

IBM Cloud Identity Portal

Guide d'intégration de l'interface EAI

IBM

IBM Cloud Identity Portal

Guide d'intégration de l'interface EAI

IBM

Guide d'intégration de l'interface EAI

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)

*Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex*

© Copyright IBM France 2016. Tous droits réservés.

© **Copyright IBM Corporation 2015, 2016.**

Table des matières

Avis aux lecteurs canadiens v

**Intégration de l'interface EAI de Cloud
Identity Portal 1**

Présentation 1
Authentification et autorisation 1
 Authentification avec la norme HTTPS 2
 Authentification avec REST 2
 Vérification du statut d'authentification 3
Arrêt de session 4
 Déconnexion de WebSEAL. 4
Intégration des médias sociaux 5
 Authentification d'un utilisateur avec les médias
 sociaux 5

Authentification d'un utilisateur avec REST 6
Gestion de sessions 7
 Transfert d'une session par SMS 7
 Création d'une session de navigateur Web 7
 Récupération d'une session de navigateur Web 9
Réponses à des demandes spécifiques 9
 Pages de réponse par défaut 9
 Programme de réponse configurable 10

Remarques 11

Marques 13

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.

Intégration de l'interface EAI de Cloud Identity Portal

Intégrez Cloud Identity Portal à l'application EAI (External Authentication Interface).



L'application EAI (External Authentication Interface) prend en charge l'authentification et la gestion de sessions pour les ressources Web protégées par Cloud Identity Portal.

Présentation

Intégrez Cloud Identity Portal à l'application EAI (External Authentication Interface). Cette application prend en charge l'authentification et la gestion de sessions pour les ressources Web protégées.

Etat API

Chaque API du présent guide d'intégration EAI a un statut disponible vérifié. Les applications d'intégration EAI disponibles sont :

- Authentification avec la norme HTTPS
- Authentification avec REST
- Vérification du statut d'authentification
- Déconnexion de WebSEAL
- Authentification d'un utilisateur avec les médias sociaux
- Authentification d'un utilisateur avec REST
- Transfert d'une session qui utilise SMS
- Création d'une session de navigateur Web
- Récupération d'une session de navigateur Web

Contenu des sujets connexes :

- Réponses à des demandes spécifiques
 - Pages de réponse par défaut
 - Programme de réponse configurable

Authentification et autorisation

L'authentification utilise la norme HTTPS et REST.

REST signifie Representational State Transfer. Une API REST est un service qui traite un nombre quelconque de demandes d'autorisation : demandes des utilisateurs, groupes et membres de groupe, par exemple, pour l'accès à un serveur. Les types de demande incluent GET, POST, PUT et DELETE. Les clients ou différents types d'utilisateur du portail administratif demandent un accès en envoyant des demandes et en recevant des réponses qui utilisent les protocoles

HTTP. Le service d'API REST répond alors. Les demandes et réponses pour Cloud Identity Portal sont formatées comme objets JSON.

Les services basés sur REST sont appelés services RESTful.

Authentification avec la norme HTTPS

Authentification d'un utilisateur avec la norme HTTPS.

Méthode

POST /EAI/Login

Tentez d'authentifier un utilisateur avec un POST standard et un réacheminement de réponse.

Exemple de demande cURL

```
curl -X POST -d "username=gordita&password=IluvTr3ats!&redirect=https://your.site.com/protected/index.html&reprompt=https://your.site.com/index.html" https://gateway.domain.com/EAI/Login
```

Paramètres de demande

Tableau 1. Paramètres de demande

Nom du paramètre	Description
username	Nom de l'utilisateur.
password	Mot de passe fourni.
redirect	URL où l'utilisateur doit être envoyé.
reprompt	URL où l'utilisateur doit être envoyé en cas de tentative d'authentification infructueuse.

Résultats

200: La configuration spécifique au client peut générer un 200, avec réacheminement **JavaScript** à l'emplacement spécifié. Si la configuration spécifique au client réussit, l'utilisateur est envoyé à l'URL de réacheminement. Si la configuration spécifique au client échoue, l'utilisateur est envoyé à l'URL de nouvelle invite.

302: Réacheminement dans tous les cas.

autherror: Un paramètre de la chaîne de requête est ajouté à l'URL de nouvelle invite. L'URL de nouvelle invite indique l'erreur qui s'est produite lors de la tentative d'authentification. Si un incident se produit, WebSEAL renvoie à la page d'erreur configurée.

Authentification avec REST

Authentifiez un utilisateur avec REST.

Méthode

POST /EAI/api/login

Tentez d'authentifier un utilisateur.

Exemple de demande cURL

```
curl -X POST -H "Content-Type:application/x-www-form-urlencoded" -d
"username=gordita&password=IluvTr3ats!" https://gateway.domain.com/EAI/api/
login
```

Paramètres de demande

Tableau 2. Paramètres de demande

Nom du paramètre	Description
username	Nom de l'utilisateur.
password	Mot de passe fourni.

Exemple de réponse

```
{
"status" : "Authentication successful."
}
```

Résultats

status

200: OK pour le succès.

401: Non autorisé pour toute autre réponse.

403: Interdit si le compte est verrouillé pour une raison quelconque.

50X: Si une erreur est présente sur le serveur.

En cas de succès, les cookies de session de l'utilisateur sont aussi renvoyés.

Vérification du statut d'authentification

Vérifiez le statut d'authentification d'un utilisateur.

Méthode

GET /EAI/api/session/isAuthenticated

Essayez de contrôler le statut d'authentification d'un utilisateur.

Exemple de demande cURL

```
curl https://gateway.domain.com/EAI/api/session/isAuthenticated
```

Paramètres de demande

Aucun.

Exemple de réponse

```
{ status: "no"}
```

Résultats

200: OK pour toutes les demandes. L'attribut de statut du contenu indique si l'utilisateur est authentifié ou non.

Statut :

- `yes` : une session authentifiée est en cours.
- `no` : aucune session authentifiée n'est en cours.

Arrêt de session

Vous pouvez arrêter une session qui utilise un paramètre **WebSEAL** traditionnel. **WebSEAL** est la seule méthode d'arrêt de session disponible actuellement.

Le paramètre **WebSEAL**, `/pkmslogout`, permet la suppression de tous les cookies **WebSEAL** et efface la session de l'utilisateur. Ce dernier est réacheminé après la fin du processus.

Déconnexion de WebSEAL

Terminez une session d'utilisateur en effaçant tous les cookies de session de **WebSEAL** et en réacheminant l'utilisateur à une page d'arrivée de déconnexion.

Le réacheminement peut être configuré dans cet appel ou par le programme de réponse configurable. Si vous souhaitez utiliser le réacheminement pour que le navigateur ne soit pas réacheminé mais que les cookies soient toujours supprimés, vous pouvez encore appeler cette URL à partir d'une balise d'image masquée.

```

```

Méthode

GET `/pkmslogout`

Exemple de demande cURL

```
curl https://gateway.domain.com/pkmslogout?redirect=http://gateway.domain.com
```

Paramètres de demande

La demande concerne un contenu JSON avec les attributs suivants.

Tableau 3. Paramètres de demande

Nom du paramètre	Description
<code>redirect</code>	Emplacement où envoyer l'utilisateur une fois la session arrêtée.

Exemple de réponse

```
HTTP/1.1 302 Moved Temporarily content-length: 1680 content-type: text/html ... location: <emplacement de déconnexion> ...
Set-Cookie: PD-ID=;
Max-Age=0;
Domain=.pb.com;
Path=/; Expires="Sun, 01-Jan-1995 01:00:00 GMT"; Secure
Set-Cookie: PD-ECC=;
Max-Age=0;
Domain=.pb.com;
Path=/; Expires="Sun, 01-Jan-1995 01:00:00 GMT"; Secure
```

Résultats

status

200: OK pour le succès.

401: Non autorisé en cas d'échec pour une raison quelconque.

500: Si une erreur est présente sur le serveur. En cas de succès, la session de l'utilisateur est arrêtée sur **WebSEAL**.

Intégration des médias sociaux

Authentification d'utilisateur avec les médias sociaux.

Authentification d'un utilisateur avec les médias sociaux

Tentez d'authentifier un utilisateur en appelant les médias sociaux et en utilisant un POST classique.

Méthode

POST /EAI/Login/social/{plateforme}

plateforme correspond à la plateforme de médias sociaux pour l'authentification. Les médias sociaux sont pris en charge par Spring Social.

Prise en charge planifiée par le **fournisseur** : *facebook, google, qq, renren, wechat, weibo* et *yahoo*.

Exemple de demande cURL

```
curl -X POST -H "Content-Type: application/x-www-form-urlencoded" -d "token=123445&appId=com.your.site.app&redirect=https://your.site.com/protected/
```

```
index.html&reprompt=https://your.site.com/index.html"https://gateway.domain.com/EAI /Login/social/facebook
```

Paramètres de demande

Contenu JSON qui comporte les paramètres suivants.

Tableau 4. Paramètres de demande

Nom du paramètre	Description
token	Jeton d'accès de l'utilisateur.
appId	Identificateur d'application pré-partagée. Cet identificateur permet à Cloud Identity Service de déterminer la clé d'interface de programmation (API) à utiliser.
redirect	URL où l'utilisateur doit être envoyé en cas d'authentification réussie.
reprompt	URL où l'utilisateur doit être envoyé en cas d'authentification infructueuse.

Résultats

200: OK pour le succès. La configuration spécifique au client peut générer un 200 avec un réacheminement JavaScript. En cas de succès, l'utilisateur est

envoyé à l'URL de réacheminement. En cas d'échec, l'utilisateur est envoyé à l'URL de nouvelle invite. Un paramètre de la chaîne de requête, **autherror**, est ajouté à l'URL de nouvelle invite qui indique l'erreur survenue pendant la tentative d'authentification.

302: Réacheminement dans tous les cas.

401: Non autorisé en cas d'échec pour une raison quelconque. Les messages d'erreur sont configurables sur n'importe quelle chaîne voulue et peuvent être traduits (localisés) sur la base de l'environnement local ou de la langue préférée. Contactez le responsable de la distribution IBM® pour plus de détails sur la personnalisation de ce paramètre **401 unauthorized** pour toute autre réponse.

En cas de succès, les cookies de session de l'utilisateur sont aussi renvoyés.

Authentification d'un utilisateur avec REST

Tentez d'authentifier un utilisateur en appelant les médias sociaux et l'API REST.

Méthode

POST /EAI/api/login/social/{plateforme}

La plateforme correspond à la **plateforme** de médias sociaux pour l'authentification. Les médias sociaux sont pris en charge par Spring Social.

Prise en charge planifiée par le **fournisseur** : *facebook, google, qq, renren, wechat, weibo et yahoo*.

Exemples de demandes cURL

```
curl -X POST -d '{"token":"123445","appId":"com.your.site.app"}' -H "Content-Type: application/json" https://gateway.domain.com/EAI/api/login/social/facebook
```

```
curl -X POST -H "Content-Type: application/json" "https://gateway.domain.com/EAI/api/login/social/yahoo?token=12345&appId=com.your.site.app"
```

Paramètres de demande

Type de contenu : **application/json**.

Tableau 5. Paramètres de demande

Nom du paramètre	Description
token	Jeton d'accès de l'utilisateur.
appId	Identificateur d'application partagée. Cet identificateur permet à Cloud Identity Service de déterminer la clé d'interface de programmation (API) à utiliser.

Exemple de réponse

```
{status: success}
```

Résultats

200: OK pour le succès.

401: Non autorisé en cas d'échec pour une raison quelconque.

403: Interdit si le compte de médias sociaux de l'utilisateur est incomplet et qu'aucun profil utilisateur ne peut être créé.

500: Si une erreur est présente sur le serveur.

En cas de succès, les cookies de session de l'utilisateur sont aussi renvoyés.

Gestion de sessions

Création, transfert et récupération de sessions.

Transfert d'une session par SMS

Une fois qu'un utilisateur est déjà authentifié, crée une session dans un nouveau domaine DNS (Domain Name Service, service de noms de domaine).

Une session valide doit exister. L'environnement doit être configuré pour le service SMS (Short Message Service).

Méthode

POST /EAI/api/session/resumeSession

Exemple de demande cURL

```
curl -X POST -d "sessionID=123456&redirect=https://your.site.com/protectedResource" https://gateway.domain.com/EAI/api/session/resumeSession
```

Paramètres de demande

Les demandes incluent un contenu JSON qui comporte les paramètres suivants.

Tableau 6. Paramètres de demande

Nom du paramètre	Description
sessionID	ID session SMS de l'utilisateur.
redirect	URL où envoyer l'utilisateur après avoir repris la session.

Résultats

200: La configuration spécifique au client peut générer un **200**, avec réacheminement **JavaScript:** à l'emplacement spécifié.

302: Réacheminement.

Failure: Si un incident se produit, **WebSEAL** renvoie à la page d'erreur configurée.

En cas de succès, les cookies de session de l'utilisateur sont aussi renvoyés.

Création d'une session de navigateur Web

Créez une session de navigateur Web à partir du jeton de vérification de session.

Créez une session Web pour le domaine en cours. La création d'une session Web nécessite que l'utilisateur soit déjà authentifié par l'API **GmaApi** et qu'un jeton de vérification de session existe pour l'utilisateur.

Méthode

[GET | POST]

/EAI/api/session/createSessionFromToken

Exemple de demande cURL

```
curl -X POST -d "token=7470f51f-2f5f-470e-8bea-402ae678bafb
&redirect=https://your.site.com/protectedResource" https://
gateway.domain.com/EAI/api/session/createSessionFromToken
```

Paramètres de demande

Contenu JSON qui comporte les paramètres suivants.

Tableau 7. Paramètres de demande

Nom du paramètre	Description
token	Facultatif. Valeur sessionVerificationToken de l'utilisateur, si vous créez une session pour un utilisateur qui s'est authentifié par GmaApi .
redirect	Facultatif. URL où envoyer l'utilisateur après avoir repris la session.

Résultats

200: La configuration spécifique au client peut générer un **200** avec réacheminement **JavaScript:** à l'emplacement spécifié.

302: Réacheminement.

LSG-SESSION-ID: Cookie LSG-SESSION-ID qui représente le descripteur d'ID session SMS de l'utilisateur.

WebSEAL: Cookies de la session **WebSEAL** (PD-S-SESSION-ID) de l'utilisateur. Si un incident se produit, **WebSEAL** renvoie à la page d'erreur configurée.

Exemple de séquence de commandes

1. Authentifiez l'utilisateur en appelant les données de formulaire **username** et **password** :

```
curl -X POST -H "Content-Type:application/x-www-form-urlencoded" -H
"Authorization: Basic ZWFpLWNSaWVudDo=" -d "grant_type=password
&username=ID_utilisateur&password=mot_passe_utilisateur"
https://gateway.domain.com/EAI/oauth/tokenOù la valeur ID_utilisateur est
la valeur d'attribut gtwyPrincipalName et mot_passe_utilisateur est la valeur
d'attribut du mot de passe de l'utilisateur.
```

2. Emettez une demande GET en plaçant le jeton **OAuthbearer** renvoyé depuis l'étape 1 dans l'**en-tête d'authentification** :

```
curl -H "Authorization: Bearer 56d512a9-4fa34ac6-a72a-76d66ed84d21"
https://gateway.domain.com/EAI/api/me/startWebSession
```


3. Émettez une demande GET en plaçant la valeur **entry** renvoyée dans la **chaîne de requête**. Utilisez le nom de zone **token** pour cette valeur :

```
curl https://gateway.domain.com/EAI/api/session/  
createSessionFromToken?token =4683caf7-c937-4edc-8105-bfa075f4d6ff -v
```

Le résultat inclut ici **PD-S-SESSION-ID** qui peut être utilisé pour **getSession**.

Remarque : Des différences de syntaxe existent entre les systèmes d'exploitation : Windows, Linux et Mac. Par exemple, sous Windows, les guillemets ne sont pas nécessaires.

Récupération d'une session de navigateur Web

Récupère le cookie de service SMS (Short Message Service) pour la session de l'utilisateur.

Nécessite que l'utilisateur soit authentifié par l'interface EAI (External Application Interface).

Méthode

[POST] /EAI/api/session/getSession

Exemple de demande cURL

```
curl https://gateway.domain.com/EAI/api/session/getSession
```

Paramètres de demande

Aucun.

Résultats

200: OK pour le succès.

LSG-SESSION-ID: Cookie LSG-SESSION-ID qui représente le descripteur d'ID session SMS de l'utilisateur.

Réponses à des demandes spécifiques

L'interface EAI détermine la page correcte à fournir en réponse à des demandes spécifiques.

Pages de réponse par défaut

Pour un ensemble d'opérations spéciales, l'interface EAI comprend un composant appelé **programme de réponse** qui détermine la page correcte à fournir.

Par exemple, supposez qu'un utilisateur essaie d'accéder à une ressource protégée mais doit d'abord s'authentifier. **WebSEAL** envoie une demande au **programme de réponse** indiquant que l'utilisateur doit se connecter. Le **programme de réponse** fournit alors la page de connexion. Ces pages de connexion et les autres pages d'authentification sont configurables pour chaque domaine. D'autre part, l'équipe de services peut fournir des modèles de page d'authentification.

Les pages d'authentification sont :

- **Connexion**

- **Déconnexion**
- **Changement de mot de passe** (pour les mots de passe expirés)
- **Changement de mot de passe réussi**, page présentée uniquement lorsqu'un utilisateur n'a pas d'autre ressource.
- **Erreur**, pour les erreurs de serveur **WebSEAL** uniquement.
- **Authentification à un niveau de sécurité supérieur**, uniquement pour l'authentification renforcée.
- **Aide**, pour les opérations que **WebSEAL** ne peut pas prendre en charge.

Programme de réponse configurable

Au lieu d'utiliser les pages par défaut, le **programme de réponse** peut également être configuré pour renvoyer à un emplacement du choix du client.

Pour chaque opération prise en charge, le **programme de réponse** peut être configuré pour analyser l'URL de référence entrante, pour déterminer si cette URL correspond à un modèle particulier et pour réacheminer le navigateur vers un emplacement configuré.

Consultez le tableau suivant des destinations des opérations :

Tableau 8. Destinations des opérations

Opération	Référencement	Destination
connexion	https://*.foo.com	https://www.foo.com/login
déconnexion	https://*.foo.com	https://www.foo.com/logout
mot de passe	https://*.foo.com	https://www.foo.com/selfservice
post-connexion	https://*.foo.com	https://www.foo.com/postlogin

Comme décrit dans le tableau, l'**URL référente** peut comporter des caractères génériques sur la base d'expressions régulières. Si cette fonction de caractères génériques est activée et qu'une **opération** et un **référent** correspondent à une destination, le navigateur est envoyé vers l'URL de destination. Celle-ci inclut l'**URL référente** comme paramètre de **chaîne de requête**.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Pour les demandes de licence concernant les informations utilisant un jeu de caractères à double octet (DBCS), prenez contact avec le service Propriété intellectuelle IBM dans votre pays, ou envoyez des demandes, en écrivant à :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales. 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. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, apporter des améliorations et/ou modifications aux produits et/ou programmes décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 79758 U.S.A

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions du Livret Contractuel IBM, des Conditions Internationales d'Utilisation de Logiciels IBM ou de tout autre contrat équivalent.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web «Copyright and trademark information» à l'adresse www.ibm.com/legal/copytrade.shtml.

Java™ ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.



Imprimé en France