

IBM Security Directory Server  
Version 6.3.1.5

*Installation und Konfiguration*





IBM Security Directory Server  
Version 6.3.1.5

*Installation und Konfiguration*



**Hinweis**

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen in „Bemerkungen“ auf Seite 275 gelesen werden.

**Impressum**

Diese Veröffentlichung ist eine Übersetzung des Handbuchs  
*IBM Security Directory Server, Version 6.3.1.2, Installation and Configuration Guide*,  
IBM Form SC27-2747-02,  
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 1998, 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

<b>Informationen zu dieser Veröffentlichung</b> . . . . .	<b>vii</b>
Zugriff auf Veröffentlichungen und Terminologie	vii
Eingabehilfen . . . . .	ix
Technische Schulung . . . . .	ix
Informationen zur Unterstützung . . . . .	ix
Erklärung zu geeigneten Sicherheitsvorkehrungen . . . . .	x
<b>Kapitel 1. Planung für die Installation</b> . . . . .	<b>1</b>
<b>Kapitel 2. Installationsübersicht</b> . . . . .	<b>3</b>
Erforderlicher Plattenspeicherplatz . . . . .	3
Vorbereitung von Installationsmedien . . . . .	6
Software von Passport Advantage herunterladen . . . . .	7
Verzeichnisstruktur heruntergeladener Dateien . . . . .	7
Installationsvoraussetzungen . . . . .	15
Auf verschiedenen Betriebssystemen erforderliche vorausgesetzte Pakete . . . . .	15
Voraussetzung für LDAP-Client unter PowerPC LE . . . . .	17
Benutzer und Gruppe idsldap . . . . .	17
Installationsmethoden . . . . .	19
<b>Kapitel 3. Installation mit IBM Installation Manager.</b> . . . . .	<b>21</b>
Übersicht über IBM Installation Manager . . . . .	21
Unterstützte Betriebssysteme . . . . .	22
Installationspakettypen für IBM Security Directory Server . . . . .	22
Installationsrichtlinien . . . . .	23
IBM Security Directory Server-Komponenten . . . . .	24
Anpassung der Installation von IBM Security Directory Server . . . . .	27
Standardinstallationspositionen . . . . .	28
Installationsrepositorys . . . . .	29
Installation starten . . . . .	29
Installation mit dem Launchpad starten . . . . .	29
Installation durch Festlegen von Repository-Vorgaben starten . . . . .	31
Installation mit IBM Installation Manager . . . . .	32
Unbeaufsichtigte Installation . . . . .	37
Unbeaufsichtigte Installation mit Antwortdatei . . . . .	38
<b>Kapitel 4. Mit IBM Installation Manager Änderungen vornehmen</b> . . . . .	<b>41</b>
Features mit IBM Installation Manager ändern . . . . .	41

<b>Kapitel 5. IBM Installation Manager-Protokolldateien</b> . . . . .	<b>47</b>
<b>Kapitel 6. IBM Security Directory Server-Pakete abfragen</b> . . . . .	<b>49</b>
<b>Kapitel 7. Native Installation und Konfiguration mit Scripts</b> . . . . .	<b>51</b>
Installationsroadmap . . . . .	51
IBM Security Directory Server-Pakete auf Linux-, Solaris- und HP-UX-Plattformen installieren . . . . .	52
Installationsprotokolle überprüfen . . . . .	54
<b>Kapitel 8. Installation von IBM DB2</b> . . . . .	<b>55</b>
<b>Kapitel 9. IBM Java Development Kit für IBM Security Directory Server</b> . . . . .	<b>57</b>
<b>Kapitel 10. Installation von IBM Global Security Kit.</b> . . . . .	<b>59</b>
IBM Global Security Kit mit <code>installp</code> installieren . . . . .	60
IBM Global Security Kit mit Linux-Dienstprogrammen installieren . . . . .	61
IBM Global Security Kit mit Solaris-Dienstprogrammen installieren . . . . .	62
IBM Global Security Kit mit HP-UX-Dienstprogrammen installieren . . . . .	63
IBM Global Security Kit unter Windows installieren . . . . .	64
Unbeaufsichtigte Installation von IBM Global Security Kit unter Windows . . . . .	65
<b>Kapitel 11. Installation von Sprachenpaketen</b> . . . . .	<b>67</b>
Sprachenpakete für die Installation . . . . .	68
Sprachenpakete mit Betriebssystemdienstprogrammen installieren . . . . .	69
<b>Kapitel 12. Installation mit den Befehlszeilendienstprogrammen des Betriebssystems</b> . . . . .	<b>71</b>
Installation mit AIX-Dienstprogrammen . . . . .	71
Pakete für die Installation auf einem AIX-System . . . . .	72
Installation mit SMIT . . . . .	74
Installation mit <code>installp</code> . . . . .	75
Installation mit Linux-Dienstprogrammen . . . . .	77
Pakete für die Installation auf einem Linux-System . . . . .	77
Installation mit Linux-Dienstprogrammen . . . . .	79
Installation mit Solaris-Dienstprogrammen . . . . .	81
Pakete für die Installation auf einem Solaris-System . . . . .	81
Installation mit Solaris-Dienstprogrammen . . . . .	83

Installation mit HP-UX-Dienstprogrammen . . . . .	84
Pakete für die Installation auf einem HP-UX Itanium-System . . . . .	84
Installation mit HP-UX-Dienstprogrammen . . . . .	85

**Kapitel 13. Überprüfung der IBM Security Directory Server-Features . . . . . 87**

IBM Security Directory Server-Features mit IBM Installation Manager überprüfen . . . . .	87
IBM Security Directory Server-Features unter Windows überprüfen . . . . .	87
IBM Security Directory Server-Pakete überprüfen . . . . .	89
Version des <b>Webverwaltungstools</b> überprüfen . . . . .	89
Installation von IBM Global Security Kit unter Windows überprüfen . . . . .	90
Installation von IBM Global Security Kit unter AIX, Linux, Solaris und HP-UX überprüfen . . . . .	90

**Kapitel 14. Upgrades von Instanzen von Vorgängerversionen durchführen . . . . . 93**

Umgebung vor dem Upgrade einer Instanz einrichten . . . . .	94
Upgrade einer Instanz einer Vorgängerversion mit dem Befehl <b>idsimigr</b> durchführen . . . . .	96
Upgrades von Instanzen von Vorgängerversionen auf einem anderen Computer durchführen . . . . .	97
Unterstützte Betriebssysteme für Upgrades einer fernen Instanz . . . . .	98
Upgrade einer fernen Instanz einer Vorgängerversion mit dem Befehl <b>idsimigr</b> durchführen . . . . .	98
Links zu Client- und Serverdienstprogrammen . . . . .	100

**Kapitel 15. Migration von Daten und Lösungen von einer Instanz einer Vorgängerversion . . . . . 101**

Instanz mit DB2 ESE-Datenbank auf eine Instanz mit DB2 WSE-Datenbank migrieren . . . . .	102
Protokollverwaltungslösung migrieren . . . . .	103
SNMP-Lösung migrieren . . . . .	104
Active Directory-Synchronisationslösung migrieren	105
Vorgängerversion der Webverwaltungstool-Konfiguration migrieren . . . . .	106
<b>idswmigr</b> . . . . .	107
Webverwaltungstool manuell migrieren . . . . .	108

**Kapitel 16. Manuelle Bereitstellung des Webverwaltungstools . . . . . 113**

Integrierte Version von WebSphere Application Server manuell installieren . . . . .	113
Standardports für das <b>Webverwaltungstool</b> . . . . .	114
<b>Webverwaltungstool</b> in der integrierten Version von WebSphere Application Server implementieren . . . . .	115
<b>Webverwaltungstool</b> in WebSphere Application Server implementieren . . . . .	117
Integrierte Version von WebSphere Application Server für die Verwendung des <b>Webverwaltungstools</b> starten . . . . .	119
Auf das <b>Webverwaltungstool</b> zugreifen . . . . .	120
Webanwendungsserver stoppen . . . . .	121

HTTPS mit einer integrierten Version von WebSphere Application Server . . . . .	122
<b>Webverwaltungstool</b> aus der integrierten Version von WebSphere Application Server deinstallieren . . . . .	123

**Kapitel 17. Planung für die Instanzkonfiguration . . . . . 125**

Benutzer und Gruppen, die einer Verzeichnisserverinstanz zugeordnet sind . . . . .	125
Namenskonventionen . . . . .	126
Anforderungen für die Erstellung von Benutzern und Gruppen . . . . .	127
Konfigurationsplanung . . . . .	129
UTF-8-Unterstützung . . . . .	130
UTF-8 in einem Verzeichnisserver verwenden	130
LDIF-Dateien mit UTF-8-Werten mithilfe von Serverdienstprogrammen erstellen . . . . .	131
Unterstützte IANA-Zeichensätze . . . . .	132
ASCII-Zeichen von 33 bis 126 . . . . .	134

**Kapitel 18. Instanzerstellung und -verwaltung . . . . . 137**

<b>Instance Administration Tool</b> starten . . . . .	138
<b>Instance Administration Tool</b> für das Upgrade einer Instanz starten . . . . .	139
Erstellung von Verzeichnisserverinstanzen . . . . .	140
Instanzerstellung mit <b>Instance Administration Tool</b> . . . . .	140
Standardverzeichnisserverinstanz erstellen . . . . .	141
Verzeichnisserverinstanz mit angepassten Einstellungen erstellen . . . . .	143
Proxy-Server-Instanz mit angepassten Einstellungen erstellen . . . . .	150
Instanz mit dem Befehlszeilendienstprogramm konfigurieren . . . . .	154
Upgrade einer Instanz einer Vorgängerversion mit dem <b>Instance Administration Tool</b> durchführen . . . . .	156
Upgrade einer fernen Instanz einer Vorgängerversion mit dem <b>Instance Administration Tool</b> durchführen . . . . .	157
Instanzerstellung aus einer bereits vorhandenen Instanz . . . . .	160
Kopie einer vorhandenen Instanz mit dem <b>Instance Administration Tool</b> erstellen . . . . .	162
Kopie einer vorhandenen Instanz mit dem Befehlszeilendienstprogramm erstellen . . . . .	164
Verzeichnisserver und Verwaltungsserver starten oder stoppen . . . . .	165
Verzeichnisserver und Verwaltungsserver starten oder stoppen . . . . .	165
Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen . . . . .	166
Konfiguration von Verzeichnisserverinstanzen verwalten . . . . .	167
<b>Konfigurationstool</b> über das <b>Instance Administration Tool</b> öffnen . . . . .	167
TCP/IP-Einstellungen von Instanzen ändern . . . . .	168

TCP/IP-Einstellungen einer Instanz mit dem <b>Instance Administration Tool</b> ändern . . . . .	168
TCP/IP-Einstellungen einer Instanz mit Befehlszeilendienstprogrammen ändern . . . . .	169
Informationen zu einer Instanz anzeigen . . . . .	170
Instanzinformationen mit dem <b>Instance Administration Tool</b> anzeigen. . . . .	170
Informationen zu einer Instanz mit dem Befehlszeilendienstprogramm anzeigen . . . . .	171
Verzeichnisserverinstanzen löschen . . . . .	171
Instanz mit dem <b>Instance Administration Tool</b> löschen . . . . .	172
Instanz mit dem Befehlszeilendienstprogramm löschen . . . . .	173

## Kapitel 19. Verzeichnisstruktur überprüfen . . . . . 175

## Kapitel 20. Instanzkonfiguration . . . 177

<b>Konfigurationstool</b> starten . . . . .	178
Verzeichnisserver und Verwaltungsserver mithilfe des <b>Konfigurationstools</b> starten oder stoppen . . . . .	178
Verzeichnisserver und Verwaltungsserver mit dem <b>Konfigurationstool</b> starten oder stoppen . . . . .	179
Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen . . . . .	179
Hauptadministrator-DNs für eine Instanz verwalten . . . . .	180
Hauptadministrator-DN mit dem <b>Konfigurationstool</b> verwalten . . . . .	180
Hauptadministrator-DN mit dem Befehlszeilendienstprogramm verwalten. . . . .	181
Hauptadministratorkennwort für eine Instanz verwalten. . . . .	182
Hauptadministratorkennwort mit dem <b>Konfigurationstool</b> verwalten. . . . .	182
Hauptadministratorkennwort mit dem Befehlszeilendienstprogramm verwalten . . . . .	183
Datenbankkonfiguration für Verzeichnisserverinstanzen. . . . .	183
Datenbank mit dem <b>Konfigurationstool</b> für eine Instanz konfigurieren. . . . .	184
Datenbank mit dem Befehlszeilendienstprogramm für eine Instanz konfigurieren . . . . .	188
Verwaltung des DB2-Datenbankadministratorkennworts . . . . .	190
Administratorkennwort der DB2-Datenbank mit dem <b>Konfigurationstool</b> ändern . . . . .	191
Administratorkennwort der DB2-Datenbank mit dem Befehlszeilendienstprogramm ändern. . . . .	192
Datenbanken von Verzeichnisserverinstanzen dekonfigurieren . . . . .	193
Datenbank mit dem <b>Konfigurationstool</b> von einer Instanz dekonfigurieren . . . . .	193
Datenbank mit dem Befehlszeilendienstprogramm von einer Instanz dekonfigurieren . . . . .	194
Datenbankoptimierung . . . . .	195
Datenbank mit dem <b>Konfigurationstool</b> optimieren . . . . .	195

Datenbank mit dem Befehlszeilendienstprogramm optimieren. . . . .	196
Datenbankpflege . . . . .	196
Datenbankpflege mit dem <b>Konfigurationstool</b> ausführen . . . . .	197
Datenbankpflege mit dem Befehlszeilendienstprogramm ausführen. . . . .	197
Verzeichnisserverbackup. . . . .	198
Datenbank einer Verzeichnisserverinstanz mit dem <b>Konfigurationstool</b> sichern . . . . .	199
Proxy-Server-Instanz mit dem <b>Konfigurationstool</b> sichern. . . . .	200
Verzeichnisserver wiederherstellen . . . . .	201
Datenbank eines Verzeichnisseservers mit dem <b>Konfigurationstool</b> wiederherstellen . . . . .	202
Proxy-Server-Instanz mit dem <b>Konfigurationstool</b> wiederherstellen . . . . .	203
Leistung eines Verzeichnisseservers optimieren. . . . .	203
Verzeichnisserver mit dem <b>Konfigurationstool</b> für die Leistungsoptimierung konfigurieren . . . . .	205
Verzeichnisserver mit dem Befehlszeilendienstprogramm für die Leistungsoptimierung konfigurieren . . . . .	208
Änderungsprotokollverwaltung für Verzeichnisserverinstanzen. . . . .	209
Änderungsprotokoll mit dem <b>Konfigurationstool</b> konfigurieren . . . . .	209
Änderungsprotokoll mit dem Befehlszeilendienstprogramm konfigurieren . . . . .	210
Änderungsprotokoll mit dem <b>Konfigurationstool</b> dekonfigurieren . . . . .	211
Änderungsprotokoll mit dem Befehlszeilendienstprogramm dekonfigurieren. . . . .	212
Suffixkonfiguration . . . . .	213
Suffix mit dem <b>Konfigurationstool</b> hinzufügen . . . . .	213
Suffix mit dem Befehlszeilendienstprogramm hinzufügen . . . . .	214
Suffix mit dem <b>Konfigurationstool</b> entfernen . . . . .	215
Suffix mit dem Befehlszeilendienstprogramm entfernen. . . . .	216
Schemaverwaltung . . . . .	216
Schemadatei mit dem <b>Konfigurationstool</b> verwalten. . . . .	217
Schemadatei mit dem Befehlszeilendienstprogramm verwalten . . . . .	218
Schemavalidierungsregel mit dem <b>Konfigurationstool</b> konfigurieren . . . . .	219
LDIF-Datenmanagement. . . . .	220
LDIF-Daten mit dem <b>Konfigurationstool</b> importieren . . . . .	221
LDIF-Daten mit dem <b>Konfigurationstool</b> prüfen . . . . .	222
LDIF-Daten mit dem <b>Konfigurationstool</b> exportieren . . . . .	223
Active Directory-Synchronisation. . . . .	225
Active Directory-Synchronisation konfigurieren und ausführen . . . . .	226
Active Directory-Synchronisation mit dem <b>Konfigurationstool</b> konfigurieren . . . . .	227
Active Directory-Synchronisation mit dem Befehlszeilendienstprogramm konfigurieren . . . . .	229

**Kapitel 21. Automatisches Starten von Verzeichnisserverinstanzen beim Start des Betriebssystems . . . . . 231**

Automatisches Starten für eine Verzeichnisserverinstanz unter Windows konfigurieren . . . . . 231  
Automatisches Starten für eine Verzeichnisserverinstanz unter UNIX konfigurieren . . . . . 233

**Kapitel 22. Fixpackstrategie . . . . . 237**

Fixpacks mit IBM Installation Manager installieren 237  
    Fixpacks unbeaufsichtigt installieren. . . . . 239  
Fixpacks mit nativen Scripts installieren . . . . . 240

**Kapitel 23. IBM Security Directory Server deinstallieren: Übersicht . . . . . 241**

**Kapitel 24. Deinstallation von IBM Security Directory Server und zusätzlich erforderlicher Software . . . . . 243**

Deinstallation mit IBM Installation Manager . . . . . 244  
    Deinstallation mit IBM Installation Manager . . . . . 244  
    Unbeaufsichtigte Deinstallation mit Antwortdatei . . . . . 245  
    Unbeaufsichtigte Deinstallation mit dem Befehl `imcl uninstall`. . . . . 247  
Deinstallation von IBM Security Directory Server mit Betriebssystemdienstprogrammen . . . . . 248  
    Deinstallation mit AIX-Dienstprogrammen . . . . . 248  
    Deinstallation mit Linux-Dienstprogrammen . . . . . 250  
    Deinstallation mit Solaris-Dienstprogrammen . . . . . 251  
    Deinstallation mit HP-UX-Dienstprogrammen . . . . . 252  
Deinstallation von IBM DB2 mit DB2-Befehlen . . . . . 253  
Deinstallation von IBM Global Security Kit mithilfe von Betriebssystemdienstprogrammen . . . . . 253

IBM Global Security Kit mit SMIT deinstallieren 254  
IBM Global Security Kit mit `installp` deinstallieren . . . . . 254  
IBM Global Security Kit mit Linux-Dienstprogrammen deinstallieren . . . . . 254  
IBM Global Security Kit mit Solaris-Dienstprogrammen deinstallieren . . . . . 255  
IBM Global Security Kit mit HP-UX-Dienstprogrammen deinstallieren . . . . . 256  
IBM Global Security Kit unter Windows deinstallieren . . . . . 256  
Deinstallation von Sprachenpaketen . . . . . 257  
    Sprachenpakete mit Betriebssystemdienstprogrammen deinstallieren . . . . . 257

**Anhang A. Directory Services Markup Language . . . . . 259**

**Anhang B. Beispieldatenbank laden und Server starten . . . . . 261**

**Anhang C. Datei `ldapdb.properties` manuell aktualisieren . . . . . 263**

**Anhang D. Eingabehilfefunktionen für Security Directory Server . . . . . 265**

**Index . . . . . 267**

**Bemerkungen . . . . . 275**



---

## 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)

Die Veröffentlichung *IBM Security Directory Server Installation und Konfiguration* enthält Informationen zur Installation, Konfiguration und Deinstallation von IBM Security Directory Server. Außerdem enthält sie Informationen zur Durchführung eines Upgrades von einer Vorgängerversion des Produkts.

---

## Zugriff auf Veröffentlichungen und Terminologie

Dieser Abschnitt enthält Folgendes:

- Liste der Veröffentlichungen in der „IBM Security Directory Server-Bibliothek“
- Links zu „Onlineveröffentlichungen“ auf Seite viii
- Link auf die „IBM Terminologiewebsite“ auf Seite ix

### 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 Administrator-tasks 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 benötigten 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 Fehlermeldungen 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 Kontaktaufnahme mit IBM Support erfasst werden müssen
- Verschiedene Methoden zur Kontaktaufnahme 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.

---

# Kapitel 1. Planung für die Installation

Sie müssen Hardware, Software, Benutzerrollen, Sicherheit und andere Anforderungen für Ihre Verzeichnisserverumgebung vor der Installation von IBM Security Directory Server festlegen.

## Planungsroadmap

Verwenden Sie die in diesem Abschnitt enthaltene Prüfliste, um einen Server zu installieren.

Wenn Sie ein Upgrade von einem Vorgängerrelease ausführen, dürfen Sie diese Prüfliste allerdings nicht verwenden. Befolgen Sie stattdessen die Anweisungen in Kapitel 14, „Upgrades von Instanzen von Vorgängerversionen durchführen“, auf Seite 93.

Gehen Sie wie folgt vor, um den Server zu installieren:

1. Lesen Sie die Kurzübersicht, um sich einen Überblick über die Komponenten von IBM Security Directory Server zu verschaffen, die von Ihnen installiert werden:
2. Stellen Sie sicher, dass auf dem verwendeten System die Mindestanforderungen für Hardware und Software erfüllt sind. Informationen zu den Anforderungen finden Sie unter „Erforderlicher Plattenspeicherplatz“ auf Seite 3.
3. Installieren Sie IBM Security Directory Server mithilfe von IBM Installation Manager.
4. Melden Sie sich auf Windows-Systemen nach dem Neustart des Systems mit der Benutzer-ID an, die auch bei der Installation verwendet wurde.
5. Verwenden Sie zur Verwaltung der Verzeichnisserverinstanzen das Instance Administration Tool.
6. (Optional) Prüfen Sie die Installation und die Konfiguration, indem Sie die LDIF-Beispieldatei in die Datenbank laden. Weitere Informationen hierzu finden Sie unter Anhang B, „Beispieldatenbank laden und Server starten“, auf Seite 261.
7. Starten Sie die Verzeichnisserverinstanz und (sofern dieses Tool installiert ist) auch das Webverwaltungstool.
8. Informationen zur Konfiguration und Verwendung des Servers und des Webverwaltungstools finden Sie im Abschnitt Verwaltung der IBM Security Directory Server-Dokumentation.

Wenn Sie einen vollständigen Verzeichnisserver installiert haben und nun die Struktur Ihrer Datenbank planen möchten, dann lesen Sie die Informationen unter „Konfigurationsplanung“ auf Seite 129.



---

## Kapitel 2. Installationsübersicht

Sie müssen den Computer vorbereiten und den passenden Installationsmodus für IBM Security Directory Server für Ihre Umgebung auswählen.

Das IBM Installation Manager-basierte Installationsprogramm wird für Windows, Linux64 und AIX bereitgestellt. Wrapperinstallationsprogramme sind für IBM Security Directory Server auf UNIX-Systemen außer Linux 64 und AIX verfügbar. Bei dem Installation Manager-basierten Installationsprogramm werden die grafische Benutzeroberfläche und die unbeaufsichtigte Installation für IBM Security Directory Server V6.3.1 unterstützt.

---

### Erforderlicher Plattenspeicherplatz

Für die erfolgreiche Installation von IBM Security Directory Server sowie der zusätzlich erforderlichen Software muss auf Ihrem Computer der erforderliche Plattenspeicherplatz verfügbar sein. Der erforderliche Plattenspeicherplatz variiert je nach dem Betriebssystem, dem Feature von IBM Security Directory Server und der zusätzlich erforderlichen Software, die Sie für die Installation auswählen.

#### Erforderlicher Plattenspeicherplatz unter Windows

**Anmerkung:** Wenn Sie das Proxy-Server-Feature oder das vollständige Verzeichnisserver-Feature für die Installation auswählen, müssen Sie die Größen für Client SDK, IBM Java Development Kit und den Java-Client nur ein einziges Mal hinzufügen.

*Tabelle 1. Erforderlicher Plattenspeicherplatz für Komponenten von IBM Security Directory Server und die zusätzlich erforderliche Software unter Windows*

Installierbares Feature	Plattenspeicherplatz für die Installation (in MB)
Client Software Development Kit	25 MB
IBM Java Development Kit	200 MB
Java-Client	124 MB
Implementiertes Webverwaltungstool (umfasst die integrierte Version von WebSphere Application Server und das in der integrierten Version von WebSphere Application Server implementierte Webverwaltungstool)	440 MB
Implementierung des Webverwaltungstools in der integrierten Version von WebSphere Application Server oder in WebSphere Application Server	260 MB
Basisserver	23 MB
Proxy-Server (hierbei müssen die Größen für Client SDK, den Java-Client und den Basisserver addiert werden)	40 MB
Vollständiger Verzeichnisserver (hierbei müssen die Größen für Client SDK, den Java-Client und den Basisserver addiert werden)	8 MB
IBM DB2	763 MB

Tabelle 1. Erforderlicher Plattenspeicherplatz für Komponenten von IBM Security Directory Server und die zusätzlich erforderliche Software unter Windows (Forts.)

Installierbares Feature	Plattenspeicherplatz für die Installation (in MB)
IBM Global Security Kit	11 MB

## Erforderlicher Plattenspeicherplatz unter AIX

**Anmerkung:** Wenn Sie das Proxy-Server-Feature oder das vollständige Verzeichnisserver-Feature für die Installation auswählen, müssen Sie die Größen für Client SDK, IBM Java Development Kit und den Java-Client nur ein einziges Mal hinzufügen.

Tabelle 2. Erforderlicher Plattenspeicherplatz für Komponenten von IBM Security Directory Server und die zusätzlich erforderliche Software unter AIX

Installierbares Feature	Plattenspeicherplatz für die Installation (in MB)
Client Software Development Kit	8 MB
IBM Java Development Kit	200 MB
Java-Client	91 MB
Implementiertes Webverwaltungstool (umfasst die integrierte Version von WebSphere Application Server und das in der integrierten Version von WebSphere Application Server implementierte Webverwaltungstool)	443 MB
Implementierung des Webverwaltungstools in der integrierten Version von WebSphere Application Server oder in WebSphere Application Server	500 MB
SSL-Webverwaltungstool	51 MB
Basisserver	39 MB
Proxy-Server (hierbei müssen die Größen für Client SDK, den Java-Client und den Basisserver addiert werden)	4 MB
Vollständiger Verzeichnisserver (hierbei müssen die Größen für Client SDK, den Java-Client und den Basisserver addiert werden)	12 MB
IBM DB2	1250 MB
IBM Global Security Kit	16 MB

## Erforderlicher Plattenspeicherplatz unter Linux

**Anmerkung:** Wenn Sie das Proxy-Server-Feature oder das vollständige Verzeichnisserver-Feature für die Installation auswählen, müssen Sie die Größen für Client SDK, IBM Java Development Kit und den Java-Client nur ein einziges Mal hinzufügen.



Tabelle 3. Erforderlicher Plattenspeicherplatz für Komponenten von IBM Security Directory Server und die zusätzlich erforderliche Software unter Linux

Installierbares Feature	Plattenspeicherplatz für die Installation (in MB)
Client Software Development Kit	9 MB
IBM Java Development Kit	200 MB
Java-Client	166 MB
Implementiertes Webverwaltungstool (umfasst die integrierte Version von WebSphere Application Server und das in der integrierten Version von WebSphere Application Server implementierte Webverwaltungstool)	443 MB
Implementierung des Webverwaltungstools in der integrierten Version von WebSphere Application Server oder in WebSphere Application Server	375 MB
Basisserver	32 MB
Proxy-Server (hierbei müssen die Größen für Client SDK, den Java-Client und den Basisserver addiert werden)	40 MB
Vollständiger Verzeichnisserver (hierbei müssen die Größen für Client SDK, den Java-Client und den Basisserver addiert werden)	8 MB
IBM DB2 (System x Linux)	460 MB
IBM DB2 (System zLinux)	670 MB
IBM DB2 (System i und System p Linux)	520 MB
IBM DB2 (AMD64/EM64T Linux)	1300 MB
IBM Global Security Kit	40 MB

**Anmerkung:** (gilt für ein Installation Manager-basiertes Installationsprogramm) Im Verzeichnis für gemeinsam genutzte Ressourcen sind 200 MB Festplattenspeicherplatz erforderlich. Im Installationsverzeichnis von IBM Security Directory Server sind weitere 200 MB Festplattenspeicherplatz erforderlich.

Speicherbedarf für das temporäre Standardverzeichnis des Systems: Wenn DB2 für die Installation ausgewählt wird, sind 2048 MB + 500 MB freier Speicherplatz im Verzeichnis "temp" erforderlich. Ohne DB2 sind 500 MB freier Speicherplatz im Verzeichnis "temp" erforderlich.

## Erforderlicher Plattenspeicherplatz unter Solaris

**Anmerkung:** Wenn Sie das Server- und das Proxy-Server-Feature für die Installation auswählen, müssen Sie die Größen für den C-Client, IBM Java Development Kit und Java-Client nur ein einziges Mal hinzufügen.

Tabelle 4. Erforderlicher Plattenspeicherplatz für Komponenten von IBM Security Directory Server und die zusätzlich erforderliche Software unter Solaris

Installierbare Komponente	Plattenspeicherplatz für die Installation (in MB)	Anmerkungen
C-Client	11 MB	

Tabelle 4. Erforderlicher Plattenspeicherplatz für Komponenten von IBM Security Directory Server und die zusätzlich erforderliche Software unter Solaris (Forts.)

Installierbare Komponente	Plattenspeicherplatz für die Installation (in MB)	Anmerkungen
IBM Java Development Kit		
Java-Client	145 MB	
Server	47 MB	Größen von C-Client und Java-Client hinzufügen
Proxy-Server	40 MB	Größen von C-Client und Java-Client hinzufügen
<b>Webverwaltungstool</b>	470 MB	Umfasst die integrierte Version von WebSphere Application Server und das in der integrierten Version von WebSphere Application Server implementierte <b>Webverwaltungstool</b>
IBM DB2	1155 MB	
IBM Global Security Kit	34 MB	

## Erforderlicher Plattenspeicherplatz unter HP-UX

Tabelle 5. Erforderlicher Plattenspeicherplatz für Komponenten von IBM Security Directory Server und die zusätzlich erforderliche Software unter HP-UX

Installierbare Komponente	Plattenspeicherplatz für die Installation (in MB)
C-Client	26 MB
IBM Java Development Kit	
Java-Client	172 MB
IBM Global Security Kit	41 MB

## Vorbereitung von Installationsmedien

Das IBM Security Directory Server-Produktpaket enthält IBM Security Directory Server, die dafür zusätzlich erforderliche Software und das Installationsprogramm. Sie können die Installationsmedien von den Installations-DVDs oder von der Passport Advantage-Website abrufen.

Das Produkt IBM Security Directory Server steht in drei unterschiedlichen Dateitypen zur Verfügung: .zip, .tar und .iso. .iso-Dateien enthalten mehrere Dateien, die mehreren .zip- oder .tar-Dateien entsprechen.

Tabelle 6. Das Produkt IBM Security Directory Server steht auf den unterschiedlichen Betriebssystemen in den folgenden Formaten zur Verfügung

AIX, Linux, Solaris und Windows	AIX, Linux, Solaris und HP-UX	Windows
ISO-Image (.iso-Datei)	Bandarchivdateien (.tar-Dateien)	Archivdateien (.zip-Dateien)

Führen Sie die folgenden Tasks durch, um DVDs als Installationsmedien zu verwenden:

- Erstellen Sie für Ihr Betriebssystem ein DVD-Image vom IBM Security Directory Server-Produktimage.
- Speichern Sie das IBM Security Directory Server-Produktimage auf der Festplatte des Computers und ordnen Sie es bei Bedarf über eine Mountoperation zu.

Wenn Sie die Archivdateien des Produkts herunterladen, müssen die folgenden Anforderungen erfüllt sein:

1. Laden Sie alle benötigten Archivdateien in dasselbe Verzeichnis herunter. Laden Sie die Archivdateien nicht in eine Verzeichnisposition herunter, deren Pfadname Leerzeichen enthält.
2. Dekomprimieren Sie alle Archivdateien im selben Verzeichnis, dessen Verzeichnispfad keine Leerzeichen enthält. Der Verzeichnispfad des Installationsprogramms darf kein Leerzeichen enthalten.

Informationen zum Herunterladen des Produkts IBM Security Directory Server von Passport Advantage finden Sie im Kapitel „Software von Passport Advantage herunterladen“.

Nach dem Vorbereiten der Installationsmedien müssen Sie die Softwarevoraussetzungen für Ihr Betriebssystem erfüllen. Informationen dazu finden Sie im Kapitel „Installationsvoraussetzungen“ auf Seite 15.

## Software von Passport Advantage herunterladen

Zur Installation von IBM Security Directory Server müssen Sie die Software von IBM Passport Advantage herunterladen.

### Vorbereitende Schritte

Für den Zugriff auf IBM Passport Advantage müssen Sie sich registrieren und eine Kundenaccountnummer und ein Kennwort abrufen.

### Vorgehensweise

1. Öffnen Sie die Website von IBM Passport Advantage unter [http://www.ibm.com/software/howtobuy/passportadvantage/pao\\_customers.htm](http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm).
2. Klicken Sie auf **Customer sign in**.
3. Geben Sie im Feld **IBM ID** Ihre IBM ID ein.
4. Geben Sie im Feld **Password** Ihr Kennwort ein.
5. Klicken Sie auf **Sign in**.
6. Folgen Sie den Anweisungen, um die Software von IBM Security Directory Server herunterzuladen.

## Verzeichnisstruktur heruntergeladener Dateien

Nach dem Herunterladen der Installationsdateien für IBM Security Directory Server müssen Sie die Verzeichnisstruktur überprüfen.

### Verzeichnisstruktur für Pakete für Windows

Die Dateinamen der Pakete von Security Directory Server 6.3.1 für Windows lauten wie folgt:

DVD-Image: sds631-win.iso

- ZIP-Dateien: – sds631-win-base.zip (Security Directory Server 6.3.1 Client und Server)
- sds631-win-db2.zip (DB2 V9.7)
- sds631-win-ewas.zip (integrierte Version von WebSphere Application Server 7.0.0.29)
- sds631-win-gskit.zip (GSKit 8.0)
- sds631-win-jdk.zip (IBM Java Development Kit)
- sds631-win-IM.zip (IBM Installation Manager)

Nach der Erstellung der DVD oder dem Dekomprimieren der ZIP-Dateien erhalten Sie folgende Verzeichnisstruktur:

- \sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
- ibm\_gskit\ (GSKit)
- license\ (Lizenzen für Security Directory Server und andere verfügbare Produkte)
- quickstart\ (Handbuch für den Schnelleinstieg in Englisch und anderen Sprachen)
- entitlement\ (Berechtigungsdateien für den Proxy-Server)
- entitlement.txt
- tools\ (Tools einschließlich "migbkup")
- migbkup.bat
- ibm\_db2\_32bit\ (DB2)
- ibm\_db2\_64bit\ (DB2)
- ibm\_ewas\_32bit\ (integrierte Version von WebSphere Application Server)
- ibm\_ewas\_64bit\ (integrierte Version von WebSphere Application Server)
- ibm\_im\_32bit\ (IBM Installation Manager)
- ibm\_im\_64bit\ (IBM Installation Manager)
- ibm\_jdk\ (IBM Java Development Kit)
- ibm\_sds\ (Dateien des Installationsprogramms)
- atoc
- files
- native
- Offerings
- plugins
- ShareableEntities
- build.properties
- repository.config
- repository.xml
- launchpad\
  - SilentInstallScripts\ (Antwortdateien für die unbeaufsichtigte Installation)
  - autorun.inf
  - imLauncherWindows.bat
  - launchpad.exe
  - launchpad.ini
  - launchpad64.exe
  - launchpad64.ini
- sds\_install.xml
- write\_sds\_path.bat

## Reines Clientpaket für Windows

ZIP-Datei: – sds631-win-client.zip (Security Directory Server 6.3.1 Client)

Nach dem Dekomprimieren der ZIP-Datei erhalten Sie folgende Verzeichnisstruktur:

- \sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
- ibm\_gskit\ (GSKit 8)

- jdk\ (IBM Java Development Kit)
- ibm\_im\_32bit (IBM Installation Manager)
- ibm\_im\_64bit (IBM Installation Manager)
- ibm\_sds\ (Dateien des Installationsprogramms)
- launchpad\
- SilentInstallScripts\
- autorun.inf
- license\ (Lizenzen für Security Directory Server und andere verfügbare Produkte)
- quickstart\ (Handbuch für den Schnelleinstieg in Englisch und anderen Sprachen)
- ibm\_im\_32bit\ (IBM Installation Manager)
- ibm\_im\_64bit\ (IBM Installation Manager)
- imLauncherWindows.bat
- launchpad.exe
- launchpad.ini
- launchpad64.exe
- launchpad64.ini
- sds\_install.xml
- write\_sds\_path.bat

## Verzeichnisstruktur für Serverpakete für AIX

Die Dateinamen der Pakete von Security Directory Server 6.3.1 für AIX lauten wie folgt:

DVD-Image: sds631-aix-ppc64.iso

TAR-Dateien: - tds63-aix-ppc64-base.tar

(Security Directory Server 6.3.1 Client und Server)

- sds631-aix-ppc64-db2.tar (DB2 V9.7)

- sds631-aix-ppc64-ewas.tar

(integrierte Version von WebSphere Application Server 7.0.0.29)

- sds631-aix-ppc64-gskit.tar (GSKit 8.0)

- sds631-aix-ppc64-jdk.tar (IBM Java Development Kit)

- sds631-aix-ppc64-IM.tar (IBM Installation Manager)

Nach der Erstellung der DVD oder dem Dekomprimieren der TAR-Dateien erhalten Sie folgende Verzeichnisstruktur:

/sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)

- license/ (Lizenzen für Security Directory Server und andere verfügbare Produkte)
- quickstart/ (Handbuch für den Schnelleinstieg in Englisch und anderen Sprachen)
- ibm\_im (IBM Installation Manager)
- ibm\_db2/ (DB2)
- ibm\_ewas/ (integrierte Version von WebSphere Application Server)
- ibm\_gskit/ (GSKit 8)
- ibm\_jdk/ (IBM Java Development Kit)
- ibm\_sds/ (Dateien des Installationsprogramms)
- atoc/
- files/
- native/
- Offerings/
- plugins/
- ShareableEntities
- build.properties
- repository.config
- repository.xml

- tools/ (Tools einschließlich "migbkup")
- launchpad/
- SilentInstallScripts/
- launchpad.sh
- sds\_install.xml
- write\_sds\_path.sh
- entitlement/ (Berechtigungsdateien für den Proxy-Server)
- native / (native Pakete)

## Reines Clientpaket für AIX

ZIP-Datei: - sds631-aix-ppc64-client.tar (Security Directory Server 6.3.1 Client)

Nach dem Dekomprimieren der ZIP-Datei erhalten Sie folgende Verzeichnisstruktur:

- \sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
  - ibm\_gskit\ (GSKit 8)
  - ibm\_jdk\ (IBM Java Development Kit)
  - ibm\_im\ (IBM Installation Manager)
  - ibm\_sds\ (Dateien des Installationsprogramms)
  - launchpad\
  - SilentInstallScripts\
  - autorun.inf
  - license\ (Lizenzen für Security Directory Server und andere verfügbare Produkte)
  - quickstart\ (Handbuch für den Schnelleinstieg in Englisch und anderen Sprachen)
  - ibm\_im\ (IBM Installation Manager)
  - imLauncherWindows.bat
  - launchpad.exe
  - launchpad.ini
  - sds\_install.xml
  - write\_sds\_path.bat

## Verzeichnisstruktur für Serverpakete für Linux x86\_64

Die Dateinamen der Serverpakete von Security Directory Server 6.3.1 für Linux x86\_64 lauten wie folgt:

- DVD-Image: sds631-linux-x86-64.iso
- TAR-Dateien: - sds631-linux-x86-64-base.tar  
(IBM Security Directory Server 6.3.1 Client und Server)
  - sds631-linux-x86-64-IM.tar (IBM Installation Manager)
  - sds631-linux-x86-64-gskit.tar (GSKit 8)
  - sds631-linux-x86-64-db2.tar (DB2 V9.7)
  - sds631-linux-x86-64-ewas.tar  
(integrierte Version von WebSphere Application Server 7.0.0.29)
  - sds631-linux-x86-64-jdk.tar (IBM Java Development Kit)

Nach der Erstellung der DVD oder dem Dekomprimieren der TAR-Dateien erhalten Sie folgende Verzeichnisstruktur:

- /sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
  - license/ (Lizenzen für Security Directory Server und andere verfügbare Produkte)
  - quickstart/ (Handbuch für den Schnelleinstieg in Englisch und anderen Sprachen)
  - ibm\_im (IBM Installation Manager)
  - ibm\_db2/ (DB2)

- ibm\_ewas/ (integrierte Version von WebSphere Application Server)
- ibm\_gskit/ (GSKit 8)
- ibm\_jdk/ (IBM Java Development Kit)
- ibm\_sds/ (Dateien des Installationsprogramms)
- atoc/
- files/
- native/
- Offerings/
- plugins/
- ShareableEntities
- build.properties
- repository.config
- repository.xml
  
- tools/ (Tools einschließlich "migbkup")
- launchpad/
- SilentInstallScripts/
- launchpad.sh
- sds\_install.xml
- write\_sds\_path.sh
- entitlement/ (Berechtigungsdateien für den Proxy-Server)
- native / (natives Paket)

## Reines Clientpaket für Linux x86\_64

ZIP-Datei: - sds631-linux-x86-64-client.tar (Security Directory Server 6.3.1 Client)

Nach dem Dekomprimieren der ZIP-Datei erhalten Sie folgende Verzeichnisstruktur:

- \sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
- ibm\_jdk\ (IBM Java Development Kit)
- ibm\_im (IBM Installation Manager)
- ibm\_sds\ (Dateien des Installationsprogramms)
- launchpad\
- SilentInstallScripts\
- autorun.inf
- license\ (Lizenzen für Security Directory Server und andere verfügbare Produkte)
- quickstart\ (Handbuch für den Schnelleinstieg in Englisch und anderen Sprachen)
- ibm\_im\ (IBM Installation Manager)
- imLauncherWindows.bat
- launchpad.exe
- launchpad.ini
- sds\_install.xml
- write\_sds\_path.bat

## Verzeichnisstruktur für Serverpakete für Linux x86

Die Dateinamen der Serverpakete von Security Directory Server 6.3.1 für Linux x86 lauten wie folgt:

DVD-Image: sds631-linux-x86.iso

TAR-Dateien: - sds631-linux-x86-base.tar

(IBM Security Directory Server 6.3.1 Client und Server)

- sds631-linux-x86-gskit.tar (GSKit 8)
- sds631-linux-x86-db2.tar (DB2 v9.7)

- sds631-linux-x86-ewas.tar  
(integrierte Version von WebSphere Application Server 7.0.0.29)
- sds631-linux-x86-jdk.tar (IBM Java Development Kit)

Nach der Erstellung der DVD oder dem Dekomprimieren der TAR-Dateien erhalten Sie folgende Verzeichnisstruktur:

- /sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
- appsrv/ (integrierte Version von WebSphere Application Server)
- db2 (DB2)
- gskit/ (GSKit 8)
- jdk/ (IBM Java Development Kit)
- ids\_detectGskitVersion
- idsinstall\_i
- idsNativeInstall.sh
- images/ (native Images)
- license (Lizenzen für Security Directory Server und andere Produkte)
- responseFile.txt (Antwortdatei)

### Reines Clientpaket für Linux x86

ZIP-Datei: - sds631-linux-x86-client.tar (Security Directory Server 6.3.1 Client)

Nach dem Dekomprimieren der ZIP-Datei erhalten Sie folgende Verzeichnisstruktur:

- \sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
- gskit/(GSKit 8)
- image/
- license/ (Lizenzen für Security Directory Server und andere Produkte)
- jdk (IBM Java Development Kit)

### Verzeichnisstruktur für Serverpakete für Linux PPC

Die Dateinamen der Serverpakete von Security Directory Server 6.3.1 für Linux PPC lauten wie folgt:

- DVD-Image: sds631-linux-ppc64.iso
- TAR-Dateien: - sds631-linux-ppc64-base.tar  
(IBM Security Directory Server 6.3.1 Client und Server)
- sds631-linux-ppc64-gskit.tar (GSKit 8)
- sds631-linux-ppc64-db2.tar (DB2 V9.7)
- sds631-linux-ppc64-ewas.tar  
(integrierte Version von WebSphere Application Server 7.0.0.29)
- sds631-linux-ppc64-jdk.tar (IBM Java Development Kit)

Nach der Erstellung der DVD oder dem Dekomprimieren der TAR-Dateien erhalten Sie folgende Verzeichnisstruktur:

- /sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
- appsrv/ (integrierte Version von WebSphere Application Server)
- db2 (DB2)
- gskit/ (GSKit 8)
- jdk/ (IBM Java Development Kit)
- ids\_detectGskitVersion
- idsinstall\_i



- idsNativeInstall.sh
- images/ (native Images)
- license (Lizenzen für Security Directory Server und andere Produkte)
- responseFile.txt (Antwortdatei)

## Reines Clientpaket für Linux PPC

ZIP-Datei: - sds631-linux-ppc64-client.tar (Security Directory Server 6.3.1 Client)

Nach dem Dekomprimieren der ZIP-Datei erhalten Sie folgende Verzeichnisstruktur:

- \sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
  - gskit/(GSKit 8)
  - image/
  - license/ (Lizenzen für Security Directory Server und andere Produkte)
  - jdk (IBM Java Development Kit)

## Verzeichnisstruktur für Serverpakete für Linux S/390

Die Dateinamen der Serverpakete von Security Directory Server 6.3.1 für Linux S/390 lauten wie folgt:

- DVD-Image: sds631-linux-s390x.iso
- TAR-Dateien: - sds631-linux-s390x-base.tar
  - (IBM Security Directory Server 6.3.1 Client und Server)
  - sds631-linux-s390x-gskit.tar (GSKit 8)
  - sds631-linux-s390x-db2.tar (DB2 V9.7)
  - sds631-linux-s390x-ewas.tar
    - (integrierte Version von WebSphere Application Server 7.0.0.29)
  - sds631-linux-s390x-jdk.tar (IBM Java Development Kit)

Nach der Erstellung der DVD oder dem Dekomprimieren der TAR-Dateien erhalten Sie folgende Verzeichnisstruktur:

- /sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
  - appsrv/ (integrierte Version von WebSphere Application Server)
  - db2 (DB2)
  - gskit/ (GSKit 8)
  - jdk/ (IBM Java Development Kit)
  - ids\_detectGskitVersion
  - idsinstall\_i
  - idsNativeInstall.sh
  - images/ (native Images)
  - license (Lizenzen für Security Directory Server und andere Produkte)
  - responseFile.txt (Antwortdatei)

## Reines Clientpaket für Linux S/390

ZIP-Datei: - sds631-linux-s390x-client.tar (Security Directory Server 6.3.1 Client)

Nach dem Dekomprimieren der ZIP-Datei erhalten Sie folgende Verzeichnisstruktur:

- \sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
  - gskit/(GSKit 8)

- image/
- license/ (Lizenzen für Security Directory Server und andere Produkte)
- jdk (IBM Java Development Kit)

## **Verzeichnisstruktur für Serverpakete für Solaris x86\_64**

Die Dateinamen der Serverpakete von Security Directory Server 6.3.1 für Solaris x86\_64 lauten wie folgt:

- DVD-Image: sds631-solaris-x86-64.iso  
 TAR-Dateien: - sds631-solaris-x86-64-base.tar  
 (IBM Security Directory Server 6.3.1 Client und Server)
- sds631-solaris-x86-64-gskit.tar (GSKit 8)
  - sds631-solaris-x86-64-db2.tar(DB2 v9.7)
  - sds631-solaris-x86-64-ewas.tar  
 (integrierte Version von WebSphere Application Server 7.0.0.29)
  - sds631-solaris-x86-64-jdk.tar (IBM Java Development Kit)

Nach der Erstellung der DVD oder dem Dekomprimieren der TAR-Dateien erhalten Sie folgende Verzeichnisstruktur:

- /sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
- appsrv/ (integrierte Version von WebSphere Application Server)
  - db2 (DB2)
  - gskit/ (GSKit 8)
  - jdk/ (IBM Java Development Kit)
  - ids\_detectGskitVersion
  - idsinstall\_i
  - idsNativeInstall.sh
  - images/ (native Images)
  - license (Lizenzen für Security Directory Server und andere Produkte)
  - responseFile.txt (Antwortdatei)

## **Reines Clientpaket für Solaris x86\_64**

- ZIP-Datei: - sds631-solaris-x86-64-client.tar (Security Directory Server 6.3.1 Client)

Nach dem Dekomprimieren der ZIP-Datei erhalten Sie folgende Verzeichnisstruktur:

- \sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
- gskit/(GSKit 8)
  - image/
  - license/ (Lizenzen für Security Directory Server und andere Produkte)
  - jdk (IBM Java Development Kit)

## **Verzeichnisstruktur für Serverpakete für Solaris SPARC**

Die Dateinamen der Serverpakete von Security Directory Server 6.3.1 für Solaris SPARC lauten wie folgt:

- DVD-Image:  
 TAR-Dateien: - sds631-solaris-sparc.iso
- sds631-solaris-sparc-base.tar  
 (IBM Security Directory Server 6.3.1 Client und Server)
  - sds631-solaris-sparc-gskit.tar (GSKit 8)

- sds631-solaris-sparc-db2.tar (DB2 v9.7)
- sds631-solaris-sparc-ewas.tar  
(integrierte Version von WebSphere Application Server 7.0.0.29)
- sds631-solaris-sparc-jdk.tar (IBM Java Development Kit)

Nach der Erstellung der DVD oder dem Dekomprimieren der TAR-Dateien erhalten Sie folgende Verzeichnisstruktur:

- /sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
  - appsrv/ (integrierte Version von WebSphere Application Server)
  - db2 (DB2)
  - gskit/ (GSKit 8)
  - jdk/ (IBM Java Development Kit)
  - ids\_detectGskitVersion
  - idsinstall\_i
  - idsNativeInstall.sh
  - images/ (native Images)
  - license (Lizenzen für Security Directory Server und andere Produkte)
  - responseFile.txt (Antwortdatei)

### Reines Clientpaket für Solaris SPARC

ZIP-Datei: - sds631-solaris-sparc-client.tar (Security Directory Server 6.3.1 Client)

Nach dem Dekomprimieren der ZIP-Datei erhalten Sie folgende Verzeichnisstruktur:

- \sdsV6.3.1 (Ausgangsverzeichnis der dekomprimierten Dateien)
  - gskit/ (GSKit 8)
  - image/
  - license/ (Lizenzen für Security Directory Server und andere Produkte)
  - jdk (IBM Java Development Kit)

---

## Installationsvoraussetzungen

Für die Installation von IBM Security Directory Server und der dafür zusätzlich erforderlichen Software müssen möglicherweise vorausgesetzte Programme für Ihr Betriebssystem installiert werden. Die Softwarevoraussetzungen müssen vor der Installation von IBM Security Directory Server und der dafür zusätzlich erforderlichen Software installiert werden.

### Auf verschiedenen Betriebssystemen erforderliche vorausgesetzte Pakete

Sie müssen Ihren Computer mit den vorausgesetzten Paketen aktualisieren, die für die Installation von IBM Security Directory Server und der dafür zusätzlich erforderlichen Komponenten erforderlich sind.

Auf AIX-, Linux-, Solaris- und HP-UX-Betriebssystemen (Itanium) ist die Korn-Shell erforderlich. Unter SuSE Linux Enterprise Server ist PDKSH erforderlich.

Für die Installation von IBM Security Directory Server unter den folgenden Betriebssystemen sind die folgenden vorausgesetzten Pakete erforderlich:

**AIX** Laden Sie für die Installation von rpm-Paketen unter AIX den rpm-Paketmanager für AIX-Systeme von der Website <ftp://public.dhe.ibm.com/aix/freeSoftware/aixtoolbox/INSTALLP/ppc/rpm.rte> herunter.

Tabelle 7. Die auf AIX-Betriebssystemen erforderlichen vorausgesetzten Pakete

Pakete	Grund	Downloadadresse
Web-Browser Mozilla Firefox für AIX	Zum Öffnen des Launchpads unter AIX wird eine unterstützte Version eines Browsers benötigt.	Weitere Informationen zu Web-Browsern für AIX finden Sie auf der Website <a href="http://www.ibm.com/systems/power/software/aix/browsers/">http://www.ibm.com/systems/power/software/aix/browsers/</a> .
gtk+ RPM (gtk2-2.10.6-4.aix5.2.ppc.rpm)	Für Eclipse wurden die Fenstersystemanforderungen auf UNIX-Betriebssystemen von motif in gtk geändert. Aufgrund dieser Fenstersystemänderung in Eclipse müssen unter AIX die gtk-Bibliotheken für die Unterstützung der grafischen Benutzeroberfläche installiert werden. Bei IBM Installation Manager ist die grafische Benutzeroberfläche der Assistentenmodus für die Operation.	Weitere Informationen zur Installation der gtk-Bibliotheken finden Sie in den technischen Hinweisen Required gtk libraries for Installation Manager on AIX auf der Website <a href="http://www.ibm.com/support/docview.wss?uid=swg21631478">http://www.ibm.com/support/docview.wss?uid=swg21631478</a> .
tar für GNU	Um Archivdateien zu dekomprimieren, die mit IBM Security Directory Server auf AIX-Systemen bereitgestellt werden, ist das Dateiarchivprogramm für GNU erforderlich. Sie müssen den Pfad des GNU-Programms tar festlegen, bevor im tar-Programm das Betriebssystem angegeben wird. Das GNU-Programm tar wird im Verzeichnis /opt/freeware/bin installiert und das tar-Programm wird mit dem Betriebssystem im Verzeichnis /usr/bin bereitgestellt. Um den Pfad /opt/freeware/bin festzulegen, führen Sie den folgenden Befehl aus: export PATH=/opt/freeware/bin:\$PATH.	Um die GNU-Archivdatei tar herunterzuladen, besuchen Sie die Website <a href="http://www.ibm.com/systems/power/software/aix/linux/toolbox/alpha.html">http://www.ibm.com/systems/power/software/aix/linux/toolbox/alpha.html</a> .
Dateigruppe X11.adt.lib	Die Dateigruppe X11.adt.lib ist eine Voraussetzung für die Installation der Pakete idsldap.cltjava631 und idsldap.webadmin631 auf AIX-Systemen.	

Tabelle 7. Die auf AIX-Betriebssystemen erforderlichen vorausgesetzten Pakete (Forts.)

Pakete	Grund	Downloadadresse
x1C.rte 8.0.0.6 und x1C.aix50.rte 8.0.0.6 oder höhere Versionen	Für IBM C++ Runtime Environment Components for AIX sind die Laufzeitversionen x1C.rte 8.0.0.6 und x1C.aix50.rte 8.0.0.6 oder höher erforderlich.	
bos.loc.iso.en_US 5.3.0.0	Für IBM Security Directory Server Version 6.3.1 ist eine Mindestversion der Dateigruppe bos.loc.iso.en_US 5.3.0.0 für die Basisebene der Ländereinstellungen des Systems erforderlich.	

## Voraussetzung für LDAP-Client unter PowerPC LE

Um den IBM Security Directory Server-Client unter PowerPC LE (Little Endian) auszuführen, müssen Sie IBM Advance Toolchain Version 7.1 auf dem PowerPC LE-System installieren.

IBM Advance Toolchain Version 7.1 muss installiert werden, unabhängig davon, ob Sie den LDAP-Client ausführen oder mithilfe einer Verbindung zur bereitgestellten Bibliothek eigene Clients schreiben möchten.

Informationen zum Herunterladen und Installieren von IBM Advanced Toolchain Version 7.1 für Ihr Betriebssystem enthält die IBM Advanced Toolchain-Dokumentation.

## Benutzer und Gruppe idsldap

Wenn Sie die Features Server oder Proxy Server für die Installation auswählen, kann das Installationsprogramm den Benutzer und die Gruppe idsldap erstellen.

Das Installationsprogramm erstellt den Benutzer und die Gruppe idsldap, sofern noch nicht vorhanden.

**Anmerkung:** Unter AIX, Linux und Solaris wird bei der Installation mit den Betriebssystemdienstprogrammen der Benutzer idsldap erstellt, sofern noch nicht vorhanden. Wenn jedoch das Verzeichnis /home/idsldap unter Linux und AIX bzw. das Verzeichnis /export/home/idsldap unter Solaris bereits vorhanden ist, kann der Benutzer idsldap möglicherweise nicht erstellt werden. Stellen Sie daher sicher, dass das Ausgangsverzeichnis für idsldap noch nicht vorhanden ist, wenn der Benutzer idsldap noch nicht vorhanden ist.

Für Ihre Umgebung ist es erforderlich, dass Sie den Benutzer und die Gruppe idsldap steuern. Diese können vor der Installation erstellt werden. Der Benutzer und die Gruppe idsldap müssen die folgenden Anforderungen erfüllen:

- Der Benutzer idsldap muss Mitglied der Gruppe idsldap sein.
- Unter AIX, Linux und Solaris muss der Rootbenutzer Mitglied der Gruppe idsldap sein. Unter Windows muss der Administrator Mitglied der Gruppe idsldap sein.
- Für den Benutzer idsldap muss ein Ausgangsverzeichnis vorhanden sein.

- Unter AIX, Linux und Solaris muss die Standardshell für den Benutzer `idsldap` die Korn-Shell sein.
- Für den Benutzer `idsldap` kann optional ein Kennwort festgelegt werden.
- Der Benutzer `idsldap` kann der Verzeichnisserverinstanzeigner sein.

Es müssen alle Anforderungen erfüllt sein, damit IBM Security Directory Server installiert werden kann. Wenn der Benutzer `idsldap` vorhanden ist, aber nicht alle Anforderungen erfüllt sind, schlägt die Installation des Features Proxy Server möglicherweise fehl.

**Anmerkung:** Weitere Informationen zu den Anforderungen an Benutzer-IDs für Instanzeigner, Verzeichnisinstanzeigner und Datenbankeigner finden Sie im Kapitel „Benutzer und Gruppen, die einer Verzeichnisserverinstanz zugeordnet sind“ auf Seite 125.

Sie können **Instance Administration Tool** zum Erstellen von Benutzern und Gruppen erstellen, wenn Sie eine Verzeichnisserverinstanz erstellen. Zum Erstellen des Benutzers und der Gruppe `idsldap` und zum ordnungsgemäßen Einrichten können auch die Dienstprogramme des Betriebssystems verwendet werden.

## Beispiele

Führen Sie die folgenden Betriebssystemdienstprogramme zum Erstellen der Gruppe `idsldap`, des Benutzers `idsldap` und des Kennworts sowie zum Hinzufügen von Root als Mitglied der Gruppe `idsldap` aus.

### Auf AIX-Systemen:

Führen Sie zum Erstellen der Gruppe `idsldap` den folgenden Befehl aus:

```
mkgroup idsldap
```

Führen Sie zum Erstellen der Benutzer-ID `idsldap` als Mitglied der Gruppe `idsldap` und zum Festlegen der Korn-Shell als Standardshell den folgenden Befehl aus:

```
mkuser pgrp=idsldap home=/home/idsldap shell=/bin/ksh idsldap
```

Führen Sie zum Festlegen des Kennworts für den Benutzer `idsldap` den folgenden Befehl aus:

```
passwd idsldap
```

Führen Sie zum Hinzufügen der Rootbenutzer-ID als Mitglied der Gruppe `idsldap` den folgenden Befehl aus:

```
/usr/bin/chgrpmem -m + root idsldap
```

### Auf Linux-Systemen:

Führen Sie zum Erstellen der Gruppe `idsldap` den folgenden Befehl aus:

```
groupadd idsldap
```

Führen Sie zum Erstellen der Benutzer-ID `idsldap` als Mitglied der Gruppe `idsldap` und zum Festlegen der Korn-Shell als Standardshell den folgenden Befehl aus:

```
useradd -g idsldap -d /home/idsldap -m -s /bin/ksh idsldap
```

Führen Sie zum Festlegen des Kennworts für den Benutzer `idsldap` den folgenden Befehl aus:

```
passwd idsldap
```

Führen Sie zum Hinzufügen der Rootbenutzer-ID als Mitglied der Gruppe `idsldap` den folgenden Befehl aus:

```
usermod -G idsldap,rootgroups root
```

Sie können die Werte von `rootgroups` für Ihren Computer mit dem Befehl `groups root` abrufen.

#### **Auf Solaris-Systemen:**

Führen Sie zum Erstellen der Gruppe `idsldap` den folgenden Befehl aus:

```
groupadd idsldap
```

Führen Sie zum Erstellen der Benutzer-ID `idsldap` als Mitglied der Gruppe `idsldap` und zum Festlegen der Korn-Shell als Standardshell den folgenden Befehl aus:

```
useradd -g idsldap -d /export/home/idsldap -m -s /bin/ksh idsldap
```

Führen Sie zum Festlegen des Kennworts für den Benutzer `idsldap` den folgenden Befehl aus:

```
passwd idsldap
```

Führen Sie zum Hinzufügen der Rootbenutzer-ID als Mitglied der Gruppe `idsldap` den folgenden Befehl aus:

```
usermod -G idsldap,root idsldap
```

Verwenden Sie ein entsprechendes Tool, um die Rootbenutzer-ID so zu ändern, dass Root Mitglied der Gruppe `idsldap` wird.

Weitere Informationen zum Befehl zum Hinzufügen von Benutzern und Gruppen finden Sie in der Dokumentation zu Ihrem Betriebssystem.

---

## **Installationsmethoden**

Für die Installation von IBM Security Directory Server und der dafür zusätzlich erforderlichen Software müssen Sie die am besten geeignete Installationsmethode für Ihre Umgebung auswählen.

Sie können IBM Security Directory Server und die dafür zusätzlich erforderliche Software mithilfe der folgenden Methoden installieren:

- Installation mit IBM Installation Manager
- Installation mit den Befehlszeilendienstprogrammen des Betriebssystems

#### **Vorsicht:**

- **Auf einem Computer dürfen keine unterschiedlichen Installationsmodi verwendet werden. Sie können die Installation von IBM Security Directory Server entweder mithilfe von IBM Installation Manager oder mithilfe der Befehlszeilendienstprogramme des Betriebssystems durchführen, aber nicht auf beide Arten. Wenn Sie beide Installationsmodi verwenden, werden möglicherweise nicht die richtigen Pakete für ein Feature installiert.**
- **Vermeiden Sie es, DB2 und eine integrierte Version von WebSphere Application Server manuell in den jeweiligen Standardinstallationspfaden, die von IBM Installation Manager verwendet werden, zu installieren. Bei der Installation, Änderung oder Deinstallation mithilfe von IBM Installation Manager können durch eine derartige manuelle Installation Fehler verursacht werden. Weitere Informationen zum Standardinstallationspfad finden Sie im Kapitel „Standardinstallationspositionen“ auf Seite 28.**





---

## Kapitel 3. Installation mit IBM Installation Manager

IBM Installation Manager ist ein Tool für die Installation und Wartung von IBM Security Directory Server und der dafür zusätzlich erforderlichen Software.

---

### Übersicht über IBM Installation Manager

IBM Installation Manager ist ein Installationsassistent, der Sie durch die Schritte zum Installieren, Ändern, Aktualisieren, Durchführen von Rollbacks oder Deinstallieren von IBM Produkten führt. Für die Installation können ferne oder lokale Software-Repositorys verwendet werden.

IBM Installation Manager hilft Ihnen außerdem auf folgende Art und Weise beim Verwalten von IBM Anwendungen und Paketen, die auf Ihrem Computer installiert werden:

- Durch Aufzeichnen von Installationen
- Durch Bestimmen und Anzeigen von für die Installation verfügbaren Paketen
- Durch Prüfen von Voraussetzungen und gegenseitigen Abhängigkeiten

IBM Installation Manager umfasst sechs Assistenten, durch die das Verwalten von Paketen vereinfacht wird:

- Der Assistent zum **Installieren** unterstützt Sie beim Installationsprozess. Es können mehrere Pakete gleichzeitig installiert werden. Sie können die Standardeinstellungen akzeptieren oder die Einstellungen ändern, um eine angepasste Installation zu erstellen, wo es möglich ist. Vor der Installation wird Ihnen eine vollständige Zusammenfassung Ihrer im Assistenten vorgenommenen Auswahl angezeigt.
- Der Assistent für **Aktualisierungen** sucht nach verfügbaren Updates der Pakete, die auf Ihrem System installiert sind. Informationen zu den Inhalten der Updates werden im Assistenten bereitgestellt. Sie können auswählen, ob ein Update angewendet werden soll.
- Der Assistent zum **Ändern** hilft Ihnen beim Ändern bestimmter Elemente von Paketen, die Sie bereits installiert haben. Während der Erstinstallation eines Pakets können Sie die zu installierenden Features auswählen. Wenn Sie später weitere Features benötigen, können Sie den Assistenten zum Ändern von Paketen verwenden, um diese zu Ihrem Paket hinzuzufügen. Sie können auch Features entfernen.
- Der Assistent für die **Verwaltung von Lizenzen** hilft Ihnen beim Einrichten der Lizenzen für Ihre Pakete. Verwenden Sie diesen Assistenten zum Ändern Ihrer Testlizenz in eine Volllizenz, zum Einrichten Ihres Servers für Floating-Lizenzen und zum Auswählen der für die einzelnen Pakete zu verwendenden Lizenztypen.
- Der Assistent für **Rollbacks** hilft Ihnen beim Zurücksetzen von Paketen auf eine Vorgängerversion.
- Mithilfe des Assistenten zum **Deinstallieren** werden Pakete vom Computer entfernt. Es können mehrere Pakete gleichzeitig deinstalliert werden.

---

## Unterstützte Betriebssysteme

Sie können IBM Installation Manager für die Installation von IBM Security Directory Server unter AIX (ppc64), Linux (AMD64/EM64T-Architektur) und Microsoft Windows verwenden.

In den folgenden Abschnitten sind die Betriebssystemversionen aufgelistet, die für die Installation von IBM Security Directory Server mit IBM Installation Manager unterstützt werden.

Gehen Sie wie folgt vor, wenn Sie IBM Security Directory Server auf einem Betriebssystem installieren möchten, das nicht in den folgenden Abschnitten aufgelistet ist:

1. Prüfen Sie, ob die Version des Betriebssystems für IBM Security Directory Server unterstützt wird. Eine Liste für alle unterstützten Betriebssysteme finden Sie in der *Produktübersicht zu IBM Security Directory Server*.
2. Wenn sie unterstützt wird, können Sie die Befehlszeilendienstprogramme des Betriebssystems für die Installation von IBM Security Directory Server verwenden.

### AIX (ppc64)

- AIX Version 6.1
- AIX Version 7.1

### Linux (AMD64/EM64T)

- Red Hat Enterprise Linux 5, Advanced Platform
- Red Hat Enterprise Linux 6
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11

### Microsoft Windows (x64)

- Microsoft Windows Server 2008 R2, Enterprise Edition
- Microsoft Windows Server 2008 R2, Standard Edition
- Microsoft Windows Server 2008, Enterprise Edition
- Microsoft Windows Server 2008, Standard Edition
- Microsoft Windows Server 2012, Standard Edition

---

## Installationspakettypen für IBM Security Directory Server

Um das richtige Installationspaket für IBM Security Directory Server auszuwählen, müssen Sie die verfügbaren Installationspakettypen kennen.

Die folgenden Installationspakettypen für IBM Security Directory Server sind für die Installation mit IBM Installation Manager verfügbar:

*Tabelle 8. Installationspakettyp für IBM Security Directory Server und die für die Installation verfügbaren Features*

Alle Features	Features im vollständigen Produktinstallationsprogramm	Features im Nur-Client-Installationsprogramm
IBM DB2	Ja	Nein
IBM Global Security Kit	Ja	Ja
C-Client	Ja	Ja
IBM Java Development Kit	Ja	Ja

Tabelle 8. Installationspakettyp für IBM Security Directory Server und die für die Installation verfügbaren Features (Forts.)

Alle Features	Features im vollständigen Produktinstallationsprogramm	Features im Nur-Client-Installationsprogramm
Java-Client	Ja	Ja
Server	Ja	Nein
Proxy-Server	Ja	Nein
Webverwaltungstool	Ja	Nein

**Anmerkung:** Wenn Sie das **Webverwaltungstool** installieren, stellt IBM Installation Manager eine Option zum Installieren einer integrierten Version von WebSphere Application Server bereit.

---

## Installationsrichtlinien

Vor der Installation von IBM Security Directory Server mit IBM Installation Manager müssen Sie einige Beschränkungen beachten.

### Installationsmethode

Wenn Sie IBM Security Directory Server installieren, können Sie auswählen, ob Sie die Installation mithilfe von IBM Installation Manager oder über die Befehlszeilendienstprogramme des Betriebssystems durchführen möchten. Bei weiteren Installationen oder Deinstallationen von IBM Security Directory Server-Paketen, -Features und Fixpacks auf demselben System muss dieselbe Installationsmethode verwendet werden. Wenn Sie IBM Security Directory Server beispielsweise mithilfe von IBM Installation Manager installieren, dürfen Sie nicht die Befehlszeilendienstprogramme verwenden, um Features zu installieren oder das Produkt zu deinstallieren. Wenn Sie dies doch tun, kann die Installation von IBM Security Directory Server beschädigt oder nicht verwendbar werden.

### IBM Installation Manager-Version

IBM Installation Manager wird ab Version 1.7.0 für die Installation von IBM Security Directory Server unterstützt. Auf der Seite **Install Packages** von IBM Installation Manager wird eine Fehlermeldung angezeigt und Sie können in den folgenden Szenarios nicht mit der Installation fortfahren:

- Sie versuchen, die Installation von IBM Security Directory Server mit einer Vorgängerversion von IBM Installation Manager zu starten.
- Beim Starten der Installation von IBM Security Directory Server vom Launchpadprogramm wird eine Vorgängerversion von IBM Installation Manager erkannt.

### Mehrfachinstallation

Es ist nicht möglich, eine einzige Version von IBM Security Directory Server mehrfach auf demselben System zu installieren. Wenn Sie das Installationspaket für dieselbe Version erneut auswählen, wird in IBM Installation eine Warnung generiert und Sie können nicht mit der Installation fortfahren. Unterschiedliche Versionen von IBM Security Directory Server können jedoch auf demselben System koexistieren.

### Installationsposition auf AIX- und Linux-Systemen:

IBM Security Directory Server kann auf AIX- und Linux-Systemen nur in der vordefinierten Position installiert werden. Der Pfad wird standardmäßig im Feld **Installation Directory** in IBM Installation Manager angegeben. Dieses Feld kann in IBM Installation Manager bearbeitet werden, aber wenn Sie den standardmäßig angegebenen Pfad ändern, können Sie nicht auf **Next** klicken, um mit der Installation fortzufahren. Setzen Sie den Pfad wieder auf den Standardinstallationspfad für IBM Security Directory Server zurück.

Diese Beschränkung gilt nicht für Microsoft Windows-Betriebssysteme. IBM Security Directory Server kann auf Microsoft Windows-Betriebssystemen in einer beliebigen Position installiert werden. Auch wenn Sie die Standardinstallationsposition für IBM Security Directory Server ausgewählt haben, werden das enthaltene Verzeichnis `idsinstinfo` und die enthaltene Datei `idsinstances.ldif` immer auf der von `%SystemDrive%` angegebenen Partition erstellt. Wenn IBM Security Directory Server auf dem Laufwerk E: installiert wird und sich das Betriebssystem auf dem Laufwerk C: befindet, fallen Ihnen möglicherweise die folgenden Änderungen auf:

- Das Verzeichnis `idsinstinfo` wird auf dem Laufwerk C: (`C:\idsinstinfo`) statt im Verzeichnis `E:\Program Files\IBM\ldap` erstellt.

Weitere Informationen zu den Standardinstallationspositionen finden Sie im Kapitel „Standardinstallationspositionen“ auf Seite 28.

---

## IBM Security Directory Server-Komponenten

Wenn Sie IBM Security Directory Server mit IBM Installation Manager installieren, können Sie die zu installierenden Komponenten auswählen. In IBM Installation Manager werden die Abhängigkeiten aller ausgewählten Komponenten angezeigt.

Die folgenden IBM Security Directory Server-Komponenten stehen für die Installation zur Verfügung:

### IBM DB2

Sie können IBM DB2 als Feature installieren. Wenn eine unterstützte Version von IBM DB2 installiert wird, muss nicht die DB2-Version installiert werden, die im IBM Security Directory Server-Paket bereitgestellt wird. Informationen zu unterstützten Versionen von DB2 für verschiedene Betriebssysteme finden Sie in der *Produktübersicht zu IBM Security Directory Server*.

Für den vollständigen Verzeichnisserver ist IBM DB2 erforderlich, weil die Verzeichnisdaten in einer DB2-Datenbank gespeichert werden. IBM DB2 ist für Proxy Server nicht erforderlich.

### IBM Global Security Kit

Sie können IBM Global Security Kit (GSKit) zusammen mit anderen Features von IBM Security Directory Server als Feature installieren. GSKit ist ein optionales Feature, das nur erforderlich ist, wenn Sie ein SSL- (Secure Sockets Layer) oder TLS- (Transport Layer Security) Kommunikationsprotokoll verwenden möchten. GSKit muss sowohl auf Server- als auch auf Clientsystemen installiert sein, damit sichere Verbindungen aufgebaut und verwendet werden können.

### C-Client

Sie können C Client entweder als selbständiges Feature oder zusammen mit anderen Features von IBM Security Directory Server installieren. Das Feature C Client ist nicht von anderen Features abhängig. Die Features Ser-

ver und Proxy Server sind jedoch von C Client abhängig. Wenn Sie die Features Server oder Proxy Server installieren, wird das Feature C Client automatisch für die Installation ausgewählt.

C Client ist ein Client-SDK (Software Development Kit), das die erforderlichen Tools zum Entwickeln von LDAP-Anwendungen in der Programmiersprache C bereitstellt. Das C Client-Paket enthält die folgenden Dateien und Anwendungen:

- Clientbibliotheken, die eine Gruppe von APIs (Application Programming Interfaces, Anwendungsprogrammierschnittstellen) für die Programmiersprache C bereitstellen
- C-Headerdateien zum Erstellen und Kompilieren von LDAP-Anwendungen
- C-Server und -Clientdienstprogramme
- Beispielprogramme im Quellenformat

### **IBM Java Development Kit**

Sie können IBM Java Development Kit entweder als selbständiges Feature oder zusammen mit anderen Features von IBM Security Directory Server installieren. Wenn Sie IBM Java Development Kit installieren, extrahiert IBM Installation Manager die komprimierte Datei in das Unterverzeichnis java in der Installationsposition von IBM Security Directory Server. IBM Java Development Kit stellt IBM Java SDK und Java 1.6 SR 14 bereit. Zum Kompilieren von Java-Beispielprogrammen und zum Ausführen von Java-Programmen wie **Instance Administration Tool (idsxinst)** und dem **Konfigurationstool (idsxcfg)** ist IBM Java Development Kit erforderlich.

### **Java-Client**

Sie können Java Client entweder als selbständiges Feature oder zusammen mit anderen Features von IBM Security Directory Server installieren. Das Java Client-Feature ist nicht von anderen Features abhängig. Die Features Server und Proxy Server sind jedoch von Java Client abhängig. Wenn Sie die Features Server oder Proxy Server installieren, wird das Feature Java Client automatisch für die Installation ausgewählt.

Java Client enthält das IBM Security Directory Server JNDI-Toolkit und Java Client-Dienstprogramme.

**Server** Sie können Server zusammen mit anderen Features von IBM Security Directory Server als Feature installieren. Das Feature Server ist von den Features C Client und Java Client abhängig. Wenn Sie das Feature Server für die Installation auswählen, werden auch die Features C Client und Java Client für die Installation ausgewählt.

Server muss einen vollständigen Verzeichnisserver oder einen LDAP-Server erstellen. Sie müssen einen vollständigen Verzeichnisserver mit einer Datenbankinstanz konfigurieren. Dieser verarbeitet Clientanforderungen, für die auf in der Datenbank gespeicherte Einträge zugegriffen werden muss. Für einen vollständigen Verzeichnisserver ist DB2 erforderlich.

### **Proxy-Server**

Sie können Proxy Server zusammen mit anderen Features von IBM Security Directory Server als Feature installieren. Das Feature Proxy Server ist von den Features C Client und Java Client abhängig. Wenn Sie das Feature Proxy Server für die Installation auswählen, werden auch die Features C Client und Java Client für die Installation ausgewählt.

Proxy Server ist ein LDAP-Server, der als Front-End-Einheit für das Verzeichnis eingesetzt wird. Er dient zur Authentifizierung von Clientanforde-

rungen für das gesamte Verzeichnis und leitet Anforderungen an vollständige Verzeichnisserver weiter. Proxy Server kann auch am Front-End eines Serverclusters oder eines verteilten Verzeichnisses zur Bereitstellung von Failover und Lastausgleich eingesetzt werden.

### **Webverwaltungstool**

Sie können das **Webverwaltungstool** entweder als selbständiges Feature oder zusammen mit anderen Features von IBM Security Directory Server installieren. Das **Webverwaltungstool** ist ein optionales Feature, das erforderlich ist, wenn Sie Ihren Verzeichnisserver über Fernzugriff verwalten möchten. Zur Verwendung des **Webverwaltungstools** müssen Sie das Tool auf einer unterstützten Version der integrierten Version von WebSphere Application Server oder von WebSphere Application Server implementieren.

Wenn Sie das **Webverwaltungstool** installieren, werden DSML-Dateien (Directory Services Markup Language) auch auf Ihren Computer kopiert. Weitere Informationen zu DSML finden Sie in Anhang A, „Directory Services Markup Language“, auf Seite 259.

Sie können das **Webverwaltungstool** als Konsole zum Verwalten von Verzeichnissen verwenden. Diese können von den folgenden Typen sein:

- IBM Security Directory Server Version 6.3.1
- IBM Security Directory Server Version 6.3
- IBM Security Directory Server Version 6.2
- IBM Security Directory Server Version 6.1
- IBM Security Directory Server Version 6.0
- i5/OS V5 R4
- z/OS V1 R6 Integrated Security Services
- z/OS V1 R8 Integrated Security Services
- z/OS V1 R8 IBM Tivoli Directory Server
- z/OS V1 R9 IBM Tivoli Directory Server
- z/OS V1 R10 IBM Tivoli Directory Server

**Wichtig:** Unter z/OS wird das Verwalten von Verzeichnisdaten unterstützt, aber nicht die Serververwaltung.

### **Integrierte Version von WebSphere Application Server**

Sie können eine integrierte Version von WebSphere Application Server installieren, wenn Sie die Installation des **Webverwaltungstools** auswählen. Die integrierte Version von WebSphere Application Server ist nur erforderlich, wenn Sie das **Webverwaltungstool** bereitstellen und ausführen möchten. Wenn auf Ihrem System eine unterstützte Version von WebSphere Application Server installiert ist, können Sie auswählen, dass keine integrierte Version von WebSphere Application Server installiert werden soll. Sie können das **Webverwaltungstool** auf einem vorhandenen WebSphere Application Server oder auf einer auf Ihrem System installierten integrierten Version von WebSphere Application Server installieren.

## Anpassung der Installation von IBM Security Directory Server

Sie können die Installation von IBM Security Directory Server entsprechend Ihrer Produktverwendung anpassen.

Sie können die Installation von IBM Security Directory Server für einen der folgenden Zwecke kategorisieren:

- Vollständiges Produkt
- Vollständiger Verzeichnisserver
- Proxy-Server
- Client
- Verwaltung über einen fernen Server mithilfe des **Webverwaltungstools**

*Tabelle 9. IBM Security Directory Server-Features für die Installation basierend auf der Verwendung des Produkts*

Alle Features	Vollständiger Verzeichnisserver	Proxy-Server	Client	Verwaltung über einen fernen Server mithilfe des Webverwaltungstools
IBM DB2	Ja	Nein	Nein	Nein
IBM Global Security Kit	Ja	Ja	Ja	Nein
C-Client	Ja	Ja	Ja	Nein
IBM Java Development Kit	Ja	Ja	Ja	Nein
Java-Client	Ja	Ja	Ja	Nein
Server	Ja	Nein	Nein	Nein
Proxy-Server	Nein	Ja	Nein	Nein
<b>Webverwaltungstool</b>	Optional	Optional	Nein	Ja

**Anmerkung:** Wenn Sie das **Webverwaltungstool** installieren, stellt IBM Installation Manager eine Option zum Installieren einer integrierten Version von WebSphere Application Server bereit.

Sie können optional eine integrierte Version von WebSphere Application Server und das **Webverwaltungstool** für die Installation mit einem vollständigen Verzeichnisserver und einem Proxy-Server auswählen.

## Standardinstallationspositionen

Wenn Sie IBM Installation Manager für die Installation ausführen, werden IBM Security Directory Server und die dafür zusätzlich erforderliche Software in der vordefinierten Installationsposition installiert.

Tabelle 10. Die Standardinstallationspositionen von IBM Security Directory Server, IBM DB2, der integrierten Version von WebSphere Application Server und IBM Java Development Kit.

Betriebssystem	IBM Security Directory Server	IBM DB2	Integrierte Version von WebSphere Application Server	IBM Java Development Kit
Linux	/opt/ibm/ldap/V6.3.1	/opt/ibm/sdsV6.3.1db2	/opt/ibm/ldap/V6.3.1/appsrv	/opt/ibm/ldap/V6.3.1/java
AIX	/opt/IBM/ldap/V6.3.1	/opt/IBM/sdsV6.3.1db2	/opt/IBM/ldap/V6.3.1/appsrv	/opt/IBM/ldap/V6.3.1/java
Microsoft Windows	C:\Program Files\IBM\ldap\V6.3.1	C:\Program Files\IBM\sdsV6.3.1db2	C:\Program Files\IBM\ldap\V6.3.1\appsrv	C:\Program Files\IBM\ldap\V6.3.1\java

IBM Security Directory Server kann auf AIX- und Linux-Systemen nur in der vordefinierten Position installiert werden. Der Pfad wird standardmäßig im Feld **Installation Directory** in IBM Installation Manager angegeben. Dieses Feld kann in IBM Installation Manager bearbeitet werden, aber wenn Sie den standardmäßig angegebenen Pfad ändern, können Sie nicht auf **Next** klicken, um mit der Installation fortzufahren. Setzen Sie den Pfad wieder auf den Standardinstallationspfad für IBM Security Directory Server zurück.

Diese Beschränkung gilt nicht für Microsoft Windows-Betriebssysteme. IBM Security Directory Server kann auf Microsoft Windows-Betriebssystemen in einer beliebigen Position installiert werden. Auch wenn Sie die Standardinstallationsposition für IBM Security Directory Server ausgewählt haben, werden das enthaltene Verzeichnis `idsinstinfo` und die enthaltene Datei `idsinstances.ldif` immer auf der von `%SystemDrive%` angegebenen Partition erstellt. Wenn IBM Security Directory Server auf dem Laufwerk E: installiert wird und sich das Betriebssystem auf dem Laufwerk C: befindet, fallen Ihnen möglicherweise die folgenden Änderungen auf:

- Das Verzeichnis `idsinstinfo` wird auf dem Laufwerk C: (`C:\idsinstinfo`) statt im Verzeichnis `E:\Program Files\IBM\ldap` erstellt.



---

## Installationsrepositorys

Das Installationsrepository ist die Position, in der die IBM Security Directory Server-Pakete für die Installation zur Verfügung stehen.

Sie können IBM Security Directory Server von einer der folgenden Speicherpositionen installieren:

- Produktkonfigurationsdatenträger
- Fernes, gemeinsam genutztes Laufwerk oder ein lokales Verzeichnis, das ein elektronisches Image des Installationspakets enthält

Sie können das Repository zum Starten einer Installation auf die folgenden Arten verwenden:

- Verwenden Sie das Launchpad zum Starten einer Installation von:
  - einem Produktkonfigurationsdatenträger
  - einem elektronischen Image des Installationspakets auf einem fernen gemeinsam genutzten Laufwerk oder einem lokalen Verzeichnis

Wenn Sie das Launchpad verwenden, ist der Installationsprozess bereits mit der Position des Repositorys, das das Installationspaket enthält, konfiguriert.

- Starten Sie IBM Installation Manager direkt und geben Sie die Repositoryvorgaben manuell an. Beispiel:
  - Die URL für das Repository auf einem Web-Server
  - Den Pfad zu einem fernen gemeinsam genutzten Laufwerk, auf dem sich das Produktpaket befindet

---

## Installation starten

Sie können die Installation von IBM Security Directory Server entweder über das Launchpad oder über IBM Installation Manager starten, wobei die Repository-Vorgaben festgelegt sein müssen.

### Installation mit dem Launchpad starten

Das Launchpad stellt eine integrierte Position zum Starten des Installationsprozesses bereit.

#### Informationen zu diesem Vorgang

Sie können eine Installation in folgenden Szenarios mit dem Launchpad starten:

- Installation von einem Produktinstallationsdatenträger
- Installation von einem lokalen Verzeichnis oder einem fernen gemeinsam genutzten Laufwerk, das ein elektronisches Image des Produktpakets enthält

Wenn Sie die Installation mit dem Launchpad starten, wird IBM Installation Manager automatisch installiert, wenn sich auf Ihrem System keine unterstützte Version befindet.

## Vorgehensweise

1. Wechseln Sie in das Stammverzeichnis Ihres Installationspakets.
  - Wenn Sie den Produktinstallationsdatenträger von IBM Security Directory Server verwenden, legen Sie den Datenträger in das Plattenlaufwerk ein.
  - Wenn Sie die Installation von einem elektronischen Image des Produktinstallationspakets ausführen, wechseln Sie in das Verzeichnis, in dem sich das Image befindet.
2. Start Sie das Launchpad.

**Anmerkung:** Klicken Sie auf Windows-Betriebssystemen mit der rechten Maustaste auf die .exe-Datei des Launchpads und wählen Sie **Als Administrator ausführen** aus.

Betriebssystem	Befehl:
32-Bit-Windows	launchpad.exe
64-Bit-Windows	launchpad64.exe
AIX und Linux	./launchpad.sh

Das Launchpad von IBM Security Directory Server wird gestartet und die Begrüßungsseite wird angezeigt.

3. Wählen Sie auf der Begrüßungsseite in der Liste mit den Sprachen die gewünschte Sprache aus und klicken Sie auf **OK**.
4. Klicken Sie im Navigationsbereich auf der linken Seite auf **Installation von IBM Security Directory Server**.
5. Klicken Sie auf der Seite **Installation** auf den Link zum Starten des Installationsprogramms von IBM Security Directory Server. IBM Installation Manager wird gestartet.
6. Stellen Sie sicher, dass die folgenden Pakete für die Installation ausgewählt werden:
  - IBM Installation Manager (Wird nur aufgeführt, wenn auf Ihrem System noch keine unterstützte Version installiert ist.)
  - IBM Security Directory Server
7. Fahren Sie mit den Schritten zur Installation von IBM Security Directory Server fort. Siehe „Installation mit IBM Installation Manager“ auf Seite 32.
8. Klicken Sie auf **Exit**, wenn Sie die Installation abgeschlossen haben.

## Ergebnisse

Wenn Sie die Installation von IBM Security Directory Server mit dem Launchpad starten, erstellt das Launchpad eine temporäre Datei namens `sds631.temp`, die den Pfadnamen des Datenträgers enthält. Die Datei `sds631.temp` wird auf dem Betriebssystem an der folgenden Position erstellt.

### AIX und Linux

`/tmp`

### Microsoft Windows

Das in der Variablen `TEMP` festgelegte standardmäßige temporäre Verzeichnis des Systems

Es ist nicht möglich, eine einzige Version von IBM Security Directory Server mehrfach auf demselben System zu installieren. Wenn Sie das Installationspaket für dieselbe Version erneut auswählen, wird in IBM Installation eine Warnung generiert

und Sie können nicht mit der Installation fortfahren. Unterschiedliche Versionen von IBM Security Directory Server können jedoch auf demselben System koexistieren.

## Nächste Schritte

Fahren Sie mit den Schritten zur Installation von IBM Security Directory Server fort. Siehe „Installation mit IBM Installation Manager“ auf Seite 32.

## Installation durch Festlegen von Repository-Vorgaben starten

Wenn die unterstützte Version von IBM Installation Manager auf Ihrem System installiert ist, können Sie das Tool direkt starten und die Repository-Vorgaben angeben.

## Vorbereitende Schritte

IBM Installation Manager wird ab Version 1.7.0 für die Installation von IBM Security Directory Server unterstützt. Auf der Seite **Install Packages** von IBM Installation Manager wird eine Fehlermeldung angezeigt und Sie können in den folgenden Szenarios nicht mit der Installation fortfahren:

- Sie versuchen, die Installation von IBM Security Directory Server mit einer Vorgängerversion von IBM Installation Manager zu starten.
- Beim Starten der Installation von IBM Security Directory Server vom Launchpadprogramm wird eine Vorgängerversion von IBM Installation Manager erkannt.

Wenn sich auf Ihrem System eine frühere Version als IBM Installation Manager Version 1.7.0 befindet, müssen Sie ein Upgrade auf Version 1.7.0 oder höher durchführen. Zur Installation der erforderlichen Version von IBM Installation Manager stehen Ihnen die folgenden Verfahren zu Verfügung.

- Starten Sie die Installation von IBM Installation Manager mit dem Launchpad. Weitere Informationen hierzu finden Sie unter „Installation mit dem Launchpad starten“ auf Seite 29.
- Laden Sie IBM Installation Manager Version 1.7.0 oder höher für Ihr Betriebssystem herunter. Weitere Informationen zur Installation von IBM Installation Manager im unbeaufsichtigten Modus finden Sie in der Dokumentation zu IBM Installation Manager unter <http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome>.

## Informationen zu diesem Vorgang

Sie können die Installation starten, indem Sie in den folgenden Installationsszenarios die Repository-Vorgaben festlegen:

- Installation von einem lokalen Verzeichnis oder einem fernen gemeinsam genutzten Laufwerk, das das von IBM Passport Advantage heruntergeladene Produktpaket enthält
- Installation von einer URL für das Repository auf einem Web-Server

## Vorgehensweise

1. Starten Sie IBM Installation Manager.

### Windows

Klicken Sie im Menü **Start** auf **Alle Programme > IBM Installation Manager > IBM Installation Manager**.

### AIX und Linux

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein. Ändern Sie den folgenden Standardpfad, wenn IBM Installation Manager an einer anderen Position installiert ist.

```
/opt/IBM/InstallationManager/eclipse/IBMIM
```

2. Klicken Sie auf der Startseite von IBM Installation Manager auf **File > Preferences**.
3. Klicken Sie auf der Seite **Repositories** auf **Add Repository**.
4. Geben Sie auf der Seite **Add Repository** die URL der Repository-Position ein oder navigieren Sie zu ihr und legen Sie einen Dateipfad fest.
5. Klicken Sie auf **OK**. Wenn Sie eine HTTPS- oder eine eingeschränkte Repository-Position angegeben haben, werden Sie aufgefordert, eine Benutzer-ID und ein Kennwort einzugeben. Die neue oder geänderte Repository-Position wird aufgeführt.
6. Klicken Sie auf **Test Connections**, um den Zugriff auf das Repository zu überprüfen.
7. Klicken Sie auf **OK**, um die Seite **Repositories** zu schließen.

### Ergebnisse

Es ist nicht möglich, eine einzige Version von IBM Security Directory Server mehrfach auf demselben System zu installieren. Wenn Sie das Installationspaket für dieselbe Version erneut auswählen, wird in IBM Installation eine Warnung generiert und Sie können nicht mit der Installation fortfahren. Unterschiedliche Versionen von IBM Security Directory Server können jedoch auf demselben System koexistieren.

### Nächste Schritte

Fahren Sie mit den Schritten zur Installation von IBM Security Directory Server fort. Siehe „Installation mit IBM Installation Manager“.

---

## Installation mit IBM Installation Manager

Führen Sie die Schritte zur Installation von IBM Security Directory Server mit IBM Installation Manager aus.

### Vorbereitende Schritte

Starten Sie die Installation.

### Vorgehensweise

1. Klicken Sie auf der Startseite von IBM Installation Manager auf **Install**.
2. Wählen Sie auf der Seite **Install Packages** das Paket von IBM Security Directory Server für die Installation aus.
3. Klicken Sie auf **Next**. IBM Installation Manager überprüft Ihren Computer auf vorausgesetzte Pakete.
4. Wenn der Computer die Prüfung der Voraussetzungen nicht besteht, werden die Voraussetzungen auf der Seite **Validation Results** angezeigt.
  - a. Klicken Sie auf **Recheck Status**, um nach der Installation der vorausgesetzten Pakete zu überprüfen, ob die Voraussetzungen erfüllt sind. Weitere Informationen zu den Voraussetzungen finden Sie unter „Auf verschiedenen Betriebssystemen erforderliche vorausgesetzte Pakete“ auf Seite 15.

- b. Wenn alle Voraussetzungen erfüllt sind, klicken Sie auf **Next**.
5. Klicken Sie auf **I accept the terms in the license agreement** und anschließend auf **Next**. Die Position des Verzeichnisses für gemeinsam genutzte Ressourcen wird angezeigt.
  6. Optional: Verwenden Sie den Standardpfad oder geben Sie im Feld **Shared Resources Directory** einen Pfad an. Das Verzeichnis für gemeinsam genutzte Ressourcen dient zum Speichern von Installationsartefakten, die auf diese Weise von einer oder mehreren Produktpaketgruppen verwendet werden können. Sie können das Verzeichnis für gemeinsam genutzte Ressourcen nur bei der Erstinstallation eines Pakets angeben.
  7. Klicken Sie auf **Next**. Der Paketgruppenname und die Standardinstallationsposition werden angezeigt. Die Option **Create a new package group** ist standardmäßig ausgewählt und nur diese Option wird für die Installation von IBM Security Directory Server unterstützt. Eine Paketgruppe stellt ein Verzeichnis dar, in dem Pakete Ressourcen gemeinsam mit anderen Paketen in derselben Gruppe nutzen. Einer Paketgruppe wird automatisch ein Name zugewiesen.

**Einschränkung:**

IBM Security Directory Server kann auf AIX- und Linux-Systemen nur in der vordefinierten Position installiert werden. Der Pfad wird standardmäßig im Feld **Installation Directory** in IBM Installation Manager angegeben. Dieses Feld kann in IBM Installation Manager bearbeitet werden, aber wenn Sie den standardmäßig angegebenen Pfad ändern, können Sie nicht auf **Next** klicken, um mit der Installation fortzufahren. Setzen Sie den Pfad wieder auf den Standardinstallationspfad für IBM Security Directory Server zurück.

Eine Liste der Standardinstallationspositionen auf verschiedenen Betriebssystemen finden Sie unter „Standardinstallationspositionen“ auf Seite 28.

Diese Beschränkung gilt nicht für Microsoft Windows-Betriebssysteme. IBM Security Directory Server kann auf Microsoft Windows-Betriebssystemen in einer beliebigen Position installiert werden. Auch wenn Sie die Standardinstallationsposition für IBM Security Directory Server ausgewählt haben, werden das enthaltene Verzeichnis `idsinstinfo` und die enthaltene Datei `idsinstances.ldif` immer auf der von `%SystemDrive%` angegebenen Partition erstellt. Wenn IBM Security Directory Server auf dem Laufwerk E: installiert wird und sich das Betriebssystem auf dem Laufwerk C: befindet, fallen Ihnen möglicherweise die folgenden Änderungen auf:

- Das Verzeichnis `idsinstinfo` wird auf dem Laufwerk C: (`C:\idsinstinfo`) statt im Verzeichnis `E:\Program Files\IBM\ldap` erstellt.

8. Klicken Sie auf **Next**.
9. Wählen Sie auf der Seite **Install Packages** die erforderlichen Features aus. Wählen Sie das Markierungsfeld **Show dependencies** aus, um die von einem Feature abhängigen Elemente oder die Abhängigkeiten eines Features von anderen Features anzuzeigen.

*Tabelle 11. In einem vollständigen Produktpaket oder einem reinen Clientpaket für die Installation verfügbare IBM Security Directory Server-Features*

Alle Features	Abhängigkeiten bei der Installation	Features im vollständigen Produktpaket	Features im reinen Clientpaket
IBM DB2	Keine	Ja	Nein

Tabelle 11. In einem vollständigen Produktpaket oder einem reinen Clientpaket für die Installation verfügbare IBM Security Directory Server-Features (Forts.)

Alle Features	Abhängigkeiten bei der Installation	Features im vollständigen Produktpaket	Features im reinen Clientpaket
IBM Global Security Kit	Keine	Ja	Ja
C-Client	Keine	Ja	Ja
IBM Java Development Kit	Keine	Ja	Ja
Java-Client	Keine	Ja	Ja
Server	C-Client Java-Client	Ja	Nein
Proxy-Server	C-Client Java-Client	Ja	Nein
<b>Webverwaltungstool</b>	Keine	Ja	Nein

10. Klicken Sie auf **Next**.

11. Wenn Sie das Feature IBM DB2 für die Installation auswählen, klicken Sie auf **IBM DB2** und führen Sie eine der folgenden Aktionen aus:

- Führen Sie die folgenden Aktionen aus, um IBM DB2 zu installieren:
  - a. Klicken Sie auf **DB2 installieren**.
  - b. Geben Sie im Feld **Pfad der DB2-Installationsdatei** den Pfadnamen der DB2-Installationsdatei an. Sie können auf **Durchsuchen** klicken und den Pfad angeben.
  - c. Geben Sie unter Windows im Feld **Benutzername** die Systembenutzer-ID ein, die Sie der Gruppe DB2ADMNS oder DB2USERS zuordnen wollen. Mit Hilfe dieser Benutzer-ID können Sie lokale DB2-Anwendungen und -Tools auf dem Computer ausführen. Wenn die Benutzer-ID nicht vorhanden ist, wird der Benutzeraccount vom Installationsprogramm erstellt.
  - d. Geben Sie unter Windows im Feld **Kennwort** das Kennwort für die Benutzer-ID ein. Wenn Ihr Kennwort nicht der auf Ihrem Computer festgelegten Kennwortrichtlinie entspricht, schlägt die Installation möglicherweise fehl.
  - e. Geben Sie unter Windows im Feld **Kennwort bestätigen** das Kennwort für die Benutzer-ID ein.
  - f. Klicken Sie auf **Weiter**.
- Führen Sie eine der folgenden Aktionen aus, wenn auf Ihrem Computer eine unterstützte Version von IBM DB2 installiert ist:
  - a. Klicken Sie auf **Mit vorhandener DB2-Instanz fortsetzen**, um mit einer vorhandenen DB2-Instanz fortzufahren.

**Wichtig:** Wenn Sie die Option zum Fortfahren mit einer vorhandenen DB2-Instanz bei der Installation auswählen, aktualisiert IBM Installation Manager seine Registrierungsdatenbank mit dem Eintrag des Features DB2.

- b. Wählen Sie in der Liste eine unterstützte DB2-Version aus, die Sie mit IBM Security Directory Server verwenden wollen.
- c. Klicken Sie auf **Weiter**.

12. Wenn Sie das Feature IBM Global Security Kit für die Installation auswählen, klicken Sie auf **IBM Global Security Kit** und führen Sie eine der folgenden Aktionen aus:
- Führen Sie die folgenden Aktionen aus, wenn GSKit Version 8.0 oder höher nicht auf Ihrem Computer installiert ist:
    - a. Klicken Sie auf **GSKit installieren**.
    - b. Geben Sie im Feld **Pfad der GSKit-Installationsdatei** den Pfadnamen der GSKit-Installationsdatei an. Sie können auf **Durchsuchen** klicken und den Pfad angeben.
 

**Anmerkung:** Der angegebene Pfad muss sowohl die 64-Bit-GSKit-Installationsdatei als auch die 32-Bit-GSKit-Installationsdatei enthalten.
    - c. Klicken Sie auf **Weiter**.
  - Führen Sie eine der folgenden Aktionen aus, wenn GSKit Version 8.0 oder höher auf Ihrem Computer installiert ist:
    - a. Klicken Sie auf **Mit vorhandenem GSKit fortsetzen**, um mit einer vorhandenen GSKit-Version fortzufahren.
 

**Wichtig:** Wenn Sie die Option zum Fortfahren mit einer vorhandenen GSKit-Version bei der Installation auswählen, aktualisiert IBM Installation Manager seine Registrierungsdatenbank mit dem Eintrag des Features GSKit.
    - b. Klicken Sie auf **Weiter**.
13. Wenn Sie das Feature IBM Java Development Kit für die Installation auswählen, klicken Sie auf **IBM Java Development Kit** und führen Sie die folgenden Schritte aus:
- a. Geben Sie im Feld **IBM Java Development Kit** den Dateinamen und den Pfadnamen der komprimierten JDK-Datei an. Sie können auf **Durchsuchen** klicken und den Pfad angeben.
  - b. Klicken Sie auf **Weiter**.
14. Wenn Sie das Feature **Webverwaltungstool** für die Installation auswählen, klicken Sie auf **Webverwaltungstool** und führen Sie die folgenden Schritte aus:
- a. Führen Sie die folgenden Aktionen aus, um die integrierte Version von WebSphere Application Server zu installieren:
    - 1) Wählen Sie **Integrierte Version von WebSphere Application Server installieren** aus.
    - 2) Geben Sie im Feld **Pfad der Installationsdatei der integrierten Version von WebSphere Application Server** den Pfadnamen der integrierten Version von WebSphere Application Server an. Sie können auf **Durchsuchen** klicken und den Pfad angeben.
  - b. Führen Sie die eine der folgenden Aktionen aus, um das **Webverwaltungstool** zu implementieren.
    - Klicken Sie auf **Auf integrierte Standardversion von WebSphere Application Server implementieren**, um die Implementierung in der integrierten Version von WebSphere Application Server vorzunehmen, die sich im Standardinstallationspfad befindet.

**Anmerkung:** Ist eine Vorgängerversion des **Webverwaltungstools** vorhanden, migriert das Installationsprogramm diese auf die aktuelle Version, sofern die folgenden Bedingungen erfüllt sind:

- 1) Die Vorgängerversion des **Webverwaltungstools** und die integrierte Version von WebSphere Application Server sind im Standardinstallationspfad enthalten.
  - 2) Die Vorgängerversion des **Webverwaltungstools** ist in der integrierten Version von WebSphere Application Server implementiert, die sich im Standardinstallationspfad befindet.
  - 3) Das im Lieferumfang von IBM Security Directory Server Version 6.1, 6.2 oder 6.3 enthaltene **Webverwaltungstool** bietet Unterstützung für die Migration.
    - Klicken Sie auf **Auf vorhandenem WebSphere Application Server implementieren**, um die Implementierung auf WebSphere Application Server oder in der integrierten Version von WebSphere Application Server vorzunehmen, die sich in einem angepassten Installationspfad befindet.
      - 1) Geben Sie im Feld **Installationspfad von WebSphere Application Server oder der integrierten Version von WebSphere Application Server** den Installationspfad eines vorhandenen Webanwendungsservers an.
    - Klicken Sie auf **Später manuell implementieren**, um das **Webverwaltungstool** später manuell auf einem unterstützten Webanwendungsserver zu implementieren.
15. Klicken Sie auf **Weiter**. Die Übersichtsdaten der Installationsvorbereitung (Installationsposition, Paketliste und Repositoryangaben) werden angezeigt.
  16. Überprüfen Sie die Übersichtsdaten und klicken Sie auf **Installieren**. Die Installation wird gestartet und ein Fortschrittsanzeiger wird angezeigt. Nach der Installation wird die Übersichtsseite des Installationsabschlusses angezeigt.
  17. Klicken Sie auf den Link zum Anzeigen der Protokolldatei, um zu überprüfen, ob die Installation erfolgreich war. Weitere Informationen hierzu finden Sie in Kapitel 5, „IBM Installation Manager-Protokolldateien“, auf Seite 47.
  18. Führen Sie die eine der folgenden Aktionen aus, um eines der folgenden Programme zu starten:
    - Klicken Sie auf **Instance Administration Tool (idsxinst)**, um das **Instance Administration Tool** zu starten.
    - Klicken Sie auf **Kein**, wenn Sie kein Programm starten wollen.
  19. Klicken Sie auf **Fertig stellen**.
  20. Klicken Sie auf **Datei > Beenden**.

## Ergebnisse

Bei einer erfolgreichen Installation wird IBM Security Directory Server an der Installationsposition installiert. Informationen zu der Standardinstallationsposition finden Sie unter „Standardinstallationspositionen“ auf Seite 28. Ist die Installation eines oder mehrerer ausgewählter Features nicht erfolgreich, wird die Installation der Pakete von IBM Security Directory Server rückgängig gemacht.

## Nächste Schritte

Nach der Installation von IBM Security Directory Server müssen Sie die folgenden Aktionen ausführen:

- Um IBM Security Directory Server als vollständigen Verzeichnisserver zu verwenden, erstellen Sie eine Verzeichnisserverinstanz. Weitere Informationen hierzu finden Sie unter „Standardverzeichnisserverinstanz erstellen“ auf Seite 141.



- Um IBM Security Directory Server als Proxy-Server zu verwenden, erstellen Sie eine Proxy-Server-Instanz. Weitere Informationen hierzu finden Sie unter „Proxy-Server-Instanz mit angepassten Einstellungen erstellen“ auf Seite 150.

---

## Unbeaufsichtigte Installation

Sie können IBM Security Directory Server auf mehreren Systemen ohne manuelle Eingriffe unbeaufsichtigt installieren.

Für eine unbeaufsichtigte Installation müssen die folgenden Aktivitäten durchgeführt werden:

1. Installieren Sie IBM Installation Manager, sofern noch nicht geschehen.
2. Verwenden Sie die Standardantwortdatei oder zeichnen Sie eine angepasste Antwortdatei auf.
3. Installieren Sie die Pakete.

### Antwortdatei für unbeaufsichtigte Installation

Bei der Installation im unbeaufsichtigten Modus ist die Benutzerschnittstelle nicht verfügbar. Die Antwortdatei dient als Eingabe für die Installation. Eine Antwortdatei ist eine XML-Datei mit Daten, die zum Durchführen einer unbeaufsichtigten Installation erforderliche Daten enthält.

#### Angepasste Antwortdatei aufzeichnen

Sie können für die folgenden Tasks Antwortdateien aufzeichnen:

- Installieren von Paketen
- Ändern von Paketen
- Deinstallieren von Paketen

Zum Aufzeichnen von Antwortdateien müssen Sie die Vorgaben und Installationsaktionen mit IBM Installation Manager im Schnittstellenmodus aufzeichnen. Wenn Sie zum ersten Mal eine Antwortdatei für die unbeaufsichtigte Installation aufzeichnen, können Sie auswählen, dass die Pakete nicht mit dem Parameter `-skipInstall agentDataLocation` installiert werden sollen.

Die Daten für die Installation des Produkts werden in der *agentDataLocation*-Position gespeichert. Zum Aufzeichnen von Antwortdateien für unbeaufsichtigte Änderungen oder die unbeaufsichtigte Deinstallation des Produkts muss dieselbe *agentDataLocation*-Position mit dem Parameter `-skipInstall` verwendet werden.

Für unterschiedliche Installationsszenarios müssen unterschiedliche Antwortdateien mit unterschiedlichen *agentDataLocation*-Positionen für jedes Szenario aufgezeichnet werden.

Weitere Informationen zum Aufzeichnen einer Antwortdatei für die unbeaufsichtigte Installation finden Sie in der Dokumentation zu IBM Installation Manager unter <http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome>.

### Überprüfung der unbeaufsichtigten Installation

Wenn die Installation abgeschlossen ist, müssen Sie die unbeaufsichtigte Installation überprüfen. Die Installation kann auf die folgenden Arten überprüft werden:

- Überprüfung des Rückkehrcodes

- Überprüfung der Protokolldatei
- Überprüfung der Pakete

## Unbeaufsichtigte Installation mit Antwortdatei

Mithilfe einer unbeaufsichtigten Installation von IBM Security Directory Server können Sie die erforderlichen Pakete ohne manuellen Eingriff installieren.

### Vorbereitende Schritte

Für die unbeaufsichtigte Installation der Pakete von IBM Security Directory Server ist IBM Installation Manager ab Version 1.7.0 erforderlich.

### Informationen zu diesem Vorgang

Sie können die Standardantwortdatei verwenden oder eine angepasste Antwortdatei aufzeichnen und diese als Eingabedatei für die unbeaufsichtigte Installation verwenden.

### Vorgehensweise

1. Melden Sie sich am System als Administrator an.
2. Greifen Sie an der Installationsposition von IBM Installation Manager auf den Befehl **IBMIM** zu.

Betriebssystem	Standardposition des Befehls <b>IBMIM</b> :
Microsoft Windows	C:\Program Files\IBM\InstallationManager\eclipse
AIX und Linux	/opt/IBM/InstallationManager/eclipse

3. Optional: Führen Sie den Befehl **IBMIM** aus, um eine Antwortdatei für die Installation aufzuzeichnen.

**Tipp:** Sie können die Beispielantwortdatei für die Installation verwenden. Informationen zur Standardposition der Beispielantwortdatei finden Sie unter „Unbeaufsichtigte Installation“ auf Seite 37.

- a. Führen Sie auf den verschiedenen Betriebssystemen die folgenden Befehle aus, um die Installationsschritte aufzuzeichnen, ohne das Produkt zu installieren:

#### Microsoft Windows

```
IBMIM.exe -record path_name\responseFile.xml -skipInstall agentDataLocation
```

#### AIX und Linux

```
./IBMIM -record path_name/responseFile.xml -skipInstall agentDataLocation
```

Mit dem Befehl wird IBM Installation Manager geöffnet.

- b. Legen Sie das Repository von IBM Security Directory Server fest. Weitere Informationen finden Sie in Schritt 2 auf Seite 32.
- c. Zeichnen Sie die Installation von IBM Security Directory Server auf. Weitere Informationen finden Sie in Schritt „Installation mit IBM Installation Manager“ auf Seite 32.

4. Führen Sie den Befehl **imcl** aus, um die unbeaufsichtigte Installation mit der Antwortdatei als Eingabe zu starten. Der Befehl **imcl** sollte sich im Pfad `<IBM_Installation_Manager_install_dir>/eclipse/tools` befinden.

Betriebssystem	Befehl:
Microsoft Windows	<code>imcl.exe input path_name\ responseFile.xml -acceptLicense -showProgress</code>
AIX und Linux	<code>./imcl input path_name/responseFile.xml -acceptLicense -showProgress</code>

**Anmerkung:** Mit dem Befehl **imcl** können viele andere Parameter verwendet werden. Weitere Details finden Sie in der Hilfe zum Befehl **imcl**.

5. Überprüfen Sie die Installationszusammenfassung und die Protokolldateien.

Betriebssystem	Standardprotokollpfad:
Microsoft Windows	<code>C:\ProgramData\IBM\InstallationManager\ logs</code>
AIX und Linux	<code>/var/ibm/InstallationManager/logs/</code>

6. Überprüfen Sie, ob die Pakete von IBM Security Directory Server die erforderliche Version aufweisen.

Betriebssystem	Pakete überprüfen:
Microsoft Windows	Siehe „IBM Security Directory Server-Features mit IBM Installation Manager überprüfen“ auf Seite 87.
AIX und Linux	Siehe „IBM Security Directory Server-Features mit IBM Installation Manager überprüfen“ auf Seite 87.

## Ergebnisse

Bei einer erfolgreichen Installation wird IBM Security Directory Server an der Installationsposition von IBM Security Directory Server installiert. Informationen zu der Standardinstallationsposition finden Sie unter „Standardinstallationspositionen“ auf Seite 28. Ist die Installation eines oder mehrerer ausgewählter Features nicht erfolgreich, wird die Installation der Pakete von IBM Security Directory Server rückgängig gemacht.

## Nächste Schritte

**Anmerkung:** Wenn Sie bei der Aufzeichnung der Antwortdatei für die Installation das **Instance Administration Tool** zum Öffnen auswählen, wird das **Instance Administration Tool** nach der unbeaufsichtigten Installation von IBM Security Directory Server nicht geöffnet.

Wenn Sie das Server- oder Proxy Server-Feature für die Installation ausgewählt haben, öffnen Sie das **Instance Administration Tool**, um eine Verzeichnisserversinstanz oder eine Proxy-Server-Instanz zu erstellen. Siehe „**Instance Administration Tool** starten“ auf Seite 138.



---

## Kapitel 4. Mit IBM Installation Manager Änderungen vornehmen

Sie können mit IBM Installation Manager IBM Security Directory Server-Features, die noch nicht installiert sind, installieren und bereits installierte Features deinstallieren.

Features können nicht entfernt werden, wenn sie Voraussetzung für andere installierte Features sind. Sie können eine Abhängigkeit nur entfernen, wenn alle abhängigen Features zum Entfernen ausgewählt oder bereits entfernt sind.

**Wichtig:** Wenn Sie mit einer vorhandenen Version von DB2 oder GSKit fortfahren, aktualisiert IBM Installation Manager dessen Registry während der Installation mit dem Featureeintrag. Wenn Sie ein Feature entfernen, das mithilfe der Option **Continue with the existing** installiert wurde, werden von Installation Manager die folgenden Aktionen durchgeführt:

- Der Featureeintrag wird aus der IBM Installation Manager-Registry entfernt.
- Das Feature wird nicht vom Computer deinstalliert.

---

### Features mit IBM Installation Manager ändern

Führen Sie die Schritte zum Ändern von IBM Security Directory Server-Features mit IBM Installation Manager aus.

#### Vorbereitende Schritte

Sie müssen alle Client- und Serverprozesse von IBM Security Directory Server stoppen.

- Verzeichnisserver
- Verwaltungsserver
- LDAP-Traces
- Benutzerdefinierte LDAP-Anwendungen

Wenn irgendwelche Prozesse aktiv sind, können die Programme und Bibliotheken nicht entfernt werden.

#### Vorgehensweise

1. Starten Sie IBM Installation Manager.
  - AIX und Linux:
    - a. Öffnen Sie ein Befehlszeilenfenster und wechseln Sie in das Verzeichnis, das IBM Installation Manager enthält. Das folgende Verzeichnis ist die Standardinstallationsposition von IBM Installation Manager:  
`opt/IBM/InstallationManager/eclipse`
    - b. Führen Sie den folgenden Befehl aus:  
`./IBMIM`
  - Microsoft Windows:
    - a. Klicken Sie auf **Start > Alle Programme > IBM Installation Manager > IBM Installation Manager**.
2. Klicken Sie auf **Ändern**.

3. Wählen Sie **IBM Security Directory Server** aus und klicken Sie auf **Weiter**.
4. Auf der Seite **Modify Packages** müssen Sie die folgenden Aktionen ausführen:
  - a. Wählen Sie die Features aus, die Sie installieren wollen.
  - b. Wählen Sie die Features ab, die Sie deinstallieren wollen.

*Tabelle 12. IBM Security Directory Server-Features, die in vollständigen Produktpaketen oder reinen Clientpaketen für Änderungen verfügbar sind*

Alle Features	Abhängigkeiten bei der Installation	Features im vollständigen Produktpaket	Features im reinen Clientpaket
IBM DB2	Keine	Ja	Nein
IBM Global Security Kit	Keine	Ja	Ja
C-Client	Keine	Ja	Ja
IBM Java Development Kit	Keine	Ja	Ja
Java-Client	Keine	Ja	Ja
Server	C-Client Java-Client	Ja	Nein
Proxy-Server	C-Client Java-Client	Ja	Nein
<b>Webverwaltungstool</b>	Keine	Ja	Nein

**Wichtig:** Wenn Sie mit einer vorhandenen Version von DB2 oder GSKit fortfahren, aktualisiert IBM Installation Manager dessen Registry während der Installation mit dem Featureeintrag. Wenn Sie ein Feature entfernen, das mithilfe der Option **Continue with the existing** installiert wurde, werden von Installation Manager die folgenden Aktionen durchgeführt:

- Der Featureeintrag wird aus der IBM Installation Manager-Registry entfernt.
- Das Feature wird nicht vom Computer deinstalliert.

Falls DB2-Instanzen vorhanden sind, die Sie mit der mit IBM Installation Manager installierten DB2-Kopie erstellt haben, können Sie IBM DB2 nicht entfernen. In diesem Fall müssen Sie die DB2-Instanzen manuell entfernen und den Vorgang wiederholen. Es empfiehlt sich, vor dem Entfernen der DB2-Instanzen eine Datenbanksicherung durchzuführen.

- c. Klicken Sie auf **Next**.
5. Wenn Sie das Feature IBM DB2 für die Installation auswählen, klicken Sie auf **IBM DB2** und führen Sie eine der folgenden Aktionen aus:
  - Führen Sie die folgenden Aktionen aus, um IBM DB2 zu installieren:
    - a. Klicken Sie auf **DB2 installieren**.
    - b. Geben Sie im Feld **Pfad der DB2-Installationsdatei** den Pfadnamen der DB2-Installationsdatei an. Sie können auf **Durchsuchen** klicken und den Pfad angeben.
    - c. Geben Sie unter Windows im Feld **Benutzername** die Systembenutzer-ID ein, die Sie der Gruppe DB2ADMNS oder DB2USERS zuordnen wollen. Mithilfe dieser Benutzer-ID können Sie lokale DB2-Anwendungen und -Tools auf dem Computer ausführen. Wenn die Benutzer-ID nicht vorhanden ist, wird der Benutzeraccount vom Installationsprogramm erstellt.

- d. Geben Sie unter Windows im Feld **Kennwort** das Kennwort für die Benutzer-ID ein. Wenn Ihr Kennwort nicht der auf Ihrem Computer festgelegten Kennwortrichtlinie entspricht, schlägt die Installation möglicherweise fehl.
  - e. Geben Sie unter Windows im Feld **Kennwort bestätigen** das Kennwort für die Benutzer-ID ein.
  - f. Klicken Sie auf **Weiter**.
- Führen Sie die folgenden Schritte aus, wenn auf Ihrem Computer eine unterstützte Version von IBM DB2 installiert ist:
    - a. Klicken Sie auf **Mit vorhandener DB2-Instanz fortsetzen**, um mit einer vorhandenen DB2-Instanz fortzufahren.
 

**Wichtig:** Wenn Sie die Option zum Fortfahren mit einer vorhandenen DB2-Instanz bei der Installation auswählen, aktualisiert IBM Installation Manager seine Registrierungsdatenbank mit dem Eintrag des Features DB2.
    - b. Wählen Sie in der Liste eine unterstützte DB2-Version aus, die Sie mit IBM Security Directory Server verwenden wollen.
    - c. Klicken Sie auf **Weiter**.
6. Wenn Sie das Feature IBM Global Security Kit für die Installation auswählen, klicken Sie auf **IBM Global Security Kit** und führen Sie eine der folgenden Aktionen aus:
- Führen Sie die folgenden Schritte aus, wenn GSKit Version 8.0 oder höher nicht auf Ihrem Computer installiert ist:
    - a. Klicken Sie auf **GSKit installieren**.
    - b. Geben Sie im Feld **Pfad der GSKit-Installationsdatei** den Pfadnamen der GSKit-Installationsdatei an. Sie können auf **Durchsuchen** klicken und den Pfad angeben.
 

**Anmerkung:** Der angegebene Pfad muss sowohl die 64-Bit-GSKit-Installationsdatei als auch die 32-Bit-GSKit-Installationsdatei enthalten.
    - c. Klicken Sie auf **Weiter**.
  - Führen Sie die folgenden Schritte aus, wenn GSKit Version 8.0 oder höher auf Ihrem Computer installiert ist:
    - a. Klicken Sie auf **Mit vorhandenem GSKit fortsetzen**, um mit einer vorhandenen GSKit-Version fortzufahren.
 

**Wichtig:** Wenn Sie die Option zum Fortfahren mit einer vorhandenen GSKit-Version bei der Installation auswählen, aktualisiert IBM Installation Manager seine Registrierungsdatenbank mit dem Eintrag des Features GSKit.
    - b. Klicken Sie auf **Weiter**.
7. Wenn Sie das Feature IBM Java Development Kit für die Installation auswählen, klicken Sie auf **IBM Java Development Kit** und führen Sie die folgenden Schritte aus:
- a. Geben Sie im Feld **IBM Java Development Kit** den Dateinamen und den Pfadnamen der komprimierten JDK-Datei an. Sie können auf **Durchsuchen** klicken und den Pfad angeben.
  - b. Klicken Sie auf **Weiter**.
8. Wenn Sie das Feature **Webverwaltungstool** für die Installation auswählen, klicken Sie auf **Webverwaltungstool** und führen Sie die folgenden Schritte aus:

- a. Führen Sie die folgenden Aktionen aus, um die integrierte Version von WebSphere Application Server zu installieren:
  - 1) Wählen Sie **Integrierte Version von WebSphere Application Server installieren** aus.
  - 2) Geben Sie im Feld **Pfad der Installationsdatei der integrierten Version von WebSphere Application Server** den Pfadnamen der integrierten Version von WebSphere Application Server an. Sie können auf **Durchsuchen** klicken und den Pfad angeben.
- b. Führen Sie die eine der folgenden Aktionen aus, um das **Webverwaltungstool** zu implementieren.
  - Klicken Sie auf **Auf integrierte Standardversion von WebSphere Application Server implementieren**, um die Implementierung in der integrierten Version von WebSphere Application Server vorzunehmen, die sich im Standardinstallationspfad befindet.

**Anmerkung:** Ist eine Vorgängerversion des **Webverwaltungstools** vorhanden, migriert das Installationsprogramm diese auf die aktuelle Version, sofern die folgenden Bedingungen erfüllt sind:

- 1) Die Vorgängerversion des **Webverwaltungstools** und die integrierte Version von WebSphere Application Server sind im Standardinstallationspfad enthalten.
  - 2) Die Vorgängerversion des **Webverwaltungstools** ist in der integrierten Version von WebSphere Application Server implementiert, die sich im Standardinstallationspfad befindet.
  - 3) Das im Lieferumfang von IBM Security Directory Server Version 6.1, 6.2 oder 6.3 enthaltene **Webverwaltungstool** bietet Unterstützung für die Migration.
- Klicken Sie auf **Auf vorhandenem WebSphere Application Server implementieren**, um die Implementierung auf WebSphere Application Server oder in der integrierten Version von WebSphere Application Server vorzunehmen, die sich in einem angepassten Installationspfad befindet.
    - 1) Geben Sie im Feld **Installationspfad von WebSphere Application Server oder der integrierten Version von WebSphere Application Server** den Installationspfad eines vorhandenen Webanwendungsservers an.
  - Klicken Sie auf **Später manuell implementieren**, um das **Webverwaltungstool** später manuell auf einem unterstützten Webanwendungsserver zu implementieren.
9. Klicken Sie auf **Weiter**.

**Wichtig:** Wenn Sie mit einer vorhandenen Version von DB2 oder GSKit fortfahren, aktualisiert IBM Installation Manager dessen Registry während der Installation mit dem Featureeintrag. Wenn Sie ein Feature entfernen, das mithilfe der Option **Continue with the existing** installiert wurde, werden von Installation Manager die folgenden Aktionen durchgeführt:

- Der Featureeintrag wird aus der IBM Installation Manager-Registry entfernt.
  - Das Feature wird nicht vom Computer deinstalliert.
10. Überprüfen Sie die Übersichtsdaten und klicken Sie auf **Ändern**.
  11. Optional: Wenn bei der Änderung ein Fehler auftritt, klicken Sie auf die Option zum Anzeigen der Protokolldatei und lesen Sie die Details. Weitere Informationen hierzu finden Sie in Kapitel 5, „IBM Installation Manager-Protokolldateien“, auf Seite 47.



12. Klicken Sie auf **Fertig stellen**.
13. Klicken Sie auf **Datei > Beenden**.

## **Ergebnisse**

Wenn die Änderung erfolgreich war, können Sie die folgende Änderung beobachten:

- Die Features von IBM Security Directory Server, die Sie zum Hinzufügen ausgewählt haben, werden an der Installationsposition installiert. Informationen zu der Standardinstallationsposition finden Sie unter „Standardinstallationspositionen“ auf Seite 28.
- Die Features von IBM Security Directory Server, die Sie zum Entfernen ausgewählt haben, werden deinstalliert.



---

## Kapitel 5. IBM Installation Manager-Protokolldateien

Sie können die Installation oder Deinstallation von sowie Änderungen an IBM Security Directory Server und dessen Komponenten anhand der Protokolldateien überprüfen, die von IBM Installation Manager erstellt werden.

Wenn während der Installation oder Deinstallation von oder bei Änderungen an IBM Security Directory Server und dessen Komponenten Fehler auftreten, überprüfen Sie die Protokolldateien. IBM Installation Manager erstellt die Protokolldateien an der Standardposition.

*Tabelle 13. Die Standardpositionen der IBM Installation Manager-Protokolldateien bei den unterschiedlichen Betriebssystemen*

Betriebssystem	Standardprotokollposition von IBM Installation Manager
AIX und Linux	/var/ibm/InstallationManager/logs
Microsoft Windows	C:\ProgramData\IBM\InstallationManager\ logs

Die Standardpositionen gelten für alle unterstützten Versionen von AIX, Linux und Microsoft Windows.



---

## Kapitel 6. IBM Security Directory Server-Pakete abfragen

Überprüfen Sie die IBM Security Directory Server-Pakete, indem Sie die IBM Security Directory Server-Pakete auf unterstützten Plattformen abfragen.

### Informationen zu diesem Vorgang

Nach der Installation der IBM Security Directory Server-Pakete müssen Sie sicherstellen, dass alle Pakete die erforderliche Version aufweisen. Diese Task hilft Ihnen bei der Abfrage der Versionsnummer von installierten IBM Security Directory Server-Paketen.

### Vorgehensweise

Melden Sie sich an dem System an, auf dem Sie die IBM Security Directory Server-Pakete installiert haben, und führen Sie die Befehle mit Rootberechtigung aus.

- Auf AIX-Systemen: Führen Sie den Befehl **lslpp** aus. Beispiel:  

```
lslpp -l 'idsldap*'
```
- Auf Linux-Systemen: Führen Sie den Befehl **rpm** aus. Beispiel:  

```
rpm -qa | grep idsldap
```
- Auf Solaris-Systemen:
  1. Führen Sie den Befehl **pkginfo** aus, um die installierten Pakete aufzulisten. Beispiel:  

```
pkginfo | grep IDS1
```
  2. Führen Sie den Befehl **pkgparam** aus, um die Version eines bestimmten Pakets von IBM Security Directory Server abzufragen. Beispiel:  

```
pkgparam IDS1bc63 VERSION
```
- Auf HP-UX-Systemen (Itanium): Führen Sie den Befehl **swlist** aus. Beispiel:  

```
swlist | grep idsldap
```



---

## Kapitel 7. Native Installation und Konfiguration mit Scripts

Sie können IBM Security Directory Server mithilfe von Scripts installieren und konfigurieren.

---

### Installationsroadmap

Verwenden Sie die Roadmap zum Installieren von IBM Security Directory Server auf Linux x86-, Linux i/pSeries-, Linux s390-, Solaris- und HP-UX-Systemen.

1. Überprüfen Sie, ob auf dem verwendeten System die Mindestanforderungen für Hardware und Software erfüllt sind. Weitere Informationen finden Sie unter *Systemvoraussetzungen* im Abschnitt Produktübersicht der IBM Security Directory Server-Dokumentation.
2. Installieren Sie die Softwarevoraussetzungen, beispielsweise DB2. Stellen Sie sicher, dass der Zugriff auf die DB2-Installationsdatei möglich ist und dass Sie über die erforderlichen Berechtigungen verfügen, falls DB2 noch nicht installiert wurde.
3. Wenn Sie eines oder mehrere der folgenden Features verwenden wollen, müssen Sie die optionalen Softwarevoraussetzungen installieren. Stellen Sie sicher, dass der Zugriff auf die optionalen Softwarevoraussetzungen möglich ist und dass Sie über die erforderlichen Berechtigungen verfügen, falls die Software noch nicht installiert wurde.
  - Für die Verwendung des Webverwaltungstools ist eine unterstützte integrierte Version von WebSphere Application Server oder WebSphere Application Server erforderlich. Außerdem ist eine unterstützte Version des Browsers erforderlich.
  - Für die Verschlüsselung mit Secure Socket Layer (SSL) oder Transport Layer Security (TLS) ist eine unterstützte Version von IBM Global Security Kit (GSKit) erforderlich.
4. Verwenden Sie auf Linux x86-, Linux i/pSeries-, Linux s390-, Solaris- und HP-UX-Systemen das Installationsprogramm **idsNativeInstall**, um IBM Security Directory Server-Pakete und andere erforderliche Software zu installieren.
5. Erstellen und konfigurieren Sie nach der Installation von IBM Security Directory Server mit dem Befehl **idsdefinst** eine Verzeichnisserverinstanz.
6. Starten Sie die Verzeichnisserverinstanz.
7. Laden Sie die LDIF-Beispieldatei in die Datenbank. Informationen zur Verwendung der Verzeichnisserverinstanz finden Sie im Abschnitt Verwaltung der IBM Security Directory Server-Dokumentation.

**Anmerkung:** Das native Installationsscript **idsNativeInstall** wird nicht für Windows-, AIX- und Linux x86\_64 (64 Bit)-Betriebssysteme bereitgestellt. Verwenden Sie stattdessen IBM Installation Manager oder die Befehlszeilendienstprogramme des Betriebssystems, um die Installation unter diesen Betriebssystemen manuell durchzuführen.

---

## IBM Security Directory Server-Pakete auf Linux-, Solaris- und HP-UX-Plattformen installieren

Verwenden Sie die angegebenen Schritte, um IBM Security Directory Server-Pakete auf Linux x86-, Linux i/pSeries-, Linux s390-, Solaris- und HP-UX-Systemen zu installieren oder zu aktualisieren.

### Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, bevor Sie die Installation von IBM Security Directory Server-Paketen starten:

1. Melden Sie sich mit Rootberechtigung am System an.
2. Extrahieren Sie die Archivdatei von IBM Security Directory Server Version 6.3.1 in ein Verzeichnis (z. B. /sdsV6.3.1) mit ausreichend Plattenspeicherplatz.
3. Stoppen Sie alle Client- und Serverprozesse von IBM Security Directory Server, einschließlich des Verzeichnisseservers, des Verwaltungsservers und der angepassten LDAP-Anwendungen. Aktive Programme und Bibliotheken können nicht ersetzt werden. Wenn die Tracefunktion aktiviert wird, führen Sie `ldtrc off` aus, um den Traceprozess zu stoppen. In den Abschnitten "Grundlegende Serververwaltungstasks" und "Verzeichnisverwaltungsserver" im Abschnitt *Verwaltung* der IBM Security Directory Server-Dokumentation finden Sie Anweisungen zum Stoppen der Verzeichnisserverinstanzen und Verwaltungsserver.

### Informationen zu diesem Vorgang

Sie können den Befehl `idsNativeInstall` verwenden, um IBM Security Directory Server-Pakete auf Linux x86-, Linux i/pSeries-, Linux s390-, Solaris- und HP-UX-Systemen zu installieren oder zu aktualisieren. Sie können mit dem Befehl `idsNativeInstall` auch DB2, GSKit und die integrierte Version von WebSphere Application Server installieren, wenn diese Produkte noch nicht auf dem System installiert sind.

#### Anmerkung:

- Das native Installationsscript `idsNativeInstall` wird nicht für Windows-, AIX- und Linux x86\_64 (64-Bit)-Betriebssysteme bereitgestellt. Sie können stattdessen IBM Installation Manager oder die oBefehlszeilendienstprogramme des Betriebssystems verwenden, um die Installation unter diesen Betriebssystemen manuell durchzuführen.
- Auf HP-UX-Systemen sind reine Clientpakete von IBM Security Directory Server für die Installation oder das Upgrade verfügbar.

### Vorgehensweise

1. Wechseln Sie in das Verzeichnis mit dem Installationsprogramm `idsNativeInstall` und der Datei `responseFile.txt`. Die Dateien `idsNativeInstall` und `responseFile.txt` müssen sich in demselben Verzeichnis befinden.
2. Aktualisieren Sie die Datei `responseFile.txt` in den folgenden Einträgen. Standardmäßig sind die Werte der Featureinstallationsvariablen auf `false` eingestellt und die entsprechenden Pfadvariablen sind nicht eingestellt.
  - Stellen Sie für die Installation von DB2 die Variable `db2FeatureInstall` auf `true` ein und aktualisieren Sie die Variable `db2InstallImagePath` mit dem absoluten Pfad der DB2-Installationsdatei. Beispiel:



```
db2FeatureInstall=true
db2InstallImagePath=/sdsV6.3.1/db2
```

**Wichtig:** Bei einem vollständigen Verzeichnisserver muss DB2 auf dem System installiert werden. Wenn Sie die DB2-Variablen *db2FeatureInstall* und *db2InstallImagePath* einstellen, wird DB2 unter Linux im Pfad `/opt/ibm/sdsV6.3.1db2` oder unter Solaris im Pfad `/opt/IBM/sdsV6.3.1db2` installiert. Wenn an der angegebenen Position bereits eine DB2-Version installiert ist, überschreibt die Installation die vorhandenen Dateien.

- Stellen Sie für die Installation von GSKit die Variable *gskitFeatureInstall* auf true ein und aktualisieren Sie die Variable *gskitInstallImagePath* mit dem absoluten Pfad der GSKit-Installationsdatei. Beispiel:

```
gskitFeatureInstall=true
gskitInstallImagePath=/sdsV6.3.1/gskit
```

**Wichtig:** Damit eine Verzeichnisserverinstanz für die Kommunikation über SSL oder TLS konfiguriert werden kann, muss auf dem System die erforderliche Version von GSKit installiert werden.

- Stellen Sie für die Installation von IBM Java Development Kit die Variable *JDKFeatureInstall* auf true ein und aktualisieren Sie die Variable *JDKInstallImagePath* mit dem absoluten Pfad der Installationsdatei von IBM Java Development Kit. Beispiel:

```
JDKFeatureInstall=true
JDKInstallImagePath=/sdsV6.3.1/java/ibm-java-16sr14-linux-i386.tar
```

IBM Java Development Kit wird auf Linux- und Solaris-Systemen im Pfad `/opt/ibm/ldap/V6.3.1/java` installiert.

- Stellen Sie für die Installation der integrierten Version WebSphere Application Server die Variable *eWasFeatureInstall* auf true ein und aktualisieren Sie die Variable *eWasInstallImagePath* mit dem absoluten Pfad der Installationsdatei der integrierten Version WebSphere Application Server. Beispiel:

```
eWasFeatureInstall=true
eWasInstallImagePath=/sdsV6.3.1/appsrv
```

Die integrierte Version von WebSphere Application Server wird auf Linux- und Solaris-Systemen im Pfad `/opt/ibm/ldap/V6.3/appsrv` installiert.

- Aktualisieren Sie für die Installation von IBM Security Directory Server Version 6.3.1 für allgemeine Verfügbarkeit (GA) die Variable *tdsInstallImagePath* mit dem absoluten Pfad der Installationsdatei von IBM Security Directory Server Version 6.3.1 GA. Beispiel:

```
tdsInstallImagePath=/sdsV6.3.1
```

Wenn Sie `/sdsV6.3.1` als Pfad zur Installationsdatei von IBM Security Directory Server Version 6.3.1 angeben, müssen Sie sicherstellen, dass sich die folgenden Dateien im Verzeichnis `/sdsV6.3.1` befinden.

```
idsinstall
idsinstall_i
ids_detectGskitVersion
```

Die Pakete von IBM Security Directory Server Version 6.3.1 müssen sich im Verzeichnis `/sdsV6.3.1/tdsfiles` befinden.

3. Führen Sie an der Eingabeaufforderung den Befehl `idsNativeInstall` aus.

## Ergebnisse

Nach der Ausführung des Befehls **idsNativeInstall** installiert er die Pakete von IBM Security Directory Server. Je nach den Werten in der Antwortdatei installiert der Befehl **idsNativeInstall** außerdem DB2, GSKit, IBM Java Development Kit oder die integrierte Version von WebSphere Application Server.

**Anmerkung:** Ist IBM Security Directory Server Version 6.3.1 nicht auf dem System installiert, werden alle Komponenten von IBM Security Directory Server Version 6.3.1 installiert. IBM Security Directory Server Version 6.3.1 wird auf Linux-, Solaris- und HP-UX-Systemen im Pfad `/opt/ibm/ldap/V6.3.1/` installiert.

## Nächste Schritte

Nach der Installation von IBM Security Directory Server müssen Sie überprüfen, ob die Pakete von IBM Security Directory Server installiert wurden. Weitere Informationen zum Überprüfen der Protokolldateien finden Sie unter „Installationsprotokolle überprüfen“.

---

## Installationsprotokolle überprüfen

Ermitteln Sie die Protokolldatei, in der Sie den Installationsstatus auf Linux x86-, Linux i/pSeries-, Linux s390-, Solaris- und HP-UX-Systemen überprüfen können.

Nach Abschluss der Installation zeigt der Befehl **idsNativeInstall** entsprechende Nachrichten darüber an, ob die Installation erfolgreich war oder nicht. Prüfen Sie die Installationsprotokolle in der Protokolldatei, um zu überprüfen, ob die Pakete von IBM Security Directory Server installiert sind.

Der Name der Protokolldatei lautet `/var/idsldap/V6.3/idsNativeInstall_zeitmarke.log`.

Stellen Sie nach der Überprüfung des Installationsprotokolls sicher, dass alle Pakete erfolgreich installiert wurden und die erforderliche Version aufweisen. Weitere Informationen zum Abfragen der Versionsnummer der installierten Pakete finden Sie unter Kapitel 6, „IBM Security Directory Server-Pakete abfragen“, auf Seite 49.

---

## Kapitel 8. Installation von IBM DB2

Um eine IBM Security Directory Server-Instanz mit einer dafür konfigurierten DB2-Datenbank zu erstellen, muss auf dem Computer eine unterstützte Version von IBM DB2 installiert sein.

Auf den Installationsmedien von IBM Security Directory Server wird eine unterstützte Version von IBM DB2 bereitgestellt. Wenn Sie die Betriebssystemdienstprogramme für die Installation von IBM Security Directory Server verwenden, muss IBM DB2 installiert werden. Wenn Sie die Installation von IBM Security Directory Server durchführen, werden die Eigenschaftendateien mit den Details der unterstützten DB2-Version aktualisiert. Wenn auf Ihrem Computer eine unterstützte Version von IBM DB2 installiert ist, können Sie diese verwenden und mit Ihrer Verzeichnisserverinstanz konfigurieren. Weitere Informationen zum Aktualisieren der Datei `ldapdb.properties` finden Sie im Kapitel Anhang C, „Datei `ldapdb.properties` manuell aktualisieren“, auf Seite 263.

Verwenden Sie für die Installation von IBM DB2 die Installationsmedien von IBM Security Directory Server und rufen Sie das Verzeichnis mit der Installationsdatei für IBM DB2 auf.

Um die Installation von IBM DB2 durchführen zu können, müssen Sie die Voraussetzungen für DB2 erfüllen. Um sicherzustellen, dass Ihr Computer den Voraussetzungen für DB2 entspricht, führen Sie den Befehl **db2prereqcheck** aus. Wenn auf Ihrem Computer Pakete fehlen, muss er mit den erforderlichen Paketen aktualisiert werden.

Unter AIX, Linux und Solaris können Sie für die Installation von IBM DB2 den Befehl **db2\_install** verwenden. Verwenden Sie für die Installation von IBM DB2 unter Windows den Befehl **setup.exe**.

Wählen Sie unter System x Linux auf einer Intel 32-Bit-Architektur **Workspace Server Edition** aus, indem Sie "WSE" eingeben. Wählen Sie für andere unterstützte Betriebssysteme Enterprise Server Edition aus, indem Sie ESE eingeben.

Prüfen Sie nach der Installation von IBM DB2 die Datei `/tmp/db2_install_log.XXXXX`, um sicherzustellen, dass die Installation erfolgreich war. XXXXX steht für eine Zufallszahl, die der Installation zugeordnet ist.

Weitere Informationen zu den Voraussetzungen für DB2 und die Installation von IBM DB2 finden Sie in der Produktdokumentation zu IBM DB2 unter <http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome>.

### Kernelparameter auf Solaris-Systemen

Auf Solaris-Systemen müssen Sie vor der Installation von IBM DB2 möglicherweise die Kernelparameter in der Datei `/etc/system` aktualisieren. Zum Bestimmen der richtigen Kernelparameterwerte für Ihren Computer können Sie den Befehl **db2osconf** verwenden. Zum Konfigurieren der Solaris-Kernelparameterwerte vor der Installation von DB2 unter Solaris können Sie den Befehl **projmod** verwenden.

Auf Solaris-Systemen mit konfigurierten Zonen kann der Befehl **db2osconf** nur in der globalen Zone unter Solaris ausgeführt werden.

Weitere Informationen zum Befehl **db2osconf** finden Sie unter dem Suchbegriff **db2osconf** in der Produktdokumentation zu IBM DB2 unter <http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome>.

---

## Kapitel 9. IBM Java Development Kit für IBM Security Directory Server

Damit Java-Beispielprogramme kompiliert und Java-Programme wie **Instance Administration Tool** und das **Konfigurationstool** ausgeführt werden können, muss IBM Java Development Kit in der Installationsposition von IBM Security Directory Server dekomprimiert werden.

Auf den Installationsmedien von IBM Security Directory Server wird eine unterstützte Version von IBM Java Development Kit bereitgestellt, IBM Java 1.6 SR 14. Wenn Sie die Betriebssystemdienstprogramme für die Installation von IBM Security Directory Server verwenden, muss IBM Java Development Kit installiert werden.

Verwenden Sie für die Installation von IBM Java Development Kit die Installationsmedien von IBM Security Directory Server und rufen Sie das Verzeichnis mit der komprimierten Datei von IBM Java Development Kit auf.

Dekomprimieren Sie die IBM Java Development Kit-Archivdatei in der Installationsposition von IBM Security Directory Server. Die IBM Java Development Kit-Archivdatei wird im Verzeichnis java dekomprimiert. Weitere Informationen zur Installationsposition von IBM Security Directory Server finden Sie im Kapitel „Standardinstallationspositionen“ auf Seite 28.

Unter AIX können Sie auch tar für GNU zum Dekomprimieren der IBM Java Development Kit-Archivdatei in der Installationsposition von IBM Security Directory Server verwenden. Andernfalls müssen Sie möglicherweise das von Ihnen dekomprimierte Verzeichnis java in die Installationsposition von IBM Security Directory Server verschieben. Weitere Informationen zu den vorausgesetzten Paketen finden Sie im Kapitel „Auf verschiedenen Betriebssystemen erforderliche vorausgesetzte Pakete“ auf Seite 15.

*Tabelle 14. Für die unterschiedlichen Betriebssysteme verfügbare IBM Java Development Kit-Pakete*

Betriebssystem	Paketname
AIX	ibm-java-16sr14-aix-ppc-64.tar
System x Linux (Intel 32 Bit)	ibm-java-16sr14-linux-i386.tar
System i- und System p-Linux	ibm-java-16sr14-linux-ppc-64.tar
System z-Linux	ibm-java-16sr14-linux-s390-64.tar
Linux auf AMD64/EM64T	ibm-java-16sr14-linux-64.tar
HP-UX (Itanium)	ibm-java-16sr14-hp-itanium-64.tar
Solaris auf AMD64/EM64T	ibm-java-16sr14-solaris-amd-64.tar
Solaris SPARC	ibm-java-16sr14-solaris-sparc-64.tar
Windows 32 Bit	ibm-java-16sr14-win-i386.zip
Windows auf AMD64/EM64T	ibm-java-16sr14-win-x86_64.zip

## Beispiele

### Beispiel 1:

Führen Sie den folgenden Befehl aus, um die IBM Java Development Kit-Archivdatei auf einem Linux-System in der Installationsposition von IBM Security Directory Server zu dekomprimieren:

```
tar -xf ibm-java-16sr14-linux-64.tar -C /opt/ibm/ldap/V6.3.1/
```

---

## Kapitel 10. Installation von IBM Global Security Kit

Damit SSL (Secure Sockets Layer) und TLS (Transaction Layer Security) mit IBM Security Directory Server verwendet werden können, muss auf Ihrem Computer eine unterstützte Version von IBM Global Security Kit (GSKit) installiert sein.

Wenn die Installation mit IBM Installation Manager auf Ihren Betriebssystemen nicht unterstützt wird, können Sie die Betriebssystemdienstprogramme für die Installation von IBM Global Security Kit verwenden. GSKit muss sowohl auf den Server- als auch den Clientsystemen installiert werden, damit sichere Verbindungen hergestellt und verwendet werden können.

Für Verschlüsselungsunterstützung auf niedriger Ebene ist das GSKit-Verschlüsselungspaket erforderlich. Für Handshakeoperationen bei sicherer Kommunikation ist das GSKit-SSL-Paket erforderlich. Das GSKit-Verschlüsselungspaket ist eine Voraussetzung für das GSKit-SSL-Paket.

Auf den Installationsmedien von IBM Security Directory Server werden die folgenden GSKit-Pakete für verschiedene Betriebssysteme bereitgestellt:

**Anmerkung:** Für die Solaris-x64- und SPARC-Architekturen werden dieselben GSKit-Paketnamen verwendet.

### AIX

#### **Paketnamen von GSKit (64 Bit)**

GSKit8.gskcrypt64.ppc.rte

GSKit8.gskssl64.ppc.rte

#### **Paketnamen von GSKit (32 Bit)**

GSKit8.gskcrypt32.ppc.rte

GSKit8.gskssl32.ppc.rte

### System x Linux

#### **Paketnamen von GSKit (32 Bit)**

gskcrypt32-8.0.14.26.linux.x86.rpm

gskssl32-8.0.14.26.linux.x86.rpm

### System z-Linux

#### **Paketnamen von GSKit (64 Bit)**

gskcrypt64-8.0.14.26.linux.s390x.rpm

gskssl64-8.0.14.26.linux.s390x.rpm

#### **Paketnamen von GSKit (32 Bit)**

gskcrypt31-8.0.14.26.linux.s390.rpm

gskssl31-8.0.14.26.linux.s390.rpm

### System i- und System p-Linux

#### **Paketnamen von GSKit (64 Bit)**

gskcrypt64-8.0.14.26.linux.ppc.rpm

gskssl64-8.0.14.26.linux.ppc.rpm

**Paketnamen von GSKit (32 Bit)**

gskcrypt32-8.0.14.26.linux.ppc.rpm

gskssl32-8.0.14.26.linux.ppc.rpm

**Linux IA64 (Itanium) und Linux AMD64/EM64T**

**Paketnamen von GSKit (64 Bit)**

gskcrypt64-8.0.14.26.linux.x86\_64.rpm

gskssl64-8.0.14.26.linux.x86\_64.rpm

**Paketnamen von GSKit (32 Bit)**

gskcrypt32-8.0.14.26.linux.x86.rpm

gskssl32-8.0.14.26.linux.x86.rpm

**Solaris**

**Paketnamen von GSKit (64 Bit)**

gsk8cry64.pkg

gsk8ssl64.pkg

**Paketnamen von GSKit (32 Bit)**

gsk8cry32.pkg

gsk8ssl32.pkg

**HP-UX (Itanium)**

**Paketnamen von GSKit (64 Bit)**

gskcrypt64

gskssl64

**Paketnamen von GSKit (32 Bit)**

gskcrypt32

gskssl32

**Microsoft Windows**

**Paketnamen von GSKit (64 Bit)**

gsk8crypt64.exe

gsk8ssl64.exe

**Paketnamen von GSKit (32 Bit)**

gsk8crypt32.exe

gsk8ssl32.exe

---

## IBM Global Security Kit mit installp installieren

Mit dem Befehl **installp** können Sie die Installation von IBM Global Security Kit auf einem AIX-System ausführen.

### Vorbereitende Schritte

Greifen Sie auf die Installationsmedien von IBM Security Directory Server zu, um die Installationsdatei von IBM Global Security Kit abzurufen. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.



## Informationen zu diesem Vorgang

Das Installationsprogramm **installp** installiert IBM Global Security Kit (GSKit) auf einem AIX-System.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis `gskit`, in dem die Installationsdatei von IBM Global Security Kit gespeichert ist.
4. Führen Sie den Befehl **installp** aus, um die Pakete von IBM Global Security Kit zu installieren.
  - a. Führen Sie die folgenden Befehle aus, um die Pakete von 64-Bit-GSKit zu installieren:

```
installp -acgXd . GSKit8.gskcrypt64.ppc.rte
installp -acgXd . GSKit8.gskssl64.ppc.rte
```
  - b. Führen Sie die folgenden Befehle aus, um die Pakete von 32-Bit-GSKit zu installieren:

```
installp -acgXd . GSKit8.gskcrypt32.ppc.rte
installp -acgXd . GSKit8.gskssl32.ppc.rte
```
5. Führen Sie den folgenden Befehl aus, um zu prüfen, ob die Installation von IBM Global Security Kit erfolgreich war:

```
ls1pp -aL GSKit8*
```

### Ergebnisse

Das Installationsprogramm installiert IBM Global Security Kit auf einem AIX-System an den folgenden Positionen:

#### 64-Bit-GSKit

```
/usr/opt/ibm/gsk8_64/
```

#### 32-Bit-GSKit

```
/usr/opt/ibm/gsk8/
```

---

## IBM Global Security Kit mit Linux-Dienstprogrammen installieren

Mit dem Befehl **rpm** können Sie die Installation von IBM Global Security Kit auf einem Linux-System ausführen.

### Vorbereitende Schritte

Greifen Sie auf die Installationsmedien von IBM Security Directory Server zu, um die Installationsdatei von IBM Global Security Kit abzurufen. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

### Informationen zu diesem Vorgang

Der Befehl **rpm** installiert IBM Global Security Kit (GSKit) auf einem Linux-System. Das Beispiel zeigt die Installation von IBM Global Security Kit unter AMD64 Opteron/EM64T Linux. Setzen Sie für System z, System i, System p oder System x Linux die entsprechenden Paketnamen ein.

## Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis `gskit`, in dem die Installationsdatei von IBM Global Security Kit gespeichert ist.
4. Führen Sie den Befehl `rpm` aus, um die Pakete von IBM Global Security Kit zu installieren.
  - a. Führen Sie die folgenden Befehle aus, um die Pakete von 64-Bit-GSKit zu installieren:

```
rpm -ivh gskcrypt64-8.0.14.26.linux.x86_64.rpm
rpm -ivh gskssl64-8.0.14.26.linux.x86_64.rpm
```
  - b. Führen Sie die folgenden Befehle aus, um die Pakete von 32-Bit-GSKit zu installieren:

```
rpm -ivh gskcrypt32-8.0.14.26.linux.x86.rpm
rpm -ivh gskssl32-8.0.14.26.linux.x86.rpm
```
5. Führen Sie den folgenden Befehl aus, um zu prüfen, ob die Installation von IBM Global Security Kit erfolgreich war:

```
rpm -qa | grep -i gsk
```

## Ergebnisse

Das Installationsprogramm installiert IBM Global Security Kit auf einem Linux-System an den folgenden Positionen:

### 64-Bit-GSKit

```
/usr/local/ibm/gsk8_64/
```

### 32-Bit-GSKit

```
/usr/local/ibm/gsk8/
```

---

## IBM Global Security Kit mit Solaris-Dienstprogrammen installieren

Mit dem Befehl `pkgadd` können Sie die Installation von IBM Global Security Kit auf einem Solaris-System ausführen.

## Vorbereitende Schritte

Greifen Sie auf die Installationsmedien von IBM Security Directory Server zu. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

## Informationen zu diesem Vorgang

Der Befehl `pkgadd` installiert IBM Global Security Kit (GSKit) auf einem Solaris-System. Die Paket- und Dateinamen sind bei den Betriebssystemen Solaris SPARC und Solaris X64 identisch.

## Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis `gskit`, in dem die Installationsdatei von IBM Global Security Kit gespeichert ist.
4. Führen Sie den Befehl `pkgadd` aus, um die Pakete von IBM Global Security Kit zu installieren.

- a. Führen Sie die folgenden Befehle aus, um die Pakete von 64-Bit-GSKit zu installieren:
 

```
pkgadd -d gsk8cry64.pkg
pkgadd -d gsk8ss164.pkg
```
- b. Führen Sie die folgenden Befehle aus, um die Pakete von 32-Bit-GSKit zu installieren:
 

```
pkgadd -d gsk8cry32.pkg
pkgadd -d gsk8ss132.pkg
```
5. Führen Sie den folgenden Befehl aus, um zu prüfen, ob die Installation von IBM Global Security Kit erfolgreich war:
 

```
pkginfo | grep -i gsk
pkgparam package_name VERSION
```

Ersetzen Sie den Wert von `package_name` durch den Namen des GSKit-Pakets, um die Version zu überprüfen.

---

## IBM Global Security Kit mit HP-UX-Dienstprogrammen installieren

Mit dem Befehl **swinstall** können Sie die Installation von IBM Global Security Kit auf einem HP-UX-System ausführen.

### Vorbereitende Schritte

Greifen Sie auf die Installationsmedien von IBM Security Directory Server zu, um die Installationsdatei von IBM Global Security Kit abzurufen. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis `gskit`, in dem die Installationsdatei von IBM Global Security Kit gespeichert ist.
4. Führen Sie den Befehl **swinstall** aus, um die Pakete von IBM Global Security Kit zu installieren.
  - a. Führen Sie die folgenden Befehle aus, um die Pakete von 64-Bit-GSKit zu installieren:
 

```
swinstall -s path_to_gskit_installable/gskcrypt64 gskcrypt64
swinstall -s path_to_gskit_installable/gskss164 gskss164
```

Sie müssen den absoluten Pfadnamen der GSKit-Installationsdatei mit dem Parameter **-s** angeben.
  - b. Führen Sie die folgenden Befehle aus, um die Pakete von 32-Bit-GSKit zu installieren:
 

```
swinstall -s path_to_gskit_installable/gskcrypt32 gskcrypt32
swinstall -s path_to_gskit_installable/gskss132 gskss132
```
5. Führen Sie den folgenden Befehl aus, um zu prüfen, ob die Installation von IBM Global Security Kit erfolgreich war:
 

```
swlist | grep -i gsk
```

---

## IBM Global Security Kit unter Windows installieren

Führen Sie das Installationsprogramm von IBM Global Security Kit aus, um IBM Global Security Kit auf einem Windows-System zu installieren.

### Vorbereitende Schritte

Greifen Sie auf die Installationsmedien von IBM Security Directory Server zu, um die Installationsdatei von IBM Global Security Kit abzurufen. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

### Informationen zu diesem Vorgang

Das Beispiel zeigt die Installation von 64-Bit-GSKit Crypt und 64-Bit-GSKit SSL. Verwenden Sie für die Installation von 32-Bit-GSKit die entsprechenden Pakete. Auf dem 64-Bit-Betriebssystem von Windows können Sie sowohl 64-Bit-GSKit- als auch 32-Bit-GSKit-Pakete installieren.

### Vorgehensweise

1. Melden Sie sich als Mitglied der Administratorgruppe an.
2. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis `gskit`, in dem die Installationsdatei von IBM Global Security Kit gespeichert ist.
3. Führen Sie das Installationsprogramm von GSKit aus, um die Pakete von 64-Bit-GSKit zu installieren:
  - a. Führen Sie das Installationspaket von GSKit8 Crypt (`gsk8crypt64.exe`) aus.
  - b. Führen Sie im Installationsfenster von GSKit8 Crypt die folgenden Schritte aus:
    - 1) Geben Sie den Installationspfad für GSKit8 Crypt an.
    - 2) Klicken Sie auf **Weiter**.
    - 3) Klicken Sie auf **Installieren**.
    - 4) Klicken Sie auf **Fertig stellen**.
  - c. Führen Sie das Installationspaket von GSKit8 SSL (`gsk8ssl64.exe`) aus.
  - d. Führen Sie im Installationsfenster von GSKit8 SSL die folgenden Schritte aus:
    - 1) Geben Sie den Installationspfad für GSKit8 SSL an.
    - 2) Klicken Sie auf **Weiter**.
    - 3) Klicken Sie auf **Installieren**.
    - 4) Klicken Sie auf **Fertig stellen**.
4. Setzen Sie auf einem x86\_64-Windows-System die Variable `PATH` mit den Verzeichnissen `bin` und `lib64`, um GSKit-Befehle über die Befehlszeile auszuführen.

**Anmerkung:** Setzen Sie auf einem 32-Bit-Windows-System die Variable `PATH` mit den Verzeichnissen `bin` und `lib`.

Wenn GSKit im Pfad `C:\Program Files\IBM\gsk8` installiert wird, setzen Sie die Variable `PATH` mit den folgenden Werten:

```
set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%
set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
```

---

## Unbeaufsichtigte Installation von IBM Global Security Kit unter Windows

Führen Sie das Installationsprogramm von IBM Global Security Kit über die Eingabeaufforderung aus, um IBM Global Security Kit unbeaufsichtigt auf einem Windows-System zu installieren.

### Vorbereitende Schritte

Greifen Sie auf die Installationsmedien von IBM Security Directory Server zu, um die Installationsdatei von IBM Global Security Kit abzurufen. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

### Informationen zu diesem Vorgang

Das Beispiel zeigt die Installation von 64-Bit-GSKit Crypt und 64-Bit-GSKit SSL. Verwenden Sie für die Installation von 32-Bit-GSKit die entsprechenden Pakete. Auf dem 64-Bit-Betriebssystem von Windows können Sie sowohl 64-Bit-GSKit- als auch 32-Bit-GSKit-Pakete installieren.

### Vorgehensweise

1. Melden Sie sich als Mitglied der Administratorgruppe an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis `gskit`, in dem die Installationsdatei von IBM Global Security Kit gespeichert ist.
4. Führen Sie die folgenden Befehle aus, um die Pakete von 64-Bit-GSKit unbeaufsichtigt zu installieren:

```
gsk8crypt64.exe /s /v"/quiet"  
gsk8ssl64.exe /s /v"/quiet"
```

5. Setzen Sie auf einem x86\_64-Windows-System die Variable `PATH` mit den Verzeichnissen `bin` und `lib64`, um GSKit-Befehle über die Befehlszeile auszuführen.

**Anmerkung:** Setzen Sie auf einem 32-Bit-Windows-System die Variable `PATH` mit den Verzeichnissen `bin` und `lib`.

Wenn GSKit im Pfad `C:\Program Files\IBM\gsk8` installiert wird, setzen Sie die Variable `PATH` mit den folgenden Werten:

```
set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%  
set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
```



---

## Kapitel 11. Installation von Sprachenpaketen

Um die Verzeichnisservernachrichten in anderen Sprachen als Englisch generieren zu können, müssen die Sprachenpakete für die Sprachen installiert sein, die Sie verwenden möchten.

IBM Installation Manager kann alle Sprachenpakete, die für das Betriebssystem zur Verfügung stehen, installieren, wenn Sie ein Installations-Feature aus dem vollständigen Installationsprogramm auswählen. Die Sprachenpakete werden im Unterverzeichnis `nls` im Installationsverzeichnis von IBM Security Directory Server installiert.

**Anmerkung:** Für den Client müssen Sie keine Sprachenpakete installieren. Sie können für den Client Sprachenpakete installieren, wenn Sie möchten, dass Nachrichten für die Befehle `idslink` und `idsrmlink` in einer anderen Sprache als Englisch generiert werden. Informationen zu den Befehlen `idslink` und `idsrmlink` finden Sie in der *Befehlsreferenz*.

Sie können Sprachenpakete auf AIX- und Linux-Systemen mit IBM Installation Manager oder den Betriebssystemdienstprogrammen installieren. Die Installation von Sprachenpaketen mit IBM Installation Manager wird mit dem vollständigen Produktinstallationsprogramm von IBM Security Directory Server bereitgestellt.

**Hinweis:** Die Installation von Sprachenpaketen mit IBM Installation Manager wird nur unter AIX, Linux auf der AMD64/EM64T-Architektur und Microsoft Windows-Computern unterstützt. Bei Betriebssystemen, die die Installation von IBM Security Directory Server mit IBM Installation Manager unterstützen, dürfen die Sprachenpakete nicht manuell mit den Betriebssystemdienstprogrammen installiert werden. Wenn die Installation von Sprachenpaketen mit IBM Installation Manager für Ihr Betriebssystem nicht unterstützt wird, verwenden Sie die Betriebssystemdienstprogramme für die Installation der Sprachpakete.

*Tabelle 15. Liste der unterstützten Sprachen für die Betriebssysteme AIX, Linux, Solaris und Windows*

Sprachen	AIX	Linux	Solaris	Microsoft Windows
Tschechisch	✓			
Französisch	✓	✓	✓	✓
Deutsch	✓	✓	✓	✓
Ungarisch	✓			
Italienisch	✓	✓	✓	✓
Japanisch	✓	✓	✓	✓
Koreanisch	✓	✓	✓	✓
Polnisch	✓			
Portugiesisch (Brasilien)	✓	✓	✓	✓
Russisch	✓			
Slowakisch	✓			
Spanisch	✓	✓	✓	✓
Vereinfachtes Chinesisch	✓	✓	✓	✓

Tabelle 15. Liste der unterstützten Sprachen für die Betriebssysteme AIX, Linux, Solaris und Windows (Forts.)

Sprachen	AIX	Linux	Solaris	Microsoft Windows
Traditionelles Chinesisch	✓	✓	✓	✓

## Sprachenpakete für die Installation

Bevor Sie ein Sprachenpaket installieren, müssen Sie die Paketnamen angeben, die den einzelnen Sprachenpaketen für ein unterstütztes Betriebssystem zugeordnet sind.

### Sprache und Sprachenpaketnamen

**Hinweis:** Die Sprachenpakete für Linux werden in den folgenden Architekturen unterstützt:

- System x Linux
- System z-Linux
- AMD64 Opteron / Intel EM64T Linux
- System i- und System p-Linux

**Hinweis:** Die Sprachenpakete für Solaris werden in den folgenden Architekturen unterstützt:

- Solaris SPARC
- Solaris X64

Tabelle 16. Liste der unterstützten Sprachen mit den Sprachenpaketnamen auf den Betriebssystemen AIX, Linux und Solaris

Sprachen	AIX	Linux	Solaris
Tschechisch	idsldap.msg631.cs_CZ		
Französisch	idsldap.msg631.fr_FR	idsldap-msg631-fr-6.3.1-0.noarch.rpm	idsldap.msg631.fr.pkg
Deutsch	idsldap.msg631.de_DE	idsldap-msg631-de-6.3.1-0.noarch.rpm	idsldap.msg631.de.pkg
Ungarisch	idsldap.msg631.hu_HU		
Italienisch	idsldap.msg631.it_IT	idsldap-msg631-it-6.3.1-0.noarch.rpm	idsldap.msg631.it.pkg
Japanisch	idsldap.msg631.ja_JP	idsldap-msg631-ja-6.3.1-0.noarch.rpm	idsldap.msg631.ja.pkg
Koreanisch	idsldap.msg631.ko_KO	idsldap-msg631-ko-6.3.1-0.noarch.rpm	idsldap.msg631.ko.pkg
Polnisch	idsldap.msg631.pl_PL		
Portugiesisch (Brasilien)	idsldap.msg631.pt_BR	idsldap-msg631-pt_BR-6.3.1-0.noarch.rpm	idsldap.msg631.pt_BR.pkg
Russisch	idsldap.msg631.ru_RU		
Slowakisch	idsldap.msg631.sk_SK		
Spanisch	idsldap.msg631.es_ES	idsldap-msg631-es-6.3.1-0.noarch.rpm	idsldap.msg631.es.pkg



Tabelle 16. Liste der unterstützten Sprachen mit den Sprachenpaketnamen auf den Betriebssystemen AIX, Linux und Solaris (Forts.)

Sprachen	AIX	Linux	Solaris
Vereinfachtes Chinesisch	idsldap.msg631.zh_CN	idsldap-msg631-zh_CN-6.3.1-0.noarch.rpm	idsldap.msg631.zh_CN.pkg
Traditionelles Chinesisch	idsldap.msg631.zh_TW	idsldap-msg631-zh_TW-6.3.1-0.noarch.rpm	idsldap.msg631.zh_TW.pkg

## Sprachenpakete mit Betriebssystemdienstprogrammen installieren

Verwenden Sie für die Installation von Sprachenpaketen die Betriebssystemdienstprogramme, wenn das Betriebssystem die Installation mit IBM Installation Manager nicht unterstützt.

### Vorbereitende Schritte

Sie müssen die Installationsmedien von IBM Security Directory Server vorbereiten. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

### Informationen zu diesem Vorgang

Wenn die Nachrichten des Verzeichnisservers in einer anderen Sprache als Englisch generiert werden wollen, müssen Sie das entsprechende Sprachenpaket auf dem System installieren.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis, in dem die Installationsdatei von IBM Security Directory Server gespeichert ist.
4. Wechseln Sie in das Unterverzeichnis tdsLangpack.
5. Führen Sie zum Installieren des Sprachenpakets für eine Sprache die Befehle zur Paketinstallation aus. Im folgenden Beispiel wird die Installation des Sprachenpakets für Französisch angezeigt. Sie können jede andere Sprache installieren, indem Sie den Namen durch den passenden Paketnamen für das Betriebssystem ersetzen.

Betriebssystem	Befehl:
AIX	installp -acgXd . idsldap.msg631.fr_FR
Linux	rpm -ivh idsldap-msg631-fr-6.3.1-0.noarch.rpm
Solaris	pkgadd -d idsldap.msg631.fr.pkg

6. Überprüfen Sie, ob die Installation des Sprachenpakets erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

## Ergebnisse

Das Installationsprogramm installiert die Sprachenpakete in den folgenden Verzeichnissen:

*Tabelle 17. Standardinstallationsposition der Sprachenpakete von IBM Security Directory Server*

<b>Betriebssystem</b>	<b>Installationsposition des Sprachenpakets</b>
Linux	/opt/ibm/ldap/V6.3.1/nls/msg
AIX und Solaris	/opt/IBM/ldap/V6.3.1/nls/msg

---

## Kapitel 12. Installation mit den Befehlszeilendienstprogrammen des Betriebssystems

Sie können die Installation von IBM Security Directory Server mit den Befehlszeilendienstprogrammen des Betriebssystems ausführen, wenn Ihr System X11 nicht unterstützt.

### Vorsicht:

- Auf einem Computer dürfen keine unterschiedlichen Installationsmodi verwendet werden. Sie können die Installation von IBM Security Directory Server entweder mithilfe von IBM Installation Manager oder mithilfe der Befehlszeilendienstprogramme des Betriebssystems durchführen, aber nicht auf beide Arten. Wenn Sie beide Installationsmodi verwenden, werden möglicherweise nicht die richtigen Pakete für ein Feature installiert.
- Vermeiden Sie es, DB2 und eine integrierte Version von WebSphere Application Server manuell in den jeweiligen Standardinstallationspfaden, die von IBM Installation Manager verwendet werden, zu installieren. Bei der Installation, Änderung oder Deinstallation mithilfe von IBM Installation Manager können durch eine derartige manuelle Installation Fehler verursacht werden. Weitere Informationen zum Standardinstallationspfad finden Sie im Kapitel „Standardinstallationspositionen“ auf Seite 28.

Vor der Installation von IBM Security Directory Server müssen Sie die Installationsquelle abrufen. Das Produkt IBM Security Directory Server ist als Archivdatei und als installierbares Image verfügbar. Aus den installierbaren Images können Sie Installations-DVDs erstellen.

Bereiten Sie die Installationsmedien vor. Weitere Informationen hierzu finden Sie im Kapitel „Vorbereitung von Installationsmedien“ auf Seite 6.

**Wichtig:** Um IBM Security Directory Server als vollständigen Verzeichnisserver verwenden zu können, installieren Sie eine unterstützte Version von IBM DB2 auf dem Computer, sofern noch nicht installiert. Die Datei `ldapdb.properties` muss mit dem Pfadnamen und der Version von IBM DB2 konfiguriert werden.

---

## Installation mit AIX-Dienstprogrammen

Für die Installation von IBM Security Directory Server auf AIX-Systemen können Sie die AIX-Befehlszeilendienstprogramme verwenden.

Für die Installation von IBM Security Directory Server können Sie die folgenden Dienstprogramme verwenden:

**SMIT** Die Verwendung dieses Dienstprogramms ist die bevorzugte Installationsmethode. Weitere Informationen hierzu finden Sie unter „Installation mit SMIT“ auf Seite 74.

### **installp**

Weitere Informationen hierzu finden Sie unter „Installation mit **installp**“ auf Seite 75.

## Pakete für die Installation auf einem AIX-System

Um IBM Security Directory Server als vollständigen Verzeichnisserver, Proxy-Server oder Client auf einem AIX-System zu verwenden, müssen Sie die entsprechenden Pakete installieren.

### Pakete und Dateigruppen

IBM Security Directory Server stellt die Pakete für ein AIX-System bereit. Jedes Paket enthält eine oder mehrere Dateigruppen.

*Tabelle 18. Pakete und die darin enthaltenen Dateigruppen*

Pakete	Dateigruppen, die dem Paket zugeordnet sind
idsldap.license631	idsldap.license631.rte - Lizenz
idsldap.cltbodybase631	<ul style="list-style-type: none"><li>idsldap.cltbodybase631.rte - Laufzeitkomponente des Basisclients</li><li>idsldap.cltbodybase631.adt - SDK-Komponente des Basisclients</li></ul>
idsldap.clt32bit631	<ul style="list-style-type: none"><li>idsldap.clt32bit631.rte - 32-Bit-C-Client (ohne SSL und TLS)</li></ul>
idsldap.clt64bit631	<ul style="list-style-type: none"><li>idsldap.clt64bit631.rte - 64-Bit-C-Client (ohne SSL und TLS)</li></ul>
idsldap.clt_max_crypto32bit631	<ul style="list-style-type: none"><li>idsldap.clt_max_crypto32bit631.rte - 32-Bit-C-Client (mit SSL und TLS)</li></ul>
idsldap.clt_max_crypto64bit631	<ul style="list-style-type: none"><li>idsldap.clt_max_crypto64bit631.rte - 64-Bit-C-Client (mit SSL und TLS)</li></ul>
idsldap.cltjava631	<ul style="list-style-type: none"><li>idsldap.cltjava631.rte - <b>Java-Client</b></li></ul>
idsldap.srvbase64bit631	<ul style="list-style-type: none"><li>idsldap.srvbase64bit631.rte - Basisserver</li></ul>
idsldap.srv_max_cryptobase64bit631	<ul style="list-style-type: none"><li>idsldap.srv_max_cryptobase64bit631.rte - Basisserver (SSL)</li></ul>
idsldap.srvproxy64bit631	<ul style="list-style-type: none"><li>idsldap.srvproxy64bit631.rte - Proxy-Server (64-Bit)</li></ul>
idsldap.srv64bit631	<ul style="list-style-type: none"><li>idsldap.srv64bit631.rte - Verzeichnisserver (64-Bit)</li></ul>
idsldap.webadmin631	<ul style="list-style-type: none"><li>idsldap.webadmin631.rte - <b>Webverwaltungstool</b> (ohne SSL und TLS)</li></ul>
idsldap.webadmin_max_crypto631	<ul style="list-style-type: none"><li>idsldap.webadmin_max_crypto631.rte - <b>Webverwaltungstool</b> (mit SSL und TLS)</li></ul>
idsldap.msg631.en_US	Nicht verfügbar
idsldap.ent631	<ul style="list-style-type: none"><li>idsldap.ent631.rte - IBM Directory Server-Berechtigung (nur bei Passport Advantage bereitgestellt)</li></ul>

### Reihenfolge bei der Installation

Sie können alle Funktionen gleichzeitig installieren. Werden sie aber separat installiert, dann muss eine bestimmte Reihenfolge beachtet werden.

#### Wichtig:

- Wenn Sie Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) verwenden wollen, müssen Sie eine unterstützte Version von IBM Global Security Kit installieren.
- Für die Kerberos-Unterstützung auf AIX-Systemen ist eine unterstützte Version von Network Authentication Service erforderlich.

**Anmerkung:** Wenn der Computer X11 nicht unterstützt, können Sie die in IBM JDK bereitgestellte Installation der JDK-Komponente überspringen. Wird die JDK-Komponente nicht installiert, können Sie das **Instance Administration Tool** oder das **Konfigurationstool** möglicherweise nicht verwenden.

Tabelle 19. Installationsreihenfolge für das Client-Feature

32-Bit-Client (ohne SSL und TLS)	32-Bit-Client (mit SSL und TLS)	64-Bit-Client (ohne SSL und TLS)	64-Bit-Client (mit SSL und TLS)
1. idsldap.cltbase631	1. idsldap.cltbase631	1. idsldap.cltbase631	1. idsldap.cltbase631
2. idsldap.clt32bit631	2. idsldap.clt32bit631	2. idsldap.clt64bit631	2. idsldap.clt64bit631
3. idsldap.cltjava631	3. idsldap.clt_max_crypto32bit631	3. idsldap.cltjava631	3. idsldap.clt_max_crypto32bit631
	4. idsldap.cltjava631		4. idsldap.cltjava631

**Anmerkung:** Wenn Sie den Client-Server mit einer archivierten Berechtigungsdatei oder ein ISO-Image mit einer Berechtigung zur Installation von IBM Security Directory Server verwenden, müssen Sie zuerst die Lizenzbedingungen akzeptieren und das Paket `idsldap.license631` installieren.

Tabelle 20. Installationsreihenfolge für das vollständige Verzeichnisserver-Feature

Vollständiger 64-Bit-Verzeichnisserver (ohne SSL und TLS)	Vollständiger 64-Bit-Verzeichnisserver (mit SSL und TLS)
1. idsldap.license631	1. idsldap.license631
2. idsldap.cltbase631	2. idsldap.cltbase631
3. idsldap.clt64bit631	3. idsldap.clt64bit631
4. idsldap.cltjava631	4. idsldap.clt_max_crypto64bit631
5. idsldap.srvbase64bit631	5. idsldap.cltjava631
6. idsldap.srv64bit631	6. idsldap.srvbase64bit631
7. idsldap.msg631.en_US	7. idsldap.srv_max_cryptobase64bit631
8. idsldap.ent631	8. idsldap.srv64bit631
	9. idsldap.msg631.en_US
	10. idsldap.ent631

Tabelle 21. Installationsreihenfolge für das Proxy-Server-Feature

64-Proxy-Server (ohne SSL und TLS)	64-Proxy-Server (mit SSL und TLS)
1. idsldap.license631	1. idsldap.license631
2. idsldap.cltbase631	2. idsldap.cltbase631
3. idsldap.clt64bit631	3. idsldap.clt64bit631
4. idsldap.cltjava631	4. idsldap.clt_max_crypto64bit631
5. idsldap.srvbase64bit631	5. idsldap.cltjava631
6. idsldap.srvproxy64bit631	6. idsldap.srvbase64bit631
7. idsldap.msg631.en_US	7. idsldap.srv_max_cryptobase64bit631
8. idsldap.ent631	8. idsldap.srvproxy64bit631
	9. idsldap.msg631.en_US
	10. idsldap.ent631

**Anmerkung:** Um das **Webverwaltungstool** zu verwenden, müssen Sie es auf einem Webanwendungsserver implementieren. Weitere Informationen zur Installation einer integrierten Version von WebSphere Application Server finden Sie unter „Integrierte Version von WebSphere Application Server manuell installieren“ auf Seite 113.

Tabelle 22. Installationspaket des Webverwaltungstools

Webverwaltungstool (ohne SSL und TLS)	Webverwaltungstool (mit SSL und TLS)
1. idsldap.license631	1. idsldap.license631
2. idsldap.webadmin631	2. idsldap.webadmin_max_crypto631

Wenn Sie das **Webverwaltungstool** installieren, werden auch DSML-Dateien (DSML = Directory Services Markup Language) auf Ihren Computer kopiert. Weitere Informationen zu DSML finden Sie in Anhang A, „Directory Services Markup Language“, auf Seite 259.

## Installation mit SMIT

Mit dem Befehl **smit** können Sie die Installation von IBM Security Directory Server auf einem AIX-System ausführen.

### Vorbereitende Schritte

Sie müssen die Installationsmedien von IBM Security Directory Server vorbereiten. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

### Informationen zu diesem Vorgang

Das Installationsprogramm **smit** installiert IBM Security Directory Server auf einem AIX-System. Wenn eine unterstützte Version von IBM DB2 auf dem System installiert wird, aktualisiert der Installationsprozess die Datei `ldapdb.properties` mit dem Pfadnamen und der Version von DB2.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie den Befehl **idsLicense** aus.  
`./idsLicense`
4. Wenn Sie die Bedingungen der Softwarelizenzvereinbarung akzeptieren, geben Sie 1 ein. Sie können folgende Optionen verwenden:
  - 1: Lizenzvereinbarung akzeptieren
  - 2: Lizenzvereinbarung ablehnen und Installation beenden
  - 3: Lizenzvereinbarung drucken
  - 4: Nicht für IBM geltende Bedingungen in der Lizenzvereinbarung lesen
  - 99: Zur vorherigen Anzeige zurückkehren

Durch das Akzeptieren der Bedingungen in der Lizenzvereinbarung werden an der Installationsposition von IBM Security Directory Server die Datei `LAPID` und der Ordner `license` erstellt. Der Ordner "license" enthält die Lizenzdateien von IBM Security Directory Server in allen unterstützten Sprachen.

**Wichtig:** Ändern oder löschen Sie die Datei `LAPID` und die Lizenzdateien im Ordner "license" nicht.

5. Führen Sie den Befehl **smit install** aus. Das Fenster **Softwareinstallation und -wartung** wird geöffnet.
6. Klicken Sie auf **Software installieren und aktualisieren > Gesamte verfügbare Software installieren und aktualisieren**.
7. Wählen Sie Ihre Installationsmedien aus.
  - Führen Sie die folgenden Tasks aus, wenn Sie die Installation über die DVD vornehmen:

- a. Klicken Sie auf **Liste**, um auf die Einheit zuzugreifen, die die IBM Security Directory Server-Images enthält.
- Geben Sie im Feld **Eingabeeinheit/-verzeichnis für Software** einen Punkt (.) ein, wenn Sie die Installation über die nicht komprimierte Archivdatei vornehmen.
8. Klicken Sie auf **Ausführen**.
9. Bewegen Sie den Cursor auf den Eintrag **Zu installierende Software** und führen Sie folgende Aktionen aus:
  - a. Geben Sie `idsldap` ein, um die Dateigruppe `idsldap` zu installieren.
  - b. Klicken Sie auf **Liste**, um alle Dateigruppen aufzulisten, und wählen Sie dann die Dateigruppen aus, die Sie installieren wollen.
  - c. Klicken Sie auf **OK**.
10. Klicken Sie auf **OK**, um die Installation zu starten.
11. Vergewissern Sie sich anhand der Installationszusammenfassung am Ende der Ausgabe, ob alle Dateigruppen erfolgreich installiert wurden.
12. Nachdem die Installation abgeschlossen wurde, klicken Sie auf **Fertig**.
13. Drücken Sie zum Beenden des Programms **SMIT** die Taste F12.
14. Überprüfen Sie, ob die Installation von IBM Security Directory Server erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

## Ergebnisse

Das Installationsprogramm installiert IBM Security Directory Server auf dem AIX-System im Verzeichnis `/opt/IBM/ldap/V6.3.1`. Wenn eine unterstützte Version von IBM DB2 auf dem System installiert wird, aktualisiert der Installationsprozess die Datei `ldapdb.properties` mit dem Pfadnamen und der Version von DB2.

## Nächste Schritte

Nach der Installation von IBM Security Directory Server müssen Sie die folgende Aktion ausführen:

- Um IBM Security Directory Server als vollständigen Verzeichnisserver zu verwenden, erstellen Sie eine Verzeichnisserverinstanz. Siehe „Standardverzeichnisserverinstanz erstellen“ auf Seite 141.
- Um IBM Security Directory Server als Proxy-Server zu verwenden, erstellen Sie eine Proxy-Server-Instanz. Siehe „Proxy-Server-Instanz mit angepassten Einstellungen erstellen“ auf Seite 150.

## Installation mit `installp`

Mit dem Befehl `installp` können Sie die Installation von IBM Security Directory Server auf einem AIX-System ausführen.

## Vorbereitende Schritte

Sie müssen die Installationsmedien von IBM Security Directory Server vorbereiten. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

## Informationen zu diesem Vorgang

Das Installationsprogramm **installp** installiert IBM Security Directory Server auf einem AIX-System. Wenn eine unterstützte Version von IBM DB2 auf dem System installiert wird, aktualisiert der Installationsprozess die Datei `ldapdb.properties` mit dem Pfadnamen und der Version von DB2.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis, in dem die Installationsdatei von IBM Security Directory Server gespeichert ist.
4. Führen Sie den Befehl **idsLicense** aus.  
`./idsLicense`
5. Wenn Sie die Bedingungen der Softwarelizenzvereinbarung akzeptieren, geben Sie 1 ein. Sie können folgende Optionen verwenden:
  - 1: Lizenzvereinbarung akzeptieren
  - 2: Lizenzvereinbarung ablehnen und Installation beenden
  - 3: Lizenzvereinbarung drucken
  - 4: Nicht für IBM geltende Bedingungen in der Lizenzvereinbarung lesen
  - 99: Zur vorherigen Anzeige zurückkehren

Durch das Akzeptieren der Bedingungen in der Lizenzvereinbarung werden an der Installationsposition von IBM Security Directory Server die Datei Lapid und der Ordner `license` erstellt. Der Ordner "license" enthält die Lizenzdateien von IBM Security Directory Server in allen unterstützten Sprachen.

**Wichtig:** Ändern oder löschen Sie die Datei Lapid und die Lizenzdateien im Ordner "license" nicht.

6. Legen Sie fest, welche Pakete von IBM Security Directory Server Sie installieren wollen.

```
installp -ld . | grep idsldap
```

Es wird eine Liste mit den installierbaren Paketen für IBM Security Directory Server angezeigt.

7. Führen Sie den folgenden Befehl aus, um die Pakete zu installieren:

```
installp -acgXd . package_names
```

Führen Sie den folgenden Befehl aus, um alle Pakete von IBM Security Directory Server aus dem aktuellen Pfad zu installieren:

```
installp -acgXd . idsldap
```

8. Nach dem Abschluss der Installation generiert das System eine Installationszusammenfassung.
9. Überprüfen Sie, ob die Installation von IBM Security Directory Server erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

### Ergebnisse

Das Installationsprogramm installiert IBM Security Directory Server auf dem AIX-System im Verzeichnis `/opt/IBM/ldap/V6.3.1`. Wenn eine unterstützte Version von IBM DB2 auf dem System installiert wird, aktualisiert der Installationsprozess die



Datei `ldapdb.properties` mit dem Pfadnamen und der Version von DB2.

## Nächste Schritte

Nach der Installation von IBM Security Directory Server müssen Sie die folgenden Aktionen ausführen:

- Um IBM Security Directory Server als vollständigen Verzeichnisserver zu verwenden, erstellen Sie eine Verzeichnisserverinstanz. Weitere Informationen hierzu finden Sie unter „Standardverzeichnisserverinstanz erstellen“ auf Seite 141.
- Um IBM Security Directory Server als Proxy-Server zu verwenden, erstellen Sie eine Proxy-Server-Instanz. Weitere Informationen hierzu finden Sie unter „Proxy-Server-Instanz mit angepassten Einstellungen erstellen“ auf Seite 150.

---

## Installation mit Linux-Dienstprogrammen

Zum Installieren von IBM Security Directory Server auf Linux-Systemen können Sie die Linux-Befehlszeilendienstprogramme verwenden.

IBM Security Directory Server stellt unterschiedliche Pakete für Computer mit unterschiedlichen Betriebssystemen und Architekturen bereit. Wählen Sie die passenden Pakete für die Installation auf Ihrem Computer aus. Weitere Informationen zu den Namen der Pakete finden Sie im Kapitel „Pakete für die Installation auf einem Linux-System“.

## Pakete für die Installation auf einem Linux-System

Um IBM Security Directory Server als vollständigen Verzeichnisserver, Proxy-Server oder Client auf einem Linux-System zu verwenden, müssen Sie die entsprechenden Pakete installieren.

### Pakete für verschiedene Linux-Systeme

*Tabelle 23. Pakete mit IBM Security Directory Server für verschiedene Linux-Systeme*

IBM Security Directory Server-Pakete	AMD64 Opteron/ EM64T Linux	System i oder System p	System x	System z
IBM Directory Server - Lizenz	<code>idsldap-license631-6.3.1-0.x86_64.rpm</code>	<code>idsldap-license631-6.3.1-0.ppc.rpm</code>	<code>idsldap-license631-6.3.1-0.i386.rpm</code>	<code>idsldap-license631-6.3.1-0.s390.rpm</code>
IBM Directory Server - Basisclient	<code>idsldap-cltbase631-6.3.1-0.x86_64.rpm</code>	<code>idsldap-cltbase631-6.3.1-0.ppc.rpm</code>	<code>idsldap-cltbase631-6.3.1-0.i386.rpm</code>	<code>idsldap-cltbase631-6.3.1-0.s390.rpm</code>
IBM Directory Server - 32-Bit-Client	<code>idsldap-clt32bit631-6.3.1-0.x86_64.rpm</code>	<code>idsldap-clt32bit631-6.3.1-0.ppc.rpm</code>	<code>idsldap-clt32bit631-6.3.1-0.i386.rpm</code>	<code>idsldap-clt32bit631-6.3.1-0.s390.rpm</code>
IBM Directory Server - 64-Bit-Client	<code>idsldap-clt64bit631-6.3.1-0.x86_64.rpm</code>	<code>idsldap-clt64bit631-6.3.1-0.ppc64.rpm</code>	Nicht verfügbar	<code>idsldap-clt64bit631-6.3.1-0.s390x.rpm</code>
IBM Directory Server - Java-Client	<code>idsldap-cltjava631-6.3.1-0.x86_64.rpm</code>	<code>idsldap-cltjava631-6.3.1-0.ppc.rpm</code>	<code>idsldap-cltjava631-6.3.1-0.i386.rpm</code>	<code>idsldap-cltjava631-6.3.1-0.s390.rpm</code>
IBM Directory Server - Basisserver	<code>idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm</code>	<code>idsldap-srvbase64bit631-6.3.1-0.ppc64.rpm</code>	<code>idsldap-srvbase32bit631-6.3.1-0.i386.rpm</code>	<code>idsldap-srvbase64bit631-6.3.1-0.s390x.rpm</code>
IBM Directory Server - Proxy-Server	<code>idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm</code>	<code>idsldap-srvproxy64bit631-6.3.1-0.ppc64.rpm</code>	<code>idsldap-srvproxy32bit631-6.3.1-0.i386.rpm</code>	<code>idsldap-srvproxy64bit631-6.3.1-0.s390x.rpm</code>
IBM Directory Server - 32-Bit-Server	Nicht verfügbar	Nicht verfügbar	<code>idsldap-srv32bit631-6.3.1-0.i386.rpm</code>	Nicht verfügbar
IBM Directory Server - 64-Bit-Server	<code>idsldap-srv64bit631-6.3.1-0.x86_64.rpm</code>	<code>idsldap-srv64bit631-6.3.1-0.ppc64.rpm</code>	Nicht verfügbar	<code>idsldap-srv64bit631-6.3.1-0.s390x.rpm</code>

Tabelle 23. Pakete mit IBM Security Directory Server für verschiedene Linux-Systeme (Forts.)

IBM Security Directory Server-Pakete	AMD64 Opteron/EM64T Linux	System i oder System p	System x	System z
IBM Directory Server - Webverwaltungstool	idsldap-webadmin631-6.3.1-0.x86_64.rpm	idsldap-webadmin631-6.3.1-0.ppc.rpm	idsldap-webadmin631-6.3.1-0.i386.rpm	idsldap-webadmin631-6.3.1-0.s390.rpm
IBM Directory Server - Nachrichten in amerikanischem Englisch	idsldap-msg631-en-6.3.1-0.x86_64.rpm	idsldap-msg631-en-6.3.1-0.ppc.rpm	idsldap-msg631-en-6.3.1-0.i386.rpm	idsldap-msg631-en-6.3.1-0.s390.rpm
IBM Directory Server-Berechtigung (nur bei Passport Advantage bereitgestellt)	idsldap-ent631-6.3.1-0.x86_64.rpm	idsldap-ent631-6.3.1-0.ppc.rpm	idsldap-ent631-6.3.1-0.i386.rpm	idsldap-ent631-6.3.1-0.s390.rpm

## Paketabhängigkeit

Bei der Installation bestimmter Pakete müssen Sie zuerst die Abhängigkeiten installieren.

**Anmerkung:** Wenn Sie den Client-Server mit einer archivierten Berechtigungsdatei oder ein ISO-Image mit einer Berechtigung zur Installation von IBM Security Directory Server verwenden, müssen Sie zuerst die Lizenzbedingungen akzeptieren und das Paket `idsldap-license631-6.3.1-0.arch.rpm` installieren.

In der Tabelle wird die Paketabhängigkeit von AMD64 Opteron/EM64T Linux gezeigt. Setzen Sie für System z, System i, System p oder System x Linux die entsprechenden Paketnamen ein.

Tabelle 24. Pakete und von diesen abhängige Pakete

Paketname	Abhängig von
idsldap-clt32bit631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.x86_64.rpm
idsldap-clt64bit631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.x86_64.rpm
idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm	<ol style="list-style-type: none"> <li>idsldap-license631-6.3.1-0.x86_64.rpm</li> <li>idsldap-cltbase631-6.3.1-0.x86_64.rpm</li> <li>idsldap-clt64bit631-6.3.1-0.x86_64.rpm</li> </ol>
idsldap-srv64bit631-6.3.1-0.x86_64.rpm	<ol style="list-style-type: none"> <li>idsldap-license631-6.3.1-0.x86_64.rpm</li> <li>idsldap-cltbase631-6.3.1-0.x86_64.rpm</li> <li>idsldap-clt64bit631-6.3.1-0.x86_64.rpm</li> <li>idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm</li> </ol>
idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm	<ol style="list-style-type: none"> <li>idsldap-license631-6.3.1-0.x86_64.rpm</li> <li>idsldap-cltbase631-6.3.1-0.x86_64.rpm</li> <li>idsldap-clt64bit631-6.3.1-0.x86_64.rpm</li> <li>idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm</li> </ol>

## Reihenfolge bei der Installation

Sie können alle Funktionen gleichzeitig installieren. Werden sie aber separat installiert, dann muss eine bestimmte Reihenfolge beachtet werden.

**Wichtig:** Wenn Sie Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) verwenden wollen, müssen Sie eine unterstützte Version von IBM Global Security Kit installieren.

Im Beispiel für die Installationsreihenfolge wird AMD64 Opteron/EM64T Linux verwendet. Setzen Sie für System z, System i, System p oder System x Linux die entsprechenden Paketnamen ein.

*Tabelle 25. Installationsreihenfolge für das Client-Feature*

32-Bit-Client	64-Bit-Client
1. idsldap-cltbase631-6.3.1-0.x86_64.rpm	1. idsldap-cltbase631-6.3.1-0.x86_64.rpm
2. idsldap-clt32bit631-6.3.1-0.x86_64.rpm	2. idsldap-clt64bit631-6.3.1-0.x86_64.rpm
3. idsldap-cltjava631-6.3.1-0.x86_64.rpm	3. idsldap-cltjava631-6.3.1-0.x86_64.rpm

*Tabelle 26. Installationsreihenfolge für das vollständige Verzeichnissever-Feature und das Proxy-Server-Feature*

Vollständiger 64-Bit-Verzeichnissever	64-Proxy-Server
1. idsldap-license631-6.3.1-0.x86_64.rpm	1. idsldap-license631-6.3.1-0.x86_64.rpm
2. idsldap-cltbase631-6.3.1-0.x86_64.rpm	2. idsldap-cltbase631-6.3.1-0.x86_64.rpm
3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm	3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm
4. idsldap-cltjava631-6.3.1-0.x86_64.rpm	4. idsldap-cltjava631-6.3.1-0.x86_64.rpm
5. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm	5. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm
6. idsldap-srv64bit631-6.3.1-0.x86_64.rpm	6. idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm
7. idsldap-msg631-en-6.3.1-0.x86_64.rpm	7. idsldap-msg631-en-6.3.1-0.x86_64.rpm
8. idsldap-ent631-6.3.1-0.x86_64.rpm	8. idsldap-ent631-6.3.1-0.x86_64.rpm

**Anmerkung:** Um das **Webverwaltungstool** zu verwenden, müssen Sie es auf einem Webanwendungsserver implementieren. Weitere Informationen zur Installation einer integrierten Version von WebSphere Application Server finden Sie unter „Integrierte Version von WebSphere Application Server manuell installieren“ auf Seite 113.

*Tabelle 27. Installationspaket des Webverwaltungstools*

Webverwaltungstool
1. idsldap-license631-6.3.1-0.x86_64.rpm
2. idsldap-webadmin631-6.3.1-0.x86_64.rpm

Wenn Sie das **Webverwaltungstool** installieren, werden auch DSML-Dateien (DSML = Directory Services Markup Language) auf Ihren Computer kopiert. Weitere Informationen zu DSML finden Sie in Anhang A, „Directory Services Markup Language“, auf Seite 259.

## Installation mit Linux-Dienstprogrammen

Mit dem Befehl **rpm** können Sie die Installation von IBM Security Directory Server auf einem Linux-System ausführen.

### Vorbereitende Schritte

Sie müssen die Installationsmedien von IBM Security Directory Server vorbereiten. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

## Informationen zu diesem Vorgang

Das Installationsprogramm **rpm** installiert IBM Security Directory Server auf einem Linux-System. Wenn eine unterstützte Version von IBM DB2 auf dem System installiert wird, aktualisiert der Installationsprozess die Datei `ldapdb.properties` mit dem Pfadnamen und der Version von DB2.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis, in dem die Installationsdatei von IBM Security Directory Server gespeichert ist.
4. Führen Sie den Befehl **idsLicense** aus.  
`./idsLicense`
5. Wenn Sie die Bedingungen der Softwarelizenzvereinbarung akzeptieren, geben Sie 1 ein. Sie können folgende Optionen verwenden:
  - 1: Lizenzvereinbarung akzeptieren
  - 2: Lizenzvereinbarung ablehnen und Installation beenden
  - 3: Lizenzvereinbarung drucken
  - 4: Nicht für IBM geltende Bedingungen in der Lizenzvereinbarung lesen
  - 99: Zur vorherigen Anzeige zurückkehren

Durch das Akzeptieren der Bedingungen in der Lizenzvereinbarung werden an der Installationsposition von IBM Security Directory Server die Datei `LAPID` und der Ordner `license` erstellt. Der Ordner "license" enthält die Lizenzdateien von IBM Security Directory Server in allen unterstützten Sprachen.

**Wichtig:** Ändern oder löschen Sie die Datei `LAPID` und die Lizenzdateien im Ordner "license" nicht.

6. Führen Sie den folgenden Befehl aus, um das Paket zu installieren:  
`rpm -ivh package_name`

Führen Sie den folgenden Befehl aus, um alle Pakete von IBM Security Directory Server zu installieren:

```
rpm -ivh idsldap*
```

7. Überprüfen Sie, ob die Installation von IBM Security Directory Server erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

### Ergebnisse

Das Installationsprogramm installiert IBM Security Directory Server auf dem Linux-System im Verzeichnis `/opt/ibm/ldap/V6.3.1`. Wenn eine unterstützte Version von IBM DB2 auf dem System installiert wird, aktualisiert der Installationsprozess die Datei `ldapdb.properties` mit dem Pfadnamen und der Version von DB2.

### Nächste Schritte

Nach der Installation von IBM Security Directory Server müssen Sie die folgende Aktion ausführen:

- Um IBM Security Directory Server als vollständigen Verzeichnisserver zu verwenden, erstellen Sie eine Verzeichnisserverinstanz. Weitere Informationen hierzu finden Sie unter „Standardverzeichnisserverinstanz erstellen“ auf Seite 141.

- Um IBM Security Directory Server als Proxy-Server zu verwenden, erstellen Sie eine Proxy-Server-Instanz. Weitere Informationen hierzu finden Sie unter „Proxy-Server-Instanz mit angepassten Einstellungen erstellen“ auf Seite 150.

## Installation mit Solaris-Dienstprogrammen

Zum Installieren von IBM Security Directory Server auf Solaris-Systemen können Sie die Solaris-Befehlszeilendienstprogramme verwenden.

IBM Security Directory Server stellt dieselben Pakete für Computer mit unterschiedlichen Architekturen bereit. Es sind Pakete für die Solaris-Betriebssysteme Sun SPARC Solaris und AMD64 Opteron/EM64T verfügbar. Die Paketnamen und Dateinamen sind für beide Betriebssysteme dieselben. Weitere Informationen zu den Namen der Pakete finden Sie unter „Pakete für die Installation auf einem Solaris-System“.

Bei der Installation der IBM Security Directory Server-Pakete darf der Systemstandardwert ALLE nicht verwendet werden. Wenn Sie alle Pakete auswählen, werden diese nicht ordnungsgemäß vom System sortiert und die Installation schlägt fehl.

## Pakete für die Installation auf einem Solaris-System

Um IBM Security Directory Server als vollständigen Verzeichnisserver, Proxy-Server oder Client auf einem Solaris-System zu verwenden, müssen Sie die entsprechenden Pakete installieren.

### Pakete für Solaris-Systeme

**Wichtig:** Die Paket- und Dateinamen sind bei den Betriebssystemen Solaris SPARC und AMD64 Opteron/EM64T Solaris identisch.

*Tabelle 28. Pakete mit IBM Security Directory Server für verschiedene Solaris-Systeme*

IBM Security Directory Server-Pakete	Paketnamen	Dateiname
IBM Directory Server - Lizenz	IDS1license631	idsldap-license631.pkg
IBM Directory Server - Basisclient	IDS1bc631	idsldap.clbase631.pkg
IBM Directory Server - 32-Bit-Client	IDS132c631	idsldap.clt32bit631.pkg
IBM Directory Server - 64-Bit-Client	IDS164c631	idsldap.clt64bit631.pkg
IBM Directory Server - Java-Client	IDS1jc631	idsldap.cltjava631.pkg
IBM Directory Server - Basisserver	IDS1bs631	idsldap.srvbase64bit631.pkg
IBM Directory Server - Proxy-Server	IDS164p631	idsldap.srvproxy64bit631.pkg
IBM Directory Server - 64-Bit-Server	IDS164s631	idsldap.srv64bit631.pkg
IBM Directory Server - Webverwaltungstool	IDS1web631	idsldap.webadmin631.pkg
IBM Directory Server - Nachrichten in amerikanischem Englisch	IDS1en631	idsldap.msg631.en.pkg
IBM Directory Server-Berechtigung (nur bei Passport Advantage bereitgestellt)	IDS1ent631	idsldap.ent631.pkg

### Paketabhängigkeit

Bei der Installation bestimmter Pakete müssen Sie zuerst die Abhängigkeiten installieren.

Tabelle 29. Pakete und von diesen abhängige Pakete

Paketname	Abhängig von
idsldap.clt32bit631.pkg	idsldap.cltbase631.pkg
idsldap.clt64bit631.pkg	idsldap.cltbase631.pkg
idsldap.srvbase64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg
idsldap.srv64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg 4. idsldap.srvbase64bit631.pkg
idsldap.srvproxy64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg 4. idsldap.srvbase64bit631.pkg

## Reihenfolge bei der Installation

Wenn Sie die Pakete auf einem Solaris-System installieren, muss eine bestimmte Reihenfolge beachtet werden.

**Wichtig:** Wenn Sie Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) verwenden wollen, müssen Sie eine unterstützte Version von IBM Global Security Kit installieren.

Tabelle 30. Installationsreihenfolge für das Client-Feature

32-Bit-Client	64-Bit-Client
1. idsldap.cltbase631.pkg	1. idsldap.cltbase631.pkg
2. idsldap.clt32bit631.pkg	2. idsldap.clt64bit631.pkg
3. idsldap.cltjava631.pkg	3. idsldap.cltjava631.pkg

**Anmerkung:** Wenn Sie den Client-Server mit einer archivierten Berechtigungsdatei oder ein ISO-Image mit einer Berechtigung zur Installation von IBM Security Directory Server verwenden, müssen Sie zuerst die Lizenzbedingungen akzeptieren und das Paket `idsldap-license631.pkg` installieren.

Tabelle 31. Installationsreihenfolge für das vollständige Verzeichnisserver-Feature und das Proxy-Server-Feature

Vollständiger 64-Bit-Verzeichnisserver	64-Proxy-Server
1. idsldap-license631.pkg	1. idsldap-license631.pkg
2. idsldap.cltbase631.pkg	2. idsldap.cltbase631.pkg
3. idsldap.clt64bit631.pkg	3. idsldap.clt64bit631.pkg
4. idsldap.cltjava631.pkg	4. idsldap.cltjava631.pkg
5. idsldap.srvbase64bit631.pkg	5. idsldap.srvbase64bit631.pkg
6. idsldap.srv64bit631.pkg	6. idsldap.srvproxy64bit631.pkg
7. idsldap.msg631.en.pkg	7. idsldap.msg631.en.pkg
8. idsldap.ent631.pkg	8. idsldap.ent631.pkg

**Anmerkung:** Um das **Webverwaltungstool** zu verwenden, müssen Sie es auf einem Webanwendungsserver implementieren. Weitere Informationen zur Installation einer integrierten Version von WebSphere Application Server finden Sie unter „Integrierte Version von WebSphere Application Server manuell installieren“ auf Seite 113.

Tabelle 32. Installationspaket des **Webverwaltungstools**

Webverwaltungstool
1. idsldap-license631.pkg
2. idsldap.webadmin631.pkg

Wenn Sie das **Webverwaltungstool** installieren, werden auch DSML-Dateien (DSML = Directory Services Markup Language) auf Ihren Computer kopiert. Weitere Informationen zu DSML finden Sie in Anhang A, „Directory Services Markup Language“, auf Seite 259.

## Installation mit Solaris-Dienstprogrammen

Mit dem Befehl **pkgadd** können Sie die Installation von IBM Security Directory Server auf einem Solaris-System ausführen.

### Vorbereitende Schritte

Greifen Sie auf die Installationsmedien von IBM Security Directory Server zu. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

### Informationen zu diesem Vorgang

Das Installationsprogramm **pkgadd** installiert IBM Security Directory Server auf einem Solaris-System. Wenn eine unterstützte Version von IBM DB2 auf dem System installiert wird, aktualisiert der Installationsprozess die Datei `ldapdb.properties` mit dem Pfadnamen und der Version von DB2.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis, in dem die Installationsdatei von IBM Security Directory Server gespeichert ist.
4. Führen Sie den Befehl **idsLicense** aus.  
`./idsLicense`
5. Wenn Sie die Bedingungen der Softwarelizenzvereinbarung akzeptieren, geben Sie 1 ein. Sie können folgende Optionen verwenden:
  - 1: Lizenzvereinbarung akzeptieren
  - 2: Lizenzvereinbarung ablehnen und Installation beenden
  - 3: Lizenzvereinbarung drucken
  - 4: Nicht für IBM geltende Bedingungen in der Lizenzvereinbarung lesen
  - 99: Zur vorherigen Anzeige zurückkehren

Durch das Akzeptieren der Bedingungen in der Lizenzvereinbarung werden an der Installationsposition von IBM Security Directory Server die Datei `LAPID` und der Ordner `license` erstellt. Der Ordner "license" enthält die Lizenzdateien von IBM Security Directory Server in allen unterstützten Sprachen.

**Wichtig:** Ändern oder löschen Sie die Datei LAPID und die Lizenzdateien im Ordner "license" nicht.

6. Führen Sie den folgenden Befehl aus, um ein Paket zu installieren:

**Anmerkung:** Sie müssen die Pakete von IBM Security Directory Server auf einem Solaris-System in einer bestimmten Reihenfolge installieren. Weitere Informationen hierzu finden Sie unter „Pakete für die Installation auf einem Solaris-System“ auf Seite 81.

```
pkgadd -d package_name
```

7. Überprüfen Sie, ob die Installation von IBM Security Directory Server erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

## Ergebnisse

Das Installationsprogramm installiert IBM Security Directory Server auf dem Solaris-System im Verzeichnis /opt/IBM/ldap/V6.3.1. Wenn eine unterstützte Version von IBM DB2 auf dem System installiert wird, aktualisiert der Installationsprozess die Datei ldapdb.properties mit dem Pfadnamen und der Version von DB2.

## Nächste Schritte

Nach der Installation von IBM Security Directory Server müssen Sie die folgende Aktion ausführen:

- Um IBM Security Directory Server als vollständigen Verzeichnisserver zu verwenden, erstellen Sie eine Verzeichnisserverinstanz. Weitere Informationen hierzu finden Sie unter „Standardverzeichnisserverinstanz erstellen“ auf Seite 141.
- Um IBM Security Directory Server als Proxy-Server zu verwenden, erstellen Sie eine Proxy-Server-Instanz. Weitere Informationen hierzu finden Sie unter „Proxy-Server-Instanz mit angepassten Einstellungen erstellen“ auf Seite 150.

---

## Installation mit HP-UX-Dienstprogrammen

Zum Installieren von IBM Security Directory Server auf HP-UX-Systemen können Sie die HP-UX-Befehlszeilendienstprogramme verwenden.

IBM Security Directory Server stellt auf Itanium-Systemen (auf Intel IA64-Prozessoren basierte Server) Nur-Client-Pakete für HP-UX bereit. Weitere Informationen hierzu finden Sie unter „Pakete für die Installation auf einem HP-UX Itanium-System“.

## Pakete für die Installation auf einem HP-UX Itanium-System

Um IBM Security Directory Server als Client auf einem HP-UX-System zu verwenden, müssen Sie die entsprechenden Pakete installieren.

### Pakete für HP-UX-Systeme

IBM Security Directory Server stellt Clientpakete für HP-UX auf Itanium-Systemen (Server auf Basis von Intel IA64-Prozessoren) bereit.

*Tabelle 33. Pakete mit IBM Security Directory Server für HP-UX-Systeme*

IBM Security Directory Server-Pakete	Paketnamen
IBM Directory Server - Basisclient	ids1dap.c1tbase631.depot
IBM Directory Server - 32-Bit-Client	ids1dap.c1t32bit631.depot



Tabelle 33. Pakete mit IBM Security Directory Server für HP-UX-Systeme (Forts.)

IBM Security Directory Server-Pakete	Paketnamen
IBM Directory Server - 64-Bit-Client	idsldap.clt64bit631.depot
IBM Directory Server - Java-Client	idsldap.cltjava631.depot
IBM Directory Server - Lizenz	idsldap.license631.depot

## Paketabhängigkeit

Bei der Installation bestimmter Pakete müssen Sie zuerst die Abhängigkeiten installieren.

Tabelle 34. Pakete und von diesen abhängige Pakete

Paketname	Abhängig von
idsldap.clt32bit631.depot	idsldap.cltbase631.depot
idsldap.clt64bit631.depot	idsldap.cltbase631.depot

## Reihenfolge bei der Installation

Wenn Sie die Pakete auf einem HP-UX-System installieren, muss eine bestimmte Reihenfolge beachtet werden.

**Wichtig:** Wenn Sie Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) verwenden wollen, müssen Sie eine unterstützte Version von IBM Global Security Kit installieren.

Tabelle 35. Installationsreihenfolge für das Client-Feature

32-Bit-Client	64-Bit-Client
1. idsldap.cltbase631.depot	1. idsldap.cltbase631.depot
2. idsldap.clt32bit631.depot	2. idsldap.clt64bit631.depot
3. idsldap.cltjava631.depot	3. idsldap.cltjava631.depot

## Installation mit HP-UX-Dienstprogrammen

Mit dem Befehl **swinstall** können Sie die Installation von IBM Security Directory Server auf einem HP-UX-System ausführen.

### Vorbereitende Schritte

Sie müssen die Installationsmedien von IBM Security Directory Server vorbereiten. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

### Informationen zu diesem Vorgang

Das Installationsprogramm **swinstall** installiert IBM Security Directory Server auf einem HP-UX-System. Wenn eine unterstützte Version von IBM DB2 auf dem System installiert wird, aktualisiert der Installationsprozess die Datei `ldapdb.properties` mit dem Pfadnamen und der Version von DB2.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.

3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis, in dem die Installationsdatei von IBM Security Directory Server gespeichert ist.
4. Führen Sie den folgenden Befehl aus, um die Pakete zu installieren:

```
swinstall -s sds_installable_path/idsldap.cltbody631.depot \*
swinstall -s sds_installable_path/idsldap.cltbody32bit631.depot \*
swinstall -s sds_installable_path/idsldap.cltbody64bit631.depot \*
swinstall -s sds_installable_path/idsldap.cltbodyjava631.depot \*
```
5. Überprüfen Sie, ob die Installation von IBM Security Directory Server erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

## Ergebnisse

Das Installationsprogramm installiert IBM Security Directory Server auf dem HP-UX-System im Verzeichnis `/opt/IBM/ldap/V6.3.1`.

---

## Kapitel 13. Überprüfung der IBM Security Directory Server-Features

Nach dem Installieren, Ändern oder Deinstallieren von IBM Security Directory Server muss überprüft werden, ob die IBM Security Directory Server-Features ordnungsgemäß installiert, geändert oder deinstalliert wurden.

Sie können IBM Installation Manager oder Betriebssystemdienstprogramme verwenden, um zu überprüfen, ob die Installation, Änderung oder Deinstallation erfolgreich war.

---

### IBM Security Directory Server-Features mit IBM Installation Manager überprüfen

Prüfen Sie mit IBM Installation Manager die Features von IBM Security Directory Server und die zusätzlich erforderlichen Produkte, die Sie mit IBM Installation Manager installiert haben.

#### Vorgehensweise

1. Starten Sie IBM Installation Manager.

##### Windows

Klicken Sie im Menü **Start** auf **Alle Programme > IBM Installation Manager > IBM Installation Manager**.

##### AIX und Linux

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein. Ändern Sie den folgenden Standardpfad, wenn IBM Installation Manager an einer anderen Position installiert ist.

```
/opt/IBM/InstallationManager/eclipse/IBMIM
```

2. Klicken Sie auf der Seite **IBM Installation Manager** auf **File > View Installed Packages**.
3. Erweitern Sie auf der Seite **Installed Package** in der Liste **Installed Packages and Fixes** den Eintrag **IBM Security Directory Server**.
4. Klicken Sie in der Liste **Installed Packages and Fixes** auf die Version von IBM Security Directory Server, deren Features Sie anzeigen wollen.
5. Überprüfen Sie im Bereich **Details** die Installation der Features und der zusätzlich erforderlichen Produkte.
6. Klicken Sie auf **Close**, um die Seite **Installed Package** zu schließen.
7. Klicken Sie auf **File > Exit**, um **IBM Installation Manager** zu schließen.

---

### IBM Security Directory Server-Features unter Windows überprüfen

Sie können überprüfen, ob die Installation, Änderung oder Deinstallation von IBM Security Directory Server erfolgreich war, indem Sie die Microsoft Windows-Registrierungsdatenbank prüfen.

#### Informationen zu diesem Vorgang

Microsoft Windows enthält Registrierungseinträge, mit deren Hilfe die Software auf einem Windows-System verfolgt wird. Nach einer erfolgreichen Installation,

Änderung oder Deinstallation von IBM Security Directory Server-Features werden die Registrierungseinträge so geändert, dass die neueste Aktualisierung auf dem System aufgezeichnet wird. Ein Beispiel der Registrierungseinträge wird nach einer erfolgreichen Installation der IBM Security Directory Server-Features angezeigt. Wenn Sie IBM Security Directory Server-Features ändern oder deinstallieren, werden die Registrierungseinträge, die die Features verfolgen, geändert und zeigen dann den neuesten Status an. Die angezeigten Registrierungseinträge beziehen sich auf Microsoft Windows in einer AMD64/EM64T-Architektur.

## Vorgehensweise

1. Melden Sie sich an dem Windows-System mit Administratorrechten an.
2. Öffnen Sie die Eingabeaufforderung und führen Sie den folgenden Befehl aus:  
regedit
3. Klicken Sie im Fenster für den Registrierungseditor auf **My Computer > HKEY\_LOCAL\_MACHINE > SOFTWARE > Wow6432NODE > IBM > IDSLDAP > 6.3.1**.

**Anmerkung:** Erweitern Sie zur Überprüfung der Installation von IBM Security Directory Server auf Microsoft Windows-Systemen in einer Intel x86-Architektur (IA32) **My Computer > HKEY\_LOCAL\_MACHINE > SOFTWARE > IBM > IDSLDAP > 6.3.1**.

My Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1 zeigt die übergeordneten Versionen der auf dem System installierten IBM Security Directory Server-Features an.

BaseServerMajorVersion	6.3.1
BitMode	64
ClientMajorVersion	6.3.1
JavaClientMajorVersion	6.3.1
LDAPHome	<i>installation_location</i>
ProxyServerMajorVersion	6.3.1
ServerMajorVersion	6.3.1
WebadminMajorVersion	6.3.1
WebSphereAppSrvMajorVersion	7.0

Die untergeordneten Versionen der IBM Security Directory Server-Features, die auf dem System installiert sind, werden unter My Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1 angezeigt. Beispiel:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\BaseServer\  
BaseServerMinorVersion 1.0

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Client\  
ClientMinorVersion 1.0

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\JavaClient\  
JavaClientMinorVersion 1.0

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\ProxyServer\  
ProxyServerMinorVersion 1.0

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Server\  
ServerMinorVersion 1.0

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Webadmin\  
WebadminMinorVersion 1.0

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\WebSphereAppSrv\  
WebSphereAppSrvMinorVersion 0.25

4. Klicken Sie auf **File > Exit**, um das Fenster für den Registrierungseditor zu schließen.

---

## IBM Security Directory Server-Pakete überprüfen

Sie können überprüfen, ob die Installation von IBM Security Directory Server erfolgreich war, indem Sie das System auf IBM Security Directory Server-Pakete prüfen.

### Informationen zu diesem Vorgang

Sie müssen nach der Installation von IBM Security Directory Server sicherstellen, dass die Pakete die erforderliche Version aufweisen. Sie können die Versionsnummer von IBM Security Directory Server-Paketten abfragen.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie eine Eingabeaufforderung und führen Sie den folgenden Befehl aus:

Betriebssystem	Befehl zur Paketabfrage:
AIX	<code>lsllpp -l 'idsldap*'</code>
Linux	<code>rpm -qa   grep -i idsldap</code>
Solaris	<code>pkginfo   grep IDS1 pkgparam package_name VERSION</code>
HP-UX	<code>swlist   grep -i idsldap</code>

### Ergebnisse

Der Befehl listet die IBM Security Directory Server-Pakete auf, die auf dem System installiert sind.

---

## Version des Webverwaltungstools überprüfen

Sie müssen die Version des **Webverwaltungstools** überprüfen, um sicherzustellen, ob die Installation oder das Upgrade des **Webverwaltungstools** erfolgreich war.

### Vorgehensweise

1. Melden Sie sich mit Administratorrechten an.
2. Wechseln Sie in das Verzeichnis `ds_install_location/idstools`. `ds_install_location` steht für die Installationsposition von IBM Security Directory Server. Nachstehend sind die Standardpositionen auf verschiedenen Betriebssystemen aufgeführt:

*Tabelle 36. Standardinstallationsposition von IBM Security Directory Server auf den verschiedenen Betriebssystemen*

Betriebssysteme	Standardinstallationspositionen:
Microsoft Windows	<code>c:\Program Files\IBM\ldap\V6.3.1</code>
AIX und Solaris	<code>/opt/IBM/ldap/V6.3.1</code>
Linux	<code>/opt/ibm/ldap/V6.3.1</code>

3. Führen Sie den folgenden Befehl aus:

Betriebssysteme	Befehl:
Microsoft Windows	deploy_IDSWebApp.bat -v
AIX, Linux und Solaris	deploy_IDSWebApp -v

Der Befehl zeigt die folgenden Informationen an:

- Versions- und Datumswerte des Befehls **deploy\_IDSWebApp**
- Versions- und Datumswerte der installierten Datei IDSWebApp.war
- Versions- und Datumswerte der derzeit implementierten Datei IDSWebApp.war

## Nächste Schritte

Sie müssen die folgenden Werte prüfen:

1. Unterscheiden sich die Versions- und Datumswerte der installierten Datei IDSWebApp.war von den Versions- und Datumswerte der derzeit implementierten Datei IDSWebApp.war?
2. Wenn sich die Werte unterscheiden, implementieren Sie das neueste **Webverwaltungstool** auf dem Webanwendungsserver.

---

## Installation von IBM Global Security Kit unter Windows überprüfen

Überprüfen Sie den Status der Installation von IBM Global Security Kit (GSKit), um sicherzustellen, dass die Installation unter Windows erfolgreich war.

### Vorgehensweise

1. Öffnen Sie die Datei gskitinst.log.

Betriebssystem	Standardpfad:
Windows	C:\Program Files\IBM\ldap\V6.3.1\var

2. Überprüfen Sie, ob das folgende Verzeichnis erstellt wird: C:\Program Files\IBM\gsk8
3. Überprüfen Sie, ob die Datei gskitinst.log den Wert EXIT 0 enthält. Wenn die Installation von IBM Global Security Kit erfolgreich war, lautet der Wert "0". Andernfalls wird ein Wert ungleich null festgelegt.
4. Optional: Wenn die Installation von IBM Global Security Kit nicht erfolgreich war, werden die Fehlerdetails in der Datei C:\Program Files\IBM\ldap\V6.3.1\var\gskitinsterr.log gespeichert.

---

## Installation von IBM Global Security Kit unter AIX, Linux, Solaris und HP-UX überprüfen

Überprüfen Sie die Installation von IBM Global Security Kit (GSKit), um sicherzustellen, dass die Installation erfolgreich war.

### Informationen zu diesem Vorgang

Sie müssen nach der Installation von IBM Global Security Kit sicherstellen, dass die Pakete die erforderliche Version aufweisen. Sie können die Versionsnummer von IBM Global Security Kit abfragen.

## Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie eine Eingabeaufforderung und führen Sie den folgenden Befehl aus:

Betriebssystem	Befehl:
AIX	<code>lslpp -al   grep -i gsk</code>
Linux	<code>rpm -qa   grep -i gsk</code>
Solaris	<code>pkginfo   grep gsk</code> <code>pkgparam package_name VERSION</code>
HP-UX	<code>swlist   grep -i gsk</code>





---

## Kapitel 14. Upgrades von Instanzen von Vorgängerversionen durchführen

Um eine vorhandene Instanz in eine funktionelle Instanz eines aktuellen Release zu konvertieren und mit den vorhandenen Konfigurationsdateien fortzufahren, müssen Sie für eine Instanz ein Upgrade durchführen.

Beim Upgradeprozess werden Änderungen an den Schemadefinitionen, Änderungen an Konfigurationsdateien und die Daten einer Verzeichnisserverinstanz beibehalten.

Zum Durchführen von Upgrades von Vorgängerversionen müssen Sie den folgenden Prozess durchführen:

1. Installieren Sie IBM Security Directory Server.
2. Führen Sie ein Upgrade für eine Instanz einer Vorgängerversion durch.

Server und Clients von IBM Security Directory Server Version 6.3.1 können mit Servern und Clients der Versionen 6.0, 6.1, 6.2 und 6.3 koexistieren.

Verzeichnisserverinstanzen der folgenden Versionen können direkt auf IBM Security Directory Server Version 6.3.1 aktualisiert werden:

- IBM Security Directory Server Version 6.3
- IBM Security Directory Server Version 6.2
- IBM Security Directory Server Version 6.1

**Wichtig:** Direkte Upgrades von Instanzen von IBM Security Directory Server Version 6.0 auf IBM Security Directory Server Version 6.3.1 werden nicht unterstützt. Für Instanzen der Version 6.0 können Upgrades auf Version 6.1, 6.2 oder 6.3 und anschließend auf Version 6.3.1 durchgeführt werden.

Sie können folgendermaßen Upgrades von Instanzen von Vorgängerversionen durchführen:

- Durch Aktualisieren einer vorhandenen Instanz auf einem lokalen Computer mit IBM Security Directory Server **Instance Administration Tool (idsxinst)** oder dem Befehl **idsimigr**. Sie müssen die Verzeichnisserverinstanz, für die Sie ein Upgrade durchführen möchten, nicht entfernen. Bei vollständigen Verzeichnisserverinstanzen darf die Datenbank nicht dekonfiguriert werden. Upgrades werden nicht unterstützt, wenn die Verzeichnisserverinstanz entfernt oder dessen Datenbank dekonfiguriert wurde.
- Durch Aktualisieren einer Instanz auf einem fernen Computer mit den Befehlen **migbkup** und **idsimigr**. Weitere Informationen hierzu finden Sie unter „Upgrade einer fernen Instanz einer Vorgängerversion mit dem Befehl **idsimigr** durchführen“ auf Seite 98.

**Achtung:** Um eine Instanz nach Upgradefehlern wiederherzustellen zu können, müssen das Schema, die Konfigurationsdateien und die Datenbank gesichert werden.

## DB2-Datenbankupgrade

Wenn Sie ein Upgrade einer Instanz durchführen, wird dessen zugeordnete DB2-Datenbank ebenfalls aktualisiert, wenn die DB2-Version niedriger ist als die von IBM Security Directory Server Version 6.3.1 unterstützte. Der Befehl **idsdbmigr** wird intern zum Aktualisieren der DB2-Datenbank durchgeführt.

**Wichtig:** Direkte Upgrades einer mit DB2 Version 9.1 konfigurierten Verzeichnisserverinstanz auf eine Instanz mit DB2 Version 10.1.0.2 oder höher werden nicht unterstützt. Sie können eine mit DB2 Version 9.1 konfigurierte Instanz auf eine Instanz mit DB2 Version 10.1.0.2 oder höher wie folgt aktualisieren:

- Aktualisieren Sie die Instanz mit DB2 Version 9.1 zuerst auf eine Instanz mit DB2 Version 9.5 und dann auf eine Instanz mit DB2 Version 10.1.0.2 oder höher.
- Aktualisieren Sie die Instanz mit DB2 Version 9.1 zuerst auf eine Instanz mit DB2 Version 9.7 und dann auf eine Instanz mit DB2 Version 10.1.0.2 oder höher.

## Clientinstallationsupgrade

Wenn Sie Nur-Client-Features mit dem IBM Security Directory Server-Clientinstallationsprogramm installiert haben, muss kein Upgrade durchgeführt werden. Clients von Version 6.0, 6.1, 6.2 und 6.3 können mit Servern und Clients von Version 6.3.1 koexistieren.

---

## Umgebung vor dem Upgrade einer Instanz einrichten

Vor dem Upgrade einer vorhandenen Instanz müssen Sie die Umgebung des Verzeichnisservers einrichten.

### Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um die Umgebung einzurichten:

- Greifen Sie auf die Installationsmedien von IBM Security Directory Server zu.
- Installieren Sie IBM Security Directory Server Version 6.3.1. Siehe „Installation starten“ auf Seite 29.
- Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.

### Vorgehensweise

1. Stellen Sie sicher, dass das Betriebssystem, auf dem sich die Instanz befindet, für die ein Upgrade durchgeführt werden soll, von IBM Security Directory Server Version 6.3.1 unterstützt wird.
2. Stellen Sie sicher, dass die Instanz einer Vorgängerversion, für die ein Upgrade durchgeführt werden soll, erfolgreich startet. Wenn Sie ein Upgrade für eine Verzeichnisserverinstanz durchführen wollen, müssen Sie die Datenbank konfigurieren, sofern noch nicht geschehen.

**Achtung:** Das Upgrade eines Proxy- oder Verzeichnisservers wird nicht unterstützt, wenn der Server nicht erfolgreich startet.

3. Führen Sie eine Offlinesicherung der Instanz aus, für die Sie ein Upgrade durchführen wollen. Sichern Sie bei einer Verzeichnisserverinstanz die DB2-Datenbanken und die DB2-Einstellungen. Weitere Informationen finden Sie in der Veröffentlichung *Command Reference* unter dem Befehl **idsdbback**.
4. Führen Sie den Befehl **migbkup** aus, um die Schema- und Konfigurationsdateien zu sichern:

Betriebssystem	Befehl:
Microsoft Windows	<b>migbkup.bat</b> drive_name\idsldap-instance_name backup_directory
AIX, Linux und Solaris	<b>migbkup</b> user_home_dir/idsldap-instance_name backup_directory

Der Befehl **migbkup** befindet sich im Unterverzeichnis `tools` der Installationsmedien von IBM Security Directory Server. Falls Sie die Installation von IBM Security Directory Server ausgeführt haben, befindet sich der Befehl **migbkup** an der Installationsposition von IBM Security Directory Server im Ordner `sbin`. Das folgende Verzeichnis ist die Standardinstallationsposition auf den verschiedenen Betriebssystemen:

#### Microsoft Windows

C:\Program Files\IBM\ldap\V6.3.1

#### AIX und Solaris

/opt/IBM/ldap/V6.3.1

**Linux** /opt/ibm/ldap/V6.3.1

Mit dem Befehl **migbkup** werden die folgenden Dateien gesichert:

- `ibmslapd.conf`
- `V3.config.at`
- `V3.config.oc`
- `V3.ibm.at`
- `V3.ibm.oc`
- `V3.system.at`
- `V3.system.oc`
- `V3.user.at`
- `V3.user.oc`
- `V3.modifiedschema`
- `V3.ldapsyntaxes`
- `V3.matchingrules`
- `ibmslapdcfg.ksf`
- `ibmslapddir.ksf`
- `perftune_stat.log`
- `perftune_input.conf`
- `ibmdiradmService.cmd` (für Windows)
- `ibmslapdService.cmd` (für Windows)

Mit dem Befehl **migbkup** werden die folgenden Dateien erstellt:

- `db2info` enthält den Pfadnamen und Informationen zu der Version von DB2, die von der Verzeichnisserverinstanz verwendet wird. Der Befehl **idsimigr** oder das **Instance Administration Tool** führt mithilfe dieser Datei ein Upgrade der DB2-Instanz- und -Datenbank durch, wenn Sie ein Upgrade einer Verzeichnisserverinstanz durchführen. Für eine Proxy-Server-Instanz ist diese Datei nicht verfügbar.
  - `platforminfo` enthält die Informationen zum Betriebssystem und Prozesstyp.
5. Wenn Sie die Datei `V3.modifiedschema` einer Instanz für ein Upgrade manuell geändert haben, darf die Datei keine doppelten Objektkennungen (OIDs) für Objektklassen oder Attribute enthalten. Wenn die Datei doppelte OIDs enthält, werden diese beim Upgrade nicht beibehalten. Wenn Schemadateien doppelte

OIDs enthalten, wird die OID in `V3.modifiedschema` beibehalten. Wenn Attribute oder Objektklassen in den Schemadateien fehlen, schlägt möglicherweise der Start des Verwaltungsservers und des Prozesses `idslapd` fehl. In diesem Fall müssen Sie vor dem Start der Server die fehlenden Attribute oder Objektklassen manuell zu den Schemadateien hinzufügen.

6. Wenn Sie die Instanz mit angepassten Schemadateien konfiguriert haben, kopieren Sie die Dateien manuell in das Sicherungsverzeichnis. Beim Sichern der Schema- und Konfigurationsdateien sichert der Befehl **migbkup** die angepassten Schemadateien. Diese Schemadateien werden jedoch möglicherweise nicht verwendet, wenn Sie ein Upgrade der Instanz durchführen.

## Nächste Schritte

Führen Sie nach dem Einrichten der Umgebung den Befehl **idsimigr** oder das **Instance Administration Tool** aus, um ein Upgrade einer Instanz von einer Vorgängerversion durchzuführen. Verwenden Sie dabei eine der folgenden Methoden:

- „Upgrade einer Instanz einer Vorgängerversion mit dem Befehl **idsimigr** durchführen“
- „Upgrade einer Instanz einer Vorgängerversion mit dem **Instance Administration Tool** durchführen“ auf Seite 156

---

## Upgrade einer Instanz einer Vorgängerversion mit dem Befehl **idsimigr** durchführen

Führen Sie mit dem Befehl **idsimigr** ein Upgrade einer Verzeichnisserverinstanz oder Proxy-Server-Instanz einer Vorgängerversion auf die aktuelle Version durch.

### Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um mit dem Befehl **idsimigr** ein Upgrade einer Instanz durchzuführen:

- Installieren Sie IBM Security Directory Server. Siehe „Installation starten“ auf Seite 29.
- Richten Sie vor dem Upgrade einer Instanz die Umgebung ein. Siehe „Umgebung vor dem Upgrade einer Instanz einrichten“ auf Seite 94.
- Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.

Sie können das Upgrade einer auf dem Computer vorhandenen Instanz auch mit dem **Instance Administration Tool** durchführen. Weitere Informationen hierzu finden Sie unter „Upgrade einer Instanz einer Vorgängerversion mit dem **Instance Administration Tool** durchführen“ auf Seite 156.

### Informationen zu diesem Vorgang

Nach dem Upgrade einer Instanz einer Vorgängerversion wird die Instanz in eine vollständig funktionsfähige Instanz der aktuellen Version von IBM Security Directory Server konvertiert.

### Vorgehensweise

1. Öffnen Sie die Eingabeaufforderung.
2. Ändern Sie das aktuelle Arbeitsverzeichnis in `sbin`. Nachstehend sind die Standardpositionen auf verschiedenen Betriebssystemen aufgeführt:

### Microsoft Windows

C:\Program Files\IBM\ldap\V6.3.1\sbin

### AIX und Solaris

/opt/IBM/ldap/V6.3.1/sbin

**Linux** /opt/ibm/ldap/V6.3.1/sbin

3. Stoppen Sie den Prozess `ibmslapd` und den Verwaltungsserver der Instanz, für die Sie ein Upgrade durchführen wollen.  
`ibmslapd -I instance_name -k`  
`ibmdiradm -I instance_name -k`
4. Führen Sie keine Deinstallation der Produktversion von IBM Security Directory Server aus, die der Instanz zugeordnet ist, für die Sie ein Upgrade durchführen wollen.
5. Führen Sie den Befehl `idsimigr` aus, um ein Upgrade der Instanz von einer Vorgängerversion auf die aktuelle Version von IBM Security Directory Server durchzuführen.  
`idsimigr -I instance_name`
6. Starten Sie den Prozess `ibmslapd` und den Verwaltungsserver der Instanz.  
`ibmslapd -I instance_name -n`  
`ibmdiradm -I instance_name`
7. Führen Sie eine Offlinesicherung der Instanz durch. Weitere Informationen finden Sie unter „Verzeichnisserverbackup“ auf Seite 198.

---

## Upgrades von Instanzen von Vorgängerversionen auf einem anderen Computer durchführen

Sie können für eine vorhandene Instanz einer Vorgängerversion, die sich auf einem Computer befindet, ein Upgrade auf eine neuere Version, die sich auf einem anderen Computer befindet, durchführen.

Möglicherweise müssen Sie aus einem der folgenden Gründe über Fernzugriff ein Upgrade einer vorhandenen Instanz durchführen.

- Das Betriebssystem auf dem Computer, auf dem sich eine Instanz einer Vorgängerversion befindet, wird möglicherweise nicht von IBM Security Directory Server Version 6.3.1 unterstützt. In diesem Fall sollten Sie kein Upgrade durchführen und das Betriebssystem nicht aktualisieren.
- Sie möchten IBM Security Directory Server Version 6.3.1 auf einem Computer mit einem anderen Betriebssystem als dem installieren, auf dem eine Vorgängerversion installiert ist. Sie möchten jedoch eine Instanz mit den Informationen der vorhandenen Instanz einer Vorgängerversion erstellen. Wenn sich beispielsweise eine vorhandene Instanz einer Vorgängerversion auf einem AMD64/EM64T-Linux-System befindet, Sie aber die Serverversion 6.3.1 auf einem AIX-System verwenden möchten, müssen die beiden Betriebssysteme denselben Endian-Typ besitzen. Wenn auf dem ersten Computer Little Endian verwendet wird, muss auf dem zweiten System ebenfalls Little Endian verwendet werden. Der Endian-Typ betrifft die Anordnung der zum Darstellen von Daten im Speicher verwendeten Bits. Wenn die Betriebssysteme nicht denselben Endian-Typ besitzen, werden Upgrades von Instanzen nicht unterstützt.

Die Prozedur für Upgrades über Fernzugriff ist ähnlich wie die Prozedur für Upgrades auf demselben Computer. Dabei müssen Sie jedoch die Sicherungsdateien vom Computer auf einen Computer kopieren, auf dem IBM Security Directory Server Version 6.3.1 installiert wird.

**Anmerkung:** Wenn Sie für eine ferne Instanz von einem Computer ein Upgrade durchführen, der an Replikation teilnimmt, führen Sie die folgenden Aktionen durch:

- Aktivieren Sie die Replikation mit dem Quellsystem als Lieferant.
- Aktivieren Sie die Replikation mit dem Zielsystem als Konsument.

Durch die Replikation wird sichergestellt, dass die Updates in die Warteschlange gestellt werden und repliziert werden können, wenn das Zielsystem online geht. Replikation muss aktiviert werden, bevor die Sicherung einer Instanz auf dem Quellsystem erstellt wird.

## Unterstützte Betriebssysteme für Upgrades einer fernen Instanz

Um für eine ferne Instanz ein Upgrade auf einem geeigneten Zielbetriebssystem durchzuführen, müssen Sie die Betriebssysteme angeben, die die Quelle und das Ziel für eine Instanz darstellen.

Tabelle 37. Unterstützte Quellen- und Zielbetriebssysteme für Upgrades ferner Instanzen

Betriebssystem: Quellsystem (IBM Security Directory Server 6.3 oder früher) ↓	Betriebssystem: Zielsystem (IBM Security Directory Server Version 6.3.1)								
	Intel-32-Bit-Windows	AMD64/EM64T Windows	System x Linux (32-Bit)	AMD64/EM64T-Linux	System i- und System p-Linux	System z-Linux	AIX	Solaris SPARC	Solaris X64
Intel 32-Bit-Windows	✓	✓	✓	✓					✓
AMD/EM64T-Windows	✓	✓	✓	✓					✓
System x Linux (32-Bit)	✓	✓	✓	✓					✓
AMD/EM64T Linux	✓	✓	✓	✓					✓
System i- und System p-Linux					✓	✓	✓	✓	
System z-Linux					✓	✓	✓	✓	
AIX					✓	✓	✓	✓	
Solaris SPARC					✓	✓	✓	✓	
Solaris X64	✓	✓	✓	✓					✓

## Upgrade einer fernen Instanz einer Vorgängerversion mit dem Befehl `idsimigr` durchführen

Führen Sie mit dem Befehl `idsimigr` mit dem Parameter `-u` ein Upgrade einer fernen Verzeichnisserverinstanz oder Proxy-Server-Instanz einer Vorgängerversion auf Version 6.3.1 durch.

## Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um mit dem Befehl **idsimigr** mit dem Parameter **-u** ein Upgrade einer Instanz durchzuführen:

- Richten Sie vor dem Upgrade einer Instanz die Umgebung ein. Siehe „Umgebung vor dem Upgrade einer Instanz einrichten“ auf Seite 94.
- Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.

Sie können ein Upgrade einer fernen Instanz auch mit Sicherungsdateien durchführen, indem Sie das **Instance Administration Tool** verwenden. Weitere Informationen hierzu finden Sie unter „Upgrade einer fernen Instanz einer Vorgängerversion mit dem **Instance Administration Tool** durchführen“ auf Seite 157.

## Informationen zu diesem Vorgang

Nachdem Sie den Upgradeprozess ausgeführt haben, erstellt der Befehl **idsimigr** mit den Angaben von der fernen Instanz eine Instanz der Version 6.3.1 auf dem Computer.

## Vorgehensweise

1. Sichern Sie die Datenbank einer Verzeichnisserverinstanz, die sich auf einem fernen Computer befindet, mit dem Befehl **idsdb2ldif**.

**Wichtig:** Sichern Sie die Datenbank nicht, wenn Sie ein Upgrade für eine Proxy-Server-Instanz durchführen. Ein Proxy-Server enthält keine ihm zugeordnete Datenbank.

```
idsdb2ldif -I instance_name -o inst_out.ldif
```

Weitere Informationen zum Befehl **idsdb2ldif** finden Sie in der Veröffentlichung *Command Reference*.

2. Installieren Sie IBM Security Directory Server auf einem Computer, auf dem Sie das Upgrade der fernen Instanz durchführen wollen. Siehe „Installation starten“ auf Seite 29.
3. Führen Sie den Befehl **migbkup** der Version aus, auf die Sie das Upgrade durchführen wollen, um die Schema- und Konfigurationsdateien der fernen Instanz zu sichern:

Betriebssystem	Befehl:
Microsoft Windows	<b>migbkup.bat</b> drive_name\idsslapped-instance_name backup_directory
AIX, Linux und Solaris	<b>migbkup</b> user_home_dir/idsslapped-instance_name backup_directory

Der Befehl **migbkup** befindet sich im Unterverzeichnis `tools` der Installationsmedien von IBM Security Directory Server.

4. Kopieren Sie das Sicherungsverzeichnis `backup_directory`, das Sie mit **migbkup** erstellt haben, von dem fernen Computer auf den Computer mit IBM Security Directory Server.
5. Optional: Kopieren Sie die Datenbanksicherungsdatei `inst_out.ldif` von dem fernen Computer auf den Computer mit IBM Security Directory Server.
6. Führen Sie den Befehl **idsimigr** mit dem Parameter **-u** aus, um eine Instanz mit den Sicherungsdaten der fernen Instanz zu erstellen.

```
idsimigr -u backup_directory
```

7. Konfigurieren Sie eine Datenbank, ein Suffix sowie einen Administrator-DN und ein Kennwort für die Verzeichnisserverinstanz.

**Wichtig:** Führen Sie den Befehl **idscfgdb** zum Konfigurieren einer Datenbank nicht aus, wenn Sie ein Upgrade für eine Proxy-Server-Instanz durchführen.

```
idscfgdb -I instance_name -a db_admin_id -w db_admin_pwd -t db_name  
-l db_location  
idscfgsuf -I instance_name -s suffix  
idsdnpw -I instance_name -u admin_DN -p admin_PWD
```

8. Optional: Führen Sie den Befehl **idsldif2db** aus, um die Datenbanksicherungsdatei `inst_out.ldif` in die Verzeichnisserverinstanz zu importieren, für die ein Upgrade durchgeführt wurde.
9. Starten Sie den Prozess `ibmslapd` und den Verwaltungsserver der Instanz.  

```
ibmslapd -I instance_name -n  
ibmdiradm -I instance_name
```
10. Führen Sie eine Sicherung der Instanz durch. Weitere Informationen hierzu finden Sie unter „Verzeichnisserverbackup“ auf Seite 198.

---

## Links zu Client- und Serverdienstprogrammen

Zum Setzen von Links auf die Befehlszeilendienstprogramme und Bibliotheken des Verzeichnisseservers können Sie den Befehl **idslink** verwenden.

Nach der Installation von IBM Security Directory Server können Sie Links zu Client- und Serverdienstprogrammen setzen. Diese Links werden während der Installation nicht automatisch gesetzt.

Wenn Sie Links zu Dienstprogrammen einer Vorgängerversion von IBM Security Directory Server konfiguriert haben, bleiben diese Links bestehen, bis sie geändert werden. Verwenden Sie den Befehl `idsrmlink`, um Links zu entfernen, die mit dem Befehl **idslink** erstellt wurden.

Zum Setzen von Links auf Befehlszeilendienstprogramme wie **idsldapmodify** und **idsldapadd** oder auf Bibliotheken wie `libibmdap.so` können Sie den Befehl **idslink** verwenden. Diese Links verweisen auf die Position, in der die Dienstprogramme und Bibliotheken von IBM Security Directory Server gespeichert sind.

Weitere Informationen zu den Befehlen **idslink** und **idsrmlink** finden Sie in der *Befehlsreferenz*.



---

## Kapitel 15. Migration von Daten und Lösungen von einer Instanz einer Vorgängerversion

Sie können Verzeichnisdaten und/oder Lösungen, die Sie mit einer Instanz einer Vorgängerversion für die Verwendung einer Instanz mit Version 6.3.1 konfiguriert haben, migrieren.

### Migration von DB2-Daten von IBM DB2 Enterprise Server Edition (ESE) auf IBM DB2 Workspace Server Edition (WSE)

Unter System x Linux (Intel 32-Bit-Architektur) wird IBM DB2 ESE Version 9.7 oder höher nicht unterstützt. Unter System x Linux verwendet IBM Security Directory Server IBM DB2 WSE Version 9.7, Fixpack 6 oder höher zum Erstellen und Konfigurieren der Datenbank.

Wenn Sie eine Instanz von Version 6.1 oder 6.2 mit Daten auf Version 6.3.1 migrieren, müssen Sie möglicherweise über Fernzugriff ein Upgrade durchführen. Sie können eine Instanz mit Version 6.3 mit DB2 WSE Version 9.7 oder höher auf Version 6.3.1 mit DB2 WSE Version 9.7 oder höher aktualisieren. Ein direktes Upgrade von einer Instanz mit Version 6.1 oder 6.2 mit DB2 ESE Version 9.1 oder höher auf eine Instanz mit Version 6.3.1 mit DB2 WSE Version 9.7 oder höher unter System x Linux schlägt möglicherweise fehl. Weitere Informationen zum Migrieren einer DB2-ESE-Datenbank auf DB2 WSE finden Sie im Kapitel „Instanz mit DB2 ESE-Datenbank auf eine Instanz mit DB2 WSE-Datenbank migrieren“ auf Seite 102.

### Migration von Verzeichnisserverlösungen, die auf IBM Security Directory Integrator basieren

Für die Verwendung von Lösungen, die mit einer Vorgängerversion einer Instanz mit Version 6.3.1 konfiguriert wurden, müssen diese Lösungen migriert werden.

Die folgenden Lösungen werden unterstützt:

- Protokollverwaltungstool
- SNMP (Simple Network Management Protocol)
- Active Directory-Synchronisation

Weitere Informationen zu den Verzeichnisserverlösungen finden Sie in den Abschnitten unter *Verwaltung* in der IBM Security Directory Server-Produktdokumentation.

Damit die Lösung funktionieren kann, muss auf Ihrem Computer IBM Security Directory Integrator Version 7.1 installiert sein. Weitere Informationen zur Installation und Verwaltung von IBM Security Directory Integrator finden Sie in der Produktdokumentation im Abschnitt *Installation und Verwaltung* unter <http://www-01.ibm.com/support/knowledgecenter/SSCQGF/welcome>.

Wenn der Installationspfad von IBM Security Directory Integrator vom Standardinstallationspfad abweicht, legen Sie für die Variable *IDS\_LDAP\_TDI\_HOME* die Installationsposition von IBM Security Directory Integrator fest. Die folgenden Installationspfade sind bei den verschiedenen Betriebssystemen die Standardpfade für IBM Security Directory Integrator Version 7.1:

#### AIX, Linux und Solaris

/opt/IBM/TDI/V7.1

---

## Instanz mit DB2 ESE-Datenbank auf eine Instanz mit DB2 WSE-Datenbank migrieren

Für ein Upgrade einer Instanz der Version 6.1 oder 6.2 mit DB2 ESE auf eine Instanz der Version 6.3.1 mit DB2 WSE müssen Sie die Daten von der DB2 ESE-Datenbank in die DB2 WSE-Datenbank migrieren.

### Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um Daten von einer Instanz mit einer Vorgängerversion auf eine Instanz der Version 6.3.1 zu migrieren:

- Installieren Sie IBM Security Directory Server Version 6.3.1 mit IBM DB2 WSE. Siehe „Installation starten“ auf Seite 29.
- Richten Sie vor dem Upgrade einer Instanz die Umgebung ein. Siehe „Umgebung vor dem Upgrade einer Instanz einrichten“ auf Seite 94.
- Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.

### Vorgehensweise

1. Stoppen Sie die Verzeichnisserverinstanz, deren Verzeichnisdaten Sie migrieren wollen.
2. Führen Sie den im Lieferumfang von IBM Security Directory Server Version 6.3.1 enthaltenen Befehl **migbkup** aus, um die Instanz zu sichern. Siehe „Umgebung vor dem Upgrade einer Instanz einrichten“ auf Seite 94. Weitere Informationen zum Befehl **migbkup** finden Sie in der Veröffentlichung *Command Reference*.
3. Sichern Sie die Datenbank der Verzeichnisserverinstanz, deren Daten Sie migrieren wollen. Führen Sie die folgenden Schritte aus, um die Datenbank dsrdbm01 einer Instanz zu sichern:
  - a. Stellen Sie den Benutzerkontext auf den DB2-Instanzeigner um.

```
su - dsrdbm01
```
  - b. Führen Sie den Befehl db2profile für den Benutzer aus.

```
sqllib/db2profile
```
  - c. Sichern Sie die DB2-Datenbank der Instanz.

```
db2 backup database dsrdbm01 to database_backup_directory
```

Der Datenbankeigner muss Lese-, Schreib- und Ausführungsberechtigungen für das Verzeichnis für die Datenbanksicherung database\_backup\_directory besitzen.
  - d. Sichern Sie die Änderungsprotokolldatenbank, falls sie für die Verzeichnisserverinstanz konfiguriert ist.

```
db2 backup db ldaplog to changelog_backup_directory
```

Der Datenbankeigner muss Lese-, Schreib- und Ausführungsberechtigungen für das Verzeichnis für das Änderungsprotokoll changelog\_backup\_directory besitzen.
  - e. Führen Sie den Befehl exit aus, um den Benutzerkontext zu beenden.

4. Löschen Sie die Verzeichnisserverinstanz mit der Datenbank. Weitere Informationen zum Löschen einer Instanz mit der Datenbank finden Sie unter „Instanz mit dem Befehlszeilendienstprogramm löschen“ auf Seite 173.
5. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server Version 6.3.1.
6. Führen Sie den Befehl **idsimigr** im folgenden Format aus, um mit dem Instanzsicherungsverzeichnis ein Upgrade über Fernzugriff für eine Instanz durchzuführen.
 

```
idsimigr -I dsrdbm01 -u instance_backup_location -l instance_home_directory -n
```
7. Führen Sie den Befehl **idscfgdb** im folgenden Format aus, um die Instanz zu konfigurieren:
 

```
idscfgdb -I dsrdbm01 -a database_owner -w passwd
-t dsrdbm01 -l instance_home_directory -n
```
8. Falls die Änderungsprotokolldatenbank für die migrierte Instanz konfiguriert wurde, konfigurieren Sie die Änderungsprotokolldatenbank für die Instanz.
 

```
idscfgchglg -I dsrdbm01 -n
```
9. Stellen Sie die Datenbank aus dem Sicherungsbild wieder her. Führen Sie die folgenden Schritte aus, um die Datenbank `dsrdbm01` einer Instanz wiederherzustellen.
  - a. Stellen Sie den Benutzerkontext auf den DB2-Instanzeigner um.
 

```
su - dsrdbm01
```
  - b. Stellen Sie die DB2-Datenbank der Instanz wieder her.
 

```
db2 restore database dsrdbm01 from database_backup_directory replace existing
```
  - c. Stellen Sie die Änderungsprotokolldatenbank wieder her, falls sie für die Verzeichnisserverinstanz konfiguriert ist.
 

```
db2 restore db ldaplog from changelog_backup_directory
```
  - d. Führen Sie den Befehl `exit` aus, um den Benutzerkontext zu beenden.
10. Führen Sie die folgenden Befehle aus, um die wiederhergestellte Datenbank zu katalogisieren:
 

```
su - dsrdbm01
db2 uncatalog database dsrdbm01
db2 catalog database dsrdbm01 as dsrdbm01 authentication server
exit
```
11. Führen Sie die folgenden Befehle aus, um die wiederhergestellte Änderungsprotokolldatenbank zu katalogisieren:
 

```
su - dsrdbm01
db2 uncatalog database ldaplog
db2 catalog database ldaplog as ldaplog authentication server
exit
```
12. Starten Sie den Verzeichnisserver und den Verwaltungsserver.
 

```
ibmslapd -I dsrdbm01 -n -t
ibmdiradm -I dsrdbm01
```

---

## Protokollverwaltungslösung migrieren

Sie können eine mit einer Instanz einer Vorgängerversion konfigurierte Protokollverwaltungslösung auf eine Instanz der Version 6.3.1 migrieren.

### Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um die Protokollverwaltungslösung von einer Instanz mit einer Vorgängerversion auf eine Instanz der Version 6.3.1 zu migrieren:

- Installieren Sie IBM Security Directory Server Version 6.3.1. Siehe „Installation starten“ auf Seite 29.
- Installieren Sie IBM Security Directory Integrator Version 7.1, sofern noch nicht auf dem Computer installiert.
- Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.

## Vorgehensweise

1. Sichern Sie die Datei `solution.properties`, die sich im Verzeichnis `DS_instance_home/idsslapd-instance_name/etc/logmgt` ihrer vorhandenen Verzeichnisserverinstanz befindet.
2. Führen Sie ein Upgrade der Vorgängerversion der Instanz auf Version 6.3.1 durch. Weitere Informationen finden Sie in Kapitel 14, „Upgrades von Instanzen von Vorgängerversionen durchführen“, auf Seite 93.
3. Entfernen Sie alle Dateien und Unterverzeichnisse im Verzeichnis `DS_instance_home/idsslapd-instance_name/etc/logmgt` der Instanz, für die ein Upgrade durchgeführt wurde.
4. Wenn Ihr IBM Security Directory Integrator eine ältere Version als 7.1 aufweist, installieren Sie IBM Security Directory Integrator Version 7.1.
5. Stellen Sie den Benutzerkontext auf den Eigner der Verzeichnisserverinstanz um.  

```
su - instance_owner
```
6. Kopieren Sie die folgenden Dateien:
  - a. Kopieren Sie die Dateien und Verzeichnisse von `Directory_Integrator_v7.1_installation_location/etc` nach `DS_instance_home/idsslapd-instance_name/etc/logmgt`.
  - b. Kopieren Sie die Dateien und Verzeichnisse von `Directory_Integrator_v7.1_installation_location/serverapi` nach `DS_instance_home/idsslapd-instance_name/etc/logmgt`.
  - c. Kopieren Sie `Directory_Integrator_v7.1_installation_location/idisrv` nach `DS_instance_home/idsslapd-instance_name/etc/logmgt`.
  - d. Kopieren Sie `Directory_Integrator_v7.1_installation_location/testserver.jks` nach `DS_instance_home/idsslapd-instance_name/etc/logmgt`.
7. Erstellen Sie im Pfad `DS_instance_home/idsslapd-instance_name/etc/logmgt` das Verzeichnis `logs`.
8. Fügen Sie am Ende der Datei `DS_instance_home/idsslapd-instance_name/etc/logmgt/solutions.properties` den Eintrag `systemqueue.on=false` ein.
9. Wenn der Installationspfad von IBM Security Directory Integrator Version 7.1 vom Standardpfad abweicht, setzen Sie die Variable `IDS_LDAP_TDI_HOME` mit der Installationsposition.
10. Führen Sie die Protokollverwaltungslösung aus.

---

## SNMP-Lösung migrieren

Sie können eine mit einer Instanz einer Vorgängerversion konfigurierte SNMP-Lösung (SNMP = Simple Network Management Protocol) auf eine Instanz der Version 6.3.1 migrieren.

## Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um die SNMP-Lösung von einer Instanz mit einer Vorgängerversion auf eine Instanz der Version 6.3.1 zu migrieren:

- Installieren Sie IBM Security Directory Server Version 6.3.1. Siehe „Installation starten“ auf Seite 29.
- Installieren Sie IBM Security Directory Integrator Version 7.1, sofern noch nicht auf dem Computer installiert.
- Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.

## Vorgehensweise

1. Sichern Sie das Verzeichnis `snmp`, das sich an der Installationsposition von IBM Security Directory Server befindetet, die Ihrer vorhandenen Instanz mit der Vorgängerversion zugeordnet ist.
2. Führen Sie ein Upgrade der Vorgängerversion der Instanz auf Version 6.3.1 durch. Weitere Informationen finden Sie in Kapitel 14, „Upgrades von Instanzen von Vorgängerversionen durchführen“, auf Seite 93.
3. Ersetzen Sie die Datei `/idstools/snmp/idssnmp.conf`, die sich im Installationspfad von IBM Security Directory Server Version 6.3.1 befindet, durch die Datei `/idstools/snmp/idssnmp.conf`, die sich im Installationspfad der Vorgängerversion von IBM Security Directory Server befindet.
4. Ersetzen Sie die Datei `/idstools/snmp/idssnmp.properties`, die sich im Installationspfad von IBM Security Directory Server Version 6.3.1 befindet, durch die Datei `/idstools/snmp/idssnmp.properties`, die sich im Installationspfad der Vorgängerversion von IBM Security Directory Server befindet.
5. Ersetzen Sie die Datei `/idstools/snmp/IBM-DIRECTORYSERVER-MIB`, die sich im Installationspfad von IBM Security Directory Server Version 6.3.1 befindet, durch die Datei `/idstools/snmp/IBM-DIRECTORYSERVER-MIB`, die sich im Installationspfad der Vorgängerversion von IBM Security Directory Server befindet.
6. Ersetzen Sie die Datei `/idstools/snmp/INET-ADDRESS-MIB`, die sich im Installationspfad von IBM Security Directory Server Version 6.3.1 befindet, durch die Datei `/idstools/snmp/INET-ADDRESS-MIB`, die sich im Installationspfad der Vorgängerversion von IBM Security Directory Server befindet.
7. Wenn der Installationspfad von IBM Security Directory Integrator Version 7.1 vom Standardpfad abweicht, setzen Sie die Variable `IDS_LDAP_TDI_HOME` mit der Installationsposition.
8. Führen Sie die SNMP-Lösung aus.

---

## Active Directory-Synchronisationslösung migrieren

Sie können eine mit einer Instanz einer Vorgängerversion konfigurierte Active Directory-Synchronisationslösung auf eine Instanz der Version 6.3.1 migrieren.

## Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um die Active Directory-Synchronisationslösung von einer Instanz mit einer Vorgängerversion auf eine Instanz der Version 6.3.1 zu migrieren:

- Installieren Sie IBM Security Directory Server Version 6.3.1. Siehe „Installation starten“ auf Seite 29.
- Installieren Sie IBM Security Directory Integrator Version 7.1, sofern noch nicht auf dem Computer installiert.

- Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.

Ab IBM Security Directory Server Version 6.3.1 wird die Active Directory-Synchronisationslösung nicht weiter unterstützt. Verwenden Sie stattdessen die Lösung LDAPSync.

### Vorgehensweise

1. Führen Sie ein Upgrade der Vorgängerversion der Instanz auf Version 6.3.1 durch. Weitere Informationen finden Sie in Kapitel 14, „Upgrades von Instanzen von Vorgängerversionen durchführen“, auf Seite 93.
2. Erstellen Sie eine Verzeichnisserverinstanz. Weitere Informationen finden Sie unter „Instanzerstellung mit **Instance Administration Tool**“ auf Seite 140.
3. Konfigurieren Sie die Verzeichnisserverinstanz für die Active Directory-Synchronisation. Weitere Informationen finden Sie unter „Active Directory-Synchronisation“ auf Seite 225.
4. Stellen Sie die Änderungen wieder her, die Sie vor dem Upgrade der Instanz an der Datei `DS_instance_home/idsslapd-instance_name/etc/tdisoldir/solution.properties` vorgenommen haben.

**Anmerkung:** Wenn Sie die neu erstellte Datei `solution.properties` durch die ältere Datei ersetzen, schlägt die Active Directory-Synchronisation möglicherweise fehl. Das Format der Datei `solution.properties`, die beim Ausführen des Befehls `idsadscfg` erstellt wird, unterscheidet sich von dem der älteren Datei.

5. Führen Sie die Active Directory-Synchronisationslösung aus. Weitere Informationen zum Befehl `idsadsrun` finden Sie in der Veröffentlichung *Command Reference*.

---

## Vorgängerversion der Webverwaltungstool-Konfiguration migrieren

Migrieren Sie eine Vorgängerversion einer **Webverwaltungstool**-Konfiguration, um diese mit denselben Einstellungen mit einer neueren Version des **Webverwaltungstools** weiterhin zu verwenden.

Um eine vorhandene **Webverwaltungstool**-Konfiguration einer Vorgängerversion mithilfe des Befehls `idswmigr` zu migrieren, müssen die folgenden Bedingungen erfüllt sein:

1. Die Vorgängerversion des **Webverwaltungstools** ist auf dem Computer installiert.
2. Die Vorgängerversion der integrierten Version von WebSphere Application Server ist auf dem Computer installiert.
3. Die Vorgängerversion des **Webverwaltungstools** ist in der Vorgängerversion der integrierten Version von WebSphere Application Server bereitgestellt.
4. Installieren Sie die Version des **Webverwaltungstools**, die mit IBM Security Directory Server Version 6.3.1 bereitgestellt wird.
5. Installieren Sie die integrierte Version von WebSphere Application Server, die mit IBM Security Directory Server Version 6.3.1 bereitgestellt wird.
6. Stellen Sie nicht die Version des **Webverwaltungstools** bereit, die mit Version 6.3.1 in der integrierten Version von WebSphere Application Server bereitgestellt wird.

Das **Webverwaltungstool** der folgenden IBM Security Directory Server-Versionen, das auf der folgenden integrierten Version von WebSphere Application Server bereitgestellt wird, wird für die Migration unterstützt:

- IBM Security Directory Server Version 6.1 und integrierte Version von WebSphere Application Server 6.1.0.7 oder höher
- IBM Security Directory Server Version 6.2 und integrierte Version von WebSphere Application Server 6.1.0.13 oder höher (unter UNIX), integrierte Version von WebSphere Application Server 6.1.0.17 (unter Windows) oder höher
- IBM Security Directory Server Version 6.3 und integrierte Version von WebSphere Application Server 7.0.0.7 oder höher

Wenn Sie den Befehl **idswmigr** zum Migrieren von Konfigurationseinstellungen einer Vorgängerversion des **Webverwaltungstools** verwenden, werden durch den Befehl die folgenden Operation durchgeführt:

1. Die Konfigurationsdateien für die Vorgängerversion des **Webverwaltungstools** werden gespeichert.
2. Die Implementierung der Vorgängerversion des **Webverwaltungstools** wird von der Vorgängerversion der integrierten Version von WebSphere Application Server entfernt.
3. Ein Backup der Konfiguration der Vorgängerversion der integrierten Version von WebSphere Application Server wird in einer von Ihnen angegebenen temporären Position durchgeführt.
4. Die Konfiguration der Vorgängerversion der integrierten Version von WebSphere Application Server wird in einer Speicherposition wiederhergestellt.
5. Das **Webverwaltungstool** wird in der derzeitigen Version der integrierten Version von WebSphere Application Server bereitgestellt, die mit IBM Security Directory Server Version 6.3.1 bereitgestellt wird.
6. Die vorherigen **Webverwaltungstool**-Konfigurationsdateien werden migriert und in der höheren Version der integrierten Version von WebSphere Application Server wiederhergestellt.

**Anmerkung:** Die Migration des **Webverwaltungstools** mit IBM Installation Manager ist nur möglich, wenn die übergeordnete Version der integrierten Version von WebSphere Application Server, die migriert werden soll, niedriger ist als die übergeordnete Version der (neu installierten) integrierten Version von WebSphere Application Server.

## **idswmigr**

Mit dem Befehl **idswmigr** migrieren Sie eine vorhandene **Webverwaltungstool**-Konfiguration einer Vorgängerversion auf eine spätere Version des **Webverwaltungstools**.

### **Beschreibung**

Zum Migrieren einer vorhandenen **Webverwaltungstool**-Konfiguration einer Vorgängerversion mit dem Befehl **idswmigr** müssen folgende Bedingungen erfüllt sein:

1. Die Vorgängerversion des **Webverwaltungstools** ist auf dem Computer installiert.
2. Die Vorgängerversion der integrierten Version von WebSphere Application Server ist auf dem System installiert.
3. Die Vorgängerversion des **Webverwaltungstools** ist in der Vorgängerversion der integrierten Version von WebSphere Application Server implementiert.

4. Installieren Sie die spätere Version des **Webverwaltungstools**.
5. Installieren Sie die spätere integrierte Version von WebSphere Application Server.
6. Implementieren Sie das **Webverwaltungstool** nicht mit einer späteren Version als die integrierte Version von WebSphere Application Server.

## Übersicht

```
idswmigr -l temp_path [-s source_path -t target_path
-r profile_name -a app_name -v -o ports_path ]
```

## Optionen

Der Befehl **idswmigr** nimmt folgende Parameter an:

- a *app\_name*  
Gibt den Anwendungsnamen an. Wird kein Wert angegeben, lautet der Standardwert `IDSWebApp.war`.
- l *temp\_path*  
Gibt eine Position zum Speichern der temporären Dateien an.
- o *ports\_path*  
Gibt den vollständig qualifizierten Pfad der Portdefinitionsdatei an. Wird kein Wert angegeben, wird der folgende Standardpfad verwendet:  
**Windows**  
C:\Program Files\IBM\ldap\V6.3.1\idstools\TDSWEBPortDef.props  
**AIX und Solaris**  
/opt/IBM/ldap/V6.3.1/idstools/TDSWEBPortDef.props  
**Linux** /opt/ibm/ldap/V6.3.1/idstools/TDSWEBPortDef.props
- r *profile\_name*  
Gibt den Namen des Profils an, das der Anwendung zugeordnet ist. Wird kein Wert angegeben, lautet der Standardwert `TDSWebAdminProfile`.
- s *source\_path*  
Gibt die Quellenposition der Vorgängerversion der integrierten Version von WebSphere Application Server an.
- t *target\_path*  
Gibt die Installationsposition einer späteren Version der integrierten Version von WebSphere Application Server an.
- v  
Zeigt die Versionsinformationen an.

## Beispiele

### Beispiel 1

Zum Migrieren einer vorhandenen **Webverwaltungstool**-Konfiguration von Version 6.2 auf Version 6.3.1 führen Sie den folgenden Befehl aus:

```
idswmigr -l /tmp/web_migr -s /opt/ibm/ldap/V6.2/appsrv \
-t /opt/ibm/ldap/V6.3.1/appsrv -r TDSWebAdminProfile \
-a IDSWebApp.war
```

## Webverwaltungstool manuell migrieren

Sie können das Webverwaltungstool manuell migrieren.



## Vorbereitende Schritte

Damit das Webverwaltungstool manuell migriert werden kann, muss es zuerst installiert werden. Gehen Sie wie folgt vor, um das Webverwaltungstool manuell zu migrieren. Im vorliegenden Beispiel wird das Webverwaltungstool von IBM Security Directory Server V6.3 auf IBM Security Directory Server V6.3.1 migriert.

Unter AIX werden für die Migration ähnliche Befehle wie unter Linux verwendet. Nur der Pfad `/opt/ibm/ldap` muss durch `/opt/IBM/ldap` ersetzt werden.

## Vorgehensweise

1. Fügen Sie unter Windows den WebSphere Application Server-Service mit dem folgenden Befehl hinzu:

```
"C:\Program Files\IBM\ldap\V6.3.1\appsrv\bin\WASService.exe" -add  
TDSWebAdmin-V6.3.1 -serverName server1 -profilePath  
"C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile"  
-startType automatic
```

2. Sichern Sie die Dateien des Webverwaltungstools aus dem Vorgängerrelease.

- Unter Windows befinden sich diese Dateien im folgenden Verzeichnis:

```
C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\  
WEB-INF\classes\
```

oder

```
C:\Program Files\IBM\LDAP\V6.3\appsrv\installedApps\DefaultNode\  
IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes
```

- Unter Linux befinden sich diese Dateien im folgenden Verzeichnis:

```
/opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/installedApps/  
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
```

oder

```
/opt/ibm/ldap/V6.3/appsrv/installedApps/DefaultNode/  
IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
```

Kopieren Sie nur die fünf folgenden Dateien aus den Verzeichnissen:

```
security\console_passwd  
IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml  
IDSConfig\IDSServersConfig\IDSServersInfo.xml  
IDSConfig\IDSAppReg\IDSAppReg.xml  
IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml
```

Beispiel:

```
copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\  
security\console_passwd" c:\BackUp  
copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\  
IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml" c:\BackUp  
copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\  
IDSConfig\IDSServersConfig\IDSServersInfo.xml" c:\BackUp  
copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\  
IDSConfig\IDSAppReg\IDSAppReg.xml" c:\BackUp  
copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\  
IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml" c:\BackUp
```

3. Deinstallieren Sie die WAR-Datei aus dem Vorgängerrelease.

- Unter Windows befindet sich der Befehl im folgenden Verzeichnis:  
C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat

oder

```
C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\wsadmin.bat
```

- Unter Linux befindet sich der Befehl im folgenden Verzeichnis:  
/opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh

oder

```
/opt/ibm/ldap/V6.3/appsrv/bin/wsadmin.sh
```

```
wsadmin.bat -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
```

Beispiel:

```
"C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat"
-conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
```

4. Wenn der Server der integrierten Vorgängerversion von WebSphere Application Server aktiv ist, stoppen Sie den Anwendungsserver.

- Unter Windows befindet sich der Befehl im folgenden Verzeichnis:  
C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\stopServer.bat

oder

```
C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\stopServer.bat
```

- Unter Linux befindet sich der Befehl im folgenden Verzeichnis:  
/opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/stopServer.sh

oder

```
/opt/ibm/ldap/V6.3/appsrv/bin/stopServer.sh
```

Beispiel:

```
"C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\
stopServer.bat" server1
```

5. Prüfen Sie, ob das Profil in der neuen integrierten Version von WebSphere Application Server vorhanden ist. Ist das Profil nicht vorhanden, erstellen Sie ein neues Profil.

- Führen Sie unter Windows den folgenden Befehl aus, um ein neues Profil zu erstellen:

```
"C:\Program Files\IBM\LDAP\V6.3.1\appsrv\bin\manageprofiles.bat" -create
-profileName TDSWebAdminProfile -profilePath "C:\Program Files\IBM\
LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile" -templatePath
"C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profileTemplates\default"
-nodeName DefaultNode -hostName localhost -cellName
DefaultNode -isDefault -portsFile "C:\Program Files\IBM\LDAP\V6.3.1\idstools
\TDSWEBPortDef.props"
```

- Führen Sie unter Linux den folgenden Befehl aus, um ein neues Profil zu erstellen:

```
/opt/ibm/ldap/V6.3.1/appsrv/bin/manageprofiles.sh -create -profileName
TDSWebAdminProfile -profilePath "/opt/ibm/ldap/V6.3.1/appsrv/profiles/
TDSWebAdminProfile" -templatePath "/opt/ibm/ldap/V6.3.1/appsrv/
profileTemplates/default" -nodeName DefaultNode -hostName localhost
-cellName DefaultNode -isDefault -portsFile "/opt/ibm/ldap/V6.3.1/idstools
/TDSWEBPortDef.props"
```

6. Kopieren Sie die neue WAR-Datei in das neue WebSphere Application Server-Verzeichnis.

- Führen Sie unter Windows den folgenden Befehl aus:

```
copy "C:\Program Files\IBM\LDAP\V6.3.1\idstools\IDSWebApp.war"  
"C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\  
installableApps"
```

- Führen Sie unter Linux den folgenden Befehl aus:

```
cp "/opt/ibm/ldap/V6.3.1/idstools/IDSWebApp.war"  
"/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installableApps"
```

7. Installieren Sie die neue WAR-Datei in das neue WebSphere Application Server-Produkt.

- Führen Sie unter Windows den folgenden Befehl aus:

```
"C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin  
\wsadmin.bat" -conntype NONE -c "$AdminApp install {C:\Program Files\  
IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\installableApps\  
IDSWebApp.war} {-configroot \"C:\Program Files\IBM\LDAP\V6.3.1\  
appsrv\config\" -node DefaultNode -usedefaultbindings -nodeployejb  
-appname IDSWebApp.war -contextroot \"IDSWebApp\"}"
```

- Führen Sie unter Linux den folgenden Befehl aus:

```
"/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh"  
-conntype NONE -c "\"$AdminApp install {/opt/ibm/ldap/V6.3.1/appsrv/  
profiles/TDSWebAdminProfile/installableApps/IDSWebApp.war}  
{-configroot \"/opt/ibm/ldap/V6.3.1/appsrv/config\"  
-node DefaultNode -usedefaultbindings -nodeployejb -appname IDSWebApp.war  
-contextroot \"IDSWebApp\"}"
```

8. Stellen Sie die zuvor gespeicherten Konfigurationsdateien des Webverwaltungstools wieder her.

- Ersetzen Sie unter Windows die folgenden Dateien durch die Dateien der Sicherungskopie:

```
C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\  
classes\security\console_passwd  
C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\  
classes\IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml  
C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\  
classes\IDSConfig\IDSServersConfig\IDSServersInfo.xml  
C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\  
classes\IDSConfig\IDSAppReg\IDSAppReg.xml  
C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\  
classes\IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml
```

- Ersetzen Sie unter Linux die folgenden Dateien durch die Dateien der Sicherungskopie:

```
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/  
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/security/  
console_passwd  
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/  
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/  
IDSSessionConfig/IDSSessionMgmt.xml  
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/  
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/  
IDSServersConfig/IDSServersInfo.xml  
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/  
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
```

```
IDSAppReg/IDSAppReg.xml  
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/  
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/  
IDSSearchSettings/IDSSearchMgmt.xml
```

9. Starten Sie unter Windows den hinzugefügten Service.

```
"C:\Program Files\IBM\ldap\V6.3.1\appsrv\bin\WASService.exe"  
-start TDSWebAdmin-V6.3.1
```

10. Starten Sie unter Linux den Server.

```
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin/startServer.sh server1
```

---

## Kapitel 16. Manuelle Bereitstellung des Webverwaltungstools

Um Verzeichnisserverinstanzen mit dem **Webverwaltungstool** zu verwalten und zu administrieren, müssen Sie das **Webverwaltungstool** auf einem unterstützten Webanwendungsserver bereitstellen.

Für die Bereitstellung des **Webverwaltungstools** muss sich auf Ihrem Computer eine unterstützte Version eines Webanwendungsservers befinden. Auf Installationsmedien von IBM Security Directory Server wird eine integrierte Version von WebSphere Application Server Version 7.0.0.25 bereitgestellt. Sie können IBM Installation Manager verwenden, um die Installation des **Webverwaltungstools** durchzuführen und das Programm in einer integrierten Version von WebSphere Application Server bereitzustellen.

Wenn die Installation von IBM Security Directory Server mit IBM Installation Manager auf Ihrem Betriebssystem nicht unterstützt wird, führen Sie die Installation der integrierten Version von WebSphere Application Server manuell durch. Nach der Installation der integrierten Version von WebSphere Application Server müssen Sie das **Webverwaltungstool** in der integrierten Version von WebSphere Application Server bereitstellen.

Wenn auf Ihrem Computer eine unterstützte Version von WebSphere Application Server installiert ist, können Sie das **Webverwaltungstool** darüber bereitstellen.

WebSphere Application Server ist die Laufzeitumgebung für Java-basierte Anwendungen von IBM. Weitere Informationen finden Sie in der Produktdokumentation für WebSphere Application Server unter <http://www-01.ibm.com/support/knowledgecenter/SSEQTP/welcome>.

---

### Integrierte Version von WebSphere Application Server manuell installieren

Zum Implementieren des **Webverwaltungstools** müssen Sie die integrierte Version von WebSphere Application Server auf Ihrem Computer installieren.

#### Vorbereitende Schritte

Führen Sie zur Installation der integrierten Version von WebSphere Application Server die folgenden Schritte aus:

1. Greifen Sie auf die IBM Security Directory Server-Installationsmedien zu, die die Installationsdatei der integrierten Version von WebSphere Application Server enthalten. Weitere Informationen finden Sie unter „Vorbereitung von Installationsmedien“ auf Seite 6.

#### Informationen zu diesem Vorgang

Sie müssen die folgenden Werte angeben, um das **Webverwaltungstool** mit dem Befehl `deploy_IDSWebApp` ohne Parameter zu implementieren.

1. Geben Sie im Installationspfad von IBM Security Directory Server das Verzeichnis `appsrv` als Installationsposition für die integrierte Version von WebSphere Application Server an. Weitere Informationen zum Standardinstallationspfad

von IBM Security Directory Server finden Sie unter „Standardinstallationspositionen“ auf Seite 28.

Sie können auch eine andere Installationsposition für die integrierte Version von WebSphere Application Server angeben. In diesem Fall müssen Sie mit dem Befehl `deploy_IDSWebApp` die Parameter und Werte **-w**, **-p**, **-r** und **-o** angeben, um das **Webverwaltungstool** zu implementieren.

### Vorgehensweise

1. Melden Sie sich mit Administratorrechten an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis, in dem die Installationsdatei der integrierten Version von WebSphere Application Server enthalten ist.
4. Führen Sie den folgenden Befehl aus, um die integrierte Version von WebSphere Application Server im Standardinstallationspfad von IBM Security Directory Server zu installieren:

Betriebssysteme	Befehl:
Microsoft Windows	<code>install.bat -installRoot c:\Program Files\IBM\ldap\V6.3.1\appsrv</code>
AIX und Solaris	<code>install.sh -installRoot /opt/IBM/ldap/V6.3.1\appsrv</code>
Linux	<code>install.sh -installRoot /opt/ibm/ldap/V6.3.1\appsrv</code>

### Nächste Schritte

Installieren Sie das **Webverwaltungstool**, falls es nicht auf Ihrem Computer installiert ist. Weitere Informationen finden Sie in Kapitel 12, „Installation mit den Befehlszeilendienstprogrammen des Betriebssystems“, auf Seite 71.

Implementieren Sie das **Webverwaltungstool**, falls es bereits auf Ihrem Computer installiert ist. Siehe „**Webverwaltungstool** in der integrierten Version von WebSphere Application Server implementieren“ auf Seite 115.

---

## Standardports für das Webverwaltungstool

Um Portkonflikte bei Ports zwischen dem **Webverwaltungstool** und anderen Anwendungen zu vermeiden, müssen Sie die Standardports kennen, die vom **Webverwaltungstool** verwendet werden.

In Integrierte Version von WebSphere Application Server werden die folgenden Standardporteinstellungen für das **Webverwaltungstool** verwendet:

- HTTP-Transport (Port 1): 12100
- HTTPS-Transport (Port 2): 12101
- Port der Verwaltungskonsole (zur Verwaltung von WebSphere Application Server): 12104
- Sicherer Port der Verwaltungskonsole (zur Verwaltung von WebSphere Application Server): 12105

In Integrierte Version von WebSphere Application Server werden die folgenden Standardporteinstellungen für andere Anwendungen verwendet:

- Bootstrap-/RMI-Port: 12102
- SOAP-Verbindungsport: 12103

Andere Portnummern, die von integrierten Versionen von WebSphere Application Server verwendet werden können: 9405, 9406, 9407, 9375, 9105, 7276, 7286, 5558, 5577, 5075, 5076.

Wenn ein Portkonflikt mit einer anderen Anwendung besteht, die möglicherweise mindestens einen der Standardports verwendet, führen Sie entsprechend Ihrer Umgebung eine der folgenden Aktionen durch:

- Ändern Sie die Standardports in unbenutzte Ports und starten Sie die Anwendung mit dem unbenutzten Port.
- Wenn die Anwendung, die die Standardports verwendet, kein wichtiger Service oder Server ist, ändern Sie dessen Portnummer und geben Sie den Standardport frei.

Um die Standardportnummern, die die integrierte Version von WebSphere Application Server für die Anwendung initialisiert, zu ändern, müssen Sie die entsprechende Portnummer in der Datei `portdef.props` festlegen. Die Datei `portdef.props` befindet sich im Verzeichnis `\appsrv\profiles\TDSWebAdminProfile\properties\` in der Installationsposition von IBM Security Directory Server. Weitere Informationen zur Standardinstallationsposition von IBM Security Directory Server finden Sie im Kapitel „Standardinstallationspositionen“ auf Seite 28.

#### **HTTP-Transport - Port 1**

Um Port 1 für den HTTP-Transport zu ändern, ändern Sie den Eintrag mit der Portnummer 12100 in eine Portnummer, die nicht belegt ist.

#### **HTTPS-Transport – Port 2**

Um Port 2 für den HTTPS-Transport zu ändern, ändern Sie den Eintrag mit der Portnummer 12101 in eine Portnummer, die nicht belegt ist.

#### **Bootstrap/RMI-Port**

Um den Port für Bootstrap/RMI zu ändern, ändern Sie den Eintrag mit der Portnummer 12102 in eine Portnummer, die nicht belegt ist.

#### **SOAP-Verbindungsport**

Um den SOAP-Connector-Port zu ändern, ändern Sie den Eintrag mit der Portnummer 12103 in eine Portnummer, die nicht belegt ist.

#### **Verwaltungskonsolenport**

Um den Port für die Administrationskonsole zu ändern, ändern Sie den Eintrag mit der Portnummer 12104 in eine Portnummer, die nicht belegt ist.

#### **Port für die sichere Administrationskonsole**

Um den Port für die sichere Administrationskonsole zu ändern, ändern Sie den Eintrag mit der Portnummer 12105 in eine Portnummer, die nicht belegt ist.

---

## **Webverwaltungstool in der integrierten Version von WebSphere Application Server implementieren**

Um das **Webverwaltungstool** zu verwenden, müssen Sie es auf einem Webanwendungsserver implementieren.

## Vorbereitende Schritte

Sie müssen die folgenden Aktionen ausführen, um das **Webverwaltungstool** zu implementieren:

1. Installieren Sie das Paket des **Webverwaltungstools** auf Ihrem Betriebssystem.
2. Installieren Sie eine unterstützte Version des Webanwendungsservers.
3. Wenn Sie planen, eine vorhandene Konfiguration des **Webverwaltungstools** einer Vorgängerversion zu migrieren, dürfen Sie keine spätere Version des **Webverwaltungstools** implementieren.

## Informationen zu diesem Vorgang

Beim Implementieren des **Webverwaltungstools** löst der Befehl die folgenden Aktionen aus:

1. Frühere Versionen des **Webverwaltungstools** werden entfernt, sofern vorhanden.
2. Das **Webverwaltungstool** wird auf einem Webanwendungsserver implementiert.
3. Der Webanwendungsserver wird gestartet.

## Vorgehensweise

1. Melden Sie sich mit Administratorrechten an.
2. Wechseln Sie in das Verzeichnis *DS\_install\_location/idstools*. *DS\_install\_location* steht für die Installationsposition von IBM Security Directory Server. Nachstehend sind die Standardpositionen auf verschiedenen Betriebssystemen aufgeführt:

Betriebssysteme	Standardinstallationspositionen:
Microsoft Windows	c:\Program Files\IBM\ldap\V6.3.1
AIX und Solaris	/opt/IBM/ldap/V6.3.1
Linux	/opt/ibm/ldap/V6.3.1

3. Führen Sie den folgenden Befehl aus:

**Anmerkung:** Wenn Sie die integrierte Version von WebSphere Application Server an der Standardinstallationsposition von IBM Security Directory Server installiert haben, geben Sie für den Befehl `deploy_IDSWebApp` keine Parameter an. Weitere Informationen zum Befehl `deploy_IDSWebApp` finden Sie in der Befehlsyntax, die durch die Eingabe von `deploy_IDSWebApp -h` angezeigt wird.

Betriebssysteme	Befehl:
Microsoft Windows	<code>deploy_IDSWebApp.bat -w path_to_war_file -p was_installation_path -r profile -o ports_file</code>
AIX, Linux und Solaris	<code>deploy_IDSWebApp -w path_to_war_file -p was_installation_path -r profile -o ports_file</code>

## Ergebnisse

Der Befehl implementiert das **Webverwaltungstool** auf dem mit *was\_installation\_path* angegebenen Webanwendungsserver.



## Nächste Schritte

Für den Zugriff auf das **Webverwaltungstool** müssen Sie ein Browserfenster öffnen und `http://host_name:12100/IDSWebApp` eingeben. Die Variable `host_name` gibt den Hostnamen oder die IP-Adresse des Computers an, auf dem das **Webverwaltungstool** installiert wurde.

---

## Webverwaltungstool in WebSphere Application Server implementieren

Wenn Sie Anwendungen auf Ihrem Computer mit WebSphere Application Server verwalten wollen, können Sie das **Webverwaltungstool** in WebSphere Application Server implementieren.

### Vorbereitende Schritte

Zum Implementieren des **Webverwaltungstools** in WebSphere Application Server müssen Sie die folgenden Anforderungen erfüllen:

1. Installieren Sie das Paket des **Webverwaltungstools** auf Ihrem Betriebssystem. Siehe „Installation mit IBM Installation Manager“ auf Seite 32.
2. Auf Ihrem Computer muss eine unterstützte Version von WebSphere Application Server enthalten sein.

### Informationen zu diesem Vorgang

Auf den Installationsmedien von IBM Security Directory Server sind das **Webverwaltungstool** und die integrierte Version von WebSphere Application Server enthalten. Wenn WebSphere Application Server auf Ihrem Computer vorhanden ist, können Sie das **Webverwaltungstool** in WebSphere Application Server implementieren. Zum Implementieren des **Webverwaltungstools** müssen Sie die Datei `IDSWebApp.war` implementieren, die sich an der Installationsposition von IBM Security Directory Server im Verzeichnis `idstools` befindet.

### Vorgehensweise

1. Melden Sie sich über die URL `http://hostname_WAS_server:9060/ibm/console` an der WebSphere-Administrationskonsole an. Setzen Sie für die Variable `hostname_WAS_server` den Hostnamen oder die IP-Adresse Ihres Computers ein, auf dem WebSphere Application Server installiert ist. Wenn Sie für den Zugriff auf die WebSphere-Administrationskonsole einen angepassten Port angegeben haben, ersetzen Sie die Standardportnummer 9060 durch Ihre Portnummer.
2. Geben Sie die Benutzer-ID und das Kennwort des Benutzers ein. Der Benutzer muss über die erforderliche Berechtigung zum Ausführen von Operationen für WebSphere Application Server verfügen.
3. Klicken Sie im Navigationsbereich auf der linken Seite auf **Anwendung > Neue Anwendung**.
4. Klicken Sie auf der Seite **Neue Anwendung** auf **Neue Unternehmensanwendung**.
5. Wählen Sie je nachdem, von wo aus Sie auf die WebSphere-Administrationskonsole zugegriffen haben, auf der Seite **Pfad der neuen Anwendung** eine der folgenden Optionen aus:
  - Wenn Sie von einem lokalen Computer auf die WebSphere-Administrationskonsole zugegriffen haben, wählen Sie **Lokales Dateisystem** aus und geben Sie im Feld **Vollständiger Pfad** den Pfad zur Datei `IDSWebApp.war` ein. Sie können auch auf **Durchsuchen** klicken, um den Pfad anzugeben.

- Wenn Sie von einem fernen Computer auf die WebSphere-Administrationskonsole zugegriffen haben, wählen Sie **Fernes Dateisystem** aus und geben Sie im Feld **Vollständiger Pfad** den Pfad zur Datei `IDSWebApp.war` ein. Sie können auch auf **Durchsuchen** klicken, um den Pfad anzugeben.
6. Wählen Sie auf der Seite **Wie soll die Anwendung installiert werden** die Option **Schnell** aus und klicken Sie auf **Weiter**.
  7. Auf der Seite **Installationsoptionen auswählen** sind die Standardoptionen ausgewählt.
  8. Klicken Sie auf **Weiter**.
  9. Auf der Seite **Servern Module zuordnen** können Sie die Module den im Feld **Cluster und Server** angegebenen Servern zuordnen.
    - a. Aktivieren Sie das Markierungsfeld des erforderlichen Moduls und klicken Sie auf **Anwenden**.
    - b. Klicken Sie nach erfolgter Zuordnung auf **Weiter**.
  10. Auf der Seite **Virtuelle Hosts für Webmodule zuordnen** können Sie die Webanwendung den virtuellen Servern zuordnen. Wenn mehrere virtuelle Hosts vorhanden sind, benötigt der Server zur Auswahl des richtigen Moduls Angaben zu der WebSphere-Umgebung. In diesem Beispiel steht die Option `default_host` zur Auswahl.
  11. Klicken Sie auf **Weiter**.
  12. Geben Sie auf der Seite **Kontextstammverzeichnisse für Webmodule zuordnen** in dem entsprechenden Feld das Kontextstammverzeichnis `/IDSWebApp` ein.
  13. Ihre ausgewählten Optionen werden in einer Übersicht zusammengefasst.
  14. Klicken Sie auf **Fertig stellen**. Die Installation der Anwendung wird gestartet. Eine Installationszusammenfassung wird angezeigt.
  15. Klicken Sie auf **Speichern**, um die Änderungen in der Hauptkonfiguration zu speichern.
  16. Klicken Sie im Navigationsbereich auf der linken Seite auf **Anwendungen > Anwendungstypen > WebSphere-Unternehmensanwendungen**.
  17. Aktivieren Sie auf der Seite **Unternehmensanwendungen** das Markierungsfeld neben `IDSWebApp_war` und klicken Sie auf **Starten**.
  18. Starten Sie das **Webverwaltungstool**.
  19. Für den Zugriff auf das **Webverwaltungstool** müssen Sie einen Browser öffnen und die folgende Adresse eingeben:
    - Geben Sie für nicht sicheren Zugriff (HTTP) `http://WAS_server_hostname:9080/IDSWebApp` ein.
    - Geben Sie für sicheren Zugriff (HTTPS) `https://WAS_server_hostname:9443/IDSWebApp` ein.

Port 9080 ist der HTTP-Standardport für WebSphere Application Server, Port 9443 ist der HTTPS-Standardport. Wenn diese Ports nicht für Ihre Instanz von WebSphere Application Server konfiguriert wurden, müssen Sie die entsprechende Portnummer bereitstellen. Wenn die globale oder die Verwaltungssicherheitsfunktion für WebSphere Application Server konfiguriert wurde, müssen Sie die folgenden Anforderungen erfüllen:

    - a. Implementieren Sie das **Webverwaltungstool** in WebSphere Application Server als neues Profil.
    - b. Konfigurieren Sie SSL für das **Webverwaltungstool**.
    - c. Wenn das **Webverwaltungstool** nicht in einem Profil implementiert werden kann, müssen Sie das Zertifikat des Verzeichnisservers zum Truststore

des Profils hinzufügen. Fügen Sie für die Client-Server-Authentifizierung das Zertifikat des WebSphere Application Server-Profiles zum Truststore des Verzeichnisservers hinzu.

---

## Integrierte Version von WebSphere Application Server für die Verwendung des Webverwaltungstools starten

Starten Sie den Webanwendungsserver, der dem **Webverwaltungstool** zugeordnet ist, um Verzeichnisserverinstanzen hinzuzufügen und zu verwalten.

### Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um einen Webanwendungsserver zu starten, der dem **Webverwaltungstool** zugeordnet ist:

1. Installieren Sie das **Webverwaltungstool**.
2. Implementieren Sie das **Webverwaltungstool** auf einem unterstützten Webanwendungsserver.

**Anmerkung:** Wenn Sie IBM Installation Manager für die Installation und Implementierung des **Webverwaltungstools** in der integrierten Version von WebSphere Application Server verwenden, wird der Anwendungsserver gestartet, sobald Sie das **Webverwaltungstool** implementiert haben.

### Vorgehensweise

1. Führen Sie auf den verschiedenen Betriebssystemen die folgenden Befehle aus, um den Webanwendungsserver zu starten, der dem **Webverwaltungstool** zugeordnet ist:

#### Windows

Führen Sie den folgenden Befehl aus, wenn der Anwendungsserver nicht gestartet wird:

```
installation_path\idstools\bin\startWebadminApp.bat
```

Der Standardinstallationspfad ist C:\Program Files\IBM\ldap\V6.3.1.

#### AIX und Solaris

```
/opt/IBM/ldap/V6.3.1/idstools/bin/startWebadminApp
```

#### Linux

```
/opt/ibm/ldap/V6.3.1/idstools/bin/startWebadminApp
```

2. Öffnen Sie einen Web-Browser.
3. Geben Sie in der Adresszeile des Web-Browsers die folgende URL ein:

**Anmerkung:** Wenn Sie das **Webverwaltungstool** auf einem fernen System installiert und implementiert haben, setzen Sie für localhost den Hostnamen oder die IP-Adresse des Systems ein.

```
http://localhost:12100/IDSWebApp
```

### Nächste Schritte

Fügen Sie Server zur Konsole des **Webverwaltungstools** hinzu, um Verzeichnisserverinstanzen zu verwalten. Siehe „Auf das **Webverwaltungstool** zugreifen“ auf Seite 120.

---

## Auf das Webverwaltungstool zugreifen

Zum Verwalten von Verzeichnisserverinstanzen über Fernzugriff müssen Sie das **Webverwaltungstool** öffnen und die Verzeichnisserverinstanz für die Fernverwaltung konfigurieren.

### Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um auf das **Webverwaltungstool** zuzugreifen:

1. Installieren Sie das **Webverwaltungstool**.
2. Implementieren Sie das **Webverwaltungstool** auf einem unterstützten Webanwendungsserver.
3. Starten Sie den Webanwendungsserver, der dem **Webverwaltungstool** zugeordnet ist.

### Vorgehensweise

1. Wählen Sie eine der folgenden Optionen aus, um auf das **Webverwaltungstool** zuzugreifen:
  - Öffnen Sie einen Web-Browser und geben Sie die folgende URL ein:
    - Geben Sie für den nicht sicheren Zugriff `http://hostname:12100/IDSWebApp` ein.
    - Geben Sie für den sicheren Zugriff `https://hostname:12101/IDSWebApp` ein.
  - Öffnen Sie die folgende Datei in einem Web-Browser:

#### Windows

Öffnen Sie für nicht sicheren Zugriff `ds_installation_path\idstools\bin\idswebadmin.html`. Sie können auch auf **Start > Alle Programme > IBM Security Directory Server 6.3.1 > Webverwaltungstool** klicken.

Öffnen Sie für sicheren Zugriff `ds_installation_path\idstools\bin\idswebadminssl.html`. Sie können auch auf **Start > Alle Programme > IBM Security Directory Server 6.3.1 > Webverwaltungstool (sicher)** klicken.

#### AIX, Linux und Solaris

Öffnen Sie für nicht sicheren Zugriff `ds_installation_path/idstools/bin/idswebadmin.html`.

Geben Sie für sicheren Zugriff `ds_installation_path/idstools/bin/idswebadminssl.html` ein.

Die Variable `ds_installation_path` stellt die Installationsposition von IBM Security Directory Server dar. Weitere Informationen zur Standardposition finden Sie im Kapitel „Standardinstallationspositionen“ auf Seite 28.

2. Melden Sie sich als Konsolenadministrator bei der Konsole des **Webverwaltungstools** an:
  - a. Geben Sie im Feld **Benutzer-ID** die Zeichenfolge `superadmin` ein.
  - b. Geben Sie im Feld **Kennwort** die Zeichenfolge `secret` ein.

**Anmerkung:** Sie müssen das Kennwort des Konsolenadministrators nach der ersten Anmeldung ändern.

- c. Klicken Sie auf **Anmelden**.

3. Führen Sie die folgenden Schritte aus, um einen Verzeichnisserver zur Konsole hinzuzufügen:
  - a. Klicken Sie auf der Seite **Einführung** auf **Konsolenserver verwalten**.
  - b. Klicken Sie auf der Seite **Konsolenserver verwalten** auf **Hinzufügen**.
  - c. Geben Sie im Feld **Servername** einen eindeutigen Name für Ihren Server ein. Wenn Sie keinen Wert bereitstellen, weist die Anwendung einen Wert im Format `hostname:port` oder `IP_address:port` zu.
  - d. Geben Sie im Feld **Hostname** den Hostnamen oder die IP-Adresse des Verzeichnisseservers ein.
  - e. Geben Sie im Feld **Port** die Portnummer des Servers ein.
  - f. Wählen Sie **SSL-Verschlüsselung aktivieren** aus, um anzugeben, ob die Konsole sicher mit dem Server kommunizieren muss.
  - g. Wählen Sie **Unterstützter Verwaltungsserver** aus, um das Steuerelement für den Verwaltungsport zu aktivieren.
  - h. Geben Sie im Feld **Verwaltungsport** die Portnummer des Verwaltungsservers ein.
  - i. Klicken Sie auf **OK**, um die Änderungen anzuwenden.
4. Klicken Sie auf **Abmelden**, um sich von der Konsole des **Webverwaltungstools** abzumelden.

---

## Webanwendungsserver stoppen

Vor der Deinstallation des **Webverwaltungstools** müssen Sie sich vom **Webverwaltungsserver** abmelden und den diesem Tool zugeordneten Webanwendungsserver stoppen.

### Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um einen Webanwendungsserver zu stoppen, der dem **Webverwaltungstool** zugeordnet ist:

1. Implementieren Sie das **Webverwaltungstool** auf einem unterstützten Webanwendungsserver.
2. Starten Sie den Webanwendungsserver, der dem **Webverwaltungstool** zugeordnet ist.

### Vorgehensweise

1. Melden Sie sich auf UNIX-Systemen als Root und unter Windows als Mitglied der Administratorgruppe an.
2. Öffnen Sie die Eingabeaufforderung.
3. Wechseln Sie im Profil des **Webverwaltungstools** in das Verzeichnis `bin`. Die folgende Position ist der Standardinstallationspfad der integrierten Version von WebSphere Application Server für die Implementierung des **Webverwaltungstools**. Wenn Sie einen angepassten Installationspfad für die integrierte Version von WebSphere Application Server angegeben haben, müssen Sie entsprechende Änderungen vornehmen.

Betriebssystem	Pfad
Windows	C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin
AIX und Solaris	/opt/IBM/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin

Betriebssystem	Pfad
Linux	/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin

4. Führen Sie auf den verschiedenen Betriebssystemen die folgenden Befehle aus, um den Webanwendungsserver zu stoppen, der dem **Webverwaltungstool** zugeordnet ist:

Betriebssystem	Befehl:
Windows	stopServer.bat server1
AIX, Linux und Solaris	./stopServer server1

**Anmerkung:** Unter Windows können Sie den Dienst, der Ihrem Webanwendungsserver zugeordnet ist, auch im Fenster **Dienste** stoppen.

---

## HTTPS mit einer integrierten Version von WebSphere Application Server

Um den Webzugriff auf Ihre Anwendung zu sichern, können Sie Ihre Anwendung im HTTPS-Modus konfigurieren und starten.

Nach dem Implementieren des **Webverwaltungstools** in die integrierte Version von WebSphere Application Server können Sie Ihre Anwendung starten. Sie können eine sichere Verbindung zum **Webverwaltungstool** herstellen, indem Sie eine HTTPS-Webadresse und den sicheren Port angeben.

Um HTTPS zu verwenden, geben Sie die folgende Webadresse an, um auf das **Webverwaltungstool** zuzugreifen:

```
https://hostname:12101/IDSWebApp
```

Um eine Verbindung ohne HTTPS zu verwenden, geben Sie zum Zugreifen auf das **Webverwaltungstool** die folgende Webadresse an:

```
http://hostname:12100/IDSWebApp
```

Sie können auch die Standard-JKS-Dateien mit Zertifikaten ändern, die mit dem Webanwendungsserver für die sichere Kommunikation über SSL/TLS bereitgestellt werden. Sie können neue Schlüssel- und Truststore-Datenbankdateien für die Verwendung mit der Anwendung erstellen, die in der integrierten Version von WebSphere Application Server implementiert wurde. Die Standardschlüssel- und Truststore-Datenbankdateien sind separat und befinden sich im Verzeichnis `WAS_HOME/profiles/TDSWebAdminProfile/etc/`. Die Variable `WAS_HOME` steht für die Installationsposition der integrierten Version von WebSphere Application Server. Die Standardschlüsseldatenbankdatei ist `DummyServerKeyFile.jks` und die Standard-Truststore-Datenbankdatei ist `DummyServerTrustFile.jks`.

Wenn Sie die JKS-Dateien erstellt haben, können Sie die Schlüssel- und Truststore-Datenbankdateien ändern. Um die JKS-Dateien, -Kennwörter und -Dateiformate zu konfigurieren, ändern Sie die folgenden Einträge (durch **Fettdruck** hervorgehoben) in der Datei `WAS_HOME/profiles/TDSWebAdminProfile/config/cells/DefaultNode/security.xml` oder fügen Sie sie hinzu:

```

<keyStores xmi:id="KeyStore_DefaultNode_10"
  name="DummyServerKeyFile"
  password="{xor}CDo9Hgw="
  provider="IBMJCE"
  location="{WAS_HOME}/profiles/TDSWebAdminProfile/etc/DummyServerKeyFile.jks"
  type="JKS"
  fileBased="true"
  hostList=""
  managementScope="ManagementScope_DefaultNode_1"/>
<keyStores xmi:id="KeyStore_DefaultNode_11"
  name="DummyServerTrustFile"
  password="{xor}CDo9Hgw="
  provider="IBMJCE"
  location="{WAS_HOME}/profiles/TDSWebAdminProfile/etc/DummyServerTrustFile.jks"
  type="JKS"
  fileBased="true"
  hostList=""
  managementScope="ManagementScope_DefaultNode_1"/>

```

## Webverwaltungstool aus der integrierten Version von WebSphere Application Server deimplementieren

Wenn Sie ein vorhandenes **Webverwaltungstool** (Datei `IDSWebApp.war`) durch eine höhere Version ersetzen wollen, müssen Sie das vorhandene **Webverwaltungstool** deimplementieren.

### Vorgehensweise

1. Starten Sie den Webanwendungsserver, der dem **Webverwaltungstool** zugeordnet ist, wenn er gestoppt wurde. Siehe „Integrierte Version von WebSphere Application Server für die Verwendung des **Webverwaltungstools** starten“ auf Seite 119.
2. Wechseln Sie in das Verzeichnis `DS_install_location/idstools`. `DS_install_location` steht für die Installationsposition von IBM Security Directory Server. Nachstehend sind die Standardpositionen auf verschiedenen Betriebssystemen aufgeführt:

Betriebssysteme	Standardinstallationspositionen:
Microsoft Windows	c:\Program Files\IBM\ldap\V6.3.1
AIX und Solaris	/opt/IBM/ldap/V6.3.1
Linux	/opt/ibm/ldap/V6.3.1

3. Führen Sie den folgenden Befehl aus:

**Anmerkung:** Wenn Sie die integrierte Version von WebSphere Application Server an einer angepassten Position installiert haben, müssen Sie für den Befehl `deploy_IDSWebApp` auch die Parameter `-a`, `-w`, `-p` und `-r` angeben. Weitere Informationen zum Befehl `deploy_IDSWebApp` finden Sie in der Befehlssyntax, die durch die Eingabe von `deploy_IDSWebApp -h` angezeigt wird.

Betriebssysteme	Befehl:
Microsoft Windows	<code>deploy_IDSWebApp.bat -u</code>
AIX, Linux und Solaris	<code>deploy_IDSWebApp -u</code>





---

## Kapitel 17. Planung für die Instanzkonfiguration

Sie müssen die Konfigurationseinstellungen für Ihren Computer beschließen, bevor Sie die LDAP-Umgebung erstellen und konfigurieren.

Um eine Verzeichnisserverinstanz oder eine Proxy-Server-Instanz erstellen zu können, müssen Sie auf dem Computer zuerst eine Systembenutzer-ID erstellen, die Eigner der Instanz ist. Zum Speichern von Verzeichnisdaten in einer Verzeichnisserverinstanz müssen Sie die zu verwendende Codepage beschließen.

Für die Installation von IBM Security Directory Server und der dafür zusätzlich benötigten Softwareprodukte sowie für die Erstellung einer Verzeichnisserverinstanz müssen Sie Benutzer und Gruppen auf dem Computer erstellen. Für die Installation von für IBM Security Directory Server zusätzlich benötigten Softwareprodukten wie IBM DB2 müssen Sie eine Systembenutzer-ID für den DB2-Administrator erstellen.

---

### Benutzer und Gruppen, die einer Verzeichnisserverinstanz zugeordnet sind

Um eine Verzeichnisserverinstanz oder eine Proxy-Server-Instanz erstellen zu können, müssen Sie Benutzer und Gruppen mit den erforderlichen Berechtigungen erstellen.

Wenn Sie auf Ihrem Computer eine Instanz erstellen möchten, müssen Sie die Instanz mit einem Systembenutzer-ID verknüpfen. Diese Benutzer-ID ist der Verzeichnisserverinstanzeigner. Wenn eine Systembenutzer-ID für eine Instanz nicht vorhanden ist, müssen Sie eine Benutzer-ID auf dem Computer erstellen. Um eine Benutzer-ID für den Verzeichnisserverinstanzeigner, den Datenbankinstanzeigner und den Datenbankeigner zu erstellen, müssen Sie die Namenskonventionen befolgen. Weitere Informationen finden Sie im Kapitel „Namenskonventionen“ auf Seite 126.

Für einen vollständigen Verzeichnisserver müssen Sie außerdem Systembenutzer-IDs als Datenbankinstanzeigner und Datenbankeigner zuordnen. Sie können für alle drei Rollen dieselbe Benutzer-ID verwenden. Wenn Sie dieselbe Benutzer-ID für den Verzeichnisserverinstanzeigner, den Datenbankinstanzeigner und den Datenbankeigner verwenden, besitzen sie alle denselben Eigernamen.

Wenn Sie **Instance Administration Tool** zum Erstellen einer Verzeichnisserverinstanz verwenden, können Sie die Benutzer-ID für den Verzeichnisserverinstanzeigner mit dem Tool erstellen. Sie können auch den Befehl **idsadduser** zum Erstellen der Benutzer-ID für den Verzeichnisserverinstanzeigner verwenden. Mit diesem Befehl wird eine Benutzer-ID erstellt, die alle Anforderungen erfüllt.

Die Benutzer-ID, die Sie dem Verzeichnisserverinstanzeigner, dem Datenbankinstanzeigner und dem Datenbankeigner zuordnen, verfügt über die folgenden Rollen:

#### **Verzeichnisserverinstanzeigner**

Auf dem Computer, der als Verzeichnisserverinstanzeigner verwendet wird, muss eine Systembenutzer-ID vorhanden sein. Die Benutzer-ID des Verzeichnisserverinstanzeigners stimmt mit dem Namen der Verzeichnisserverinstanz überein.

serverinstanz überein. Diesem Benutzer wurden die Berechtigungen zum Verwalten der Verzeichnisserverinstanz zugewiesen.

Unter Windows haben Mitglieder der Administratorgruppe auch die Berechtigungen für die Verwaltung der Verzeichnisserverinstanz. Unter AIX, Linux und Solaris besitzt die Primärgruppe des Verzeichnisserverinstanzeigners auch die Berechtigungen zum Verwalten der Verzeichnisserverinstanz.

**Anmerkung:** Unter AIX, Linux und Solaris muss bei den Namen der Instanzeigner die Groß-/Kleinschreibung beachtet werden. Darüber hinaus müssen Sie hier den Namen und den Eigner der Verzeichnisserverinstanz exakt so angeben, wie die Benutzer-ID definiert wurde. Im folgenden Beispiel werden zwei unterschiedliche Eignernamen gezeigt: JoeSmith und joesmith.

#### **Datenbankinstanzeigner**

Die Benutzer-ID, die als Datenbankinstanzeigner verwendet wird, ist Eigner der Datenbankinstanz, die für eine Verzeichnisserverinstanz konfiguriert wurde. Der Datenbankinstanzname und der Name des Datenbankinstanzeigners sind identisch. Dieser Benutzer verwaltet die Datenbankinstanz. Der Verzeichnisserverinstanzeigner kann die Datenbankinstanz ebenfalls verwalten. Standardmäßig ist diese Benutzer-ID dieselbe wie die Benutzer-ID, die Verzeichnisserverinstanzeigner ist.

#### **Datenbankeigner**

Diese Benutzer-ID ist als Eigner der Datenbank definiert, die von der Verzeichnisserverinstanz zum Speichern von Verzeichnisdaten verwendet wird. Die Datenbank ist in der Datenbankinstanz gespeichert, deren Eigner der Datenbankinstanzeigner ist. In der Verzeichnisserverinstanz werden die Benutzer-ID des Datenbankeigners und das dazugehörige Kennwort zum Herstellen einer Verbindung mit der Datenbank verwendet.

## **Namenskonventionen**

Die Benutzer-ID und die Primärgruppe für eine Verzeichnisserverinstanz müssen den Namenskonventionsrichtlinien entsprechen.

Die Anforderungen der Namenskonventionen gelten für die folgenden Benutzer-IDs:

- Name der Verzeichnisserverinstanz (d. h. Benutzer-ID, die als Verzeichnisserverinstanzeigner definiert ist).
- Name der Datenbankinstanz (d. h. Benutzer-ID, die als Datenbankinstanzeigner definiert ist). Diese Benutzer-ID ist in der Regel dieselbe wie der Name der Verzeichnisserverinstanz.
- Auf AIX-, Linux- und Solaris-Systemen: Primärgruppen der Benutzer-ID für den Verzeichnisserverinstanzeigner und der Benutzer-ID für den Datenbankinstanzeigner.

**Anmerkung:** Wenn Sie eine Benutzer-ID und -gruppe erstellen, müssen Sie die entsprechenden Berechtigungen zuweisen. Weitere Informationen finden Sie unter „Anforderungen für die Erstellung von Benutzern und Gruppen“ auf Seite 127.

Die IDs der Benutzer und Gruppen müssen die folgenden Anforderungen erfüllen:

- Der Name darf maximal 8 Zeichen umfassen.
- Es darf keiner der folgenden Namen verwendet werden:

- USERS
- ADMINS
- GUESTS
- PUBLIC
- LOCAL
- idslldap
- Der Name darf mit keinem der folgenden Präfixe beginnen:
  - IBM
  - SQL
  - SYS
- Der Name darf keine Sonderzeichen oder Zeichen mit Akzent enthalten.
- Der Name darf nur die folgenden Zeichen enthalten:
  - A - Z
  - a - z
  - 0 - 9
  - \_ (Unterstrichungszeichen)
- Der Name muss mit einem der folgenden Zeichen beginnen:
  - A - Z
  - a - z

## Anforderungen für die Erstellung von Benutzern und Gruppen

Wenn Sie für Ihre Instanz Benutzer und Gruppen erstellen, müssen Sie Benutzern und Gruppen entsprechende Berechtigungen zuweisen und sie den passenden Gruppen als Mitglieder hinzufügen.

Wenn Sie die für Ihre Instanz erforderlichen Benutzer und Gruppen erstellt haben, müssen Sie ihnen die entsprechenden Berechtigungen zuweisen und die Benutzer den passenden Gruppen hinzufügen. Für Benutzer- und Gruppen-IDs müssen die folgenden Anforderungen erfüllt sein:

### Windows

- Fügen Sie den Verzeichnisserverinstanzeigner und den Datenbankinstanzeigner als Mitglieder der Administratorgruppe hinzu.
- Legen Sie für den Datenbankinstanzeigner eine gültige Ländereinstellung für die Sprache fest, in der Nachrichten des Servers erstellt werden sollen. Melden Sie sich bei Bedarf als Benutzer an und ändern Sie die Ländereinstellung in den entsprechenden Wert.

### AIX, Linux und Solaris

- Fügen Sie die Root-ID als Mitglied der Primärgruppe des Verzeichnisserverinstanzeigners und des Datenbankinstanzeigners hinzu.
- Fügen Sie die Root-ID als Mitglied der Gruppe idslldap hinzu.
- Fügen Sie den Verzeichnisserverinstanzeigner und den Datenbankinstanzeigner als Mitglieder der Gruppe idslldap hinzu.
- Erstellen Sie Ausgangsverzeichnisse für den Verzeichnisserverinstanzeigner und den Datenbankinstanzeigner.
- Weisen Sie die entsprechenden Berechtigungen für das Ausgangsverzeichnis des Verzeichnisserverinstanzeigners zu.
  - Der Verzeichnisserverinstanzeigner verfügt über das Benutzerbesitzrecht für die Instanz.

- Die Primärgruppe des Verzeichnisserverinstanzeigners verfügt über das Gruppenbesitzrecht für die Instanz.
- Sie müssen dem Verzeichnisserverinstanzeigner und dessen Primärgruppe Lese-, Schreib- und Ausführungsrechte für das Ausgangsverzeichnis zuweisen.
- Weisen Sie Lese-, Schreib- und Ausführungszugriff auf die Position, in der die Datenbank für den Verzeichnisserverinstanzeigner und dessen Primärgruppe erstellt wurde, zu.
- Der Verzeichnisserverinstanzeigner und der Datenbankinstanzeigner für eine Verzeichnisserverinstanz können unterschiedliche Benutzer sein. In diesem Fall muss der Verzeichnisserverinstanzeigner Mitglied der Primärgruppe des Datenbankinstanzeigners sein.
- Wenn der Verzeichnisserverinstanzeigner, der DB2-Instanzeigner und der Datenbankeigner unterschiedliche Benutzer sind, müssen sie alle Mitglieder derselben Gruppe sein.
- Legen Sie das Korn-Shell-Script (`/usr/bin/ksh`) als Anmeldeshell für den Verzeichnisserverinstanzeigner, den Datenbankinstanzeigner und den Datenbankeigner fest.

Das Kennwort für den Verzeichnisserverinstanzeigner, den Datenbankinstanzeigner und den Datenbankeigner muss ordnungsgemäß festgelegt und zur Verwendung bereit sein. Das Kennwort darf nicht abgelaufen sein oder die Erstvalidierung noch nicht durchlaufen haben. Ob das Kennwort ordnungsgemäß festgelegt wurde, können Sie überprüfen, indem Sie auf dem Computer auf Telnet zugreifen und sich mit der Benutzer-ID und dem zugehörigen Kennwort anmelden.

Bei der Konfiguration der Datenbank wird in der Regel das Ausgangsverzeichnis des Datenbankinstanzeigners als Position der Datenbank angegeben. Dies ist jedoch nicht zwingend erforderlich. Wenn Sie eine andere Position angeben, müssen im Ausgangsverzeichnis des Datenbankinstanzeigners 3 bis 4 MB Speicherplatz verfügbar sein. In DB2 werden Links erstellt und Dateien zum Ausgangsverzeichnis des Datenbankinstanzeigners hinzugefügt, auch wenn sich die Datenbank selbst in einer anderen Speicherposition befindet. Wenn auf dem Computer im Ausgangsverzeichnis des Datenbankinstanzeigners nicht genügend Speicherplatz zur Verfügung steht, können Sie ausreichend Speicherbereich freigeben oder das Ausgangsverzeichnis ändern.

## Beispiele

Um einen Instanzeigner zu erstellen, der die Anforderungen an einen Verzeichnisserverinstanzeigner erfüllt, können Sie den Befehl **idsadduser** ausführen. Der Befehl **idsadduser** befindet sich im Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.

### Beispiel 1:

Um unter AIX, Linux oder Solaris einen Benutzeraccount mit den folgenden Werten zu erstellen, führen Sie den Befehl **idsadduser** aus:

- Benutzername: JoeSmith
- Primärgruppe: employees
- Ausgangsverzeichnis: `/home/joe` (Verwenden Sie unter Solaris `/export/home/joe`)
- Kennwort: joespw

```
idsadduser -u JoeSmith -g employees -l /home/joe -w joespw
```

### Beispiel 2:

Um als Mitglied der Administratorgruppe unter Windows einen Benutzeraccount mit den folgenden Werten zu erstellen, führen Sie den Befehl **idsadduser** aus:

- Benutzername: JoeSmith
- Kennwort: joespw

```
idsadduser -u JoeSmith -w joespw
```

---

## Konfigurationsplanung

Für Ihre Verzeichnisserverumgebung müssen Sie den zu speichernden Datentyp, die Datenstruktur und die festzulegende Datensicherheit auswählen.

Treffen Sie zu den folgenden Punkten Entscheidungen, bevor Sie die Datenbank konfigurieren und füllen:

### Der im Verzeichnisserver zu speichernde Datentyp

Sie müssen entscheiden, welches Schema Sie für Ihren Verzeichnisserver verwenden möchten und welcher Datentyp in Ihrem Verzeichnisserver gespeichert werden soll. Der Verzeichnisserver umfasst einen Standardsatz an Attributtypdefinitionen und Objektklassendefinitionen. Um Ihre Daten anzupassen, sollten Sie Ihren angepassten Attributtyp und Objektklassendefinitionen hinzufügen, bevor Sie Einträge zum Verzeichnisserver hinzufügen.

An Schemas können Hinzufügungen oder Änderungen vorgenommen werden, wenn das Verzeichnis mit Daten gefüllt wurde. Für Schemaänderungen müssen Daten in manchen Fällen möglicherweise entfernt und erneut geladen werden.

### Die zu verwendende Codepage

Entscheiden Sie, ob Sie die Datenbank mit der lokalen Codepage oder mithilfe von UTF-8 (Universalzeichensatz) erstellen möchten. Wenn Sie eine lokale Codepage auswählen, wird aktiviert, dass IBM Security Directory Server-Anwendungen und -Benutzer Suchergebnisse in der für die jeweilige Sprache erwarteten Sortierfolge erhalten. Wenn Sie jedoch eine lokale Codepage verwenden, werden die Daten in dieser bestimmten Codepage im Verzeichnis gespeichert. Wenn Sie UTF-8 verwenden, können Sie alle UTF-8-Zeichendaten im Verzeichnis speichern. Weitere Informationen zu UTF-8 finden Sie in „UTF-8-Unterstützung“ auf Seite 130.

**Anmerkung:** Wenn Sie Sprachentags verwenden möchten, müssen Sie UTF-8 als Codepage für die Datenbank verwenden.

### Die hierarchische Struktur zum Speichern der Verzeichnisdaten

IBM Security Directory Server speichert Verzeichnisdaten in einer hierarchischen Baumstruktur. Die Namen der Einträge im Verzeichnis basieren auf der relativen Position der Einträge innerhalb der Baumstruktur. Es ist wichtig, eine für die LDAP-Umgebung geeignete logische Organisation im Verzeichnis zu definieren. Mit einer logischen Organisation ist es für Clients einfacher zu bestimmen, welcher Ast des Baumes für die erforderlichen Informationen durchsucht werden muss.

### Die Anforderungen an die Datensicherheit

Um den Zugriff auf die Verzeichnisdaten über einen nicht gesicherten Port zu verhindern, können Sie den Verzeichnisserver für sichere Kommunikation konfigurieren. Weitere Informationen zum Sichern der Daten finden Sie im Abschnitt Verwaltung der IBM Security Directory Server-Dokumentation.

### Die erforderlichen Zugriffsberechtigungen für die Verzeichnisdaten

Informationen zur Verwendung von Zugriffsberechtigungen finden Sie in den Zugriffskontrolllisten im Abschnitt Verwaltung der IBM Security Directory Server-Dokumentation.

### Notwendigkeit eines Proxy-Servers

Wenn die Verzeichnisdaten groß sind und die Umgebung viel Schreiben erfordert, ziehen Sie die Verwendung eines Proxy-Servers in Betracht. Die erforderliche Skalierung kann möglicherweise mit großen Verzeichnisumgebungen, die viel Lesen erfordern, durch Konfigurieren von Replikationen erreicht werden. Lesen Sie sich, bevor Sie sich dazu entscheiden, einen Proxy-Server zu verwenden, die Liste der unterstützten Features bei Proxy-Servern im Abschnitt Verwaltung der IBM Security Directory Server-Dokumentation durch.

---

## UTF-8-Unterstützung

Sie können einen Verzeichnisserver zum Speichern aller Landessprachenzeichen konfigurieren, die in UTF-8 dargestellt werden können.

IBM Security Directory Server unterstützt über den Zeichensatz UTF-8 (UCS Transformation Format) eine Vielzahl von Zeichen verschiedener Landessprachen. Im Protokoll LDAP Version 3 liegen alle Zeichendaten, mit denen LDAP-Clients und -Server kommunizieren, in UTF-8 vor.

Der Server bestimmt die Typen von Zeichen, die gespeichert und durchsucht werden können anhand der Codepage, die für die Konfiguration einer Datenbank verwendet wird. Sie können den Datenbankzeichensatz auf UTF-8 festlegen oder den lokalen Zeichensatz des Systems, auf dem sich der Server befindet, verwenden. Der lokale Zeichensatz basiert auf den Ländereinstellungen, der Sprache und der Codepage-Umgebung auf dem System.

Bei Angabe von UTF-8 können UTF-8-Zeichendaten im Verzeichnis gespeichert werden. LDAP-Clients auf einem System, das alle UTF-8-unterstützten Sprachen unterstützt, können ordnungsgemäß auf das Verzeichnis zugreifen und es durchsuchen. Wenn sich die LDAP-Clients auf einem System mit einem lokalen Zeichensatz befindet, können die Ergebnisse, die vom Server in einem bestimmten Zeichensatz abgerufen werden, möglicherweise nicht korrekt ordnungsgemäß vom Client angezeigt werden.

Wenn Sie eine UTF-8-Datenbank verwenden, verbessert sich die Datenbankleistung, da beim Speichern oder Anrufen von Daten von der Datenbank keine Datenkonvertierung erforderlich ist.

**Anmerkung:** Wenn Sie Sprachentags einsetzen wollen, muss die Datenbank im UTF-8-Format definiert sein.

## UTF-8 in einem Verzeichnisserver verwenden

Um entscheiden zu können, welche Codepage verwendet werden soll, müssen Sie wissen, wie ein Verzeichnisserver Codepages zum Speichern von und Zugreifen auf Verzeichnisdaten verwendet.

UTF-8-Datenbanken besitzen eine festgelegte Sortierfolge, nämlich die Binärreihenfolge der UTF-8-Zeichen. Es ist nicht möglich, in einer UTF-8-Datenbank eine sprachspezifische Sortierung vorzunehmen.

Damit Ihre LDAP-Anwendungen oder -Benutzer die folgenden Ergebnisse abrufen können, ist UTF-8 möglicherweise nicht der passende Zeichensatz für Ihre Datenbank:

- Suchvorgänge mit Sortierfiltern wie "name >= SMITH" und wenn die Reihenfolge ähnlich Ihren Ländereinstellungen sein soll.
- Suchvorgänge mit dem Steuerelement zum Sortieren der Ergebnisse und wenn die Reihenfolge ähnlich Ihren Ländereinstellungen sein soll.

In diesen Fällen müssen das LDAP-Serversystem und alle Clientsysteme mit demselben Zeichensatz und denselben Ländereinstellungen ausgeführt werden.

Eine mit den spanischen Ländereinstellungen konfigurierte LDAP-Serverdatenbank gibt zum Beispiel Suchergebnisse auf der Grundlage der Zeichen sortiert aus, wie es bei spanischsprachigen Clients erwartet wird. Durch derartige Konfigurationsbeschränkungen wird Ihre Verzeichnisbenutzercommunity auf einen einzigen Zeichensatz in dieser Ländereinstellung und auf eine einzige Sortierfolge beschränkt.

## LDIF-Dateien mit UTF-8-Werten mithilfe von Serverdienstprogrammen erstellen

Sie können die Erweiterung charset zum Erstellen eines LDIF-Formats mit UTF-8-Werten verwenden.

Die manuelle Erstellung einer LDIF-Datei, die UTF-8-Werte enthält, ist schwierig. Im LDIF-Dateiheader können Sie die Erweiterung angeben, die einen IANA-Zeichensatznamen (Internet Assigned Numbers Authority) unterstützt, sowie die Versionsnummer. Weitere Informationen zu den unterstützten IANA-Zeichensätzen finden Sie im Kapitel „Unterstützte IANA-Zeichensätze“ auf Seite 132.

### Beispiele

#### Beispiel 1:

Verwenden Sie das Tag charset, damit die Serverdienstprogramme automatisch vom angegebenen Zeichensatz in UTF-8 konvertiert werden.

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, ou=University of New Mexico, o=sample
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
title: Associate Dean
title: [title in Spanish]
jpegPhoto:< file:///usr/local/photos/jgriego.jpg
```

Im folgenden Beispiel werden alle Attributnamen mit Werten, die durch einzelne Punkte voneinander getrennt sind, vom Zeichensatz ISO-8859-1 in UTF-8 umgesetzt. Alle Attributnamen mit Werten, die mithilfe von Doppelpunkten voneinander getrennt werden, wie zum Beispiel description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd, müssen Base64-kodiert sein und in Binär- oder UTF-8-Zeichenfolgen vorliegen. Wenn Werte aus einer Datei ausgelesen werden, wie zum Beispiel das Attribut jpegPhoto, das von der Webadresse angegeben wurde, müssen diese ebenfalls binär oder in UTF-8 vorliegen. Für solche Attributwerte wird keine Umsetzung vom angegebenen charset (Zeichensatz) in UTF-8 durchgeführt.

## Beispiel 2:

Im folgenden Beispiel wird erwartet, dass der Inhalt einer LDIF-Datei ohne das Tag charset in UTF-8 vorliegt.

```
# IBM Directorysample LDIF file
#
# The suffix "o=sample" should be defined before attempting to load
# this data.
```

```
version: 1
```

```
dn: o=sample
objectclass: top
objectclass: organization
o: sample
```

```
dn: ou=Austin, o=sample
ou: Austin
objectclass: organizationalUnit
seealso: cn=Mary Smith, ou=Austin, o=sample
```

In IBM Security Directory Server kann die LDIF-Datei mit dem folgenden Inhalt ohne die Kopfzeileninformationen `version: 1` verwendet werden.

```
# IBM Directorysample LDIF file
#
#The suffix "o=sample" should be defined before attempting to load
#this data.
```

```
dn: o=sample
objectclass: top
objectclass: organization
o: sample
```

```
dn: ou=Austin, o=sample
ou: Austin
objectclass: organizationalUnit
seealso: cn=Linda Carlesberg, ou=Austin, o=sample
```

## Unterstützte IANA-Zeichensätze

Sie können IANA-Zeichensatznamen (Internet Assigned Number Authority) in einer LDIF-Datei oder in der C Client-Schnittstelle verwenden, um den Zeichensatz der Verzeichnisdaten zu ermitteln.

IBM Security Directory Server unterstützt die IANA-Zeichensatznamen (Internet Assigned Numbers Authority) nach Betriebssystem.

Weitere Informationen zu IANA-registrierten Zeichensätzen finden Sie auf der Website Character Sets unter [www.iana.org/assignments/character-sets](http://www.iana.org/assignments/character-sets).

Tabelle 38. Von IANA definierte Zeichensätze

Zeichen	Ländereinstellung					DB2-Codepage	
	HP-UX	Linux, Linux_390,	Windows	AIX	Solaris	UNIX	Windows
ISO-8859-1	X	X	X	X	X	819	1252
ISO-8859-2	X	X	X	X	X	912	1250
ISO-8859-5	X	X	X	X	X	915	1251
ISO-8859-6	X	X	X	X	X	1089	1256
ISO-8859-7	X	X	X	X	X	813	1253
ISO-8859-8	X	X	X	X	X	916	1255



Tabelle 38. Von IANA definierte Zeichensätze (Forts.)

Zeichen	Ländereinstellung					DB2-Codepage	
	HP-UX	Linux, Linux_390,	Windows	AIX	Solaris	UNIX	Windows
ISO-8859-9	X	X	X	X	X	920	1254
ISO-8859-15	X	Nicht zutreffend	X	X	X		
IBM437	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend	437	437
IBM850	Nicht zutreffend	Nicht zutreffend	X	X	Nicht zutreffend	850	850
IBM852	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend	852	852
IBM857	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend	857	857
IBM862	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend	862	862
IBM864	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend	864	864
IBM866	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend	866	866
IBM869	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend	869	869
IBM1250	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend		
IBM1251	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend		
IBM1253	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend		
IBM1254	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend		
IBM1255	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend		
IBM1256	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend		
TIS-620	Nicht zutreffend	Nicht zutreffend	X	X	Nicht zutreffend	874	874
EUC-JP	X	X	Nicht zutreffend	X	X	954	Nicht zutreffend
EUC-KR	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	X	X	970	Nicht zutreffend
EUC-CN	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	X	X	1383	Nicht zutreffend
EUC-TW	X	Nicht zutreffend	Nicht zutreffend	X	X	964	Nicht zutreffend
Shift-JIS	Nicht zutreffend	X	X	X	X	932	943
KSC	Nicht zutreffend	Nicht zutreffend	X	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	949
GBK	Nicht zutreffend	Nicht zutreffend	X	X	Nicht zutreffend	1386	1386
Big5	X	Nicht zutreffend	X	X	X	950	950
GB18030	Nicht zutreffend	X	X	X	X		

Tabelle 38. Von IANA definierte Zeichensätze (Forts.)

Zeichen	Ländereinstellung					DB2-Codepage	
	HP-UX	Linux, Linux_390,	Windows	AIX	Solaris	UNIX	Windows
HP15CN	X (ohne GB18030)						

**Anmerkung:**

- Der chinesische Standardzeichensatz GB18030 wird von den entsprechenden Patches unterstützt. Diese sind unter [www.oracle.com](http://www.oracle.com) und [www.microsoft.com](http://www.microsoft.com) verfügbar.
- Bei Windows-Betriebssystemen muss die Umgebungsvariable `zhCNGB18030` auf TRUE gesetzt werden.

## ASCII-Zeichen von 33 bis 126

Ermitteln Sie mithilfe der ASCII-Zeichentabelle, welche Zeichen als Seedwert und Saltwert für die Verschlüsselung einer Verzeichnisserverinstanz zu verwenden sind.

Sie können im Seedwert und im Saltwert für die Verschlüsselung die ASCII-Zeichen von 33 bis 126 verwenden.

Tabelle 39. ASCII-Zeichen von 33 bis 126

ASCII-Code	Zeichen	ASCII-Code	Zeichen	ASCII-Code	Zeichen
33	! Ausrufezeichen	34	" Doppeltes Anführungszeichen	35	# Nummernzeichen
36	\$ Dollarzeichen	37	% Prozentzeichen	38	& Et-Zeichen
39	' Apostroph	40	( Linke runde Klammer	41	) Rechte runde Klammer
42	* Stern	43	+ Pluszeichen	44	, Komma
45	- Silbentrennungsstrich	46	. Punkt	47	/ Schrägstrich
48	0	49	1	50	2
51	3	52	4	53	5
54	6	55	7	56	8
57	9	58	: Doppelpunkt	59	; Semikolon
60	< Kleiner-als-Zeichen	61	= Gleichheitszeichen	62	> Größer-als-Zeichen
63	? Fragezeichen	64	@ Kommerzielles A	65	A Großschreibung für a
66	B Großschreibung für b	67	C Großschreibung für c	68	D Großschreibung für d
69	E Großschreibung für e	70	F Großschreibung für f	71	G Großschreibung für g
72	H Großschreibung für h	73	I Großschreibung für i	74	J Großschreibung für j
75	K Großschreibung für k	76	L Großschreibung für l	77	M Großschreibung für m
78	N Großschreibung für n	79	O Großschreibung für o	80	P Großschreibung für p
81	Q Großschreibung für q	82	R Großschreibung für r	83	S Großschreibung für s
84	T Großschreibung für t	85	U Großschreibung für u	86	V Großschreibung für v
87	W Großschreibung für w	88	X Großschreibung für x	89	Y Großschreibung für y
90	Z Großschreibung für z	91	[ Linke eckige Klammer	92	\ Backslash

Tabelle 39. ASCII-Zeichen von 33 bis 126 (Forts.)

ASCII-Code	Zeichen	ASCII-Code	Zeichen	ASCII-Code	Zeichen
93	] Rechte eckige Klammer	94	^ Winkelzeichen	95	_ Unterstreichungszeichen
96	˘ Gravis	97	a Kleinschreibung für a	98	b Kleinschreibung für b
99	c Kleinschreibung für c	100	d Kleinschreibung für d	101	e Kleinschreibung für e
102	f Kleinschreibung für f	103	g Kleinschreibung für g	104	h Kleinschreibung für h
105	i Kleinschreibung für i	106	j Kleinschreibung für j	107	k Kleinschreibung für k
108	l Kleinschreibung für l	109	m Kleinschreibung für m	110	n Kleinschreibung für n
111	o Kleinschreibung für o	112	p Kleinschreibung für p	113	q Kleinschreibung für q
114	r Kleinschreibung für r	115	s Kleinschreibung für s	116	t Kleinschreibung für t
117	u Kleinschreibung für u	118	v Kleinschreibung für v	119	w Kleinschreibung für w
120	x Kleinschreibung für x	121	y Kleinschreibung für y	122	z Kleinschreibung für z
123	{ Linke geschweifte Klammer	124	Vertikaler Balken	125	} Rechte geschweifte Klammer
126	~ Tilde				



---

## Kapitel 18. Instanzerstellung und -verwaltung

Um einen Verzeichnisserver in einer Identitätsinfrastruktur verwenden zu können, müssen Sie eine Ihren Anforderungen entsprechende Verzeichnisserverinstanz erstellen.

Wenn die Installation von IBM Security Directory Server abgeschlossen ist, müssen Sie eine Verzeichnisserverinstanz erstellen und dann den Administrator-DN und das Kennwort für die Instanz festlegen. Sie können einen vollständigen Verzeichnisserver oder einen Proxy-Server erstellen. Um eine Verzeichnisserverinstanz oder eine Proxy-Server-Instanz erstellen zu können, müssen Sie auf dem Computer eine Systembenutzer-ID erstellen. Die Systembenutzer-ID ist der Verzeichnisserverinstanzeigner oder der Proxy-Server-Instanzeigner.

Für einen vollständigen Verzeichnisserver müssen Sie eine DB2-Datenbank erstellen und die Datenbank mit der Verzeichnisserverinstanz konfigurieren. Damit eine DB2-Datenbank erstellt werden kann, muss eine unterstützte DB2-Version auf dem Computer installiert sein. Überprüfen Sie, ob die Datei `ldapdb.properties` mit dem DB2-Installationspfad und der DB2-Version aktualisiert wurde. Weitere Informationen hierzu finden Sie unter Anhang C, „Datei `ldapdb.properties` manuell aktualisieren“, auf Seite 263.

**Anmerkung:** Wenn Sie IBM Security Directory Server **Instance Administration Tool (idsxinst)** verwenden, um eine vollständige Verzeichnisserverinstanz zu erstellen, wird auch die Datei `ldapdb.properties` im Ausgangsverzeichnis der Instanz erstellt. Unter Windows befindet sich die Datei `ldapdb.properties` im Verzeichnis `instance_home\idsslapd-instance_name\etc`. Unter AIX, Linux und Solaris befindet sich die Datei im Verzeichnis `instance_home/idsslapd-instance_name/etc`.

Erstellen und konfigurieren Sie für eine Proxy-Server-Instanz keine DB2-Datenbank mit der Proxy-Server-Instanz.

**Instance Administration Tool** ist eine grafische Benutzeroberfläche (Graphical User Interface, GUI), mit der Sie Verzeichnisserverinstanzen erstellen und verwalten können. Für die Verwendung von **Instance Administration Tool** ist IBM Java Development Kit erforderlich. Wenn Sie **Instance Administration Tool** verwenden, wird ein Assistent bereitgestellt, der Sie beim Abschließen der Task unterstützt.

Sie können **Instance Administration Tool** zum Erstellen, Anzeigen, Kopieren und Ändern von Informationen zu Instanzen sowie zum Löschen von Instanzen verwenden. Sie können das Tool auch verwenden, um die Benutzer, die Verzeichnisserverinstanzeigner sind, zu erstellen oder zu bearbeiten und Upgrades von Instanzen von Vorgängerversionen von IBM Security Directory Server durchzuführen. Sie können **Instance Administration Tool** zum Starten oder Stoppen des Servers oder des Verwaltungsservers für Ihre Instanzen verwenden. Sie können das **Konfigurationstool** auch von **Instance Administration Tool** aus öffnen.

Sie können außerdem die Befehlszeilendienstprogramme verwenden, um Verzeichnisserverinstanzen zu erstellen und zu verwalten.

---

## Instance Administration Tool starten

Starten Sie das **Instance Administration Tool**, um eine Verzeichnisserverinstanz oder eine Proxy-Server-Instanz zu erstellen oder zu verwalten.

### Vorbereitende Schritte

Zur Verwendung des **Instance Administration Tools** müssen Sie IBM Security Directory Server mit dem Server- und/oder dem Proxy-Server-Feature installieren. Melden Sie sich mit den folgenden Berechtigungsnachweisen an, um das **Instance Administration Tool** auszuführen:

#### AIX, Linux und Solaris

Melden Sie sich als Rootbenutzer an.

#### Windows

Melden Sie sich als Mitglied der Administratorgruppe an.

Im Installationspfad von IBM Security Directory Server muss IBM Java Development Kit vorhanden sein. Den Standardinstallationspfad von IBM Security Directory Server finden Sie unter „Standardinstallationspositionen“ auf Seite 28.

### Vorgehensweise

Wählen Sie eine der folgenden Optionen aus, um das **Instance Administration Tool** zu starten:

Optionen zum Öffnen des Instance Administration Tools	Befehl:
Installation des Server-Features von IBM Security Directory Server	Klicken Sie auf der Übersichtsseite auf <b>Instance Administration Tool (idsxinst)</b> . Weitere Informationen hierzu finden Sie unter „Installation mit IBM Installation Manager“ auf Seite 32.

Optionen zum Öffnen des Instance Administration Tools	<b>Befehl:</b>
Befehl <code>idsxinst</code>	<p><b>Windows</b></p> <ol style="list-style-type: none"> <li>1. Ändern Sie das aktuelle Verzeichnis in das Verzeichnis <code>sbin</code> der Installationsposition von IBM Security Directory Server.</li> <li>2. Führen Sie den Befehl <code>idsxinst</code> aus.</li> </ol> <p><b>Anmerkung:</b> Sie können auch auf <b>Start &gt; Alle Programme &gt; IBM Security Directory Server 6.3.1 &gt; Instance Administration Tool</b> klicken.</p> <p><b>AIX, Linux und Solaris</b></p> <ol style="list-style-type: none"> <li>1. Ändern Sie das aktuelle Verzeichnis in das Verzeichnis <code>sbin</code> der Installationsposition von IBM Security Directory Server.</li> <li>2. Führen Sie den Befehl <code>idsxinst</code> aus.</li> </ol> <p>Weitere Informationen zum Installationspfad von IBM Security Directory Server finden Sie unter „Standardinstallationspositionen“ auf Seite 28.</p>

## Instance Administration Tool für das Upgrade einer Instanz starten

Führen Sie das **Instance Administration Tool** mit Parametern aus, um das **Instance Administration Tool** zu öffnen und ein Upgrade einer fernen Instanz durchzuführen, die Sicherungsdaten enthält.

### Vorbereitende Schritte

Zum Durchführen eines Upgrades einer fernen Instanz müssen Sie die folgenden Anforderungen erfüllen:

- Ihr Computer muss die mit dem Befehl `migbkup` erstellten Sicherungsdaten der Instanz enthalten. Sie müssen die Version des Befehls `migbkup` verwenden, auf die Sie das Upgrade der fernen Instanz durchführen wollen.
- Melden Sie sich unter AIX, Linux und Solaris als Root an. Melden Sie sich unter Windows als Mitglied der Administratorgruppe an.

### Vorgehensweise

1. Öffnen Sie die Eingabeaufforderung.
2. Ändern Sie Ihr aktuelles Arbeitsverzeichnis in das Verzeichnis `sbin` der Installationsposition von IBM Security Directory Server. Weitere Informationen zum Standardinstallationspfad finden Sie im Kapitel „Standardinstallationspositionen“ auf Seite 28.
3. Führen Sie den Befehl `idsxinst` im folgenden Format aus:  
`idsxinst -migrate backup_directory`

Setzen Sie für die Variable *backup\_directory* die Position ein, an der Sie die mit dem Befehl **migbkup** erstellten Sicherungsdaten der Instanz gespeichert haben.

---

## Erstellung von Verzeichnisserverinstanzen

Um eine Verzeichnisserverinstanz in einer LDAP-Umgebung verwenden zu können, müssen Sie eine Instanz erstellen, die in Bezug auf die Verschlüsselung mit der vorhandenen Instanz synchronisiert wird, um die optimale Leistung zu erreichen.

Wenn Sie eine Verzeichnisserverinstanz als Kopie einer bereits vorhandenen Verzeichnisserverinstanz erstellen, werden diese beiden Verzeichnisserverinstanzen in Bezug auf die Verschlüsselung synchronisiert. Sie müssen sie nicht synchronisieren.

Wenn Sie eine Instanz erstellen, die keine Kopie einer vorhandenen Instanz ist, synchronisieren Sie die Instanz in Bezug auf die Verschlüsselung mit der vorhandenen Instanz. Sie müssen die Serverinstanzen in Bezug auf die Verschlüsselung synchronisieren, um in der folgenden Umgebung die optimale Leistung zu erreichen:

- Replikation
- Verteiltes Verzeichnis
- Import und Export von LDIF-Daten zwischen Serverinstanzen

Sie müssen die Serverinstanzen synchronisieren, bevor Sie eine der folgenden Operationen durchführen:

- Starten Sie die neue Serverinstanz.
- Führen Sie auf der Serverinstanz den Befehl **idsbulkload** aus.
- Führen Sie auf der Serverinstanz den Befehl **idsldif2db** aus.

Weitere Informationen zum Synchronisieren von Verzeichnissen finden Sie im Abschnitt *Verwaltung* der IBM Security Directory Server-Dokumentation.

Führen Sie ein Backup der Verzeichnisserverinstanz durch, wenn Sie eine Verzeichnisserverinstanz erstellt und diese mit einer DB2-Datenbank konfiguriert haben. Sichern Sie dabei die Konfiguration, das Schema, die DB2-Datenbank und die Verzeichnisschlüssel-Stashdateien. Sie können den Befehl **idsdbback** verwenden, um ein Backup einer Verzeichnisserverinstanz durchzuführen. Mit dem Befehl **idsdbrestore** können Sie bei Bedarf die Schlüssel-Stashdateien wiederherstellen. Weitere Informationen zu den Befehlen für die Sicherung und Wiederherstellung finden Sie in der *Befehlsreferenz*.

---

## Instanzerstellung mit Instance Administration Tool

Sie müssen die Anforderungen Ihrer Umgebung beurteilen und eine Verzeichnisserverinstanz in einer Phase erstellen, die für Ihre Umgebung zutreffend ist.

Sie können **Instance Administration Tool** zum Erstellen von Instanzen auf unterschiedliche Arten verwenden:

- Erstellen einer Standardinstanz mit einem Standardnamen und weiteren Einstellungen. Siehe „Standardverzeichnisserverinstanz erstellen“ auf Seite 141.
- Erstellen Sie eine Instanz mit benutzerdefinierten Einstellungen. Siehe „Verzeichnisserverinstanz mit angepassten Einstellungen erstellen“ auf Seite 143.
- Führen Sie ein Upgrade von einer Vorgängerversion von IBM Security Directory Server durch. Informationen dazu finden Sie im Kapitel „Upgrade einer Instanz“.



einer Vorgängerversion mit dem Befehl **idsimigr** durchführen“ auf Seite 96 oder „Upgrade einer Instanz einer Vorgängerversion mit dem **Instance Administration Tool** durchführen“ auf Seite 156.

- Erstellen Sie eine Instanz, die eine Kopie einer vorhandenen Instanz auf diesem oder einem anderen Computer ist. Siehe „Kopie einer vorhandenen Instanz mit dem **Instance Administration Tool** erstellen“ auf Seite 162.

## Standardverzeichnisserverinstanz erstellen

Erstellen Sie mithilfe der Option zur Erstellung der Standardinstanz eine Verzeichnisserverinstanz mit dem vordefinierten Instanznamen und den Standardeinstellungen.

### Vorbereitende Schritte

Führen Sie die folgenden Tasks aus, um eine Standardinstanz zu erstellen:

1. Installieren Sie IBM Security Directory Server mit dem Server-Feature. Siehe „Installation mit IBM Installation Manager“ auf Seite 32.
2. Installieren Sie IBM DB2. Siehe „Installation mit IBM Installation Manager“ auf Seite 32.
3. Überprüfen Sie, ob die Datei `ldapdb.properties` Angaben zum Installationspfad und der Version von DB2 enthält. Siehe Anhang C, „Datei `ldapdb.properties` manuell aktualisieren“, auf Seite 263.

### Informationen zu diesem Vorgang

Wenn sich auf Ihrem Computer eine Verzeichnisserverinstanz mit dem Standardinstanznamen befindet, können Sie die Standardverzeichnisserverinstanz nicht erstellen.

Die Standardverzeichnisserverinstanz weist die folgenden Einstellungen auf, die nicht geändert werden können:

*Tabelle 40. Einstellungen für eine Standardverzeichnisserverinstanz*

Einstellungen	Microsoft Windows	AIX und Linux	Solaris
Name	dsrdbm01	dsrdbm01	dsrdbm01
Instanzposition	c:\idsslapd-dsrdbm01	/home/dsrdbm01	/export/home/dsrdbm01
Gruppenname	Administrators	grrdbm01	grrdbm01
Administrator-DN	cn=root	cn=root	cn=root
Datenbankname	dsrdbm01	dsrdbm01	dsrdbm01

Der DB2-Tabellenbereich für die Standardverzeichnisserverinstanz ist DMS (DMS = Database Managed Storage).

Das **Instance Administration Tool** erstellt für die Standardverzeichnisserverinstanz das Suffix `o=sample`. Später können mithilfe des **Konfigurationstools** oder mit dem Befehl **idscfgsuf** weitere Suffixe hinzugefügt werden. Weitere Informationen hierzu finden Sie unter „Suffixkonfiguration“ auf Seite 213.

### Vorgehensweise

1. Starten Sie das **Instance Administration Tool**. Siehe „**Instance Administration Tool** starten“ auf Seite 138.

2. Klicken Sie auf **Instanzen erstellen**.
3. Führen Sie im Fenster **Neue Verzeichnisserverinstanz erstellen** die folgenden Schritte aus:
  - a. Klicken Sie auf **Standardinstanz erstellen**.
  - b. Klicken Sie auf **Weiter**.
  - c. Geben Sie im Feld **Benutzerkennwort** ein Kennwort für den Benutzeraccount ein, der als Eigner der Verzeichnisserverinstanz fungiert.
  - d. Geben Sie im Feld **Kennwort bestätigen** noch einmal das Kennwort für den Benutzeraccount ein, der als Eigner der Verzeichnisserverinstanz fungiert.
  - e. Geben Sie im Feld **Seedwert für die Verschlüsselung** einen Seedwert für die Verschlüsselung der Verzeichnisserverinstanz ein.

**Hinweis:** Sie müssen sich den Seedwert für die Verschlüsselung der Verzeichnisserverinstanz merken, da er möglicherweise für andere Konfigurationstasks erforderlich ist.

Der Seedwert für die Verschlüsselung darf nur druckbare ISO-8859-1 ASCII-Zeichen mit Werten zwischen 33 und 126 enthalten. Der Seedwert für die Verschlüsselung muss eine Länge von mindestens 12 und maximal 1016 Zeichen aufweisen. Informationen zu den zu verwendenden Zeichen finden Sie unter „ASCII-Zeichen von 33 bis 126“ auf Seite 134. Der Verzeichnisserver verwendet den Seedwert für die Verschlüsselung zum Generieren einer Gruppe von Werten für geheime AES-Schlüssel (AES = Advanced Encryption Standard). Die Schlüssel-Stashdatei einer Verzeichnisserverinstanz speichert die Schlüsselwerte, mit deren Hilfe das Kennwort und die Attribute verschlüsselt und entschlüsselt werden.

- f. Geben Sie im Feld **Seedwert für die Verschlüsselung bestätigen** den Seedwert für die Verschlüsselung der Verzeichnisserverinstanz ein.
  - g. Geben Sie im Feld **Kennwort für Administrator-DN** ein Kennwort für den Administrator der Verzeichnisserverinstanz ein.
  - h. Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Administrator der Verzeichnisserverinstanz ein.
  - i. Klicken Sie auf **Weiter**.
  - j. Überprüfen Sie die Angaben zu der Standardverzeichnisserverinstanz.
  - k. Klicken Sie auf **Fertig stellen**, um mit der Erstellung der Standardverzeichnisserverinstanz zu beginnen. Das Ergebnisfenster mit den Protokolldaten wird angezeigt.
4. Überprüfen Sie die im Fenster **Ergebnisse** angezeigten Protokolldaten.
  5. Klicken Sie auf **Schließen**, um das Fenster **Ergebnisse** zu schließen.
  6. Klicken Sie auf **Schließen**, um das **Instance Administration Tool** zu schließen.

## Ergebnisse

Das **Instance Administration Tool** erstellt auf dem Computer die Standardverzeichnisserverinstanz dsrdbm01.

## Nächste Schritte

Sie müssen den Prozess `ibmslapd` und den Verwaltungsserver starten, der der Verzeichnisserverinstanz zugeordnet ist. Weitere Informationen finden Sie unter „Verzeichnisserver und Verwaltungsserver starten oder stoppen“ auf Seite 165.

## Verzeichnisserverinstanz mit angepassten Einstellungen erstellen

Erstellen Sie mit **Instance Administration Server** eine Verzeichnisserverinstanz mit angepassten Werten entsprechend Ihren Anforderungen.

### Vorbereitende Schritte

Führen Sie die folgenden Tasks aus, um eine Verzeichnisserverinstanz zu erstellen:

1. Installieren Sie IBM Security Directory Server mit dem Server-Feature. Siehe „Installation mit IBM Installation Manager“ auf Seite 32.
2. Installieren Sie IBM DB2, um einen vollständigen Verzeichnisserver mit RDBM-Back-End zu erstellen. Siehe „Installation mit IBM Installation Manager“ auf Seite 32.
3. Überprüfen Sie, ob die Datei `ldapdb.properties` Angaben zum Installationspfad und der Version von DB2 enthält. Siehe Anhang C, „Datei `ldapdb.properties` manuell aktualisieren“, auf Seite 263.

### Vorgehensweise

1. Starten Sie das **Instance Administration Tool**. Siehe „**Instance Administration Tool** starten“ auf Seite 138.
2. Klicken Sie auf **Instanz erstellen**.
3. Klicken Sie in der Anzeige **Erstellen oder migrieren** des Fensters **Neue Verzeichnisserverinstanz erstellen** auf **Neue Verzeichnisserverinstanz erstellen**.
4. Klicken Sie auf **Weiter**.
5. Geben Sie in der Anzeige **Instanzdetails** des Fensters **Neue Verzeichnisserverinstanz erstellen** die folgenden Werte an:
  - a. Wählen Sie in der Liste **Benutzername** den Benutzernamen aus, der als Eigner der Verzeichnisserverinstanz fungiert. Der Verzeichnisserverinstanz wird derselbe Name zugewiesen wie dem Benutzernamen.
  - b. Wenn Sie der Instanz einen neuen Benutzeraccount zuordnen wollen, klicken Sie auf **Benutzer erstellen**. Führen Sie im Fenster **Neuen Benutzer für Verzeichnisserverinstanz erstellen** die folgenden Schritte aus:
    - 1) Geben Sie im Feld **Benutzername** den Benutzernamen ein.
    - 2) Geben Sie im Feld **Kennwort** ein Kennwort für den Benutzeraccount ein.
    - 3) Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Benutzeraccount ein.
    - 4) Geben Sie im Feld **Ausgangsverzeichnis** das für den Benutzeraccount zu konfigurierende Ausgangsverzeichnis ein. Sie können auf **Durchsuchen** klicken und das Ausgangsverzeichnis angeben.
    - 5) Geben Sie im Feld **Primärgruppe** den Namen der Primärgruppe des Benutzers ein.
    - 6) Klicken Sie auf **Erstellen**, um den Benutzeraccount zu erstellen.
  - c. Wählen Sie zum Ändern eines vorhandenen Benutzeraccounts in der Liste den Eintrag **Benutzername** aus und klicken Sie auf **Benutzer bearbeiten**. Führen Sie im Fenster **Benutzer für Verzeichnisserverinstanz bearbeiten** die folgenden Schritte aus:
    - 1) Das Feld **Benutzername** wird mit dem Benutzernamen gefüllt.
    - 2) Geben Sie im Feld **Kennwort** ein Kennwort für den Benutzeraccount ein.

- 3) Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Benutzeraccount ein.
  - 4) Geben Sie im Feld **Ausgangsverzeichnis** das für den Benutzeraccount zu konfigurierende Ausgangsverzeichnis ein. Sie können auf **Durchsuchen** klicken und das Ausgangsverzeichnis angeben.
  - 5) Geben Sie im Feld **Primärgruppe** den Namen der Primärgruppe des Benutzers ein.
  - 6) Klicken Sie auf **Bearbeiten**, um den Benutzeraccount zu bearbeiten.
6. Geben Sie im Feld **Instanzposition** die Speicherposition der Verzeichnisserverinstanz ein. Sie können auf **Durchsuchen** klicken und das Ausgangsverzeichnis der Instanz angeben. An der gewünschten Adresse müssen mindestens 30 MB freier Plattenspeicherplatz vorhanden sein. Auf Windows-Systemen muss für die Position ein Plattenlaufwerk, z. B. C:, angegeben werden. Die Dateien der Verzeichnisinstanz werden auf dem angegebenen Plattenlaufwerk im Verzeichnis `\ids\lapd-instance_name` gespeichert. Die Variable `instance_name` steht für den Namen der Verzeichnisserverinstanz. Auf AIX-, Linux- und Solaris-Systemen ist das Ausgangsverzeichnis des Eigners der Verzeichnisserverinstanz die Standardposition. Allerdings ist es möglich, einen anderen Pfad anzugeben.
  7. Geben Sie im Feld **Seedzeichenfolge für die Verschlüsselung** den Seedwert für die Verschlüsselung der Verzeichnisserverinstanz ein.

**Hinweis:** Sie müssen sich den Seedwert für die Verschlüsselung der Verzeichnisserverinstanz merken, da er möglicherweise für andere Konfigurationstasks erforderlich ist.

Der Seedwert für die Verschlüsselung darf nur druckbare ISO-8859-1 ASCII-Zeichen mit Werten zwischen 33 und 126 enthalten. Der Seedwert für die Verschlüsselung muss eine Länge von mindestens 12 und maximal 1016 Zeichen aufweisen. Informationen zu den zu verwendenden Zeichen finden Sie unter „ASCII-Zeichen von 33 bis 126“ auf Seite 134. Der Verzeichnisserver verwendet den Seedwert für die Verschlüsselung zum Generieren einer Gruppe von Werten für geheime AES-Schlüssel (AES = Advanced Encryption Standard). Die Schlüssel-Stashdatei einer Verzeichnisserverinstanz speichert die Schlüsselwerte, mit deren Hilfe das Kennwort und die Attribute verschlüsselt und entschlüsselt werden.

8. Geben Sie im Feld **Seedwert für die Verschlüsselung bestätigen** den Seedwert für die Verschlüsselung der Verzeichnisserverinstanz ein.
9. Wenn Sie einen Saltwert für die Verschlüsselung angeben wollen, klicken Sie auf **Saltwert für die Verschlüsselung verwenden**.
  - a. Geben Sie im Feld **Saltzeichenfolge für die Verschlüsselung** einen Saltwert für die Verschlüsselung der Verzeichnisserverinstanz ein. Der Saltwert für die Verschlüsselung darf nur druckbare ISO-8859-1 ASCII-Zeichen mit Werten zwischen 33 und 126 enthalten. Der Saltwert für die Verschlüsselung muss 12 Zeichen umfassen. Informationen zu den zu verwendenden Zeichen finden Sie unter „ASCII-Zeichen von 33 bis 126“ auf Seite 134. Um einen Verzeichnisserver in Bezug auf die Verschlüsselung mit einer anderen Verzeichnisserverinstanz zu synchronisieren, müssen Sie dieselben Seed- und Saltwerte für die Verschlüsselung verwenden:
  - b. Geben Sie im Feld **Saltwert für die Verschlüsselung bestätigen** den Saltwert für die Verschlüsselung der Verzeichnisserverinstanz ein.
10. Optional: Geben Sie im Feld **Instanzbeschreibung** eine Beschreibung der Verzeichnisserverinstanz ein. Die Beschreibung hilft zum Identifizieren der Instanz.

11. Klicken Sie auf **Weiter**.
12. Geben Sie in der Anzeige **DB2-Instanzdetails** im Feld **DB2-Instanzdetails** den DB2-Instanznamen für die Verzeichnisserverinstanz an.

**Anmerkung:** Die DB2-Instanz für die Verzeichnisserverinstanz darf nicht von anderen Programmen oder Produkten konfiguriert oder verwendet werden.

Standardmäßig ist der Name der DB2-Instanz mit dem Namen der Verzeichnisserverinstanz identisch. Sie können jedoch einen anderen Namen für die DB2-Instanz angeben. Wenn Sie einen anderen Namen angeben, müssen Sie darauf achten, dass auf dem Computer eine Systembenutzer-ID mit dem gleichen Namen vorhanden ist. Dieser Benutzeraccountname darf keiner anderen Verzeichnisserverinstanz zugeordnet werden.

13. Klicken Sie auf **Weiter**.
14. Wählen Sie in der Anzeige **TCP/IP-Einstellungen für multi-homed Hosts** eine der folgenden Optionen aus:
  - Wenn die Verzeichnisserverinstanz an allen IP-Adressen empfangsbereit sein soll, wählen Sie **Empfangsbereitschaft an allen konfigurierten IP-Adressen** aus.
  - Wenn die Instanz nur an einer bestimmten Gruppe der auf dem Computer konfigurierten IP-Adressen empfangsbereit sein soll, führen Sie die folgenden Schritte aus:
    - a. Deaktivieren Sie die Option **Empfangsbereitschaft an allen konfigurierten IP-Adressen**.
    - b. Wählen Sie in der Liste **IP-Adressen mit Empfangsbereitschaft auswählen** die IP-Adressen aus, an denen die Instanz empfangsbereit sein soll.
15. Klicken Sie auf **Weiter**.
16. Geben Sie in der Anzeige **TCP/IP-Porteinstellungen** die folgenden Werte an:

**Anmerkung:** Sie müssen den Verzeichnisserverports eindeutige Portnummern zuweisen, die keine Konflikte mit vorhandenen Ports verursachen, die gerade auf dem Computer verwendet werden. Auf AIX-, Linux- und Solaris-Systemen dürfen Portnummern im Bereich zwischen 1 und 1000 nur mit Rootberechtigung benutzt werden.

- a. Geben Sie im Feld **Server-Port** die Portnummer ein, die der Server als nicht sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - b. Geben Sie im Feld **Sicherer Port des Servers** die Portnummer ein, die der Server als sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - c. Geben Sie im Feld **Port des Verwaltungsservers** die Portnummer ein, die der Verwaltungsserver als nicht sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - d. Geben Sie im Feld **Sicherer Port des Verwaltungsservers** die Portnummer ein, die der Verwaltungsserver als sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - e. Klicken Sie auf **Weiter**.
17. Führen Sie in der Anzeige **Optionale Schritte** die folgenden Schritte aus:
    - a. Wählen Sie **Administrator-DN und zugehöriges Kennwort konfigurieren** aus, um den Administrator-DN und das Kennwort für die Verzeichnisserverinstanz zu konfigurieren. Sie müssen den Administrator-DN und das zugehörige Kennwort für einen Proxy-Server und einen vollständigen Verzeichnisserver festlegen.

- b. Wählen Sie **Datenbank konfigurieren** aus, um die Datenbank für die Verzeichnisserverinstanz zu konfigurieren.
  - c. Klicken Sie auf **Weiter**.
18. Führen Sie in der Anzeige **Administrator-DN und zugehöriges Kennwort konfigurieren** die folgenden Schritte aus:
- a. Geben Sie im Feld **Administrator-DN** einen gültigen DN ein oder übernehmen Sie den DN-Standardwert `cn=root`. Bei dem Wert für den Administrator-DN muss die Groß-/Kleinschreibung nicht beachtet werden. Der Benutzer mit dem Administrator-DN hat uneingeschränkten Zugriff auf alle Daten in der Verzeichnisserverinstanz.
  - b. Geben Sie im Feld **Administratorkennwort** das Kennwort für den Administrator-DN ein. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden. DBCS-Zeichen (DBCS = Double Byte Character Set) sind im Kennwort nicht zulässig.
  - c. Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Administrator-DN ein. Merken Sie sich das Kennwort.
  - d. Klicken Sie auf **Weiter**.
19. Führen Sie in der Anzeige **Datenbank konfigurieren** die folgenden Tasks aus, um die Datenbank für die Verzeichnisserverinstanz zu konfigurieren: Das **Instance Administration Tool** fügt die Datenbankinformationen für die Verzeichnisserverinstanz zur Konfigurationsdatei `ibmslapd.conf` hinzu. Wenn die Datenbank nicht vorhanden ist, erstellt das **Instance Administration Tool** die Datenbank.
- a. Geben Sie im Feld **Datenbankbenutzername** eine gültige DB2-Administrator-ID ein. Die DB2-Administrator-ID muss auf dem Computer bereits vorhanden sein und muss über die erforderliche Zugriffsberechtigung verfügen, damit die Datenbank konfiguriert werden kann.

**Anmerkung:** Die DB2-Administrator-ID muss vor dem Serverstart die passende Ländereinstellung für die Sprache festlegen, in der die Servernachrichten angezeigt werden sollen.

- b. Geben Sie im Feld **Kennwort** das Kennwort für den DB2-Administrator ein. Bei dem Kennwort wird zwischen Groß- und Kleinschreibung unterschieden.

**Anmerkung:** Wenn Sie das Systemkennwort für den DB2-Administrator ändern, kann es nicht mit dem **Instance Administration Tool** aktualisiert werden. Stattdessen muss in diesem Fall das **Konfigurationstool** oder der Befehl `idscfgdb` mit dem Parameter `-w` verwendet werden. Weitere Informationen hierzu finden Sie unter „Verwaltung des DB2-Datenbankadministratorkennworts“ auf Seite 190.

- c. Geben Sie im Feld **Datenbankname** einen DB2-Datenbanknamen ein. Der Name kann 1 bis 8 Zeichen enthalten.
- d. Optional: Wählen Sie **Erweiterte Tabellenbereichsoptionen anzeigen** aus, wenn Sie eine oder mehrere der folgenden DB2-Konfigurationseinstellungen festlegen wollen.

**Anmerkung:** DB2 kann zum Erstellen von Tabellenbereichen die Datenspeichertypen SMS (System Managed Storage) oder DMS (DMS = Database Managed Storage) verwenden. In IBM Security Directory Server wird standardmäßig DMS verwendet. In den Versionen von IBM Security Directory Server vor Version 6.2 wird für alle Datenbanken SMS verwendet. Wenn Sie die Option **Erweiterte Tabellenbereichsoptionen anzeigen** ab-

wählen, werden die Tabellenbereiche USERSPACE1 und LDAPSPACE anhand von DMS mit den Standardwerten für Größe und Position erstellt. Unter AIX, Linux und Solaris hat der Tabellenbereich USERSPACE1 den Standardpfad- und -dateinamen *database\_location/instance\_name/NODE0000/SQL00001/USPACE*. Unter Windows hat der Tabellenbereich USERSPACE1 den Standardpfad- und -dateinamen *database\_location\instance\_name\NODE0000\SQL00001\USPACE*. Unter AIX, Linux und Solaris hat der Tabellenbereich LDAPSPACE den Standardpfad- und -dateinamen *database\_location/ldap32kcont\_instance\_name/ldapspace*. Unter Windows hat der Tabellenbereich LDAPSPACE den Standardpfad- und -dateinamen *database\_location\ldap32kcont\_instance\_name\ldapspace*.

- Sie wollen die Datenbank für die Verwendung von SMS-Datenspeichern (SMS = System Managed Storage) für die DB2-Tabellenbereiche konfigurieren. Bei Verwendung von SMS ordnet der **Dateisystemmanager** des Betriebssystems den Tabellenbereich zu, in dem die DB2-Tabellen gespeichert werden, und verwaltet diesen auch.
- Sie wollen die Datenbank für die Verwendung von DMS-Datenspeichern (DMS = Database Managed Storage) für die DB2-Tabellenbereiche konfigurieren. Außerdem wollen Sie die Datenbank für die Tabellenbereiche USERSPACE1 und LDAPSPACE mit Größe und Position konfigurieren. Bei Verwendung von DMS werden die Tabellenbereiche vom Datenbankmanager verwaltet. Der Datenbankadministrator legt fest, welche Einheiten und Dateien verwendet werden sollen, und DB2 verwaltet den Speicherplatz auf diesen Einheiten und in diesen Dateien.

e. Klicken Sie auf **Weiter**.

20. Führen Sie in der Anzeige **Datenbankoptionen** die folgenden Schritte aus:

- a. Geben Sie im Feld **Installationsposition der Datenbank** den Pfad zur Speicherposition der Datenbank ein. Sie können auf **Durchsuchen** klicken, um ein Verzeichnis anzugeben. Unter Windows müssen Sie ein Plattenlaufwerk angeben, beispielsweise C:. Unter AIX, Linux und Solaris müssen Sie die Position als Verzeichnisnamen, z. B. /home/ldapdb, angeben.

**Anmerkung:** Der mindestens erforderliche Plattenspeicherplatz für eine DMS-Datenbank beträgt 1 GB. Eine SMS-Datenbank benötigt mindestens 150 MB Plattenspeicherplatz. Diese Anforderungen gelten für eine leere Datenbank. Wenn Sie Daten in der Datenbank speichern, dann ist mehr Plattenspeicherplatz erforderlich.

- b. Führen Sie die folgenden Schritte aus, um den Verzeichnisserver mit der Datenbank für die Onlinesicherung zu konfigurieren:

- 1) Wählen Sie **Für Onlinesicherung konfigurieren** aus.
- 2) Geben Sie im Feld **Datenbanksicherungsposition** die Speicherposition ein, an der das Sicherungsimage gespeichert werden soll. Sie können auf **Durchsuchen** klicken, um die gewünschte Position anzugeben.

**Anmerkung:** Die Ausführung des **Instance Administration Tools** darf nicht unterbrochen werden, während die Sicherungsoperation ausgeführt wird.

Wenn Sie die Datenbank nach Abschluss der Datenbankkonfiguration für die Onlinesicherung konfigurieren, wird eine Anfangs-Offlinesicherung der Datenbank ausgeführt. Nachdem der Vorgang der Offlinesicherung abgeschlossen ist, wird der Verwaltungsserver erneut gestartet. Sie können die Onlinesicherung für eine Verzeichnisserverinstanz auch mit dem **idscfgdb** konfigurieren. Sie können die Onlinesicherung jedoch nicht mit dem Befehl **idscfgdb** und dem Parameter **-c** dekonfigurieren. Wenn Sie die Onlinesi-

cherung für eine Instanz mit dem **Instance Administration Tool** oder dem **Konfigurationstool** durchführen, können Sie die Konfiguration mit dem **Konfigurationstool** oder dem Befehl **idscfgdb** wieder aufheben.

- c. Wählen Sie im Bereich **Zeichensatzoption** eine der folgenden Optionen aus, um einen Datenbanktyp zu erstellen:

**Anmerkung:** Erstellen Sie eine DB2-Datenbank im Universalzeichensatz, wenn in dem Verzeichnisserver Daten in mehreren Sprachen gespeichert werden sollen. Eine DB2-Datenbank im Universalzeichensatz ist auch deshalb die effizienteste Lösung, weil weniger Daten umgesetzt werden müssen. Wenn Sie Sprachentags einsetzen wollen, muss die Datenbank im UTF-8-Format definiert sein. Weitere Informationen zu UTF-8 finden Sie in „UTF-8-Unterstützung“ auf Seite 130.

- Klicken Sie auf **DB2-Datenbank im Universalzeichensatz erstellen**, um eine Datenbank im Universalzeichensatz (UCS Transformation Format, UTF-8) zu erstellen, in der LDAP-Clients Daten in diesem Format speichern können.
- Klicken Sie auf **DB2-Datenbank in der lokalen Codepage erstellen**, um eine Datenbank in der lokalen Codepage zu erstellen.

- d. Klicken Sie auf **Weiter**.

21. Wenn Sie in der Anzeige **Datenbank konfigurieren** die Option **Erweiterte Tabellenbereichsoptionen anzeigen** ausgewählt haben, müssen Sie in der Anzeige **Tabellenbereiche der Datenbank konfigurieren** die folgenden Schritte ausführen:

- a. Wählen Sie in der Liste **Tabellenbereichstyp der Datenbank auswählen** einen Datenbanktyp aus. Der Tabellenbereichstyp der Datenbank ist standardmäßig DMS. Wenn Sie SMS als Tabellenbereichstyp der Datenbank auswählen, werden alle anderen Felder inaktiviert. Die Unterstützung für DMS-Tabellenbereiche wird nur für die Tabellenbereiche USERSPACE1 und LDAPSPACE verwendet. Alle anderen Tabellenbereiche wie Katalogtabellenbereiche und Tabellenbereiche für temporäre Tabellen weisen den Typ SMS (System Managed Space) auf.

- a. Geben Sie im Bereich **USERSPACE1-Tabellenbereichsdetails** die folgenden Details an:

- 1) Wählen Sie in der Liste **Tabellenbereichscontainer** einen Containertyp aus. Wenn sich der Tabellenbereich USERSPACE1 im Dateisystem befinden soll, wählen Sie **Datei** aus. Wenn die Position des Containers für den Tabellenbereich der Datenbank sich in einem Dateisystem befindet, dann wird ein aufbereiteter DMS-Tabellenbereich erstellt. Sie können die Anfangsgröße des Tabellenbereichs und eine erweiterbare Einheitsgröße angeben. Der Tabellenbereich wird bei Bedarf automatisch erweitert. Wenn Sie den Tabellenbereich USERSPACE1 auf einer Roheinheit erstellen wollen, wählen Sie **Roheinheit** aus. Als Roheinheit wird eine Einheit bezeichnet, auf der kein Dateisystem installiert ist, z. B. eine Festplatte, die kein Dateisystem enthält. Wenn die Position des Containers für den Tabellenbereich der Datenbank sich auf einer Roheinheit befindet, dann wird ein nicht aufbereiteter DMS-Tabellenbereich erstellt. In diesem Fall ist die Größe des Containers für den Tabellenbereich der Datenbank festgelegt und kann nicht erweitert werden. Wenn Sie **Roheinheit** auswählen, müssen Sie zusammen mit der Position des Containers die Größe angeben, anstatt die entsprechenden Standardwerte zu übernehmen.

- 2) Geben Sie die folgenden Details an, wenn Sie im Feld **Tabellenbereichscontainer** die Option **Datei** ausgewählt haben:



- a) Geben Sie im Feld **Verzeichnispfad** den Verzeichnispfad an, in dem der Tabellenbereich USERSPACE1 erstellt werden soll. Sie können auf **Durchsuchen** klicken, um das gewünschte Verzeichnis auszuwählen.
  - b) Geben Sie im Feld **Dateiname** den Dateinamen des Tabellenbereich ein, den Sie erstellen wollen, oder übernehmen Sie den Standardnamen USPACE.
  - c) Geben Sie im Feld **Anfangsgröße** die Anfangsgröße für den Tabellenbereich USERSPACE1 in Seiten ein oder übernehmen Sie den Standardwert. Bei einem Tabellenbereichscontainer vom Typ **Datei** wird für den Container des Tabellenbereichs USERSPACE1 der Typ mit automatischer Inkrementierung festgelegt. Sie können im Feld **Anfangsgröße** die Anfangsgröße und im Feld **Erweiterbare Größe** eine erweiterbare Einheitengröße angeben. Standardmäßig werden für die Anfangsgröße 16-KB-Seiten und für die erweiterbare Einheitengröße 8-KB-Seiten verwendet. Die Seitengröße für den Container des Tabellenbereichs USERSPACE1 beträgt 4 KB pro Seite.
- 3) Geben Sie die folgenden Details an, wenn Sie im Feld **Tabellenbereichscontainer** die Option **Roheinheit** ausgewählt haben:
- a) Geben Sie im Feld **Einheitenpfad** die Position der Roheinheit ein. Unter Windows muss der Pfad mit `\\.\` anfangen. Ein Pfad mit dem Einheitennamen könnte beispielsweise wie folgt aussehen: `\\.\device_name`. Unter AIX, Linux und Solaris muss der Einheitenpfad eine gültiger Pfad sein.
  - b) Geben Sie im Feld **Anfangsgröße** die Anfangsgröße für den Tabellenbereich USERSPACE1 ein oder übernehmen Sie den Standardwert. Bei einem Tabellenbereichscontainer vom Typ **Roheinheit** ist die Größe des Containers für den Tabellenbereich USERSPACE1 festgelegt. Die Standardgröße beträgt 16-KB-Seiten. Zur Optimierung der Ergebnisse können Sie die Größe an Ihre Anforderungen anpassen.
- b. Geben Sie im Bereich **LDAPSPACE-Tabellenbereichsdetails** die folgenden Details an:
- 1) Wählen Sie in der Liste **Tabellenbereichscontainer** einen Containertyp aus. Wenn sich der Tabellenbereich LDAPSPACE in einem Dateisystem befinden soll, wählen Sie **Datei** aus. Wenn Sie den Tabellenbereich LDAPSPACE auf einer Roheinheit erstellen wollen, wählen Sie **Roheinheit** aus. Als Roheinheit wird eine Einheit bezeichnet, auf der kein Dateisystem installiert ist, z. B. eine Festplatte, die kein Dateisystem enthält.
  - 2) Geben Sie die folgenden Details an, wenn Sie im Feld **Tabellenbereichscontainer** die Option **Datei** ausgewählt haben:
    - a) Geben Sie im Feld **Verzeichnispfad** den Verzeichnispfad an, in dem der Tabellenbereich LDAPSPACE erstellt werden soll. Sie können auf **Durchsuchen** klicken, um das gewünschte Verzeichnis auszuwählen.
    - b) Geben Sie im Feld **Dateiname** den Dateinamen des Tabellenbereich ein, den Sie erstellen wollen, oder übernehmen Sie den Standardnamen `ldapspace`.
    - c) Geben Sie im Feld **Anfangsgröße** die Anfangsgröße für den Tabellenbereich LDAPSPACE in Seiten ein oder übernehmen Sie den Standardwert. Bei einem Tabellenbereichscontainer vom Typ **Datei** wird für den Container des Tabellenbereichs LDAPSPACE der Typ mit automatischer Inkrementierung festgelegt. Sie können im Feld **Anfangsgröße** die Anfangsgröße und im Feld **Erweiterbare Größe** eine er-

weiterbare Einheitengröße angeben. Standardmäßig werden für die Anfangsgröße 16-KB-Seiten und für die erweiterbare Einheitengröße 8-KB-Seiten verwendet. Die Seitengröße für den Container des Tabellenbereichs LDAPSPACE beträgt 32 KB pro Seite.

- 3) Geben Sie die folgenden Details an, wenn Sie im Feld **Tabellenbereichscontainer** die Option **Roheinheit** ausgewählt haben:
  - a) Geben Sie im Feld **Einheitenpfad** die Position der Roheinheit ein. Unter Windows muss der Pfad mit `\\.\` anfangen. Ein Pfad mit dem Einheitennamen könnte beispielsweise wie folgt aussehen: `\\.\device_name`. Unter AIX, Linux und Solaris muss der Einheitenpfad eine gültiger Pfad sein.
  - b) Geben Sie im Feld **Anfangsgröße** die Anfangsgröße für den Tabellenbereich LDAPSPACE ein oder übernehmen Sie den Standardwert. Bei einem Tabellenbereichscontainer vom Typ **Roheinheit** ist die Größe des Containers für den Tabellenbereich LDAPSPACE festgelegt. Die Standardgröße beträgt 16-KB-Seiten. Zur Optimierung der Ergebnisse können Sie die Größe an Ihre Anforderungen anpassen.
  - c. Wenn Sie in einem der beiden oder in beiden Feldern **Tabellenbereichscontainer** die Option **Datei** ausgewählt haben, geben Sie im Feld **Erweiterbare Größe** die Anzahl der Seiten an, um die die Tabellenbereichscontainer erweitert werden sollen.
  - d. Klicken Sie auf **Weiter**.
22. Überprüfen Sie in der Anzeige **Einstellungen überprüfen** die generierte Zusammenfassung.
23. Klicken Sie auf **Fertig stellen**, um mit der Erstellung der Verzeichnisserverinstanz zu beginnen.
24. Überprüfen Sie im Fenster **Ergebnisse** die Protokollnachrichten, die für die Instanzerstellungsoperationen generiert werden.
25. Klicken Sie auf **Schließen**, um das Fenster **Ergebnisse** zu schließen.
26. Klicken Sie auf **Schließen**, um das **Instance Administration Tool** zu schließen.

## Ergebnisse

Das **Instance Administration Tool** erstellt auf dem Computer eine Verzeichnisserverinstanz.

## Nächste Schritte

Sie müssen den Prozess `ibmslapd` und den Verwaltungsserver starten, der der Verzeichnisserverinstanz zugeordnet ist. Weitere Informationen finden Sie unter „Verzeichnisserver und Verwaltungsserver starten oder stoppen“ auf Seite 165.

## Proxy-Server-Instanz mit angepassten Einstellungen erstellen

Erstellen Sie mit **Instance Administration Server** eine Proxy-Server-Instanz mit angepassten Werten entsprechend Ihren Anforderungen.

## Vorbereitende Schritte

Führen Sie die folgenden Tasks aus, um eine Proxy-Server-Instanz zu erstellen:

1. Installieren Sie IBM Security Directory Server mit dem Proxy-Server-Feature. Siehe „Installation mit IBM Installation Manager“ auf Seite 32.

## Vorgehensweise

1. Starten Sie das **Instance Administration Tool**. Siehe „**Instance Administration Tool** starten“ auf Seite 138.
2. Klicken Sie auf **Instanz erstellen**.
3. Führen Sie in der Anzeige **Erstellen oder migrieren** des Fensters **Neue Verzeichnisserverinstanz erstellen** die folgenden Schritte aus, um eine Proxy-Server-Instanz zu erstellen:
  - a. Klicken Sie auf **Neue Verzeichnisserverinstanz erstellen**.
  - b. Klicken Sie auf **Als Proxy konfigurieren**.
4. Klicken Sie auf **Weiter**.
5. Geben Sie in der Anzeige **Instanzdetails** des Fensters **Neue Verzeichnisserverinstanz erstellen** die folgenden Werte an:
  - a. Wählen Sie in der Liste **Benutzername** den Benutzernamen aus, der als Eigner der Instanz fungiert. Der Instanz wird derselbe Name zugewiesen wie dem Benutzernamen.
  - b. Wenn Sie der Instanz einen neuen Benutzeraccount zuordnen wollen, klicken Sie auf **Benutzer erstellen**. Führen Sie im Fenster **Neuen Benutzer für Verzeichnisserverinstanz erstellen** die folgenden Schritte aus:
    - 1) Geben Sie im Feld **Benutzername** den Benutzernamen ein.
    - 2) Geben Sie im Feld **Kennwort** ein Kennwort für den Benutzeraccount ein.
    - 3) Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Benutzeraccount ein.
    - 4) Geben Sie im Feld **Ausgangsverzeichnis** das für den Benutzeraccount zu konfigurierende Ausgangsverzeichnis ein. Sie können auf **Durchsuchen** klicken und das Ausgangsverzeichnis angeben.
    - 5) Geben Sie im Feld **Primärgruppe** den Namen der Primärgruppe des Benutzers ein.
    - 6) Klicken Sie auf **Erstellen**, um den Benutzeraccount zu erstellen.
  - c. Wählen Sie zum Ändern eines vorhandenen Benutzeraccounts in der Liste den Eintrag **Benutzername** aus und klicken Sie auf **Benutzer bearbeiten**. Führen Sie im Fenster **Benutzer für Verzeichnisserverinstanz bearbeiten** die folgenden Schritte aus:
    - 1) Das Feld **Benutzername** wird mit dem Benutzernamen gefüllt.
    - 2) Geben Sie im Feld **Kennwort** ein Kennwort für den Benutzeraccount ein.
    - 3) Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Benutzeraccount ein.
    - 4) Geben Sie im Feld **Ausgangsverzeichnis** das für den Benutzeraccount zu konfigurierende Ausgangsverzeichnis ein. Sie können auf **Durchsuchen** klicken und das Ausgangsverzeichnis angeben.
    - 5) Geben Sie im Feld **Primärgruppe** den Namen der Primärgruppe des Benutzers ein.
    - 6) Klicken Sie auf **Bearbeiten**, um den Benutzeraccount zu bearbeiten.
    - 7) Klicken Sie im Bestätigungsfenster **Benutzer für Verzeichnisserverinstanz bearbeiten** auf **Ja**.
6. Geben Sie im Feld **Instanzposition** die Speicherposition der Proxy-Server-Instanz ein. Sie können auf **Durchsuchen** klicken und das Ausgangsverzeichnis der Instanz angeben. An der gewünschten Adresse müssen mindestens 30 MB freier Plattenspeicherplatz vorhanden sein. Auf Windows-Systemen muss für

die Position ein Plattenlaufwerk, z. B. C:, angegeben werden. Die Dateien der Verzeichnisinstanz werden auf dem angegebenen Plattenlaufwerk im Verzeichnis `\idslapd-instance_name` gespeichert. Die Variable `instance_name` steht für den Namen der Proxy-Server-Instanz. Auf AIX-, Linux- und Solaris-Systemen ist das Ausgangsverzeichnis des Eigners der Proxy-Server-Instanz die Standardposition. Allerdings ist es möglich, einen anderen Pfad anzugeben.

7. Geben Sie im Feld **Seedzeichenfolge für die Verschlüsselung** den Seedwert für die Verschlüsselung der Instanz ein.

**Hinweis:** Sie müssen sich den Seedwert für die Verschlüsselung der Instanz merken, da er möglicherweise für andere Konfigurationstasks erforderlich ist. Der Seedwert für die Verschlüsselung darf nur druckbare ISO-8859-1 ASCII-Zeichen mit Werten zwischen 33 und 126 enthalten. Der Seedwert für die Verschlüsselung muss eine Länge von mindestens 12 und maximal 1016 Zeichen aufweisen. Informationen zu den zu verwendenden Zeichen finden Sie unter „ASCII-Zeichen von 33 bis 126“ auf Seite 134. Der Verzeichnisserver verwendet den Seedwert für die Verschlüsselung zum Generieren einer Gruppe von Werten für geheime AES-Schlüssel (AES = Advanced Encryption Standard). Die Schlüssel-Stashdatei einer Verzeichnisserverinstanz speichert die Schlüsselwerte, mit deren Hilfe das Kennwort und die Attribute verschlüsselt und entschlüsselt werden.

8. Geben Sie im Feld **Seedwert für die Verschlüsselung bestätigen** den Seedwert für die Verschlüsselung der Instanz ein.
9. Wenn Sie einen Saltwert für die Verschlüsselung angeben wollen, klicken Sie auf **Saltwert für die Verschlüsselung verwenden**.
  - a. Geben Sie im Feld **Saltzeichenfolge für die Verschlüsselung** einen Saltwert für die Verschlüsselung der Instanz ein. Der Saltwert für die Verschlüsselung darf nur druckbare ISO-8859-1 ASCII-Zeichen mit Werten zwischen 33 und 126 enthalten. Der Saltwert für die Verschlüsselung muss 12 Zeichen umfassen. Informationen zu den zu verwendenden Zeichen finden Sie unter „ASCII-Zeichen von 33 bis 126“ auf Seite 134.
  - b. Geben Sie im Feld **Saltwert für die Verschlüsselung bestätigen** den Saltwert für die Verschlüsselung der Instanz ein.
10. Optional: Geben Sie im Feld **Instanzbeschreibung** eine Beschreibung der Instanz ein. Die Beschreibung hilft zum Identifizieren der Instanz.
11. Klicken Sie auf **Weiter**.
12. Wählen Sie in der Anzeige **TCP/IP-Einstellungen für multi-homed Hosts** eine der folgenden Optionen aus:
  - Wenn die Instanz an allen IP-Adressen empfangsbereit sein soll, wählen Sie **Empfangsbereitschaft an allen konfigurierten IP-Adressen** aus.
  - Wenn die Instanz nur an einer bestimmten Gruppe der auf dem Computer konfigurierten IP-Adressen empfangsbereit sein soll, führen Sie die folgenden Schritte aus:
    - a. Deaktivieren Sie die Option **Empfangsbereitschaft an allen konfigurierten IP-Adressen**.
    - b. Wählen Sie in der Liste **IP-Adressen mit Empfangsbereitschaft auswählen** die IP-Adressen aus, an denen die Instanz empfangsbereit sein soll.
13. Klicken Sie auf **Weiter**.
14. Geben Sie in der Anzeige **TCP/IP-Porteinstellungen** die folgenden Werte an:

**Anmerkung:** Sie müssen den Verzeichnisserverports eindeutige Portnummern zuweisen, die keine Konflikte mit vorhandenen Ports verursachen, die gerade

auf dem Computer verwendet werden. Auf AIX-, Linux- und Solaris-Systemen dürfen Portnummern im Bereich zwischen 1 und 1000 nur mit Rootberechtigung benutzt werden.

- a. Geben Sie im Feld **Server-Port** die Portnummer ein, die der Server als nicht sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - b. Geben Sie im Feld **Sicherer Port des Servers** die Portnummer ein, die der Server als sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - c. Geben Sie im Feld **Port des Verwaltungsservers** die Portnummer ein, die der Verwaltungsserver als nicht sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - d. Geben Sie im Feld **Sicherer Port des Verwaltungsservers** die Portnummer ein, die der Verwaltungsserver als sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - e. Klicken Sie auf **Weiter**.
15. Führen Sie in der Anzeige **Optionale Schritte** die folgenden Schritte aus:
- a. Wählen Sie **Administrator-DN und zugehöriges Kennwort konfigurieren** aus, um den Administrator-DN und das Kennwort für die Instanz zu konfigurieren. Sie müssen den Administrator-DN und das zugehörige Kennwort für eine Proxy-Server-Instanz festlegen.
  - b. Klicken Sie auf **Weiter**.
16. Führen Sie in der Anzeige **Administrator-DN und zugehöriges Kennwort konfigurieren** die folgenden Schritte aus:
- a. Geben Sie im Feld **Administrator-DN** einen gültigen DN ein oder übernehmen Sie den DN-Standardwert `cn=root`. Bei dem Wert für den Administrator-DN muss die Groß-/Kleinschreibung nicht beachtet werden. Der Benutzer mit dem Administrator-DN hat uneingeschränkten Zugriff auf alle Daten in der Instanz.
  - b. Geben Sie im Feld **Administratorkennwort** das Kennwort für den Administrator-DN ein. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden. DBCS-Zeichen (DBCS = Double Byte Character Set) sind im Kennwort nicht zulässig.
  - c. Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Administrator-DN ein. Merken Sie sich das Kennwort.
  - d. Klicken Sie auf **Weiter**.
17. Überprüfen Sie in der Anzeige **Einstellungen überprüfen** die generierte Zusammenfassung.
18. Klicken Sie auf **Fertig stellen**, um mit der Erstellung der Proxy-Server-Instanz zu beginnen.
19. Überprüfen Sie im Fenster **Ergebnisse** die Protokollnachrichten, die für die Instanzerstellungsoperationen generiert werden.
20. Klicken Sie auf **Schließen**, um das Fenster **Ergebnisse** zu schließen.
21. Klicken Sie auf **Schließen**, um das **Instance Administration Tool** zu schließen.

## Ergebnisse

Das **Instance Administration Tool** erstellt auf dem Computer eine Proxy-Server-Instanz.

## Nächste Schritte

Sie müssen den Verwaltungsserver und den Prozess `ibmslapd` im reinen Konfigurationsmodus starten und Back-End-Server konfigurieren. Informationen dazu finden Sie im Abschnitt *Verwaltung* der IBM Security Directory Server-Dokumentation.

## Instanz mit dem Befehlszeilendienstprogramm konfigurieren

Mit dem Befehlszeilendienstprogramm `idsicrt` können Sie eine Instanz erstellen.

### Vorbereitende Schritte

Zum Erstellen einer Instanz mit dem Befehlszeilendienstprogramm müssen Sie die folgenden Bedingungen erfüllen:

1. Installieren Sie IBM Security Directory Server mit dem Server- und/oder dem Proxy-Server-Feature. Siehe „Installation mit IBM Installation Manager“ auf Seite 32.
2. Es muss eine Systembenutzer-ID vorhanden sein, die als Eigner der Instanz fungiert. Weitere Informationen zum Erstellen einer Systembenutzer-ID finden Sie unter „Benutzer und Gruppen, die einer Verzeichnisserverinstanz zugeordnet sind“ auf Seite 125.

### Informationen zu diesem Vorgang

Bei der Ausführung des Befehls `idsicrt` werden eine Instanz und eine DB2-Datenbankinstanz für die vollständige Verzeichnisserverinstanz erstellt.

### Vorgehensweise

1. Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.
2. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
3. Führen Sie zum Erstellen einer Instanz den folgenden Befehl aus: Setzen Sie für die Variable `instance_name` den Namen einer gültigen Systembenutzer-ID ein.

Task	Befehl:
Verzeichnisserverinstanz erstellen	<code>idsicrt -I instance_name -e mysecretkey! -l instance_home</code>
Proxy-Server-Instanz erstellen	<code>idsicrt -I instance_name -e mysecretkey! -l instance_home -x</code>

Weitere Informationen zum Befehl `idsicrt` finden Sie in der Veröffentlichung *Command Reference*.

## Beispiele

### Beispiel 1:

Führen Sie den folgenden Befehl aus, um eine Verzeichnisserverinstanz mit den folgenden Werten unter AIX, Linux oder Solaris zu erstellen:

- Instanzname: `myinst`
- Nicht sicherer Port: 389
- Sicherer Port: 636
- Seedwert für die Verschlüsselung: `mysecretkey!`
- Saltwert für die Verschlüsselung: `mysecretsalt`

- Ausgangsverzeichnis der Instanz: /home/myinst unter AIX und Linux, /export/home/myinst unter Solaris

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!\
-g mysecretsalt -l /home/myinst
```

Führen Sie den folgenden Befehl aus, um eine Verzeichnisserverinstanz mit den folgenden Werten unter Windows zu erstellen:

- Instanzname: myinst
- Nicht sicherer Port: 389
- Sicherer Port: 636
- Seedwert für die Verschlüsselung: mysecretkey!
- Saltwert für die Verschlüsselung: mysecretsalt
- Ausgangsverzeichnis der Instanz: C:

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!\
-g mysecretsalt -l C:
```

### Beispiel 2:

Führen Sie den folgenden Befehl aus, um eine Proxy-Server-Instanz mit den folgenden Werten unter AIX, Linux oder Solaris zu erstellen:

- Instanzname: myproxy
- Nicht sicherer Port: 389
- Sicherer Port: 636
- Seedwert für die Verschlüsselung: mysecretkey!
- Saltwert für die Verschlüsselung: mysecretsalt
- Ausgangsverzeichnis der Instanz: /home/myproxy unter AIX und Linux, /export/home/myproxy unter Solaris

```
idsicrt -I myproxy -p 389 -s 636 -e mysecretkey!\
-g mysecretsalt -l /home/myproxy -x
```

Führen Sie den folgenden Befehl aus, um eine Proxy-Server-Instanz mit den folgenden Werten unter Windows zu erstellen:

- Instanzname: myproxy
- Nicht sicherer Port: 389
- Sicherer Port: 636
- Seedwert für die Verschlüsselung: mysecretkey!
- Saltwert für die Verschlüsselung: mysecretsalt
- Ausgangsverzeichnis der Instanz: C:

```
idsicrt -I myproxy -p 389 -s 636 -e mysecretkey!\
-g mysecretsalt -l C: -x
```

## Nächste Schritte

Führen Sie die folgenden Konfigurationsschritte aus, um eine funktionsfähige Instanz zu erstellen:

1. Konfigurieren Sie eine DB2-Datenbankinstanz für eine vollständige Verzeichnisserverinstanz.
2. Konfigurieren Sie den Administrator-DN und das Kennwort für die Instanz.
3. Konfigurieren Sie die Suffixe für die Instanz.

## Upgrade einer Instanz einer Vorgängerversion mit dem Instance Administration Tool durchführen

Führen Sie mit dem **Instance Administration Tool** ein Upgrade einer Verzeichnisserverinstanz oder Proxy-Server-Instanz einer Vorgängerversion auf Version 6.3.1 durch.

### Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um mit dem **Instance Administration Tool** ein Upgrade einer Instanz durchzuführen.

- Installieren Sie IBM Security Directory Server Version 6.3.1. Siehe „Installation starten“ auf Seite 29.
- Richten Sie vor dem Upgrade einer Instanz die Umgebung ein. Siehe „Umgebung vor dem Upgrade einer Instanz einrichten“ auf Seite 94.
- Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.

### Informationen zu diesem Vorgang

Nach dem Upgrade einer Instanz einer Vorgängerversion wird die Instanz in eine vollständig funktionsfähige Instanz von IBM Security Directory Server Version 6.3.1 konvertiert.

### Vorgehensweise

1. Öffnen Sie die Eingabeaufforderung.
2. Ändern Sie das aktuelle Arbeitsverzeichnis in sbin. Nachstehend sind die Standardpositionen auf verschiedenen Betriebssystemen aufgeführt:

#### Microsoft Windows

```
C:\Program Files\IBM\ldap\V6.3.1\sbin
```

#### AIX und Solaris

```
/opt/IBM/ldap/V6.3.1/sbin
```

```
Linux /opt/ibm/ldap/V6.3.1/sbin
```

3. Führen Sie den folgenden Befehl aus, um das **Instance Administration Tool** zu starten:

**Anmerkung:** Unter Windows verwenden Sie dazu das Menü **Start**. Klicken Sie auf **Start > Alle Programme > IBM Security Directory Server 6.3.1 > Instance Administration Tool**.

```
idsxinst
```

4. Wählen Sie eine Vorgängerversion einer Instanz aus, für die Sie ein Upgrade durchführen wollen.
5. Klicken Sie auf **Migrieren**.
6. Klicken Sie im Fenster **Verzeichnisserverinstanz migrieren** auf **Migrieren**.
7. Wenn das **Instance Administration Tool** Sie nach der Upgradeoperation zu einer Eingabe auffordert, klicken Sie auf **OK**.
8. Überprüfen Sie die Übersichtsdaten.
9. Klicken Sie auf **Schließen**, um das Fenster **Verzeichnisserverinstanz migrieren** zu schließen.
10. Führen Sie eine Offlinesicherung der Instanz durch. Weitere Informationen hierzu finden Sie unter „Verzeichnisserverbackup“ auf Seite 198.



11. Klicken Sie auf **Schließen**, um das **Instance Administration Tool** zu schließen.

## Ergebnisse

**Instance Administration Tool** führt ein Upgrade einer Vorgängerversion der Verzeichnisserverinstanz auf Version 6.3.1 durch.

## Nächste Schritte

Sie müssen den Prozess `ibmslapd` und den Verwaltungsserver starten, der der Verzeichnisserverinstanz zugeordnet ist. Weitere Informationen finden Sie unter „Verzeichnisserver und Verwaltungsserver starten oder stoppen“ auf Seite 165.

## Upgrade einer fernen Instanz einer Vorgängerversion mit dem Instance Administration Tool durchführen

Führen Sie mit dem **Instance Administration Tool** ein Upgrade einer fernen Verzeichnisserverinstanz oder Proxy-Server-Instanz einer Vorgängerversion auf Version 6.3.1 durch.

## Vorbereitende Schritte

Sie müssen die folgenden Tasks ausführen, um mit dem **Instance Administration Tool** ein Upgrade einer Instanz durchzuführen.

- Richten Sie vor dem Upgrade einer Instanz die Umgebung ein. Siehe „Umgebung vor dem Upgrade einer Instanz einrichten“ auf Seite 94.
- Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.

## Informationen zu diesem Vorgang

Nachdem Sie den Upgradeprozess ausgeführt haben, erstellt das **Instance Administration Tool** mit den Angaben von der fernen Instanz eine Instanz der Version 6.3.1 auf dem Computer.

## Vorgehensweise

1. Sichern Sie die Datenbank einer Verzeichnisserverinstanz, die sich auf einem fernen Computer befindet, mit dem Befehl **idsdb2ldif**.

**Wichtig:** Sichern Sie die Datenbank nicht, wenn Sie ein Upgrade für eine Proxy-Server-Instanz durchführen. Ein Proxy-Server enthält keine ihm zugeordnete Datenbank.

```
idsdb2ldif -I instance_name -o inst_out.ldif
```

Weitere Informationen zum Befehl **idsdb2ldif** finden Sie in der Veröffentlichung *Command Reference*.

2. Installieren Sie IBM Security Directory Server Version 6.3.1 auf einem Computer, auf dem Sie das Upgrade der fernen Instanz durchführen wollen. Siehe „Installation starten“ auf Seite 29.
3. Führen Sie den Befehl **migbkup** der Version 6.3.1 aus, auf die Sie das Upgrade durchführen wollen, um die Schema- und Konfigurationsdateien der fernen Instanz zu sichern:

Betriebssystem	Befehl:
Microsoft Windows	<b>migbkup.bat</b> drive_name\idsslapd-instance_name backup_directory
AIX, Linux und Solaris	<b>migbkup</b> user_home_dir/idsslapd-instance_name backup_directory

Der Befehl **migbkup** befindet sich im Unterverzeichnis `tools` der Installationsmedien von IBM Security Directory Server.

4. Kopieren Sie das Sicherungsverzeichnis `backup_directory`, das Sie mit **migbkup** erstellt haben, von dem fernen Computer auf den Computer mit IBM Security Directory Server Version 6.3.1.
5. Optional: Kopieren Sie die Datenbanksicherungsdatei `inst_out.ldif` von dem fernen Computer auf den Computer mit IBM Security Directory Server Version 6.3.1.
6. Starten Sie das **Instance Administration Tool**. Siehe „**Instance Administration Tool** starten“ auf Seite 138.
7. Klicken Sie auf **Instanz erstellen**.
8. Führen Sie in der Anzeige **Erstellen oder migrieren** die folgenden Tasks aus:
  - a. Klicken Sie auf **Migration von einer Verzeichnisservervorversion durchführen**.
  - b. Geben Sie im Feld **Pfad für die Sicherungskopien der Dateien eingeben** den Pfad ein, in den Sie die Sicherung der Konfigurations- und Schemadateien der fernen Instanz kopiert haben. Sie können auf **Durchsuchen** klicken und die Sicherungsposition angeben.
  - c. Klicken Sie auf **Weiter**.
9. Geben Sie in der Anzeige **Instanzdetails** des Fensters **Neue Verzeichnisserverinstanz erstellen** die folgenden Werte an:

**Anmerkung:** Wenn Sie ein Upgrade einer Instanz durchführen, können Sie die vorhandenen Benutzerdaten nicht bearbeiten.

- a. Wählen Sie in der Liste **Benutzername** den Benutzernamen aus, der als Eigner der Verzeichnisserverinstanz fungieren muss. Der Verzeichnisserverinstanz wird derselbe Name zugewiesen wie dem Benutzernamen.
- b. Wenn Sie der Instanz einen neuen Benutzeraccount zuordnen wollen, klicken Sie auf **Benutzer erstellen**. Führen Sie im Fenster **Neuen Benutzer für Verzeichnisserverinstanz erstellen** die folgenden Schritte aus:
  - 1) Geben Sie im Feld **Benutzername** den Benutzernamen ein.
  - 2) Geben Sie im Feld **Kennwort** ein Kennwort für den Benutzeraccount ein.
  - 3) Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Benutzeraccount ein.
  - 4) Geben Sie im Feld **Ausgangsverzeichnis** das für den Benutzeraccount zu konfigurierende Ausgangsverzeichnis ein. Sie können auf **Durchsuchen** klicken und das Ausgangsverzeichnis angeben.
  - 5) Geben Sie im Feld **Primärgruppe** den Namen der Primärgruppe des Benutzers ein.
  - 6) Klicken Sie auf **Erstellen**, um den Benutzeraccount zu erstellen.
10. Geben Sie im Feld **Instanzposition** die Speicherposition der Verzeichnisserverinstanz ein. Sie können auf **Durchsuchen** klicken und das Ausgangsverzeichnis der Instanz angeben. An der gewünschten Adresse müssen mindestens 30 MB freier Plattenspeicherplatz vorhanden sein. Auf Windows-Systemen muss

für die Position ein Plattenlaufwerk, z. B. C:, angegeben werden. Die Dateien der Verzeichnisinstanz werden auf dem angegebenen Plattenlaufwerk im Verzeichnis `\idsldap-instance_name` gespeichert. Die Variable `instance_name` steht für den Namen der Verzeichnisserverinstanz. Auf AIX-, Linux- und Solaris-Systemen ist das Ausgangsverzeichnis des Eigners der Verzeichnisserverinstanz die Standardposition. Allerdings ist es möglich, einen anderen Pfad anzugeben.

11. Optional: Geben Sie im Feld **Instanzbeschreibung** eine Beschreibung der Verzeichnisserverinstanz ein. Die Beschreibung hilft zum Identifizieren der Instanz.
12. Klicken Sie auf **Weiter**.
13. Klicken Sie in der Anzeige **DB2-Instanzdetails** auf **Weiter**, wenn Sie ein Upgrade einer fernen Verzeichnisserverinstanz mit den DB2-Instanzdetails durchführen. Wenn die Sicherungsdateien nicht zu einer fernen Proxy-Server-Instanz gehören, wird die Anzeige **DB2-Instanzdetails** möglicherweise nicht angezeigt.
14. Wählen Sie in der Anzeige **TCP/IP-Einstellungen für multi-homed Hosts** eine der folgenden Optionen aus:
  - Wenn die Verzeichnisserverinstanz an allen IP-Adressen empfangsbereit sein soll, wählen Sie **Empfangsbereitschaft an allen konfigurierten IP-Adressen** aus.
  - Wenn die Verzeichnisserverinstanz nur an einer bestimmten Gruppe der auf dem Computer konfigurierten IP-Adressen empfangsbereit sein soll, wählen Sie **Empfangsbereitschaft an allen konfigurierten IP-Adressen** ab. Wählen Sie in der Liste die IP-Adressen aus, an denen die Verzeichnisserverinstanz empfangsbereit sein soll.
15. Klicken Sie auf **Weiter**.
16. Geben Sie in der Anzeige **TCP/IP-Porteinstellungen** die folgenden Werte an:

**Anmerkung:** Sie müssen den Verzeichnisserverports eindeutige Portnummern zuweisen, die keine Konflikte mit vorhandenen Ports verursachen, die gerade auf dem Computer verwendet werden. Auf AIX-, Linux- und Solaris-Systemen dürfen Portnummern im Bereich zwischen 1 und 1000 nur mit Rootberechtigung benutzt werden.

- a. Geben Sie im Feld **Server-Port** die Portnummer ein, die der Server als nicht sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - b. Geben Sie im Feld **Sicherer Port des Servers** die Portnummer ein, die der Server als sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - c. Geben Sie im Feld **Port des Verwaltungsservers** die Portnummer ein, die der Verwaltungsserver als nicht sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - d. Geben Sie im Feld **Sicherer Port des Verwaltungsservers** die Portnummer ein, die der Verwaltungsserver als sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - e. Klicken Sie auf **Weiter**.
17. Überprüfen Sie in der Anzeige **Einstellungen überprüfen** die generierte Zusammenfassung.
  18. Klicken Sie auf **Fertig stellen**, um mit der Erstellung der Verzeichnisserverinstanz mit den gesicherten Konfigurations- und Schemadateien zu beginnen.

19. Überprüfen Sie im Fenster **Ergebnisse** die Protokollnachrichten, die für die Instanzerstellungsoperationen generiert werden.
20. Klicken Sie auf **Schließen**, um das Fenster **Ergebnisse** zu schließen.
21. Klicken Sie auf **Schließen**, um das **Instance Administration Tool** zu schließen.

## Ergebnisse

Das **Instance Administration Tool** erstellt auf dem Computer eine Verzeichnisserverinstanz.

## Nächste Schritte

Sie müssen den Prozess `ibmslapd` und den Verwaltungsserver starten, der der Verzeichnisserverinstanz zugeordnet ist. Siehe „Verzeichnisserver und Verwaltungsserver starten oder stoppen“ auf Seite 165.

Führen Sie eine Sicherung der Instanz durch. Informationen zum Sichern einer Verzeichnisserverinstanz finden Sie unter „Verzeichnisserverbackup“ auf Seite 198.

---

## Instanzerstellung aus einer bereits vorhandenen Instanz

Mithilfe von **Instance Administration Tool** können Sie eine Verzeichnisserverinstanz aus einer bereits vorhandenen Instanz erstellen, die sich auf einem lokalen Computer oder einem fernen Computer befindet. Der Quellenverzeichnisserver dient dabei als Schablone für die Zielverzeichnisserverinstanz.

Sie können nur mithilfe von IBM Security Directory Server **Instance Administration Tool** eine Quellenverzeichnisserverinstanz kopieren, wenn das Tool und die Instanz dieselbe Version aufweisen. Der Zielverzeichnisserver wird auf dem Computer erstellt, auf dem **Instance Administration Tool** ausgeführt wird. Befindet sich der Quellenverzeichnisserver auf einem anderen Computer, müssen die Betriebssysteme der beiden Computer nicht übereinstimmen. Auf einem Windows-System können Sie z. B. eine Verzeichnisserverinstanz erstellen, die die Kopie einer Instanz auf einem Linux-System ist.

Wenn Sie das Tool zum Kopieren einer Quelleninstanz verwenden, kann es auf Ihren Eingaben basierend die folgenden Operationen ausführen:

- Sie können einen Zielverzeichnisserver mit denselben Konfigurationseinstellungen und Schemadateien der Quellenverzeichnisserverinstanz erstellen. Dieser synchronisiert auch die Schlüssel-Stashdateien auf dem Zielsystem mit dem Quellenserver.
- Wenn die Quellenverzeichnisserverinstanz ein vollständiger Verzeichnisserver ist, ist die Zielverzeichnisserverinstanz, die erstellt wird, ebenfalls ein vollständiger Verzeichnisserver. Sie können auswählen, dass die Daten von der bereits vorhandenen Verzeichnisserverinstanz kopiert werden sollen. Wenn der Quellenverzeichnisserver für die Onlinesicherung konfiguriert wird, können Sie einen funktionalen Zielverzeichnisserver mit Einträgen in dessen Datenbank erstellen.
- Wenn die Quellenverzeichnisserverinstanz ein Proxy-Server ist, ist die Zielverzeichnisserverinstanz, die erstellt wird, ebenfalls ein Proxy-Server.
- Wenn sich der Quellenverzeichnisserver in einer Replikationsumgebung befindet, können Sie die Zielinstanz als Replikatserver oder als Peer-Server des Quellenservers konfigurieren.
- Wenn sich der Quellenverzeichnisserver in einer dezentralen Umgebung befindet, können Sie die Zielverzeichnisserverinstanz als Proxy-Server konfigurieren.

- Wenn die Quellenverzeichnisserverinstanz für sichere Kommunikation konfiguriert wird, kopiert **Instance Administration Tool** die Schlüsseldatenbankdateien auf den Zielverzeichnisserver.

Stellen Sie sicher, dass der Quellenverzeichnisserver die folgenden Bedingungen erfüllt, bevor Sie aus dem Quellenverzeichnisserver einen Verzeichnisserver erstellen:

- Der Quellenverzeichnisserver muss IBM Security Directory Server Version 6.3.1 sein. Der Quellenverzeichnisserver darf keine Instanz der Vorgängerversion sein.
- Der Quellenverzeichnisserver muss im normalen Modus ausgeführt werden. Das Kopieren einer Instanz, die im Konfigurationsmodus ausgeführt wird, wird nicht unterstützt.
- Auf den Quellenverzeichnisserver muss von dem Computer aus zugegriffen werden können, auf dem **Instance Administration Tool** ausgeführt wird.
- Um einen Zielverzeichnisserver als Replikat oder Peer erstellen zu können, muss ein Replikationskontext für die Quellenverzeichnisserverinstanz vorhanden sein. **Instance Administration Tool** kann nicht zum Einrichten des ersten Replikats oder Peers in einer Replikationstopologie verwendet werden. Die Quellenverzeichnisserverinstanz muss mindestens einen definierten Replikationskontext, eine definierte Replikationsgruppe und einen definierten Replikationsuntereintrag enthalten. Wenn Sie die Instanz als Replikat konfigurieren möchten, muss die Quelleninstanz die Erstreplikationstopologie einschließlich einer Vereinbarung mit mindestens einem anderen Server umfassen. Wenn Sie die Instanz als Peer konfigurieren möchten, muss der Quellenserver als Master für mindestens einen der Untereinträge in der Replikationskonfiguration definiert sein.
- Wenn Sie die Instanz als Peer oder Replikat erstellen möchten, wird ein neuer Replikationsuntereintrag unter dem DN `ibm-replicaGroup=default,replicationContext` erstellt. Wenn der DN nicht vorhanden ist, kann die Instanz nicht kopiert werden.

Wenn Sie Daten von der Quellenverzeichnisserverinstanz in die Zielverzeichnisserverinstanz kopieren möchten, müssen die folgenden Anforderungen erfüllt sein:

- Die DB2-Version darf für beide Verzeichnisserverinstanzen unterschiedlich sein. Eine Datenbanksicherung auf einem Betriebssystem kann von jedem Computer mit demselben Betriebssystemtyp wiederhergestellt werden. Sie können beispielsweise eine Datenbank, die mit DB2 UDB Version 9 auf Windows-Systemen erstellt wurde, auf einem System mit DB2 Version 10 wiederherstellen. Auf AIX-, Linux- und Solaris-Systemen können Sie Sicherungen, die mit DB2 UDB Version 9 erstellt wurden, auf DB2 Version 10 wiederherstellen, wenn die Endian-Einstellung (Big Endian oder Little Endian) der Sicherungs- und Wiederherstellungsbetriebssysteme übereinstimmen.
- Sie müssen die Quellenverzeichnisserverinstanz für die Onlinesicherung konfigurieren. Sie können die Onlinesicherung während der Datenbankerstkonfiguration konfigurieren. Zum Konfigurieren der Onlinesicherung können Sie **Instance Administration Tool** oder das **Konfigurationstool** verwenden.
- Sie müssen eine Anfangssicherung der Quellenverzeichnisserverinstanz im Offlinemodus vornehmen, bevor Sie **Instance Administration Tool** zum Kopieren der Verzeichnisserverinstanz verwenden. Der Pfad, den Sie für die Sicherung angeben, darf nur ein Sicherungsbild enthalten.
- Auf den Pfad mit dem Sicherungsbild muss von sowohl der Quellenverzeichnisserverinstanz als auch von der Zielverzeichnisserverinstanz aus zugegriffen werden können.

## Kopie einer vorhandenen Instanz mit dem Instance Administration Tool erstellen

Erstellen Sie mit dem **Instance Administration Tool** eine Kopie einer vorhandenen Instanz.

### Vorbereitende Schritte

Zum Erstellen einer Kopie einer vorhandenen Instanz müssen Sie die folgenden Anforderungen erfüllen:

- Starten Sie den Prozess `ibmslapd` und den Verwaltungsserver der Instanz im normalen Modus.
- Stellen Sie sicher, dass der Zugriff auf den Quellenverzeichnisserver mit dem **Instance Administration Tool** möglich ist.

### Vorgehensweise

1. Starten Sie das **Instance Administration Tool**. Siehe „**Instance Administration Tool** starten“ auf Seite 138.
2. Wählen Sie bei einer Onlinesicherung eine der folgenden Optionen aus, um eine Kopie einer vorhandenen Instanz zu erstellen:
  - Klicken Sie auf **Lokale Instanz kopieren**, um eine Kopie einer vorhandenen Instanz zu erstellen, die sich auf dem lokalen Computer befindet.
  - Klicken Sie auf **Ferne Instanz kopieren**, um eine Kopie einer vorhandenen Instanz zu erstellen, die sich auf einem fernen Computer befindet.
3. Geben Sie in der Anzeige **Verzeichnisserverinstanz kopieren** die folgenden Werte ein:
  - a. Geben Sie im Feld **Host** die IP-Adresse oder den Hostnamen ein, wenn sich der Quellenverzeichnisserver auf einem fernen Computer befindet. Befindet sich der Quellenverzeichnisserver auf einem lokalen Computer, wird das Feld mit `localhost` gefüllt und kann von Ihnen nicht bearbeitet werden.
  - b. Geben Sie im Feld **Port** die Portnummer des Verzeichniservers ein, wenn die Portnummer im Feld ungültig ist. Wenn Sie eine sichere Verbindung verwenden wollen, müssen Sie die gesicherte Portnummer der Quellenverzeichnisserverinstanz angeben.
  - c. Geben Sie im Feld **Administrator-DN** den Administrator-DN des Quellenverzeichniservers ein, wenn sich die Instanz auf einem fernen Computer befindet. Befindet sich der Quellenverzeichnisserver auf einem lokalen Computer, wird das Feld mit dem Wert für den Administrator-DN gefüllt und kann von Ihnen nicht bearbeitet werden.
  - d. Geben Sie im Feld **Kennwort** das Kennwort für den Administrator-DN ein.
  - e. Geben Sie im Feld **Seedwert für die Verschlüsselung** den Seedwert für die Verschlüsselung der Quellenverzeichnisserverinstanz ein.
  - f. Wenn der Quellenverzeichnisserver für sichere Kommunikation konfiguriert wurde und Sie auch den Zielverzeichnisserver so konfigurieren wollen, klicken Sie auf **SSL-Verbindung verwenden**.
    - 1) Geben Sie im Feld **Schlüsseldatei** den Dateinamen und den Pfad der Schlüsseldatenbankdatei ein. Sie können auf **Durchsuchen** klicken, um die gewünschte Position anzugeben.
    - 2) Geben Sie im Feld **Schlüsselname** den Namen des privaten Schlüssels ein, der aus der Schlüsseldatei des Quellenverzeichniservers verwendet werden soll.

- 3) Geben Sie im Feld **Schlüsselkennwort** das Kennwort für die Schlüssel-datenbank der Schlüsseldatei ein.
- g. Klicken Sie auf **Weiter**.
4. Führen Sie in der Anzeige **Instanzkonfiguration - Schritt 1** die folgenden Schritte aus:
  - a. Überprüfen Sie in den Feldern **Quellen-URL** und **Typ der Quelleninstanz** die Angaben zum Quellenverzeichnisserver. Der **Typ der Quelleninstanz** kann ein vollständiger Verzeichnisserver oder eine Proxy-Server-Instanz sein.
  - b. Wählen Sie **Als Peer- oder Replikationsserver konfigurieren** aus, um den Zielverzeichnisserver in einer vorhandenen Replikationstopologie als Peer oder Replikat zu konfigurieren, und wählen Sie eine der folgenden Optionen aus:
    - Klicken Sie auf **Replikat**, um den Zielverzeichnisserver als Replikat zu konfigurieren.
    - Klicken Sie auf **Peer**, um den Zielverzeichnisserver als Peer zu konfigurieren.
  - c. Geben Sie im Feld **Benutzername** die ID des Systembenutzers ein, der als Eigner der Zielverzeichnisserverinstanz fungieren muss. Der Name darf maximal 8 Zeichen umfassen. Derselbe Name wird auch für die Verzeichnisserverinstanz, die DB2-Administrator-ID, die Datenbankinstanz und die Datenbank festgelegt. Die Benutzer-ID muss auf dem Computer bereits vorhanden sein und darf keiner anderen Verzeichnisserverinstanz auf dem Computer zugeordnet sein. Detaillierte Informationen zu dieser Benutzer-ID finden Sie unter „Benutzer und Gruppen, die einer Verzeichnisserverinstanz zugeordnet sind“ auf Seite 125.
  - d. Geben Sie im Feld **Kennwort** das Kennwort für die Benutzer-ID ein.
  - e. Geben Sie im Feld **Instanzposition** die Speicherposition der Verzeichnisserverinstanz ein. Sie können auf **Durchsuchen** klicken und das Ausgangsverzeichnis der Instanz angeben. An der gewünschten Adresse müssen mindestens 30 MB freier Plattenspeicherplatz vorhanden sein. Auf Windows-Systemen muss für die Position ein Plattenlaufwerk, z. B. C:, angegeben werden. Die Dateien der Verzeichnisinstanz werden auf dem angegebenen Plattenlaufwerk im Verzeichnis `\idslapd-instance_name` gespeichert. Die Variable `instance_name` steht für den Namen der Verzeichnisserverinstanz. Auf AIX-, Linux- und Solaris-Systemen ist das Ausgangsverzeichnis des Eigners der Verzeichnisserverinstanz die Standardposition. Allerdings ist es möglich, einen anderen Pfad anzugeben.
  - f. Klicken Sie auf **Weiter**.
5. Führen Sie in der Anzeige **Instanzkonfiguration - Schritt 2** die folgenden Schritte aus:
  - a. Geben Sie im Feld **Administrator-DN** einen gültigen DN für die Zielverzeichnisserverinstanz ein. Bei dem Wert für den Administrator-DN muss die Groß-/Kleinschreibung nicht beachtet werden. Der Benutzer mit dem Administrator-DN hat uneingeschränkten Zugriff auf alle Daten in der Verzeichnisserverinstanz.
  - b. Geben Sie im Feld **Kennwort** das Kennwort für den Administrator-DN ein. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden. DBCS-Zeichen (DBCS = Double Byte Character Set) sind im Kennwort nicht zulässig.
  - c. Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Administrator-DN ein. Merken Sie sich das Kennwort.

- d. Wählen Sie **Daten von Quelleninstanz in neue Instanz kopieren** aus, um Daten aus der Datenbank des Quellenservers auf den Zielservers zu kopieren, und führen Sie die folgenden Schritte aus:

**Anmerkung:** Wurde die Option zum Erstellen des Zielverzeichniservers als Peer oder Replikat ausgewählt, ist dieses Markierungsfeld ausgewählt und kann nicht abgewählt werden.

- 1) Geben Sie im Feld **Pfad für Sicherungsimagen** den Pfadnamen des Sicherungsimagen des Quellenservers ein. Sie können auf **Durchsuchen** klicken, um die gewünschte Position anzugeben. Wenn die Quelleninstanz sich auf einem fernen Computer befindet, muss der Sicherungspfad gemeinsam genutzt werden, damit sowohl der Quellen- als auch der Zielcomputer darauf zugreifen können. Ein Beispiel für einen gemeinsam genutzten Pfad ist eine NFS-Dateisystem mit Lese- und Schreibzugriff.
- e. Klicken Sie auf **Weiter**.
6. Überprüfen Sie in der Anzeige **Einstellungen überprüfen** die generierte Zusammenfassung.
  7. Klicken Sie auf **Fertig stellen**, um die Erstellung von Kopien der Quellenverzeichniserver zu starten.
  8. Überprüfen Sie im Fenster **Ergebnisse** die Protokollnachrichten, die für die Instanzerstellungsoperationen generiert werden.
  9. Klicken Sie auf **Schließen**, um das Fenster **Ergebnisse** zu schließen.
  10. Klicken Sie auf **Schließen**, um das **Instance Administration Tool** zu schließen.

## Ergebnisse

Das **Instance Administration Tool** erstellt auf dem Computer eine Kopie der Quellenverzeichniserverinstanz.

## Nächste Schritte

Sie müssen den Prozess `ibmslapd` und den Verwaltungsserver starten, der der Verzeichniserverinstanz zugeordnet ist. Siehe „Verzeichniserver und Verwaltungsserver starten oder stoppen“ auf Seite 165.

Führen Sie eine Sicherung der Instanz durch. Informationen zum Sichern einer Verzeichniserverinstanz finden Sie unter „Verzeichniserverbackup“ auf Seite 198.

## Kopie einer vorhandenen Instanz mit dem Befehlszeilendienstprogramm erstellen

Mit dem Befehlszeilendienstprogramm `idsideploy` können Sie eine Kopie einer Instanz erstellen.

## Vorbereitende Schritte

Zum Erstellen einer Kopie einer vorhandenen Instanz müssen Sie die folgenden Anforderungen erfüllen:

- Starten Sie den Prozess `ibmslapd` und den Verwaltungsserver der Quelleninstanz im normalen Modus. Siehe „Verzeichniserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.
- Stellen Sie sicher, dass der Zugriff auf den Quellenverzeichniserver mit dem Computer möglich ist, auf dem Sie die Kopie der Instanz erstellen wollen.



## Vorgehensweise

1. Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.
2. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
3. Führen Sie den folgenden Befehl aus, um eine Instanzkopie ohne die Daten von einer vorhandenen Verzeichnisserverinstanz zu erstellen:

```
idsideploy -sU ldap://host:port -sD src_adminDN -sw src_adminPWD  
-e encryptionseed -I instance_name -a instPWD -D adminDN  
-w adminPWD -l inst_location
```

Weitere Informationen zum Befehl **idsideploy** finden Sie in der Veröffentlichung *Command Reference*.

---

## Verzeichnisserver und Verwaltungsserver starten oder stoppen

Um eine Verzeichnisserverinstanz verwenden zu können, müssen der Prozess `ibmslapd` und der Verwaltungsserver, der der Instanz zugeordnet ist, gestartet werden.

Wenn Sie die Konfiguration eines Verzeichnisseservers ändern, müssen Sie den Server und den Verwaltungsserver möglicherweise stoppen und neu starten, damit die Änderungen wirksam werden. Sie können den Verzeichnisserver und den Verwaltungsserver nur stoppen, wenn er im normalen Modus oder im Konfigurationsmodus ausgeführt wird.

Sie können **Instance Administration Server** oder Serverdienstprogramme wie **ibmslapd** und **ibmdiradm** verwenden, um die Server zu starten und zu stoppen. Der Prozess `ibmslapd` wird dem Verzeichnisserver zugeordnet. Die Verzeichnisserverinstanz kann mit **Instance Administration Tool** nur im normalen Modus gestartet werden. Verwenden Sie die Befehlszeilenoptionen zum Starten eines Verzeichnisseservers im reinen Konfigurationsmodus.

Ein Verzeichnisserver kann einen der folgenden Status aufweisen:

- Gestartet
- Gestoppt
- Gestartet (Nur Konfiguration)

Ein Verwaltungsserver kann einen der folgenden Status aufweisen:

- Gestartet
- Gestoppt

## Verzeichnisserver und Verwaltungsserver starten oder stoppen

Mit dem **Instance Administration Tool** können Sie den Verzeichnisserver und/oder den Verwaltungsserver, der einer Instanz zugeordnet ist, starten oder stoppen.

### Vorbereitende Schritte

Zum Starten oder Stoppen eines Verzeichnisseservers und eines Verwaltungsservers müssen Sie die folgenden Bedingungen erfüllen:

1. Es muss eine Instanz mit derselben Version wie das **Instance Administration Tool** vorhanden sein.

2. Wenn keine solche Instanz vorhanden ist, erstellen Sie sie. Siehe „Standardverzeichnisserverinstanz erstellen“ auf Seite 141 oder „Verzeichnisserverinstanz mit angepassten Einstellungen erstellen“ auf Seite 143.

### Vorgehensweise

1. Starten Sie das **Instance Administration Tool**. Siehe „**Instance Administration Tool** starten“ auf Seite 138.
2. Wählen Sie in der **Liste der auf dem System installierten Verzeichnisserverinstanzen** eine Instanz mit derselben Version wie das **Instance Administration Tool** aus.
3. Klicken Sie auf **Starten/Stoppen**, um den Verzeichnisserver und/oder den Verwaltungsserver einer Instanz zu starten oder zu stoppen.
4. Führen Sie im Fenster **Serverstatus verwalten** die folgenden Aktionen aus:
  - Führen Sie die folgenden Schritte aus, um den Verzeichnisserver und/oder den Verwaltungsserver einer Instanz zu starten:
    - Klicken Sie zum Starten des Verzeichniservers auf **Server starten**.
    - Klicken Sie zum Starten des Verwaltungsservers auf **Verwaltungsserver starten**.
    - Klicken Sie auf **OK**.
  - Führen Sie die folgenden Schritte aus, um den Verzeichnisserver und/oder den Verwaltungsserver zu stoppen:
    - Klicken Sie zum Stoppen des Verzeichniservers auf **Server stoppen**.
    - Klicken Sie zum Stoppen des Verwaltungsservers auf **Verwaltungsserver stoppen**.
    - Klicken Sie auf **OK**.
5. Klicken Sie auf **Schließen**, um das Fenster **Serverstatus verwalten** zu schließen.
6. Klicken Sie auf **Schließen**, um das **Instance Administration Tool** zu schließen.

## Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen

Mit den Befehlszeilendienstprogrammen können Sie den Verzeichnisserver und/oder den Verwaltungsserver, der einer Instanz zugeordnet ist, starten oder stoppen.

### Vorbereitende Schritte

Zum Starten oder Stoppen eines Verzeichniservers und eines Verwaltungsservers müssen Sie die folgenden Bedingungen erfüllen:

- Es muss eine Instanz mit derselben Version wie die Befehlszeilendienstprogramme vorhanden sein. Wenn keine solche Instanz vorhanden ist, erstellen Sie sie. Siehe „Standardverzeichnisserverinstanz erstellen“ auf Seite 141 oder „Verzeichnisserverinstanz mit angepassten Einstellungen erstellen“ auf Seite 143.

### Vorgehensweise

1. Melden Sie sich am Computer mit der erforderlichen Berechtigung an. Weitere Informationen finden Sie in Kapitel 20, „Instanzkonfiguration“, auf Seite 177.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.

4. Führen Sie die folgenden Befehle aus, um den Server und den Verwaltungsserver einer Instanz *instance\_name* zu starten: Setzen Sie für die Variable *instance\_name* den Instanznamen ein.  

```
ibmslapd -I instance_name  
ibmdiradm -I instance_name
```
5. Führen Sie die folgenden Befehle aus, um den Server und den Verwaltungsserver einer Instanz zu stoppen: Setzen Sie für die Variable *instance\_name* den Instanznamen ein.  

```
ibmslapd -I instance_name -k  
ibmdiradm -I instance_name -k
```

---

## Konfiguration von Verzeichnisserverinstanzen verwalten

Zum Überprüfen des Status und zum Verwalten und Ändern der Konfiguration von Verzeichnisserverinstanzen oder Proxy-Server-Instanzen können Sie das **Konfigurationstool** verwenden.

Zum Verwalten und Ändern der Konfiguration von Verzeichnisserverinstanzen oder Proxy-Server-Instanzen derselben Version können Sie das **Konfigurationstool** verwenden. Die Version des **Konfigurationstools**, die mit einer Version von IBM Security Directory Server zum Verwalten von Verzeichnisserverinstanzen oder Proxy-Server-Instanzen von vorherigen oder neueren Versionen bereitgestellt wird, kann nicht verwendet werden.

Das **Konfigurationstool** kann mithilfe einer der folgenden Optionen für eine Instanz geöffnet werden:

- Verwenden Sie **Instance Administration Tool**.
- Führen Sie den Befehl **idsxcfg** mit dem Instanznamen als Parameterwert aus.

Weitere Informationen zum **Konfigurationstool** finden Sie in Kapitel 20, „Instanzkonfiguration“, auf Seite 177.

## Konfigurationstool über das Instance Administration Tool öffnen

Öffnen Sie das **Konfigurationstool** von IBM Security Directory Server, um die Konfiguration einer Verzeichnisserverinstanz oder einer Proxy-Server-Instanz zu verwalten oder zu ändern.

### Vorbereitende Schritte

Zum Verwalten einer Instanz mit dem **Konfigurationstool** müssen Sie die folgenden Bedingungen erfüllen:

- Es muss eine Instanz mit derselben Version wie das **Konfigurationstool** vorhanden sein. Wenn keine solche Instanz vorhanden ist, erstellen Sie sie. Siehe „Standardverzeichnisserverinstanz erstellen“ auf Seite 141 oder „Verzeichnisserverinstanz mit angepassten Einstellungen erstellen“ auf Seite 143.

### Vorgehensweise

1. Starten Sie das **Instance Administration Tool**. Siehe „**Instance Administration Tool** starten“ auf Seite 138.
2. Wählen Sie in der **Liste der auf dem System installierten Verzeichnisserverinstanzen** eine Instanz mit derselben Version wie das **Instance Administration Tool** aus.

3. Klicken Sie auf **Verwalten**, um die Instanz mit dem **Konfigurationstool** zu verwalten. Das Fenster **Konfigurationstool** von IBM Security Directory Server wird für die Instanz geöffnet.
4. Klicken Sie auf **Datei > Beenden**, um das **Konfigurationstool** zu schließen.
5. Klicken Sie im Bestätigungsfenster des **Konfigurationstools** auf **Ja**.

---

## TCP/IP-Einstellungen von Instanzen ändern

Zum Ändern der TCP/IP-Einstellungen für eine Verzeichnisserverinstanz oder eine Proxy-Server-Instanz können Sie **Instance Administration Tool** oder die Befehlszeilendienstprogramme verwenden.

Um die TCP/IP-Einstellungen für eine Instanz zu ändern, müssen die Version der Instanz und von **Instance Administration Tool** übereinstimmen.

### TCP/IP-Einstellungen einer Instanz mit dem Instance Administration Tool ändern

Mit dem **Instance Administration Tool** können Sie die TCP/IP-Einstellungen einer vorhandenen Instanz ändern.

#### Vorbereitende Schritte

Zum Ändern der TCP/IP-Einstellungen einer Instanz mit dem **Instance Administration Tool** müssen Sie die folgenden Bedingungen erfüllen:

1. Es muss eine Instanz mit derselben Version wie das **Instance Administration Tool** vorhanden sein.
2. Stoppen Sie den Verzeichnisserver und den Verwaltungsserver der Instanz. Siehe „Verzeichnisserver und Verwaltungsserver starten oder stoppen“ auf Seite 165.

#### Vorgehensweise

1. Starten Sie das **Instance Administration Tool**. Siehe „**Instance Administration Tool** starten“ auf Seite 138.
2. Wählen Sie in der **Liste der auf dem System installierten Verzeichnisserverinstanzen** eine Instanz mit derselben Version wie das **Instance Administration Tool** aus.
3. Klicken Sie auf **TCP/IP-Einstellungen bearbeiten**, um die TCP/IP-Einstellungen der Instanz zu ändern. Das Fenster **TCP/IP-Einstellungen bearbeiten** für die Instanz wird geöffnet.
4. Wählen Sie im Fenster **TCP/IP-Einstellungen bearbeiten** eine der folgenden Optionen aus:
  - Wenn die Instanz an allen auf dem Computer konfigurierten IP-Adressen empfangsbereit sein soll, wählen Sie **Empfangsbereitschaft an allen konfigurierten IP-Adressen** aus.
  - Wenn die Instanz nur an einer bestimmten Gruppe der auf dem Computer konfigurierten IP-Adressen empfangsbereit sein soll, führen Sie die folgenden Schritte aus:
    - a. Deaktivieren Sie die Option **Empfangsbereitschaft an allen konfigurierten IP-Adressen**.
    - b. Wählen Sie in der Liste **IP-Adressen mit Empfangsbereitschaft auswählen** die IP-Adressen aus, an denen die Instanz empfangsbereit sein soll.
5. Klicken Sie auf **Weiter**.

6. Geben Sie in der Anzeige **Portdetails** die folgenden Werte an:

**Anmerkung:** Sie müssen den Verzeichnisserverports eindeutige Portnummern zuweisen, die keine Konflikte mit vorhandenen Ports verursachen, die gerade auf dem Computer verwendet werden. Auf AIX-, Linux- und Solaris-Systemen dürfen Portnummern im Bereich zwischen 1 und 1000 nur mit Rootberechtigung benutzt werden.

- a. Geben Sie im Feld **Server-Port** die Portnummer ein, die der Server als nicht sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - b. Geben Sie im Feld **Sicherer Port des Servers** die Portnummer ein, die der Server als sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - c. Geben Sie im Feld **Port des Verwaltungsservers** die Portnummer ein, die der Verwaltungsserver als nicht sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - d. Geben Sie im Feld **Sicherer Port des Verwaltungsservers** die Portnummer ein, die der Verwaltungsserver als sicheren Port verwenden soll. Diese Nummer muss zwischen 1 und 65535 liegen.
  - e. Klicken Sie auf **Fertig stellen**.
7. Überprüfen Sie im Fenster **TCP/IP-Ergebnisse bearbeiten** die Protokollnachrichten, die für die Bearbeitung der TCP/IP-Einstellungen generiert werden.
  8. Klicken Sie auf **Schließen**, um das Fenster **TCP/IP-Ergebnisse bearbeiten** zu schließen.
  9. Klicken Sie auf **Schließen**, um das **Instance Administration Tool** zu schließen.

## TCP/IP-Einstellungen einer Instanz mit Befehlszeilendienstprogrammen ändern

Mit den Befehlen **idssethost** und **idssetport** können Sie die TCP/IP- und Porteinstellungen einer vorhandenen Instanz ändern.

### Vorbereitende Schritte

Zum Ändern der TCP/IP-Einstellungen einer Instanz mit Befehlszeilendienstprogrammen müssen Sie die folgenden Bedingungen erfüllen:

1. Es muss eine Instanz mit derselben Version wie die Befehlszeilendienstprogramme vorhanden sein.
2. Stoppen Sie den Verzeichnisserver und den Verwaltungsserver der Instanz. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

### Vorgehensweise

1. Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.
2. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
3. Wählen Sie eine der folgenden Optionen aus, um die IP-Adressen des Verzeichnisservers *instance\_name* zu aktualisieren: Setzen Sie für die Variable *instance\_name* den Instanznamen ein.

Zu bindende IP-Adresse	Befehl:
Eine bestimmte IP-Adresse (xx.xx.xx.xx) auf dem Computer	<code>idssethost -I instance_name -i xx.xx.xx.xx</code>
Alle auf dem Computer konfigurierten IP-Adressen	<code>idssethost -I instance_name -i all</code>

- Wählen Sie eine der folgenden Optionen aus, um die Portnummern des Verzeichnisseservers *instance\_name* zu aktualisieren: Setzen Sie für die Variable *instance\_name* den Instanznamen ein.

**Anmerkung:** Sie müssen den Verzeichnisseserverports eindeutige Portnummern zuweisen, die keine Konflikte mit vorhandenen Ports verursachen, die gerade auf dem Computer verwendet werden. Auf AIX-, Linux- und Solaris-Systemen dürfen Portnummern im Bereich zwischen 1 und 1000 nur mit Rootberechtigung benutzt werden.

Zu konfigurierende Ports	Befehl:
Server-Port	<code>idssetport -I instance_name -p port_no</code>
Sicherer Port des Servers	<code>idssetport -I instance_name -s secure_port</code>
Port des Verwaltungsservers	<code>idssetport -I instance_name -a adm_port</code>
Sicherer Port des Verwaltungsservers	<code>idssetport -I instance_name -c adm_secure_port</code>

Weitere Informationen zu den Befehlen **idssethost** und **idssetport** finden Sie in der Veröffentlichung *Command Reference*.

- Starten Sie den Verzeichnisseserver und den Verwaltungsserver. Siehe „Verzeichnisseserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

---

## Informationen zu einer Instanz anzeigen

Mithilfe von **Instance Administration Tool** oder dem Befehlszeilendienstprogramm können Instanzdetails wie das Instanzausgangsverzeichnis, IP-Adressen und Ports angezeigt werden.

Es können Informationen zu allen auf dem Computer vorhandenen Instanzen angezeigt werden. Der Instanzstatus kann "Gestoppt" oder "Gestartet" sein.

Der Befehl **idsilist** ermöglicht auch das Anzeigen ähnlicher Informationen für eine Instanz oder für alle auf dem Computer verfügbaren Instanzen. Weitere Informationen zum Befehl **idsilist** finden Sie in der *Befehlsreferenz*.

## Instanzinformationen mit dem Instance Administration Tool anzeigen

Mit dem **Instance Administration Tool** können Sie die Details einer vorhandenen Instanz anzeigen.

### Vorgehensweise

- Starten Sie das **Instance Administration Tool**. Siehe „**Instance Administration Tool** starten“ auf Seite 138.
- Wählen Sie in der **Liste der auf dem System installierten Verzeichnisseserverinstanzen** eine Instanz aus, deren Details Sie anzeigen wollen.

3. Klicken Sie auf **Anzeigen**. Das Fenster **Instanzdetails anzeigen** mit allgemeinen Angaben und TCP/IP-Details zu der ausgewählten Instanz wird angezeigt.
4. Klicken Sie auf **Schließen**, um das Fenster **Instanzdetails anzeigen** zu schließen.
5. Klicken Sie auf **Schließen**, um das **Instance Administration Tool** zu schließen.

## Informationen zu einer Instanz mit dem Befehlszeilendienstprogramm anzeigen

Mit dem Befehl **idsilist** können Sie Informationen zu einer vorhandenen Instanz anzeigen.

### Vorgehensweise

1. Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.
2. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
3. Führen Sie den passenden Befehl **idsilist** aus, um Informationen zu den Instanzen auf einem Computer anzuzeigen:

Task	Befehl:
Alle Instanzen auflisten	<code>idsilist</code>
Alle Instanzen mit vollständigen Informationen und kompletter Beschreibung auflisten	<code>idsilist -a</code>
Alle Instanzen mit vollständigen, unformatierten Informationen auflisten	<code>idsilist -r</code>
Bestimmte Instanz auflisten	<code>idsilist -I instance_name</code>
Bestimmte Instanz mit vollständigen Informationen und kompletter Beschreibung auflisten	<code>idsilist -I instance_name -a</code>
Bestimmte Instanz mit vollständigen, unformatierten Informationen auflisten	<code>idsilist -I instance_name -r</code>

Weitere Informationen zum Befehl **idsilist** finden Sie in der *Befehlsreferenz*.

---

## Verzeichnisserverinstanzen löschen

Sie können **Instance Administration Tool** oder das Befehlszeilendienstprogramm zum Löschen einer Verzeichnisserverinstanz oder einer Proxy-Server-Instanz verwenden.

Möglicherweise müssen Sie eine Instanz von einem Computer löschen, wenn Sie eine Instanz auf einen anderen Computer migriert haben oder Sie die Instanz nicht mehr benötigen.

Wenn Sie einen Verzeichnisserver mit einer DB2-Datenbank löschen, ist es empfehlenswert, vor dem Löschen der Instanz ein Backup durchzuführen. Wenn Sie eine Proxy-Server-Instanz löschen, ist es empfehlenswert, ein Backup von der Instanz durchzuführen.

**Anmerkung:** Für Proxy-Server-Instanzen ist das Löschen einer Instanz die einzige gültige Option.

Mit **Instance Administration Tool** können Sie zwischen den folgenden Optionen wählen:

- Eine Verzeichnisserverinstanz löschen und die Datenbankinstanz beibehalten
- Eine Verzeichnisserverinstanz löschen und die zugehörige DB2-Datenbankinstanz entfernen

Mit dem Befehl **idsidrop** können Sie zwischen den folgenden Optionen wählen:

- Eine Verzeichnisserverinstanz löschen und die Datenbankinstanz beibehalten
- Eine Verzeichnisserverinstanz löschen und die zugehörige DB2-Datenbankinstanz entfernen
- Die Verzeichnisserverinstanz von der DB2-Datenbankinstanz dekonfigurieren und die Verzeichnisserverinstanz nicht löschen

Weitere Informationen zum Befehl **idsidrop** finden Sie in der *Befehlsreferenz*.

## Instanzen mit dem Instance Administration Tool löschen

Mit dem **Instance Administration Tool** können Sie eine Verzeichnisserverinstanz oder eine Proxy-Server-Instanz löschen.

### Vorbereitende Schritte

Zum Ändern der TCP/IP-Einstellungen einer Instanz mit dem **Instance Administration Tool** müssen Sie die folgenden Bedingungen erfüllen:

1. Es muss eine Instanz mit derselben Version wie das **Instance Administration Tool** vorhanden sein.
2. Stoppen Sie den Verzeichnisserver und den Verwaltungsserver der Instanz. Siehe „Verzeichnisserver und Verwaltungsserver starten oder stoppen“ auf Seite 165.

### Vorgehensweise

1. Starten Sie das **Instance Administration Tool**. Siehe „**Instance Administration Tool** starten“ auf Seite 138.
2. Wählen Sie in der **Liste der auf dem System installierten Verzeichnisserverinstanzen** eine Instanz mit derselben Version wie das **Instance Administration Tool** aus.
3. Klicken Sie auf **Löschen**, um die Löschoperation zu starten.
4. Führen Sie im Fenster **Verzeichnisserverinstanz löschen** die folgenden Schritte aus:
  - a. Wählen Sie eine der folgenden Löschmethoden aus:
    - Klicken Sie auf **Nur Verzeichnisserverinstanz löschen**, um nur die Verzeichnisserverinstanz, nicht jedoch die zugehörige DB2-Datenbankinstanz zu löschen.

**Anmerkung:** Bei einer Proxy-Server-Instanz ist **Nur Verzeichnisserverinstanz löschen** die einzige gültige Option.

- Klicken Sie auf **Verzeichnisserverinstanz und zugehörige Datenbankinstanz löschen**, um nur die Verzeichnisserverinstanz mit der zugehörigen DB2-Datenbankinstanz zu löschen.
- b. Klicken Sie auf **Löschen**.
- c. Klicken Sie im Fenster **Warnung** auf **Ja**, um die Löschung der Instanz zu bestätigen.



- d. Klicken Sie im Fenster **Informationen** auf **OK**.
- e. Klicken Sie auf **Schließen**, um das Fenster **Verzeichnisserverinstanz löschen** zu schließen.
- f. Klicken Sie auf **Schließen**, um das **Instance Administration Tool** zu schließen.

## Instanz mit dem Befehlszeilendienstprogramm löschen

Mit dem Befehl **idsidrop** können Sie eine vorhandene Instanz löschen.

### Vorbereitende Schritte

Zum Löschen einer Instanz mit dem Befehlszeilendienstprogramm müssen Sie die folgenden Bedingungen erfüllen:

1. Es muss eine Instanz mit derselben Version wie das Befehlszeilendienstprogramm vorhanden sein.
2. Stoppen Sie den Verzeichnisserver und den Verwaltungsserver der Instanz. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

### Vorgehensweise

1. Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.
2. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
3. Wählen Sie eine der folgenden Optionen aus, um eine Instanz *instance\_name* zu löschen. Setzen Sie für die Variable *instance\_name* den Instanznamen ein.

Task	Befehl:
Verzeichnisserverinstanz löschen und zugehörige Datenbankinstanz beibehalten	<code>idsidrop -I instance_name</code>
Verzeichnisserverinstanz löschen und zugehörige Datenbankinstanz ebenfalls löschen	<code>idsidrop -I instance_name -r</code>
Zugehörige Datenbankinstanz dekonfigurieren, ohne die Verzeichnisserverinstanz zu löschen	<code>idsidrop -I instance_name -R</code>

Weitere Informationen zum Befehl **idsidrop** finden Sie in der Veröffentlichung *Command Reference*.



---

## Kapitel 19. Verzeichnisstruktur überprüfen

Nach der Installation von IBM Security Directory Server muss die Verzeichnisstruktur überprüft werden.

### Windows-32-Bit- und -64-Bit-Systeme

Nach der Installation von IBM Security Directory Server auf einem Windows-Betriebssystem finden Sie die folgenden Verzeichnisse und Dateien in der Installationsposition, zum Beispiel: C:\Program Files\IBM\LDAP\V6.3.1 (Sie können die Installationsposition ändern).

- appsrv
- etc
- java
- lib
- messages
- bin
- examples
- javali
- lib64
- nls
- var
- codeset
- idstools
- jre
- license
- properties
- config
- include
- ldapcfg.ico
- logs
- sbin

### Linux-64-Bit-Systeme

Nach der Installation von IBM Security Directory Server auf einem Linux-Betriebssystem finden Sie die folgenden Verzeichnisse und Dateien in der Installationsposition, zum Beispiel: /opt/ibm/ldap/V6.3.1 (Sie können die Installationsposition nicht ändern).

- bin
- codeset
- config
- etc
- examples
- idstools
- include
- javali
- LAPID
- lib
- lib64
- nls

properties  
sbin  
tmp  
web

---

## Kapitel 20. Instanzkonfiguration

Für die Konfiguration einer Verzeichnisserverinstanz oder einer Proxy-Server-Instanz entsprechend Ihren Anforderungen können Sie das **Konfigurationstool** oder die Befehlszeilendienstprogramme verwenden.

Das IBM Security Directory Server-**Konfigurationstool** (**idsxcfg**) ist eine grafische Benutzeroberfläche (GUI), mithilfe derer Sie eine Instanz konfigurieren können. Für die Verwendung des **Konfigurationstools** ist Java Development Kit erforderlich.

Um das **Konfigurationstool** zu starten, müssen Sie sich mit den folgenden Berechtigungsnachweisen anmelden:

### AIX, Linux oder Solaris

- Rootbenutzer
- Verzeichnisserverinstanzeigner
- Benutzer-ID aus der Primärgruppe des Verzeichnisserverinstanzeigners

### Windows

- Benutzer-ID aus der Standardadministratorgruppe

Sie können das **Konfigurationstool** auch zum Ändern Ihrer vorhandenen Verzeichnisserverkonfiguration verwenden.

Das **Konfigurationstool** kann für die folgenden Tasks für eine vollständige Verzeichnisserverinstanz verwendet werden:

- Starten oder Stoppen des Servers
- Verwalten des Hauptadministrator-DNs und -Kennworts
- Konfigurieren und Dekonfigurieren einer DB2-Datenbank für eine Verzeichnisserverinstanz
- Optimieren der einer Instanz zugeordneten Datenbank
- Pflegen der DB2-Datenbank mit indexierter DB2-Organisation oder DB2-Zeilenumkomprimierung
- Sichern und Wiederherstellen der Datenbank
- Optimieren der Leistung der Verzeichnisserverinstanz
- Aktivieren und Inaktivieren des Änderungsprotokolls
- Hinzufügen und Entfernen von Suffixen
- Hinzufügen und Entfernen von Schemadateien
- Importieren und Exportieren von LDIF-Daten
- Konfigurieren der Active Directory-Synchronisation

Das **Konfigurationstool** kann für die folgenden Tasks für eine Proxy-Server-Instanz verwendet werden:

- Starten oder Stoppen des Servers
- Verwalten des Hauptadministrator-DNs und -Kennworts
- Hinzufügen und Entfernen von Suffixen
- Hinzufügen und Entfernen von Schemadateien
- Sichern und Wiederherstellen der Instanz

---

## Konfigurationstool starten

Starten Sie das IBM Security Directory Server **Konfigurationstool** für eine Instanz, um die Instanz entsprechend den Anforderungen Ihrer Verzeichnisumgebung zu konfigurieren.

### Vorbereitende Schritte

Zum Verwalten einer Instanz mit dem **Konfigurationstool** müssen Sie die folgenden Bedingungen erfüllen:

- Es muss eine Instanz mit derselben Version wie das **Konfigurationstool** vorhanden sein. Wenn keine solche Instanz vorhanden ist, erstellen Sie sie. Siehe „Verzeichnisserverinstanz mit angepassten Einstellungen erstellen“ auf Seite 143 oder „Proxy-Server-Instanz mit angepassten Einstellungen erstellen“ auf Seite 150.
- Im Installationspfad von IBM Security Directory Server muss IBM Java Development Kit vorhanden sein. Den Standardinstallationspfad von IBM Security Directory Server finden Sie unter „Standardinstallationspositionen“ auf Seite 28.

### Vorgehensweise

1. Melden Sie sich am Computer mit den erforderlichen Berechtigungen an. Weitere Informationen finden Sie in Kapitel 20, „Instanzkonfiguration“, auf Seite 177.
2. Öffnen Sie eine Eingabeaufforderung.
3. Ändern Sie das aktuelle Verzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Führen Sie den Befehl **idsxcfg** im folgenden Format aus: Setzen Sie für die Variable `instance_name` den Instanznamen ein.  

```
idsxcfg -I instance_name
```

Das Fenster **Konfigurationstool** von IBM Security Directory Server wird für die angegebene Instanz geöffnet.

5. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
6. Klicken Sie im Bestätigungsfenster des **Konfigurationstools** auf **Ja**.

---

## Verzeichnisserver und Verwaltungsserver mithilfe des Konfigurationstools starten oder stoppen

Sie können das **Konfigurationstool** zum Starten des Prozesses `ibmslapd` und des Verwaltungsservers verwenden, der einer Instanz zugeordnet ist.

Wenn Sie die Konfiguration eines Verzeichnisseservers ändern, müssen Sie den Server und den Verwaltungsserver möglicherweise stoppen und neu starten, damit die Änderungen wirksam werden. Sie können den Verzeichnisserver und den Verwaltungsserver nur stoppen, wenn er im normalen Modus oder im Konfigurationsmodus ausgeführt wird.

Zum Starten und Stoppen des Servers und des Verwaltungsservers können Sie das **Konfigurationstool** oder Serverdienstprogramme wie `ibmslapd` und `ibmdiradm` verwenden. Der Prozess `ibmslapd` wird dem Verzeichnisserver zugeordnet. Die Verzeichnisserverinstanz kann mit dem **Konfigurationstool** nur im normalen Modus gestartet werden. Verwenden Sie die Befehlszeilenoptionen zum Starten eines Verzeichnisseservers im reinen Konfigurationsmodus.

Ein Verzeichnisserver kann einen der folgenden Status aufweisen:

- Gestartet
- Gestoppt
- Gestartet (Nur Konfiguration)

Ein Verwaltungsserver kann einen der folgenden Status aufweisen:

- Gestartet
- Gestoppt

## Verzeichnisserver und Verwaltungsserver mit dem Konfigurationstool starten oder stoppen

Mit dem **Konfigurationstool** können Sie den Verzeichnisserver und/oder den Verwaltungsserver, der einer Instanz zugeordnet ist, starten oder stoppen.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool starten**“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Serverstatus verwalten**.
3. Überprüfen Sie auf der Seite **Aktueller Status** den aktuellen Status des Servers und des Verwaltungsservers.
4. Führen Sie auf der Seite **Aktueller Status** die folgenden Aktionen aus:
  - Führen Sie die folgenden Schritte aus, um den Verzeichnisserver und/oder den Verwaltungsserver einer Instanz zu starten:
    - Klicken Sie zum Starten des Verzeichnisseservers auf **Server starten**.
    - Klicken Sie zum Starten des Verwaltungsservers auf **Verwaltungsserver starten**.
    - Klicken Sie im Fenster **Informationen** auf **OK**.
  - Führen Sie die folgenden Schritte aus, um den Verzeichnisserver und/oder den Verwaltungsserver zu stoppen:
    - Klicken Sie zum Stoppen des Verzeichnisseservers auf **Server stoppen**.
    - Klicken Sie zum Stoppen des Verwaltungsservers auf **Verwaltungsserver stoppen**.
    - Klicken Sie im Fenster **Informationen** auf **OK**.
5. Klicken Sie auf **Schließen**, um die Seite **Aktueller Status** zu schließen.
6. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
7. Klicken Sie im Bestätigungsfenster des **Konfigurationstools** auf **Ja**.

## Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen

Mit den Befehlszeilendienstprogrammen können Sie den Verzeichnisserver und/oder den Verwaltungsserver, der einer Instanz zugeordnet ist, starten oder stoppen.

### Vorbereitende Schritte

Zum Starten oder Stoppen eines Verzeichnisseservers und eines Verwaltungsservers müssen Sie die folgenden Bedingungen erfüllen:

- Es muss eine Instanz mit derselben Version wie die Befehlszeilendienstprogramme vorhanden sein. Wenn keine solche Instanz vorhanden ist, erstellen Sie sie. Siehe „Standardverzeichniserverinstanz erstellen“ auf Seite 141 oder „Verzeichniserverinstanz mit angepassten Einstellungen erstellen“ auf Seite 143.

### Vorgehensweise

1. Melden Sie sich am Computer mit der erforderlichen Berechtigung an. Weitere Informationen finden Sie in Kapitel 20, „Instanzkonfiguration“, auf Seite 177.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Führen Sie die folgenden Befehle aus, um den Server und den Verwaltungsserver einer Instanz `instance_name` zu starten: Setzen Sie für die Variable `instance_name` den Instanznamen ein.

```
ibmslapd -I instance_name
ibmdiradm -I instance_name
```

5. Führen Sie die folgenden Befehle aus, um den Server und den Verwaltungsserver einer Instanz zu stoppen: Setzen Sie für die Variable `instance_name` den Instanznamen ein.

```
ibmslapd -I instance_name -k
ibmdiradm -I instance_name -k
```

---

## Hauptadministrator-DNs für eine Instanz verwalten

Damit Sie auf die Konfigurations- und alle Verzeichnisdaten einer Instanz zugreifen können, müssen Sie einen definierten Namen (DN) für den Hauptadministrator einer Instanz erstellen und konfigurieren.

Der Administrator-DN ist der DN, der vom Hauptadministrator einer Instanz verwendet wird. Für eine Instanz kann nur ein einziger Hauptadministrator erstellt werden.

Der Standard-DN ist `cn=root`. Beim DN-Wert muss Groß-/Kleinschreibung nicht beachtet werden.

Ein DN enthält `Attribut:Wert`-Paare, die durch Kommas getrennt werden. Im Folgenden wird ein Beispiel für einen DN-Wert gezeigt:

```
cn=Ben Gray,ou=dept_audit,o=sample
```

Zum Festlegen oder Ändern des Hauptadministrator-DNs können Sie das **Konfigurationstool** oder das Befehlszeilendienstprogramm `idsdnpw` verwenden. Zum Festlegen oder Ändern des Hauptadministrator-DNs muss der Prozess `ibmslapd`, der der Instanz zugeordnet ist, gestoppt werden.

### Hauptadministrator-DN mit dem Konfigurationstool verwalten

Mit dem **Konfigurationstool** können Sie den Hauptadministrator-DN für eine Instanz konfigurieren.

#### Vorbereitende Schritte

Zum Konfigurieren des Hauptadministrator-DN für eine Instanz müssen Sie die folgenden Anforderungen erfüllen:

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.



## Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Administrator-DN verwalten**.
3. Geben Sie im Feld **Administrator-DN** den DN für den Hauptadministrator ein oder übernehmen Sie den DN-Standardwert `cn=root`.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **OK**, um Ihre Aktion zu bestätigen.
6. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
7. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Nächste Schritte

Starten Sie den Verzeichnissever. Siehe „Verzeichnissever und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## Hauptadministrator-DN mit dem Befehlszeilendienstprogramm verwalten

Mit dem Befehlszeilendienstprogramm **idsdnpw** können Sie den Hauptadministrator-DN einer Instanz verwalten.

### Vorbereitende Schritte

Zum Konfigurieren des Hauptadministrator-DN für eine Instanz müssen Sie die folgenden Anforderungen erfüllen:

- Stoppen Sie den Verzeichnissever. Siehe „Verzeichnissever und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

### Informationen zu diesem Vorgang

Wenn Sie für den Administrator-DN keinen Wert angeben, wird in der Datei `ibmslapd.conf` der Standardwert `cn=root` für die Verzeichnisseverinstanz festgelegt. Sie müssen das Hauptadministratorkennwort für eine Instanz angeben.

Wenn Sie kein Kennwort angeben, fordert Sie der Befehl **idsdnpw** zur Eingabe eines Kennworts auf. Das Kennwort wird bei der Eingabe an der Eingabeaufforderung nicht angezeigt.

### Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisseverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Führen Sie zum Festlegen des Administrator-DN für eine Instanz den folgenden Befehl aus: Setzen Sie für `instance_name`, `adminDN` und `adminPWD` Werte entsprechend Ihren Anforderungen ein.

```
idsdnpw -I instance_name -u adminDN -p adminPWD
```

Weitere Informationen zum Befehl **idsdnpw** finden Sie in der Veröffentlichung *Command Reference*.

## Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

---

## Hauptadministrator Kennwort für eine Instanz verwalten

Um sich bei einer Instanz zu authentifizieren und auf die Konfiguration und alle Verzeichnisdaten zugreifen zu können, müssen Sie ein Hauptadministrator Kennwort für eine Instanz erstellen und konfigurieren.

Beim Administrator Kennwort muss die Groß-/Kleinschreibung beachtet werden. Sie können für das Kennwort keine Doppelbytezeichen verwenden, da dies nicht unterstützt wird. Speichern Sie das Administrator Kennwort für die zukünftige Verwendung.

Sie können das **Konfigurationstool** oder das Befehlszeilendienstprogramm **idsdnpw** zum Konfigurieren des Hauptadministrator Kennworts verwenden. Zum Konfigurieren des Administrator Kennworts muss der Prozess **ibmslapd**, der der Instanz zugeordnet ist, gestoppt werden.

Wenn die Verwaltungskennwortrichtlinie aktiviert wird, muss das Hauptadministrator Kennwort den Anforderungen der Verwaltungskennwortrichtlinie entsprechen. Informationen zur Kennwortrichtlinie finden Sie im Abschnitt *Verwaltung* der IBM Security Directory Server-Dokumentation.

## Hauptadministrator Kennwort mit dem Konfigurationstool verwalten

Mit dem **Konfigurationstool** können Sie das Kennwort des Hauptadministrators für eine Instanz konfigurieren.

### Vorbereitende Schritte

Zum Konfigurieren des Kennworts für den Hauptadministrator einer Instanz müssen Sie die folgenden Anforderungen erfüllen:

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Administrator Kennwort verwalten**.
3. Geben Sie im Feld **Administrator Kennwort** das Kennwort für den Hauptadministrator ein.
4. Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Hauptadministrator ein.
5. Klicken Sie auf **OK**.
6. Klicken Sie auf **OK**, um Ihre Aktion zu bestätigen.
7. Klicken Sie auf **OK**, um die Seite **Administrator Kennwort verwalten** zu schließen.
8. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.

9. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

### Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## Hauptadministratorkennwort mit dem Befehlszeilendienstprogramm verwalten

Mit dem Befehlszeilendienstprogramm **idsdnpw** können Sie das Hauptadministratorkennwort einer Instanz verwalten.

### Vorbereitende Schritte

Zum Konfigurieren des Hauptadministratorkennworts für eine Instanz müssen Sie die folgenden Anforderungen erfüllen:

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

### Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisserverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Führen Sie zum Festlegen des Administratorkennworts für eine Instanz den folgenden Befehl aus: Setzen Sie für `instance_name`, `adminDN` und `adminPWD` Werte entsprechend Ihren Anforderungen ein.

```
idsdnpw -I instance_name -u adminDN -p adminPWD
```

Weitere Informationen zum Befehl **idsdnpw** finden Sie in der Veröffentlichung *Command Reference*.

### Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

---

## Datenbankkonfiguration für Verzeichnisserverinstanzen

Um eine Instanz als Verzeichnisserver verwenden und Verzeichnisdaten speichern zu können, muss für die Instanz eine DB2-Datenbank konfiguriert werden.

Sie können **Instance Administration Tool**, das **Konfigurationstool** oder den Befehl **idscfgdb** zum Erstellen und Konfigurieren von DB2-Datenbanken verwenden. Der Verzeichnisserver muss gestoppt werden, bevor die Datenbank konfiguriert oder dekonfiguriert werden kann. Weitere Informationen zum Befehl **idscfgdb** finden Sie in der *Befehlsreferenz*.

Wenn Sie die Standardinstanz mit **Instance Administration Tool** erstellen möchten, wird auch die DB2-Datenbankinstanz für die Instanz erstellt und konfiguriert. Bei Proxy-Server-Instanzen muss keine DB2-Datenbank konfiguriert werden.

Wenn Sie eine DB2-Datenbank für eine Instanz konfigurieren, wird die Konfigurationsdatei der Instanz mit den DB2-Datenbankinformationen aktualisiert. Das Tool erstellt auch die Einstellungen für die Datenbank und die lokalen Prüfschleifen.

Die Datenbankeinstellungen sowie die Einstellungen für den lokalen Loopback-Service werden, sofern diese noch nicht definiert sind, nun erstellt. Sie können festlegen, ob Sie die Datenbank als lokale Codepagedatenbank oder als UTF-8-Datenbank erstellen möchten. Die Standardcodepage, die für die DB2-Datenbankerstellung verwendet wird, ist UTF-8.

## Datenbank mit dem Konfigurationstool für eine Instanz konfigurieren

Konfigurieren Sie mithilfe des **Konfigurationstools** die DB2-Datenbank für eine Verzeichnisserverinstanz.

### Vorbereitende Schritte

Führen Sie die folgenden Tasks aus, um eine DB2-Datenbank für eine Verzeichnisserverinstanz zu konfigurieren:

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.
- Es muss eine Systembenutzer-ID vorhanden sein, die als Eigner der DB2-Datenbankinstanz fungiert. Weitere Informationen zu den Anforderungen an die Systembenutzer-ID finden Sie unter „Benutzer und Gruppen, die einer Verzeichnisserverinstanz zugeordnet sind“ auf Seite 125.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Datenbanktasks** > **Datenbank konfigurieren**.
3. Wählen Sie auf der Seite **Datenbank konfigurieren** eine der folgenden Optionen aus:
  - Führen Sie die folgenden Schritte aus, um eine Datenbank für eine Instanz zu konfigurieren:
    - a. Geben Sie im Feld **Datenbankbenutzername** die ID des Systembenutzers ein, der als Eigner der Datenbank fungieren muss. Die Verzeichnisserverinstanz verwendet diese Systembenutzer-ID, um eine Verbindung zur Datenbank herzustellen.
    - b. Geben Sie im Feld **Kennwort** das Kennwort für den Datenbankadministrator ein.
    - c. Geben Sie im Feld **Datenbankname** den Datenbanknamen ein.
    - d. Wählen Sie **Erweiterte Tabellenbereichsoptionen anzeigen** aus, wenn Sie eine oder mehrere der folgenden DB2-Konfigurationseinstellungen festlegen wollen.
      - Sie wollen die Datenbank für die Verwendung von SMS-Datenspeichern (SMS = System Managed Storage) für die DB2-Tabellenbereiche konfigurieren. Bei Verwendung von SMS ordnet der **Dateisystemmanager** des Betriebssystems den Tabellenbereich zu, in dem die DB2-Tabellen gespeichert werden, und verwaltet diesen auch.
      - Sie wollen die Datenbank für die Verwendung von DMS-Datenspeichern (DMS = Database Managed Storage) für die DB2-Tabellenberei-

che konfigurieren. Außerdem wollen Sie die Datenbank für die Tabellenbereiche USERSPACE1 und LDAPSPACE mit Größe und Position konfigurieren. Bei Verwendung von DMS werden die Tabellenbereiche vom Datenbankmanager verwaltet. Der Datenbankadministrator legt fest, welche Einheiten und Dateien verwendet werden sollen, und DB2 verwaltet den Speicherplatz auf diesen Einheiten und in diesen Dateien.

Wenn Sie **Erweiterte Tabellenbereichsoptionen anzeigen** nicht auswählen, wird eine DB2-Datenbank mit den Tabellenbereichen USERSPACE1 und LDAPSPACE anhand von DMS mit den Standardwerten für Größe und Position erstellt. Wenn Sie eine Instanz mit einer vorhandenen Datenbank konfigurieren, wird **Erweiterte Tabellenbereichsoptionen anzeigen** inaktiviert, wenn Sie den Namen einer vorhandenen Datenbank im Feld **Datenbankname** eingeben.

- e. Klicken Sie auf **Weiter**.
- Führen Sie die folgenden Schritte aus, um das Kennwort des Datenbankadministrators noch einmal zu konfigurieren:
  - a. Klicken Sie auf **Kennwort zurücksetzen**.
  - b. Geben Sie im Feld **Kennwort** das Kennwort für den Datenbankadministrator ein.
  - c. Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Datenbankadministrator ein.
  - d. Klicken Sie auf **Weiter**.
4. Führen Sie die folgenden Schritte aus, wenn Sie eine DB2-Datenbank erstellen und konfigurieren:
  - a. Geben Sie im Feld **Installationsposition der Datenbank** den Pfad zur Speicherposition der Datenbank ein. Sie können auf **Durchsuchen** klicken, um ein Verzeichnis anzugeben. Unter Windows müssen Sie ein Plattenlaufwerk angeben, beispielsweise C:. Unter AIX, Linux und Solaris müssen Sie die Position als Verzeichnisnamen, z. B. /home/1dapdb, angeben.

**Anmerkung:** Der mindestens erforderliche Plattenspeicherplatz für eine DMS-Datenbank beträgt 1 GB. Eine SMS-Datenbank benötigt mindestens 150 MB Plattenspeicherplatz. Diese Anforderungen gelten für eine leere Datenbank. Wenn Sie Daten in der Datenbank speichern, dann ist mehr Plattenspeicherplatz erforderlich.

- b. Führen Sie die folgenden Schritte aus, um den Verzeichnisserver mit der Datenbank für die Onlinesicherung zu konfigurieren:
  - 1) Wählen Sie **Für Onlinesicherung konfigurieren** aus.
  - 2) Geben Sie im Feld **Datenbanksicherungsposition** die Speicherposition ein, an der das Sicherungsimago gespeichert werden soll. Sie können auf **Durchsuchen** klicken, um die gewünschte Position anzugeben.

**Anmerkung:** Die Ausführung des **Konfigurationstools** darf nicht unterbrochen und der Vorgang nicht abgebrochen werden, während die Sicherungsoperation ausgeführt wird.

Wenn Sie die Datenbank nach Abschluss der Datenbankkonfiguration für die Onlinesicherung konfigurieren, wird eine Anfangs-Offlinesicherung der Datenbank ausgeführt. Nachdem der Vorgang der Offlinesicherung abgeschlossen ist, wird der Verwaltungsserver erneut gestartet. Sie können die Onlinesicherung für eine Verzeichnisserverinstanz auch mit dem **idscfgdb** konfigurieren. Sie können die Onlinesicherung jedoch nicht mit dem Befehl **idscfgdb** und dem Parameter **-c** dekonfigurieren. Wenn Sie die Onlinesi-

cherung für eine Instanz mit dem **Instance Administration Tool** oder dem **Konfigurationstool** durchführen, können Sie die Konfiguration mit dem **Konfigurationstool** oder dem Befehl **idscfgdb** wieder aufheben.

- c. Wählen Sie im Bereich **Zeichensatzoption** eine der folgenden Optionen aus, um einen Datenbanktyp zu erstellen:

**Anmerkung:** Erstellen Sie eine DB2-Datenbank im Universalzeichensatz, wenn in dem Verzeichnisserver Daten in mehreren Sprachen gespeichert werden sollen. Eine DB2-Datenbank im Universalzeichensatz ist auch deshalb die effizienteste Lösung, weil weniger Daten umgesetzt werden müssen. Wenn Sie Sprachentags einsetzen wollen, muss die Datenbank im UTF-8-Format definiert sein. Weitere Informationen zu UTF-8 finden Sie in „UTF-8-Unterstützung“ auf Seite 130.

- Klicken Sie auf **DB2-Datenbank im Universalzeichensatz erstellen**, um eine Datenbank im Universalzeichensatz (UCS Transformation Format, UTF-8) zu erstellen, in der LDAP-Clients Daten in diesem Format speichern können.
- Klicken Sie auf **DB2-Datenbank in der lokalen Codepage erstellen**, um eine Datenbank in der lokalen Codepage zu erstellen.

- d. Klicken Sie auf **Weiter**.

5. Wenn Sie **Erweiterte Tabellenbereichsoptionen anzeigen** ausgewählt haben, müssen Sie die folgenden Schritte ausführen:

- a. Wählen Sie in der Liste **Tabellenbereichstyp der Datenbank auswählen** einen Datenbanktyp aus. Der Tabellenbereichstyp der Datenbank ist standardmäßig DMS. Wenn Sie SMS als Tabellenbereichstyp der Datenbank auswählen, werden alle anderen Felder inaktiviert. Die Unterstützung für DMS-Tabellenbereiche wird nur für die Tabellenbereiche USERSPACE1 und LDAPSPACE verwendet. Alle anderen Tabellenbereiche wie Katalogtabellenbereiche und Tabellenbereiche für temporäre Tabellen weisen den Typ SMS (System Managed Space) auf.

- a. Geben Sie im Bereich **USERSPACE1-Tabellenbereichsdetails** die folgenden Details an:

- 1) Wählen Sie in der Liste **Tabellenbereichscontainer** einen Containertyp aus. Wenn sich der Tabellenbereich USERSPACE1 im Dateisystem befinden soll, wählen Sie **Datei** aus. Wenn die Position des Containers für den Tabellenbereich der Datenbank sich in einem Dateisystem befindet, dann wird ein aufbereiteter DMS-Tabellenbereich erstellt. Sie können die Anfangsgröße des Tabellenbereichs und eine erweiterbare Einheitsgröße angeben. Der Tabellenbereich wird bei Bedarf automatisch erweitert. Wenn Sie den Tabellenbereich USERSPACE1 auf einer Roheinheit erstellen wollen, wählen Sie **Roheinheit** aus. Als Roheinheit wird eine Einheit bezeichnet, auf der kein Dateisystem installiert ist, z. B. eine Festplatte, die kein Dateisystem enthält. Wenn die Position des Containers für den Tabellenbereich der Datenbank sich auf einer Roheinheit befindet, dann wird ein nicht aufbereiteter DMS-Tabellenbereich erstellt. In diesem Fall ist die Größe des Containers für den Tabellenbereich der Datenbank festgelegt und kann nicht erweitert werden. Wenn Sie **Roheinheit** auswählen, müssen Sie zusammen mit der Position des Containers die Größe angeben, anstatt die entsprechenden Standardwerte zu übernehmen.

- 2) Geben Sie die folgenden Details an, wenn Sie im Feld **Tabellenbereichscontainer** die Option **Datei** ausgewählt haben:

- a) Geben Sie im Feld **Verzeichnispfad** den Verzeichnispfad an, in dem der Tabellenbereich USERSPACE1 erstellt werden soll. Sie können auf **Durchsuchen** klicken, um das gewünschte Verzeichnis auszuwählen.
  - b) Geben Sie im Feld **Dateiname** den Dateinamen des Tabellenbereich ein, den Sie erstellen wollen, oder übernehmen Sie den Standardnamen USPACE.
  - c) Geben Sie im Feld **Anfangsgröße** die Anfangsgröße für den Tabellenbereich USERSPACE1 in Seiten ein oder übernehmen Sie den Standardwert. Bei einem Tabellenbereichscontainer vom Typ **Datei** wird für den Container des Tabellenbereichs USERSPACE1 der Typ mit automatischer Inkrementierung festgelegt. Sie können im Feld **Anfangsgröße** die Anfangsgröße und im Feld **Erweiterbare Größe** eine erweiterbare Einheitengröße angeben. Standardmäßig werden für die Anfangsgröße 16-KB-Seiten und für die erweiterbare Einheitengröße 8-KB-Seiten verwendet. Die Seitengröße für den Container des Tabellenbereichs USERSPACE1 beträgt 4 KB pro Seite.
- 3) Geben Sie die folgenden Details an, wenn Sie im Feld **Tabellenbereichscontainer** die Option **Roheinheit** ausgewählt haben:
- a) Geben Sie im Feld **Einheitenpfad** die Position der Roheinheit ein. Unter Windows muss der Pfad mit `\\.\` anfangen. Ein Pfad mit dem Einheitennamen könnte beispielsweise wie folgt aussehen: `\\.\device_name`. Unter AIX, Linux und Solaris muss der Einheitenpfad eine gültiger Pfad sein.
  - b) Geben Sie im Feld **Anfangsgröße** die Anfangsgröße für den Tabellenbereich USERSPACE1 ein oder übernehmen Sie den Standardwert. Bei einem Tabellenbereichscontainer vom Typ **Roheinheit** ist die Größe des Containers für den Tabellenbereich USERSPACE1 festgelegt. Die Standardgröße beträgt 16-KB-Seiten. Zur Optimierung der Ergebnisse können Sie die Größe an Ihre Anforderungen anpassen.
- b. Geben Sie im Bereich **LDAPSPACE-Tabellenbereichsdetails** die folgenden Details an:
- 1) Wählen Sie in der Liste **Tabellenbereichscontainer** einen Containertyp aus. Wenn sich der Tabellenbereich LDAPSPACE in einem Dateisystem befinden soll, wählen Sie **Datei** aus. Wenn Sie den Tabellenbereich LDAPSPACE auf einer Roheinheit erstellen wollen, wählen Sie **Roheinheit** aus. Als Roheinheit wird eine Einheit bezeichnet, auf der kein Dateisystem installiert ist, z. B. eine Festplatte, die kein Dateisystem enthält.
  - 2) Geben Sie die folgenden Details an, wenn Sie im Feld **Tabellenbereichscontainer** die Option **Datei** ausgewählt haben:
    - a) Geben Sie im Feld **Verzeichnispfad** den Verzeichnispfad an, in dem der Tabellenbereich LDAPSPACE erstellt werden soll. Sie können auf **Durchsuchen** klicken, um das gewünschte Verzeichnis auszuwählen.
    - b) Geben Sie im Feld **Dateiname** den Dateinamen des Tabellenbereich ein, den Sie erstellen wollen, oder übernehmen Sie den Standardnamen `ldapspace`.
    - c) Geben Sie im Feld **Anfangsgröße** die Anfangsgröße für den Tabellenbereich LDAPSPACE in Seiten ein oder übernehmen Sie den Standardwert. Bei einem Tabellenbereichscontainer vom Typ **Datei** wird für den Container des Tabellenbereichs LDAPSPACE der Typ mit automatischer Inkrementierung festgelegt. Sie können im Feld **Anfangsgröße** die Anfangsgröße und im Feld **Erweiterbare Größe** eine er-

weiterbare Einheitengröße angeben. Standardmäßig werden für die Anfangsgröße 16-KB-Seiten und für die erweiterbare Einheitengröße 8-KB-Seiten verwendet. Die Seitengröße für den Container des Tabellenbereichs LDAPSPACE beträgt 32 KB pro Seite.

- 3) Geben Sie die folgenden Details an, wenn Sie im Feld **Tabellenbereichscontainer** die Option **Roheinheit** ausgewählt haben:
  - a) Geben Sie im Feld **Einheitenpfad** die Position der Roheinheit ein. Unter Windows muss der Pfad mit `\\.\` anfangen. Ein Pfad mit dem Einheitennamen könnte beispielsweise wie folgt aussehen: `\\.\device_name`. Unter AIX, Linux und Solaris muss der Einheitenpfad eine gültiger Pfad sein.
  - b) Geben Sie im Feld **Anfangsgröße** die Anfangsgröße für den Tabellenbereich LDAPSPACE ein oder übernehmen Sie den Standardwert. Bei einem Tabellenbereichscontainer vom Typ **Roheinheit** ist die Größe des Containers für den Tabellenbereich LDAPSPACE festgelegt. Die Standardgröße beträgt 16-KB-Seiten. Zur Optimierung der Ergebnisse können Sie die Größe an Ihre Anforderungen anpassen.
  - c. Wenn Sie in einem der beiden oder in beiden Feldern **Tabellenbereichscontainer** die Option **Datei** ausgewählt haben, geben Sie im Feld **Erweiterbare Größe** die Anzahl der Seiten an, um die die Tabellenbereichscontainer erweitert werden sollen.
6. Klicken Sie auf **Fertig stellen**.
7. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
8. Überprüfen Sie die Protokolle, die bei der Datenbankkonfiguration generiert werden.
9. Klicken Sie auf **Schließen**, um die Seite **Datenbank konfigurieren** zu schließen.
10. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
11. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Nächste Schritte

Nachdem Sie eine Datenbank konfiguriert haben, müssen Sie für eine Instanz die folgenden Konfigurationsschritte ausführen:

- Konfigurieren Sie den Hauptadministrator-DN und das Kennwort. Siehe „Hauptadministrator-DN mit dem **Konfigurationstool** verwalten“ auf Seite 180 und „Hauptadministratorkennwort mit dem **Konfigurationstool** verwalten“ auf Seite 182.
- Konfigurieren Sie die erforderlichen Suffixe. Weitere Informationen finden Sie im Kapitel „Suffixkonfiguration“ auf Seite 213.

## Datenbank mit dem Befehlszeilendienstprogramm für eine Instanz konfigurieren

Konfigurieren Sie mit dem Befehlszeilendienstprogramm **idscfgdb** eine DB2-Datenbank für eine Verzeichnisserverinstanz.

### Vorbereitende Schritte

Führen Sie die folgenden Tasks aus, um eine DB2-Datenbank für eine Verzeichnisserverinstanz zu konfigurieren:



- Setzen Sie die Umgebungsvariable *DB2COMM* nicht, wenn Sie eine Datenbank konfigurieren.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.
- Es muss eine Systembenutzer-ID vorhanden sein, die als Eigner der DB2-Datenbankinstanz fungiert. Weitere Informationen zu den Anforderungen an die Systembenutzer-ID finden Sie unter „Benutzer und Gruppen, die einer Verzeichnisserverinstanz zugeordnet sind“ auf Seite 125.

## Informationen zu diesem Vorgang

Mit dem Befehl **idscfgdb** werden die folgenden Operationen ausgeführt:

- Die Datenbank wird erstellt und mit einer Verzeichnisserverinstanz konfiguriert. Die Einstellungen für die lokale Schleife werden erstellt, sofern diese noch nicht definiert sind.
- Es werden Angaben zur Datenbank zu der Datei *ibmslapd.conf* der Verzeichnisserverinstanz hinzugefügt.

Sie können hierbei angeben, ob die Datenbank in der lokalen Codepage oder im UTF-8-Format (Standardeinstellung) generiert werden soll.

## Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisserverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis *sbin* der Installationsposition von IBM Security Directory Server.
4. Führen Sie den folgenden Befehl aus, um eine DB2-Datenbank mit den folgenden Werten für eine Verzeichnisserverinstanz zu konfigurieren:
  - Instanzname: *ldapdb*
  - Datenbankname: *ldapdb*
  - ID des DB2-Datenbankadministrators: *ldapdb*
  - Kennwort des DB2-Datenbankadministrators: *ldapdb123*
  - Speicherposition der Datenbank: */home/ldapdb*

```
idscfgdb -I ldapdb -a ldapdb -w ldapdb123 -t ldapdb
-l /home/ldapdb
```

Geben Sie unter Windows den Namen des Plattenlaufwerks für die Speicherposition der Datenbank an. Geben Sie unter Solaris eine geeignete Speicherposition der Datenbank an. Weitere Informationen zum Befehl **idscfgdb** finden Sie in der Veröffentlichung *Command Reference*. Mit diesem Befehl wird eine Datenbank mit DMS-Tabellenbereichen mit Standardgrößen konfiguriert.

## Beispiele

### Beispiel 1:

Führen Sie den Befehl **idscfgdb** mit den folgenden Werten aus, um eine Datenbank mit einem DMS-Tabellenbereich in einem Dateisystem und mit einer bestimmten Größe für den Tabellenbereich zu konfigurieren:

- Instanzname: *ldapdb*
- Datenbankname: *ldapdb*
- ID des DB2-Datenbankadministrators: *dbadmin*
- Kennwort des DB2-Datenbankadministrators: *ldapdb123*

- Speicherposition der Datenbank: c:\dblocation
- Speicherposition des Tabellenbereichs USERSPACE1: c:\dblocation\ldapinst\tablespaceloc\USPACE
- Containergröße der USERSPACE1-Tabellenbereiche: 10.000 Seiten
- Erweiterungsgröße: 16 Seiten

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb
-w ldapdb123 -n -l c:\dblocation
-u c:\dblocation\ldapinst\tablespaceloc\USPACE -U 10000 -z 16
```

### Beispiel 2:

Führen Sie den Befehl **idscfgdb** mit den folgenden Werten aus, um die gleiche Datenbank mit SMS-Tabellenbereichen zu konfigurieren.

- Instanzname: ldapdb
- Datenbankname: ldapdb
- ID des DB2-Datenbankadministrators: dbadmin
- Kennwort des DB2-Datenbankadministrators: ldapdb123
- Speicherposition der Datenbank: c:\dblocation

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb
-w ldapdb123 -n -l c:\dblocation
-m SMS
```

## Nächste Schritte

Nachdem Sie eine Datenbank konfiguriert haben, müssen Sie für eine Instanz die folgenden Konfigurationsschritte ausführen:

- Konfigurieren Sie den Hauptadministrator-DN und das Kennwort. Siehe „Hauptadministrator-DN mit dem Befehlszeilendienstprogramm verwalten“ auf Seite 181 und „Hauptadministrator Kennwort mit dem Befehlszeilendienstprogramm verwalten“ auf Seite 183.
- Konfigurieren Sie die erforderlichen Suffixe. Weitere Informationen finden Sie im Kapitel „Suffixkonfiguration“ auf Seite 213.

---

## Verwaltung des DB2-Datenbankadministratorkennworts

Wenn Sie das Systemkennwort für den DB2-Instanzeigner ändern, müssen Sie die Konfigurationsdatei für die Verzeichnisserverinstanz mit dem Kennwort aktualisieren.

Wenn Sie das Systemkennwort für den DB2-Instanzeigner einer Datenbank ändern, die mit einer Instanz konfiguriert wurde, wird das Kennwort in der Instanzkonfigurationsdatei nicht aktualisiert. Wenn das Datenbankadministratorkennwort in der Konfigurationsdatei einer Instanz nicht mit dem Systemkennwort des DB2-Instanzeigners übereinstimmt, der der Datenbank zugeordnet ist, kann die Instanz möglicherweise nicht im normalen Modus gestartet werden. Sie müssen die Instanzkonfigurationsdatei mit dem neuesten Kennwort für den DB2-Instanzeigner aktualisieren.

Zum Aktualisieren des Kennworts für den DB2-Datenbankadministrator können Sie das **Konfigurationstool**, den Befehl **idscfgdb** oder den Befehl **idsldapmodify** verwenden.

Wenn Sie das **Konfigurationstool** oder den Befehl **idscfgdb** zum Ändern des Datenbankadministratorkennworts verwenden, muss der Verzeichnisserver vor dem Ändern des Kennworts gestoppt werden. Um das Datenbankadministratorkenn-

wort mit dem Befehl **idsldapmodify** zu ändern, müssen Sie den Verzeichnisserver im Konfigurationsmodus starten. Führen Sie den Befehl **idsldapmodify** mit dem Hauptadministrator des Verzeichnisservers oder als Mitglied der lokalen Administratorgruppe mit der Rolle `dirdata` aus.

Weitere Informationen zu den Befehlen **idscfgdb** und **idsldapmodify** finden Sie in der *Befehlsreferenz*.

## Administratorkennwort der DB2-Datenbank mit dem Konfigurationstool ändern

Mit dem **Konfigurationstool** können Sie das Administratorkennwort der DB2-Datenbank in der Konfigurationsdatei der Verzeichnisserverinstanz aktualisieren.

### Vorbereitende Schritte

Führen Sie die folgenden Tasks aus, um das Administratorkennwort der DB2-Datenbank in der Konfigurationsdatei der Instanz zu aktualisieren:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem **Konfigurationstool** für eine Instanz konfigurieren“ auf Seite 184.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Informationen zu diesem Vorgang

Das **Konfigurationstool** aktualisiert das Administratorkennwort der DB2-Datenbank in der Konfigurationsdatei der Verzeichnisserverinstanz. Wenn das Änderungsprotokoll für die Instanz konfiguriert ist, aktualisiert das Tool auch das Kennwort für den Eigner der Änderungsprotokolldatenbank in der Konfigurationsdatei.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Datenbanktasks > Datenbank konfigurieren**.
3. Führen Sie auf der Seite **Datenbank konfigurieren** die folgenden Schritte aus:
  - a. Wählen Sie **Kennwort zurücksetzen** aus.
  - b. Geben Sie im Feld **Kennwort** das Kennwort für den Datenbankadministrator ein.
  - c. Geben Sie im Feld **Kennwort bestätigen** das Kennwort für den Datenbankadministrator ein.
  - d. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **Fertig stellen**.
5. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
6. Überprüfen Sie die Protokolle, die bei der Konfiguration des Datenbankkennworts generiert werden.
7. Klicken Sie auf **Schließen**, um die Seite **Datenbank konfigurieren** zu schließen.
8. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
9. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Nächste Schritte

Starten Sie den Verzeichnissever. Siehe „Verzeichnissever und Verwaltungsserver mit dem Konfigurationstool starten oder stoppen“ auf Seite 179.

## Administratorkennwort der DB2-Datenbank mit dem Befehlszeilendienstprogramm ändern

Mit dem Befehlszeilendienstprogramm **idscfgdb** oder **idsldapmodify** können Sie das Administratorkennwort der DB2-Datenbank in der Konfigurationsdatei der Verzeichnisseverinstanz aktualisieren.

### Vorbereitende Schritte

Führen Sie die folgenden Tasks aus, um das Administratorkennwort der DB2-Datenbank in der Konfigurationsdatei der Instanz zu aktualisieren:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisseverinstanz vorhanden sein. Siehe „Datenbank mit dem Befehlszeilendienstprogramm für eine Instanz konfigurieren“ auf Seite 188.

### Informationen zu diesem Vorgang

Mit dem Befehl **idscfgdb** können Sie die Konfigurationsdatei einer Instanz mit dem Administratorkennwort der DB2-Datenbank aktualisieren. Sie müssen vor der Ausführung des Befehls **idscfgdb** den Verzeichnissever stoppen.

Mit dem Befehl **idsldapmodify** können Sie das Kennwort ändern, wenn die Verzeichnisseverinstanz aktiv ist. Führen Sie den Befehl **idsldapmodify** mit dem Hauptadministrator des Verzeichnissevers oder als Mitglied der lokalen Administratorgruppe mit der Rolle `dirdata` aus.

Weitere Informationen zu den Befehlen **idscfgdb** und **idsldapmodify** finden Sie in der Veröffentlichung *Command Reference*.

### Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisseverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Wählen Sie eine der folgenden Methoden aus, um das Administratorkennwort der DB2-Datenbank zu ändern:
  - Führen Sie die folgenden Schritte aus, um das Administratorkennwort der DB2-Datenbank mit dem Befehl **idscfgdb** zu ändern:
    - a. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
    - b. Stoppen Sie den Verzeichnissever. Siehe „Verzeichnissever und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.
    - c. Führen Sie den Befehl **idscfgdb** im folgenden Format aus:

```
idscfgdb -I instance_name -w db2adminPWD
```
    - d. Starten Sie den Verzeichnissever. Siehe „Verzeichnissever und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.
  - Führen Sie die folgenden Schritte aus, um das Administratorkennwort der DB2-Datenbank mit dem Befehl **idsldapmodify** zu ändern:

- a. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis bin der Installationsposition von IBM Security Directory Server.
- b. Führen Sie den Befehl **idsldapmodify** im folgenden Format aus:  

```
idscfgdb -h IP_address -p port -D adminDN -w adminPWD -i file1.ldif
```

Die Datei file1.ldif enthält die folgenden Einträge:

```
dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas,  
cn=Configuration  
changetype: modify  
replace: ibm-slapdDbUserPW  
ibm-slapdDbUserPW: db2adminPWD
```

- c. Starten Sie den Verzeichnisserver erneut. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

---

## Datenbanken von Verzeichnisserverinstanzen dekonfigurieren

Um eine vorhandene Verzeichnisserverinstanz mit einer anderen DB2-Datenbank verwenden zu können, muss die vorhandene DB2-Datenbank von einer Instanz dekonfiguriert werden.

Für eine Verzeichnisserverinstanz können Sie eine Datenbank nur dekonfigurieren, wenn Sie die DB2-Datenbank für die Instanz konfiguriert haben.

Mit dem **Konfigurationstool** oder dem Befehl **idsucfgdb** können Sie zwischen den folgenden Operationen wählen:

- Entfernen der DB2-Datenbankinformationen aus der Konfigurationsdatei einer Verzeichnisserverinstanz. Bei dieser Operation dekonfiguriert das Dienstprogramm die DB2-Datenbank von einer Instanz und löscht die DB2-Datenbank nicht.
- Entfernen der DB2-Datenbankinformationen aus der Konfigurationsdatei einer Verzeichnisserverinstanz und Löschen der DB2-Datenbank. Bei dieser Operation wird die DB2-Datenbank gelöscht und alle Daten gehen verloren.

Nach dem Dekonfigurieren der DB2-Datenbank von einer Verzeichnisserverinstanz besteht für die Instanz kein Zugriff mehr auf die Datenbank.

Für Proxy-Server-Instanzen werden Datenbankdekonfigurationen nicht unterstützt.

Weitere Informationen zum Befehl **idsucfgdb** finden Sie in der *Befehlsreferenz*.

## Datenbank mit dem Konfigurationstool von einer Instanz dekonfigurieren

Dekonfigurieren Sie mithilfe des **Konfigurationstools** die DB2-Datenbank von einer Verzeichnisserverinstanz.

### Vorbereitende Schritte

Zum Dekonfigurieren der DB2-Datenbank von einer Instanz muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem **Konfigurationstool** für eine Instanz konfigurieren“ auf Seite 184.

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Datenbanktasks > Datenbank dekonfigurieren**.
3. Führen Sie auf der Seite **Datenbank dekonfigurieren** die folgenden Schritte aus:
  - a. Wählen Sie im Bereich mit den Optionen eine der folgenden Optionen aus:
    - Klicken Sie auf **Datenbank dekonfigurieren**, um die DB2-Datenbank von einer Instanz zu dekonfigurieren, ohne sie zu löschen:
    - Klicken Sie auf **Datenbank dekonfigurieren**, um die DB2-Datenbank von einer Instanz zu dekonfigurieren und sie zu löschen:
  - b. Wählen Sie **Sicherungskopie der Datenbank entfernen** aus, um die Sicherungskopie der Datenbank von der Instanz zu löschen, wenn die Datenbank für die Onlinesicherung konfiguriert wurde.
  - c. Klicken Sie auf **Dekonfigurieren**, um die Dekonfiguration zu starten.
  - d. Klicken Sie im Bestätigungsfenster auf **Ja**.
4. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
5. Überprüfen Sie die Protokolle, die bei der Dekonfiguration generiert werden.
6. Klicken Sie auf **Abbrechen**, um die Seite **Datenbank dekonfigurieren** zu schließen.
7. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
8. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Datenbank mit dem Befehlszeilendienstprogramm von einer Instanz dekonfigurieren

Dekonfigurieren Sie mit dem Befehlszeilendienstprogramm **idsucfgdb** die DB2-Datenbank von einer Verzeichnisserverinstanz.

### Vorbereitende Schritte

Zum Dekonfigurieren der DB2-Datenbank von einer Instanz muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem Befehlszeilendienstprogramm für eine Instanz konfigurieren“ auf Seite 188.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

### Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisserverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Wählen Sie eine der folgenden Optionen aus, um die DB2-Datenbank von einer Instanz zu dekonfigurieren:

- Führen Sie den Befehl **idsucfgdb** im folgenden Format aus, um die Datenbank von einer Verzeichnisserverinstanz zu dekonfigurieren:  
`idsucfgdb -I instance_name`
- Führen Sie den Befehl **idsucfgdb** im folgenden Format aus, um die Datenbank von einer Verzeichnisserverinstanz zu dekonfigurieren und zu löschen:  
`idsucfgdb -I instance_name -r`

---

## Datenbankoptimierung

Zum Verbessern der Suchleistung der DB2-Datenbank können Sie die Datenbank optimieren und die DB2-Statistikdaten für die Datenbanktabellen aktualisieren.

Zum Optimieren der DB2-Datenbank können Sie das **Konfigurationstool** oder den Befehl **idsrunstats** verwenden. Führen Sie die DB2-Optimierungsoperation regelmäßig oder nach Datenbankaktualisierungen wie Datenimportoperationen aus.

Wenn Sie die Datenbankoptimierung ausführen, sammelt das Tool Statistikdaten zu allen Indexen, die in Tabellen definiert werden, und aktualisiert diese. Diese Statistikdaten werden beim DB2-Abfrageoptimierungsprogramm verwendet, um den optimalen Pfad zum Zugreifen auf die Daten zu bestimmen.

Sie können keine DB2-Optimierung ausführen, wenn die Instanz ein Proxy-Server ist oder die Instanz mit keiner DB2-Datenbank konfiguriert wurde.

Weitere Informationen zum Befehl **idsrunstats** finden Sie in der *Befehlsreferenz*.

## Datenbank mit dem Konfigurationstool optimieren

Mit dem **Konfigurationstool** können Sie die einer Instanz zugeordnete DB2-Datenbank optimieren.

### Vorbereitende Schritte

Zum Optimieren der DB2-Datenbank einer Instanz muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem **Konfigurationstool** für eine Instanz konfigurieren“ auf Seite 184.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Datenbanktasks > Datenbank optimieren**.
3. Führen Sie auf der Seite **Datenbank optimieren** die folgenden Schritte aus:
  - a. Klicken Sie auf **Optimieren**, um die Optimierungsoperation zu starten.
  - b. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
  - c. Überprüfen Sie die Protokolle, die bei der Datenbankoptimierung generiert werden.
  - d. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
4. Klicken Sie auf **Schließen**, um die Seite **Datenbank optimieren** zu schließen.

5. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
6. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Datenbank mit dem Befehlszeilendienstprogramm optimieren

Mit dem Befehlszeilendienstprogramm **idsrunstats** können Sie die einer Instanz zugeordnete DB2-Datenbank optimieren.

### Vorbereitende Schritte

Zum Optimieren der DB2-Datenbank einer Instanz muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem Befehlszeilendienstprogramm für eine Instanz konfigurieren“ auf Seite 188.

### Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisserverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Führen Sie den Befehl **idsrunstats** im folgenden Format aus, um die DB2-Datenbank zu optimieren:

```
idsrunstats -I instance_name
```

Weitere Informationen zum Befehl **idsrunstats** finden Sie in der Veröffentlichung *Command Reference*.

---

## Datenbankpflege

Um Such- oder Aktualisierungsvorgänge bei Instanzen zu verbessern, führen Sie eine DB2-Indexreorganisation oder eine DB2-Zeilenkomprimierung durch.

Zum Ausführen einer DB2-Indexreorganisation oder DB2-Zeilenkomprimierung können Sie das **Konfigurationstool** oder den Befehl **idsdbmaint** verwenden.

Wenn DB2-Tabellen einer Datenbank mit mehreren Einfügungen oder Löschungen aktualisiert werden, nehmen Such- und Aktualisierungsoperationen bei der Datenbank mehr Zeit in Anspruch. Wenn Sie den DB2-Index reorganisieren, wird die Leistung bei Such- und Aktualisierungsoperationen verbessert.

Wenn Sie eine DB2-Zeilenkomprimierung ausführen, sucht das Tool nach sich wiederholenden Mustern und ersetzt diese durch kürzere Symbolzeichenfolgen. Das Tool führt nur Analysen und Zeilenkomprimierungen durch, wenn die Komprimierung eine Verbesserung von mehr als 30 Prozent bringt.

Sie können den Befehl **idsdbmaint** auch verwenden, um einen SMS-Tabellenbereich in einen DMS-Tabellenbereich oder umgekehrt zu konvertieren. Tabellenbereichskonvertierung wird vom **Konfigurationstool** nicht unterstützt. Weitere Informationen zum Befehl **idsdbmaint** finden Sie in der *Befehlsreferenz*.



## Datenbankpflege mit dem Konfigurationstool ausführen

Mit dem **Konfigurationstool** können Sie die einer Instanz zugeordnete DB2-Datenbank pflegen.

### Vorbereitende Schritte

Zum Pflegen der DB2-Datenbank einer Instanz muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem **Konfigurationstool** für eine Instanz konfigurieren“ auf Seite 184.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Datenbanktasks > Pflege**.
3. Führen Sie auf der Seite **Pflege** die folgenden Schritte aus:
  - a. Wählen Sie die DB2-Datenbankpflegeoperation aus, die Sie ausführen wollen:
    - Klicken Sie zur Ausführung der DB2-Indexreorganisation auf **Indexreorganisation ausführen**.
    - Klicken Sie zur Ausführung der DB2-Zeilenkomprimierung auf **Tabellen überprüfen und Zeilenkomprimierung ausführen**.
  - b. Klicken Sie auf **OK**.
  - c. Klicken Sie im Fenster zur Ausführung der Task auf **OK**.
  - d. Überprüfen Sie die Protokolle, die bei der Datenbankpflege generiert werden.
  - e. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
4. Klicken Sie auf **Schließen**, um die Seite **Pflege** zu schließen.
5. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
6. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

### Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## Datenbankpflege mit dem Befehlszeilendienstprogramm ausführen

Mit dem Befehlszeilendienstprogramm **idsdbmaint** können Sie in der einer Instanz zugeordneten DB2-Datenbank eine Pflegeoperation ausführen.

### Vorbereitende Schritte

Zum Ausführen einer Pflegeoperation für die DB2-Datenbank muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem Befehlszeilendienstprogramm für eine Instanz konfigurieren“ auf Seite 188.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

### Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisserverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Führen Sie den Befehl **idsdbmaint** im folgenden Format aus, um eine DB2-Indexreorganisation auszuführen:

```
idsdbmaint -I instance_name -i
```

Weitere Informationen zum Befehl **idsdbmaint** finden Sie in der Veröffentlichung *Command Reference*.

5. Führen Sie den Befehl **idsdbmaint** im folgenden Format aus, um eine DB2-Zeilenkomprimierung auszuführen:

```
idsdbmaint -I instance_name -r
```

### Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

---

## Verzeichnisserverbackup

Um eine Verzeichnisserverinstanz nach einem Ausfall wiederherstellen zu können, müssen Sie regelmäßig ein Backup der Verzeichnisserverinstanz durchführen.

Zum Sichern einer Instanz können Sie das **Konfigurationstool** oder den Befehl **idsdbback** verwenden. Der Befehl **idsdbback** kann nicht zum Sichern von Proxy-Server-Instanzen verwendet werden, da einem Proxy-Server keine Datenbank zugeordnet ist.

Mit dem Befehl **idscfgdb** können Sie eine Datenbank konfigurieren, die einer Instanz zur Onlinesicherung zugeordnet ist. Sie können eine Onlinesicherung jedoch nicht mit dem Befehl **idscfgdb** und dem Parameter **-c** dekonfigurieren. Wenn Sie eine Onlinesicherung für eine Instanz mit **Instance Administration Tool** oder mithilfe des **Konfigurationstools** konfigurieren, können Sie sie mit dem **Konfigurationstool** oder dem Befehl **idscfgdb** dekonfigurieren. Die zuverlässigsten Ergebnisse erhalten Sie, wenn Sie **Instance Administration Tool** oder das **Konfigurationstool** zum Konfigurieren einer Onlinesicherung für eine Instanz mit einer Datenbank verwenden.

Sie können auch den Befehl **idsdb2ldif** zum Exportieren der Einträge in einem Verzeichnisserver in eine LDIF-Datei verwenden. Sie können den Befehl **migbkup** zum Sichern von Schema- und Konfigurationsdateien für eine Verzeichnisserverinstanz und eine Proxy-Server-Instanz verwenden. Weitere Informationen zu den Befehlen **idsdbback**, **idsdb2ldif** und **migbkup** finden Sie in der *Befehlsreferenz*. Weitere Informationen zum richtigen Befehl für Ihre Umgebung finden Sie im Abschnitt *Performance Tuning and Capacity Planning* in der IBM Security Directory Server-Dokumentation.

Mit dem **Konfigurationstool** können Sie die folgenden Aktionen durchführen:

- Die Konfigurationseinstellungen für eine Verzeichnisserverinstanz oder eine Proxy-Server-Instanz sichern
- Die Verzeichnisserverinstanz und die dazugehörige Datenbank sichern
- Die Verzeichnisserverinstanz und die Änderungsprotokolldatenbank (sofern für eine Instanz konfiguriert) sichern

Weitere Informationen zu den Operationen für die Sicherung und Wiederherstellung finden Sie im Abschnitt *Verwaltung* in der IBM Security Directory Server-Dokumentation.

## Datenbank einer Verzeichnisserverinstanz mit dem Konfigurationstool sichern

Mit dem **Konfigurationstool** können Sie eine Verzeichnisserverinstanz und deren Datenbank sichern, damit nach einem Fehler die Wiederherstellung möglich ist.

### Vorbereitende Schritte

Zum Sichern einer Verzeichnisserverinstanz mit deren Datenbank muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem **Konfigurationstool** für eine Instanz konfigurieren“ auf Seite 184.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Sichern/Wiederherstellen > Datenbank sichern**.
3. Führen Sie auf der Seite **Datenbank sichern** die folgenden Schritte aus:
  - a. Geben Sie im Feld **Sicherungsverzeichnis** den Verzeichnispfad ein, in dem alle Verzeichnisdaten und die Konfigurationsdateien gespeichert werden sollen. Sie können auch auf **Durchsuchen** klicken, um den Verzeichnispfad anzugeben.
  - b. Wählen Sie bei einer Onlinesicherung eine der folgenden Optionen aus:
    - Um den Verzeichnisserver und dessen Datenbank für die Onlinesicherung zu konfigurieren, sofern dies nicht bereits erfolgt ist, wählen Sie **Datenbankkonfiguration zur Unterstützung der Onlinesicherung aktualisieren** aus.
    - Um eine Onlinesicherung für die Verzeichnisserverinstanz auszuführen, wenn Onlinesicherung auf dem Server konfiguriert wurde, wählen Sie **Onlinesicherung ausführen** aus.
  - c. Um die Änderungsprotokolldatenbank der Instanz zu sichern, wenn das Änderungsprotokoll konfiguriert wurde, wählen Sie **Änderungsprotokolldaten in Sicherung einschließen** aus.
  - d. Um die Datenbankdateien von der Sicherung auszuschließen, wählen Sie **Datenbankdateien nicht sichern** aus. Wenn Sie **Datenbankdateien nicht sichern** auswählen, werden die Dateien der Datenbank und der Änderungsprotokolldatenbank für die Verzeichnisserverinstanz nicht gesichert. Das Tool sichert die Dateien für die Verzeichnisserverinstanz, z. B. die Schlüssel-Stubdateien, Schema- und Konfigurationsdateien.

- e. Um zu entscheiden, ob die Sicherung bei Vorhandensein des Sicherungsverzeichnisses fortgesetzt werden soll, wählen Sie eine der folgenden Optionen aus:
  - Um das Sicherungsverzeichnis zu erstellen, wenn es nicht vorhanden ist, klicken Sie auf **Gegebenenfalls Sicherungsverzeichnis erstellen**.
  - Wenn das Sicherungsverzeichnis nicht vorhanden ist und Sie das Verzeichnis nicht erstellen wollen, klicken Sie auf **Anhalten, wenn das Sicherungsverzeichnis nicht gefunden wird**. Wenn das Sicherungsverzeichnis nicht vorhanden ist und Sie diese Option auswählen, wird die Datenbank nicht gesichert.

**Anmerkung:** Die Ausführung des **Konfigurationstools** darf nicht unterbrochen werden, während die Sicherungsoperation ausgeführt wird.

- f. Klicken Sie auf **Sichern**, um die Sicherungsoperation zu starten.
  - g. Wenn der Verzeichnisserver für die Sicherungsoperation gestoppt werden muss, klicken Sie auf **Ja**.
  - h. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
  - i. Überprüfen Sie die Protokolle, die bei der Sicherungsoperation generiert werden.
  - j. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
  - k. Klicken Sie auf **Schließen**, um die Seite **Datenbank sichern** zu schließen.
4. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
  5. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Proxy-Server-Instanz mit dem Konfigurationstool sichern

Mit dem **Konfigurationstool** können Sie eine Proxy-Server-Instanz sichern, damit nach einem Fehler die Wiederherstellung möglich ist.

### Vorbereitende Schritte

Damit eine Proxy-Server-Instanz gesichert werden kann, muss eine Proxy-Server-Instanz vorhanden sein. Siehe „Proxy-Server-Instanz mit angepassten Einstellungen erstellen“ auf Seite 150.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Sichern/Wiederherstellen > Instanz sichern**.
3. Führen Sie auf der Seite **Instanz sichern** die folgenden Schritte aus:
  - a. Geben Sie im Feld **Sicherungsverzeichnis** den Verzeichnispfad ein, in dem die Schema- und Konfigurationsdateien gespeichert werden sollen. Sie können auch auf **Durchsuchen** klicken, um den Verzeichnispfad anzugeben.
  - b. Bei einer Proxy-Server-Instanz ist das Markierungsfeld **Datenbankdateien nicht sichern** ausgewählt.
  - c. Um zu entscheiden, ob die Sicherung bei Vorhandensein des Sicherungsverzeichnisses fortgesetzt werden soll, wählen Sie eine der folgenden Optionen aus:

- Um das Sicherungsverzeichnis zu erstellen, wenn es nicht vorhanden ist, klicken Sie auf **Gegebenenfalls Sicherungsverzeichnis erstellen**.
- Wenn das Sicherungsverzeichnis nicht vorhanden ist und Sie das Verzeichnis nicht erstellen wollen, klicken Sie auf **Anhalten, wenn das Sicherungsverzeichnis nicht gefunden wird**. Wenn das Sicherungsverzeichnis nicht vorhanden ist und Sie diese Option auswählen, wird die Proxy-Server-Instanz nicht gesichert.

**Anmerkung:** Die Ausführung des **Konfigurationstools** darf nicht unterbrochen werden, während die Sicherungsoperation ausgeführt wird.

- d. Klicken Sie auf **Sichern**, um die Sicherungsoperation zu starten.
  - e. Wenn die Instanz für die Operation gestoppt werden muss, klicken Sie auf **Ja**.
  - f. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
  - g. Überprüfen Sie die Protokolle, die bei der Sicherungsoperation generiert werden.
  - h. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
  - i. Klicken Sie auf **Schließen**, um die Seite **Instanz sichern** zu schließen.
4. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
  5. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

---

## Verzeichnisse wiederherstellen

Wenn bei Ihrer Verzeichnisseverinstanz ein Fehler auftritt, können Sie das neueste Sicherungsimago der Instanz wiederherstellen.

Zum Wiederherstellen von Verzeichnisdaten und optional zum Konfigurieren von zuvor gesicherten Konfigurationseinstellungen können Sie das **Konfigurationstool** oder den Befehl **idsdbestore** verwenden. Vor dem Wiederherstellen der Datenbank und/oder der Konfigurationseinstellungen muss der Verzeichnissever gestoppt werden.

Bei Proxy-Servern können Sie die Konfigurationseinstellungen wiederherstellen. Führen Sie bei Proxy-Servern den Befehl **idsdbestore** mit dem Parameter **-x** aus.

Bei Instanzen mit einer DB2-Datenbank können Sie die Datenbank in eine Datenbank und Datenbankinstanz mit demselben Namen wiederherstellen, der für die Datenbanksicherung verwendet wurde. Bei Verzeichnisseverinstanzen mit einer DB2-Datenbank ist eine Wiederherstellung nur möglich, wenn eine Datenbank für die Verzeichnisseverinstanz konfiguriert wurde. Mithilfe des Befehls **idsdbestore** wird die Sicherungsdatenbank in der derzeit konfigurierten Datenbank wiederhergestellt. Der Befehl schlägt fehl, wenn die gesicherte Datenbankinstanz und die Datenbank nicht mit der konfigurierten Datenbankinstanz und der entsprechenden Datenbank übereinstimmen. Zum Wiederherstellen der Datenbank müssen die Position der gesicherten Datenbank und der Datenbank, die durch den Befehl wiederhergestellt wird, dieselben sein.

Weitere Informationen zum Befehl **idsdbestore** finden Sie in der *Befehlsreferenz*.

## Datenbank eines Verzeichnisseservers mit dem Konfigurationstool wiederherstellen

Mit dem **Konfigurationstool** können Sie eine Verzeichnisseserverinstanz und deren Datenbank aus einem Sicherungsimago wiederherstellen.

### Vorbereitende Schritte

Zum Wiederherstellen einer Verzeichnisseserverinstanz und deren Datenbank muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisseserverinstanz vorhanden sein. Siehe „Datenbank mit dem **Konfigurationstool** für eine Instanz konfigurieren“ auf Seite 184.
- Es muss ein Sicherungsimago der Verzeichnisseserverinstanz vorhanden sein. Siehe „Datenbank einer Verzeichnisseserverinstanz mit dem **Konfigurationstool** sichern“ auf Seite 199.
- Stoppen Sie den Verzeichnisseserver. Siehe „Verzeichnisseserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Sichern/Wiederherstellen > Datenbank wiederherstellen**.
3. Führen Sie auf der Seite **Datenbank wiederherstellen** die folgenden Schritte aus:
  - a. Geben Sie im Feld **Wiederherstellungsverzeichnis** den Pfad zu dem Verzeichnis ein, in dem sich das Sicherungsimago der Instanz befindet. Sie können auch auf **Durchsuchen** klicken, um den Verzeichnispfad anzugeben.
  - b. Wenn nur die Verzeichnisdaten, nicht aber die Konfigurationseinstellungen aus dem Sicherungsimago wiederhergestellt werden sollen, wählen Sie **Aktuelle Konfigurationseinstellungen beibehalten** aus. Wenn Sie sowohl die Datenbank als auch die Konfigurationseinstellungen wiederherstellen wollen, müssen Sie die Option **Aktuelle Konfigurationseinstellungen beibehalten** abwählen.
  - c. Wenn für die Instanz das Änderungsprotokoll konfiguriert wurde und Sie die Änderungsprotokolldaten wiederherstellen wollen, wählen Sie **Änderungsprotokolldaten in Wiederherstellung einschließen** aus.
  - d. Klicken Sie auf **Wiederherstellen**, um die Wiederherstellungsoperation zu starten.
  - e. Wenn der Verzeichnisseserver für die Operation gestoppt werden muss, klicken Sie auf **Ja**.
  - f. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
  - g. Überprüfen Sie die Protokolle, die bei der Wiederherstellungsoperation generiert werden.
  - h. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
  - i. Klicken Sie auf **Schließen**, um die Seite **Datenbank wiederherstellen** zu schließen.
4. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
5. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Proxy-Server-Instanz mit dem Konfigurationstool wiederherstellen

Mit dem **Konfigurationstool** können Sie eine Proxy-Server-Instanz wiederherstellen, damit nach einem Fehler die Wiederherstellung möglich ist.

### Vorbereitende Schritte

Zum Wiederherstellen einer Proxy-Server-Instanz muss die Proxy-Server-Instanz die folgenden Anforderungen erfüllen:

- Es muss eine Proxy-Server-Instanz vorhanden sein. Siehe „Proxy-Server-Instanz mit angepassten Einstellungen erstellen“ auf Seite 150.
- Es muss ein Sicherungsimage der Proxy-Server-Instanz vorhanden sein. Siehe „Proxy-Server-Instanz mit dem **Konfigurationstool** sichern“ auf Seite 200.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Sichern/Wiederherstellen > Instanz wiederherstellen**.
3. Führen Sie auf der Seite **Instanz wiederherstellen** die folgenden Schritte aus:
  - a. Geben Sie im Feld **Wiederherstellungsverzeichnis** den Pfad zu dem Verzeichnis ein, in dem sich das Sicherungsimage der Instanz befindet. Sie können auch auf **Durchsuchen** klicken, um den Verzeichnispfad anzugeben.
  - b. Wenn Sie die Konfigurationseinstellungen aus dem Sicherungsimage nicht wiederherstellen wollen, wählen Sie **Aktuelle Konfigurationseinstellungen beibehalten** aus.
  - c. Klicken Sie auf **Wiederherstellen**, um die Wiederherstellungsoperation zu starten.
  - d. Wenn der Verzeichnisserver für die Operation gestoppt werden muss, klicken Sie auf **Ja**.
  - e. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
  - f. Überprüfen Sie die Protokolle, die bei der Wiederherstellungsoperation generiert werden.
  - g. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
  - h. Klicken Sie auf **Schließen**, um die Seite **Instanz wiederherstellen** zu schließen.
4. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
5. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

---

## Leistung eines Verzeichnisseservers optimieren

Sie können Verzeichnisserverinstanzen optimieren, um die Leistung beim Suchen und Aktualisieren zu verbessern.

Zum Optimieren einer Verzeichnisserverinstanz können Sie das **Konfigurationstool** oder den Befehl **idsperf tune** ausführen. Das Tool generiert Einstellungswerte für die Leistungsoptimierung für die Verzeichnisservercaches und DB2-Pufferpools.

Das Tool generiert die Optimierungseinstellungen, die auf den Werten basieren, die Sie zur Verzeichnisserverinstanz angegeben haben. Das Tool kann die Optimierungseinstellungen für eine Instanz auch aktualisieren. Das Tool führt ein Backup der Datei `ibmslapd.conf` durch und speichert es im Ausgangsverzeichnis für eine Verzeichnisserverinstanz in der Datei `logs/ibmslapd.conf.save`.

Das Tool speichert die Informationen, die Sie im Ausgangsverzeichnis für eine Verzeichnisserverinstanz in der Datei `logs/perftune_input.conf` angegeben haben.

Beim **Konfigurationstool** oder dem Befehl **idsperftune** werden die Werte verwendet, die Sie zum Berechnen der folgenden Optimierungseinstellungen für die Instanz angegeben haben:

- Größe des Eintragscaches
- Filtercachegröße
- Cachegröße für Gruppenmitglieder
- Umgebungsbeschränkung für den Cache für Gruppenmitglieder
- Pufferpoolgröße DB2 LDAPDB
- Pufferpoolgröße DB2 IBMDEFAULTDB

Wenn Ihre Verzeichnisserverinstanz ausgeführt wird, überwacht das Tool die Leistung der Instanz und stellt die Informationen aus der Datenbankstatusprüfung bereit. Die Informationen aus der Datenbankstatusprüfung umfassen die folgenden DB2-Parameter:

- DB2 NUM\_IOSERVERS
- DB2 NUM\_IOCLEANERS
- CATALOGCACHE\_SZ
- PCKCACHESZ
- LOGFILSIZ
- LOCKLIST

Wenn Sie die erweiterte Optimierung für eine Instanz ausführen, erfasst und analysiert das Tool Daten über die Verzeichnisserverinstanz. Die Instanz muss für eine Weile ausgeführt werden, damit DB2-Optimierungsdaten während der Analyse der Datenbankstatusprüfung erfasst werden können. Das Tool generiert die Optimierungswerte für die folgenden DB2-Parameter und speichert Sie in der Datei `logs/perftune_stat.log` für die Instanz.

- SORTHEAP
- MAXFILOP
- DBHEAP
- CHNGPGS\_THRESH
- NUM\_IOSERVERS
- NUM\_IOCLEANERS

Der Allgemeinzustand für die DB2-Parameter kann durch einen der folgenden Werte angezeigt werden:

- OK
- Zunahme
- Abnahme
- Nicht gesammelt



Der Allgemeinzustand der DB2-Parameter, die nicht analysiert wurden, erhalten den Wert Nicht gesammelt. Sie können die angegebenen Werte verwenden, um zu entscheiden, welche DB2-Parameter Sie für eine bessere Leistung optimieren können.

Für eine bessere Leistung müssen Sie das Tool für eine Instanz ausführen, sobald die Anfangsverzeichnisdaten geladen werden. Führen Sie das Tool nach der Erstopptimierung regelmäßig aus, insbesondere nach dem Hinzufügen vieler Einträge oder nach dem Ändern des Inhalts von Einträgen. Weitere Informationen zum Optimieren einer Verzeichnisserverinstanz finden Sie im Abschnitt *Performance Tuning and Capacity Planning* in der IBM Security Directory Server-Dokumentation.

Das **Konfigurationstool** und der Befehl **idsperf tune** können nicht zum Optimieren einer Proxy-Server-Instanz oder einer Instanz, die nicht mit einer Datenbank konfiguriert wurde, verwendet werden.

## Verzeichnisserver mit dem Konfigurationstool für die Leistungsoptimierung konfigurieren

Mit dem **Konfigurationstool** können Sie einen Verzeichnisserver optimieren, so dass die Leistung der Such- und Aktualisierungsoperationen verbessert wird.

### Vorbereitende Schritte

Zum Optimieren einer Verzeichnisserverinstanz muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem **Konfigurationstool** für eine Instanz konfigurieren“ auf Seite 184.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Datenbanktasks > Leistungsoptimierung**.
3. Führen Sie auf der Seite **Leistungsoptimierung** die folgenden Schritte aus:
  - a. Geben Sie im Feld **Prozentsatz des verfügbaren Systemspeichers, der dieser Verzeichnisinstanz zugeordnet wird** den Prozentsatz des Systemspeichers an, der der Instanz zugeordnet werden soll. Der verfügbare Systempeicher wird zwischen mehreren Verzeichnisserverinstanzen oder zwischen Instanzen und anderen Servern aufgeteilt, deren Ausführung Sie auf dem System planen. Das Tool verwendet den angegebenen Wert zur Berechnung der Größe für den Eintrags- und den Filtercache.
  - b. Geben Sie im Feld **Geplante Gruppenanzahl** die Anzahl der Gruppen ein, die Sie voraussichtlich zu der Instanz hinzufügen. Das Tool verwendet den angegebenen Wert zur Berechnung der Größe für die Verzeichnisservercaches.
  - c. Geben Sie im Feld **Maximale Anzahl der Mitglieder einer Gruppe, auf die häufig verwiesen wird** die durchschnittliche Anzahl der Mitglieder für Gruppen ein, auf die häufig verwiesen wird.
  - d. Wählen Sie im Bereich **Anzahl der Einträge und durchschnittliche Eintragsgröße** eine der folgenden Optionen aus:
    - Wenn Sie die Anzahl der Einträge im Verzeichnis und die durchschnittliche Eintragsgröße schätzen wollen, führen Sie folgende Schritte aus:

- 1) Geben Sie im Feld **Geplante Eintragsanzahl** die Gesamtzahl der Einträge ein, die für die Instanz eingeplant sind. Das Tool versucht, die Anzahl der Einträge in der Verzeichnisserverinstanz festzustellen. Falls dies nicht möglich ist, wird der Standardwert von 10.000 Einträgen verwendet. Das Tool verwendet diesen Wert zur Berechnung der Größe für die Verzeichnisservercaches.
  - 2) Geben Sie im Feld **Durchschnittliche Größe eines Eintrags** die Durchschnittsgröße (in Byte) eines Eintrags in der Instanz an. Das Tool versucht, die Größe eines Eintrags in der Verzeichnisserverinstanz zu berechnen. Wenn dies nicht möglich ist, wird der Standardwert von 2650 Byte verwendet. Das Tool verwendet diesen Wert zur Berechnung der Größe für die Verzeichnisservercaches.
- Wenn das Tool die Gesamtzahl der Einträge und die durchschnittliche Eintragsgröße feststellen soll, klicken Sie auf **Aus Serverinstanzdatenbank laden**. Daraufhin füllt das Tool die Felder **Geplante Eintragsanzahl** und **Durchschnittliche Größe eines Eintrags**.
- e. Wählen Sie im Bereich **Aktualisierungsfrequenz** eine der folgenden Optionen aus:
- Wenn Sie häufige Aktualisierungen der Instanz erwarten, klicken Sie auf **Häufige Aktualisierungen**. (Als häufige Aktualisierung wird eine durchschnittliche Aktualisierungsrate von mehr als einer Aktualisierung für jeweils 500 Suchoperationen betrachtet.)
  - Wenn Aktualisierungen seltener zu erwarten sind oder in Gruppen zusammengefasst und zu bestimmten Zeiten innerhalb des Tages ausgeführt werden, klicken Sie auf **Aktualisierungen im Stapelbetrieb**.

Das Tool verwendet diese Informationen zum Definieren der Größe für den Filtercache. Der Filtercache ist nur dann von Nutzen, wenn an der Instanz selten Aktualisierungen ausgeführt und die gleichen Suchoperationen mehrmals ausgeführt werden. Wenn häufige Aktualisierungen erwartet werden, wird der Filtercache auf den Wert 0 gesetzt. Wenn Aktualisierungen selten oder im Stapelbetrieb erwartet werden, dann wird für den Filtercache der Wert von 1024 Filtercacheeinträgen definiert.

- f. Wenn das Tool Leistungsanalysewerte bereitstellen soll, müssen Sie **Erfassung zusätzlicher Systemdaten für erweiterte Optimierung aktivieren** auswählen.
- Wenn Sie das Markierungsfeld auswählen, werden die beiden DB2-Monitorschalter BUFFERPOOL und SORTHEAP aktiviert. Die Leistung der Verzeichnisserverinstanz verringert sich möglicherweise, wenn das Tool die DB2-Monitorschalter aktiviert, um die Daten zu erfassen.
  - Sie müssen das Markierungsfeld zu einem Zeitpunkt auswählen, zu dem in Ihrer Umgebung ein normales Aufkommen an Verzeichnisaktivität herrscht, um exakte Daten für die bestmögliche Optimierung der Verzeichnisserverinstanz zu erhalten. Wenn Sie die Statusprüfung der Datenbank zu einem Zeitpunkt mit geringer Systemaktivität auf dem Server ausführen, enthält das Ergebnis in der Regel keine optimalen Leistungswerte.
- g. Klicken Sie auf **Weiter**. Die Seite **Leistungsoptimierung: Überprüfung** wird geöffnet.
4. Führen Sie auf der Seite **Leistungsoptimierung: Überprüfung** die folgenden Schritte aus:
- a. Überprüfen Sie in der Liste mit den Daten zur Statusprüfung der Datenbank die vom Tool generierten Einstellungen für die Leistungsoptimierung. Wenn keine Datenbankaktivitäten für die Instanz vorliegen, ist die Liste

mit den Daten zur Statusprüfung der Datenbank möglicherweise leer. Die Liste wird gefüllt, wenn das Tool Angaben zu mindestens einem für DB2 relevanten Parameter erfasst. Die Optimierungseinstellungen werden außerdem in der Datei `perftune_stat.log` protokolliert.

- b. Klicken Sie auf **Datenbankparameter optimieren**, um die Werte der Datenbankparameter zu ändern. Das Fenster **Datenbankparameter** wird geöffnet.
- c. Geben Sie im Fenster **Datenbankparameter** Werte für die folgenden Datenbankparameter an:
  - 1) Geben Sie im Feld **Heapspeicher für Datenbank** die maximale Speicherkapazität (in Seiten) ein, die für den Heapspeicher für die Datenbank festgelegt werden soll. Der Heapspeicher für die Datenbank enthält Steuerblockdaten für Tabellen, Indizes, Tabellenbereiche und Pufferpools. Außerdem enthält er Speicherplatz für den Protokollpuffer und temporären Speicher, der von den verschiedenen Dienstprogrammen benutzt wird.
  - 2) Geben Sie im Feld **Paketcachegröße** die Größe (in Seiten) ein, die zum Caching bestimmter Abschnitte für statisches und dynamisches SQL sowie für XQuery-Anweisungen für eine Datenbank verwendet werden soll.
  - 3) Geben Sie im Feld **Protokollpuffergröße** die Größe (in Seiten) für den Puffer ein, der für Protokollsätze zugeordnet werden muss. Sie müssen die Menge des Heapspeichers für die Datenbank angeben, die als Puffer für Protokollsätze verwendet werden soll.
  - 4) Geben Sie im Feld **Maximal zulässige Anzahl der pro Anwendung geöffneten Datenbankdateien** die maximale Anzahl der Dateikennungen ein, die für einen Datenbankagenten geöffnet sein können.
  - 5) Geben Sie im Feld **Grenzwert für geänderte Seiten** den Prozentsatz der geänderten Seiten ein.
  - 6) Geben Sie im Feld **Sortierspeichergöße** die maximale Größe für den Sortierspeicher in Seiten ein. Der Sortierspeicher kann für private Speicherseiten für private Sortiervorgänge oder für gemeinsam genutzte Speicherseiten für gemeinsame Sortiervorgänge verwendet werden.
  - 7) Geben Sie im Feld **Protokolldateigröße** die Größe der Protokolldateien (in KB) ein. Dieser Parameter definiert die Größe aller primären und sekundären Protokolldateien.
  - 8) Geben Sie im Feld **Datenbankprotokollpfad** die Position ein, an der die Protokolldateien gespeichert werden sollen. Sie können auf **Durchsuchen** klicken, um die gewünschte Position anzugeben.
  - 9) Klicken Sie auf **OK**, um die festgelegten Werte zu speichern und die Datenbankparameter mit den Werten zu aktualisieren. Wenn Sie keine Werte für Parameter angeben, werden die Standardwerte festgelegt.
5. Wählen Sie eine der folgenden Optionen aus, um zu entscheiden, ob die Verzeichnis- und Datenbankeinstellungen mit den Optimierungswerten aktualisiert werden sollen:
  - Klicken Sie auf **Ja, die empfohlenen Werte zum Aktualisieren der Verzeichnis- und Datenbankkonfigurationseinstellungen verwenden**, um die Optimierungseinstellungen für Ihre Verzeichnisserverinstanz zu aktualisieren
  - Klicken Sie auf **Nein, aktuelle Einstellungen beibehalten**, wenn die Optimierungseinstellungen nicht verwendet werden sollen. Die Konfigurationseinstellungen werden nicht aktualisiert.

6. Klicken Sie auf **Fertig stellen**, um die Änderungen anzuwenden.
7. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
8. Überprüfen Sie die Protokolle, die beim Aktualisieren der Optimierungseinstellungen generiert werden.
9. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
10. Klicken Sie auf **Schließen**, um die Seite **Leistungsoptimierung** zu schließen.
11. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
12. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Verzeichnissever mit dem Befehlszeilendienstprogramm für die Leistungsoptimierung konfigurieren

Mit dem Befehlszeilendienstprogramm **idsperftune** können Sie einen Verzeichnissever optimieren, sodass die Leistung der Such- und Aktualisierungsoperationen verbessert wird.

### Vorbereitende Schritte

Zum Optimieren einer Verzeichnisseverinstanz muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisseverinstanz vorhanden sein. Siehe „Datenbank mit dem Befehlszeilendienstprogramm für eine Instanz konfigurieren“ auf Seite 188.

### Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisseverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Führen Sie den Befehl **idsperftune** aus, um einen Verzeichnissever und dessen Datenbank zu optimieren.

- Führen Sie den Befehl **idsperftune** aus, um die grundlegenden Optimierungsoperationen für den Verzeichnissever auszuführen:

```
idsperftune -I instance_name -i property_file -B -u
```

Wenn Sie den Parameter **-u** angeben, werden die Einstellungen des LDAP-Cache und des DB2-Pufferpools auf dem Server und in der Datenbank aktualisiert. Wenn Sie den Parameter **-u** nicht angeben, werden die Optimierungseinstellungen nur in der Datei `perftune_stat.log` protokolliert.

- Führen Sie den Befehl **idsperftune** im folgenden Format aus, um die Anzahl der Einträge und die durchschnittliche Eintragsgröße aus einer Instanz und deren Datenbank abzurufen:

```
idsperftune -I instance_name -s
```

- Führen Sie den Befehl **idsperftune** aus, um die erweiterten Optimierungsoperationen für den Verzeichnissever auszuführen:

```
idsperftune -I instance_name -i property_file -A -m
```

Wenn Sie den Parameter **-m** angeben, werden die Monitorschalter für `BUFFERPOOL` und `SORT` aktiviert. Sie müssen den Befehl zu einem Zeitpunkt

ausführen, zu dem in Ihrer Umgebung ein normales Aufkommen an Verzeichnisaktivität herrscht, um exakte Daten für die bestmögliche Optimierung Ihrer Instanz zu erhalten.

Weitere Informationen zum Befehl **idsperftune** finden Sie in der Veröffentlichung *Command Reference*.

---

## Änderungsprotokollverwaltung für Verzeichnisserverinstanzen

Sie können die Änderungsprotokolldatenbank für das Erfassen von Änderungen am Schema oder an Verzeichniseinträgen einer Instanz konfigurieren.

Im Änderungsprotokoll werden alle Aktualisierungsoperationen wie `add`, `delete`, `modify` und `modrtn`, die an Verzeichnisserverinstanzen vorgenommen werden, erfasst. Sie können Clientdienstprogramme zum Abrufen der Änderungsprotokolldaten verwenden, die aufgezeichnet werden, wenn Änderungen an einer Verzeichnisserverdatenbank vorgenommen werden.

Sie können das **Konfigurationstool** oder die Befehlszeilendienstprogramme zum Aktivieren oder Inaktivieren der Änderungsprotokolldatenbank verwenden. Der Verzeichnisserver muss gestoppt werden, bevor die Änderungsprotokolldatenbank konfiguriert oder dekonfiguriert werden kann.

Verwenden Sie den Befehl **idscfgchglg**, um das Änderungsprotokoll für einen Verzeichnisserver zu konfigurieren. Verwenden Sie den Befehl **idsucfgchglg**, um das Änderungsprotokoll für einen Verzeichnisserver zu dekonfigurieren. Eine Änderungsprotokolldatenbank kann nicht für eine Proxy-Server-Instanz konfiguriert werden.

Damit Sie das Änderungsprotokoll für eine Verzeichnisserverinstanz konfigurieren können, müssen die folgenden Bedingungen erfüllt sein:

1. Es muss eine DB2-Instanz mit dem Namen der Verzeichnisserverinstanz vorhanden sein.
2. Sie müssen eine Datenbank für die Verzeichnisserverinstanz konfigurieren.
3. Unter AIX, Linux und Solaris muss der lokale Prüfschleifenservice in der Datei `/etc/services` registriert sein.

Wenn Sie eine Änderungsprotokolldatenbank konfigurieren, wird sie in derselben Datenbankinstanz erstellt wie die Datenbank der Verzeichnisserverinstanz. Für die Änderungsprotokolldatenbank sind 30 MB zusätzlicher Festplattenspeicherplatz erforderlich. Wenn Sie das Änderungsprotokoll konfigurieren, wird der Änderungsprotokolleintrag der Konfigurationsdatei der Verzeichnisserverinstanz hinzugefügt.

## Änderungsprotokoll mit dem Konfigurationstool konfigurieren

Konfigurieren Sie mithilfe des **Konfigurationstools** die Änderungsprotokolldatenbank mit einer Verzeichnisserverinstanz.

### Vorbereitende Schritte

Zum Konfigurieren des Änderungsprotokolls für eine Instanz muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem **Konfigurationstool** für eine Instanz konfigurieren“ auf Seite 184.

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Änderungsprotokoll verwalten**.
3. Führen Sie auf der Seite **Änderungsprotokoll verwalten** die folgenden Schritte aus:
  - a. Wählen Sie **Datenbank für Änderungsprotokoll aktivieren** aus, um das Änderungsprotokoll zu konfigurieren.
  - b. Geben Sie im Bereich **Maximale Anzahl der Protokolleinträge** die maximale Anzahl an Einträgen an, die in der Änderungsprotokolldatenbank erfasst werden sollen.
    - Klicken Sie auf **Uneingeschränkt**, um eine unbegrenzte Anzahl von Einträgen im Änderungsprotokoll zu erfassen.
    - Klicken Sie auf **Einträge** und geben Sie die gewünschte Eintragsanzahl an, um eine bestimmte Anzahl von Einträgen zu erfassen. Die Standardanzahl an Einträgen ist 1.000.000.
  - c. Geben Sie im Bereich **Maximale Verweildauer** den maximalen Zeitraum an, für den die Einträge in der Änderungsprotokolldatenbank gespeichert werden sollen.
    - Klicken Sie auf **Uneingeschränkt**, um die Einträge im Änderungsprotokoll unbegrenzt zu speichern.
    - Klicken Sie auf **Verweildauer** und geben Sie die Anzahl der Tage und Stunden ein.
  - d. Klicken Sie auf **Aktualisieren**, um die Änderungen anzuwenden.
  - e. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
  - f. Überprüfen Sie die Protokolle, die bei der Konfiguration der Änderungsprotokolldatenbank generiert werden.
  - g. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
  - h. Klicken Sie auf **Schließen**, um die Seite **Änderungsprotokoll verwalten** zu schließen.
4. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
5. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

### Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## Änderungsprotokoll mit dem Befehlszeilendienstprogramm konfigurieren

Konfigurieren Sie mit dem Befehlszeilendienstprogramm **idscfgchg1g** die Änderungsprotokolldatenbank für eine Verzeichnisserverinstanz.

## Vorbereitende Schritte

Zum Konfigurieren des Änderungsprotokolls für eine Instanz muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem Befehlszeilendienstprogramm für eine Instanz konfigurieren“ auf Seite 188.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

## Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisserverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Führen Sie den Befehl **idscfgchglg** aus, um das Änderungsprotokoll für eine Verzeichnisserverinstanz zu konfigurieren.
  - Führen Sie den Befehl **idscfgchglg** aus, um ein Änderungsprotokoll für eine Instanz zu konfigurieren, für das keine Zeitdauer- und Größenbeschränkung gilt:  

```
idscfgchglg -I instance_name -m 0
```
  - Führen Sie den Befehl **idscfgchglg** aus, um ein Änderungsprotokoll für eine Instanz zu konfigurieren, für das eine Größenbeschränkung von 1.000.000 Einträgen und eine Zeitdauerbeschränkung von 25 Stunden gilt:  

```
idscfgchglg -I instance_name -m 1000000 -y 1 -h 1
```

Weitere Informationen zum Befehl **idscfgchglg** finden Sie in der Veröffentlichung *Command Reference*.

## Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

## Änderungsprotokoll mit dem Konfigurationstool dekonfigurieren

Dekonfigurieren Sie mithilfe des **Konfigurationstools** die Änderungsprotokoll Datenbank von einer Verzeichnisserverinstanz.

## Vorbereitende Schritte

Zum Dekonfigurieren des Änderungsprotokolls von einer Instanz muss die Instanz die folgenden Anforderungen erfüllen:

- Das Änderungsprotokoll für eine Instanz muss konfiguriert sein. Siehe „Änderungsprotokoll mit dem **Konfigurationstool** konfigurieren“ auf Seite 209.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.

2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Änderungsprotokoll verwalten**.
3. Führen Sie auf der Seite **Änderungsprotokoll verwalten** die folgenden Schritte aus:
  - a. Wählen Sie **Datenbank für Änderungsprotokoll aktivieren** ab, um das Änderungsprotokoll zu dekonfigurieren.
  - b. Klicken Sie auf **Aktualisieren**, um die Änderungen anzuwenden.
  - c. Klicken Sie im Fenster **Änderungsprotokoll verwalten** auf **Ja**, um die Aktion zu bestätigen.
  - d. Überprüfen Sie die Protokolle, die beim Dekonfigurieren der Änderungsprotokolldatenbank generiert werden.
  - e. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
  - f. Klicken Sie auf **Schließen**, um die Seite **Änderungsprotokoll verwalten** zu schließen.
4. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
5. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

### Nächste Schritte

Starten Sie den Verzeichnissever. Siehe „Verzeichnissever und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## Änderungsprotokoll mit dem Befehlszeilendienstprogramm dekonfigurieren

Dekonfigurieren Sie mit dem Befehlszeilendienstprogramm **idsucfgchglg** die Änderungsprotokolldatenbank von einer Verzeichnisseverinstanz.

### Vorbereitende Schritte

Zum Dekonfigurieren des Änderungsprotokolls von einer Instanz muss die Instanz die folgenden Anforderungen erfüllen:

- Das Änderungsprotokoll für eine Instanz muss konfiguriert sein. Siehe „Änderungsprotokoll mit dem Befehlszeilendienstprogramm konfigurieren“ auf Seite 210.
- Stoppen Sie den Verzeichnissever. Siehe „Verzeichnissever und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

### Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisseverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Führen Sie den Befehl **idsucfgchglg** im folgenden Format aus, um das Änderungsprotokoll für eine Verzeichnisseverinstanz zu dekonfigurieren:  
`idsucfgchglg -I instance_name`

Weitere Informationen zum Befehl **idsucfgchglg** finden Sie in der Veröffentlichung *Command Reference*.



## Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

---

## Suffixkonfiguration

Um eine Verzeichnishierarchie erstellen zu können, müssen Sie das erforderliche Suffix für Ihre Verzeichnisserverinstanz konfigurieren.

Ein Suffix ist ein Namenskontext. Dabei handelt es sich um einen DN (definierter Name), der den höchsten Eintrag in einer Verzeichnishierarchie angibt. LDAP verwendet das relative Benennungsschema. Ein DN ist also auch das Suffix für alle Einträge in einer Verzeichnishierarchie. Sie können in einem Verzeichnisserver mehrere Suffixe hinzufügen, die jeweils eine Verzeichnishierarchie angeben. Wenn Sie ein Suffix hinzufügen, wird der Eintrag zur Konfigurationsdatei einer Verzeichnisserverinstanz hinzugefügt. Das folgende Beispiel zeigt einen Suffixeintrag:  
o=sample

Zum Hinzufügen oder Entfernen von Suffixen können Sie das **Konfigurationstool** verwenden. Sie können auch den Befehl **idscfgsuf** zum Hinzufügen von Suffixen und den Befehl **idsucfgsuf** zum Entfernen von Suffixen verwenden. Der Verzeichnisserver muss vor dem Hinzufügen oder Entfernen eines Suffixes gestoppt werden. Weitere Informationen zu den Befehlen **idscfgsuf** und **idsucfgsuf** finden Sie in der *Befehlsreferenz*.

Systemdefinierte Suffixe können nicht aus einer Verzeichnisserverinstanz entfernt werden. Diese Suffixe sind in Proxy-Server-Instanzen nicht verfügbar. Die folgenden Suffixe werden vom System definiert:

- cn=localhost
- cn=configuration
- cn=ibmpolicies
- cn=Deleted Objects

Beim Hinzufügen von Einträgen zu einem Verzeichnisserver müssen die folgenden Aspekte beachtet werden:

- Für Suffix-DNs müssen einem Verzeichnisserver Suffixeinträge hinzugefügt werden.
- Ein definierter Eintragsname, der zu einem Verzeichnisserver hinzugefügt wird, muss ein Suffix enthalten, das mit dem Suffixwert für den definierten Namen übereinstimmt. Das folgende Beispiel zeigt einen Eintrag mit einem definierten Suffixnamen: ou=Marketing,o=sample.
- Sie können auf einer Proxy-Server-Instanz oder auf einem Verzeichnisserver, der nicht mit einer DB2-Datenbank konfiguriert ist, keine Einträge hinzufügen.

Wenn eine Abfrage ein Suffix enthält, das mit keinem der in der lokalen Datenbank konfigurierten Suffixe übereinstimmt, wird diese Abfrage an den LDAP-Server verwiesen, der durch den Standardverweis festgelegt ist. Wird kein LDAP-Standardverweis angegeben, wird die folgende Nachricht erstellt: Objekt nicht vorhanden.

## Suffix mit dem Konfigurationstool hinzufügen

Mit dem **Konfigurationstool** können Sie ein Suffix zu einer Instanz hinzufügen.

## Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um ein Suffix zu einer Instanz hinzuzufügen:

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## Informationen zu diesem Vorgang

Wenn Sie ein Suffix zu einer Instanz hinzufügen, wird der Suffixeintrag zur Konfigurationsdatei einer Instanz hinzugefügt.

## Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Suffixe verwalten**.
3. Führen Sie auf der Seite **Suffixe verwalten** die folgenden Schritte aus:
  - a. Geben Sie im Feld "Suffix-DN" das Suffix ein, das Sie zu der Instanz hinzufügen wollen.
  - b. Klicken Sie auf **Hinzufügen**.
  - c. Klicken Sie auf **OK**, um die Änderungen anzuwenden.
4. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
5. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## Suffix mit dem Befehlszeilendienstprogramm hinzufügen

Mit dem Befehlszeilendienstprogramm **idscfgsuf** können Sie ein Suffix zu einer Instanz hinzufügen.

## Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um ein Suffix zu einer Instanz hinzuzufügen:

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

## Informationen zu diesem Vorgang

Wenn Sie ein Suffix zu einer Instanz hinzufügen, wird der Suffixeintrag zur Konfigurationsdatei einer Instanz hinzugefügt.

## Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisserverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.

4. Wählen Sie zum Hinzufügen des Suffix `o=sample` zu einer Instanz den Befehl **idscfgsuf** im folgenden Format:  
`idscfgsuf -I instance_name -s "o=sample"`

Weitere Informationen zum Befehl **idscfgsuf** finden Sie in der Veröffentlichung *Command Reference*.

## Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

## Suffix mit dem Konfigurationstool entfernen

Mit dem **Konfigurationstool** können Sie ein Suffix aus einer Verzeichnisserverinstanz entfernen.

### Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um ein Suffix aus einer Verzeichnisserverinstanz zu entfernen:

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Informationen zu diesem Vorgang

Wenn Sie ein Suffix aus einer Instanz entfernen, wird der Suffixeintrag aus der Konfigurationsdatei einer Instanz entfernt.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Suffixe verwalten**.
3. Führen Sie auf der Seite **Suffixe verwalten** die folgenden Schritte aus:
  - a. Wählen Sie in der Liste **Aktuelle Suffix-DNs** das Suffix aus, das entfernt werden soll. Bei einem vollständigen Verzeichnisserver können Sie die folgenden systemdefinierten Suffixe nicht entfernen:
    - `cn=localhost`
    - `cn=configuration`
    - `cn=ibmpolicies`
    - `cn=Deleted Objects`
  - b. Klicken Sie auf **Entfernen**.
  - c. Klicken Sie im Bestätigungsfenster **Suffixe verwalten** auf **OK**.
  - d. Klicken Sie auf **OK**, um die Änderungen anzuwenden.
4. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
5. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## Suffix mit dem Befehlszeilendienstprogramm entfernen

Mit dem Befehlszeilendienstprogramm **idsucfgsuf** können Sie ein Suffix aus einer Instanz entfernen.

### Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um ein Suffix aus einer Instanz zu entfernen:

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Informationen zu diesem Vorgang

Wenn Sie ein Suffix aus einer Instanz entfernen, wird der Suffixeintrag aus der Konfigurationsdatei einer Instanz entfernt. Bei einem vollständigen Verzeichnisserver können Sie die folgenden systemdefinierten Suffixe nicht entfernen:

- cn=localhost
- cn=configuration
- cn=ibmpolicies
- cn=Deleted Objects

### Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisserverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Führen Sie den Befehl **idsucfgsuf** aus, um das Suffix `o=sample` aus einer Instanz zu entfernen:

```
idsucfgsuf -I instance_name -s "o=sample"
```

Weitere Informationen zum Befehl **idsucfgsuf** finden Sie in der Veröffentlichung *Command Reference*.

### Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

---

## Schemaverwaltung

Wenn Sie möchten, dass eine Instanz Klassen für benutzerdefinierte Objekte und Attribute unterstützt, müssen Sie eine Schemadatei hinzufügen, in der die Klassen für benutzerdefinierte Objekte und Attribute definiert sind.

Zum Verwalten der Schemadateien können Sie das **Konfigurationstool** oder Befehlszeilendienstprogramme wie **idscfgsch** oder **idsucfgsch** verwenden. Die Schemadatei muss auf dem Computer bereits vorhanden sein. Weitere Informationen zu den Befehlen **idscfgsch** und **idsucfgsch** finden Sie in der *Befehlsreferenz*.

Der Verzeichnisserver muss vor dem Hinzufügen oder Entfernen von Schemadateien gestoppt werden.

Wenn Sie Schemadateien hinzufügen oder entfernen, wird die Konfigurationsdatei der Instanz aktualisiert. Sie können die folgenden Operationen zur Schemaverwaltung durchführen:

- Schemadateien zur Liste mit Schemadateien hinzufügen, die beim Serverstart geladen wird.
- Schemadateien aus der Liste mit Schemadateien löschen, die beim Serverstart aktualisiert wird.
- Typ der Gültigkeitsprüfung ändern, die für Schemadateien durchgeführt wird.

Die folgenden systemdefinierten Schemadateien können nicht entfernt werden:

- V3.config.at
- V3.config.oc
- V3.ibm.at
- V3.ibm.oc
- V3.system.at
- V3.system.oc
- V3.user.at
- V3.user.oc
- V3.ldapsyntaxes
- V3.matchingrules
- V3.modifiedschema

Sie können das **Konfigurationstool** auch verwenden, um die Schemaprüfregel festzulegen, mit der überprüft wird, ob die Einträge den Schemaregeln entsprechen. Die Standardschemaprüfregel ist Version 3 (abgeschwächt). Die folgenden Schemaprüfregeln werden von einem Verzeichnisserver unterstützt:

#### **Version 3 (strikt)**

Auf dem Server werden mithilfe von LDAP Version 3 (strikt) Validierungsprüfungen der Einträge durchgeführt. Bei dieser Art von Prüfung müssen alle übergeordneten Objektklassen beim Hinzufügen von Einträgen vorhanden sein.

#### **Version 3 (abgeschwächt)**

Auf dem Server werden mithilfe von LDAP Version 3 (abgeschwächt) Validierungsprüfungen der Einträge durchgeführt. Bei dieser Art von Prüfung müssen nicht alle übergeordneten Objektklassen beim Hinzufügen von Einträgen vorhanden sein. LDAP Version 3 (abgeschwächt) ist die Standardschemaprüfregel.

#### **Version 2**

Auf dem Server werden mithilfe von LDAP Version 2 Prüfungen der Einträge durchgeführt.

**Keine** Auf dem Server werden keine Validierungsprüfungen durchgeführt.

## **Schemadatei mit dem Konfigurationstool verwalten**

Mit dem **Konfigurationstool** können Sie Schemadateien für eine Instanz verwalten.

### **Vorbereitende Schritte**

Führen Sie die folgenden Schritte aus, um Schemadateien für eine Instanz zu verwalten:

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## Informationen zu diesem Vorgang

Wenn Sie eine Schemadatei hinzufügen oder entfernen, wird die Konfigurationsdatei einer Instanz mit dem Schemaeintrag aktualisiert.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Schemadateien verwalten**.
3. Wählen Sie auf der Seite **Schemadateien verwalten** die Operation aus, die Sie ausführen wollen.
  - Führen Sie die folgenden Schritte aus, um eine Schemadatei zur Konfigurationsdatei einer Instanz hinzuzufügen:
    - a. Geben Sie im Feld **Pfad und Dateiname** den Namen der Schemadatei und den Pfad ein. Sie können auf **Durchsuchen** klicken und den Namen und die Position der Schemadatei angeben.
    - b. Klicken Sie auf **Hinzufügen**.
  - Führen Sie die folgenden Schritte aus, um eine Schemadatei aus der Konfigurationsdatei einer Instanz zu entfernen:
    - a. Wählen Sie in der Liste mit den aktuellen Schemadateien die Schemadatei aus, die entfernt werden soll.
    - b. Klicken Sie auf **Entfernen**.
    - c. Klicken Sie im Bestätigungsfenster **Schemadateien verwalten** auf **OK**.
4. Klicken Sie auf **OK**, um die Änderungen anzuwenden.
5. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
6. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

### Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## Schemadatei mit dem Befehlszeilendienstprogramm verwalten

Mit den Befehlszeilendienstprogrammen können Sie Schemadateien für eine Verzeichnisserverinstanz verwalten.

### Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um Schemadateien für eine Instanz zu verwalten:

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

## Informationen zu diesem Vorgang

Wenn Sie eine Schemadatei hinzufügen oder entfernen, wird die Konfigurationsdatei einer Instanz mit dem Schemaeintrag aktualisiert.

## Vorgehensweise

1. Melden Sie sich als Eigner der Verzeichnisserverinstanz an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Wählen Sie zum Verwalten einer Schemadatei für eine Instanz die Operation aus, die Sie ausführen wollen.
  - Wählen Sie zum Hinzufügen einer Schemadatei zu einer Instanz den Befehl **idscfgsch** im folgenden Format:  
`idscfgsch -I instance_name -s schema_file.oc`
  - Wählen Sie zum Entfernen einer Schemadatei aus einer Instanz den Befehl **idsucfgsch** im folgenden Format:  
`idsucfgsch -I instance_name -s schema_file.oc`

Weitere Informationen zum Befehl **idscfgsch** oder **idsucfgsch** finden Sie in der Veröffentlichung *Command Reference*.

## Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

## Schemavalidierungsregel mit dem Konfigurationstool konfigurieren

Mit dem **Konfigurationstool** können Sie eine Schemavalidierungsregel für eine Instanz konfigurieren.

### Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um eine Schemavalidierungsregel für eine Instanz zu konfigurieren:

- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Informationen zu diesem Vorgang

Wenn Sie eine Schemavalidierungsregel konfigurieren, wird die Konfigurationsdatei einer Instanz mit dem Wert aktualisiert.

## Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Schemadateien verwalten**.
3. Wählen Sie auf der Seite **Schemadateien verwalten** im Bereich **Regeln für die Schemavalidierung** eine der folgenden Schemavalidierungsregeln aus:
  - Klicken Sie auf **Version 3 (strikt)**, um eine strikte Validierung gemäß LDAP Version 3 zu konfigurieren.
  - Klicken Sie auf **Version 3 (abgeschwächt)**, um eine abgeschwächte Validierung gemäß LDAP Version 3 zu konfigurieren.
  - Klicken Sie auf **Version 2**, um eine Validierung gemäß LDAP Version 2 zu konfigurieren.

- Klicken Sie auf **Keine**, um anzugeben, dass keine Validierung erforderlich ist.
- 4. Klicken Sie auf **OK**, um die Änderungen anzuwenden.
- 5. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
- 6. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Nächste Schritte

Starten Sie den Verzeichnissever. Siehe „Verzeichnissever und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

---

## LDIF-Datenmanagement

Um Verzeichnisdaten verwenden zu können, müssen Sie einer Verzeichnisseverinstanz Daten aus einer bereits vorhandenen Instanz oder aus einer LDIF-Datei (LDAP Data Interchange Format) hinzufügen.

Sie können das **Konfigurationstool** zum Importieren von Daten aus einer LDIF-Datei oder zum Exportieren von Daten aus einer Datenbank in eine LDIF-Datei verwenden. Mit LDIF werden LDAP-Einträge im Textformat dargestellt. Wenn Sie Daten importieren, können Sie Einträge zu einer leeren Verzeichnisdatenbank oder zu einer Datenbank, die bereits Einträge enthält, hinzufügen. Sie können das **Konfigurationstool** auch zum Prüfen der Daten in der LDIF-Datei verwenden, ohne Daten zum Verzeichnis hinzuzufügen.

Sie können Daten zu Instanzen hinzufügen, die mit DB2-Datenbanken konfiguriert wurden. Verzeichnisdaten können nicht zu Proxy-Server-Instanzen hinzugefügt werden, da dies nicht unterstützt wird.

Wenn Sie LDIF-Daten von einer anderen Serverinstanz importieren möchten, müssen Sie die Serverinstanzen in Bezug auf die Verschlüsselung synchronisieren. Sie müssen die bidirektionale Verschlüsselung zwischen Verzeichnisseverinstanzen synchronisieren, um die bei der Serverkommunikation zum Verschlüsseln und Entschlüsseln von Daten benötigte Zeit zu reduzieren. Wenn Sie LDIF-Daten, die nicht in Bezug auf die Verschlüsselung synchronisiert wurden, importieren, werden AES-verschlüsselte Einträge in der Datei nicht importiert. Weitere Informationen zum Synchronisieren der bidirektionalen Verschlüsselung finden Sie in der *Befehlsreferenz*.

Wenn die Serverinstanzen nicht in Bezug auf die Verschlüsselung synchronisiert werden, geben Sie den Seedwert für die Verschlüsselung und den Saltwert für die Verschlüsselung des Zielservers an, wenn sie eine LDIF-Datei von einem Quellenserver exportieren. Die AES-verschlüsselten Daten werden mithilfe der AES-Schlüssel des Quellenservers entschlüsselt und dann mithilfe des Seedwerts für die Verschlüsselung und des Saltwerts des Zielservers verschlüsselt. Diese verschlüsselten Daten werden in der LDIF-Datei gespeichert.

Um Daten zu importieren zu können, müssen vor dem Starten des Prozesses die folgenden Anforderungen erfüllt sein:

- Bei Proxy-Server-Instanzen oder Instanzen, die nicht mit einer DB2-Datenbank konfiguriert sind, ist es nicht möglich, LDIF-Daten zu importieren oder zu exportieren.
- Fügen Sie auf dem Zielserver, auf den die Daten importiert werden sollen, die erforderlichen Suffixe hinzu. Weitere Informationen finden Sie im Kapitel „Suffixkonfiguration“ auf Seite 213.



- Der Zielsever, auf den die Daten importiert werden sollen, muss gestoppt werden.

Optimieren Sie die Datenbank nach dem Laden großer Datenmengen, zum Beispiel nach dem Füllen der Datenbank, mit dem Dienstprogramm **idsbulkload**. Durch diese Operation kann die Leistung der Datenbank verbessert werden.

Sie können zum Importieren, Exportieren oder Prüfen der LDIF-Daten auch die folgenden Befehlszeilendienstprogramme verwenden:

- Verwenden Sie die Dienstprogramme **idsldif2db** oder **idsbulkload** zum Importieren von Daten aus einer LDIF-Datei.
- Zum Exportieren von Daten in eine LDIF-Datei können Sie das Dienstprogramm **idsdb2ldif** verwenden.
- Um Daten in der LDIF-Datei zu prüfen, verwenden Sie das Dienstprogramm **idsbulkload**.

Weitere Informationen zu den Befehlszeilendienstprogrammen finden Sie in der *Befehlsreferenz*.

## Beispiele

Um den Saltwert für die Verschlüsselung eines Servers abzurufen, führen Sie den Befehl **idsldapsearch** im folgenden Format aus:

```
idsldapsearch -h host_name -p port -D adminDN -w adminPWD \
  -b "cn=crypto,cn=localhost" objectclass=* ibm-slapdCryptoSalt

ibm-slapdCryptoSalt=:SxaQ+.qdKor
```

Die Zeichenfolge nach dem Gleichheitszeichen (=) im Attribut `ibm-slapdCryptoSalt` ist der Saltwert für die Verschlüsselung. In diesem Beispiel ist `:SxaQ+.qdKor` der Saltwert für die Verschlüsselung.

## LDIF-Daten mit dem Konfigurationstool importieren

Mit dem **Konfigurationstool** können Sie Daten aus einer LDIF-Datei in eine Verzeichnisserverinstanz importieren.

### Vorbereitende Schritte

Zum Importieren von Daten aus einer LDIF-Datei in eine Instanz muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem **Konfigurationstool** für eine Instanz konfigurieren“ auf Seite 184.
- Die erforderlichen Suffixeinträge müssen konfiguriert sein. Siehe „Suffix mit dem **Konfigurationstool** hinzufügen“ auf Seite 213.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsverzeichnis mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **LDAP-Tasks > LDIF-Daten importieren**.
3. Führen Sie auf der Seite **LDIF-Daten importieren** die folgenden Schritte aus:

- a. Geben Sie im Feld **Pfad und Name der LDIF-Datei** den Pfad und Dateinamen der LDIF-Datei ein, aus der die Daten importiert werden sollen. Sie können auch auf **Durchsuchen** klicken und den Namen und Pfad der LDIF-Datei angeben.
  - b. Wenn nachfolgende Leerzeichen aus den Daten entfernt werden sollen, wählen Sie **nachgestellte Leerzeichen in Standardimport oder Bulkload entfernen** aus.
  - c. Wählen Sie je nach der Anzahl der Einträge, die Sie importieren wollen, eine passende Option aus:
    - Klicken Sie auf **Standardimport**, um die Daten mit dem Dienstprogramm **idsldif2db** zu importieren. Verwenden Sie die Option, wenn die LDIF-Datei nur wenige Einträge enthält.
    - Klicken Sie auf **Bulkload**, um die Daten mit dem Dienstprogramm **idsbulkload** zu importieren. Bei LDIF-Dateien mit einer größeren Anzahl an Einträgen importiert das Dienstprogramm **idsbulkload** die Daten schneller als **idsldif2db**.
  - d. Wenn Sie für den Datenimport die Option **Bulkload** ausgewählt haben, müssen Sie angeben, welche Validierungstypen Sie für die LDIF-Daten ausführen wollen:
    - 1) Wählen Sie **Schemaüberprüfung aktivieren** aus, um zu überprüfen, ob die LDIF-Daten dem Schema entsprechen.
    - 2) Wählen Sie **ACL-Überprüfung aktivieren** aus, um zu überprüfen, ob die LDIF-Daten die entsprechenden ACLs enthalten.
  - e. Klicken Sie auf **Importieren**, um die Importoperation zu starten.
  - f. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
  - g. Überprüfen Sie die Protokolle, die bei der Importoperation der LDIF-Daten generiert werden.
  - h. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
  - i. Klicken Sie auf **Schließen**, um die Seite **LDIF-Daten importieren** zu schließen.
4. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
  5. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179. Optimieren Sie die Datenbank nach dem Laden großer Datenmengen, zum Beispiel nach dem Füllen der Datenbank, mit dem Dienstprogramm **idsbulkload**. Weitere Informationen zum Optimieren der Datenbank finden Sie unter „Datenbank mit dem **Konfigurationstool** optimieren“ auf Seite 195.

## LDIF-Daten mit dem Konfigurationstool prüfen

Sie können das **Konfigurationstool** zum Prüfen der LDIF-Datei für das Verzeichnisserverschema verwenden, ohne Daten zur Datenbank hinzuzufügen.

### Vorbereitende Schritte

Zum Prüfen von Daten in einer LDIF-Datei mit dem Verzeichnisserverschema muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem **Konfigurationstool** für eine Instanz konfigurieren“ auf Seite 184.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **LDAP-Tasks > LDIF-Daten importieren**.
3. Führen Sie auf der Seite **LDIF-Daten importieren** die folgenden Schritte aus:
  - a. Geben Sie im Feld **Pfad und Name der LDIF-Datei** den Pfad und Dateinamen der LDIF-Datei ein, aus der die Daten importiert werden sollen. Sie können auch auf **Durchsuchen** klicken und den Namen und Pfad der LDIF-Datei angeben.
  - b. Klicken Sie auf **Nur Datenvalidierung**.
  - c. Klicken Sie auf **Importieren**, um die Datenprüfung zu starten.
  - d. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.
  - e. Überprüfen Sie die Protokolle, die bei der Datenprüfung generiert werden.
  - f. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
  - g. Klicken Sie auf **Schließen**, um die Seite **LDIF-Daten importieren** zu schließen.
4. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
5. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

### Nächste Schritte

Starten Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

## LDIF-Daten mit dem Konfigurationstool exportieren

Mit dem **Konfigurationstool** können Sie Verzeichnisdaten aus einer Instanz in eine LDIF-Datei exportieren.

### Vorbereitende Schritte

Zum Exportieren von Daten aus einer Instanz in eine LDIF-Datei muss die Instanz die folgenden Anforderungen erfüllen:

- Es muss eine mit einer DB2-Datenbank konfigurierte Verzeichnisserverinstanz vorhanden sein. Siehe „Datenbank mit dem **Konfigurationstool** für eine Instanz konfigurieren“ auf Seite 184.
- Die Instanz muss Verzeichniseinträge enthalten.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.
2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **LDAP-Tasks > LDIF-Daten exportieren**.

3. Führen Sie auf der Seite **LDIF-Daten exportieren** die folgenden Schritte aus:
  - a. Geben Sie im Feld **Pfad und Name der LDIF-Datei** den Pfad und Dateinamen der LDIF-Datei ein, in die die Daten exportiert werden sollen. Sie können auch auf **Durchsuchen** klicken und den Namen und Pfad der LDIF-Datei angeben.
  - b. Wenn die Datei bereits vorhanden ist und mit Daten überschrieben werden soll, wählen Sie **Überschreiben, falls Datei vorhanden** aus.
  - c. Wählen Sie **Aktive Attribute exportieren** aus, um die aktiven Attribute wie `creatorsName`, `createTimestamp`, `modifiersName` und `modifyTimestamp` zu exportieren. Die aktiven Attribute werden vom Server erstellt und geändert, wenn ein Verzeichniseintrag erstellt bzw. geändert wird. Die Attribute enthalten Informationen zu dem Benutzer, der den Eintrag erstellt oder geändert hat, sowie zur Uhrzeit, zu der der Eintrag erstellt bzw. geändert wurde. Diese Einträge werden als Steuerelement im Base-64-Format in der LDIF-Datei abgelegt.
  - d. Wählen Sie **Daten für AES-Zielservers exportieren** aus, wenn Daten auf einen AES-Zielservers (AES = Advanced Encryption Standard) importiert werden sollen und die Verschlüsselung des Servers nicht mit dem Quellenservers synchronisiert ist.
  - e. Wählen Sie **Gelöschte Einträge exportieren** aus, wenn die Einträge exportiert werden sollen, die zwar gelöscht wurden, jedoch weiterhin in der Tombstone-Unterverzeichnisstruktur gespeichert sind. Weitere Informationen zur Tombstone-Unterverzeichnisstruktur finden Sie im Abschnitt Verwaltung der IBM Security Directory Server-Dokumentation.
  - f. Geben Sie nach der Auswahl von **Daten für AES-Zielservers exportieren** die folgenden Werte an:
    - Geben Sie im Feld **Seedwert für die Verschlüsselung** den Seedwert für die Verschlüsselung des Zielservers ein.
    - Geben Sie im Feld **Saltwert für die Verschlüsselung** den Saltwert für die Verschlüsselung des Zielservers ein. Weitere Informationen zum Abrufen des Saltwerts für die Verschlüsselung finden Sie unter „LDIF-Datenmanagement“ auf Seite 220.
  - g. Geben Sie im Feld **Filtereintrags-DN** den DN eines gültigen Replikationsfilters ein, um einen Filter für Einträge anzugeben, die in die LDIF-Datei exportiert werden sollen. Der Filter exportiert bestimmte Datenbankeinträge, die die Kriterien für die LDIF-Datei erfüllen. Weitere Informationen zu den Replikationsfiltern finden Sie im Abschnitt Verwaltung der IBM Security Directory Server-Dokumentation.
  - h. Wenn Sie Kommentare zur LDIF-Datei hinzufügen wollen, geben Sie diese im Feld **Kommentare** ein.
  - i. Wenn Sie Einträge in einer bestimmten Unterverzeichnisstruktur exportieren wollen, geben Sie im Feld **DN der Unterverzeichnisstruktur** deren DN ein. Der DN der Unterverzeichnisstruktur gibt den obersten Eintrag der Unterverzeichnisstruktur an, die in die LDIF-Datei geschrieben werden soll. Die Unterverzeichnisstruktur und alle in der Verzeichnishierarchie darunter enthaltenen Einträge werden in die Datei geschrieben. Wenn Sie einen DN der Unterverzeichnisstruktur angeben, werden alle in der Datenbank gespeicherten Einträge in die Ausgabedatei geschrieben. Die Einträge werden anhand der Suffixe identifiziert, die in der Konfigurationsdatei der Verzeichnisserversinstanz angegeben werden.
  - j. Klicken Sie auf **Exportieren**, um die Exportoperation zu starten.
  - k. Klicken Sie auf **OK**, um die Ausführung der Task zu bestätigen.

- l. Überprüfen Sie die Protokolle, die bei der Exportoperation der LDIF-Daten generiert werden.
  - m. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
  - n. Klicken Sie auf **Schließen**, um die Seite **LDIF-Daten exportieren** zu schließen.
4. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
  5. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

---

## Active Directory-Synchronisation

Sie können die Einträge im Container für Benutzer und Gruppen in Microsoft Active Directory mit einer IBM Security Directory Server-Instanz synchronisieren. Die Datensynchronisation von Active Directory in eine Verzeichnisserverinstanz ist unidirektional.

**Anmerkung:** Ab IBM Security Directory Server Version 6.3.1 wird die Active Directory-Synchronisationslösung nicht weiter unterstützt. Verwenden Sie stattdessen die Lösung LDAPSync.

Sie können das Konfigurationstool oder Befehlszeilendienstprogramme wie **idsadscfg** oder **idsadsrun** verwenden, um eine Active Directory-Synchronisation zu konfigurieren und auszuführen.

**Anmerkung:** Die Synchronisation von Benutzern und Gruppen von Active Directory in eine IBM Security Directory Server-Instanz über IBM Security Directory Proxy Server wird nicht unterstützt.

Bei der Active Directory-Synchronisation wird IBM Security Directory Integrator für die Synchronisation der Benutzer- und Gruppencontainer verwendet. Vor der Verwendung der Active Directory-Synchronisation müssen Sie IBM Security Directory Integrator installieren.

IBM Security Directory Integrator ist für die folgenden Aktionen erforderlich:

- Ausführen der Konfiguration
- Starten, Stoppen, Neustarten und Überwachen von Operationen

Berücksichtigen Sie die folgenden Punkte beim Konfigurieren der Active Directory-Synchronisation:

- Die Anwendung für die Active Directory-Synchronisation und IBM Security Directory Integrator müssen sich auf demselben Computer wie die Verzeichnisserverinstanz befinden.
- Mit der Active Directory-Synchronisation wird nur der Benutzer- und Gruppencontainer synchronisiert. Das Tool synchronisiert keine anderen Objekte oder Container in eine Verzeichnisserverinstanz.
- Die Lösung prüft auch die Gruppenzugehörigkeit des Benutzereintrags und der Benutzereintrag wird zu denjenigen Gruppen in der Instanz hinzugefügt, die mit Active Directory synchronisiert werden. Wenn ein bereits vorhandener Benutzereintrag aus dem Benutzercontainer entfernt wird, wird dieser Eintrag aus der Instanz gelöscht. Außerdem wird der Benutzereintrag aus allen Gruppen in der Instanz gelöscht.

- Mit der Active Directory-Synchronisation können keine verschachtelten Organisationseinheiten (ou) synchronisiert werden.
- Es ist nicht möglich, mehrere Attribute von Active Directory einem einzelnen Attribut in einer Verzeichnisserverinstanz zuzuordnen.
- Das Attribut userpassword von Active Directory kann keiner Verzeichnisserverinstanz zugeordnet werden. Das Benutzerkennwort wird nicht von dieser Lösung synchronisiert.
- Mit der Active Directory-Synchronisation können Benutzer und Gruppen aus einem Benutzercontainer von Active Directory oder aus mehreren in eine einzige Organisationseinheit (ou) eines Verzeichnisseservers synchronisiert werden. Das Tool kann jedoch nicht mehrere Benutzer- und Gruppencontainer von Active Directory in mehrere Organisationseinheiten (ou) eines Verzeichnisseservers synchronisieren.
- Sie können angeben, dass mehrere Benutzercontainer mit einer einzigen Organisationseinheit (ou) in einem Verzeichnisserver synchronisiert werden sollen. Verwenden Sie hierzu das Semikolon (;) als Trennzeichen. Andere Zeichen werden als Trennzeichen nicht unterstützt. Wenn Sie als Trennzeichen ein Semikolon (;) verwenden, setzen Sie das Argument in Anführungszeichen ("). Im folgenden Beispiel wird ein Semikolon (;) als Trennzeichen verwendet:  
"ou=SWUGroups,dc=adsync,dc=com;ou=STGGroups,dc=adsync,dc=com"
- Das Attribut SAMAccountName in Active Directory wird zum Erstellen des Attributs \$dn in IBM Security Directory Server verwendet. Das Attribut SAMAccountName ist in einer Domäne eindeutig und es gibt keine Konflikte beim Synchronisieren mehrerer Active Directory-Benutzercontainer in eine einzige Organisationseinheit eines Verzeichnisseservers.
- Die Lösung unterstützt sichere Verbindungen zu Active Directory, aber nicht zu Verzeichnisserverinstanzen.
- Wenn Sie den Administrator-DN und/oder das zugehörige Kennwort für eine Verzeichnisserverinstanz ändern, nachdem Sie die Active Directory-Synchronisation konfiguriert haben, müssen Sie die Konfiguration der Active Directory-Synchronisation wiederholen.
- Wenn Benutzer- oder Gruppencontainer aus Active Directory während der Ausführung der Active Directory-Synchronisation geändert werden, müssen Sie die Active Directory-Synchronisation mit den neuen Namen erneut konfigurieren. Andernfalls wird das Active Directory-Synchronisationsprogramm möglicherweise nicht ausgeführt.
- Wenn Sie IBM Security Directory Server-Benutzer und -Gruppen mit einem anderen Tool als der Active Directory-Synchronisation ändern, funktioniert die Active Directory-Synchronisation möglicherweise nicht ordnungsgemäß.

## Active Directory-Synchronisation konfigurieren und ausführen

Konfigurieren Sie die Active Directory-Synchronisation und führen Sie sie aus, um Benutzer- und Gruppencontainer von Active Directory mit einer Instanz von IBM Security Directory Server zu synchronisieren.

### Vorbereitende Schritte

Zum Konfigurieren und Ausführen der Active Directory-Synchronisation müssen Sie die folgende Software installieren:

- IBM Security Directory Server
- IBM Security Directory Integrator

## Vorgehensweise

1. Wenn Sie IBM Security Directory Integrator in einem angepassten Pfad installiert haben, setzen Sie die Umgebungsvariable `IDS_LDAP_TDI_HOME` mit dem Installationspfad.

**Anmerkung:** Setzen Sie die Umgebungsvariable auf einem Windows-System mit einem Installationspfad, der weder Leerzeichen noch Anführungszeichen enthält. Verwenden Sie bei der Pfadangabe den Kurznamen.

Der Standardinstallationspfad von IBM Security Directory Integrator lautet:

### AIX und Solaris

`/opt/IBM/TDI/V7.1`

**Linux** `/opt/ibm/TDI/V7.1`

### Windows

`C:\Program Files\IBM\TDI\V7.1`

2. Optional: Laden Sie die Beispieldateien `users.ldif` und `groups.ldif` in Active Directory.
3. Führen Sie den Befehl `idsadscfg` aus, um die Active Directory-Synchronisation zu konfigurieren. Sie können die Active Directory-Synchronisation auch die Ausführung des **Konfigurationstools** konfigurieren. Mit dem Befehl werden die Dateien `adsync_private.prop` und `adsync_public.prop` erstellt.
4. Ändern Sie die Datei `adsync_public.prop`, um optionale Attribute und SSL-Parameter anzupassen. Informationen zu den Dateien und zur sicheren Kommunikation finden Sie im Abschnitt *Verwaltung* in der IBM Security Directory Server-Dokumentation.
5. Führen Sie den Befehl `idsadsrun` aus, um die Active Directory-Synchronisation zu starten. Sie werden von dem Befehl gefragt, ob Sie eine vollständige Synchronisation und anschließend eine Echtzeitsynchronisation durchführen oder die Echtzeitsynchronisation starten wollen. Die Active Directory-Synchronisation erkennt die Änderungen an den Active Directory-Einträgen und synchronisiert sie mit den Einträgen in IBM Security Directory Server.
6. Optional: Führen Sie IBM Security Directory Integrator **Administration and Monitoring Console** aus, um die Synchronisation zu verwalten und zu überwachen.

## Active Directory-Synchronisation mit dem Konfigurationstool konfigurieren

Konfigurieren Sie mithilfe des **Konfigurationstools** die Active Directory-Synchronisation mit einer Verzeichnisserverinstanz.

### Vorbereitende Schritte

Zum Konfigurieren der Active Directory-Synchronisation müssen Sie die folgenden Anforderungen erfüllen:

- Installieren Sie IBM Security Directory Integrator.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit dem **Konfigurationstool** starten oder stoppen“ auf Seite 179.

### Vorgehensweise

1. Starten Sie das **Konfigurationstool** für eine Instanz. Siehe „**Konfigurationstool** starten“ auf Seite 178.

2. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Active Directory-Synchronisation**.
3. Geben Sie auf der Seite **Active Directory-Synchronisation: Instanzdetails** die Konfigurationsdetails zu der Instanz von IBM Security Directory Server an. Ihre Angaben werden in den Dateien `adsync_private.properties` und `adsync_public.properties` gespeichert. Die Dateien werden im Ausgangsverzeichnis der Instanz im Unterverzeichnis `etc/tdisoldir` gespeichert.
4. Geben Sie im Feld **Verzeichnissuffix** das Suffix des Verzeichnisservers an, das für die Active Directory-Synchronisation verwendet werden soll. Im Feld **LDAP-URL** ist die URL für die Verzeichnisserverinstanz angegeben. Dieses Feld kann nicht bearbeitet werden.
5. Geben Sie im Feld **Eintrags-DN für Gruppencontainer** den DN eines vorhandenen Containers ein, in den Gruppen, die von Active Directory stammen, kopiert werden sollen. Die Gruppen und Zugehörigkeiten von Benutzern zu den Gruppen werden zwischen Active Directory und IBM Security Directory Server synchronisiert. Wenn Sie einen Benutzer zu einer Active Directory-Gruppe hinzufügen oder daraus entfernen, wird der Eintrag zu der entsprechenden Gruppe in der IBM Security Directory Server-Instanz hinzugefügt bzw. aus dieser entfernt.
6. Geben Sie im Feld **Eintrags-DN für Benutzercontainer** den DN eines vorhandenen Containers ein, in den Benutzer, die von Active Directory stammen, kopiert werden sollen.
7. Wenn Sie eine SSL-Verbindung zu Active Directory herstellen wollen, müssen Sie **SSL-Verbindung zu Active Directory verwenden** auswählen. Eine SSL-Verbindung zu IBM Security Directory Server wird nicht unterstützt. Informationen zu den Schritten zum Konfigurieren einer SSL-Verbindung zu Active Directory finden Sie im Abschnitt *Verwaltung* der IBM Security Directory Server-Dokumentation.
8. Klicken Sie auf **Weiter**. Daraufhin wird die Seite **Active Directory-Synchronisation: Active Directory-Details** aufgerufen.
9. Geben Sie im Feld **Hostadresse** den Hostnamen oder die IP-Adresse des Active Directory-Domänencontrollers ein.
10. Geben Sie im Feld **Host-Port** den Port ein, der von Active Directory verwendet wird.
11. Geben Sie im Feld **Anmeldename** den Anmeldenamen ein, den IBM Security Directory Integrator für die Bindung zu Active Directory verwenden muss. Die Anmelde-ID muss über die erforderliche Berechtigung zum Lesen der Active Directory-Einträge verfügen, die an die Verzeichnisserverinstanz weitergeleitet werden sollen.
12. Geben Sie im Feld "Anmeldekennwort" das Kennwort ein, das IBM Security Directory Integrator für die Bindung zu Active Directory verwenden muss.
13. Geben Sie im Feld **Suchbasis** die Unterverzeichnisstruktur in Active Directory ein, über die Sie die Änderungen an die Instanz weitergeben wollen. Die Änderungen an den Benutzereinträgen in dieser Unterverzeichnisstruktur werden an die Verzeichnisserverinstanz weitergegeben. Um alle Benutzer in Active Directory-Gruppen an die Instanz weiterzugeben, müssen Sie die Suchbasis in der Hierarchie von Active Directory nach oben versetzen.
14. Geben Sie im Feld **Eintrags-DN für Gruppencontainer** den DN des Active Directory-Containers ein, über den die Gruppen mit der Instanz synchronisiert werden sollen.
15. Geben Sie im Feld **Eintrags-DN für Benutzercontainer** den DN des Active Directory-Containers ein, über den die Benutzereinträge mit der Instanz synchronisiert werden sollen.



16. Klicken Sie auf **Fertig stellen**. Das Fenster **Active Directory-Synchronisation: Ergebnisse** wird geöffnet.
17. Überprüfen Sie die Protokollnachrichten, die für die Konfiguration der Active Directory-Synchronisation generiert werden.
18. Klicken Sie auf **Ergebnisse löschen**, um den Inhalt der Protokolle zu löschen.
19. Klicken Sie auf **Schließen**, um die Seite **Active Directory-Synchronisation** zu schließen.
20. Klicken Sie auf **Datei > Beenden**, um das Fenster **Konfigurationstool** zu schließen.
21. Klicken Sie auf **Ja**, um Ihre Aktion zu bestätigen.

## Active Directory-Synchronisation mit dem Befehlszeilendienstprogramm konfigurieren

Konfigurieren Sie mithilfe des Befehlszeilendienstprogramms **idsadscfg** die Active Directory-Synchronisation mit einer Verzeichnisserverinstanz.

### Vorbereitende Schritte

Zum Konfigurieren der Active Directory-Synchronisation müssen Sie die folgenden Anforderungen erfüllen:

- Installieren Sie IBM Security Directory Integrator.
- Stoppen Sie den Verzeichnisserver. Siehe „Verzeichnisserver und Verwaltungsserver mit Befehlszeilendienstprogrammen starten oder stoppen“ auf Seite 166.

### Vorgehensweise

1. Melden Sie sich unter AIX, Linux oder Solaris als Root und unter Windows als Mitglied der Administratorgruppe an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Unterverzeichnis `sbin` der Installationsposition von IBM Security Directory Server.
4. Führen Sie den Befehl **idsadscfg** im folgenden Format aus, um die Active Directory-Synchronisation mit einer Instanz zu konfigurieren:

```
idsadscfg -I instance_name -adH ldap://LDAP_server1:389 -adb dc=adsynctest,dc=com
-adD cn=administrator,cn=users,dc=adsynctest,dc=com -adw secret -adg ou=testgroup1,
dc=adsynctest,dc=com -adu ou=testuser1,dc=adsynctest,dc=com -idss o=sample -idsg
ou=Testgroup1,ou=groups,o=sample -idsu ou=Testuser1,ou=users,o=sample
```

Weitere Informationen zum Befehl **idsadscfg** finden Sie in der Veröffentlichung *Command Reference*.

### Nächste Schritte

Führen Sie den Befehl **idsadsrun** aus, um die Active Directory-Synchronisation zu starten. Weitere Informationen zum Befehl **idsadsrun** finden Sie in der Veröffentlichung *Command Reference*.



---

## Kapitel 21. Automatisches Starten von Verzeichnisserverinstanzen beim Start des Betriebssystems

Sie können Verzeichnisserverinstanzen so konfigurieren, dass sie automatisch gestartet werden, wenn ein Computer nach der Wartung oder einem Upgrade erneut gestartet wird.

Wenn Sie eine Verzeichnisserverinstanz starten, wird der Verwaltungsserver gestartet, wenn die Erstellung der Instanz erfolgreich war. Zum Starten eines Verzeichnisservers mit einer DB2-Datenbank muss der Prozess `ibmslapd` oder `idsslapd` für die Instanz gestartet werden.

Wenn Sie einen Computer erneut starten, müssen Sie sowohl den Verwaltungsserver als auch den Prozess `ibmslapd` starten, die der Instanz zugeordnet sind. Sie können jedoch Services und Prozesse, die einer Instanz zugeordnet sind, so konfigurieren, dass sie automatisch auf Ihrem Betriebssystem gestartet werden.

Um die Verzeichnisserverinstanz unter AIX, Linux oder Solaris beim Betriebssystemstart zu starten, muss die Datei `/etc/inittab` mit den Serverinformationen aktualisiert werden. In der Datei `inittab` sind die Prozesse angegeben, die beim Systemstart und für den normalen Betrieb gestartet werden müssen. Fügen Sie der Datei `inittab` einen Eintrag für den Verzeichnisserver im folgenden Format hinzu:  
`id:runlevels:action:process`

Für die Attribute in der Datei `inittab` sind die folgenden Werte erforderlich:

**id** Dieses Attribut enthält in der Datei eine eindeutige ID mit 1-4 Ziffern.

### **runlevels**

Das Attribut `runlevels` steht für den `runlevel`-Modus des Betriebssystems, in dem der Prozess automatisch gestartet wird. Er bezieht sich auf die Betriebsart eines AIX-, Linux- oder Solaris-Betriebssystems. Die Konfiguration des Attributs `runlevels` ist für die verschiedenen Betriebssysteme unterschiedlich. Konfigurationsdetails zum Attribut `runlevel` finden Sie im Handbuch Ihres Betriebssystems.

**action** `action` gibt den Aktionstyp an.

### **process**

Das Attribut `process` gibt den zu startenden Prozess an.

---

## Automatisches Starten für eine Verzeichnisserverinstanz unter Windows konfigurieren

Im Fenster **Dienste** können Sie das automatische Starten einer Verzeichnisserverinstanz unter Windows konfigurieren.

### Vorbereitende Schritte

Um eine Verzeichnisserverinstanz so zu konfigurieren, dass sie nach dem Start des Betriebssystems automatisch gestartet wird, muss Ihr Computer die folgenden Anforderungen erfüllen:

- Der Computer muss eine Verzeichnisserverinstanz enthalten, die im normalen Modus ausgeführt werden kann.

## Informationen zu diesem Vorgang

Unter Windows können Sie einen Verzeichnisserver, den Prozess `idsslapd`, im Fenster **Dienste** oder mit dem Befehl `idsslapd` starten. Bei einer Verzeichnisserverinstanz mit einer DB2-Datenbank müssen Sie festlegen, dass sich der Service, der dem Verzeichnisserver zugeordnet wird, nach dem DB2-Instanzservice richtet. Bei einer Verzeichnisserverinstanz mit einer DB2-Datenbank muss DB2 gestartet werden, damit der Prozess `idsslapd` starten kann. Wenn Sie die Abhängigkeit nicht festlegen und im Feld **Starttyp** die Einstellung **Automatic** (Automatisch) für den dem Server zugeordneten Service konfigurieren, tritt beim Neustart des Computers möglicherweise ein Fehler auf. Bei einer Proxy-Server-Instanz müssen Sie die Abhängigkeit von dem Service, der der DB2-Instanz zugeordnet ist, nicht konfigurieren.

Verwenden Sie bei einer Proxy-Server-Instanz die Schritte 1, 2, 4, 5 und 6.

### Vorgehensweise

1. Melden Sie sich als Mitglied der Administratorgruppe an.
2. Führen Sie die folgenden Schritte aus, um das Fenster **Dienste** zu öffnen:
  - a. Klicken Sie auf **Start > Ausführen**.
  - b. Geben Sie im Feld **Öffnen** die Zeichenfolge `services.msc` ein.
  - c. Klicken Sie auf **OK**.
3. Suchen Sie den DB2-Servicenamen, der Ihrer Verzeichnisserverinstanz zugeordnet ist, die automatisch gestartet werden soll. Der Servicename fängt mit `DB2 - SDSV631DB2` an. Wenn Ihr DB2-Instanzname `DSRDBM01` lautet, ist der Eintrag `DB2 - SDSV631DB2 - DSRDBM01`. Doppelklicken Sie auf den Service und notieren Sie im Feld **Anzeigename** den ersten Wert nach `DB2 - SDSV631DB2` -. Im vorliegenden Beispiel ist der Wert `DSRDBM01`.
4. Suchen Sie den Service für die Verzeichnisserverinstanz, die automatisch gestartet werden soll. Der Servicename fängt mit `IBM Security Directory Server Instance 6.3.1` an. Wenn Ihr DB2-Instanzname `dsrdbm01` lautet, ist der Eintrag `IBM Security Directory Server Instance 6.3.1 - dsrdbm01`. Doppelklicken Sie auf den Service und notieren Sie im Feld **Anzeigename** den ersten Wert nach `IBM Security Directory Server Instance 6.3.1` -. Im vorliegenden Beispiel für die Instanz `dsrdbm01` ist der Wert `idsslapd-dsrdbm01`.
5. Wählen Sie im Fenster mit den Eigenschaften von `IBM Security Directory Server Instance 6.3.1 - dsrdbm01` in der Liste **Starttyp** den Eintrag **Automatic** aus.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Datei > Beenden**, um das Fenster **Dienste** zu schließen.
8. Führen Sie die folgenden Schritte aus, um die Windows-Registrierungsdatenbank zu öffnen:
  - a. Klicken Sie auf **Start > Ausführen**.
  - b. Geben Sie im Feld **Öffnen** die Zeichenfolge `regedit` ein.
  - c. Klicken Sie auf **OK**.
9. Wechseln Sie im linken Navigationsfenster zu **Computer > HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Services**.
10. Suchen Sie den Service, der Ihrer Verzeichnisserverinstanz zugeordnet ist. Im Beispiel ist dies `idsslapd-dsrdbm01`.
11. Klicken Sie auf den Service, der Ihrer Instanz zugeordnet ist.

12. Doppelklicken Sie auf der rechten Seite des Fensters auf das Attribut `DependOnService`.
13. Fügen Sie im Fenster **Mehrteilige Zeichenfolge bearbeiten** den Namen für den DB2-Service, der der Instanz zugeordnet ist, unter **LanmanServer** hinzu. Im Beispiel ist dies `DSRDBM01`.
14. Klicken Sie auf **OK**. Dadurch wird eine Abhängigkeit von dem DB2-Service erstellt.
15. Klicken Sie auf **Datei > Beenden**, um die Windows-Registrierungsdatenbank zu schließen.

## Ergebnisse

Nach dem Neustart des Computers wird die Verzeichnisserverinstanz automatisch gestartet.

---

## Automatisches Starten für eine Verzeichnisserverinstanz unter UNIX konfigurieren

Aktualisieren Sie die Datei `/etc/inittab` mit den Verzeichnisservereinträgen, um automatisches Starten einer Verzeichnisserverinstanz unter AIX, Linux oder Solaris zu konfigurieren.

### Vorbereitende Schritte

Um eine Verzeichnisserverinstanz so zu konfigurieren, dass sie nach dem Start des Betriebssystems automatisch gestartet wird, muss Ihr Computer die folgenden Anforderungen erfüllen:

- Der Computer muss eine Verzeichnisserverinstanz enthalten, die im normalen Modus ausgeführt werden kann.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Fügen Sie die folgenden Einträge zur Datei `/etc/inittab` hinzu, um eine Verzeichnisserverinstanz oder eine Proxy-Server-Instanz für das automatische Starten zu konfigurieren:
  - a. Fügen Sie die folgenden Einträge hinzu, um den Prozess `idsslapd` und den Verwaltungsserver hinzuzufügen, der einer Verzeichnisserverinstanz zugeordnet ist.

```
AIX   srv1:2:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
        instance_name > /dev/null 2>&1 #Autostart IBM Directory Server
        Instance
```

```
adm1:2:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
        instance_name > /dev/null 2>&1 #Autostart IBM Directory
        Administration Server
```

```
Linux srv1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmslapd -I
        instance_name > /dev/null 2>&1 #Autostart IBM Directory Server
        Instance
```

```
adm1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmdiradm -I
        instance_name > /dev/null 2>&1 #Autostart IBM Directory
        Administration Server
```

## Solaris

```
srv1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmslapd -I  
instance_name > /dev/null 2>&1 #Autostart IBM Directory Server  
Instance
```

```
adm1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I  
instance_name > /dev/null 2>&1 #Autostart IBM Directory  
Administartion Server
```

Setzen Sie für die Variable *instance\_name* den Instanznamen ein.

- b. Um den Prozess *idsslapd* und den Verwaltungsserver hinzuzufügen, der einer Proxy-Server-Instanz zugeordnet ist, müssen Sie zuerst die Verzeichnisserverinstanzen starten. Sie müssen alle Verzeichnisseverinstanzen starten, bevor Sie den Proxy-Server starten. Wenn sich auf Ihrem Computer vollständige Verzeichnisseverinstanzen und ein Proxy-Server befinden, kalkulieren Sie eine Verzögerung zwischen dem Start des vollständigen Verzeichnisseverinstanzen und dem Start des Proxy-Servers ein. Im folgenden Beispiel tritt die Verzögerung dadurch auf, dass ein Eintrag im Format *id:2345:wait* zur Datei */etc/inittab* hinzugefügt wird.

```
AIX  srv1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I  
instance_name1 > /dev/null 2>&1 #Autostart IBM Directory  
Server Instance
```

```
adm1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I  
instance_name1 > /dev/null 2>&1 #Autostart IBM Directory  
Administartion Server
```

```
srv2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I  
instance_name2 > /dev/null 2>&1 #Autostart IBM Directory  
Server Instance
```

```
adm2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I  
instance_name2 > /dev/null 2>&1 #Autostart IBM Directory  
Administartion Server
```

```
srv3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I  
proxy_instance1 -k > /dev/null 2>&1 #Autostart IBM Directory  
Proxy Server Instance
```

```
adm3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I  
proxy_instance1 -k > /dev/null 2>&1 #Autostart IBM Directory  
Administartion Server
```

```
srv4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I  
proxy_instance1 > /dev/null 2>&1 #Autostart IBM Directory  
Proxy Server Instance
```

```
adm4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I  
proxy_instance1 > /dev/null 2>&1 #Autostart IBM Directory  
Administartion Server
```

Setzen Sie für die Variablen *instance\_name1* und *instance\_name2* die Namen Ihrer Verzeichnisseverinstanzen ein. Setzen Sie für die Variable *proxy\_instance1* den Namen Ihrer Proxy-Server-Instanz ein.

## Ergebnisse

Nachdem die Einträge zur Datei `/etc/inittab` hinzugefügt wurden, kann die Verzeichnisserverinstanz (vollständiger Server oder Proxy-Server) nach dem Neustart des Systems automatisch gestartet werden.





---

## Kapitel 22. Fixpackstrategie

Suchen Sie Informationen zu Fixpacks und Patches für IBM Security Directory Server.

Fixpacks und Patches für AIX, Linux, Solaris und HP-UX für die native scriptbasierte Installation sind verfügbar.

IBM Installation Manager-basierte Patches und Fixpacks für Windows sind verfügbar.

IBM Installation Manager-basierte Patches oder Fixpacks können in der grafischen Benutzeroberfläche und im unbeaufsichtigten Installationsmodus installiert werden.

Sie können die Version des installierten Patches oder Fixpacks mit IBM Installation Manager auf eine der folgenden Arten ermitteln:

- Wählen Sie **File > View Installed Packages** aus.
- Verwenden Sie den Befehl **imcl** im Unterverzeichnis 'tools' des Installationsverzeichnisses von IBM Installation Manager.

Prüfen Sie auf UNIX-Systemen die Versionen der nativen Pakete, um die Version des installierten Patches oder Fixpacks zu ermitteln.

**Anmerkung:** Nachdem das native Fixpack auf die Basisversion angewendet wurde, darf keine Änderung oder Deinstallation mit IBM Installation Manager vorgenommen werden. Verwenden Sie nach der Anwendung des nativen Fixpacks nur die native Methode für weitere Operationen.

---

### Fixpacks mit IBM Installation Manager installieren

Verwenden Sie IBM Installation Manager, um unter Microsoft Windows-Betriebssystemen Fixpacks anzuwenden oder Service-Stream-Erweiterungen zu installieren.

#### Vorbereitende Schritte

- Lesen Sie die Informationen zur Fixpackstrategie.
- Stellen Sie sicher, dass IBM Installation Manager Version 1.7.0 oder höher auf Ihrem System installiert ist. Weitere Informationen enthält die IBM Installation Manager-Dokumentation.
- Vor dem Starten der Fixpackinstallation müssen Sie alle aktiven Prozesse oder Services für IBM Security Directory Server stoppen. Dies kann manuell erfolgen oder durch Klicken auf die Option zum Stoppen aller blockierenden Prozesse in Installation Manager.

#### Informationen zu diesem Vorgang

Das Fixpack aktualisiert nur Komponenten, die bereits installiert sind. Sie müssen das Produkt aktualisieren, bevor Sie mit dem **Assistenten für Änderungen** Komponenten installieren, die auf Ihrem System noch nicht installiert sind.

Das Fixpack führt keine Aktualisierung für IBM DB2, IBM GSKit, IBM embedded WebSphere Application Server und für IBM Java Development Kit durch. Verwenden Sie den **Assistenten für Änderungen**, um diese Software zu aktualisieren.

## Vorgehensweise

1. Laden Sie das Fixpack von <http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631> herunter.
2. Legen Sie die Repository-Vorgaben in IBM Installation Manager fest.
  - a. Um IBM Installation Manager über das Menü **Start** zu starten, klicken Sie auf **Alle Programme > IBM Installation Manager > IBM Installation Manager**.
  - b. Klicken Sie auf der Startseite von IBM Installation Manager auf **File > Preferences**.
  - c. Klicken Sie auf der Seite **Repositories** auf **Add Repository**.
  - d. Geben Sie auf der Seite **Add Repository** eine der folgenden Repository-Positionen an:
    - Dateipfad für ein lokales Verzeichnis oder ein fernes, gemeinsam genutztes Laufwerk mit dem Produktpaket, das von der IBM Support-Website heruntergeladen wurde
    - Die URL für das Repository auf einem Web-Server
  - e. Klicken Sie auf **OK**. Wenn Sie eine HTTPS- oder eine eingeschränkte Repository-Position angegeben haben, werden Sie aufgefordert, eine Benutzer-ID und ein Kennwort einzugeben. Die neue oder geänderte Repository-Position wird aufgeführt.
  - f. Klicken Sie auf **Test Connections**, um den Zugriff auf das Repository zu überprüfen.
  - g. Klicken Sie auf **OK**, um die Seite **Repositories** zu schließen.
3. Starten Sie die Installation.
  - Wenn IBM Security Directory Server Version 6.3.1 nicht auf Ihrem System installiert ist, führen Sie die folgenden Schritte aus:
    - a. Klicken Sie auf der Startseite von IBM Installation Manager auf **Install**. Der Assistent zum **Installieren** unterstützt Sie beim Installationsprozess.
    - b. Führen Sie das in „Installation mit IBM Installation Manager“ auf Seite 32 beschriebene Installationsverfahren durch.
  - Wenn IBM Security Directory Server Version 6.3.1 auf Ihrem System installiert ist, führen Sie die folgenden Schritte aus, um das Fixpack anzuwenden:
    - a. Klicken Sie auf der Startseite von IBM Installation Manager auf **Update**. Der **Assistent für Aktualisierungen** sucht nach verfügbaren Updates für die Pakete, die auf Ihrem System installiert sind.
    - b. Wählen Sie **IBM Security Directory Server** aus. Das Installationsverzeichnis, in dem Version 6.3.1 installiert wurde, wird verwendet und kann nicht geändert werden. Klicken Sie auf **Next**.
    - c. Wählen Sie das Produkt **IBM Security Directory Server** zum Aktualisieren aus und anschließend das Update, das angewendet werden soll (**Version 6.3.1.5**). Klicken Sie auf **Next**.
    - d. Akzeptieren Sie die Lizenz für das Fixpack und klicken Sie anschließend auf **Next**.
    - e. Die zu aktualisierenden Komponenten werden standardmäßig ausgewählt. Nur die Komponenten, die bereits auf dem System installiert sind, werden zum Aktualisieren angezeigt. Klicken Sie auf **Next**.

**Anmerkung:** Wenn Sie versuchen, eine der standardmäßigen Auswahlen zu inaktivieren, wird die betreffende Komponente zum Deinstallieren markiert.

**Einschränkung:** IBM DB2 ist auf dieser Seite zwar als Komponente aufgelistet und standardmäßig zum Aktualisieren ausgewählt, wird jedoch nicht aktualisiert. Die vorausgesetzte Software wird nicht aktualisiert, wenn Sie den **Assistenten für Aktualisierungen** in IBM Installation Manager auswählen. Wählen Sie die Komponente IBM DB2 nicht ab, da sonst die Serverkomponente ebenfalls abgewählt wird.

- f. Überprüfen Sie die Angaben auf der Übersichtsseite und klicken Sie anschließend auf **Next**, um die Installation zu starten.
4. Überprüfen Sie Ihre Installation. Informationen zur Überprüfung mit IBM Installation Manager und zur Überprüfung für das von Ihnen verwendete Betriebssystem finden Sie unter Kapitel 13, „Überprüfung der IBM Security Directory Server-Features“, auf Seite 87.

## Nächste Schritte

Verwenden Sie zum Deinstallieren des Fixpacks den **Rollback-Assistenten**, der die Vorgängerversion des Pakets wiederherstellt.

## Fixpacks unbeaufsichtigt installieren

Sie können IBM Installation Manager verwenden, um Fixpacks unbeaufsichtigt zu installieren.

**Anmerkung:** In einer Antwortdatei für Aktualisierungen kann keine Komponente angegeben werden, die noch nicht installiert ist. Andernfalls schlägt der Aktualisierungsprozess fehl.

## Neue Antwortdatei für die Fixpackinstallation erstellen

Wenn die bei der Produktinstallation verwendete Antwortdatei nicht zur Verfügung steht, erfassen Sie eine neue Antwortdatei.

1. Starten Sie IBM Installation Manager in einem simulierten Installationsmodus. Beispiel:

```
C:\Programme\IBM\Installation Manager\eclipse\IBMIM.exe  
-record c:\SDS_6310\install_resp.xml -skipInstall agentDataLocation
```

Dabei gilt Folgendes:

Die Position *agentDataLocation* wird zum Speichern der Daten für die Produktinstallation verwendet.

2. Geben Sie als Repository-Vorgabe die Version 6.3.1.0 an.
3. Schließen Sie den simulierten Installationsprozess ab.
4. Schließen Sie IBM Installation Manager. Eine Antwortdatei für den Installationsprozess wird erstellt, ohne das Produkt zu installieren.
5. Führen Sie die im folgenden Abschnitt angegebenen Schritte aus.

## Installation mit der Antwortdatei für die vorherige Produktinstallation

1. Bearbeiten Sie die Datei `install_resp.xml` und nehmen Sie die folgenden Änderungen vor:
  - a. Geben Sie den Repository-Pfad der Version 6.3.1.5 an.  
`<repository location='C:\SDS_6315\ibm_sds' />`
  - b. Geben Sie als Angebotsversion die Version 6.3.1.5 an.  
`<offering id='com.ibm.security.directoryserver.v631' version='6.3.1.5' profile=.....`

2. Starten Sie die unbeaufsichtigte Installation, um das Fixpack anzuwenden. Beispiel:

```
C:\Programme\IBM\Installation Manager\eclipse\tools\imcl.exe  
input c:\SDS_6310\install_resp.xml -acceptLicense -showProgress
```

In diesem Befehl können Sie bei Bedarf auch die Option `-stopBlockingProcesses` verwenden, um alle blockierenden Prozesse unbeaufsichtigt zu stoppen, bevor das Fixpack installiert wird.

---

## Fixpacks mit nativen Scripts installieren

Führen Sie das bereitgestellte Script über die Befehlszeile aus, um Fixpacks zu installieren oder Service-Stream-Erweiterungen auf AIX-, Linux- oder Solaris-Systemen zu installieren.

### Vorbereitende Schritte

Lesen Sie die Informationen zur Fixpackstrategie.

### Vorgehensweise

1. Laden Sie das Fixpack von <http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631> herunter.
2. Extrahieren Sie das Fixarchiv in ein Verzeichnis mit genügend freiem Speicherplatz. Details zum Inhalt des Fixpacks (einschließlich Verzeichnis- und Dateinamen) enthält die im Fixpack enthaltene *README*-Datei.
3. Stoppen Sie alle zugehörigen Client- und Serverprozesse für IBM Security Directory Server. Zur Gruppe der Dämonprozesse gehören der Verzeichnisserver, der Verwaltungsserver, der Proxy-Server (falls verwendet) sowie alle angepassten LDAP-Anwendungen. Aktive Programme und Bibliotheken können nicht ersetzt werden. Wenn die Tracefunktion aktiviert ist, führen Sie den Befehl **ldtrc off** aus, um die Tracefunktion zu stoppen. Informationen zum Stoppen der Verzeichnisserverinstanzen und Verwaltungsprozesse enthalten die Abschnitte unter Basic server administration tasks in der IBM Security Directory Server-Dokumentation.
4. Wechseln Sie in der Befehlszeile in das Verzeichnis, in das Sie das Fixarchiv extrahiert haben.
5. Führen Sie den folgenden Befehl als root aus:  

```
idsinstall -u -f
```

Das Installationsprogramm installiert Aktualisierungen für die Komponenten, die bereits auf Ihrem System installiert sind.

6. Überprüfen Sie Ihre Installation.
  - a. Das Installationsprogramm zeigt eine Nachricht an, die angibt, ob die Installation erfolgreich durchgeführt wurde. Überprüfen Sie das Installationsprotokoll im Verzeichnis `/tmp/idsinstall_zeitmarke`.
  - b. Wenn die Installation nicht erfolgreich durchgeführt wurde oder eine Nachricht darauf hinweist, dass nicht alle Pakete installiert wurden, beheben Sie die im Protokoll angegebenen Fehler (z. B. fehlender Plattenspeicherplatz). Führen Sie anschließend das Installationsprogramm erneut aus und stellen Sie sicher, dass alle Pakete erfolgreich installiert werden.
  - c. Überprüfen Sie die Versionsnummer der Pakete, um sicherzustellen, dass die richtigen Versionen installiert sind. Anweisungen hierzu finden Sie unter Kapitel 6, „IBM Security Directory Server-Pakete abfragen“, auf Seite 49.

---

## Kapitel 23. IBM Security Directory Server deinstallieren: Übersicht

Dieser Abschnitt enthält eine Übersicht für die Deinstallation des Produkts IBM Security Directory Server und wichtige Vorbereitungen für die Deinstallation.

### Vorbereitende Schritte

Zum Deinstallieren von IBM Security Directory Server müssen Sie sich auf AIX-, Linux-, Solaris- oder HP-UX-Systemen als Root anmelden und auf Windows-Systemen als Mitglied der Administratorgruppe.


### Informationen zu diesem Vorgang

Wenn Sie IBM Security Directory Server deinstallieren, werden die Instanzen und deren Konfigurationsdateien nicht entfernt.

### Vorgehensweise

1. Stoppen Sie alle Client- oder Serverprozesse von IBM Security Directory Server, einschließlich des Verzeichnisservers, des Verwaltungsdämons und der angepassten LDAP-Anwendungen. Aktive Programme und Bibliotheken können nicht ersetzt werden. Wenn die Tracefunktion aktiviert wird, führen Sie den Befehl **ldtrc off** aus, um sie zu inaktivieren.
2. Verwenden Sie entsprechend dem Betriebssystem und dem Modus der Installation von IBM Security Directory Server denselben Modus bei der Deinstallation von IBM Security Directory Server. Die folgenden Methoden zur Deinstallation von IBM Security Directory Server sind verfügbar:
  - a. Deinstallationsprogramm der grafischen Benutzerschnittstelle
  - b. Betriebssystemdienstprogramme Die Paketnamen auf Linux-Systemen weichen bei Aktualisierungen leicht von der Version für allgemeine Verfügbarkeit (GA) ab. Der Paketname des Basisclients der GA-Version unter xSeries Linux beispielsweise lautet `idsldap-clbase63-6.3.0-0.i386.rpm`. Mit dem Befehl **rpm -qa** können Sie alle Pakete auflisten.
3. Fragen Sie nach der Deinstallation von IBM Security Directory Server ab, ob alle IBM Security Directory Server-Pakete erfolgreich entfernt wurden. Weitere Informationen hierzu finden Sie unter Kapitel 6, „IBM Security Directory Server-Pakete abfragen“, auf Seite 49.

### Zugehörige Informationen:

 <http://www-01.ibm.com/support/knowledgecenter/SSVJJU/welcome>  
Weitere Informationen finden Sie unter *IBM Security Directory Server deinstallieren* im Abschnitt *Installation und Konfiguration* in der IBM Security Directory Server-Produktdokumentation.



---

## Kapitel 24. Deinstallation von IBM Security Directory Server und zusätzlich erforderlicher Software

Wenn Sie Ihren Computer für einen anderen Zweck verwenden oder stilllegen möchten, möchten Sie IBM Security Directory Server und die dafür zusätzlich erforderliche Software möglicherweise entfernen.

Sie können IBM Installation Manager oder Betriebssystemdienstprogramme für die Deinstallation von IBM Security Directory Server verwenden. Derselbe Modus, der für die Installation verwendet wurde, muss auch für die Deinstallation verwendet werden. Es muss entweder IBM Installation Manager für sowohl Installation als auch Deinstallation verwendet werden oder es müssen die Betriebssystemdienstprogramme für sowohl Installation als auch Deinstallation verwendet werden. Für die Installation und Deinstallation dürfen keine unterschiedlichen Modi verwendet werden.

Wenn IBM Security Directory Server vom Computer entfernt werden soll, müssen die folgenden Bedingungen vor der Deinstallation beachtet werden:

1. Sie müssen alle Client- und Serverprozesse von IBM Security Directory Server stoppen.
  - Verzeichnisserver
  - Verwaltungsserver
  - LDAP-Traces
  - **Webverwaltungstool** und der zugeordnete Anwendungsserver
  - Benutzerdefinierte LDAP-Anwendungen
2. Wenn die Installation von IBM Security Directory Server erneut auf dem Computer durchgeführt werden soll, muss die Verzeichnisserverinstanz nicht gelöscht und die DB2-Datenbank nicht für die Instanz dekonfiguriert werden. Wenn IBM Security Directory Server von Ihrem Computer entfernt werden soll, bleiben die Verzeichnisserverinstanzen intakt, bis sie manuell entfernt oder dekonfiguriert werden.
3. Der Benutzer und die Gruppe `idsldap`, die während der Installation von IBM Security Directory Server erstellt wurden, verbleiben nach der Deinstallation auf dem System. Beachten Sie vor der Deinstallation von IBM Security Directory Server von AIX-, Linux- oder Solaris-Systemen die zusätzlichen Bedingungen.
  - Wenn Sie den definierten Benutzer/die definierte Gruppe `idsldap` nicht benötigen, verwenden Sie zum Entfernen die Betriebssystemdienstprogramme. Der Benutzer und die Gruppe `idsldap` sind sowohl für den Proxy-Server als auch den vollständigen Verzeichnisserver erforderlich und müssen auf dem Computer vorhanden sein, wenn IBM Security Directory Server installiert ist.
  - Wenn Sie den Benutzer `idsldap`, aber nicht das Ausgangsverzeichnis dieses Benutzers entfernen, können Probleme auftreten, wenn der Benutzer `idsldap` während der Installation von IBM Security Directory Server erstellt wird. Stellen Sie daher sicher, dass das Ausgangsverzeichnis des Benutzers `idsldap` entfernt wurde, bevor Sie diesen entfernen. Wenn Sie den Befehl **userdel** zum Entfernen des Benutzers `idsldap` verwenden, stellen Sie sicher, dass der Parameter **-r** zum Entfernen des Ausgangsverzeichnisses verwendet wird: `userdel -r idsldap`.

4. Unter Windows werden die Verwaltungsserver- und Verzeichnisserverdienste während der Deinstallation von IBM Security Directory Server entfernt. Diese Dienste werden bei der Installation von IBM Security Directory Server nicht ersetzt. Sie können den Befehl `idsstlapd` zum Hinzufügen des Server-Services und den Befehl `idsdiradm` zum Hinzufügen des Verwaltungs-Server-Services verwenden. Weitere Informationen zu den Befehlen `idsstlapd` und `idsdiradm` finden Sie in der Befehlsreferenz von *IBM Security Directory Server*.

---

## Deinstallation mit IBM Installation Manager

Wenn Sie für die Installation von IBM Security Directory Server IBM Installation Manager verwendet haben, müssen Sie IBM Installation Manager auch für die Deinstallation von IBM Security Directory Server und dessen Komponenten verwenden.

Wenn Sie IBM Installation Manager für die Deinstallation von IBM Security Directory Server verwenden, entfernt das Programm IBM Security Directory Server und die dafür zusätzlich erforderliche Software vollständig. Sie können die Features von IBM Security Directory Server während der Deinstallation mit IBM Installation Manager nicht selektiv entfernen.

Wenn Sie die Version von IBM DB2, die mit IBM Security Directory Server bereitgestellt wird, installiert haben, müssen alle DB2-Instanzen, die mit der DB2-Version erstellt wurden, entfernt werden, damit IBM DB2 erfolgreich deinstalliert werden kann. Wenn eine mit dieser DB2-Version erstellte DB2-Instanz auf Ihrem Computer verbleibt, wird DB2 bei der Deinstallation von IBM Security Directory Server nicht entfernt. In IBM Installation Manager werden Fehlermeldungen in einer Protokoll-datei gespeichert.

Sie müssen entweder IBM Installation Manager oder Betriebssystemdienstprogramme zum Installieren, Ändern oder Deinstallieren von IBM Security Directory Server und dessen Komponenten verwenden. IBM Installation Manager und Betriebssystemdienstprogramme können nicht zusammen zum Installieren, Ändern oder Deinstallieren von IBM Security Directory Server und dessen Komponenten verwendet werden.

## Deinstallation mit IBM Installation Manager

Verwenden Sie IBM Installation Manager für die Deinstallation von IBM Security Directory Server, wenn Sie IBM Security Directory Server mithilfe von IBM Installation Manager installiert haben.

### Vorbereitende Schritte

Sie müssen alle Client- und Serverprozesse von IBM Security Directory Server stoppen.

- Verzeichnisserver
- Verwaltungsserver
- LDAP-Traces
- Benutzerdefinierte LDAP-Anwendungen

Wenn irgendwelche Prozesse aktiv sind, können die Programme und Bibliotheken nicht entfernt werden.



## Vorgehensweise

1. Starten Sie IBM Installation Manager.
  - AIX und Linux:
    - a. Öffnen Sie ein Befehlszeilenfenster und wechseln Sie in das Verzeichnis, das IBM Installation Manager enthält. Das folgende Verzeichnis ist die Standardinstallationsposition von IBM Installation Manager:  
`opt/IBM/InstallationManager/eclipse`
    - b. Führen Sie den folgenden Befehl aus:  
`./IBMIM`
  - Microsoft Windows:
    - a. Klicken Sie auf **Start > Alle Programme > IBM Installation Manager > IBM Installation Manager**.
2. Klicken Sie auf **Uninstall**.
3. Wählen Sie **IBM Security Directory Server** mit der entsprechenden Version aus und klicken Sie auf **Next**.
4. Prüfen Sie im Fenster **Uninstall Packages** die für die Deinstallation ausgewählten Pakete.

**Wichtig:** Wenn Sie mit einer vorhandenen Version von DB2 oder GSKit fortfahren, aktualisiert IBM Installation Manager dessen Registry während der Installation mit dem Featureeintrag. Wenn Sie ein Feature entfernen, das mithilfe der Option **Continue with the existing** installiert wurde, werden von Installation Manager die folgenden Aktionen durchgeführt:

- Der Featureeintrag wird aus der IBM Installation Manager-Registry entfernt.
- Das Feature wird nicht vom Computer deinstalliert.

Falls DB2-Instanzen vorhanden sind, die Sie mit der mit IBM Installation Manager installierten DB2-Kopie erstellt haben, können Sie IBM Security Directory Server nicht deinstallieren. In diesem Fall müssen Sie die DB2-Instanzen manuell entfernen und den Vorgang wiederholen. Es empfiehlt sich, vor dem Entfernen der DB2-Instanzen eine Datenbanksicherung durchzuführen.

5. Klicken Sie auf **Uninstall**. Nach Abschluss der Deinstallation zeigt IBM Installation Manager an, ob die Deinstallation erfolgreich war oder nicht.
6. Optional: Wenn bei der Deinstallation ein Fehler auftritt, klicken Sie auf die Option zum Anzeigen der Protokolldatei und lesen Sie die Details. Weitere Informationen hierzu finden Sie in Kapitel 5, „IBM Installation Manager-Protokolldateien“, auf Seite 47.
7. Klicken Sie auf **Fertig stellen**.
8. Klicken Sie auf **Datei > Beenden**.

## Ergebnisse

IBM Installation Manager deinstalliert IBM Security Directory Server und die zugehörigen Komponenten.

## Unbeaufsichtigte Deinstallation mit Antwortdatei

Führen Sie die folgenden Schritte aus, um mit einer Antwortdatei eine unbeaufsichtigte Deinstallation von Komponenten von IBM Security Directory Server durchzuführen.

## Vorbereitende Schritte

Für die unbeaufsichtigte Deinstallation der Pakete von IBM Security Directory Server ist IBM Installation Manager ab Version 1.7.0 erforderlich.

## Informationen zu diesem Vorgang

Sie können die Standardantwortdatei verwenden oder eine angepasste Antwortdatei aufzeichnen und diese als Eingabedatei für die unbeaufsichtigte Deinstallation verwenden.

## Vorgehensweise

1. Melden Sie sich am System als Administrator an.
2. Greifen Sie an der Installationsposition von IBM Installation Manager auf den Befehl **IBMIM** zu.

Betriebssystem	Standardposition des Befehls <b>IBMIM</b> :
Microsoft Windows	C:\Program Files\IBM\ InstallationManager\eclipse
AIX und Linux	/opt/IBM/InstallationManager/eclipse

3. Optional: Führen Sie den Befehl **IBMIM** aus, um eine Antwortdatei für die unbeaufsichtigte Deinstallation aufzuzeichnen.
  - a. Führen Sie auf den verschiedenen Betriebssystemen die folgenden Befehle aus:

### Microsoft Windows

```
IBMIM.exe -record path_name\uninstall_responseFile.xml  
-skipInstall agentDataLocation
```

### AIX und Linux

```
./IBMIM -record path_name/uninstall_responseFile.xml  
-skipInstall agentDataLocation
```

Mit dem Befehl wird IBM Installation Manager geöffnet.

- b. Zeichnen Sie die Deinstallation von IBM Security Directory Server auf. Weitere Informationen finden Sie unter 2 auf Seite 245.
4. Führen Sie den Befehl **IBMIM** aus, um die unbeaufsichtigte Deinstallation mit der Antwortdatei als Eingabe zu starten.

Betriebssystem	Befehl:
Microsoft Windows	IBMIM.exe -silent -input path_name\uninstall_responseFile.xml -noSplash
AIX und Linux	./IBMIM -silent -input path_name/uninstall_responseFile.xml -noSplash

5. Überprüfen Sie die Deinstallationszusammenfassung und die Protokolldateien.

Betriebssystem	Standardprotokollpfad:
Microsoft Windows	C:\ProgramData\IBM\InstallationManager\ logs
AIX und Linux	/var/ibm/InstallationManager/logs/

- Überprüfen Sie, ob die Pakete von IBM Security Directory Server deinstalliert wurden.

Betriebssystem	Pakete überprüfen:
Microsoft Windows	Siehe „IBM Security Directory Server-Features unter Windows überprüfen“ auf Seite 87.
AIX und Linux	Siehe „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

## Ergebnisse

IBM Installation Manager deinstalliert Komponenten von IBM Security Directory Server unbeaufsichtigt.

## Unbeaufsichtigte Deinstallation mit dem Befehl `imcl uninstall`

Führen Sie die folgenden Schritte aus, um mit dem Befehl `imcl uninstall` eine unbeaufsichtigte Deinstallation von Komponenten von IBM Security Directory Server durchzuführen.

### Vorbereitende Schritte

Für die unbeaufsichtigte Installation der Pakete von IBM Security Directory Server ist IBM Installation Manager ab Version 1.7.0 erforderlich.

### Informationen zu diesem Vorgang

Mit dem Befehl `imcl uninstall` können Sie IBM Security Directory Server im unbeaufsichtigten Modus deinstallieren.

### Vorgehensweise

- Melden Sie sich am System als Administrator an.
- 
- Führen Sie im Verzeichnis `<IBM_Installation_Manager_install_dir>/eclipse/tools` den Befehl `imcl listInstalledPackages` aus.

Betriebssystem	Befehl
Microsoft Windows	<code>imcl.exe listInstalledPackages</code>
AIX und Linux	<code>./imcl listInstalledPackages</code>

Dieser Befehl listet alle von IBM Installation Manager installierten Pakete auf.

- Führen Sie den Befehl `imcl uninstall com.ibm.security.directoryserver.v631_6.3.1.0` aus. Verwenden Sie den Security Directory Server-Eintrag, der für die Ausgabe für den oben genannten Befehl `imcl listInstalledPackages` dient.

Betriebssystem	Befehl:
Microsoft Windows	<code>imcl.exe uninstall com.ibm.security.directoryserver.v631_6.3.1.0</code>
AIX und Linux	<code>./imcl uninstall com.ibm.security.directoryserver.v631_6.3.1.0</code>

## Ergebnisse

IBM Installation Manager deinstalliert Komponenten von IBM Security Directory Server unbeaufsichtigt.

---

## Deinstallation von IBM Security Directory Server mit Betriebssystemdienstprogrammen

Wenn Sie für die Installation von IBM Security Directory Server Betriebssystemdienstprogramme verwendet haben, müssen Sie die Betriebssystemdienstprogramme auch für die Deinstallation von IBM Security Directory Server verwenden.

Auf den Betriebssystemen AIX, Linux, Solaris und HP-UX können Sie für die Deinstallation von IBM Security Directory Server die Betriebssystemdienstprogramme verwenden. Unter Windows müssen Sie für die Installation und Deinstallation von IBM Security Directory Server IBM Installation Manager verwenden. Weitere Informationen finden Sie unter „Deinstallation mit IBM Installation Manager“ auf Seite 244.

Wenn Sie die Betriebssystemdienstprogramme für die Deinstallation von IBM Security Directory Server verwenden, wird IBM Security Directory Server vom Programm entfernt. Sie können die Features von IBM Security Directory Server während der Deinstallation mit Betriebssystemdienstprogrammen selektiv entfernen.

Stoppen Sie vor der Deinstallation von IBM Security Directory Server alle Client- und Serverprozesse von IBM Security Directory Server.

- Verzeichnisserver
- Verwaltungsserver
- LDAP-Traces
- **Webverwaltungstool** und der zugeordnete Anwendungsserver
- Benutzerdefinierte LDAP-Anwendungen

Wenn Sie eine Verzeichnisserverinstanz mit einer DB2-Datenbank erstellt und konfiguriert haben, werden diese bei einer Deinstallation von IBM Security Directory Server mithilfe der Betriebssystemdienstprogramme nicht entfernt.

## Deinstallation mit AIX-Dienstprogrammen

Für die Deinstallation von IBM Security Directory Server von AIX-Systemen können Sie die AIX-Befehlszeilendienstprogramme verwenden.

Für die Deinstallation von IBM Security Directory Server können Sie die folgenden Dienstprogramme verwenden:

**SMIT** Die Verwendung dieses Dienstprogramms ist die bevorzugte Deinstallationsmethode. Weitere Informationen hierzu finden Sie unter „Deinstallation mit SMIT“.

### **installp**

Weitere Informationen hierzu finden Sie unter „Deinstallation mit **installp**“ auf Seite 249.

## Deinstallation mit SMIT

Mit dem Befehl **smit** können Sie die Deinstallation von IBM Security Directory Server von einem AIX-System ausführen.

## Vorbereitende Schritte

Sie müssen alle Client- und Serverprozesse von IBM Security Directory Server stoppen.

- Verzeichnisserver
- Verwaltungsserver
- LDAP-Traces
- **Webverwaltungstool** und der zugeordnete Anwendungsserver
- Benutzerdefinierte LDAP-Anwendungen

## Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie den Befehl **smit** aus. Das Fenster **Softwareinstallation und -wartung** wird geöffnet.
4. Wählen Sie **Softwareinstallation und Wartung > Softwarewartung und Dienstprogramme** aus.
5. Wählen Sie **Installierte Software entfernen** aus.
6. Drücken Sie im Feld **Softwarename** die Taste **F4**, um die Liste der installierten Software aufzurufen. Sie können in dem Feld den Wert `idsldap` eingeben, um alle IBM Security Directory Server-Pakete aufzulisten.
7. Wählen Sie die zu entfernenden Pakete aus und drücken Sie dann die Eingabetaste.

## Ergebnisse

Das Dienstprogramm SMIT entfernt IBM Security Directory Server von dem AIX-System. Wenn Sie ausgewählt haben, dass alle IBM Security Directory Server-Pakete entfernt werden sollen, entfernt das Dienstprogramm auch das Installationsverzeichnis von IBM Security Directory Server (`/opt/IBM/ldap/V6.3.1`) von dem AIX-System.

## Nächste Schritte

Überprüfen Sie, ob die Deinstallation von IBM Security Directory Server erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

## Deinstallation mit `installp`

Mit dem Befehl `installp` können Sie die Deinstallation von IBM Security Directory Server von einem AIX-System ausführen.

## Vorbereitende Schritte

Sie müssen alle Client- und Serverprozesse von IBM Security Directory Server stoppen.

- Verzeichnisserver
- Verwaltungsserver
- LDAP-Traces
- **Webverwaltungstool** und der zugeordnete Anwendungsserver
- Benutzerdefinierte LDAP-Anwendungen

## Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie den folgenden Befehl aus, um die Pakete von IBM Security Directory Server zu ermitteln, die Sie entfernen wollen:

```
lslpp -l 'idsldap*'
```

4. Führen Sie den folgenden Befehl aus, um ein Paket von IBM Security Directory Server zu entfernen:

```
installp -u package_name
```

Entfernen Sie alle Pakete von IBM Security Directory Server, um IBM Security Directory Server vollständig zu entfernen. Bei der Deinstallation von IBM Security Directory Server müssen Sie die Pakete in der umgekehrten Reihenfolge wie bei der Installation angeben. Weitere Informationen zu der Reihenfolge finden Sie unter „Pakete für die Installation auf einem AIX-System“ auf Seite 72. Führen Sie den folgenden Befehl aus, um das Paket `idsldap.ent631` zu entfernen:

```
installp -u idsldap.ent631
```

## Nächste Schritte

Überprüfen Sie, ob die Deinstallation von IBM Security Directory Server erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

## Deinstallation mit Linux-Dienstprogrammen

Für die Deinstallation von IBM Security Directory Server von Linux-Systemen können Sie die Linux-Befehlszeilendienstprogramme verwenden.

Die Namen der IBM Security Directory Server-Pakete für die verschiedenen Betriebssysteme und Architekturen sind unterschiedlich. Überprüfen Sie daher vor der Deinstallation die installierten IBM Security Directory Server-Pakete.

## Deinstallation mit Linux-Dienstprogrammen

Mit dem Befehl `rpm` können Sie die Deinstallation von IBM Security Directory Server von einem Linux-System ausführen.

## Vorbereitende Schritte

Sie müssen alle Client- und Serverprozesse von IBM Security Directory Server stoppen.

- Verzeichnisserver
- Verwaltungsserver
- LDAP-Traces
- **Webverwaltungstool** und der zugeordnete Anwendungsserver
- Benutzerdefinierte LDAP-Anwendungen

## Informationen zu diesem Vorgang

Das folgende Beispiel zeigt die Deinstallation von IBM Security Directory Server-Paketen von einem AMD64 Opteron/EM64T Linux-System. Setzen Sie für System z, System i, System p oder System x Linux die entsprechenden Paketnamen ein.

## Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie den folgenden Befehl aus, um die Pakete von IBM Security Directory Server zu ermitteln, die Sie entfernen wollen:

```
rpm -qa | grep -i idsldap
```

4. Führen Sie den folgenden Befehl aus, um ein Paket von IBM Security Directory Server zu entfernen:

```
rpm -ev package_name
```

Entfernen Sie alle Pakete von IBM Security Directory Server, um IBM Security Directory Server vollständig zu entfernen. Bei der Deinstallation von IBM Security Directory Server müssen Sie die Pakete in der umgekehrten Reihenfolge wie bei der Installation angeben. Weitere Informationen zu der Reihenfolge finden Sie unter „Pakete für die Installation auf einem Linux-System“ auf Seite 77. Führen Sie den folgenden Befehl aus, um das Paket `idsldap-srv64bit631-6.3.1-0.x86_64.rpm` zu entfernen:

```
rpm -ev idsldap-srv64bit631-6.3.1-0.x86_64.rpm
```

## Nächste Schritte

Überprüfen Sie, ob die Deinstallation von IBM Security Directory Server erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

## Deinstallation mit Solaris-Dienstprogrammen

Zum Deinstallieren von IBM Security Directory Server von Solaris-Systemen können Sie die Solaris-Befehlszeilendienstprogramme verwenden.

Die IBM Security Directory Server-Paketnamen für Solaris SPARC- und Solaris X64-Systeme sind identisch.

### Deinstallation mit Solaris-Dienstprogrammen

Mit dem Befehl `pkgrm` können Sie die Deinstallation von IBM Security Directory Server von einem Solaris-System ausführen.

### Vorbereitende Schritte

Sie müssen alle Client- und Serverprozesse von IBM Security Directory Server stoppen.

- Verzeichnisserver
- Verwaltungsserver
- LDAP-Traces
- **Webverwaltungstool** und der zugeordnete Anwendungsserver
- Benutzerdefinierte LDAP-Anwendungen

## Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie den folgenden Befehl aus, um die Pakete von IBM Security Directory Server zu ermitteln, die Sie entfernen wollen:

```
pkginfo | grep -i IDS1
```

4. Führen Sie den folgenden Befehl aus, um ein Paket von IBM Security Directory Server zu entfernen:

```
pkgrm package_name
```

Entfernen Sie alle Pakete von IBM Security Directory Server, um IBM Security Directory Server vollständig zu entfernen. Bei der Deinstallation von IBM Security Directory Server müssen Sie die Pakete in der umgekehrten Reihenfolge wie bei der Installation angeben. Weitere Informationen zu der Reihenfolge finden Sie unter „Pakete für die Installation auf einem Solaris-System“ auf Seite 81. Führen Sie den folgenden Befehl aus, um das Paket `IDS1ent631` zu entfernen:

```
pkgrm IDS1ent631
```

### Nächste Schritte

Überprüfen Sie, ob die Deinstallation von IBM Security Directory Server erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

## Deinstallation mit HP-UX-Dienstprogrammen

Zum Deinstallieren von IBM Security Directory Server von HP-UX-Systemen können Sie die HP-UX-Befehlszeilendienstprogramme verwenden.

Auf HP-UX-Computern (Itanium) werden nur IBM Security Directory Server-Clientpakete unterstützt.

### Deinstallation mit HP-UX-Dienstprogrammen

Mit dem Befehl `swremove` können Sie die Deinstallation von IBM Security Directory Server von einem HP-UX-System ausführen.

### Vorbereitende Schritte

Sie müssen alle Clientprozesse von IBM Security Directory Server stoppen.

- LDAP-Traces
- Benutzerdefinierte LDAP-Anwendungen

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie den folgenden Befehl aus, um die Pakete von IBM Security Directory Server zu ermitteln, die Sie entfernen wollen:

```
swlist | grep -i idsldap
```

4. Führen Sie den folgenden Befehl aus, um ein Paket von IBM Security Directory Server zu entfernen:

```
swremove package_name
```

Entfernen Sie alle Pakete von IBM Security Directory Server, um IBM Security Directory Server vollständig zu entfernen. Bei der Deinstallation von IBM Security Directory Server müssen Sie die Pakete in der umgekehrten Reihenfolge wie bei der Installation angeben. Weitere Informationen zu der Reihenfolge finden Sie unter „Pakete für die Installation auf einem HP-UX Itanium-System“ auf Seite 84. Führen Sie den folgenden Befehl aus, um das Paket `idsldap.cltjava631.depot` zu entfernen:

```
swremove idsldap.cltjava631.depot
```



## Nächste Schritte

Überprüfen Sie, ob die Deinstallation von IBM Security Directory Server erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

---

## Deinstallation von IBM DB2 mit DB2-Befehlen

Wenn Sie die IBM DB2-Version, die mit IBM Security Directory Server bereitgestellt wurde, manuell installiert haben, verwenden Sie die DB2-Befehle, um IBM DB2 von dem Computer zu entfernen.

Wenn Sie die IBM DB2-Version mit IBM Installation Manager während der Installation von IBM Security Directory Server installiert haben, wird IBM DB2 in einer vordefinierten Position installiert. Weitere Informationen zur Standardposition finden Sie im Kapitel „Standardinstallationspositionen“ auf Seite 28. Wenn Sie die IBM DB2-Version mit IBM Installation Manager installiert haben, müssen Sie IBM Installation Manager auch für die Deinstallation von IBM DB2 verwenden.

Wenn sich auf Ihrem Computer DB2-Instanzen für die IBM DB2-Version befinden, müssen Sie die DB2-Instanzen vor der Deinstallation von IBM DB2 manuell entfernen. Es ist empfehlenswert, DB2-Datenbanken und Daten vor der Deinstallation zu sichern.

Wenn Sie IBM DB2 manuell mit DB2-Befehlen in einer benutzerdefinierten Position installiert haben, verwenden Sie die DB2-Befehle auch für die Deinstallation von IBM DB2. Führen Sie unter AIX, Linux und Solaris für die Deinstallation von IBM DB2 den Befehl **db2\_deinstall** im Verzeichnis *DB2\_installation\_location/install/* aus. Führen Sie unter Windows für die Deinstallation von IBM DB2 den Befehl **db2unins** im Verzeichnis *DB2\_installation\_location\bin* aus. Weitere Informationen zur Deinstallation von IBM DB2 finden Sie in der Produktdokumentation zu IBM DB2 unter <http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome>.

---

## Deinstallation von IBM Global Security Kit mithilfe von Betriebssystemdienstprogrammen

Wenn Sie für die Installation von IBM Global Security Kit (GSKit) Betriebssystemdienstprogramme verwendet haben, verwenden Sie die Betriebssystemdienstprogramme auch für die Deinstallation von GSKit.

Sie können Betriebssystemdienstprogramme für die Deinstallation von GSKit auf Computern mit den Betriebssystemen AIX, Linux, Solaris und HP-UX verwenden.

Unter Windows können Sie die Deinstallation von GSKit nur manuell durchführen, wenn Sie während der Installation mit IBM Installation Manager ausgewählt haben, dass eine installierte GSKit-Version verwendet werden soll. Wenn IBM Security Directory Server auf Ihrem Computer installiert ist, darf GSKit nicht entfernt werden, während es verwendet wird. Wenn Sie die neueste GSKit-Version verwenden, muss IBM Installation Manager verwendet werden, um das GSKit-Feature zu ändern, damit es aus der Registry entfernt werden kann. Danach kann die Deinstallation von GSKit durchgeführt werden.

## IBM Global Security Kit mit SMIT deinstallieren

Mit dem Befehl **smit** können Sie die Deinstallation von IBM Global Security Kit (GSKit) von einem AIX-System ausführen.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie den Befehl **smit** aus. Das Fenster **Softwareinstallation und -wartung** wird geöffnet.
4. Wählen Sie **Softwareinstallation und Wartung > Softwarewartung und Dienstprogramme** aus.
5. Wählen Sie **Installierte Software entfernen** aus.
6. Drücken Sie im Feld **Softwarename** die Taste **F4**, um die Liste der installierten Software aufzurufen. Sie können in dem Feld den Wert **GSKit** eingeben, um alle GSKit-Pakete aufzulisten.
7. Setzen Sie den Wert für **Abhängige Software entfernen?** auf Ja, um die Softwareprodukte und Aktualisierungen zu entfernen, die von dem Produkt abhängig sind, das Sie entfernen wollen.
8. Wählen Sie die zu entfernenden Pakete aus und drücken Sie dann die Eingabetaste.
9. Überprüfen Sie, ob die Deinstallation von GSKit erfolgreich war.

```
lslpp -l 'GSK*'
```

## IBM Global Security Kit mit installp deinstallieren

Mit dem Befehl **installp** können Sie die Deinstallation von IBM Global Security Kit (GSKit) von einem AIX-System ausführen.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie den folgenden Befehl aus, um die GSKit-Pakete zu ermitteln, die Sie entfernen wollen:

```
lslpp -l 'GSK*'
```

4. Führen Sie den folgenden Befehl aus, um ein GSKit-Paket zu entfernen:

```
installp -u package_name
```

Entfernen Sie alle GSKit-Pakete derselben Version, um GSKit vollständig zu entfernen. Zur Deinstallation von GSKit müssen Sie zuerst das GSKit SSL-Paket und danach das GSKit Crypt-Paket entfernen. Führen Sie den folgenden Befehl aus, um die Pakete **GSKit8.gskssl64.ppc.rte** und **GSKit8.gskcrypt64.ppc.rte** zu entfernen:

```
installp -u GSKit8.gskssl64.ppc.rte  
installp -u GSKit8.gskcrypt64.ppc.rte
```

5. Überprüfen Sie, ob die Deinstallation von GSKit erfolgreich war.

```
lslpp -l 'GSK*'
```

## IBM Global Security Kit mit Linux-Dienstprogrammen deinstallieren

Mit dem Befehl **rpm** können Sie die Deinstallation von IBM Global Security Kit (GSKit) von einem Linux-System ausführen.

## Informationen zu diesem Vorgang

Das folgende Beispiel zeigt die Deinstallation von GSKit-Paketen von einem AMD64 Opteron/EM64T Linux-System. Setzen Sie für System z, System i, System p oder System x Linux die entsprechenden Paketnamen ein.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie den folgenden Befehl aus, um die GSKit-Pakete zu ermitteln, die Sie entfernen wollen:

```
rpm -qa | grep -i gsk
```

4. Führen Sie den folgenden Befehl aus, um ein GSKit-Paket zu entfernen:

```
rpm -ev package_name
```

Entfernen Sie alle GSKit-Pakete derselben Version, um GSKit vollständig zu entfernen. Zur Deinstallation von GSKit müssen Sie zuerst das GSKit SSL-Paket und danach das GSKit Crypt-Paket entfernen. Führen Sie den folgenden Befehl aus, um die Pakete `gskssl64-8.0-14.26.x86_64` und `gskcrypt64-8.0-14.26.x86_64` zu entfernen:

```
rpm -ev gskssl64-8.0-14.26.x86_64  
rpm -ev gskcrypt64-8.0-14.26.x86_64
```

5. Überprüfen Sie, ob die Deinstallation von GSKit erfolgreich war.

```
rpm -qa | grep -i gsk
```

## IBM Global Security Kit mit Solaris-Dienstprogrammen deinstallieren

Mit dem Befehl `pkgrm` können Sie die Deinstallation von IBM Global Security Kit (GSKit) von einem Solaris-System ausführen.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie den folgenden Befehl aus, um die GSKit-Pakete zu ermitteln, die Sie entfernen wollen:

```
pkginfo | grep -i gsk
```

4. Führen Sie den folgenden Befehl aus, um ein GSKit-Paket zu entfernen:

```
pkgrm package_name
```

Entfernen Sie alle GSKit-Pakete derselben Version, um GSKit vollständig zu entfernen. Zur Deinstallation von GSKit müssen Sie zuerst das GSKit SSL-Paket und danach das GSKit Crypt-Paket entfernen. Führen Sie den folgenden Befehl aus, um die Pakete `gsk8ssl64` und `gsk8cry64` zu entfernen:

```
pkgrm gsk8ssl64  
pkgrm gsk8cry64
```

5. Überprüfen Sie, ob die Deinstallation von GSKit erfolgreich war.

```
pkginfo | grep -i gsk
```

## IBM Global Security Kit mit HP-UX-Dienstprogrammen deinstallieren

Mit dem Befehl **swremove** können Sie die Deinstallation von IBM Global Security Kit (GSKit) von einem HP-UX-System ausführen.

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie den folgenden Befehl aus, um die GSKit-Pakete zu ermitteln, die Sie entfernen wollen:

```
swlist | grep -i gsk
```

4. Führen Sie den folgenden Befehl aus, um ein GSKit-Paket zu entfernen:

```
swremove package_name
```

Entfernen Sie alle GSKit-Pakete derselben Version, um GSKit vollständig zu entfernen. Zur Deinstallation von GSKit müssen Sie zuerst das GSKit SSL-Paket und danach das GSKit Crypt-Paket entfernen. Führen Sie den folgenden Befehl aus, um die Pakete `gkssl64` und `gskcrypt64` zu entfernen:

```
swremove gkssl64  
swremove gskcrypt64
```

5. Überprüfen Sie, ob die Deinstallation von GSKit erfolgreich war.

```
swlist | grep -i gsk
```

## IBM Global Security Kit unter Windows deinstallieren

Verwenden Sie die Befehle von IBM Global Security Kit (GSKit), um GSKit von einem Windows-System zu deinstallieren.

### Informationen zu diesem Vorgang

Im Beispiel wird die unbeaufsichtigte Deinstallation der Pakete von 64-Bit-GSKit SSL und 64-Bit-GSKit Crypt von einem Windows-System in einer AMD64/EM64T-Architektur gezeigt. Für ein Windows-Betriebssystem in einer IA32/x86-Architektur werden andere Namen verwendet. Informationen zu den Namen der GSKit-Pakete finden Sie in Kapitel 10, „Installation von IBM Global Security Kit“, auf Seite 59.

**Anmerkung:** Sie können auch auf **Start > Systemsteuerung > Programme hinzufügen oder entfernen** klicken, um die GSKit-Pakete zu entfernen.

### Vorgehensweise

1. Melden Sie sich als Mitglied der Administratorgruppe an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ändern Sie das aktuelle Arbeitsverzeichnis in das Verzeichnis `gskit`, in dem die Installationsdatei von IBM Global Security Kit gespeichert ist.
4. Führen Sie die folgenden Befehle aus, um die Pakete von 64-Bit-GSKit unbeaufsichtigt zu entfernen: Entfernen Sie alle GSKit-Pakete derselben Version, um GSKit vollständig zu entfernen. Zur Deinstallation von GSKit müssen Sie zuerst das GSKit SSL-Paket und danach das GSKit Crypt-Paket entfernen.

```
gsk8ssl64.exe /s /x /v"/quiet"  
gsk8crypt64.exe /s /x /v"/quiet"
```

## Deinstallation von Sprachenpaketen

Um die Deinstallation von IBM Security Directory Server durchzuführen, müssen Sie die auf Ihrem Computer installierten Sprachenpakete deinstallieren.

Wenn Sie IBM Security Directory Server und Sprachenpakete auf Ihrem Computer mit IBM Installation Manager installiert haben, müssen Sie IBM Installation Manager auch für die Deinstallation der Sprachenpakete verwenden.

Wenn Sie die Dienstprogramme des Betriebssystems für die Installation der Sprachpakete verwendet haben, müssen Sie die Dienstprogramme des Betriebssystems auch für die Deinstallation der Sprachenpakete verwenden.

Alle Sprachenpakete werden vom System deinstalliert, außer Sie wählen die Features Proxy Server oder Server für die Installation aus.

## Sprachenpakete mit Betriebssystemdienstprogrammen deinstallieren

Verwenden Sie für die Deinstallation eines Sprachenpaketes die Betriebssystemdienstprogramme, wenn Sie dieses Sprachenpaket mit den Betriebssystemdienstprogrammen installiert haben.

### Vorbereitende Schritte

Stoppen Sie vor der Deinstallation von Sprachenpaketen von IBM Security Directory Server alle Client- und Serverprozesse von IBM Security Directory Server.

- Verzeichnisserver
- Verwaltungsserver
- LDAP-Traces
- Benutzerdefinierte LDAP-Anwendungen

### Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Öffnen Sie die Eingabeaufforderung.
3. Ermitteln Sie die Sprachenpakete auf Ihrem Computer, die entfernt werden sollen:

Betriebssystem	Befehl:
AIX	<code>ls1pp -l 'idsldap.msg631*'</code>
Linux	<code>rpm -qa   grep -i idsldap-msg631</code>
Solaris	<code>pkginfo   grep IDS1</code>

4. Führen Sie zum Deinstallieren des Sprachenpakets für eine Sprache die Befehle zur Paketdeinstallation aus. Im folgenden Beispiel wird die Deinstallation des Sprachenpakets für Französisch angezeigt. Sie können jede andere Sprache deinstallieren, indem Sie die Namen durch die passenden Paketnamen für das Betriebssystem ersetzen.

Betriebssystem	Befehl:
AIX	<code>installp -u idsldap.msg631.fr_FR</code>
Linux	<code>rpm -ev idsldap-msg631-fr-6.3.1-0.noarch.rpm</code>

<b>Betriebssystem</b>	<b>Befehl:</b>
Solaris	pkgm IDS1fr631

5. Überprüfen Sie, ob die Installation des Sprachenpakets erfolgreich war. Weitere Informationen hierzu finden Sie unter „IBM Security Directory Server-Pakete überprüfen“ auf Seite 89.

---

## Anhang A. Directory Services Markup Language

Sie können Directory Services Markup Language verwenden, um die Verzeichnisstrukturinformationen, Verzeichnisabfragen und -aktualisierungen und Ergebnisse von Verzeichnisoperationen im XML-Format darzustellen.

Wenn Sie die Installation des **Webverwaltungstools** von IBM Security Directory Server abschließen, wird eine Archivdatei von DSML-Dateien (Directory Services Markup Language) mit dem Namen `DSML.zip` auf Ihrem Computer gespeichert. Die Datei `DSML.zip` wird im Unterverzeichnis `idstools` in der Installationsposition von IBM Security Directory Server gespeichert. Weitere Informationen zur Standardinstallationsposition von IBM Security Directory Server finden Sie im Kapitel „Standardinstallationspositionen“ auf Seite 28.

Die Datei `DSML.zip` enthält DSML-Installationsdateien und -Dokumentationen, die Sie durch die Installation, Konfiguration und Verwendung von DSML führen. Die Datei `DSML.zip` enthält die folgenden Dateien:

### **DSMLReadme.txt**

In der Datei `DSMLReadme.txt` sind die im Paket enthaltenen Dateien und Anweisungen für die Installation und Konfiguration von DSML aufgeführt.

### **dsm1.pdf**

Die Datei `dsm1.pdf` ist eine PDF-Datei, in der die Verwendung von DSML beschrieben wird.

### **dsm1.htm**

Die Datei `dsm1.htm` ist eine HTML-Datei, in der die Verwendung von DSML beschrieben wird.





---

## Anhang B. Beispieldatenbank laden und Server starten

Laden Sie die Beispieldatenbank und starten Sie den Verzeichnissever, um Einträge hinzuzufügen, zu aktualisieren und zu suchen.

### Vorbereitende Schritte

Erstellen Sie eine Verzeichnisseverinstanz. Weitere Informationen finden Sie unter „Erstellung von Verzeichnisseverinstanzen“ auf Seite 140.

### Informationen zu diesem Vorgang

Mit dem **Konfigurationstool** können Sie LDIF-Daten in einen Verzeichnissever laden und den Server starten.

### Vorgehensweise

1. Führen Sie den folgenden Befehl aus, um das **Konfigurationstool** zu starten:  
`idsxcfg -I instance_name`
2. Klicken Sie im Navigationsbereich auf der linken Seite auf **LDAP-Tasks > LDIF-Daten importieren**.
3. Geben Sie im Feld **Pfad und Name der LDIF-Datei** den Namen der LDIF-Datei mit dem Pfad ein. Sie können auch auf "Durchsuchen" klicken und die LDIF-Datei angeben. Nachstehend sind der Standardpfad und der Standardname der LDIF-Datei auf verschiedenen Betriebssystemen aufgeführt:

#### Windows

`installation_path\examples\sample.ldif`

#### AIX und Solaris

`/opt/IBM/ldap/V6.3.1/examples/sample.ldif`

**Linux** `/opt/ibm/ldap/V6.3.1/examples/sample.ldif`

4. Klicken Sie auf **Standardimport**.
5. Klicken Sie auf **Importieren**.
6. Führen Sie die folgenden Aktionen aus, um die Verzeichnisseverinstanz zu starten:
  - a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Serverstatus verwalten**.
  - b. Klicken Sie auf **Server starten**.



---

## Anhang C. Datei `ldapdb.properties` manuell aktualisieren

Wenn Sie IBM Security Directory Server auf einem Computer installieren, der keine unterstützte Version von IBM DB2 enthält, wird die Datei `ldapdb.properties` bei der Installation nicht gefüllt. In diesem Fall müssen Sie eine unterstützte Version von IBM DB2 installieren und die Datei `ldapdb.properties` anschließend manuell aktualisieren.

### Vorbereitende Schritte

Sie müssen sicherstellen, dass das vollständige Verzeichnisserverpaket installiert ist.

### Vorgehensweise

1. Installieren Sie eine unterstützte Version von IBM DB2, sofern noch nicht installiert.
2. Führen Sie den Befehl `db21s` aus, um die auf dem Computer installierten DB2-Versionen und deren Installationspfad aufzuführen.
3. Aktualisieren Sie die Datei `ldapdb.properties` mit der unterstützten DB2-Version und dem Installationspfad. Standardposition der Datei `ldapdb.properties` mit Beispielwerten für die verschiedenen Betriebssysteme:

#### Microsoft Windows

```
C:\Program Files\IBM\ldap\V6.3.1\etc\ldapdb.properties
currentDB2InstallPath=C:\Program Files\IBM\SQLLIB
currentDB2Version=9.7.0.6
```

#### AIX und Solaris

```
/opt/IBM/ldap/V6.3.1/etc/ldapdb.properties
currentDB2InstallPath=/opt/IBM/db2/V9.7
currentDB2Version=9.7.0.6
```

#### Linux

```
/opt/ibm/ldap/V6.3.1/etc/ldapdb.properties
currentDB2InstallPath=/opt/ibm/db2/V9.7
currentDB2Version=9.7.0.6
```

4. Speichern Sie die Datei `ldapdb.properties`.



---

## Anhang D. Eingabehilfefunktionen für Security Directory Server

Die Eingabehilfefunktionen unterstützen Benutzer mit körperlichen Behinderungen wie z. B. eingeschränkter Beweglichkeit oder eingeschränktem Sehvermögen beim erfolgreichen Einsatz von IT-Produkten.

Im Wesentlichen können Benutzer dieses Produkts auf die Eingabehilfen für folgende Aktionen zurückgreifen:

- Hilfstechnologien wie Sprachausgabesoftware bringen zu Gehör, was auf dem Bildschirm angezeigt wird. Weitere Informationen zur Verwendung der Technologien für behindertengerechte Bedienung in diesem Produkt finden Sie in der Produktdokumentation der betreffenden Hilfstechnologie.
- Ausführen bestimmter oder äquivalenter Funktionen ausschließlich über die Tastatur.
- Vergrößern der Bildschirmanzeige.

Zudem wurde die Produktdokumentation optimiert, um den behindertengerechten Zugang zu erleichtern:

- Die gesamte Dokumentation ist im HTML-Format verfügbar, damit Benutzer im Bedarfsfall auf Sprachausgabesoftware zurückgreifen können.
- Sämtliche Abbildungen in der Dokumentation sind mit erläuternden Texten versehen, die Benutzern mit Sehbehinderung den Inhalt der Bilder verdeutlichen.

### Eingabehilfen

Die folgende Liste umfasst die wichtigsten Eingabehilfen von IBM Security Directory Server.

- Unterstützung ausschließlich über die Tastatur ausgeführter Operationen.
- Unterstützung von Schnittstellen, die von Sprachausgabeprogrammen häufig verwendet werden.
- Mit einer Tasterkennung ausgestattete Tasten, die nicht durch einfaches Berühren aktiviert werden.

Die Dokumentation zu IBM Security Directory Server ist für die behindertengerechte Bedienung aktiviert. Die Eingabehilfen der Dokumentation werden im Onlinedokumentationsset beschrieben.

### Navigation über die Tastatur

Standardtastenkürzel und Direktaufruftasten werden vom Produkt unterstützt und sind im Betriebssystem dokumentiert. Weitere Informationen finden Sie in der Dokumentation Ihres Betriebssystems.

Dieses Produkt arbeitet mit den Standardnavigationstasten von Microsoft Windows.

## **Vergrößern der Bildschirmanzeige.**

Sie können die Informationen in den Programmfenstern mit den Funktionen des Betriebssystems vergrößern, unter dem das Programm ausgeführt wird. Unter Microsoft Windows können Sie z. B. die Bildschirmauflösung verringern, um die Schrift zu vergrößern. Weitere Informationen finden Sie in der Dokumentation Ihres Betriebssystems.

## **IBM und Eingabehilfen**

Im IBM Human Ability and Accessibility Center finden Sie weitere Informationen zu den Initiativen und Aktivitäten von IBM in Bezug auf die Verwendung von Eingabehilfen: <http://www.ibm.com/able>

---

# Index

## A

- Active Directory
  - Synchronisation starten 226
- Active Directory-Synchronisation
  - Konfiguration 226
- Active Directory-Synchronisationslösung, Migration
  - Konfiguration 105
- AIX
  - Installation mit SMIT 74
- AIX, automatisches Starten des Verzeichnisseservers
  - allgemeine Informationen 231
  - Konfiguration 233
- AIX, Deinstallation mit "installp"
  - GSKit 254
  - Verzeichnissever 249
- AIX, erforderlicher Plattenspeicherplatz
  - Verzeichnissever, Komponenten 3
- AIX, GSKit
  - Deinstallation mit SMIT 254
- AIX, Installation mit "installp"
  - IBM Global Security Kit 60
  - Verzeichnissever 75
- AIX, Verzeichnissever
  - Deinstallation mit SMIT 249
- AIX-Dienstprogramme, Deinstallation
  - Sprachenpakete 257
- AIX-Dienstprogramme, Installation
  - Sprachenpakete 69
- Anwendungsserver stoppen, Webanwendungsserver
  - Konfiguration 121
- ASCII-Zeichen
  - 33 bis 126 134
  - unterstützte Seedzeichenfolge für die Verschlüsselung 134
- Automatisches Starten, Verzeichnissever
  - allgemeine Informationen 231
- Automatisches Starten des Verzeichnisseservers, AIX
  - Konfiguration 233
- Automatisches Starten des Verzeichnisseservers, Linux
  - Konfiguration 233
- Automatisches Starten des Verzeichnisseservers, Solaris
  - Konfiguration 233
- Automatisches Starten des Verzeichnisseservers, Windows
  - Konfiguration 231

## B

- Befehl, Migration
  - Webverwaltungstool, idswmigr 107
- Benutzer und Gruppe, idslsap
  - allgemeine Informationen 17
  - Voraussetzungen 17

- Benutzer und Gruppen, Datenbankeigner
  - allgemeine Informationen 125
- Benutzer und Gruppen, Datenbankinstanzeigner
  - allgemeine Informationen 125
- Benutzer und Gruppen, Verzeichnissever
  - allgemeine Informationen 125
- Benutzer und Gruppen, Verzeichnisseverinstanzeigner
  - allgemeine Informationen 125
- Betriebssystem, Sprachenpaket
  - Paketnamen 68
- Betriebssystemdienstprogramme, Deinstallation des Verzeichnisseservers
  - allgemeine Informationen 248
- Betriebssystemdienstprogramme, Deinstallation von GSKit
  - allgemeine Informationen 253
- Betriebssystemdienstprogramme, Installation des Verzeichnisseservers
  - allgemeine Informationen 71
- Betriebssysteme, Aktualisierung
  - vorausgesetzte Pakete 15

## C

- Clientdienstprogramme, DB2-Datenbank-administrator
  - Kennwort, Konfiguration 192
- Clientdienstprogramme, LDIF-Datenmanagement
  - allgemeine Informationen 220
- Clientdienstprogramme, Links
  - allgemeine Informationen 100
- Codepage, DB2
  - Zeichensatz, IANA 132
- Codepage, Unterschiede
  - UTF-8, Ländereinstellung 130

## D

- Daten und Lösungen, Migration
  - allgemeine Informationen 101
- Datenbank, Konfigurationsplanung
  - allgemeine Informationen 129
  - Codepage 129
  - hierarchische Struktur 129
  - Zugriffsberechtigungen 129
- DB2, Datenmigration
  - allgemeine Informationen 101
  - Konfiguration 102
- DB2, Verzeichnissever
  - allgemeine Informationen 55
- DB2-Codepage
  - Ländereinstellung, IANA 132
- DB2-Datenbank, Konfiguration
  - Instance Administration Tool 143
- DB2-Datenbank, Konfigurationstool
  - Dekonfiguration 193
  - Kennwort, Konfiguration 191
- DB2-Datenbank, Konfigurationstool (*Forts.*)
  - Konfiguration 184
- DB2-Datenbank, Onlinesicherung
  - Instance Administration Tool 143
- DB2-Datenbank, Serverdienstprogramme
  - Konfiguration 188
- DB2-Deinstallation, DB2-Befehle
  - allgemeine Informationen 253
- DB2-Eigenschaftendatei, Verzeichnissever
  - Konfiguration 263
- Deimplementierung, Webverwaltungstool
  - Konfiguration 123
- Deinstallation, AIX-Dienstprogramme
  - allgemeine Informationen 248
- Deinstallation, Befehl "GSKit"
  - GSKit 256
- Deinstallation, Befehl "installp"
  - GSKit 254
  - Verzeichnissever 249
- Deinstallation, Befehl "pkgrm"
  - GSKit 255
  - Verzeichnissever 251
- Deinstallation, Befehl "rpm"
  - GSKit 255
  - Verzeichnissever 250
- Deinstallation, Befehl "swremove"
  - GSKit 256
  - Verzeichnissever 252
- Deinstallation, DB2
  - allgemeine Informationen 253
- Deinstallation, Dienstprogramm SMIT
  - GSKit 254
  - Verzeichnissever 249
- Deinstallation, HP-UX-Dienstprogramme
  - allgemeine Informationen 252
- Deinstallation, IBM Installation Manager
  - IBM Security Directory Server 244
- Deinstallation, Linux-Dienstprogramme
  - allgemeine Informationen 250
- Deinstallation, Solaris-Dienstprogramme
  - allgemeine Informationen 251
- Deinstallation, Sprachenpakete
  - AIX-Dienstprogramme 257
  - allgemeine Informationen 257
  - Linux-Dienstprogramme 257
  - Solaris-Dienstprogramme 257
- Deinstallation, Verzeichnissever
  - allgemeine Informationen 243
- Deinstallation mit Betriebssystemdienstprogrammen, Verzeichnissever
  - allgemeine Informationen 248
- Deinstallation mithilfe von Betriebssystemdienstprogrammen, GSKit
  - allgemeine Informationen 253
- Directory Services Markup Language
  - allgemeine Informationen 259

## E

- Eingabehilfen ix, 265
- erforderlicher Plattenspeicherplatz
  - Verzeichnisservers, Komponenten 3

## F

- Features, Änderung
  - IBM Security Directory Server-Features 41
- Features, Deinstallation
  - IBM Security Directory Server 244
- Features, Überprüfung
  - IBM Security Directory Server 87
- Fehlerbehebung ix
- Fehlerbestimmung ix
- Fernes Upgrade, Instance Administration Tool
  - Instanz mit Sicherungsdaten 139
- Fernverwaltung, Instanz
  - Webverwaltungstool, Konfiguration 120
- Fixpacks 237

## G

- GSKit, Installationsprüfung
  - UNIX 90
- GSKit, Überprüfung
  - Windows 90
- GSKit-Deinstallation, Betriebssystemdienstprogramme
  - allgemeine Informationen 253

## H

- Hauptadministrator, Verwaltung
  - allgemeine Informationen 180
- Hauptadministratorkennwort, Verwaltung
  - allgemeine Informationen 182
- HP-UX, Deinstallation mit "swremove"
  - GSKit 256
  - Verzeichnisservers 252
- HP-UX, erforderlicher Plattenspeicherplatz
  - Verzeichnisservers, Komponenten 3
- HP-UX, Installation mit "swinstall"
  - IBM Global Security Kit 63
  - Verzeichnisservers 85
- HTTPS, integrierte Version von WebSphere Application Server
  - allgemeine Informationen 122

## I

- IBM
  - Softwareunterstützung ix
  - Support Assistant ix
- IBM Installation Manager, Änderungen am Verzeichnisservers
  - allgemeine Informationen 41
- IBM Installation Manager, Deinstallation des Verzeichnisservers
  - allgemeine Informationen 244

- IBM Installation Manager, Installation des Verzeichnisservers
  - unterstütztes Betriebssystem, allgemeine Informationen 22
- IBM Installation Manager, Installation starten
  - Verzeichnisservers 32
- IBM Installation Manager, Protokolle
  - allgemeine Informationen 47
  - Positionen 47
- IBM JDK, Verzeichnisservers
  - allgemeine Informationen 57
- IBM Security Directory Server
  - Installationsszenarios 27
- IBM Security Directory Server, Änderung
  - Features 41
- IBM Security Directory Server, Deinstallation
  - Features 244
- IBM Security Directory Server, IBM Installation Manager
  - Installation starten, Konfiguration 29
  - Installation starten, Methoden 29
- IBM Security Directory Server, Installation
  - allgemeine Informationen 23
  - vorausgesetzte Pakete 15
- IBM Security Directory Server, Installationsmedien
  - allgemeine Informationen 6
- IBM Security Directory Server, Installationspakete
  - Typen, allgemeine Informationen 22
- IBM Security Directory Server, Installationsrepositorys
  - allgemeine Informationen 29
- IBM Security Directory Server, Installationsszenarios
  - allgemeine Informationen 27
- IBM Security Directory Server, Komponenten
  - allgemeine Informationen 24
- IBM Security Directory Server, Passport Advantage
  - Produkt herunterladen 7
- IBM Security Directory Server, Überprüfung
  - Features 87
  - zusätzlich erforderliches Produkt, DB2 87
  - zusätzlich erforderliches Produkt, GSKit 87
  - zusätzlich erforderliches Produkt, integrierte Version von WebSphere Application Server 87
- Implementierung
  - Webverwaltungstool 116
- Implementierung, Webverwaltungstool
  - allgemeine Informationen 113
  - WebSphere Application Server 117
- Installation
  - Befehl pkgadd 83
  - HP-UX-Dienstprogramme 84
  - manuell
    - HP-UX 84
  - Verzeichnisserverspakete unter Solaris 81

- Installation, AIX-Dienstprogramme
  - allgemeine Informationen 71
- Installation, Befehl "install"
  - IBM Global Security Kit 60
  - Verzeichnisservers 75
- Installation, Befehl "pkgadd"
  - IBM Global Security Kit 62
- Installation, Befehl "rpm"
  - IBM Global Security Kit 61
  - Verzeichnisservers 79
- Installation, Befehl "swinstall"
  - IBM Global Security Kit 63
- Installation, DB2
  - allgemeine Informationen 55
- Installation, Dienstprogramm SMIT
  - Verzeichnisservers 74
- Installation, GSKit
  - allgemeine Informationen 59
  - Paketnamen 59
- Installation, IBM Global Security Kit
  - Windows 64
- Installation, IBM Installation Manager
  - allgemeine Informationen 21
  - Übersicht 21
- Installation, IBM JDK
  - allgemeine Informationen 57
- Installation, Linux-Dienstprogramme
  - allgemeine Informationen 77
- Installation, manuell
  - integrierte Version von WebSphere Application Server 113
- Installation, Planung
  - allgemeine Informationen 1
- Installation, Position
  - Verzeichnisstruktur 175
- Installation, Repository-Konfiguration
  - Verzeichnisservers 31
- Installation, Solaris-Dienstprogramme
  - Verzeichnisservers 81
- Installation, Sprachenpakete
  - AIX-Dienstprogramme 69
  - allgemeine Informationen 67
  - Linux-Dienstprogramme 69
  - Solaris-Dienstprogramme 69
- Installation, Tool
  - IBM Installation Manager 21
- Installation, Übersicht
  - IBM Installation Manager 21
- Installation, Umgebungsvoraussetzungen
  - allgemeine Informationen 1
- Installation, Verzeichnisservers
  - Betriebssystemdienstprogramme 71
  - IBM Installation Manager 32
  - Launchpad, Konfiguration 29
  - Repository 31
  - swinstall, Befehl 85
- Installation, Verzeichnisserverspakete unter AIX
  - allgemeine Informationen 72
- Installation, Verzeichnisserverspakete unter Linux
  - allgemeine Informationen 77
- Installation, Windows
  - IBM Global Security Kit 64
- Installation mit installp
  - IBM Global Security Kit 60
  - Verzeichnisservers 75



- Installation mit swinstall
  - IBM Global Security Kit 63
- Installationskomponenten, IBM Security Directory Server
  - allgemeine Informationen 24
- Installationsmedien, IBM Security Directory Server
  - allgemeine Informationen 6
- Installationsmethoden
  - allgemeine Informationen 19
- Installationspakete, Typen
  - allgemeine Informationen 22
- Installationspositionen
  - Standard, allgemeine Informationen 28
- Installationsprüfung, GSKit
  - UNIX 90
- Installationsrepositorys
  - allgemeine Informationen 29
- Installationsszenarios, IBM Security Directory Server
  - allgemeine Informationen 27
- Installationsübersicht, Verzeichnisserver
  - allgemeine Informationen 3
- Installationsvoraussetzungen
  - allgemeine Informationen 15
- Installationsvoraussetzungen, IBM Security Directory Server
  - allgemeine Informationen 23
- installp, Deinstallation
  - GSKit 254
  - Verzeichnisserver 249
- Instance Administration Server, Instanzerstellung
  - angepasste Einstellungen 143
  - Standardinstanz 141
- Instance Administration Server, Proxy-Server-Instanz erstellen
  - angepasste Einstellungen 150
- Instance Administration Tool
  - Upgradeinstanz 156
- Instance Administration Tool, fernes Upgrade
  - Instanz mit Sicherungsdaten 139
- Instance Administration Tool, Instanz kopieren
  - Konfiguration 162
- Instance Administration Tool, Instanz löschen
  - allgemeine Informationen 171
  - Konfiguration 172
- Instance Administration Tool, Instanz starten oder stoppen
  - allgemeine Informationen 165
- Instance Administration Tool, Instanzdetails anzeigen
  - allgemeine Informationen 170
  - Konfiguration 170
- Instance Administration Tool, Konfiguration
  - Instanz kopieren 162
  - Server starten oder stoppen 165
  - Verwaltungsserver starten oder stoppen 165
- Instance Administration Tool, öffnen
  - Konfiguration 138
  - Konfigurationstool 167

- Instance Administration Tool, starten
  - Konfiguration 138
- Instance Administration Tool, TCP/IP-Einstellungen ändern
  - Instanz 168
  - Konfiguration 168
- Instance Administration Tool, Upgrade
  - ferne Instanz 157
- Instance Administration Tool, Verwaltungsserver starten oder stoppen
  - Konfiguration 165
- Instance Administration Tool, Verzeichnisserver starten oder stoppen
  - Konfiguration 165
- Instanz, Benutzer und Gruppen
  - Berechtigungen, allgemeine Informationen 127
  - Erstellung, allgemeine Informationen 127
- Instanz, Erstellung
  - allgemeine Informationen 140
- Instanz, Upgrade
  - Umgebung, einrichten 94
- Instanz, Webverwaltungstool
  - Fernverwaltung, Konfiguration 120
- Instanzerstellung, Methoden
  - allgemeine Informationen 137
- Instanzerstellung, Optionen
  - Instance Administration Tool 140
- Instanzerstellung, Systemkonfiguration
  - allgemeine Informationen 125
- Integrierte Version von WebSphere Application Server
  - Installation 113
- Integrierte Version von WebSphere Application Server, HTTPS
  - allgemeine Informationen 122

## K

- Konfiguration, Planungsdatenbank
  - allgemeine Informationen 129
- Konfigurationstool
  - allgemeine Informationen 167, 177
- Konfigurationstool, Active Directory-Synchronisation
  - Konfiguration 227
- Konfigurationstool, Administrator-DN verwalten
  - Konfiguration 180
- Konfigurationstool, Administratorkennwort verwalten
  - Konfiguration 182
- Konfigurationstool, Änderungsprotokoll
  - allgemeine Informationen 209
  - Konfiguration 209
- Konfigurationstool, Änderungsprotokoll inaktivieren
  - Konfiguration 211
- Konfigurationstool, Backup
  - allgemeine Informationen 198
- Konfigurationstool, Datenbank sichern
  - Konfiguration 199
- Konfigurationstool, Datenbank wiederherstellen
  - Konfiguration 202

- Konfigurationstool, Datenbankadministratorkennwort
  - allgemeine Informationen 190
- Konfigurationstool, Datenbankkonfiguration
  - allgemeine Informationen 183
- Konfigurationstool, Datenbankoptimierung
  - allgemeine Informationen 195
- Konfigurationstool, Datenbankpflege
  - allgemeine Informationen 196
- Konfigurationstool, DB2-Datenbank Dekonfiguration
  - 193
  - Konfiguration 184
- Konfigurationstool, DB2-Datenbankadministrator
  - Kennwort, Konfiguration 191
- Konfigurationstool, Dekonfiguration der Datenbank
  - allgemeine Informationen 193
- Konfigurationstool, Instanz starten oder stoppen
  - allgemeine Informationen 178
- Konfigurationstool, Konfiguration
  - Server starten oder stoppen 179
  - Verwaltungsserver starten oder stoppen 179
- Konfigurationstool, LDIF-Daten exportieren
  - Konfiguration 223
- Konfigurationstool, LDIF-Daten importieren
  - Konfiguration 221
- Konfigurationstool, LDIF-Daten prüfen
  - Konfiguration 222
- Konfigurationstool, LDIF-Datenmanagement
  - allgemeine Informationen 220
- Konfigurationstool, Leistungsoptimierung
  - Verzeichnisserver 205, 208
- Konfigurationstool, öffnen
  - Konfiguration 178
- Konfigurationstool, Proxy-Server sichern
  - Konfiguration 200
- Konfigurationstool, Proxy-Server wiederherstellen
  - Konfiguration 203
- Konfigurationstool, Schemaverwaltung
  - allgemeine Informationen 216
- Konfigurationstool, Serverkonfiguration
  - allgemeine Informationen 167
- Konfigurationstool, starten
  - Konfiguration 178
- Konfigurationstool, Suffix
  - allgemeine Informationen 213
- Konfigurationstool, verwalten
  - Administrator-DN, Konfiguration 180
  - Administratorkennwort, Konfiguration 182
- Konfigurationstool, Verwaltungsserver starten oder stoppen
  - Konfiguration 179
- Konfigurationstool, Verzeichnisserver
  - Datenbank optimieren, Konfiguration 195

- Konfigurationstool, Verzeichnisserver (Forts.)
  - Datenbank pflegen, Konfiguration 197
  - Schema verwalten, Konfiguration 217
  - Schemavalidierungsregel, Konfiguration 219
  - Suffix entfernen, Konfiguration 215
  - Suffix hinzufügen, Konfiguration 214
- Konfigurationstool, Verzeichnisserver starten oder stoppen Konfiguration 179
- Konfigurationstool, Wiederherstellung allgemeine Informationen 201
- Kurse ix

## L

- Landessprache, Zeichen UTF-8 130
- Launchpad, Installation Verzeichnisserver 29
- LDIF-Datei, Erstellung UTF-8-Werte 131
- Linux, automatisches Starten des Verzeichniservers allgemeine Informationen 231 Konfiguration 233
- Linux, Deinstallation mit "rpm" GSKit 255 Verzeichnisserver 250
- Linux, erforderlicher Plattenspeicherplatz Verzeichnisserver, Komponenten 3
- Linux, Installation mit "rpm" IBM Global Security Kit 61 Verzeichnisserver 79
- Linux-Dienstprogramme, Deinstallation Sprachenpakete 257
- Linux-Dienstprogramme, Installation Sprachenpakete 69

## M

- Manuelle Deinstallation, AIX-Dienstprogramme allgemeine Informationen 248
- Manuelle Deinstallation, HP-UX-Dienstprogramme allgemeine Informationen 252
- Manuelle Deinstallation, Linux-Dienstprogramme allgemeine Informationen 250
- Manuelle Deinstallation, Solaris-Dienstprogramme allgemeine Informationen 251
- Manuelle Installation integrierte Version von WebSphere Application Server 113
- Manuelle Installation, AIX-Dienstprogramme allgemeine Informationen 71
- Manuelle Installation, Linux-Dienstprogramme allgemeine Informationen 77

- Methoden für die Installation allgemeine Informationen 19

## N

- Namenskonventionen, Verzeichnisserverinstanz Benutzer-ID, Primärgruppe 126

## O

- Öffnen, Webverwaltungstool Konfiguration 120
- online Terminologie vii Veröffentlichungen vii

## P

- Pakete zur Installation, Verzeichnisserver HP-UX 84
- Paketnamen Sprachenpaket 68
- Passport Advantage, herunterladen IBM Security Directory Server 7
- Passport Advantage, IBM Security Directory Server Produkt herunterladen 7
- pkgadd, Installation IBM Global Security Kit 62 Verzeichnisserver 83
- pkgm, Deinstallation GSKit 255 Verzeichnisserver 251
- Protokollpositionen IBM Installation Manager 47
- Protokollverwaltungslösung, Migration Konfiguration 103
- Proxy-Server, Administrator-DN verwalten Konfiguration 180, 181
- Proxy-Server, Administratorkennwort verwalten Konfiguration 182, 183
- Proxy-Server, Backup allgemeine Informationen 198 Konfiguration 200
- Proxy-Server, Erstellung Systemkonfiguration 125
- Proxy-Server, Hauptadministrator allgemeine Informationen 180
- Proxy-Server, Hauptadministratorkennwort allgemeine Informationen 182
- Proxy-Server, Instanz löschen allgemeine Informationen 171 Konfiguration 172
- Proxy-Server, Instanzdetails anzeigen allgemeine Informationen 170 Konfiguration 170
- Proxy-Server, Instanzerstellung angepasste Einstellungen 150
- Proxy-Server, Instanzkonfiguration allgemeine Informationen 177
- Proxy-Server, Konfiguration ändern allgemeine Informationen 167

- Proxy-Server, Konfiguration verwalten allgemeine Informationen 167
- Proxy-Server, öffnen Konfigurationstool 167
- Proxy-Server, Schema verwalten Konfiguration 217, 218
- Proxy-Server, Schemavalidierungsregel Konfiguration 219
- Proxy-Server, Serverdienstprogramme Instanz löschen, Konfiguration 173 Instanzdetails anzeigen, Konfiguration 171 TCP/IP-Einstellungen ändern, Konfiguration 169
- Proxy-Server, Status allgemeine Informationen 167
- Proxy-Server, Suffix entfernen Konfiguration 215, 216
- Proxy-Server, Suffix hinzufügen Konfiguration 214
- Proxy-Server, TCP/IP-Einstellungen ändern allgemeine Informationen 168 Konfiguration 168
- Proxy-Server, Wiederherstellung allgemeine Informationen 201 Konfiguration 203
- Proxy-Server-Instanz Upgrade 96
- Proxy-Server-Instanz, Erstellung Instance Administration Server 150
- Proxy-Server-Instanz, fernes Upgrade Konfiguration, idsimigr -u 99

## R

- rpm, Deinstallation GSKit 255 Verzeichnisserver 250
- rpm, Installation IBM Global Security Kit 61 Verzeichnisserver 79

## S

- Schulung ix
- Serverdienstprogramm, Datenbank optimieren Konfiguration 196
- Serverdienstprogramme idsimigr, Befehl 96 idsimigr, Befehl, -u 99 Instance Administration Tool 156
- Serverdienstprogramme, Active Directory-Synchronisation Konfiguration 229
- Serverdienstprogramme, Administrator-DN verwalten Konfiguration 181
- Serverdienstprogramme, Administratorkennwort verwalten Konfiguration 183
- Serverdienstprogramme, Änderungsprotokoll allgemeine Informationen 209 Konfiguration 211

- Serverdienstprogramme, Änderungsprotokoll inaktivieren
    - Konfiguration 212
  - Serverdienstprogramme, Backup
    - allgemeine Informationen 198
  - Serverdienstprogramme, Befehlszeile
    - Server starten oder stoppen 165
  - Serverdienstprogramme, Datenbankadministratorerkennungswort
    - allgemeine Informationen 190
  - Serverdienstprogramme, Datenbankkonfiguration
    - allgemeine Informationen 183
  - Serverdienstprogramme, Datenbankoptimierung
    - allgemeine Informationen 195
  - Serverdienstprogramme, Datenbankpflege
    - allgemeine Informationen 196
    - Konfiguration 197
  - Serverdienstprogramme, DB2-Datenbank
    - Konfiguration 188
  - Serverdienstprogramme, DB2-Datenbankadministrator
    - Kennwort, Konfiguration 192
  - Serverdienstprogramme, Dekonfiguration der Datenbank
    - allgemeine Informationen 193
  - Serverdienstprogramme, Erstellung LDIF-Datei, UTF-8-Werte 131
  - Serverdienstprogramme, Hauptadministrator
    - allgemeine Informationen 180
  - Serverdienstprogramme, Hauptadministratorerkennungswort
    - allgemeine Informationen 182
  - Serverdienstprogramme, Instanz kopieren
    - Konfiguration 164
  - Serverdienstprogramme, Instanz löschen
    - Konfiguration 173
  - Serverdienstprogramme, Instanzdetails anzeigen
    - Konfiguration 171
  - Serverdienstprogramme, Instanzerstellung
    - Konfiguration 154
  - Serverdienstprogramme, Konfiguration
    - Instanz kopieren 164
    - Server starten oder stoppen 166, 179
    - Verwaltungsserver starten oder stoppen 166, 179
  - Serverdienstprogramme, LDIF-Dateierstellung
    - idsbulkload 131
    - idsdb2ldif 131
    - idsldif2db 131
  - Serverdienstprogramme, LDIF-Datenmanagement
    - allgemeine Informationen 220
  - Serverdienstprogramme, Links
    - allgemeine Informationen 100
  - Serverdienstprogramme, Schemaverwaltung
    - allgemeine Informationen 216
  - Serverdienstprogramme, Suffix
    - allgemeine Informationen 213
  - Serverdienstprogramme, TCP/IP-Einstellungen ändern
    - Konfiguration 169
  - Serverdienstprogramme, verwalten
    - Administrator-DN, Konfiguration 181
    - Administratorkennwort, Konfiguration 183
  - Serverdienstprogramme, Verwaltungsserver starten oder stoppen
    - Konfiguration 166, 179
  - Serverdienstprogramme, Verzeichnisse
    - DB2-Datenbank dekonfigurieren 194
    - Schema verwalten, Konfiguration 218
    - Suffix entfernen, Konfiguration 216
    - Suffix hinzufügen, Konfiguration 214
  - Serverdienstprogramme, Verzeichnisse
    - server starten oder stoppen
      - Konfiguration 166, 179
  - Serverdienstprogramme, Wiederherstellung
    - allgemeine Informationen 201
  - SMIT, Deinstallation
    - GSKit 254
    - Verzeichnisserver 249
  - SMIT-Installation
    - Verzeichnisserver 74
  - SNMP-Lösung, Migration
    - Konfiguration 105
  - Solaris, automatisches Starten des Verzeichnisserver
    - allgemeine Informationen 231
    - Konfiguration 233
  - Solaris, Deinstallation mit "pkgmgr"
    - GSKit 255
    - Verzeichnisserver 251
  - Solaris, erforderlicher Plattenspeicherplatz
    - Verzeichnisserver, Komponenten 3
  - Solaris, Installation mit "pkgadd"
    - IBM Global Security Kit 62
  - Solaris-Dienstprogramme, Deinstallation
    - Sprachenpakete 257
  - Solaris-Dienstprogramme, Installation
    - Sprachenpakete 69
  - Sprachenpaket, Paketnamen
    - Betriebssystem 68
  - Sprachenpakete, Betriebssystem unterstützte Sprachen 67
  - Sprachenpakete, Deinstallation
    - allgemeine Informationen 257
  - Sprachenpakete, Installation
    - allgemeine Informationen 67
  - Standardinstallationspositionen
    - allgemeine Informationen 28
  - Standardinstanz, Erstellung
    - Instance Administration Server 141
  - Standardports, Webverwaltungstool
    - allgemeine Informationen 114
  - Starten, Webverwaltungstool
    - Konfiguration 120
  - swinstall, Installation
    - Verzeichnisserver 85
  - swremove, Deinstallation
    - GSKit 256
    - Verzeichnisserver 252
  - Synchronisation
    - Active Directory zu Security Directory Server 17, 225
- ## T
- Terminologie vii
- ## U
- Überprüfung, Version
    - Webverwaltungstool 89
  - Überprüfung, Verzeichnisserver
    - allgemeine Informationen 87
  - Überprüfung unter AIX, Verzeichnisserver
    - Konfiguration 89
  - Überprüfung unter HP-UX, Verzeichnisserver
    - Konfiguration 89
  - Überprüfung unter Linux, Verzeichnisserver
    - Konfiguration 89
  - Überprüfung unter Solaris, Verzeichnisserver
    - Konfiguration 89
  - Überprüfung unter Windows, Verzeichnisserver
    - Konfiguration 87
  - Umgebung, einrichten
    - Instanz, Upgrade 94
  - Unbeaufsichtigte Änderung, Antwortdatei
    - Konfiguration 38
  - Unbeaufsichtigte Änderungen, Antwortdatei
    - allgemeine Informationen 37
  - Unbeaufsichtigte Deinstallation
    - GSKit 256
  - Unbeaufsichtigte Deinstallation, Antwortdatei
    - allgemeine Informationen 37
    - Konfiguration 38, 246
  - Unbeaufsichtigte Deinstallation, Befehl "imcl"
    - Konfiguration 247
  - Unbeaufsichtigte Installation, Antwortdatei
    - allgemeine Informationen 37
    - Konfiguration 38
  - Unbeaufsichtigte Installation, IBM Global Security Kit
    - Windows 65
  - Unbeaufsichtigte Installation, Windows
    - IBM Global Security Kit 65
  - Unterstützte Betriebssysteme
    - Upgradeinstanz, fern 98
  - Upgrade, Instanz
    - allgemeine Informationen 93
  - Upgrade, Proxy-Server-Instanz
    - idsimigr, Befehl 96
  - Upgrade, Verzeichnisinstanz
    - idsimigr, Befehl 96
  - Upgrade einer fernen Instanz, Konfiguration
    - Instance Administration Tool 157

- Upgrade einer Instanz, Konfiguration
  - fern, idsimigr -u 99
  - fern, Instance Administration Tool 157
  - idsimigr, Befehl, -u 99
- Upgrade einer Instanz, remote allgemeine Informationen 97
- Upgradeinstanz
  - fern, unterstützte Betriebssysteme 98
  - Instance Administration Tool 156
- UTF-8
  - Landessprache, Zeichen 130

## V

- Veröffentlichungen
  - Liste für dieses Produkt vii
  - Onlinezugriff vii
- Verwaltungsserver, Starten oder Stoppen allgemeine Informationen 165, 178
- Verzeichnisinformationen, Directory Services Markup Language allgemeine Informationen 259
- Verzeichnisinstanz
  - Upgrade 96
- Verzeichnisinstanz, fernes Upgrade
  - Konfiguration, idsimigr -u 99
- Verzeichnisserver
  - Daten laden 261
  - DB2-Datenbank dekonfigurieren 193
  - Instanzerstellung 140
  - Pakete für die Installation unter Solaris 81
  - Server starten 261
  - Starten, Webanwendungsserver 119
- Verzeichnisserver, Active Directory
  - Synchronisation, allgemeine Informationen 17, 225
- Verzeichnisserver, Active Directory-Synchronisation
  - Konfiguration 227, 229
- Verzeichnisserver, Administrator-DN verwalten
  - Konfiguration 180, 181
- Verzeichnisserver, Administratorkennwort verwalten
  - Konfiguration 182, 183
- Verzeichnisserver, Änderungen allgemeine Informationen 41
- Verzeichnisserver, Änderungsprotokoll allgemeine Informationen 209
  - Konfiguration 209, 211
- Verzeichnisserver, Änderungsprotokoll inaktivieren
  - Konfiguration 211, 212
- Verzeichnisserver, Backup allgemeine Informationen 198
- Verzeichnisserver, Benutzer und Gruppen allgemeine Informationen 125
  - Berechtigungen, allgemeine Informationen 127
  - Erstellung, allgemeine Informationen 127
  - Voraussetzungen 125
- Verzeichnisserver, Client- und Serverdienstprogramme
  - Links, allgemeine Informationen 100

- Verzeichnisserver, Datenbank sichern
  - Konfiguration 199
- Verzeichnisserver, Datenbank wiederherstellen
  - Konfiguration 202
- Verzeichnisserver, Datenbankadministratorkennwort
  - allgemeine Informationen 190
- Verzeichnisserver, Datenbankkonfiguration
  - allgemeine Informationen 183
- Verzeichnisserver, Datenbankoptimierung
  - allgemeine Informationen 195
- Verzeichnisserver, Datenbankpflege
  - allgemeine Informationen 196
- Verzeichnisserver, DB2
  - allgemeine Informationen 55
- Verzeichnisserver, DB2-Datenbank
  - Dekonfiguration 194
  - Optimierung 195, 196
  - Pflege 197
- Verzeichnisserver, DB2-Datenbank konfigurieren
  - Konfiguration 184, 188
- Verzeichnisserver, DB2-Datenbankadministrator
  - Kennwort, Konfiguration 191, 192
- Verzeichnisserver, DB2-Eigenschaftendatei
  - Konfiguration 263
- Verzeichnisserver, Deinstallation
  - allgemeine Informationen 243, 244
- Verzeichnisserver, Deinstallation mit AIX-Dienstprogrammen
  - allgemeine Informationen 248
- Verzeichnisserver, Dekonfiguration der Datenbank
  - allgemeine Informationen 193
- Verzeichnisserver, Erstellung
  - allgemeine Informationen 160
  - Systemkonfiguration 125
- Verzeichnisserver, Hauptadministrator
  - allgemeine Informationen 180
- Verzeichnisserver, Hauptadministratorkennwort
  - allgemeine Informationen 182
- Verzeichnisserver, Hinzufügen von Instanzen
  - Konfiguration 162
- Verzeichnisserver, IBM JDK
  - allgemeine Informationen 57
- Verzeichnisserver, Implementierung
  - Webverwaltungstool 116
- Verzeichnisserver, Installation
  - Anforderungen, allgemeine Informationen 1
  - Betriebssystemdienstprogramme 71
  - IBM Installation Manager 32
  - Launchpad, Konfiguration 29
  - Repository 31
  - Voraussetzungen, allgemeine Informationen 15
- Verzeichnisserver, Installation mit AIX-Dienstprogrammen
  - allgemeine Informationen 71

- Verzeichnisserver, Installation mit IBM Installation Manager
  - unterstütztes Betriebssystem, allgemeine Informationen 22
- Verzeichnisserver, Installationsübersicht
  - allgemeine Informationen 3
- Verzeichnisserver, Installationsvoraussetzungen
  - allgemeine Informationen 15
- Verzeichnisserver, Instance Administration Tool
  - allgemeine Informationen 137
- Verzeichnisserver, Instanz hinzufügen
  - Replikationstopologie 160
- Verzeichnisserver, Instanz löschen
  - allgemeine Informationen 171
  - Konfiguration 172
- Verzeichnisserver, Instanzdetails anzeigen
  - allgemeine Informationen 170
  - Konfiguration 170
- Verzeichnisserver, Instanzerstellung
  - allgemeine Informationen 137, 140
  - angepasste Einstellungen 143
  - Instance Administration Tool 140
  - Konfiguration 154, 164
  - Standardinstanz 141
- Verzeichnisserver, Instanzkonfiguration
  - allgemeine Informationen 177
- Verzeichnisserver, Instanzverwaltung
  - allgemeine Informationen 137
- Verzeichnisserver, Komponenten
  - erforderlicher Plattenspeicherplatz 3
- Verzeichnisserver, Konfiguration ändern
  - allgemeine Informationen 167
- Verzeichnisserver, Konfiguration verwalten
  - allgemeine Informationen 167
- Verzeichnisserver, Konfigurationstool
  - Leistungsoptimierung 205, 208
- Verzeichnisserver, Kopie
  - allgemeine Informationen 160
- Verzeichnisserver, LDIF-Daten exportieren
  - Konfiguration 223
- Verzeichnisserver, LDIF-Daten importieren
  - Konfiguration 221
- Verzeichnisserver, LDIF-Daten prüfen
  - Konfiguration 222
- Verzeichnisserver, LDIF-Datenmanagement
  - allgemeine Informationen 220
- Verzeichnisserver, Leistung
  - Optimierung, allgemeine Informationen 203
- Verzeichnisserver, manuelle Installation
  - Solaris 81
- Verzeichnisserver, Migration der Active Directory-Synchronisationslösung
  - Konfiguration 105
- Verzeichnisserver, Migration der Datenbank
  - Konfiguration 102
- Verzeichnisserver, Migration der Protokollverwaltungslösung
  - Konfiguration 103

- Verzeichnisse, Migration der SNMP-Lösung
  - Konfiguration 105
- Verzeichnisse, Migration von Lösungen
  - allgemeine Informationen 101
- Verzeichnisse, Namenskonventionen
  - allgemeine Informationen 126
  - Benutzer-ID, Primärgruppe 126
- Verzeichnisse, öffnen
  - Konfigurationstool 167
- Verzeichnisse, Optimierung
  - allgemeine Informationen 203
  - Leistung, allgemeine Informationen 203
- Verzeichnisse, Pakete zur Installation unter AIX
  - allgemeine Informationen 72
- Verzeichnisse, Pakete zur Installation unter Linux
  - allgemeine Informationen 77
- Verzeichnisse, Schema verwalten
  - Konfiguration 217, 218
- Verzeichnisse, Schemavalidierungsregel
  - Konfiguration 219
- Verzeichnisse, Schemaverwaltung
  - allgemeine Informationen 216
- Verzeichnisse, Serverdienstprogramme
  - Instanz löschen, Konfiguration 173
  - Instanzdetails anzeigen, Konfiguration 171
  - TCP/IP-Einstellungen ändern, Konfiguration 169
- Verzeichnisse, Solaris
  - Installation mit "pkgadd" 83
- Verzeichnisse, Starten oder Stoppen
  - allgemeine Informationen 165, 178
- Verzeichnisse, Status
  - allgemeine Informationen 167
- Verzeichnisse, Suffix
  - allgemeine Informationen 213
- Verzeichnisse, Suffix entfernen
  - Konfiguration 215, 216
- Verzeichnisse, Suffix hinzufügen
  - Konfiguration 214
- Verzeichnisse, Synchronisation
  - allgemeine Informationen 17, 225
- Verzeichnisse, TCP/IP-Einstellungen ändern
  - allgemeine Informationen 168
  - Konfiguration 168
- Verzeichnisse, Überprüfung
  - allgemeine Informationen 87
  - Version des Webverwaltungstools 89
- Verzeichnisse, Überprüfung unter AIX
  - Konfiguration 89
- Verzeichnisse, Überprüfung unter HP-UX
  - Konfiguration 89
- Verzeichnisse, Überprüfung unter Linux
  - Konfiguration 89
- Verzeichnisse, Überprüfung unter Solaris
  - Konfiguration 89

- Verzeichnisse, Überprüfung unter Windows
  - Konfiguration 87
- Verzeichnisse, unbeaufsichtigte Änderung
  - Konfiguration 38
- Verzeichnisse, unbeaufsichtigte Änderungen
  - allgemeine Informationen 37
- Verzeichnisse, unbeaufsichtigte Deinstallation
  - allgemeine Informationen 37
  - Konfiguration 38, 246, 247
- Verzeichnisse, unbeaufsichtigte Installation
  - allgemeine Informationen 37
  - Konfiguration 38
- Verzeichnisse, Upgrade von Instanzen
  - allgemeine Informationen 93
- Verzeichnisse, Wiederherstellung
  - allgemeine Informationen 201
- Verzeichnisse, Verdeinstallation, Betriebssystemdienstprogramme
  - allgemeine Informationen 248
- Verzeichnisse, Verzeichnisinstanz, Erstellung
  - Instance Administration Server 143
  - Konfiguration 154
- Verzeichnisse, Verzeichnisse, HP-UX
  - allgemeine Informationen 84
- Verzeichnisse, Verzeichnisstruktur
  - Installation, Position 175
- Verzeichnisse, Verzeichnisstruktur, heruntergeladene Dateien
  - AIX 7
  - Linux 7
  - Solaris 7
  - Windows 7

## W

- Webadresse, HTTPS
  - allgemeine Informationen 122
- Webanwendungsserver, Anwendungsserver stoppen
  - Konfiguration 121
- Webanwendungsserver, starten
  - Konfiguration 119
- WebSphere Application Server, Webverwaltungstool implementieren
  - Konfiguration 117
- Webverwaltungstool
  - Konfiguration migrieren 106
  - Migration, allgemeine Informationen 106
  - Migration, Befehl "idswmigr" 107
- Webverwaltungstool, Deimplementierung
  - Konfiguration 123
- Webverwaltungstool, Implementierung
  - allgemeine Informationen 113
  - WebSphere Application Server 117
- Webverwaltungstool, Standardports
  - allgemeine Informationen 114
- Windows, automatisches Starten des Verzeichnisseservers
  - allgemeine Informationen 231
  - Konfiguration 231

- Windows, Deinstallation
  - GSKit 256
- Windows, erforderlicher Plattenspeicherplatz
  - Verzeichnisse, Komponenten 3
- Windows, GSKit
  - Überprüfung 90
- Windows, Installation
  - IBM Global Security Kit 64
- Windows, unbeaufsichtigte Installation
  - IBM Global Security Kit 65

## Z

- Zeichen, Landessprache
  - UTF-8 130
- Zeichensatz, IANA
  - Codepage, DB2 132
- Zugriff, Webverwaltungstool
  - Konfiguration 120



---

## 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 Quellsprache geschrieben sind und Programmier Techniken 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 Anwendungspogrammierschnittstellen 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](http://ibm.com) sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicennamen 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](http://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.





SC12-4464-02

