacement_installation*`/configuration`.
2. Ouvrez le fichier `cogstartup.xml` dans un éditeur.
3. Identifiez le paramètre chiffré que vous voulez modifier en consultant l'aide et les commentaires de descriptifs qui se trouvent devant la balise de début des éléments `<crn:parameter>`.
4. Modifiez la valeur de l'élément `<crn:value>` pour qu'il soit conforme à votre environnement.

   **Conseil :** Utilisez l'attribut type pour déterminer le type de données de la propriété de configuration.
5. Faites passer la valeur de chiffrement à Faux.

   Par exemple :

   ```
   <crn:value encrypted="false">
   ```
6. Répétez les tâches 3 à 5 jusqu'à ce que les valeurs de configuration soient adaptées à votre environnement.
7. Sauvegardez et fermez le fichier.
8. Saisissez la commande de configuration suivante :

   ```
   ./cogconfig.sh -s
   ```

### Résultats

Les nouveaux paramètres sont enregistrés et chiffrés.

## Paramètres globaux sous UNIX et Linux

Si la console connectée à l'ordinateur UNIX ou Linux ne prend pas en charge les interfaces utilisateur graphiques de type Java, vous devez éditer manuellement le fichier `coglocale.xml`.

Vous pouvez modifier les paramètres globaux :

- pour spécifier la langue utilisée dans l'interface utilisateur lorsque celle spécifiée dans les paramètres régionaux de l'utilisateur n'est pas disponible
- pour spécifier les paramètres régionaux utilisés dans les rapports lorsque ceux de l'utilisateur ne sont pas disponibles
- pour ajouter une prise en charge de devise ou de paramètres régionaux aux données du rapport ou aux métadonnées
- pour ajouter une prise en charge de langue à l'interface utilisateur.

Par défaut, les composants d'IBM Cognos Analytics appliquent une forme normalisée à tous les paramètres régionaux, qui peuvent provenir de différentes sources et se présenter sous divers formats. Cela signifie que tous les paramètres régionaux étendus sont conformes à une définition de langue et de code régional.

Pour pouvoir ajouter la prise en charge d'une langue à l'interface utilisateur, vous devez installer les fichiers linguistiques sur tous les ordinateurs de l'installation répartie. Pour en savoir davantage, contactez le responsable du support technique.

### Exemple 1

Un rapport est disponible dans Content Manager dans deux langues régionales, telles que en-us (anglais des Etats-Unis) et fr-fr (français de France), mais les paramètres régionaux de l'utilisateur sont définis sur fr-ca (français du Canada). IBM Cognos utilise les mappages de paramètres régionaux pour déterminer le rapport à afficher pour l'utilisateur.

Tout d'abord, IBM Cognos vérifie dans Content Manager si le rapport est disponible dans le paramètre régional de l'utilisateur. Si tel n'est pas le cas, IBM Cognos associe les paramètres régionaux de l'utilisateur à un paramètre régional normalisé configuré dans l'onglet Correspondances des paramètres régionaux (contenu). Comme le paramètre régional de l'utilisateur est fr-ca, il est mappé à fr. IBM Cognos utilise la valeur mappée pour vérifier si le rapport est disponible en français. Dans ce cas, le rapport est disponible en en-us et fr-fr, mais pas en fr.

IBM Cognos  met ensuite en correspondance les rapports disponibles avec des paramètres régionaux normalisés. Ainsi, en-us devient en, et fr-fr devient fr.

Du fait que tant le rapport que les paramètres régionaux de l'utilisateur sont mis en correspondance avec fr, l'utilisateur dont les paramètres régionaux indiquent la langue fr-ca voit s'afficher le rapport en fr-fr.

### Exemple 2

Le paramètre régional de l'utilisateur et les paramètres régionaux de rapport sont tous associés à la même langue. IBM Cognos  sélectionne les paramètres régionaux à utiliser. Par exemple, si le paramètre régional de l'utilisateur est en-ca (English-Canada) et que les rapports sont disponibles en anglais des Etats-Unis (en-us) et en anglais du Royaume-uni (en-gb), IBM Cognos associe chaque paramètre régional à en. L'utilisateur visualise le rapport conformément aux paramètres régionaux choisis par IBM Cognos.

### Exemple 3

Les paramètres régionaux du rapport et ceux de l'utilisateur ne sont pas mis en correspondance avec une langue commune. IBM Cognos  sélectionne la langue. Dans ce cas, il peut s'avérer nécessaire de configurer le mappage. Par exemple, si un rapport est disponible en anglais des Etats-Unis (en-us) et français de France (fr-fr) et que le paramètre régional de l'utilisateur indique la langue espagnol d'Espagne (es-es), IBM Cognos sélectionne la langue.

## Modification manuelle des paramètres globaux sous UNIX et Linux

Procédez comme suit pour changer les paramètres globaux sur UNIX et Linux en utilisant le fichier `coglocale`.

### Procédure

1. Sur chaque ordinateur sur lequel vous avez installé Content Manager, accédez au répertoire *emplacement_installation*`/configuration`.
2. Ouvrez le fichier `coglocale.xml` dans un éditeur.

3. Ajoutez ou modifiez l'élément et l'attribut requis entre les balises de début et de fin.

   Les éléments, attributs et balises de début et de fin sont répertoriés dans le tableau suivant.

*Tableau 49. Balises des paramètres globaux*

| Type d'élément | Balise de début | Balise de fin |
|---|---|---|
| Language | <supportedProductLocales> | </supportedProductLocales> |
| Paramètres régionaux de contenu | <supportedContentLocales> | </supportedContentLocales> |
| Devise | <supportedCurrencies> | </supportedCurrencies> |
| Mappage des paramètres régionaux | <productLocaleMap> | </productLocaleMap> |
| Mappage des paramètres régionaux (contenu) | <contentLocaleMap> | </contentLocaleMap> |
| Polices | <supportedFonts> | </supportedFonts> |
| Paramètres de cookie, emplacement des archives pour les rapports | <parameter name="*setting*"> | </parameter> |

   **Conseil :** Pour supprimer un support, supprimez l'élément.
4. Sauvegardez et fermez le fichier.

### Résultats

**Conseil :** Utilisez un éditeur XML de validation afin de valider les modifications par rapport aux règles dans le fichier `cogstartup.xsd` situé dans le répertoire *`emplacement_installation`*`/configuration.`

Si vous ajoutez un code de devise qui n'est pas pris en charge, vous devez l'ajouter manuellement au fichier `i18n_res.xml` dans le répertoire *`emplacement_installation`*`/bin/`. Copiez ce fichier sur chaque ordinateur IBM Cognos de votre installation.

## Démarrage et arrêt de Cognos Analytics en mode silencieux sous UNIX et Linux

Vous exécutez IBM Cognos Configuration en mode silencieux pour appliquer les paramètres de configuration et démarrer les services sur des ordinateurs UNIX ou Linux qui ne prennent pas en charge une interface graphique basée sur Java.

Avant d'exécuter l'outil de configuration en mode silencieux, vous devez vous assurer que le fichier `cogstartup.xml` est valide, conformément aux règles définies dans le fichier `cogstartup.xsd`. Le fichier `cogstartup.xsd` se trouve dans le répertoire *`emplacement_installation`*`/configuration`.

## Démarrage de Cognos Analytics en mode silencieux sous UNIX et Linux

Procédez comme suit pour démarrer le logiciel IBM Cognos Analytics en mode silencieux.

### Procédure

1. Vérifiez que le fichier `cogstartup.xml`, situé dans le répertoire *emplacement_installation*`/configuration`, a été modifié pour votre environnement.

   Pour en savoir davantage, reportez-vous à la section «Modification manuelle des paramètres de configuration par défaut», à la page 291.
2. Accédez au répertoire *emplacement_installation*`/bin64`.
3. Saisissez la commande suivante :

   ```
   ./cogconfig.sh -s
   ```

   **Conseil :** Pour consulter les messages de journal générés au cours d'une configuration sans surveillance, ouvrez le fichier `cogconfig_response.csv` situé dans le répertoire *emplacement_installation*`/logs`.

### Résultats

IBM Cognos Configuration applique les paramètres de configuration définis dans le fichier `cogstartup.xml`, chiffre les données d'identification, crée des certificats numériques et, le cas échéant, démarre un service ou un processus Cognos.

## Arrêt de Cognos Analytics en mode silencieux sous UNIX et Linux

Procédez comme suit pour arrêter le logiciel IBM Cognos Analytics en mode silencieux.

### Procédure

1. Accédez au répertoire *emplacement_installation*`/bin64`.
2. Saisissez la commande suivante :

   ```
   ./cogconfig.sh -stop
   ```

# Chapitre 11. Installation sans surveillance, désinstallation et configuration

Utilisez une installation, une désinstallation ou une configuration sans surveillance pour :

- Installer une configuration identique sur plusieurs ordinateurs du réseau.
- Automatiser le processus d'installation et de configuration en définissant des options et des paramètres pour les utilisateurs.
- Installer et configurer des composants dans un environnement UNIX ou Linux non doté de XWindows.
- Désinstaller IBM Cognos Analytics.

Avant de mettre en place une installation et une configuration sans surveillance, assurez-vous que la configuration système requise est entièrement respectée et que tous les autres logiciels nécessaires sont dûment installés et configurés.

## Utilisation d'une installation sans surveillance

Procédez comme suit pour dupliquer une installation à partir d'un ordinateur vers un autre sans que le système vous demande d'entrer des informations.

### Procédure

1. Effectuez la tâche «Utilisation d'un fichier de modèle de réponse pour créer une installation facile ou personnalisée», à la page 301 ou lancez l'assistant d'installation avec un paramètre pour enregistrer un fichier de réponses. Par exemple :

   Windows : `ca_srv_<plateforme>_<génération>.exe -r "C:\ResponseFile\ResponseFile.properties"`.

   UNIX ou Linux : `./ca_srv_<plateforme>_<génération> -r "./ResponseFile/ResponseFile.properties"`

   **Remarque :** Le répertoire, par exemple `C:\ResponseFile`, doit exister avant le lancement de l'assistant.

   11.0.6 Il n'est pas nécessaire de procéder à une installation complète pour créer un fichier de réponses. Vous pouvez lancer l'installation avec l'option -r et l'exécuter jusqu'au panneau récapitulatif, puis la quitter. Le fichier de propriétés de réponses est créé lorsque le programme d'installation se ferme.
2. Une fois l'installation terminée, modifiez le fichier de réponses si nécessaire.

   Le fichier de réponses contient les valeurs qui ont été utilisées lorsque l'assistant a été lancé pour le créer. Le mot de passe saisi lors de l'installation est chiffré dans le fichier de réponses.
3. Sur l'ordinateur où vous prévoyez d'installer le logiciel, effectuez l'une des opérations suivantes :
   - Insérez le CD-ROM d'installation du produit approprié et copiez son contenu sur le disque dur de l'ordinateur.
   - Copiez les fichiers d'installation du produit que vous avez téléchargés sur l'ordinateur.

4. Dans une fenêtre de commande ou de terminal, accédez au répertoire du système d'exploitation dans lequel vous avez copié les fichiers d'installation, et entrez la commande suivante :
   - Sous Windows, où *emplacement* est le répertoire dans lequel vous avez créé ou copié le fichier *fichier_de_réponses* :

     ca_srv_<plateforme>_<génération> -f *emplacement\fichier_de_réponses* -i silent

     **Conseil :**

     Lancez le fichier de réponses de l'installation sans surveillance à partir d'un fichier de traitement par lot. De cette manière, le processus d'installation attend la fin de l'installation avant d'effectuer ses retours. Ajoutez également une commande echo %errorlevel% à la fin du fichier de traitement par lots pour connaître le code de sortie de l'installation des entrées du fichier de traitement par lots. Par exemple, *emplacement_installation*\ ca_srv_win64_11.0.3.16051211.exe -i silent -f *emplacement*\ *fichier_de_réponses* echo %errorlevel%

     Si une erreur se produit lors de l'installation, une fenêtre d'invite de commande peut afficher rapidement certaines informations importantes. Un code de sortie égal à 0 (zéro) indique la réussite. Si le code de sortie est différent de 0, il existe deux options.

     a. Affichez le journal d'installation situé dans *emplacement_installation*\ logs\IBM_Cognos_Analytics_Install_<horodatage>.log
     b. Affichez un journal sortant supplémentaire situé dans le dossier temp de l'utilisateur %TEMPDIR%\install_output_log_cognos_analytics.txt. Ce fichier journal affiche la liste des codes de sortie possibles, ainsi que leur description. Vous pouvez également rechercher l'expression Install Error: pour avoir plus de détails.
   - Sous UNIX ou Linux:

     ./ca_srv_<plateforme>_<génération> -f *emplacement/fichier_de_réponses* -i silent
   - Pour une installation dans une langue prise en charge, utilisez l'option -l <code_lang>.

     Par exemple, pour une installation en français et la création d'un fichier de réponses :

     Windows : ca_srv_<plateforme>_<génération>.exe -l <code_lang> –r *emplacement\fichier_de_réponses*.

     UNIX ou Linux : ./ca_srv_<plateforme>_<génération> -l <code_lang> –r *emplacement/fichier_de_réponses*

     Pour utiliser le fichier de réponses et effectuer une installation en français, par exemple dans Windows :

     c:\CAinstallkit\ca_srv_win64_11.0.3.16051211.exe -l fr -i silent -f c:\responselocation\responsefile.properties echo %errorlevel%

*Tableau 50. Codes de langue pris en charge*

| Code | Langue |
|---|---|
| en | Anglais |
| es | Espagnol |
| fr | Français |

*Tableau 50. Codes de langue pris en charge (suite)*

| Code | Langue |
|---|---|
| it | Italien |
| ja | Japonais |
| ko | Coréen |
| pt_BR | Portugais (Brésil) |
| zh_CN | Chinois simplifié |
| zh_TW | Chinois traditionnel |

### Résultats

Si le statut renvoyé est différent de zéro (0), vérifiez les messages d'erreur des fichiers de journalisation. Les erreurs sont enregistrées dans le répertoire *emplacement_installation*\logs, dans un journal d'erreurs récapitulatif. Le format de nom de fichier est tl-*code_produit-version-aaaammjj-hhmm*_summary-error.txt.

Si des erreurs surviennent avant qu'une initialisation suffisante ne se soit produite, les messages de journal sont envoyés dans un fichier journal dans le répertoire Temp. Le format de nom de fichier est tl-*code_produit-version-aaaammjj-hhmm*.txt.

Lorsque toutes les erreurs sont résolues, vous pouvez procéder à une configuration sans surveillance.

## Utilisation d'un fichier de modèle de réponse pour créer une installation facile ou personnalisée

Deux modèles de fichier de réponses sont décrits dans cette rubrique pour vous aider à créer des installations automatiques sans exécuter d'installation pour générer un fichier de réponses.

.

### Procédure

1. Coupez et collez le modèle de cette rubrique pour créer le fichier de réponses à utiliser, pour une installation facile ou personnalisée.
2. Modifiez le fichier de réponses que vous avez créé en suivant les commentaires d'instruction du fichier.

**Modèle de fichier de réponses d'une installation personnalisée :**

```
#Template of Response file for IBM Cognos Analytic Software Silent installation
#
#This template is for a "Custom" install. If you want to do an "Easy" install
#please use other template, located below.
#
#(C) Copyright IBM(R) Corp. 2016. All rights reserved.

#Remember to make a copy of this file before editing it.

#Please DO NOT change the following variable since this is a "Custom" install
BISRVR_INSTALLTYPE_CUSTOM=1

#Required - Install type for "Custom" install
```

```
#------------------------------------------------------------
#You must select one of the following install types
#  If you want to perform "Custom/First Install",
#    set BISRVR_CUSTOM_FIRST to be 1, set the other to be 0
#  If you want to perform "Custom/Connect and install",
#    set BISRVR_CUSTOM_EXPAND to be 1, set the other to be 0
#------------------------------------------------------------
BISRVR_CUSTOM_FIRST=
BISRVR_CUSTOM_EXPAND=

#Required - Features
#-------------------------------------------------------------------------
#For "Custom/First install", feature DATATIER must be selected.
#    Other features can be selected at the same time too.
#For Custom Expand Install, you must select at least one of the features.
#
#BISRVR_FEATURE_DATATIER is called "Content repository" in GUI install.
#BISRVR_FEATURE_APPTIER is called "Application services" in GUI install.
#BISRVR_FEATURE_GATEWAY is called "Optional Gateway" in GUI install.
#-------------------------------------------------------------------------
BISRVR_FEATURE_DATATIER=
BISRVR_FEATURE_APPTIER=
BISRVR_FEATURE_GATEWAY=

#Required - Install Location
#-------------------------------------------
#The installation location
#It is called "Install location" in GUI
# DEFAULT:
#   on UNIX, and Linux
#      /opt/ibm/cognos/analytics
#   on Windows
#   C:\\Program Files\\ibm\\cognos\\analytics
#-------------------------------------------
USER_INSTALL_DIR=

#Required - Input Required for "Custom/Connect and install"
#-----------------------------------------------------------------------------
#The URL of the First Install and Cognos administrator credentials are required for
#  "Custom/Connect and install"
#
#BISRVR_CANALYTICS_URL is called "Cognos Analytics URL" in GUI install
#BISRVR_NAMESPACE is called "Namespace" in GUI install
#BISRVR_COGNOSUSER is called "Cognos administrator user ID" in GUI install
#BISRVR_COGNOSUSER_PASSWORD is called "Password" in GUI install.
# The password must be encrypted. It can be obtained by recording a GUI install.
#-----------------------------------------------------------------------------
BISRVR_CANALYTICS_URL=
BISRVR_NAMESPACE=
BISRVR_COGNOSUSER=
BISRVR_COGNOSUSER_PASSWORD=

#Optional - Options for Windows Install
#-----------------------------------------------------------------------------
#The following two entries are for Windows only
#BISRVR_SHORTCUT is called "Program folder" in GUI install
#BISRVR_ALLUSERS is called "Make shortcut visible to all users in the Start menu"
# in GUI install. Set to 1 if you want the shortcut visible.
#-----------------------------------------------------------------------------
#BISRVR_SHORTCUT=
#BISRVR_ALLUSERS=

#End of Custom install template
#-----------------------------------------------------------------------------
```

**Modèle de fichier de réponses d'une installation facile :**

```
#Template of Response file for IBM Cognos Analytic Software Silent installation
#
#This template is for an "Easy" install. If you want to do a "Custom" install
#please use other template, located above.
#
#(C) Copyright IBM(R) Corp. 2016. All rights reserved.

#Remember to make a copy of this file before editing it.

#Required - Install type for "Easy install"
#-----------------------------------------------------------------
#You must select one of the following install types
#  If you want to perform "Easy install/First Install",
#    set BISRVR_INSTALLTYPE_READY to be 1, set the other to be 0
#  If you want to perform "Easy install/Connect and Install",
#    set BISRVR_INSTALLTYPE_EXPAND to be 1, set the other to be 0
#-----------------------------------------------------------------
BISRVR_INSTALLTYPE_READY=
BISRVR_INSTALLTYPE_EXPAND=

#Required - Install Location
#-------------------------------------------
#The installation location
#It is called "Install location" in GUI
# DEFAULT:
#   on UNIX, and Linux
#      /opt/ibm/cognos/analytics
#   on Windows
#   C:\\Program Files\\ibm\\cognos\\analytics
#-------------------------------------------
USER_INSTALL_DIR=

#Required - Input Required for "Easy install"
#-------------------------------------------------------------------------
#Cognos administrator credentials are required for "Easy install".
#BISRVR_COGNOSUSER is called "Cognos administrator user ID" in GUI install.
#BISRVR_COGNOSUSER_PASSWORD is called "Password" in GUI install.
# The password must be encrypted. It can be obtained by recording a GUI install.
#-------------------------------------------------------------------------
BISRVR_COGNOSUSER=
BISRVR_COGNOSUSER_PASSWORD=

#Required - Input Required for "Easy install/Connect and Install"
#-----------------------------------------------------------------
#BISRVR_CANALYTICS_URL is called "Cognos Analytics URL" in GUI install
#-----------------------------------------------------------------
#BISRVR_CANALYTICS_URL=

#Optional - Options for Windows Install
#-------------------------------------------------------------------------
#The following two entries are for Windows only
#BISRVR_SHORTCUT is called "Program folder" in GUI install
#BISRVR_ALLUSERS is called "Make shortcut visible to all users in the Start menu"
# in GUI install. Set to 1 if you want the shortcut visible.
#-------------------------------------------------------------------------
#BISRVR_SHORTCUT=
#BISRVR_ALLUSERS=

#End of Easy install template
#-------------------------------------------------------------------------
```

## Que faire ensuite

Exécutez votre fichier de réponses en suivant les instructions de la rubrique «Utilisation d'une installation sans surveillance», à la page 299.

# Utilisation d'une configuration sans surveillance

Pour utiliser une configuration sans surveillance, vous devez exporter une configuration à partir d'une installation existante dans laquelle sont installés les mêmes composants IBM Cognos Analytics. Vous pouvez ensuite exécuter IBM Cognos Configuration en mode silencieux.

La configuration exportée contient les propriétés des composants IBM Cognos Analytics que vous avez installés sur un ordinateur.

## Avant de commencer

Vérifiez que les paramètres de configuration sur l'ordinateur où vous exportez la configuration peuvent être utilisés sur un autre ordinateur sur lequel les mêmes composants sont installés. Par exemple, si vous avez remplacé la partie de nom d'hôte localhost de la propriété URI de la passerelle par une adresse IP ou un nom d'ordinateur, vérifiez que cette valeur convient pour la configuration du nouvel ordinateur.

## Procédure

1. Dans IBM Cognos Configuration, dans le menu **Fichier**, cliquez sur **Exporter en tant que**.
2. Lorsque vous êtes invité à indiquer si le contenu déchiffré doit être exporté, cliquez sur **Oui**.
3. Si vous voulez exporter la configuration actuelle vers un autre dossier, dans la zone **Rechercher dans**, localisez et ouvrez le dossier.
4. Dans la zone **Nom de fichier**, saisissez un nom pour le fichier de configuration.
5. Cliquez sur **Enregistrer**.
6. Copiez le fichier de configuration exporté dans le répertoire *emplacement_installation*/configuration de l'ordinateur sur lequel vous prévoyez d'utiliser la configuration sans surveillance.
7. Renommez le fichier en cogstartup.xml.
8. Accédez au répertoire *emplacement_installation*/bin ou *emplacement_installation*/bin64.
9. Saisissez la commande suivante :
   - Sous UNIX ou Linux, saisissez
     ```
     ./cogconfig.sh -s
     ```
   - Sur Windows, tapez :
     ```
     cogconfig.bat -s
     ```

   **Conseil :** Pour consulter les messages de journal générés au cours d'une configuration sans surveillance, ouvrez le fichier cogconfig_response.csv situé dans le répertoire *emplacement_installation*/logs.

   Pour contrôler le bon déroulement de la configuration sans surveillance, vérifiez le statut renvoyé. Une valeur nulle (0) indique que l'installation s'est effectuée correctement. Toute autre valeur indique qu'une erreur s'est produite.

## Résultats

IBM Cognos Configuration applique les paramètres de configuration définis dans le fichier cogstartup.xml, chiffre les données d'identification, crée des certificats numériques et, le cas échéant, démarre le service ou le processus IBM Cognos.

## Utilisation d'une désinstallation sans surveillance

Utilisez une désinstallation sans surveillance pour automatiser la suppression des composants sur plusieurs ordinateurs ayant les mêmes composants ou des composants d'un environnement UNIX ou Linux ne disposant pas de XWindows.

**Conseil :** Si des outils de surveillance, tels que Process Explorer ou MMC (Microsoft Management Console) sont en cours d'exécution lors de la désinstallation, ils interféreront avec la suppression des services. Cela s'applique à tous les services en général. Par exemple, après la désinstallation de Cognos Analytics, les services du produit, tels qu'ApacheDS, IBM Cognos et Informix, ne seront pas intégralement supprimés, mais seront affichés dans le panneau des services comme arrêtés et désactivés. Pour éviter cela, aucun outil de surveillance ne doit être en cours d'exécution lors de la désinstallation. L'arrêt de ces outils de surveillance après la désinstallation terminera également la suppression des services.

### Procédure

Depuis la ligne de commande, lancez l'assistant d'installation avec les paramètres suivants :
Windows : *emplacement_installation*`/Uninstall_IBM_Cognos_Analytics.exe -i silent`.
UNIX ou Linux : `./`*emplacement_installation*`/Uninstall_IBM_Cognos_Analytics -i silent`

# Chapitre 12. Désinstallation d'IBM Cognos Analytics

Il est important d'utiliser les programmes de désinstallation afin de supprimer totalement l'ensemble des fichiers et des modifications apportées aux fichiers système. Pour désinstaller IBM Cognos Analytics, vous devez désinstaller les composants serveur et les outils de modélisation.

Si vous exécutez IBM Cognos Analytics dans un environnement de serveur d'applications, utilisez l'outil d'administration proposé par ce serveur pour arrêter l'application si elle est en cours d'exécution et annuler le déploiement de la partie Java des composants d'IBM Cognos Analytics. De nombreux serveurs d'applications ne suppriment pas intégralement les répertoires ou les fichiers d'application déployés lors de l'annulation d'un déploiement ; par conséquent, vous devrez peut-être effectuer cette action manuellement. Après avoir annulé le déploiement des composants d'IBM Cognos Analytics, suivez la procédure décrite dans cette section pour effectuer la désinstallation sous UNIX et Microsoft Windows.

**Conseil :** Si des outils de surveillance, tels que Process Explorer ou MMC (Microsoft Management Console) sont en cours d'exécution lors de la désinstallation, ils interféreront avec la suppression des services. Cela s'applique à tous les services en général. Par exemple, après la désinstallation de Cognos Analytics, les services du produit, tels qu'ApacheDS, IBM Cognos et Informix, ne seront pas intégralement supprimés, mais seront affichés dans le panneau des services comme arrêtés et désactivés. Pour éviter cela, aucun outil de surveillance ne doit être en cours d'exécution lors de la désinstallation. L'arrêt de ces outils de surveillance après la désinstallation terminera également la suppression des services.

**Important :** Ne supprimez pas les fichiers de configuration et de données si vous procédez à une mise à niveau d'IBM Cognos Analytics et voulez utiliser les données de configuration avec la nouvelle version.

## Désinstallation d'IBM Cognos Analytics sous UNIX ou Linux

Si vous n'avez plus besoin d'IBM Cognos Analytics ou si vous procédez à une mise à niveau sur votre système d'exploitation UNIX ou Linux, désinstallez-le.

La désinstallation ne supprime pas tous les fichiers modifiés depuis l'installation, tels que les fichiers de configuration et les fichiers de données utilisateur. L'emplacement d'installation reste sur l'ordinateur. Tant que vous ne supprimez pas ces fichiers manuellement, ils sont conservés.

### Procédure

1. Si la console connectée à l'ordinateur ne prend pas en charge les interfaces utilisateur graphiques Java, trouvez l'ID (PID) du processus IBM Cognos Analytics à l'aide de la commande suivante :

   ```
   ps -ef | grep cogbootstrapservice
   ```

2. Arrêtez le processus IBM Cognos Analytics :
   - Si vous utilisez XWindows, démarrez IBM Cognos Configuration et cliquez sur **Arrêter** dans le menu **Actions**.

- Si vous n'utilisez pas X Windows, saisissez :

  ```
  kill -TERM pid
  ```

3. Pour désinstaller IBM Cognos Analytics, accédez au répertoire *emplacement_installation* et saisissez la commande appropriée :
   - Si vous utilisez X Windows, saisissez :

     ```
     ./uninst -u
     ```

   - Si vous n'utilisez pas XWindows, exécutez une désinstallation sans surveillance (voir «Utilisation d'une installation sans surveillance», à la page 299).
4. Suivez les invites pour achever la désinstallation.
5. Supprimez tous les fichiers Internet temporaires sur les ordinateurs du navigateur Web.

## Désinstallation d'IBM Cognos Analytics sous Microsoft Windows

Si vous n'avez plus besoin d'IBM Cognos Analytics ou si vous procédez à une mise à niveau, désinstallez tous les composants d'IBM Cognos Analytics et le service IBM Cognos.

Si vous avez installé plusieurs composants dans le même emplacement, l'assistant de désinstallation vous permet de choisir les packs à désinstaller. Tous les composants du pack seront désinstallés. Vous devez répéter le processus de désinstallation sur chaque ordinateur contenant des composants d'IBM Cognos Analytics.

Il n'est pas nécessaire de sauvegarder les fichiers de configuration et de données sur un système d'exploitation Microsoft Windows. Ces fichiers sont conservés pendant la désinstallation.

Fermez tous les programmes avant de désinstaller IBM Cognos Analytics. Dans le cas contraire, il est possible que certains fichiers ne soient pas supprimés.

La désinstallation ne supprime pas tous les fichiers modifiés depuis l'installation, tels que les fichiers de configuration et les fichiers de données utilisateur. L'emplacement d'installation reste sur l'ordinateur. Tant que vous ne supprimez pas ces fichiers, ils sont conservés. Ne supprimez pas les fichiers de configuration et de données si vous procédez à une mise à niveau d'IBM Cognos Analytics et voulez utiliser les données de configuration avec la nouvelle version.

### Procédure

1. Dans le menu **Démarrer**, cliquez sur **Tous les programmes** > **IBM Cognos Analytics** > **Désinstaller IBM Cognos Analytics**.

   L'**Assistant de désinstallation** s'affiche.

   **Conseil :** IBM Cognos Analytics est le nom par défaut du dossier de programme créé lors de l'installation. Si vous avez choisi un autre nom, ouvrez ce dossier pour trouver le programme.
2. Suivez les instructions de désinstallation des composants.

   Le fichier `cognos_uninst_log.htm` enregistre les activités que l'assistant de désinstallation exécute lors de la désinstallation des fichiers.

   **Conseil :** Pour trouver le fichier journal, recherchez-le dans le répertoire Temp.

3. Supprimez tous les fichiers Internet temporaires sur les ordinateurs du navigateur Web.

   Pour en savoir davantage, reportez-vous à la documentation sur le navigateur Web.

## Récupération après l'échec de la désinstallation

En cas d'échec de la désinstallation, il peut rester des fichiers, des entrées de registre et des services qui auraient dû être supprimés. Cette rubrique décrit les instructions à suivre pour les installations simple et personnalisée.

### Procédure

1. Pour une première installation simple :
   a. Supprimez Informix en exécutant la commande de désinstallation Informix :

      *emplacement_installation*\informix\bin\ifxdeploy.exe -u *emplacement_installation*\informix -c

   a. Supprimez la clé de registre suivante : HKEY_LOCAL_MACHINE\SOFTWARE\Informix\Online\ol_cognoscm
   b. Supprimez le dossier d'installation *emplacement_installation*
   c. S'il s'agit de la seule installation InstallAnywhere existante sur votre machine, vous pouvez supprimer le fichier de registre InstallAnywhere : %PROGRAM FILES%\Zero G Registry\.com.zerog.registry.xml
2. Pour toutes les autres installations :
   a. Supprimez le dossier d'installation *emplacement_installation*
   b. S'il s'agit de la seule installation InstallAnywhere existante sur votre machine, vous pouvez supprimer le fichier de registre InstallAnywhere :

      Sous Windows (répertoire masqué) : %PROGRAM FILES%\Zero G Registry\.com.zerog.registry.xml

      Sous UNIX : fichier de registre : .com.zerog.registry.xml dont l'emplacement est le suivant :

      - En cas de connexion en tant que root, le registre global se trouve dans /var
      - En cas de connexion en tant qu'utilisateur, il se trouve dans le répertoire de base de l'utilisateur.

      Si vous ne connaissez pas le statut des installations InstallAnywhere, vous pouvez renommer simplement ce fichier afin d'en conserver une copie.

# Chapitre 13. Archivage de contenu IBM Cognos

Le stockage du contenu archivé dans votre référentiel externe vous permet de respecter les exigences de conformité réglementaire et d'accroître l'évolutivité et les performances des produits IBM Cognos en réduisant la taille du contenu dans le magasin de contenu.

Le logiciel prend en charge IBM FileNet Content Manager avec le référentiel externe IBM FileNet CMIS. Si la version 1 d'IBM Filenet CMIS est déjà installée, mettez à niveau ce logiciel à l'aide du groupe de correctifs, version 2. L'archivage de contenu peut également être configuré pour utiliser votre système de fichiers.

Les administrateurs peuvent établir une connexion entre une source de données et un référentiel externe pour permettre de déplacer du contenu du magasin de contenu vers le référentiel. Les utilisateurs peuvent ensuite voir le contenu archivé dans le référentiel externe. En fournissant des résultats de recherche pour le contenu récent et archivé, les utilisateurs peuvent effectuer des comparaisons critiques entre les données en cours et les données historiques. Ce dispositif efficace permet à votre entreprise de répondre aux exigences commerciales et réglementaires de manière transparente pour l'utilisateur.

Le contenu archivé dans le référentiel externe n'est pas géré dans l'environnement IBM Cognos. Par exemple, si vous supprimez des rapports dans IBM Cognos Analytics, les sorties archivées ne sont pas supprimées de votre référentiel externe.

Pour en savoir davantage sur l'administration des archives, reportez-vous au manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Deux scénarios de flux de travaux sont possibles pour l'archivage de contenu. Le premier flux de travaux permet aux administrateurs d'archiver des packs et des dossiers après l'installation du logiciel d'archivage de contenu IBM Cognos. Le deuxième flux de travaux permet aux administrateurs de créer des connexions de référentiel pour les nouveaux packs et dossiers.

## Flux de travaux 1 : Archivage de contenu après installation du logiciel de connectivité

Les administrateurs peuvent archiver la sortie de rapport enregistrée pour des packs et des dossiers spécifiques ou pour tous, après l'installation ou la mise à niveau d'IBM Cognos Analytics. Ce flux de travaux doit être exécuté une seule fois car l'intégralité du contenu se trouve dans le magasin de contenu.

- Créer une connexion de source de données au référentiel externe.
- Sélectionner les connexions de référentiel pour les packs et dossiers à archiver.
- Créer et exécuter une tâche de maintenance d'archivage en vue de sélectionner les dossiers et les packs à archiver dans le référentiel externe.

Après avoir défini une connexion de référentiel pour les packs et les dossiers, toute nouvelle sortie de rapport est automatiquement archivée et il n'est pas nécessaire de réexécuter la tâche de maintenance d'archivage.

### Flux de travaux 2 : Création de connexions de référentiel pour les nouveaux packs et dossiers

Les administrateurs peuvent créer des connexions de référentiel pour les nouveaux packs et dossiers en effectuant les tâches suivantes :

- Créer une connexion de source de données au référentiel externe.
- Sélectionner les connexions de référentiel pour les packs et dossiers à archiver.

## Utilisation des tâches de maintenance d'archivage de contenu

La tâche de maintenance d'archivage de contenu permet de créer une référence aux versions de rapport dans les dossiers et les packs que vous sélectionnez et configurez. La sélection des dossiers et des packs marque leur contenu et celui-ci est conservé dans le magasin de contenu jusqu'à son archivage dans votre référentiel externe.

Il est important de noter que cette tâche ne déplace pas le contenu du magasin de contenu vers le référentiel externe. Vous devez en premier sélectionner des connexions de référentiel pour vos packs et dossiers. Les versions de rapport dans les dossiers et les packs qui ne sont pas marqués pour archivage peuvent être supprimés dans le magasin de contenu.

Une fois le contenu marqué, la tâche d'archivage de contenu est terminée. Dans Content Manager, une tâche d'arrière-plan recherche les éléments marqués puis les copie et les sauvegarde dans le référentiel externe.

L'importation de contenu dans un dossier ou un pack configuré pour être archivé dans un référentiel externe ne déplace pas et n'archive pas le contenu importé dans le référentiel. Un administrateur doit exécuter une tâche de maintenance de contenu d'archivage pour ce dossier ou ce pack en vue d'archiver le contenu importé.

## Tâches d'arrière-plan

Les tâches XML d'arrière-plan utilisées pour déplacer le contenu du magasin de contenu vers le référentiel externe sont archiveTask.xml et deleteTask.xml. Le fichier archiveTask.xml déplace le contenu marqué vers un référentiel externe. Vous pouvez également utiliser ce fichier pour définir le nombre d'exécutions de l'agent et les sorties d'archivage aux formats sélectionnés. Le fichier deleteTask.xml est un fichier de configuration qui extrait et supprime de la file d'attente les objets de version marqués. Ne modifiez pas ce fichier.

## Conservation des identificateurs de contenu avant l'archivage

Si vous le souhaitez, vous pouvez conserver les identificateurs de contenu avant l'archivage de la sortie de rapport.

Les identificateurs des objets présents dans le magasin de contenu sont supprimés et remplacés par défaut par les nouveaux identificateurs lorsque vous exécutez et importez un déploiement et déplacez le contenu vers un environnement cible. Dans certains cas cependant, les identificateurs de contenu doivent être conservés, par exemple, lorsque vous déplacez une sortie de rapport vers un référentiel de rapport externe.

# Configuration de l'archivage de contenu

Vous devez configurer votre environnement en vue de l'archivage de contenu. Pour que les changements de configuration prennent effet, vous devez arrêter, puis démarrer les services IBM Cognos.

## Création d'un emplacement de fichier pour un référentiel de système de fichiers

Pour archiver des rapports ou des spécifications de rapport dans un référentiel de système de fichiers d'archivage de contenu IBM Cognos, vous devez créer une valeur alias qui pointe vers un emplacement de fichier sur un disque local ou un partage réseau.

### Avant de commencer

Vous devez être un administrateur et avoir accès à l'emplacement du fichier. Content Manager et les composants du groupe de serveurs d'applications doivent pouvoir accéder à cet emplacement à l'aide d'un identificateur URI de fichier.

### Procédure

1. S'il est actif, arrêtez le service IBM Cognos.
2. Démarrez IBM Cognos Configuration.
3. Cliquez sur **Actions** > **Editer la configuration globale.**
4. Dans l'onglet **Général**, sélectionnez **Racines alias**, cliquez dans la zone de valeur, puis sur le bouton Editer, et dans la boîte de dialogue **Valeur - Racines d'alias**, cliquez sur **Ajouter**.
5. Dans la colonne **Nom de la racine alias**, saisissez un nom unique pour le référentiel de système de fichiers.

   **Remarque :** Le nombre d'alias pouvant être créés n'est pas limité.
6. Entrez le chemin d'accès à l'emplacement du système de fichiers, où chemin-système-fichiers correspond au chemin d'accès complet à un emplacement de système de fichiers existant :
   - Sous Windows, dans la colonne **windowsURI**, saisissez `file:///` suivi par le chemin local, par exemple `file:///c:/chemin-système-fichiers` ou saisissez `file://` suivi par le nom du serveur et le chemin de partage, par exemple `file://server/share`.
   - Sous UNIX ou Linux, dans la colonne **unixURI**, saisissez `file:///` suivi par le chemin local, par exemple `file:///chemin-système-fichiers`.

   **Remarque :** Les chemins relatifs, comme `file:///../chemin-système-fichiers`, ne sont pas pris en charge.

   Dans une installation répartie, l'ordinateur Content Manager et l'ordinateur des composants du groupe de serveurs d'applications doivent tous deux avoir accès à l'emplacement de fichier. Utilisez les deux identificateurs URI uniquement dans une installation répartie. L'identificateur URI UNIX et l'identificateur URI Windows d'une racine d'alias doivent pointer vers le même emplacement sur le système de fichiers.
7. Cliquez sur le bouton **OK**.
8. Redémarrez le service IBM Cognos. Cette opération peut prendre quelques minutes.

### Résultats

Utilisez ce nom de référentiel de système de fichiers pour créer une connexion de source de données à utiliser avec le logiciel d'archivage de contenu Cognos. Pour en savoir davantage, voir le document *IBM Cognos - Guide d'administration et de sécurité.*

## Importation des définitions et propriétés des classes personnalisées dans IBM FileNet Content Manager

Pour utiliser l'archivage de contenu IBM Cognos, vous devez importer un ensemble de classes personnalisées et de fichiers de propriétés dans IBM FileNet Content Manager.

Les définitions et propriétés des classes personnalisées incluent les métadonnées propres à FileNet. Vous pouvez installer à tout moment des classes et des fichiers de propriétés personnalisés.

### Procédure

1. Si l'archivage FileNet est configuré, accédez au répertoire *emplacement_installation*/configuration/repository/filenet/upgrade/.
2. Si l'archivage FileNet n'est pas déjà configuré, accédez au répertoire *emplacement_installation*/configuration/repository/filenet/new/.
3. Copiez le fichier CMECMIntegrationObjects_CEExport._xxx.xml vers un dossier local sur le serveur FileNet.
4. Ouvrez l'outil d'administration FileNet Enterprise Manager et connectez-vous au domaine pour le référentiel externe FileNet.
5. Sélectionnez un magasin d'objet cible et cliquez sur **Import All Items** pour importer les définitions dans le magasin d'objet.
6. Dans le panneau Options d'importation, cliquez sur **Import Manifest File** et accédez à l'emplacement des fichiers CMECMIntegrationObjects_CEExport._xxx.xml.
7. Sélectionnez le fichier CMECMIntegrationObjects_CEExport_Manifest.xml et cliquez sur **Import**.
8. Redémarrez FileNet Content Engine et l'application FileNet CMIS afin d'appliquer les modifications à l'environnement.

   **Remarque :** La mise à jour des modifications sur tous les noeuds FileNet peut prendre beaucoup de temps.

## Importation des propriétés et définitions de classes personnalisées dans IBM Content Manager 8

Pour utiliser l'archivage de contenu IBM Cognos avec IBM Content Manager 8, vous devez importer un ensemble de fichiers de propriétés et classes personnalisés. Vous devez mettre à jour le fichier de configuration CMIS avec les types de dossier IBM Cognos.

Les définitions et propriétés des classes personnalisées incluent les métadonnées propres à IBM Content Manager 8. Vous pouvez installer des fichiers de classe personnalisée et de propriétés à tout moment.

Il n'y a pas de Resource Manager défini durant le processus d'installation, il existe des messages d'erreur concernant des conflits lors du processus d'importation.

## Avant de commencer

IBM Content Manager 8 doit être installé avec un référentiel externe IBM Content Manager 8 CMIS version 1.1.

## Procédure

1. Ouvrez le **client d'administration système** Content Manager 8.
2. Dans le menu principal, cliquez sur **Outils** > **Importer XML**.
3. Dans la fenêtre des **options d'importation XML**, à la section du **fichier à importer** :
   - Dans la zone **Data model file**, cliquez sur **Browse**, et sélectionnez le fichier `CMECMIntegrationTypes_RMImport_Manifest.xsd` à partir duquel vous souhaitez importer les objets.
   - Dans la zone **Administrative objects file**, cliquez sur **Browse**, et sélectionnez le fichier `CMECMIntegrationTypes_RMImport_MimeTypes.xml` pour importer le fichier d'objets administratifs.

   L'emplacement par défaut est le répertoire *emplacement_installation*`/configuration/repository/contentManager8/New`.
4. Pour afficher les conflits, dans la fenêtre des **options d'importation XML** dans les **options de traitement**, sélectionnez **Process interactively**.
5. Cliquez sur **Importer** pour démarrer le processus d'importation.
   a. Dans la fenêtre **Import Preprocessor Results**, développez **Item Types**, puis cliquez deux fois sur un type d'élément indiquant un conflit.
   b. Dans la fenêtre **Details of Import Definition and Target Definition**, dans la colonne **Resulting Target**, sélectionnez les noms pour **Resource Manager** et **Collection** créés lors de l'installation de Content Manager 8, puis cliquez sur **Accept**.
   c. Répétez les étapes a et b pour chaque type d'élément indiquant un conflit.
6. Après avoir résolu tous les conflits, dans la fenêtre **Import Preprocessor Results**, cliquez sur **Continue**.
7. Dans la fenêtre **Confirm Import Selection**, cliquez sur **Import**.
8. Une fois l'importation terminée, cliquez sur **OK**.
9. Pour mettre à jour le fichier de configuration CMIS afin de détecter les types de dossier IBM Cognos, lancez le programme de configuration CMIS for Content Manager 8 pour créer un profil.
10. Ouvrez le fichier `cmpathservice.properties` dans le dossier de profils de configuration IBM CMIS for Content Manager.

    Pour UNIX, le chemin de fichier par défaut est : `/opt/IBM/CM_CMIS/profiles/profile1`

    Pour Windows, le chemin de fichier par défaut est : `C:\Program Files\IBM\CM_CMIS\profiles\profile1`

    a. Localisez la ligne `folderTypes`.
    b. Ajoutez les types de dossier IBM Cognos COGNOSREPORT et REPORTVERSION en majuscules. Séparez chaque type de dossier par une virgule.

    ```
    Exemple :
    folderTypes = ClbFolder,COGNOSSREPORT,REPORTVERSION
    ```

    c. Enregistrez et fermez le fichier.

11. Lancez le programme de configuration CMIS for Content Manager 8 et sélectionnez l'option de redéploiement du fichier de configuration CMIS automatique.

    **Remarque :** Pour plus d'informations sur le déploiement manuel de CMIS, voir Manually deploying IBM CMIS for Content Manager (http://pic.dhe.ibm.com/infocenter/cmgmt/v8r4m0/topic/com.ibm.installingcmcmis.doc/cmsde001.htm).
12. Dans la console d'administration WebSphere Application Server Liberty Profile, redémarrez **CMIS for Content Manager Application**.

## Spécification d'une heure possible pour exécuter le processus d'archivage

Pour maintenir des performances système élevées lors des heures de pointe, vous pouvez configurer une période d'interruption afin d'indiquer à quel moment les tâches d'archivage ou de suppression s'exécutent.

Une période d'interruption est une période temporaire pendant laquelle le mouvement des données est refusé. Par défaut, aucune période d'interruption n'est définie lors de l'installation du logiciel.

### Procédure

1. Accédez au répertoire *emplacement_installation*/webapps/p2pd/WEB-INF/cm/tasks/manager.
2. A l'aide d'un éditeur de texte XML, ouvrez le fichier tasksManager.xml.
3. Par exemple, pour spécifier une période d'interruption hebdomadaire entre 8h00 et 17h00, du mardi au vendredi, ajoutez l'élément <blackoutPeriods> suivant comme élément enfant de l'élément backgroundTasksManager.
   - start time = <hour>08</hour>
   - stop time = <hour>17</hour>
   - jours =

     ```
     <day>Tuesday</day>
     <day>Wednesday</day>
     <day>Thursday</day>
     <day>Friday</day>
     ```
4. Si nécessaire, réduisez le nombre d'unités d'exécution disponibles pour les processus d'archivage et de suppression. Le nombre maximal d'unités d'exécution est de 7.
5. Sauvegardez et fermez le fichier.
6. Redémarrez les activités d'arrière-plan sur le service Content Manager.

## Spécification de l'heure d'exécution des unités d'exécution

Vous pouvez utiliser des unités d'exécution pour planifier le temps de traitement du système d'exploitation.

Les tâches en arrière-plan d'archivage et de suppression utilisent des unités d'exécution pour déplacer le contenu. Les unités d'exécution sont des unités de temps de traitement planifiées par le système d'exploitation.

### Procédure

1. Accédez au répertoire *emplacement_installation*/webapps/p2pd/WEB-INF/cm/tasks/config.

2. A l'aide d'un éditeur de texte XML, ouvrez le fichier archiveTask.xml.
3. Par exemple, pour configurer trois unités d'exécution qui s'exécutent de minuit à 8h00, une unité d'exécution qui s'exécute de 8h00 à 17h00, aucune unité d'exécution qui s'exécute de 17h00 à minuit et toutes les unités d'exécution qui s'exécutent chaque jour de la semaine, ajoutez l'élément XML <executionPeriods> suivant comme élément enfant de l'élément backgroundTask.

```
  <executionPeriods>
 <executionPeriod>
  <threads>3</threads>
  <startTime>
   <hour>00</hour>
   <minute>00</minute>
  </startTime>
  <stopTime>
   <hour>08</hour>
   <minute>00</minute>
  </stopTime>
  <days>
   <day>Monday</day>
   <day>Tuesday</day>
   <day>Wednesday</day>
   <day>Thursday</day>
   <day>Friday</day>
   <day>Saturday</day>
   <day>Sunday</day>
  </days>
 </executionPeriod>
 <executionPeriod>
  <startTime>
   <hour>08</hour>
   <minute>00</minute>
  </startTime>
  <stopTime>
   <hour>17</hour>
   <minute>00</minute>
  </stopTime>
  <days>
   <day>Monday</day>
   <day>Tuesday</day>
   <day>Wednesday</day>
   <day>Thursday</day>
   <day>Friday</day>
   <day>Saturday</day>
   <day>Sunday</day>
  </days>
 </executionPeriod>
</executionPeriods>
```

4. Sauvegardez et fermez le fichier.

## Archivage des formats sélectionnés de sorties de rapport

Vous pouvez configurer l'archivage de manière à le limiter à des formats de sortie spécifiques. Par défaut, les sorties de n'importe quel format, notamment PDF, XML, HTML et Excel, sont archivées.

Vous pouvez limiter l'archivage de formats de sortie spécifiques au référentiel.

### Procédure

1. Accédez au répertoire *emplacement_installation*/webapps/p2pd/WEB-INF/cm/tasks/config.
2. A l'aide d'un éditeur de texte XML, ouvrez le fichier archiveTask.xml.

3. Par exemple, pour définir l'archivage des versions de sortie de rapport PDF uniquement, ajoutez l'élément XML <outputFormats> suivant comme élément enfant de l'élément XML runOptions.

```
<outputFormats>
   <outputFormat>PDF</outputFormat>
  </outputFormats>
```

Vous pouvez utiliser l'exemple d'élément outputFormats existant et modifier la liste afin de spécifier les formats de sortie à archiver.

Vous ne pouvez pas archiver de manière sélective plusieurs versions de sortie de rapport de fichier, par exemple HTML avec des graphiques.

Sauvegardez et fermez le fichier.

## Spécification de l'absence d'archivage pour les spécifications de rapport

Par défaut, la sortie de spécification de rapport est archivée. Les spécifications de rapport décrivent comment ont été générées les données dans un rapport.

Pour désactiver l'archivage des spécifications de rapport, vous devez modifier deux fichiers : CM.xml et CM_FILENET.xml ou CM_CM8.xml, selon que vous archiviez le contenu dans un référentiel IBM FileNet Content Manager ou un référentiel IBM Content Manager 8.

### Procédure

1. Accédez au répertoire *emplacement_installation*/webapps/p2pd/WEB-INF/repositories/config.
2. A l'aide d'un éditeur de texte XML, ouvrez le fichier CM.xml.
3. Mettez en commentaire ou supprimez la ligne suivante : <property name="specifications" metadataPropertyName="specification" useTempFile="true"
4. Sauvegardez et fermez le fichier.
5. Accédez au répertoire *emplacement_installation*/webapps/p2pd/WEB-INF/repositories/config.
6. Effectuez l'une des opérations suivantes :
   - Si vous archivez le contenu dans FileNet, ouvrez le fichier nommé CM.xml dans un éditeur de texte.
   - Si vous archivez le contenu dans IBM Content Manager 8, ouvrez le fichier nommé CM.xml dans un éditeur de texte.
7. Commentez ou supprimez l'élément suivant :

```
<property repositoryName="REPORTEXECUTIONSPECIFICATION" repositoryType="ASSOCIATED"
metadataPropertyName="specification">
        <associatedObjectTypes>
          <objectType name="VERSIONSPECIFICATION">
           <properties>
           <property repositoryName="cmis:name" repositoryType="STRING"
metadataPropertyName="reportVersionDefaultName"  valueHandler="com.cognos.cm.
repositoryPluginFramework.
PropertyValueAppendStringHandler" valueHandlerArgument="_specification"/>
          </properties>
         </objectType>
        </associatedObjectTypes>
       </property>
```

**Remarque :** Dans le fichier CM.xml, la valeur de objectType name est <objectType name="$t!-2_VERSIONSPECIFICATIONv-1">.

8. Redémarrez les activités d'arrière-plan sur le service Content Manager. Pour plus d'informations, voir le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

# Annexe A. Options de ligne de commande d'IBM Cognos Configuration

Utilisez les options de ligne de commande avec la commande de configuration pour modifier le comportement d'IBM Cognos Configuration au démarrage.

*Tableau 51. Options de ligne de commande et descriptions*

| Option | Descriptions |
|---|---|
| `-h` | Affiche les commandes d'IBM Cognos Configuration. |
| `-s` | Exécute IBM Cognos Configuration en mode silencieux.<br><br>Utilise les valeurs de propriété définies dans le fichier `cogstartup.xml` pour configurer les composants installés et démarre tous les services.<br><br>`./cogconfig.sh -s`<br><br>`cogconfig.bat -s` |
| `-stop` | Arrête tous les services IBM Cognos.<br><br>`./cogconfig.sh -stop`<br><br>`cogconfig.bat -stop` |
| `-startupfile` *`chemin/fichier.xml`* | Exécute IBM Cognos Configuration à l'aide d'un autre fichier que `cogstartup.xml` dans le répertoire *`emplacement_installation`*`/configuration`. |
| `-test` | Utilise les valeurs de propriété définies dans le fichier `cogstartup.xml` pour tester les paramètres de configuration.<br><br>`./cogconfig.sh -test`<br><br>`cogconfig.bat -test` |
| `-notest` | Démarre IBM Cognos Configuration, les tâches de test automatique étant désactivées.<br><br>`./cogconfig.sh -notest`<br><br>`cogconfig.bat -notest`<br><br>Cette option ne doit pas être utilisée lors du premier démarrage du produit ou lors de modifications de configuration. |
| `-utf8` | Enregistre la configuration avec l'encodage UTF-8.<br><br>`./cogconfig.sh -s -utf8`<br><br>`cogconfig.bat -s -utf8` |

*Tableau 51. Options de ligne de commande et descriptions (suite)*

| Option | Descriptions |
|---|---|
| `-l` *`ID langue`* | Exécute IBM Cognos Configuration en utilisant la langue spécifiée par l'identificateur de langue.<br><br>Pour exécuter l'outil de configuration en mode silencieux en chinois simplifié<br><br>`./cogconfig.sh -l zh-cn`<br><br>`cogconfig.bat -l zh-cn` |
| `-e` *`filename.xml`* | Exporte les paramètres de configuration en cours dans le fichier spécifié.<br><br>`./cogconfig.sh -e` *`filename`*`.xml`<br><br>`cogconfig.bat -e` *`nom_fichier`*`.xml` |
| `-log` | Crée un fichier historique des erreurs `cogconfig.`*`timestamp`*`.log` dans le répertoire *`emplacement_cognos`*`/logs`.<br><br>`./cogconfig.sh -log`<br><br>`cogconfig.bat -log` |
| `-java:{local\|env}` | Exécute IBM Cognos Configuration sur les systèmes d'exploitation Microsoft Windows à partir de la version de Java Runtime Environment définie comme :<br>• `env` : au niveau de l'environnement à l'aide d'une variable d'environnement **`JAVA_HOME`**<br>• `local` : au niveau local à partir du répertoire *`emplacement_installation`*`/bin/jre`<br><br>Si vous ne définissez pas cet indicateur, IBM Cognos utilise le paramètre de la variable d'environnement **`JAVA_HOME`**.<br><br>Pour exécuter IBM Cognos Configuration en mode silencieux, à l'aide de la machine JVM locale, entrez la commande suivante :<br><br>`./cogconfig.sh -s -java:local`<br><br>`cogconfig.bat -s -java:local` |

Vous pouvez utiliser plusieurs options de ligne de commande à la fois. Par exemple, vous pouvez exécuter IBM Cognos Configuration en mode silencieux en envoyant tous les messages d'erreur vers un fichier journal.

# Annexe B. Traitement des incidents

Ces informations de référence et solutions de traitement des incidents constituent un outil pratique pour résoudre des problèmes spécifiques détectés durant ou après l'installation de composants IBM Cognos Business Intelligence.

Les problèmes se caractérisent par leurs symptômes. Chaque symptôme permet de remonter à une ou plusieurs causes en utilisant des outils et techniques de traitement des incidents spécifiques. Une fois le problème identifié, il est possible de le résoudre en exécutant une série d'actions.

Les fichiers journaux sont utiles pour le traitement des incidents. La communauté de support est un autre outil de traitement des incidents précieux. Elle est accessible via le site IBM Support Portal (s'ouvre dans une nouvelle fenêtre). Quel que soit votre problème relatif vos produits IBM Cognos, la communauté de support peut vous aider à trouver des solutions.

Si vous ne parvenez pas à résoudre un problème, votre ultime recours est le responsable du support technique. Pour analyser un problème, ce dernier a besoin d'informations sur la situation et les symptômes que vous observez. Pour l'aider à diagnostiquer la cause du problème, réunissez les données nécessaires avant de le contacter.

## Traitement des incidents

Le *traitement des incidents* est une approche systématique de résolution des incidents. L'objectif du traitement des incidents consiste à déterminer pour quelle raison un élément ne fonctionne pas comme prévu et comment résoudre l'incident.

La première étape du processus de traitement des incidents consiste à décrire le problème de manière exhaustive. La description du problème aide l'utilisateur et le responsable du support technique IBM à savoir où chercher la cause du problème. Dans cette étape, vous devez vous poser les questions de base suivantes :

- Quels sont les symptômes du problème ?
- Où se produit le problème ?
- A quel moment se produit le problème ?
- Sous quelles conditions le problème se produit-il ?
- Le problème peut-il être reproduit ?

Les réponses à ces questions permettent généralement d'obtenir une bonne description du problème et mène ensuite à sa résolution.

### Quels sont les symptômes du problème ?

Lorsque vous commencez à décrire un problème, la question la plus évidente est "Quel est le problème ?" Cette question peut sembler directe mais elle peut être divisée en plusieurs sous-questions qui permettent d'obtenir une image plus précise du problème. Ces sous-questions peuvent inclure :

- Qu'est-ce ou qui rapporte le problème ?
- Quels sont les codes d'erreur et messages ?

- Comment le système échoue-t-il ? Par exemple, le problème est-il une boucle, un blocage, une panne, une dégradation de la performance ou un résultat incorrect ?

## Où se produit le problème ?

La détermination de l'origine du problème n'est pas toujours simple mais constitue l'une des étapes les plus importantes de la résolution. Il peut exister de nombreuses couches de technologie entre les composants de génération de rapports et les composants posant problème. Les réseaux, les disques et les pilotes ne représentent qu'une petite partie des composants à prendre en compte lorsque vous recherchez des informations sur un problème.

Les questions suivantes vous aident à isoler la couche du problème :

- Le problème est-il spécifique à une plateforme ou à un système d'exploitation ou est-il commun à plusieurs plateformes ou systèmes d'exploitation ?
- L'environnement et la configuration en cours sont-ils pris en charge ?

Si une couche signale le problème, cela ne signifie pas nécessairement que ce dernier provient de cette couche. Une partie de l'identification de l'origine du problème consiste à comprendre l'environnement dans lequel il existe. Prenez le temps de décrire en détail l'environnement du problème, notamment le système d'exploitation et la version, tous les logiciels et versions correspondants ainsi que le matériel. Confirmez l'exécution dans un environnement pris en charge ; des informations sur de nombreux problèmes pouvant être remontées à des niveaux de logiciels incompatibles n'étant pas destinés à s'exécuter ensemble ou n'ayant pas été entièrement testés ensemble.

## A quel moment se produit le problème ?

Présentez le déroulement détaillé des événements ayant mené à l'échec, tout particulièrement lorsqu'il n'y a qu'une seule occurrence. Il est plus facile de décrire le déroulement en commençant par la fin : commencez par le moment où l'erreur a été signalée (aussi précisément que possible, voire jusqu'aux millisecondes) et remontez la suite des événements à l'aide des journaux et informations disponibles. Généralement, vous n'avez pas besoin de remonter plus loin que le premier événement suspect du journal de diagnostics.

Pour décrire le déroulement détaillé des événements, répondez aux questions suivantes :

- Le problème se produit-il uniquement à un certain moment du jour ou de la nuit ?
- A quelle fréquence se produit le problème ?
- Quelle séquence d'événements provoque le signalement du problème ?
- Le problème se produit-il suite à une modification de l'environnement, telle qu'une mise à niveau ou l'installation de logiciel ou de matériel ?

## Sous quelles conditions le problème se produit-il ?

Il est important, pour le traitement des incidents, de savoir quels sont les systèmes et applications en cours d'exécution au moment où le problème se produit. Ces questions sur votre environnement peuvent vous aider à identifier la cause du problème :

- Le problème se produit-il toujours lors de l'exécution de la même tâche ?

- Est-ce qu'il faut une séquence d'événements particulière pour que le problème se produise ?
- Est-ce que d'autres applications échouent en même temps ?

La réponse à ce type de questions peut vous aider à expliquer l'environnement dans lequel se produit le problème et peut permettre de mettre en corrélation des dépendances. Sachez que ce n'est pas parce que plusieurs problèmes se produisent simultanément qu'ils sont nécessairement liés.

### Le problème peut-il être reproduit ?

Les problèmes que vous pouvez reproduire sont souvent plus faciles à résoudre. Ils peuvent cependant aussi présenter un inconvénient : si leur impact sur votre activité est significatif, vous ne souhaiterez pas les reproduire. Si possible, recréez le problème dans un environnement de test ou de développement qui offre généralement une plus grande flexibilité et un plus grand contrôle lors de l'investigation. Répondez aux questions suivantes :

- Le problème peut-il être recréé sur un système test ?
- Plusieurs utilisateurs ou applications rencontrent-ils le même type de problème ?
- Le problème peut-il être recréé en exécutant une seule commande, un ensemble de commandes ou une application particulière ?

## Recherche dans les bases de connaissances

Le plus souvent, vous trouverez des solutions aux problèmes en recherchant dans les bases de connaissances IBM. Vous pouvez optimiser vos résultats en utilisant les ressources, les outils de support et les méthodes de recherche disponibles.

### Pourquoi et quand exécuter cette tâche

Vous pouvez trouver des informations utiles en procédant à des recherches dans le centre de documentation d'IBM Cognos, mais des recherches plus poussées sont parfois nécessaires pour résoudre certains problèmes.

### Procédure

Pour rechercher des informations dans les bases de connaissance, utilisez les approches suivantes :

- Recherchez le contenu qui vous intéresse à l'aide d'IBM Support Portal.

  IBM Support Portal est une vue unifiée et centralisée de tous les outils de support technique et de toutes les informations relatifs aux systèmes, logiciels et services IBM. IBM Support Portal vous permet d'accéder au portefeuille de support électronique IBM. Vous pouvez personnaliser les pages pour mettre l'accent sur les informations et ressources dont vous avez besoin pour la prévention des problèmes et une résolution plus rapide. Familiarisez-vous avec le portail de support IBM en visualisant les vidéos de démonstration sur cet outil. Ces vidéos présentent IBM Support Portal, explorent les ressources de traitement des incidents ainsi que d'autres ressources et montrent comment personnaliser la page en déplaçant, ajoutant et supprimant des portlets.
- Recherchez le contenu relatif à IBM Cognos en utilisant l'une des ressources techniques supplémentaires suivantes :
  - Rapports APAR IBM Cognos Analytics (rapports sur les problèmes)
  - Forums et communautés IBM Cognos .

- Recherchez du contenu à l'aide de la recherche générique IBM. Vous pouvez utiliser la recherche générique IBM en entrant votre chaîne de recherche dans la zone de recherche de toute page ibm.com.
- Recherchez du contenu en utilisant un moteur de recherche externe tel que Google, Yahoo ou Bing. Si vous utilisez un moteur de recherche externe, vos résultats incluront probablement des informations se trouvant en dehors du domaine ibm.com. Vous pourrez cependant parfois y trouver des informations intéressantes pour la résolution des problèmes sur des produits IBM en consultant des groupes de discussion, des forums et des blogues ne se trouvant pas sur ibm.com.

  **Conseil :** Indiquez «IBM» et le nom du produit à votre recherche si vous recherchez des informations sur un produit IBM.

## Obtention de correctifs

Un correctif de produit peut être disponible pour résoudre votre problème.

### Procédure

Pour trouver et installer des correctifs :

1. Identifiez le correctif nécessaire (Fix Central) (ouvre une nouvelle fenêtre) (http://www.ibm.com/support/fixcentral/)
2. Téléchargez le correctif. Ouvrez le document de téléchargement et suivez le lien dans la section «Download package».
3. Appliquez le correctif en suivant les instructions de la section «Installation Instructions» du document de téléchargement.
4. Abonnez-vous pour recevoir des notifications hebdomadaires par courrier électronique sur les correctifs ainsi que d'autres informations du support IBM.

## Prise de contact avec le support IBM

Le support IBM permet d'accéder à de nombreuses ressources IBM en vue d'obtenir de l'aide sur des questions logicielles.

### Avant de commencer

Après avoir tenté de trouver une réponse ou une solution à l'aide des options d'auto-assistance telles que les notes techniques, vous pouvez contacter le support IBM. Avant de contacter le support IBM, votre entreprise doit disposer d'un contrat de maintenance IBM actif et vous devez être autorisé à soumettre des problèmes à IBM. Vous devez également disposer des informations suivantes à portée de main :

- votre numéro d'identification client,
- le numéro de votre demande de service s'il s'agit d'une demande en cours,
- le numéro de téléphone auquel vous êtes joignable,
- la version du logiciel que vous utilisez,
- la version du système d'exploitation que vous utilisez,
- une description de ce que vous faisiez lorsque le problème s'est produit,
- le texte exact des messages d'erreur qui s'affichent,
- les actions entreprises pour tenter de résoudre le problème.

Pour plus d'informations sur les types de support disponibles, reportez-vous à la rubrique Support portfolio dans le document *Software Support Handbook* (ouvre une nouvelle fenêtre).

### Procédure

Pour contacter le support IBM concernant un problème, exécutez les étapes suivantes :

1. Définissez le problème, rassemblez des informations d'arrière-plan et déterminez la gravité du problème. Pour plus d'informations, voir la rubrique Getting IBM support (ouvre une nouvelle fenêtre) dans le document *Software Support Handbook*.
2. Rassemblez des informations de diagnostic.
3. Soumettez le problème au support IBM de l'une des manières suivantes :
   - A l'aide de l'assistant de support IBM (ISA) : Utilisez cette fonction pour ouvrir, mettre à jour et afficher une demande de service électronique avec IBM. Toutes les données collectées peuvent être associées à la demande de service. L'analyse est alors accélérée et le temps de résolution réduit.
   - En ligne via le portail d'assistance IBM Support Portal (ouvre une nouvelle fenêtre) : Vous pouvez ouvrir, mettre à jour et afficher toutes vos demandes de service à partir du portlet de demande de service sur la page de Demande de service.
   - Par téléphone : Pour connaître le numéro de téléphone à appeler, consultez la page Web Directory of worldwide contacts (ouvre une nouvelle fenêtre).

### Résultats

Si le problème que vous soumettez concerne un problème logiciel ou une documentation manquante ou inappropriée, le support IBM crée un rapport officiel d'analyse de programme (APAR). Le rapport APAR décrit le problème en détail. Lorsque cela est possible, le support IBM fournit une solution palliative que vous pouvez mettre en oeuvre jusqu'à ce que le rapport APAR soit résolu et qu'un correctif soit distribué. IBM publie quotidiennement les rapports APAR résolus sur le site Web du support IBM pour que les autres utilisateurs rencontrant le même problème puissent bénéficier de la même résolution.

## Echange d'informations avec IBM

Pour diagnostiquer ou identifier un problème, vous pouvez fournir au support IBM les données et informations de votre système.

Dans d'autres cas, le support IBM peut vous proposer des outils ou des utilitaires à utiliser pour la détermination du problème.

### Envoi d'informations au support IBM

Pour réduire le temps nécessaire à la résolution de votre problème, vous pouvez envoyer des informations de trace et de diagnostic au support IBM.

#### Procédure

Pour soumettre des informations de diagnostic au support IBM :

1. Ouvrez un enregistrement PMR. Vous pouvez utiliser IBM Support Assistant (ouvre une nouvelle fenêtre) ou l'outil de demande de service IBM (ouvre une nouvelle fenêtre).
2. Collectez les données de diagnostic dont vous avez besoin. Les données de diagnostic permettent de réduire le temps nécessaire à la résolution de votre enregistrement PMR. Vous pouvez collecter ces données de diagnostic manuellement ou automatiquement.

3. Compressez les fichiers à l'aide du programme TRSMAIN ou AMATERSE. Téléchargez l'utilitaire gratuit du site IBM sur le système IBM Cognos Analytics et installez-le à l'aide de la commande TSO RECEIVE.
4. Transférez les fichiers sur IBM. Vous pouvez utiliser l'une des méthodes suivantes pour transférer les fichiers sur IBM :
   - Outil de demande de service (ouvre une nouvelle fenêtre)
   - Les méthodes standard de téléchargement des données : FTP, HTTP
   - Les méthodes sécurisées de téléchargement des données : FTPS, SFTP, HTTPS
   - Courrier électronique

   Si vous utilisez un produit IBM Cognos et ServiceLink / IBMLink pour soumettre des enregistrements PMR, vous pouvez envoyer des données de diagnostic au support IBM dans un courrier électronique ou en utilisant un protocole FTP.

   Toutes ces méthodes d'échange de données sont expliquées sur le site du service de support IBM (ouvre une nouvelle fenêtre).

### Réception d'informations à partir du support IBM

Les représentants du support technique IBM peuvent occasionnellement vous demander de télécharger des outils de diagnostic ou d'autres fichiers. Vous pouvez utiliser le protocole FTP pour télécharger ces fichiers.

#### Avant de commencer

Assurez-vous que votre interlocuteur du support technique IBM vous a indiqué le serveur préféré à utiliser pour le téléchargement des fichiers et le répertoire et les noms de fichiers exacts auxquels accéder.

#### Procédure

Pour télécharger des fichiers à partir du support IBM :

1. Utilisez le protocole FTP pour vous connecter au site fourni par votre interlocuteur du support technique IBM et connectez-vous en tant qu'`anonyme`. Utilisez votre adresse de courrier électronique comme mot de passe.
2. Accédez au répertoire approprié :
   a. Accédez au répertoire `/fromibm`.
      ```
      cd fromibm
      ```
   b. Accédez au répertoire indiqué par votre interlocuteur du support technique IBM.
      ```
      cd nameofdirectory
      ```
3. Activez le mode binaire pour votre session.
   ```
   binary
   ```
4. Utilisez la commande **get** pour télécharger le fichier indiqué par votre interlocuteur du support technique IBM.
   ```
   get filename.extension
   ```
5. Fermez votre session FTP.
   ```
   quit
   ```

## Abonnement aux mises à jour du support

Pour connaître les informations importantes sur les produits IBM que vous utilisez, vous pouvez vous abonner aux mises à jour.

## Pourquoi et quand exécuter cette tâche

L'abonnement aux mises à jour vous permet de recevoir des informations techniques importantes ainsi que des mises à jour pour des outils de support et des ressources spécifiques. Vous pouvez vous abonner aux mises à jour en utilisant l'une des deux approches suivantes :

**Flux RSS et abonnements aux média sociaux**

Les abonnements aux flux RSS et aux média sociaux suivants sont disponibles pour IBM Cognos Analytics :

- Flux RSS d'un forum developerWorks (ouvre une nouvelle fenêtre).
- Flux RSS pour le site du support d'IBM Cognos Analytics (ouvre une nouvelle fenêtre)

Pour obtenir des informations d'ordre général sur le flux RSS, notamment sur les étapes de démarrage, ainsi qu'une liste des pages Web IBM activées pour RSS, consultez le site IBM Software Support RSS feeds (ouvre une nouvelle fenêtre).

**Mes notifications**

Avec Mes notifications, vous pouvez vous abonner aux mises à jour du support pour tout produit IBM. Vous pouvez indiquer que vous souhaitez recevoir des notifications quotidiennes ou hebdomadaires par courrier électronique. Vous pouvez spécifier le type d'informations que vous souhaitez recevoir, par exemple des publications, des conseils et astuces, des notifications flash sur les produits (également appelées alertes), des téléchargements et des pilotes. Mes notifications vous permettent de personnaliser et de catégoriser les produits pour lesquels vous souhaitez être informés et les méthodes de livraison correspondant le mieux à vos besoins.

## Procédure

Pour vous abonner aux mises à jour du support :

1. Abonnez-vous aux flux RSS du *produit*.
2. Pour vous abonner à Mes notifications, commencez par accéder à IBM Support Portal (ouvre une nouvelle fenêtre) et cliquez sur **Mes notifications** dans le portlet **Notifications**.
3. Si vous êtes déjà enregistré pour My support, connectez-vous et passez à l'étape suivante. Si vous n'êtes pas enregistré, cliquez sur **Register now**. Remplissez le formulaire d'enregistrement en utilisant votre adresse de courrier électronique comme ID IBM et en cliquant sur **Submit**.
4. Cliquez sur **Edit profile**.
5. Cliquez sur **Add products** et choisissez une catégorie de produit, par exemple **Software**.
6. Dans la seconde liste, sélectionnez un segment de produit, par exemple **Data & Information Management**.
7. Dans la troisième liste, sélectionnez un sous-segment de produit, par exemple **Bases_de_données**.
8. Sélectionnez les produits pour lesquels vous souhaitez recevoir des mises à jour.
9. Cliquez sur **Add products**.
10. Une fois tous les produits vous intéressant sélectionnés, cliquez sur **Subscribe to email** dans l'onglet **Edit profile**.

11. Sélectionnez **Please send these documents by weekly email**.
12. Mettez à jour votre adresse de courrier électronique si nécessaire.
13. Dans **Documents list**, sélectionnez la catégorie de produit, par exemple **Software**.
14. Sélectionnez les types de documents pour lesquels vous souhaitez recevoir des informations.
15. Cliquez sur **Update**.

### Résultats

Tant que vous n'avez pas modifié vos préférences de flux RSS et My Notifications, vous recevez des notifications des mises à jour que vous avez demandées. Si nécessaire, vous pouvez modifier vos préférences (par exemple, si vous arrêtez d'utiliser un produit et commencez à en utiliser un autre).

## Fichiers journaux

Les fichiers journaux peuvent vous aider à traiter des problèmes car ils enregistrent les activités qui ont lieu lorsque vous utilisez un produit.

Les opérations exécutées dans IBM Cognos Analytics sont enregistrées dans divers fichiers journaux à des fins de suivi. Par exemple, si vous êtes confronté à des problèmes lors de l'installation d'IBM Cognos Analytics, consultez le fichier journal de transfert afin de savoir quelles activités l'assistant d'installation a effectuées durant le transfert des fichiers.

Avant d'afficher les fichiers journaux, vérifiez qu'ils contiennent les informations dont vous avez besoin.

Utilisez IBM Cognos Administration pour définir le niveau de détail à journaliser pour chaque catégorie.

Pour plus d'informations, voir le manuel *IBM Cognos Analytics - Guide d'administration et de sécurité*.

Utilisez IBM Cognos Configuration pour spécifier la taille, le nombre et l'emplacement des fichiers journaux, ainsi que pour configurer les propriétés du serveur de journalisation.

Lors d'une opération de traitement des incidents, les fichiers ci-après peuvent vous être utiles :

### Fichier journal de transfert

Ce fichier est utilisé pour consigner les composants que vous avez installés, des informations sur l'espace disque, les sélections que vous avez faites dans les boîtes de dialogue de transfert et les erreurs éventuelles détectées par l'Assistant d'installation lors du transfert des composants. Il enregistre également les activités que l'Assistant d'installation exécute lors du transfert de fichiers.

Le fichier journal des transferts se trouve dans le répertoire *emplacement_installation*\logs. Le nom de fichier inclut le nom du produit et l'horodatage. Exemple de format du nom de fichier :

```
IBM_Cognos_Analytics_Install_04_21_2016_11_00_59.log
```

## Fichier journal de configuration de l'installation

Ce fichier journal enregistre toutes les activités de configuration lors de l'installation. Par exemple, il consigne le port disponible pour le répartiteur.

Le fichier journal récapitulatif des erreurs de transfert se trouve dans le répertoire *emplacement_installation*\logs. Il est nommé install_configuration.log

## Fichier de configuration de démarrage

Ce fichier est utilisé pour consigner vos choix de configuration chaque fois que vous enregistrez vos paramètres de propriété. Le fichier s'appelle cogstartup.xml.

Si vous n'êtes pas en mesure d'enregistrer la configuration ou rencontrez des problèmes, vous pouvez revenir à un fichier de configuration antérieur. Les fichiers de sauvegarde de la configuration se trouvent dans le répertoire *emplacement_installation*/configuration. Voici un exemple du format de nom de fichier pour des fichiers de configuration de sauvegarde :

```
cogstartup_200811231540.xml
```

## Fichier de verrouillage de configuration de démarrage

Ce fichier est créé à chaque fois que vous exécutez IBM Cognos Configuration. Il vous empêche d'ouvrir plusieurs fenêtres d'IBM Cognos Configuration.

Si vous avez des difficultés à ouvrir IBM Cognos Configuration, vérifiez la présence du fichier cogstartup.lock dans le répertoire *emplacement_installation*/configuration. Si le fichier est présent alors qu'IBM Cognos Configuration n'est pas ouvert, cela signifie qu'IBM Cognos Configuration n'a pas été arrêté correctement la dernière fois que vous l'avez utilisé. Vous pouvez supprimer ce fichier .lock et ouvrir IBM Cognos Configuration.

## Fichier de configuration des paramètres régionaux

Ce fichier est utilisé pour consigner les choix de configuration posés dans IBM Cognos Configuration concernant les paramètres régionaux de produit et de contenu, le mappage des paramètres régionaux et la prise en charge des devises.

Si vous rencontrez des problèmes de prise en charge des langues dans l'interface utilisateur ou dans les rapports, utilisez ces fichiers pour suivre les changements. Les fichiers de sauvegarde de la configuration se trouvent dans le répertoire *emplacement_installation*/configuration. Exemple de format du nom de fichier :

```
coglocale_200811231540.xml
```

## Fichier journal d'exécution

Le fichier journal par défaut d'IBM Cognos nommé cogaudit.log, ou d'autres fichiers journaux configurés pour recevoir des messages de journal du serveur de journalisation, consignent des informations après le démarrage du service IBM Cognos Analytics. Ils se trouvent dans le répertoire *emplacement_installation*/logs. Si vous avez configuré une autre destination pour les messages de journal, vérifiez le fichier ou la base de données appropriée.

Certains messages de journal signalent des problèmes. La plupart de ces messages contiennent uniquement des informations, mais d'autres peuvent vous aider à diagnostiquer des problèmes dans votre environnement d'exécution.

## Fichier journal de passerelle

Les passerelles enregistrent des erreurs dans le fichier journal de passerelle qui se trouve dans le répertoire *emplacement_installation*/logs.

Vous pouvez utiliser le fichier journal de passerelle pour traiter des problèmes empêchant la passerelle de traiter les demandes ou d'utiliser le chiffrement. Les symptômes de ces problèmes sont les suivants :

- Les ID utilisateur et les mots de passe sont inopérants.
- Le code d'accès unique ne fonctionne pas.
- Le répartiteur s'exécute, mais les utilisateurs reçoivent un message d'erreur indiquant que le serveur IBM Cognos Analytics est indisponible.

Le nom du fichier journal de passerelle est le suivant (où *interface_passerelle* est cgi, mod2 (module Apache 2.0) ou isapi) :

gw*interface_passerelle*.log (par exemple, gwcgi.log)

## Fichier journal de désinstallation

Ce fichier est utilisé pour consigner les activités que l'Assistant de désinstallation exécute lors de la désinstallation de fichiers. Le fichier journal s'intitule cognos_uninst_log.htm et se trouve dans le répertoire Temp. Vous pouvez utiliser le fichier journal pour traiter les problèmes liés à la désinstallation des composants IBM Cognos Analytics.

## Fichier journal du mode silencieux

Ce fichier est utilisé pour consigner les activités qu'IBM Cognos Configuration exécute en cours d'exécution en mode silencieux. Ce fichier journal se nomme cogconfig_response.csv et se trouve dans le répertoire *emplacement_installation*/logs.

# Annexe C. Avis sur l'obsolescence

Cette rubrique liste les fonctions qui seront obsolètes dans les éditions à venir d'IBM Cognos Analytics.

- L'utilisation du répertoire *emplacement_installation*\webapps\p2pd\WEB-INF\lib pour rechercher les pilotes JDBC sera obsolète dans les éditions à venir. Ce répertoire sera remplacé par *emplacement_installation*\drivers.

# Annexe D. A propos du présent manuel

Ce document est destiné à être utilisé avec IBM Cognos Analytics. IBM Cognos Analytics est un produit Web intégrant des fonctions de génération de rapports et de tableaux de bord, d'analyse et de gestion d'événements.

Ce guide contient des instructions relatives à l'installation, la mise à niveau, la configuration et les tests d'IBM Cognos Analytics.

## Utilisateurs concernés

Pour utiliser ce guide, vous devez être familiarisé avec un certain nombre de concepts, tels que

- La génération de rapports
- Les bases de données et les entrepôts de données
- Les problèmes de sécurité
- L'administration de base de Windows ou d'UNIX
- L'environnement serveur en place et l'infrastructure de sécurité de votre organisation

## Recherche d'informations

Pour rechercher la documentation des produits sur le Web, y compris toutes les documentations traduites, accédez au site IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter). Les mises à jour des Notes sur l'édition sont publiées sur le site IBM Knowledge Center et comprennent des liens vers les dernières notes techniques et les APAR.

Vous pouvez également lire les versions PDF des fichiers d'aide en ligne des produits en cliquant sur les liens PDF en haut de chaque page HTML, ou en accédant à la page Web de documentation des produits IBM Cognos (www.ibm.com/support/docview.wss?uid=swg27047187).

## Instructions prospectives

La présente documentation décrit les fonctionnalités actuelles du produit. Elle peut contenir des références à des éléments qui ne sont pas disponibles actuellement. Cela n'implique aucune disponibilité ultérieure de ces éléments. De telles références ne constituent en aucun cas un engagement, une promesse ou une obligation légale de fournir un élément, un code ou une fonctionnalité. Le développement, la disponibilité et le calendrier de mise à disposition des fonctions demeurent à la seule discrétion d'IBM.

## Clause de décharge relative aux exemples

La société Vacances et Aventure, Ventes VA, et toutes les variantes du nom Vacances et Aventure, ainsi que Planning Sample, décrivent des opérations métier fictives. Celles-ci contiennent des données qui servent d'exemple à IBM et à ses clients pour développer des applications d'exemple. Ces données fictives comprennent des exemples de données pour des transactions de vente, la distribution de produits, des données financières et les ressources humaines. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles

serait purement fortuite. D'autres fichiers d'exemple peuvent contenir des données fictives générées manuellement ou par une machine, des données factuelles compilées à partir de sources académiques ou publiques, ou des données utilisées avec l'autorisation du détenteur des droits d'auteur, à utiliser comme échantillon de données pour développer des exemples d'application. Les noms de produit référencés peuvent être les marques de leurs propriétaires respectifs. Toute reproduction sans autorisation est interdite.

# Index

## Nombres



## A



## B



## C

# D



# E

# F



# G



# H



# I

# J

# L



# M



# N

# O



# P



# Q

# R



# S

# T



# U



# V

## W