IBM Cloud Identity Portal

Handbuch zur EAI-Integration

IBM Cloud Identity Portal

Handbuch zur EAI-Integration

Handbuch zur EAI-Integration

Inhaltsverzeichnis

EAI-Integration von Cloud Identity Portal

Integrieren Sie Cloud Identity Portal in die Anwendung "External Authentication Interface" (EAI).

Die Anwendung "External Authentication Interface" (EAI) ist für das Authentifizierungs- und Sitzungsmanagement für Webressourcen verantwortlich, die durch Cloud Identity Portal geschützt werden.

Übersicht

Integrieren Sie Cloud Identity Portal in die Anwendung "External Authentication Interface" (EAI). Die Anwendung "EAI" ist für das Authentifizierungs- und Sitzungsmanagement für geschützte Webressourcen verantwortlich.

API-Status

Jede API in diesem Handbuch zur EAI-Integration hat einen bestätigten Verfügbarkeitsstatus. Folgende EAI-Anwendungen sind verfügbar:

- Mit Standard-HTTPS authentifizieren
- Mit REST authentifizieren
- Authentifizierungsstatus überprüfen
- WebSEAL-Abmeldung
- Einen Benutzer mit Social Media authentifizieren
- Einen Benutzer mit Social Media mit REST authentifizieren
- Eine Sitzung übertragen, die SMS verwendet
- Eine Web-Browser-Sitzung erstellen
- Eine Web-Browser-Sitzung abrufen

Zugehörige Themen sind:

- Antworten auf bestimmte Anforderungen
  - Standardantwortseiten
  - Konfigurierbarer Responder

Authentifizierung und Autorisierung

Die Authentifizierung verwendet Standard-HTTPS und -REST.

REST steht für "Representational State Transfer". Eine REST-API ist ein Service, der eine beliebige Anzahl an Autorisierungsanforderungen bearbeitet. Diese Anforderungen stammen von Benutzern, Gruppen und Gruppenmitgliedern, die z. B. Zugriff auf einen Server benötigen. Zu den Anforderungstypen gehören "GET", "POST", "PUT" und "DELETE". Clients oder unterschiedliche Typen von Benutzern des Verwaltungsportals fordern den Zugriff durch Senden von Anforderungen und

Empfangen von Antworten an, die jeweils HTTP-Protokolle verwenden. Anschließend sendet der REST-API-Service eine Antwort. Anforderungen und Antworten für Cloud Identity Portal werden als JSON-Objekte formatiert.

Ein Service, der auf REST basiert, wird als "REST-konformer Service" bezeichnet.

Mit Standard-HTTPS authentifizieren

Ein Benutzer kann mit Standard-HTTPS authentifiziert werden.

Methode

```
POST /EAI/Login
```

Versucht, einen Benutzer mit einem Standard-POST und einer Antwortweiterleitung zu authentifizieren.

cURL-Beispielanforderung

```
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
```

Anforderungsparameter

Tabelle 1. Anforderungsparameter

Parametername	Beschreibung
username	Der **username** (Benutzername) des Benutzers.
password	Das angegebene **password** (Kennwort).
redirect	Die URL, zu der der Benutzer nach einer erfolgreichen Authentifizierung weitergeleitet wird.
reprompt	Die URL, zu der der Benutzer nach einem fehlgeschlagenen Authentifizierungsversuch weitergeleitet wird.

Gibt zurück

200: Eine kundenspezifische Konfiguration gibt möglicherweise "200" mit einer **JavaScript**-Weiterleitung zu der angegebenen Position zurück. Wenn die kundenspezifische Konfiguration erfolgreich ist, wird der Benutzer zu der Weiterleitungs-URL geleitet. Wenn die kundenspezifische Konfiguration fehlschlägt, wird der Benutzer zu einer URL mit einer erneuten Eingabeaufforderung weitergeleitet.

302: Weiterleitung in allen Fällen.

autherror: Ein Parameter für eine Abfragezeichenfolge wird an die URL mit einer erneuten Eingabeaufforderung angehängt. Die URL mit der erneuten Eingabeaufforderung gibt den Fehler an, der beim Authentifizierungsversuch aufgetreten ist. Wenn ein Fehler auftritt, leitet WebSEAL die Anforderung zur konfigurierten Fehlerseite weiter.

Mit REST authentifizieren

Ein Benutzer kann mit REST authentifiziert werden.

Methode

```
POST /EAI/api/login
```

Versucht, einen Benutzer zu authentifizieren.

cURL-Beispielanforderung

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

Anforderungsparameter

Tabelle 2. Anforderungsparameter

Parametername	Beschreibung
username	Der **username** (Benutzername) des Benutzers.
password	Das angegebene **password** (Kennwort).

Beispielantwort

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

Gibt zurück

status

200: OK bedeutet Erfolg.

401: Nicht berechtigt für jede andere Antwort.

403: Nicht zulässig, falls der Account aus irgendeinem Grund gesperrt ist.

50X: Wenn ein Fehler auf dem Server aufgetreten ist.

Bei Erfolg werden die Sitzungscookies des Benutzers ebenfalls zurückgegeben.

Authentifizierungsstatus überprüfen

Überprüfung des Authentifizierungsstatus eines Benutzers.

Methode

```
GET /EAI/api/session/isAuthenticated
```

Versucht, den Authentifizierungsstatus eines Benutzers zu überprüfen.

cURL-Beispielanforderung

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

Anforderungsparameter

Keine.

Beispielantwort

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

Gibt zurück

200: OK für alle Anforderungen. Das Statusattribut der Nutzdaten gibt an, ob der Benutzer authentifiziert ist oder nicht.

Status:

- yes: Eine authentifizierte Sitzung ist aktiv.
- no: Es ist keine authentifizierte Sitzung aktiv.

Beendigung der Sitzung

Sie können eine Sitzung beenden, die traditionelles **WebSEAL** verwendet. **WebSEAL** ist die einzige Methode zur Beendigung von Sitzungen, die derzeit verfügbar ist.

WebSEAL und /pkmslogout ermöglichen das Entfernen aller **WebSEAL**-Cookies und das Löschen der Sitzung des Benutzers. Sobald der Prozess abgeschlossen ist, wird der Benutzer umgeleitet.

WebSEAL-Abmeldung

Beendet die Sitzung eines Benutzers, löscht alle **WebSEAL**-Sitzungscookies und leitet den Benutzer zu einer Abmeldungs-Landing-Page weiter.

Die Weiterleitung kann entweder in diesem Aufruf oder über den konfigurierbaren Responder konfiguriert werden. Wenn Sie die Weiterleitung so verarbeiten möchten, dass der Browser nicht weitergeleitet wird, die Cookies aber dennoch entfernt werden, können Sie diese URL trotzdem aus einem verdeckten Bildtag heraus aufrufen.

```
<img src="/pkmslogout" style="display:none" height="1" width="1" />
```

Methode

```
GET /pkmslogout
```

cURL-Beispielanforderung

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

Anforderungsparameter

Die Anforderung gilt für JSON-Nutzdaten, die die folgenden Parameter enthalten.

Tabelle 3. Anforderungsparameter

Parametername	Beschreibung
redirect	Die Position, zu der der Benutzer weitergeleitet wird, wenn die Sitzung beendet wird.

Beispielantwort

```
HTTP/1.1 302 Moved Temporarily content-length: 1680 content-type:
text/html ... location: <logout location> ...
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
```

Gibt zurück

status

200: OK bedeutet Erfolg.

401: Nicht berechtigt, falls die Anforderung aus irgendeinem Grund fehlgeschlagen ist.

500: Wenn ein Fehler auf dem Server aufgetreten ist. Bei Erfolg wird die Sitzung des Benutzers in **WebSEAL** beendet.

Social-Media-Integration

Benutzerauthentifizierung über Social Media.

Einen Benutzer mit Social Media authentifizieren

Versucht, einen Benutzer durch Aufruf von Social Media und durch ein traditionelles POST zu authentifizieren.

Methode

```
POST /EAI/Login/social/{platform}
```

platform entspricht der Social-Media-Plattform für die Authentifizierung. Unterstützung für Social Media wird durch Spring Social bereitgestellt.

Unterstützung für folgende **provider** ist geplant: *facebook*, *google*, *qq*, *renren*, *wechat*, *weibo* und *yahoo*.

cURL-Beispielanforderung

```
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
```

Anforderungsparameter

JSON-Nutzdaten, die die folgenden Parameter enthalten.

Tabelle 4. Anforderungsparameter

Parametername	Beschreibung
token	Das **token** für den Zugriff des Benutzers.
appId	Eine zuvor geteilte Anwendungs-ID, die Cloud Identity Service ermöglicht zu bestimmen, welcher API-Schlüssel verwendet werden soll.

Tabelle 4. Anforderungsparameter (Forts.)

Parametername	Beschreibung
redirect	Die URL, zu der der Benutzer nach einer erfolgreichen Authentifizierung weitergeleitet wird.
reprompt	Die URL, zu der der Benutzer nach einem fehlgeschlagenen Authentifizierungsversuch weitergeleitet wird.

Gibt zurück

200: OK bedeutet Erfolg. Eine kundenspezifische Konfiguration gibt möglicherweise "200" mit einer JavaScript-Weiterleitung zurück. Bei Erfolg (`success`) wird der Benutzer zur Weiterleitungs-URL geleitet. Bei Fehlschlagen (`failure`) wird der Benutzer zu einer URL mit einer erneuten Eingabeaufforderung weitergeleitet. Ein Parameter für eine Abfragezeichenfolge (**autherror**) wird an die URL mit einer erneuten Eingabeaufforderung angehängt. Er gibt den Fehler an, der beim Authentifizierungsversuch aufgetreten ist.

302: Weiterleitung in allen Fällen.

401: Nicht berechtigt, falls die Anforderung aus irgendeinem Grund fehlgeschlagen ist. Fehlernachrichten sind als jede beliebige Zeichenfolge konfigurierbar und können basierend auf der Ländereinstellung oder der bevorzugten Sprache übersetzt (lokalisiert) werden. Wenden Sie sich an die zuständige IBM® Delivery-Kundenkontaktadresse, um Details zur Anpassung von **401 unauthorized** für andere Antworten zu erhalten.

Bei Erfolg werden die Sitzungscookies des Benutzers ebenfalls zurückgegeben.

Einen Benutzer mit Social Media mit REST authentifizieren

Versucht, einen Benutzer durch Aufruf von Social Media und die REST-API zu authentifizieren.

Methode

```
POST /EAI/api/login/social/{platform}
```

Die Plattform entspricht der Social-Media-Plattform (**platform**), die für die Authentifizierung verwendet werden sollen. Unterstützung für Social Media wird durch Spring Social bereitgestellt.

Unterstützung für folgende **provider** ist geplant: *facebook*, *google*, *qq*, *renren*, *wechat*, *weibo* und *yahoo*.

cURL-Beispielanforderungen

```
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"
```

Anforderungsparameter

Inhaltstyp: **application/json**.

Tabelle 5. Anforderungsparameter

Parametername	Beschreibung
token	Das Token für den Benutzerzugriff.
appId	Eine geteilte Anwendungs-ID, die Cloud Identity Service ermöglicht zu bestimmen, welcher API-Schlüssel verwendet werden soll.

Beispielantwort

```
{status: success}
```

Gibt zurück

200: OK bedeutet Erfolg.

401: Nicht berechtigt, falls die Anforderung aus irgendeinem Grund fehlgeschlagen ist.

403: Nicht zulässig, wenn der Social-Media-Account des Benutzers unvollständig ist und kein Benutzerprofil erstellt werden kann.

500: Wenn ein Fehler auf dem Server aufgetreten ist.

Bei Erfolg werden die Sitzungscookies des Benutzers ebenfalls zurückgegeben.

Sitzungsmanagement

Sitzungen werden erstellt, übertragen und abgerufen.

Eine Sitzung mithilfe von SMS übertragen

Wenn ein Benutzer bereits authentifiziert ist, wird eine Sitzung in einer neuen DNS-Domäne (Domain Name Service) erstellt.

Es muss eine gültige Sitzung vorhanden sein. Die Umgebung muss für SMS (Short Message Service) konfiguriert sein.

Methode

```
POST /EAI/api/session/resumeSession
```

cURL-Beispielanforderung

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

Anforderungsparameter

Eine Anforderung umfasst JSON-Nutzdaten, die die folgenden Parameter enthalten.

Tabelle 6. Anforderungsparameter

Parametername	Beschreibung
sessionID	Die SMS-Sitzungs-ID des Benutzers.
redirect	Die URL, zu der der Benutzer weitergeleitet werden soll, nachdem Sie die Sitzung wiederaufgenommen haben.

Gibt zurück

200: Eine kundenspezifische Konfiguration gibt möglicherweise **200** mit einer **JavaScript:**-Weiterleitung zu der angegebenen Position zurück.

302: Weiterleitung.

Failure: Wenn ein Fehler auftritt, leitet **WebSEAL** die Anforderung zur konfigurierten Fehlerseite weiter.

Bei Erfolg werden die Sitzungscookies des Benutzers ebenfalls zurückgegeben.

Eine Web-Browser-Sitzung erstellen

Sie können eine Web-Browser-Sitzung aus dem Sitzungsverifizierungstoken erstellen.

Sie erstellen eine Websitzung für die aktuelle Domäne. Zum Erstellen einer Websitzung ist es erforderlich, dass der Benutzer bereits über die **GmaApi** authentifiziert ist und dass ein Sitzungsverifizierungstoken für den Benutzer vorhanden ist.

Methode

```
[GET | POST]

/EAI/api/session/createSessionFromToken
```

cURL-Beispielanforderung

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

Anforderungsparameter

JSON-Nutzdaten, die die folgenden Parameter enthalten.

Tabelle 7. Anforderungsparameter

Parametername	Beschreibung
token	Optional. Der Wert für **sessionVerificationToken** für den Benutzer, wenn Sie eine Sitzung für einen Benutzer erstellen, der über die **GmaApi** authentifiziert wurde.
redirect	Optional. Die URL, zu der der Benutzer weitergeleitet werden soll, nachdem Sie die Sitzung wiederaufgenommen haben.

Gibt zurück

200:. Eine kundenspezifische Konfiguration gibt möglicherweise **200** mit einer **JavaScript:**-Weiterleitung zu der angegebenen Position zurück.

302: Weiterleitung.

LSG-SESSION-ID: Das LSG-SESSION-ID-Cookie, das den SMS-Sitzungs-ID-Handle des Benutzers darstellt.

WebSEAL: Sitzungscookies für die **WebSEAL**-Sitzung (PD-S-SESSION-ID) des Benutzers. Wenn ein Fehler auftritt, leitet **WebSEAL** die Anforderung zur konfigurierten Fehlerseite weiter.

Beispielbefehlsfolge

1. Der Benutzer wird durch Aufrufen der Formulardaten für **username** und **password** authentifiziert:
   `curl -X POST -H "Content-Type:application/x-www-form-urlencoded" -H "Authorization: Basic ZWFpLWNsaWVudDo=" -d "grant_type=password &username=`*userid*`&password=`*user_password*`" https://gateway.domain.com/EAI/oauth/token`Dabei steht der Wert **userid** für den Attributwert **gtwyPrincipalName** des Benutzers und **user_password** für den Attributwert des Kennworts des Benutzers.
2. Eine GET-Anforderung wird gesendet, die das Token **OAuthbearer**, das in Schritt 1 zurückgegeben wurde, in den **Authentication Header** positioniert:
   `curl -H "Authorization: Bearer `*56d512a9-4fa34ac6-a72a-76d66ed84d21*`" https://gateway.do main.com/EAI/api/me/startWebSession`
3. Eine GET-Anforderung wird gesendet, die den zurückgegebenen Wert für **entry** in der Abfragezeichenfolge (**query string**) positioniert. Verwenden Sie einen Feldnamen von **token** für diesen Wert:
   `curl https://gateway.domain.com/EAI/api/session/createSessionFromToken?token =`*4683caf7-c937-4edc-8105-bfa075f4d6ff* `-v`

Die Rückgabe darauf enthält eine **PD-S-SESSION-ID**, die für **getSession** verwendet werden kann.

Anmerkung: Es gibt Unterschiede in der Syntax zwischen den folgenden Betriebssystemen: Windows, Linux und Mac. In Windows sind z. B. keine Anführungszeichen erforderlich.

Eine Web-Browser-Sitzung abrufen

Ruft das SMS-Cookie (Short Message Service) für die Sitzung des Benutzers ab.

Es ist erforderlich, dass der Benutzer über die EAI (External Application Interface) authentifiziert wird.

Methode

`[POST] /EAI/api/session/getSession`

cURL-Beispielanforderung

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

Anforderungsparameter

Keine.

Gibt zurück

200: OK bedeutet Erfolg.

LSG-SESSION-ID: Das LSG-SESSION-ID-Cookie, das den SMS-Sitzungs-ID-Handle des Benutzers darstellt.

Antworten auf bestimmte Anforderungen

Die EAI bestimmt die richtige Seite, die als Antwort auf bestimmte Anforderungen bereitgestellt wird.

Standardantwortseiten

Für besondere Operationen bietet die EAI eine Komponente, die als **Responder** bezeichnet wird. Sie bestimmt die richtige Seite, die bereitgestellt werden soll.

Beispiel: Angenommen, ein Benutzer versucht, auf eine geschützte Ressource zuzugreifen. Er muss sich jedoch zuerst authentifizieren. **WebSEAL** sendet eine Anforderung an den **Responder**, die angibt, dass sich der Benutzer anmelden muss. Der **Responder** stellt daraufhin die Anmeldeseite bereit. Diese Anmeldeseiten sowie andere Authentifizierungsseiten sind für jede Domäne konfigurierbar. Das Service-Team kann Authentifizierungsseitenvorlagen bereitstellen.

Die Authentifizierungsseiten lauten wie folgt:

- **Login**
- **Logout**
- **Password change** (für abgelaufene Kennwörter)
- **Successful password change** wird nur angezeigt, wenn ein Benutzer nicht über andere Ressourcen verfügt.
- **Error**, nur für **WebSEAL**-Serverfehler.
- **Step-up**, nur für erweiterte Authentifizierung.
- **Help**, für Operationen, für die **WebSEAL** keinen Service bereitstellen kann.

Konfigurierbarer Responder

Anstatt für die Verwendung der Standardseiten kann der **Responder** auch für die Weiterleitung zu einer vom Kunden ausgewählten Position konfiguriert werden.

Für jede unterstützte Operation kann der **Responder** konfiguriert werden, die eingehende Referrer-URL zu analysieren, zu bestimmen, ob diese URL mit einem bestimmten Muster übereinstimmt, und den Browser zu einer konfigurierten Position weiterzuleiten.

Weitere Informationen finden Sie in der folgenden Operationszieltabelle:

Tabelle 8. Operationsziele

Operation	Referrer	Ziel
login	`https://*.foo.com`	`https://www.foo.com/login`
logout	`https://*.foo.com`	`https://www.foo.com/logout`

Tabelle 8. Operationsziele (Forts.)

Operation	Referrer	Ziel
password	`https://*.foo.com`	`https://www.foo.com/selfservice`
postlogin	`https://*.foo.com`	`https://www.foo.com/postlogin`

Wie in der Tabelle beschrieben, kann die **Referrer URL** ein Platzhalter sein, der auf regulären Ausdrücken basiert. Wenn diese Platzhalterfunktion aktiviert ist und eine bestimmte **Operation** und ein **Referrer** mit einem Ziel übereinstimmt, wird der Browser zu der betreffenden Ziel-URL weitergeleitet. Die Ziel-URL umfasst die **Referrer URL** als einen Parameter vom Typ **Query String** (Abfragezeichenfolge).

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
2Z4A/101

11400 Burnet Road
Austin, TX 79758
U.S.A

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesen Informationen beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Java™ und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Linux ist eine Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Gedruckt in Deutschland