IBM Security Directory Server
Version 6.3.1.5

Berichterstellung

SC43-1260-00

IBM Security Directory Server
Version 6.3.1.5

Berichterstellung

SC43-1260-00

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen in „Bemerkungen" auf Seite 19 gelesen werden.

Impressum

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Security Directory Server, Version 6.3.1.2, Reporting Guide,
IBM Form SC27-6531-00,
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2014

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
TSC Germany
Kst. 2877
Juni 2014

Inhaltsverzeichnis

Informationen zu dieser Veröffentlichung

IBM® Security Directory Server, früher bekannt als IBM Tivoli Directory Server, ist eine IBM Implementierung von Lightweight Directory Access Protocol für folgende Betriebssysteme:

- Microsoft Windows
- AIX
- Linux (System x, System z, System p und System i)
- Solaris
- Hewlett-Packard UNIX (HP-UX) (Itanium)

IBM Security Directory Server Berichterstellung enthält Informationen zu den Tools und der Software zum Generieren von Verzeichnisserverberichten.

Zugriff auf Veröffentlichungen und Terminologie

Dieser Abschnitt enthält Folgendes:

- Liste der Veröffentlichungen in der „IBM Security Directory Server-Bibliothek"
- Links zu „Onlineveröffentlichungen" auf Seite vi
- Link auf die „IBM Terminologiewebsite" auf Seite vii

IBM Security Directory Server-Bibliothek

Die Bibliothek von IBM Security Directory Server umfasst die folgenden Veröffentlichungen:

- *IBM Security Directory Server Version 6.3.1.5 Produktübersicht*, IBM Form GC12-5009-01

  Diese Veröffentlichung enthält Informationen zu dem Produkt IBM Security Directory Server, zu neuen Features im aktuellen Release sowie zu den Systemanforderungen.
- *IBM Security Directory Server Version 6.3.1.5 Leitfaden für den Schnelleinstieg*, IBM Form GI11-3259-02

  Diese Veröffentlichung enthält Informationen, die Ihnen den Einstieg in IBM Security Directory Server erleichtern. Sie umfasst eine kurze Produktbeschreibung und ein Diagramm zur Architektur sowie Verweise auf die Website mit der Produktdokumentation und Installationsanweisungen.
- *IBM Security Directory Server Version 6.3.1.5 Installation und Konfiguration*, IBM Form SC12-4464-02

  Diese Veröffentlichung enthält umfassende Informationen zur Installation, Konfiguration und Deinstallation von IBM Security Directory Server. Außerdem enthält sie Informationen zur Durchführung eines Upgrades von einer Vorgängerversion des Produkts auf die aktuelle Version von IBM Security Directory Server.
- *IBM Security Directory Server Version 6.3.1.5 Verwaltung*, IBM Form SC12-4463-02

  Diese Veröffentlichung enthält Anweisungen zur Ausführung von Administratortasks über das Webverwaltungstool und die Befehlszeile.
- *IBM Security Directory Server Version 6.3.1.5 Berichterstellung*, IBM Form SC43-1260-00

Diese Veröffentlichung enthält Beschreibungen der Tools und Software zur Berichterstellung für IBM Security Directory Server.

- *IBM Security Directory Server Version 6.3.1.5 Command Reference*, IBM Form SC27-2753-02

  Diese Veröffentlichung enthält eine Beschreibung der Syntax und der Verwendung der Befehlszeilendienstprogramme, die zum Lieferumfang von IBM Security Directory Server gehören.

- *IBM Security Directory Server Version 6.3.1.5 Server Plug-ins Reference* , IBM Form SC27-2750-02

  Diese Veröffentlichung enthält Informationen zum Schreiben von Server-Plug-ins.

- *IBM Security Directory Server Version 6.3.1.5 Programming Reference*, IBM Form SC27-2754-02

  Diese Veröffentlichung enthält Informationen zum Schreiben von LDAP-Clientanwendungen (LDAP = Lightweight Directory Access Protocol) in C und in Java™.

- *IBM Security Directory Server Version 6.3.1.5 Performance Tuning and Capacity Planning Guide*, IBM Form SC27-2748-02

  Diese Veröffentlichung enthält Informationen zur Optimierung des Verzeichnisservers zur Erzielung einer besseren Systemleistung. Sie beschreibt die erforderliche Plattenspeicherkapazität und andere Hardwareanforderungen für Verzeichnisse unterschiedlicher Größe und mit unterschiedlichem Aufkommen an Schreib- und Leseoperationen. In der Veröffentlichung werden außerdem bereits bekannte Arbeitsszenarios für die unterschiedlichen Verzeichnisebenen beschrieben. Darüber hinaus finden Sie dort Informationen zum benötigte Platten- und Hauptspeicherplatz und allgemeine Empfehlungen.

- *IBM Security Directory Server Version 6.3.1.5 Troubleshooting Guide*, IBM Form GC27-2752-02

  Diese Veröffentlichung enthält Informationen zu möglicherweise auftretenden Problemen und zu den Fehlerbehebungsmaßnahmen, die Sie ausführen können, bevor Sie sich an die zuständige IBM Softwareunterstützungsfunktion wenden.

- *IBM Security Directory Server Version 6.3.1.5 Error Message Reference*, IBM Form GC27-2751-02

  Diese Veröffentlichung enthält eine Liste aller Warn- und Fehlernachrichten zu IBM Security Directory Server.

Onlineveröffentlichungen

IBM veröffentlicht an den folgenden Positionen Informationen, wenn das Produkt freigegeben wird und wenn die Veröffentlichungen aktualisiert werden:

Website mit der IBM Security Directory Server-Dokumentation
Unter http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm wird die Begrüßungsseite der Dokumentation zu diesem Produkt angezeigt.

IBM Security Systems Documentation Central und Begrüßungsseite
IBM Security Systems Documentation Central stellt eine alphabetische Liste der gesamten Produktdokumentation zu IBM Security Systems bereit. Außerdem finden Sie Links zur Produktdokumentation zu bestimmten Versionen der einzelnen Produkte.

Die Dokumentation unter Welcome to IBM Security Systems enthält eine Einführung in die Dokumentation zu IBM Security Systems sowie Links und allgemeine Informationen zu dieser Dokumentation.

IBM Publication Center
Die Site http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss bietet angepasste Suchfunktionen, mit deren Hilfe Sie alle benötigten IBM Veröffentlichungen auffinden.

IBM Terminologiewebsite

Die IBM Terminologiewebsite konsolidiert die Terminologie von Produktbibliotheken an einer zentralen Position. Der Zugriff auf die Terminologiewebsite erfolgt unter: http://www.ibm.com/software/globalization/terminology.

Eingabehilfen

Die Eingabehilfefunktionen unterstützen Benutzer mit körperlichen Behinderungen wie z. B. eingeschränkter Beweglichkeit oder eingeschränktem Sehvermögen beim erfolgreichen Einsatz von Softwareprodukten. Das vorliegende Produkt unterstützt behindertengerechte Tools, die die Elemente der Benutzerschnittstelle ansagen und die Navigation in dieser Schnittstelle vereinfachen. Sie können die Funktionen der grafischen Benutzerschnittstelle anstatt mit der Maus auch über die Tastatur aufrufen.

Weitere Informationen finden Sie in der *Produktübersicht für IBM Security Directory Server* im Anhang zu den Eingabehilfen.

Technische Schulung

Informationen zur technischen Schulung finden Sie auf der folgenden IBM Schulungswebsite unter: http://www.ibm.com/software/tivoli/education.

Informationen zur Unterstützung

IBM Support bietet Unterstützung bei Codeproblemen und kurzen Routinefragen zur Installation oder Verwendung. Sie können auf die Website "IBM Software Support" direkt unter der Adresse http://www.ibm.com/software/support/probsub.html zugreifen.

Die Veröffentlichung *IBM Security Directory Server Troubleshooting Guide* enthält Details zu folgenden Punkten:

- Informationen, die vor der Kontaktaufname mit IBM Support erfasst werden müssen
- Verschiedene Methoden zur Kontaktaufname mit IBM Support
- Verwendung von IBM Support Assistant
- Anweisungen und Fehlerbestimmungsressourcen zum eigenständigen Eingrenzen und Beheben eines Problems

Anmerkung: Die Registerkarte **Community and Support** im Information Center des Produkts kann weitere Unterstützungsressourcen bereitstellen.

Erklärung zu geeigneten Sicherheitsvorkehrungen

Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Vorbeugung, Erkennung und Reaktion auf unbefugten Zugriff innerhalb des Unternehmens und von außen. Unbefugter Zugriff kann dazu führen, dass Informationen geändert, gelöscht, veruntreut oder missbräuchlich verwendet werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Attacken. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine unbefugte Verwendung oder einen unbefugten Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines umfassenden Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vor zerstörerischen oder unzulässigen Handlungen Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vor zerstörerischen oder unzulässigen Handlungen Dritter schützen.

Prüfberichterstellung in IBM Security Directory Server

Mit IBM Security Directory Server werden die Tools und die Software zum Generieren von Prüfberichten bereitgestellt, die auf den Prüfprotokolldateien basieren.

Anwendungsbereite Berichte

Die folgenden anwendungsbereiten statischen Berichte werden bereitgestellt:

Prüfbericht zu Konfigurationsänderungen
Ermöglicht Administratoren, Berichte zu Änderungen an der Verzeichnisserverkonfiguration zu generieren.

Die Berichte basieren auf den folgenden Eingabeparametern:

- Startdatum und -zeit
- Enddatum und -zeit

Prüfbericht zur LDAP-Authentifizierung
Ermöglicht Administratoren, Berichte zu Bindungsereignissen und fehlgeschlagenen Bindungsereignissen zu generieren.

Die Berichte basieren auf den folgenden Eingabeparametern:

- Startdatum und -zeit
- Enddatum und -zeit
- Bindungs-DN für Benutzer
- Client-IP
- Operationsergebnis

Bericht zu LDAP-Kennwortrichtlinienverstößen
Ermöglicht Administratoren, Berichte zu aufgrund von Kennwortrichtlinienverletzungen gescheiterten Versuchen, Benutzerkennwörter zu ändern, zu generieren.

Die Berichte basieren auf den folgenden Eingabeparametern:

- Startdatum und -zeit
- Enddatum und -zeit
- Bindungs-DN für Benutzer

Bericht zu Suchvorgängen mit langer Laufzeit
Ermöglicht Administratoren, Berichte zu Suchoperationen zu generieren, für deren Durchführung mehr als die angegebene Zeit benötigt wurde.

Die Berichte basieren auf den folgenden Eingabeparametern:

- Startdatum und -zeit
- Enddatum und -zeit
- Operationsantwortzeit in Millisekunden

Prüfbericht zu Benutzeraktivitäten
Ermöglicht Administratoren, Berichte zu Benutzeroperationen zu generieren.

Die Berichte basieren auf den folgenden Eingabeparametern:

- Startdatum und -zeit
- Enddatum und -zeit
- Bindungs-DN für Benutzer

Angepasste Berichte

Sie können auch mithilfe von Cognos Workspace Advanced angepasste Prüfberichte erstellen. Weitere Informationen finden Sie unter „Angepasste Berichte erstellen" auf Seite 15.

Voraussetzungen für die Prüfberichterstellung

Sie müssen die Voraussetzungen erfüllen, bevor Sie mit dem Konfigurieren der Prüfberichterstellung für IBM Security Directory Server beginnen.

IBM Security Directory Server unterstützt IBM Cognos Business Intelligence Server Version 10.2.1.

Sie müssen folgende Software installieren:

IBM Cognos Business Intelligence Server Version 10.2.1.
Um diese Software zu installieren, befolgen Sie die Prozedur im Abschnitt *Install* der Dokumentation zu IBM Cognos Business Intelligence 10.2.1. Führen Sie die Schritte im Abschnitt 'Installing and Configuring Product Components on One Computer' durch.

Web-Server
Führen Sie folgende Schritte aus, um die unterstützten Web-Server anzuzeigen:

1. Klicken Sie auf der Startseite der Dokumentation zu IBM Cognos Business Intelligence 10.2.1 auf den Link **IBM Cognos 10.2.1 Business Intelligence software environments**.
2. Klicken Sie auf der Seite *IBM Cognos Business Intelligence 10.2 Supported Software Environments* auf die Registerkarte **10.2.1**.
3. Klicken Sie im Abschnitt *IBM Cognos Business Intelligence 10.2.1* in der Spalte **Requirements by type** auf den Link **Software**.
4. Suchen Sie auf der Seite *Related software for Cognos Business Intelligence 10.2.1* den Abschnitt *Web Servers*.
5. Stellen Sie sicher, dass einer der genannten unterstützten Web-Server auf Ihrem System installiert ist.

Datenquellen
Führen Sie folgende Schritte aus, um die unterstützten Datenquellen anzuzeigen:

1. Klicken Sie auf der Startseite der Dokumentation zu IBM Cognos Business Intelligence 10.2.1 auf den Link **IBM Cognos 10.2.1 Business Intelligence software environments**.
2. Klicken Sie auf der Seite *IBM Cognos Business Intelligence 10.2 Supported Software Environments* auf die Registerkarte **10.2.1**.
3. Klicken Sie im Abschnitt *IBM Cognos Business Intelligence 10.2.1* in der Spalte **Requirements by type** auf den Link **Software**.
4. Suchen Sie auf der angezeigten Seite *Related software for Cognos Business Intelligence 10.2.1* den Abschnitt *Data Sources*. Stellen Sie sicher, dass eine der genannten unterstützten Datenquellen auf Ihrem System installiert und konfiguriert ist.

IBM Security Directory Integrator
Damit das Protokollverwaltungstool funktioniert, müssen Sie IBM Security Directory Integrator ab Version 7.1.0.8 installieren. Installationsanweisun-

gen können Sie dem Abschnitt *Installation* in der Dokumentation für IBM Security Directory Integrator entnehmen.

Konfiguration der Prüfberichterstellung

Bevor Sie Prüfberichte generieren können, müssen Sie mehrere Komponenten installieren und konfigurieren.

- Prüfdatenbank
- IBM Cognos-Berichtskomponenten
- Berichtspaket
- Datenquelle
- Protokollverwaltungstool

In den folgenden Abschnitten werden die Schritte der Installation und Konfiguration dieser Komponenten beschrieben.

Prüfdatenbank erstellen und konfigurieren

Bei der Prüfdatenbank handelt es sich um eine DB2-Datenbank, in die alle Prüfereignisse aus der Prüfprotokolldatei der Verzeichnisserverinstanz geschrieben werden. Sie können die Prüfdatenbank mithilfe der Scripts erstellen und konfigurieren, die bei der Installation von IBM Security Directory Server bereitgestellt werden.

Informationen zu diesem Vorgang

Die Prüfberichterstellung von IBM Security Directory Server unterstützt nur DB2-Datenbanken.

Vorgehensweise

1. Installieren Sie DB2 auf dem System, auf dem die Prüfdatenbank erstellt werden soll.
2. Kopieren Sie das Dienstprogramm **idscfgauditdb** und die Datei `sdsAuditDB.sql` aus den folgenden Positionen:

   UNIX-Systeme

   SDS-Installationsverzeichnis`/report/idscfgauditdb`

   SDS-Installationsverzeichnis`/report/sdsAuditDB.sql`

   Windows-Systeme

   SDS-Installationsverzeichnis`\report\idscfgauditdb.cmd`

   SDS-Installationsverzeichnis`\report\sdsAuditDB.sql`
3. Legen Sie beide Dateien auf dem System, auf dem die Prüfdatenbank erstellt werden soll, im selben Verzeichnis ab.
4. Führen Sie das Dienstprogramm **idscfgauditdb** mit den entsprechenden Parametern aus. Informationen dazu enthält der Abschnitt **idscfgauditdb** utility in der Dokumentation für IBM Security Directory Server.

Ergebnisse

Die Prüfdatenbankinstanz, die Datenbank und die Tabellen wurden erstellt.

Nächste Schritte

Installieren und konfigurieren Sie die Berichtskomponenten.

IBM Cognos-Berichtskomponenten installieren und konfigurieren

Nach dem Konfigurieren der Prüfdatenbank müssen die IBM Cognos-Berichtskomponenten installiert und konfiguriert werden.

Informationen zu diesem Vorgang

Führen Sie während des Datenbankkonfigurationsprozesses folgende Schritte durch:

- Legen Sie die Umgebungsvariable `JAVA_HOME` so fest, dass sie auf die JVM verweist, die vom Anwendungsserver verwendet wird.
- Verwenden Sie die Unternehmensdatenbank als IBM Cognos-Content-Store.
- Löschen Sie die bereits vorhandene Datenquelle und erstellen Sie eine neue Datenquelle, um eine Option zum Generieren von DDL während der Erstellung einer Content-Store-Datenbank zu erstellen. Informationen zum Erstellen von Datenquellen finden Sie im Abschnitt 'Datenquellen erstellen'.

Sie finden die folgenden Prozeduren zum Installieren von IBM Cognos-Berichtskomponenten in der Dokumentation zu IBM Cognos Business Intelligence 10.2.1.

Vorgehensweise

1. Stellen Sie sicher, dass Cognos Business Intelligence entsprechend den Anweisungen unter Voraussetzungen installiert wird.
2. IBM Security Directory Server installiert die Prüfberichte. Sie finden die Berichte im Verzeichnis *SDS-Installationsverzeichnis*`/report/SDSAuditReportingPackage.zip`.
3. Erstellen Sie nach der Installation des Cognos Business Intelligence-Servers in der Datenbank einen Content Store. Führen Sie die Schritte in den folgenden Abschnitten entsprechend Ihrem Betriebssystem durch.
   a. Starten Sie IBM Cognos Configuration.
   b. Erstellen Sie eine Content-Store-Datenbank.
4. Konfigurieren Sie das Web-Gateway. Führen Sie die Schritte im Abschnitt 'Installing and configuring the gateway' durch.
5. Konfigurieren Sie den Web-Server. Führen Sie die Schritte im Abschnitt 'Configuring the web server' durch.

Nächste Schritte

Importieren Sie das Berichtspaket.

Berichtspakete importieren

Importieren Sie ein Berichtspaket, um mit Modellen für gebündelte Berichte und mit statischen Berichten arbeiten zu können.

Vorbereitende Schritte

Führen Sie vor dem Importieren des Berichtspakets die folgenden Schritte durch:

- Kopieren Sie die Berichtspaketdatei `SDSAuditReportingPackage.zip` in das Verzeichnis, in dem Ihre Bereitstellungsarchive gespeichert sind. Die Standardposition ist `c10_location/deployment`. Siehe „IBM Cognos-Berichtskomponenten installieren und konfigurieren".

- Um auf den Bereich '**Content Administration**' in '**IBM Cognos Administration**' zugreifen zu können, müssen Sie die erforderlichen Berechtigungen für die Funktion zur Sicherung von Verwaltungstasks besitzen.

Vorgehensweise

1. Greifen Sie auf den IBM Cognos Gateway-URI zu.

   Beispiel:

   `https://`*`Hostname:Portnummer`*`/ibmcognos/cgi-bin/cognos.cgi`

   Dabei gilt Folgendes:

   `Hostname` steht für die IP-Adresse oder der Netzhostname, mit der bzw. mit dem angegeben wird, wo das IBM Cognos-Gateway konfiguriert ist.

   `Portnummer` steht für den Port, auf dem das IBM Cognos-Gateway konfiguriert ist.
2. Klicken Sie auf **Launch**.
3. Klicken Sie im Fenster '**IBM Cognos Administration**' auf die Registerkarte **Configuration**.
4. Klicken Sie auf **Content Administration**.
5. Löschen Sie den Verlauf.
6. Klicken Sie auf der Symbolleiste auf das Symbol **New Import**. Der Assistent 'New Import' wird geöffnet.
7. Wählen Sie aus der Liste **Deployment Archive** den Eintrag `SDSAuditReportingPackage.zip` aus.
8. Klicken Sie auf **Next**.
9. Fügen Sie im Feld **Specify a name and description** die Beschreibung und die QuickInfo hinzu.
10. Klicken Sie auf **Next**.
11. Wählen Sie im Feld **Select the public folders and directory** das angezeigte Modell aus.
12. Geben Sie auf der Seite '**Specify the general options**' an, ob Zugriffsberechtigungen und Verweise auf externe Namespaces und ein Eigner für die Einträge eingeschlossen werden sollen, nachdem diese importiert wurden.
13. Klicken Sie auf **Next**. Die Übersichtsinformationen werden geöffnet.
14. Prüfen Sie die Übersichtsinformationen und klicken Sie dann auf **Next**.
15. Klicken Sie auf der Seite '**Select an action**' auf **Save and run once**.
16. Klicken Sie nach dem Absenden der Dateiimportoperation auf **Finish**.

Ergebnisse

Sie können das Berichtspaket nun verwenden, um Berichte zu erstellen und Beispielberichte auszuführen. Beispielberichte sind im Berichtsmodell auf der Registerkarte **Public Folders** im IBM Cognos-Portal verfügbar.

Nächste Schritte

Erstellen Sie eine Datenquelle.

Datenquellen erstellen

Um mit der IBM Security Directory Server Cognos-Berichterstellung arbeiten zu können, müssen Sie eine Datenquelle erstellen.

Informationen zu diesem Vorgang

- Sie müssen den Datenquellennamen `SDSAudit` verwenden.
- Kopieren Sie die Datei `db2cli.dll` aus dem Installationsverzeichnis des DB2-Clients in den Ordner *IBM Cognos-Installationsverzeichnis*`/bin`.
- Die Datenquelle muss auf die Prüfdatenbank verweisen. Siehe „Prüfdatenbank erstellen und konfigurieren” auf Seite 3.

Vorgehensweise

Um eine Datenquelle zu erstellen, öffnen Sie die Dokumentation zu IBM Cognos Business Intelligence 10.2.1 und führen Sie die Schritte im Abschnitt 'Create a Data Source' durch.

Nächste Schritte

Konfigurieren Sie das Protokollverwaltungstool zum Schreiben von Prüfereignissen in die Prüfdatenbank.

Protokollverwaltungstool konfigurieren

Konfigurieren Sie das Protokollverwaltungstool zum Schreiben von Prüfereignissen in die Prüfdatenbank.

Informationen zu diesem Vorgang

Das ursprüngliche Protokollverwaltungstool für IBM Directory Server wurde nun funktional erweitert. Prüfereignisse können nun vom Prüfprotokoll gelesen und analysiert und in die Prüfdatenbank geschrieben werden. Weitere Informationen zur Prüfdatenbank finden Sie im Abschnitt „Prüfdatenbank erstellen und konfigurieren” auf Seite 3.

Um das Protokollverwaltungstool zum Schreiben von Prüfereignissen in die Prüfdatenbank zu konfigurieren, müssen Sie die Eigenschaftendatei der Prüfdatenbank in *SDS-Installationsverzeichnis*`/idstools/idslogmgmt/idsauditdb.properties` aktualisieren.

Vorgehensweise

1. Öffnen Sie die Datei `idsauditdb.properties`.
2. Legen Sie den Wert der Eigenschaft **`IDS_AUDITDB_JDBCURL`** auf den Hostnamen oder die IP-Adresse der Prüfdatenbank fest.
3. Legen Sie den Wert der Eigenschaft **`IDS_AUDITDB_JDBCUSERNAME`** auf den DB2-Datenbankinstanzeigner für die Prüfdatenbank fest.
4. Legen Sie den Wert für **`IDS_AUDITDB_JDBCPASSWORD`** auf das Kennwort des Instanzeigners fest.
5. Melden Sie sich mithilfe der Berechtigungsnachweise des Verzeichnisserverinstanzeigners bei dem System an, auf dem die Verzeichnisserverinstanz ausgeführt wird.
6. Legen Sie die Umgebungsvariable **`IDS_LOGMGMT_ENABLE_AUDIT_COGNOS`** auf `true` fest.

7. Führen Sie das Protokollverwaltungstool mithilfe des folgenden Befehls aus:
   `idslogmgmt –I Instanzname`

   Anmerkung: Aus Sicherheitsgründen wird vorgeschlagen, dass Sie nach Schritt 7 den Inhalt des Werts **IDS_AUDITDB_JDBCPASSWORD** in der Datei `sds_install_dir/idstools/idslogmgmt/idsauditdb.properties` löschen.

Ergebnisse

Mit dem Protokollverwaltungstool werden Prüfereignisse aus der Prüfprotokolldatei der Verzeichnisserverinstanz gelesen, analysiert und in der Prüfprotokolldatei in die Prüfdatenbank geschrieben.

Nächste Schritte

Sie können nun in IBM Cognos die IBM Security Directory Server-Prüfberichterstellung erstellen.

Globalisierung

Sie können die Globalisierungsfunktionen des Prüfberichtspakets von IBM Security Directory Server verwenden, um Berichte in Ihrer eigenen Sprache zu erstellen.

Unterstützte Sprachen

IBM Security Directory Server Cognos-Berichte unterstützen die folgenden Sprachen:

- cs=Tschechisch
- de=Deutsch
- en=Englisch
- es=Spanisch
- fr=Französisch
- hu=Ungarisch
- it=Italienisch
- ja=Japanisch
- ko=Koreanisch
- pl=Polnisch
- pt_BR=Portugiesisch (Brasilien)
- ru=Russisch
- sk=Slowakisch
- zh_CN=Vereinfachtes Chinesisch
- zh_TW=Traditionelles Chinesisch

Anmerkung: Angepasste Berichte werden nur in englischer Sprache unterstützt.

Nachrichten

In den Berichten wird in einigen Spaltenwerten möglicherweise die Nachricht 'Language not supported' angezeigt. Diese Nachricht wird angezeigt, wenn Sie eine Sprache auswählen, die nicht vom Berichtsmodell unterstützt wird.

Sprachvorgaben festlegen

Sie können personalisieren, wie Daten im IBM Cognos-Arbeitsbereich angezeigt werden, in dem Sie Ihre Vorgaben ändern. Sie können die Produktsprache oder die Inhaltssprache festlegen, um das bevorzugte Ausgabeformat für die Berichte zu erhalten.

Vorbereitende Schritte

Installieren und konfigurieren Sie IBM Cognos Business Intelligence Server.

Vorgehensweise

1. Klicken Sie im Fenster '**IBM Cognos Connection**' auf **My Area Options**  .
2. Klicken Sie auf **My Preferences**.
3. Wählen Sie im Fenster '**Set Preferences**' im Abschnitt '**Regional options**' die Option **Product language** aus. Mit der Produktsprache wird die Sprache angegeben, die auf der Benutzerschnittstelle von IBM Cognos verwendet wird.
4. Wählen Sie im Fenster '**Set Preferences**' im Abschnitt '**Regional options**' die Option **Content language** aus. Mit der Inhaltssprache wird die Sprache angegeben, die zum Anzeigen und Erstellen von Inhalten in IBM Cognos verwendet wird, zum Beispiel Daten in den Berichten.
5. Klicken Sie auf **OK**.

Ergebnisse

Sie können die Berichte oder die Benutzerschnittstelle in der von Ihnen ausgewählten Sprache anzeigen.

Berichtsmodellobjekte

Verwenden Sie die Informationen zu Objekten und Berichtsmodellnamen, Namespaces und Entitäten, um mit Berichtsmodellen zum Erstellen angepasster Prüfberichte zu arbeiten.

Abfrageelemente

Das kleinste Teil des Modells in einem Bericht. Es stellt ein einzelnes Merkmal von etwas dar, zum Beispiel das Datum, an dem ein Produkt eingeführt wurde.

Abfragesubjekte oder Dimensionen enthalten Abfrageelemente. Ein Abfragesubjekt zum Beispiel, das auf eine ganze Tabelle verweist, enthält Abfrageelemente, die die einzelnen Spalten in der Tabelle darstellen.

Abfrageelemente sind die wichtigsten Objekte beim Erstellen von Berichten. Beim Erstellen ihrer Berichte werden Abfrageelementeigenschaften verwendet.

Abfragesubjekte

Eine Gruppe von Abfrageelementen, die eine von Anfang an bestehende Beziehung haben. In den meisten Fällen verhalten sich Abfragesubjekte wie Tabellen. Mit Abfragesubjekten wird dieselbe Gruppe von Zeilen erstellt, unabhängig davon, welche Spalten abgefragt wurden.

Pakete

Eine Teilmenge der Dimensionen, Abfragesubjekte und anderer Objekte, die in dem Projekt definiert werden. Ein Paket wird auf dem IBM Cognos-Server publiziert. Es werden Berichte, Analysen und Ad-hoc-Abfragen erstellt.

Namespaces

Zum eindeutigen Identifizieren von Abfrageelementen, Dimensionen, Abfragesubjekten und anderen Objekten. Importieren Sie unterschiedliche Datenbanken in einzelne Namespaces, um doppelte Namen zu vermeiden.

Anmerkung: Der Namespace für das Prüfberichterstellungsmodell von Security Directory Server heißt Prüfung.

Abfragesubjekte für den Namespace Prüfung

Der Namespace für das Prüfberichterstellungsmodell von Security Directory Server heißt Prüfung. Im Folgenden werden die Abfragesubjekte im Namespace Prüfung aufgelistet.

LDAP-Prüfung

Steht für die Kombination aus allen Headern und allgemeinen Attributen in einem Prüfereignis für eine IBM Security Directory Server-Instanz. Beispiel: Prüfversion, Zeitmarke, Bindungs-DN, Client-IP und -Port, Operationsergebnis, LDAP-Clientsteuerelemente und -kritikalität, Operationsantwortzeit usw.

Prüfhinzufügung

Steht für die Ereignisattribute, die nur für LDAP-Hinzufügungsereignisse gelten. Beispiel: Eintrag und Attribute.

Prüfbindung

Steht für die Ereignisattribute, die nur für LDAP-Bindungsereignisse gelten. Beispiel: Authentifizierungsauswahl, Authentifizierungsmechanismus usw.

Prüfvergleich

Steht für die Ereignisattribute, die nur für LDAP-Vergleichsereignisse gelten. Beispiel: Eintrag und Attribut.

Prüflöschung

Steht für die Ereignisattribute, die nur für LDAP-Löschereignisse gelten. Beispiel: Eintrag.

Erweiterte Prüfoperationen

Steht für die Ereignisattribute, die nur für erweiterte LDAP-Operationsereignisse gelten. Beispiel: OID.

Prüfung DN-Änderung

Steht für die Ereignisattribute, die nur für LDAP-DN-Änderungsereignisse gelten. Beispiel: Eintrag, Neuer RDN, Alten RDN löschen, Neue übergeordnete Instanz.

Benachrichtigungen bei registrierten Ereignissen prüfen
Steht für die Ereignisattribute, die nur für Benachrichtigungsereignisse bei LDAP-Ereignisregistrierungen gelten. Beispiel: Ereignis-ID, Basis, Bereich und Operationstyp.

Suche prüfen
Steht für die Ereignisattribute, die nur für LDAP-Suchereignisse gelten. Beispiel: Basis, Bereich, Filter, Aliasnamen dereferenzieren, Ausschließliche Typen, Attribute und Zurückgegebene Einträge.

Benachrichtigungen bei deregistrierten Ereignissen prüfen
Steht für die Ereignisattribute, die nur für Benachrichtigungsereignisse bei LDAP-Ereignisderegistrierungen gelten. Beispiel: ID.

Abfrageelemente für den Namespace Prüfung

Im Folgenden werden die Abfrageelemente im Namespace Prüfung aufgelistet.

LDAP-Prüfung
Das Abfragesubjekt für LDAP-Prüfungen besitzt die folgenden Abfrageelemente:

Prüfversion
Steht für die Prüfversion. Wenn die Prüfversion 3 ist, hat **Audit Version** den Wert `AuditV3`.

Prüfzeitmarke
Steht für die Zeitmarke des Zeitpunkts, an dem das Ereignis geprüft wurde. Entspricht der Zeitmarke, die sich im Headerabschnitt des Prüfprotokolls befindet.

Ereignistyp
Steht für den Operationstyp, zum Beispiel `V3 Bind`, `V3 Modify` usw. Entspricht dem Operationstyp, der sich im Prüfheader befindet.

Bindungs-DN
Steht für den Bindungs-DN. Bei nicht authentifizierten oder anonymen V3-Anforderungen hat dieses Feld den Wert `<*CN=NULLDN*>`. Entspricht dem Bindungs-DN im Prüfheader.

Client-IP
Steht für die Client-IP im Prüfheader.

Client-Port
Steht für den Client-Port im Prüfheader.

Verbindungs-ID
Steht für die LDAP-Verbindungs-ID. Entspricht dem Attribut `connectionID` im Prüfheader.

Zeitmarke Empfang
Steht für die Zeitmarke des Zeitpunkts, an dem die Anforderung empfangen wurde. Entspricht dem Attribut `received` im Prüfheader.

Operationsergebnis
Zeigt das Ergebnis oder den Status der LDAP-Operation an. Entspricht der Ergebniszeichenfolge im Prüfheader.

Eindeutige ID
Die eindeutige Anforderungs-ID, die im Steuerelement gespeichert werden soll. Die Client-IP ist die ursprüngliche IP des Clients, die im Steuerelement gespeichert werden soll. Wenn 'critical' den Wert

'true' besitzt, wird die Kritikalität des Steuerelements auf 'true' gesetzt. Ist der Wert 'false', wird die Kritikalität auf 'false' gesetzt.

Client-IP für die Prüfsteuerung
Steht für die Client-IP, die mit der Prüfsteuerung gesendet wird. Entspricht dem Attribut `ClientIP` im Prüfprotokoll.

Anforderungs-ID
Steht für die Anforderungs-ID, die mit den zusätzlichen Informationen gesendet wird, wenn es sich bei der Steuerung um die Prüfsteuerung handelt und die Serverprüfung zum Prüfen der zusätzlichen Informationen konfiguriert ist. Entspricht dem Attribut `RequestID` im Prüfprotokoll.

Normalisiert
Steht für das Attribut `Normalized` in den zusätzlichen Informationen, die bei der Gruppenberechtigungsprüfung gesendet werden. Der Wert lautet `TRUE` oder `FALSE`.

Steuerwert

Autorisierungsgruppe
Steht für den Gruppennamen, der bei einer Gruppenberechtigungsprüfung gesendet wird, wenn die Serverprüfung zum Prüfen der Gruppe konfiguriert ist. Entspricht dem Attribut `Group` im Prüfprotokoll.

LDAP-Steuerelement und -Kritikalität
Steht für die Zeichenfolge, die für das LDAP-Steuerelement steht, und ihre Kritikalität, die in der Anforderung gesendet wird. Entsprechen einer Kombination der Attribute `control` und `criticality` im Prüfprotokoll.

Proxy-DN
Steht für den Proxy-DN, wenn es sich bei der Steuerung um eine Proxy-Berechtigungssteuerung handelt. Entspricht dem Attribut `ProxyDN` im Prüfprotokoll.

Operationsantwortzeit
Steht für den Unterschied zwischen dem Zeitpunkt, an dem die Anforderung empfangen wurde, und dem Zeitpunkt, an dem die Antwort gesendet wurde, in Millisekunden. Entspricht dem Attribut `operationResponseTime` im Prüfprotokoll.

Zeit in der Workerwarteschlange
Steht für die Zeit, die die Anforderung in der Workerwarteschlange verbracht hat, bevor die Ausführung der Operation initiiert wurde, in Millisekunden. Entspricht dem Attribut `timeOnWorkQ` im Prüfprotokoll.

Wartezeit für RDBM-Sperre
Steht für die Zeit, die das Anfordern von Sperren für RDBM-Caches während der Ausführung der Operation in Anspruch genommen hat, in Millisekunden. Entspricht dem Attribut `rdbmLockWaitTime` im Prüfprotokoll.

Client-E/A-Zeit
Steht für die Zeit, die das Empfangen der vollständigen Operationsanforderung und das Zurückgeben der vollständigen Operationsantwort in Anspruch genommen hat, in Millisekunden. Entspricht dem Attribut `clientIOTime` im Prüfprotokoll.

Prüfhinzufügung
Das Abfragesubjekt für Prüfhinzufügung besitzt die folgenden Abfrageelemente:

Eintrag hinzufügen
Steht für den DN des hinzugefügten Eintrags. Entspricht dem Attribut `entry` im LDAP-Hinzufügungsereignis.

Attribute hinzufügen
Steht für die Attribute des hinzugefügten Eintrags. Entspricht dem Attribut `attributes` im LDAP-Hinzufügungsereignis.

Prüfbindung
Das Abfragesubjekt für Prüfbindungen besitzt die folgenden Abfrageelemente:

Benutzername
Steht für den DN des Eintrags, der die Bindung durchgeführt hat. Entspricht dem Attribut `name` im Bindungsereignis.

Authentifizierungsauswahl
Entspricht dem Attribut `authenticationChoice` im LDAP-Bindungsereignis. Die gültigen Werte lauten `unknown`, `simple`, `krbv42LDAP`, `krbv42DSA` und `sasl`.

Authentifizierungsmechanismus
Entspricht dem Attribut `authenticationMechanism` im LDAP-Bindungsereignis.

Zugeordneter Name
Entspricht dem Attribut `mappedname` im LDAP-Bindungsereignis.

Authentifizierungs-ID
Entspricht dem Attribut `authzId` im LDAP-Bindungsereignis.

Administratoraccountstatus
Entspricht dem Attribut `Admin Acct Status` im LDAP-Bindungsereignis. Die gültigen Werte lauten `Not Locked`, `Locked` und `Lock Cleared`.

Bindungs-DN für Durchgriff
Steht für den Bindungs-DN, der von IBM Security Directory Server verwendet wird, um ein Durchgriffsverzeichnis zu binden. Entspricht dem Attribut `passthroughBindDN` im Prüfprotokoll.

Durchgriffsserver
Steht für die IP-Adresse und den Port des Hostnamens des Durchgriffsverzeichnis. Entspricht dem Attribut `passthroughServer` im Prüfprotokoll.

Bindungs-RC für Durchgriff
Steht für den Rückgabecode (RC) im Durchgriffsverzeichnis. Entspricht dem Attribut `passthroughBindRC` im Prüfprotokoll.

Prüfvergleich
Das Abfragesubjekt für Prüfvergleiche besitzt die folgenden Abfrageelemente:

Eintrag vergleichen
Steht für den DN des Eintrags, für den die Vergleichsoperation durchgeführt wurde. Entspricht dem Attribut `entry` im LDAP-Vergleichsereignis.

Attribut vergleichen
Steht für den Namen des Attributs, für das die Vergleichsoperation durchgeführt wurde. Entspricht dem Attribut `attribute` im LDAP-Vergleichsereignis.

Prüflöschung
Das Abfragesubjekt für Prüflöschung besitzt die folgenden Abfrageelemente:

Eintrag löschen
Steht für den DN des gelöschten Eintrags. Entspricht dem Attribut `entry` im LDAP-Löschereignis.

Erweiterte Prüfoperationen
Das Abfragesubjekt für erweiterte Prüfoperationen besitzt die folgenden Abfrageelemente:

OID Steht für die OID der durchgeführten erweiterten Operation. Entspricht dem Attribut `OID` im erweiterten LDAP-Ereignis.

Prüfung DN-Änderung
Das Abfragesubjekt für die Prüfung der DN-Änderung besitzt die folgenden Abfrageelemente:

DN-Änderung Eintrag
Steht für den DN des Eintrags, für den die DN-Änderungsoperation durchgeführt wurde. Entspricht dem Attribut `entry` im LDAP-DN-Änderungsereignis.

Neuer RDN
Steht für das neue RDN-Attribut des LDAP-Eintrags, für den die DN-Änderungsoperation durchgeführt wurde. Entspricht dem Attribut `newrdn` im LDAP-DN-Änderungsereignis.

Alten RDN löschen
Gibt an, ob das alte RDN-Attribut aus dem LDAP-Eintrag gelöscht wurde. Entspricht dem Attribut `deleteoldrdn` im LDAP-DN-Änderungsereignis.

Neue übergeordnete Instanz
Steht für den DN des neuen übergeordneten Elements des LDAP-Eintrags, für den die DN-Änderungsoperation durchgeführt wurde. Entspricht dem Attribut `newSuperior` im LDAP-DN-Änderungsereignis.

Änderungen prüfen
Das Abfragesubjekt zum Prüfen von Änderungen besitzt die folgenden Abfrageelemente:

Objekt ändern
Steht für den DN des Eintrags, für den die Änderungsoperation durchgeführt wurde. Entspricht dem Attribut `object` im LDAP-Änderungsereignis.

Aktion und Attribut ändern
Zeigt eine Liste der Kombinationen aus Änderungsaktionen und Namen der Attribute an, die bei der Änderungsoperation involviert waren.

Benachrichtigungen bei registrierten Ereignissen prüfen
Das Abfragesubjekt zum Prüfen von Benachrichtigungen bei registrierten Ereignissen besitzt die folgenden Abfrageelemente:

Ereignis-ID
Steht für die ID des registrierten Ereignisses. Entspricht dem Attribut `eventID` im Prüfprotokoll.

Basis für Benachrichtigung bei registrierten Ereignissen
Steht für den DN der untergeordneten Baumstruktur, für die das Ereignis registriert ist. Entspricht dem Attribut `base` im Prüfprotokoll.

Bereich für Benachrichtigung bei registrierten Ereignissen
Steht für den Bereich der Operation. Entspricht dem Attribut `scope` im Prüfprotokoll.

Operationstyp
Steht für den Typ von Operationen, für die die Ereignisregistrierung durchgeführt wurde. Entspricht dem Attribut `type` im Prüfprotokoll.

Suche prüfen
Das Abfragesubjekt zum Prüfen von Suchen besitzt die folgenden Abfrageelemente:

Suchbasis
Steht für die Suchbasis, die bei der LDAP-Suchoperation verwendet wird. Entspricht dem Attribut `base` im LDAP-Suchereignis.

Suchbereich
Steht für den Suchbereich, der bei der LDAP-Suchoperation verwendet wird. Entspricht dem Attribut `scope` im LDAP-Suchereignis.

Aliasnamen dereferenzieren
Zeigt an, ob der Server die Aliasnamen dereferenzieren muss. Entspricht dem Attribut `derefAliases` im LDAP-Suchereignis.

Filter Steht für den Suchfilter, der bei der Suchoperation verwendet wird. Entspricht dem Attribut `filter` im LDAP-Suchereignis.

Ausschließliche Typen
Gibt an, ob die Suchoperation nur Attribute anfordert. Entspricht dem Attribut `typesOnly` im LDAP-Suchereignis.

Suchattribute
Steht für die Liste der Attribute, die bei der Suchanforderung angefordert wurden. Entspricht dem Attribut `attributes` im LDAP-Suchereignis.

Zurückgegebene Einträge
Gibt die Anzahl der Einträge zurück, die bei einer Suchoperation zurückgegeben wurden. Entspricht dem Attribut `numberOfEntriesReturned` im LDAP-Suchereignis.

Benachrichtigungen bei deregistrierten Ereignissen prüfen
Das Abfragesubjekt zum Prüfen von Benachrichtigungen bei deregistrierten Ereignissen besitzt die folgenden Abfrageelemente:

ID Steht für die ID des unregistrierten Ereignisses. Entspricht dem Attribut `ID` im Prüfprotokoll.

Angepasste Berichte erstellen

Sie können mithilfe von IBM Cognos Workspace Advanced angepasste Prüfberichte erstellen.

Vorgehensweise

1. Fügen Sie in IBM Cognos Workspace die allgemeinen Abfrageelemente aus dem LDAP-Prüfabfragesubjekt ein.
2. Fügen Sie basierend auf den jeweiligen Ereignistypen weitere Abfrageelemente aus den ereignisspezifischen Abfragesubjekten ein. Um zum Beispiel einen angepassten Prüfbericht zu LDAP-Vergleichsoperationen zu erstellen, können Sie die folgenden Abfrageelemente einfügen:
   - Prüfversion
   - Prüfzeitmarke
   - Ereignistyp
   - Bindungs-DN
   - Client-IP
   - Operationsantwortzeit

   Nun würden alle in der Prüfdatenbank verfügbaren Prüfereignisse angezeigt.
3. Fügen Sie einen angepassten Filter hinzu. Sie können zum Beispiel einem Ereignistyp einen angepassten Filter hinzufügen, um nur die Vergleichsereignisse einzubeziehen. Nun würden nur die Ereignisse angezeigt, die mit LDAP-Vergleichsoperationen in Beziehung stehen.
4. Fügen Sie beliebige weitere Abfrageelemente ein, die vom ereignisspezifischen Abfragesubjekt für Sie erforderlich sind, zum Beispiel Prüfvergleich.
5. Speichern Sie den Bericht im von Ihnen benötigten Format.

Index

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 dieser Dokumentation 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 78758 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 diesem Dokument 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 in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

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.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können unter Umständen von den hier genannten Preisen abweichen.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

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.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für

die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit IBM Anwendungsprogrammierschnittstellen konform sind.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Beispielprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_. Alle Rechte vorbehalten.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM 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.

Adobe, Acrobat, PostScript und alle auf Adobe basierenden Marken sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

IT Infrastructure Library ist eine eingetragene Marke der Central Computer and Telecommunications Agency. Die Central Computer and Telecommunications Agency ist nunmehr in das Office of Government Commerce eingegliedert worden.

Intel, das Intel-Logo, Intel Inside, das Intel Inside-Logo, Intel Centrino, das Intel Centrino-Logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium und Pentium sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA oder anderen Ländern.

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.

ITIL ist als eingetragene Marke und eingetragene Gemeinschaftsmarke des Office of Government Commerce beim US Patent and Trademark Office registriert.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

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

Cell Broadband Engine wird unter Lizenz verwendet und ist eine Marke der Sony Computer Entertainment, Inc. in den USA und/oder anderen Ländern.

Linear Tape-Open, LTO, das LTO-Logo, Ultrium und das Ultrium-Logo sind Marken von HP, IBM Corp. und Quantum in den USA und anderen Ländern.

SC43-1260-00