

**IBM Security Directory Server**  
バージョン 6.3.1.5

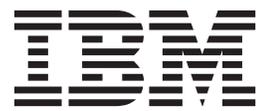
# インストールと構成のガイド





**IBM Security Directory Server**  
バージョン 6.3.1.5

# インストールと構成のガイド



お願い

本書および本書で紹介する製品をご使用になる前に、297 ページの『特記事項』に記載されている一般情報をお読みください。

注: 本書は、*IBM Security Directory Server* バージョン 6.3.1.5 (製品番号 5724-J39)、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典: SC27-2747-02  
IBM Security Directory Server  
Version 6.3.1.5  
Installation and Configuration Guide

発行: 日本アイ・ビー・エム株式会社

担当: トランスレーション・サービス・センター

© Copyright IBM Corporation 1998, 2014.

# 目次

本書について . . . . .	vii
資料および用語集へのアクセス . . . . .	vii
アクセシビリティ . . . . .	ix
技術研修 . . . . .	ix
サポート情報 . . . . .	ix
適切なセキュリティの実施について . . . . .	x

## 第 1 章 インストールの計画 . . . . . 1

## 第 2 章 インストールの概要 . . . . . 3

ディスク・スペース要件 . . . . .	3
インストール・メディアの準備 . . . . .	6
パスポート・アドバンテージからのソフトウェアの ダウンロード . . . . .	7
ダウンロードしたファイルのディレクトリー構造 . . . . .	8
インストールの前提条件 . . . . .	16
各種オペレーティング・システムに必要な前提条 件パッケージ . . . . .	16
PowerPC LE での LDAP クライアントの前提条 件 . . . . .	18
idsldap ユーザーおよびグループ . . . . .	18
インストール方法 . . . . .	20

## 第 3 章 IBM Installation Manager を使 用したインストール . . . . . 23

IBM Installation Manager の概要 . . . . .	23
サポートされるオペレーティング・システム . . . . .	24
IBM Security Directory Server のインストール・パッ ケージ・タイプ . . . . .	24
インストールに関するガイドライン . . . . .	25
IBM Security Directory Server のコンポーネント . . . . .	26
IBM Security Directory Server のインストールのカス タマイズ . . . . .	29
デフォルトのインストール・ロケーション . . . . .	30
インストール・リポジトリ . . . . .	31
インストールの開始 . . . . .	31
ランチパッドを使用したインストールの開始 . . . . .	31
リポジトリ設定を設定することによるインスト ールの開始 . . . . .	33
IBM Installation Manager を使用したインストール . . . . .	35
サイレント・モード・インストール . . . . .	39
応答ファイルを使用したサイレント・インストー ル . . . . .	40

## 第 4 章 IBM Installation Manager を使 用した変更 . . . . . 43

IBM Installation Manager を使用した機能変更 . . . . .	43
--	----

## 第 5 章 IBM Installation Manager の口 グ・ファイル . . . . . 49

## 第 6 章 IBM Security Directory Server パッケージの照会 . . . . . 51

## 第 7 章 スクリプトを使用したネイティ ブ・インストールおよび構成 . . . . . 53

インストール・ロードマップ . . . . .	53
Linux、Solaris、および HP-UX の各プラットフォー ムへの IBM Security Directory Server パッケージの インストール . . . . .	54
インストール・ログの検証 . . . . .	56

## 第 8 章 IBM DB2 のインストール . . . . . 57

## 第 9 章 IBM Security Directory Server 用の IBM Java Development Kit . . . . . 59

## 第 10 章 IBM Global Security Kit のイ ンストール . . . . . 61

installp を使用した IBM Global Security Kit のイ ンストール . . . . .	62
Linux ユーティリティを使用した IBM Global Security Kit のインストール . . . . .	63
Solaris ユーティリティを使用した IBM Global Security Kit のインストール . . . . .	64
HP-UX ユーティリティを使用した IBM Global Security Kit のインストール . . . . .	65
Windows での IBM Global Security Kit のインスト ール . . . . .	66
Windows での IBM Global Security Kit のサイレン ト・インストール . . . . .	67

## 第 11 章 言語パックのインストール . . . . . 69

インストール用の各言語パックのパッケージ . . . . .	70
オペレーティング・システムのユーティリティを 使用した言語パックのインストール . . . . .	71

## 第 12 章 オペレーティング・システム・ コマンド行ユーティリティを使用したイ ンストール . . . . . 73

AIX ユーティリティを使用したインストール . . . . .	73
AIX システムへのインストール用パッケージ . . . . .	74
SMIT を使用したインストール . . . . .	76
installp を使用したインストール . . . . .	78
Linux ユーティリティを使用したインストール . . . . .	80
Linux システムへのインストール用パッケージ . . . . .	80
Linux ユーティリティを使用したインストール . . . . .	83

Solaris ユーティリティを使用したインストール	84
Solaris システムへのインストール用パッケージ	84
Solaris ユーティリティを使用したインストール	86
HP-UX ユーティリティを使用したインストール	88
HP-UX Itanium システムへのインストール用パッケージ	88
HP-UX ユーティリティを使用したインストール	89

## 第 13 章 IBM Security Directory Server の機能の検証 . . . . . 91

IBM Installation Manager を使用した IBM Security Directory Server 機能の検証	91
IBM Security Directory Server 機能の Windows 上での検証	92
IBM Security Directory Server パッケージの検証	93
Web 管理ツールのバージョンの検証	93
IBM Global Security Kit の Windows へのインストールの検証	94
IBM Global Security Kit の AIX、Linux、Solaris、および HP-UX へのインストールの検証	95

## 第 14 章 前バージョンのインスタンスのアップグレード . . . . . 97

インスタンスをアップグレードする前の環境の設定	98
<b>idsimigr</b> コマンドを使用した前のバージョンのインスタンスのアップグレード	100
別のコンピューターに対する前のバージョンのインスタンスのアップグレード	102
リモート・インスタンスのアップグレード用にサポートされるオペレーティング・システム	102
<b>idsimigr</b> コマンドを使用した前のバージョンのリモート・インスタンスのアップグレード	103
クライアントおよびサーバー・ユーティリティへのリンク	105

## 第 15 章 前バージョンのインスタンスからのデータおよびソリューションの移行 . . . . . 107

DB2 ESE データベースを使用するインスタンスから DB2 WSE データベースを使用するインスタンスへの移行	108
ログ管理ソリューションの移行	110
SNMP ソリューションの移行	111
Active Directory との同期ソリューションの移行	112
前のバージョンの Web 管理ツール構成の移行	113
<b>idswmigr</b>	114
Web 管理ツールの手動での移行	115

## 第 16 章 手動による Web 管理ツールのデプロイメント . . . . . 121

手動による WebSphere Application Server 組み込みバージョンのインストール	121
Web 管理ツールのデフォルト・ポート	122

WebSphere Application Server 組み込みバージョンへの Web 管理ツールのデプロイ	124
WebSphere Application Server への Web 管理ツールのデプロイ	125
Web 管理ツールを使用するための WebSphere Application Server 組み込みバージョンの始動	127
Web 管理ツールへのアクセス	128
Web アプリケーション・サーバーの停止	130
WebSphere Application Server 組み込みバージョンでの HTTPS	131
Web 管理ツールの WebSphere Application Server 組み込みバージョンからのアンデプロイ	132

## 第 17 章 インスタンス構成の計画 . . . . . 133

ディレクトリー・サーバー・インスタンスに関連付けられたユーザーとグループ	133
命名規則	134
ユーザーとグループ作成の要件	135
構成の計画	137
UTF-8 サポート	138
ディレクトリー・サーバーでの UTF-8 の使用	139
サーバー・ユーティリティの使用による UTF-8 値を持つ LDIF ファイルの作成	139
サポートされる IANA 文字セット	141
33 番から 126 番までの ASCII 文字	142

## 第 18 章 インスタンスの作成および管理 . . . . . 145

インスタンス管理ツールの始動	146
インスタンスをアップグレードするためのインスタンス管理ツールの始動	147
ディレクトリー・サーバー・インスタンス作成	148
インスタンス管理ツールを使用したインスタンス作成	149
デフォルトのディレクトリー・サーバー・インスタンスの作成	149
カスタム設定を使用したディレクトリー・サーバー・インスタンスの作成	151
カスタム設定を使用したプロキシ・サーバー・インスタンスの作成	160
コマンド行ユーティリティを使用したインスタンスの作成	163
インスタンス管理ツールを使用した前のバージョンのインスタンスのアップグレード	165
インスタンス管理ツールを使用した前のバージョンのリモート・インスタンスのアップグレード	167
既存のインスタンスからのインスタンス作成	170
インスタンス管理ツールを使用した既存のインスタンスのコピーの作成	172
コマンド行ユーティリティを使用した既存のインスタンスのコピーの作成	175
ディレクトリー・サーバーおよび管理サーバーの始動または停止	176
ディレクトリー・サーバーおよび管理サーバーの始動または停止	176

コマンド行ユーティリティを使用したディレク トリー・サーバーおよび管理サーバーの始動また は停止 . . . . .	177
ディレクトリー・サーバー・インスタンス構成の管 理 . . . . .	178
インスタンス管理ツールから構成ツールを開く	178
インスタンスの TCP/IP 設定の変更 . . . . .	179
インスタンス管理ツールを使用したインスタ ンスの TCP/IP 設定の変更 . . . . .	179
コマンド行ユーティリティを使用したインスタ ンスの TCP/IP 設定の変更 . . . . .	180
インスタンスに関する情報の表示 . . . . .	182
インスタンス管理ツールを使用したインスタ ンスに関する情報の表示 . . . . .	182
コマンド行ユーティリティを使用したインスタ ンスに関する情報の表示 . . . . .	182
ディレクトリー・サーバー・インスタンスの削除	183
インスタンス管理ツールを使用したインスタ ンスの削除 . . . . .	183
コマンド行ユーティリティを使用したインスタ ンスの削除 . . . . .	184
<b>第 19 章 ディレクトリー構造の検証</b>	<b>187</b>
<b>第 20 章 インスタンス構成</b>	<b>189</b>
構成ツールの開始 . . . . .	190
構成ツールを使用したディレクトリー・サーバーお よび管理サーバーの始動または停止 . . . . .	190
構成ツールを使用したディレクトリー・サーバー および管理サーバーの始動または停止 . . . . .	191
コマンド行ユーティリティを使用したディレク トリー・サーバーおよび管理サーバーの始動また は停止 . . . . .	192
インスタンスの 1 次管理者 DN の管理 . . . . .	192
構成ツールを使用した 1 次管理者 DN の管理	193
コマンド行ユーティリティを使用した 1 次管 理者 DN の管理 . . . . .	193
インスタンスの 1 次管理者パスワードの管理 . . . . .	194
構成ツールを使用した 1 次管理者パスワードの 管理 . . . . .	195
コマンド行ユーティリティを使用した 1 次管 理者パスワードの管理 . . . . .	195
ディレクトリー・サーバー・インスタンスのデー タベース構成 . . . . .	196
構成ツールを使用したインスタンスのデー タベースの構成 . . . . .	197
コマンド行ユーティリティを使用したインスタ ンスのデータベースの構成 . . . . .	202
DB2 データベース管理者パスワードの管理 . . . . .	204
構成ツールを使用した DB2 データベース管理 者パスワードの変更 . . . . .	204
コマンド行ユーティリティを使用した DB2 デ ータベース管理者パスワードの変更 . . . . .	205
ディレクトリー・サーバー・インスタンスからのデ ータベース構成解除 . . . . .	206

構成ツールを使用したインスタンスからの DB2 データベースの構成解除 . . . . .	207
コマンド行ユーティリティを使用したインスタ ンスからの DB2 データベースの構成解除 . . . . .	208
データベースの最適化 . . . . .	209
構成ツールを使用したデータベースの最適化 . . . . .	209
コマンド行ユーティリティを使用したデー タベースの最適化 . . . . .	210
データベース保守 . . . . .	210
構成ツールを使用したデータベース保守の実行	211
コマンド行ユーティリティを使用したデー タベース保守の実行 . . . . .	211
ディレクトリー・サーバーのバックアップ . . . . .	212
構成ツールを使用したディレクトリー・サー バー・インスタンスのデータベースのバックアップ	213
構成ツールを使用したプロキシ・サーバー・イ ンスタンスのバックアップ . . . . .	215
ディレクトリー・サーバーの復元 . . . . .	216
構成ツールを使用したディレクトリー・サー バーのデータベースの復元 . . . . .	216
構成ツールを使用したプロキシ・サーバー・イ ンスタンスの復元 . . . . .	217
ディレクトリー・サーバーのパフォーマンス・チュ ーニング . . . . .	218
構成ツールを使用したパフォーマンス・チュ ーニングのためのディレクトリー・サーバーの構成 . . . . .	220
コマンド行ユーティリティを使用したパフォー マンス・チューニングのためのディレクトリー・ サーバーの構成 . . . . .	223
ディレクトリー・サーバー・インスタンスのための 変更ログ管理 . . . . .	224
構成ツールを使用した変更ログの構成 . . . . .	224
コマンド行ユーティリティを使用した変更ログ の構成 . . . . .	225
構成ツールを使用した変更ログの構成解除 . . . . .	226
コマンド行ユーティリティを使用した変更ログ の構成解除 . . . . .	227
サフィックス構成 . . . . .	228
構成ツールを使用したサフィックスの追加 . . . . .	229
コマンド行ユーティリティを使用したサフィッ クスの追加 . . . . .	229
構成ツールを使用したサフィックスの削除 . . . . .	230
コマンド行ユーティリティを使用したサフィッ クスの削除 . . . . .	231
スキーマ管理 . . . . .	232
構成ツールを使用したスキーマ・ファイルの管理	233
コマンド行ユーティリティを使用したスキ ーマ・ファイルの管理 . . . . .	234
構成ツールを使用したスキーマ妥当性検査の構成	235
LDIF データ管理 . . . . .	236
構成ツールを使用した LDIF データのインポ ート . . . . .	237
構成ツールを使用した LDIF データの検証 . . . . .	239
構成ツールを使用した LDIF データのエクスポ ート . . . . .	239
Active Directory との同期 . . . . .	241

Active Directory との同期の構成および実行 . . .	243
構成ツールを使用した Active Directory との同期 の構成. . . . .	244
コマンド行ユーティリティを使用した Active Directory との同期の構成 . . . . .	245

**第 21 章 オペレーティング・システムの  
始動時におけるディレクトリー・サー  
バー・インスタンスの自動始動 . . . . . 247**

Windows でのディレクトリー・サーバー・インスタ ンスの自動始動の構成 . . . . .	247
UNIX でのディレクトリー・サーバー・インスタ ンスの自動始動の構成 . . . . .	249

**第 22 章 フィックスパックの計画 . . . . . 253**

IBM Installation Manager を使用したフィックスパ ックのインストール . . . . .	253
フィックスパックのサイレント・モード・インス トール. . . . .	255
ネイティブ・スクリプトを使用したフィックスパ ックのインストール. . . . .	256

**第 23 章 IBM Security Directory  
Server のアンインストール: 概要 . . . . . 259**

**第 24 章 IBM Security Directory  
Server および相互要件ソフトウェアの  
アンインストール . . . . . 261**

IBM Installation Manager を使用したアンインスト ール . . . . .	262
IBM Installation Manager を使用したアンインス トール. . . . .	262
応答ファイルを使用したサイレント・アンインス トール. . . . .	264
<b>imcl uninstall</b> コマンドを使用したサイレン ト・アンインストール . . . . .	265
オペレーティング・システムのユーティリティを 使用した IBM Security Directory Server のアンイン ストール . . . . .	266
AIX ユーティリティを使用したアンインスト ール . . . . .	267
Linux ユーティリティを使用したアンインスト ール . . . . .	269

Solaris ユーティリティを使用したアンインス トール. . . . .	270
HP-UX ユーティリティを使用したアンインス トール. . . . .	271
DB2 コマンドを使用した IBM DB2 のアンインス トール. . . . .	272
オペレーティング・システムのユーティリティを 使用した IBM Global Security Kit のアンインスト ール . . . . .	272
SMIT を使用した IBM Global Security Kit のア ンインストール. . . . .	273
<b>installp</b> を使用した IBM Global Security Kit のアンインストール . . . . .	273
Linux ユーティリティを使用した IBM Global Security Kit のアンインストール . . . . .	274
Solaris ユーティリティを使用した IBM Global Security Kit のアンインストール . . . . .	274
HP-UX ユーティリティを使用した IBM Global Security Kit のアンインストール . . . . .	275
Windows での IBM Global Security Kit のアン インストール . . . . .	275
言語パックのアンインストール . . . . .	276
オペレーティング・システムのユーティリ ティを使用した言語パックのアンインストール. . . . .	276

**付録 A. Directory Services Markup  
Language (DSML) . . . . . 279**

**付録 B. サンプル・データベースのロー  
ドおよびサーバーの始動 . . . . . 281**

**付録 C. 手動による ldapdb.properties  
ファイルの更新 . . . . . 283**

**付録 D. Security Directory Server の  
アクセシビリティ機能 . . . . . 285**

**索引 . . . . . 287**

**特記事項. . . . . 297**

---

## 本書について

IBM® Security Directory Server (以前の名称は IBM Tivoli® Directory Server) は、以下のオペレーティング・システム向けの Lightweight Directory Access Protocol の IBM の実装です。

- Microsoft Windows
- AIX®
- Linux (System x®、System z®、System p®、および System i®)
- Solaris
- Hewlett-Packard UNIX (HP-UX) (Itanium)

「*IBM Security Directory Server インストールと構成のガイド*」には、IBM Security Directory Server のインストール、構成、およびアンインストールに関する情報が記載されています。また、前のバージョンからのアップグレードに関する情報も記載されています。

---

## 資料および用語集へのアクセス

このセクションには、以下が含まれています。

- 『IBM Security Directory Server ライブラリー』の資料のリスト。
- viii ページの『オンライン資料』へのリンク。
- ix ページの『IBM Terminology Web サイト』へのリンク。

### IBM Security Directory Server ライブラリー

IBM Security Directory Server ライブラリーでは以下の資料を入手できます。

- *IBM Security Directory Server* バージョン 6.3.1.5 製品概要、GA88-7243-01

IBM Security Directory Server 製品、現行リリースでの新機能、およびシステム要件に関する情報が記載されています。

- *IBM Security Directory Server* バージョン 6.3.1.5 クイック・スタート・ガイド、GI88-4247-02

IBM Security Directory Server の使用を開始するための有用な情報が提供されています。簡単な製品説明とアーキテクチャーの図、製品資料 Web サイトへのアクセス方法とインストールの説明が記載されています。

- *IBM Security Directory Server* バージョン 6.3.1.5 インストールと構成のガイド、SA88-4191-02

IBM Security Directory Server のインストール、構成、およびアンインストールに関する詳細な情報が記載されています。IBM Security Directory Server の前のバージョンからのアップグレードに関する情報も記載されています。

- *IBM Security Directory Server* バージョン 6.3.1.5 管理ガイド、SA88-4190-02

Web 管理ツールおよびコマンド行による管理用タスクの説明が記載されています。

- *IBM Security Directory Server* バージョン 6.3.1.5 レポーティング・ガイド、SC43-1267-00

IBM Security Directory Server のレポートを作成するためのツールおよびソフトウェアについて説明します。

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

IBM Security Directory Server に組み込まれているコマンド行ユーティリティーの構文および使用法について説明しています。

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

サーバー・プラグインの作成方法が記載されています。

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

C および Java™ での Lightweight Directory Access Protocol (LDAP) クライアント・アプリケーションの作成に関する情報が記載されています。

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

パフォーマンス改善のためのディレクトリー・サーバーのチューニング方法が記載されています。さまざまなサイズおよびさまざまな読み取り/書き込み率を持つディレクトリーについての、ディスク要件およびその他のハードウェア要件が記載されています。ディレクトリーと使用ディスク量およびメモリー量の各レベルごとに、既知の作業シナリオを示します。また、経験法則も提案します。

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

起こりうる問題、および IBM ソフトウェア・サポートに連絡する前に実行できる修正措置に関する情報が記載されています。

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

IBM Security Directory Server に関連付けられている、すべての警告メッセージとエラー・メッセージのリストが記載されています。

## オンライン資料

IBM では、製品のリリース時および資料の更新時に、以下の場所に製品資料を掲載します。

### IBM Security Directory Server 資料の Web サイト

<http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm> サイトには、この製品の資料のウェルカム・ページが表示されます。

### IBM Security Systems Documentation Central およびウェルカム・ページ

IBM Security Systems Documentation Central では、すべての IBM Security Systems 製品資料のアルファベット順のリストが提供されています。また、各製品の特定のバージョンの製品資料へのリンクを見つけることもできます。

Welcome to IBM Security Systems documentation には、IBM Security Systems の資料、資料の概要、資料へのリンク、および資料の一般情報が記載されています。

### IBM Publications Center

このサイト ( <http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss> ) には、必要なすべての IBM 資料を見つけるのに役立つカスタマイズ検索機能が用意されています。

### IBM Terminology Web サイト

IBM Terminology Web サイトは、製品ライブラリーの用語を 1 つのロケーションに統合したものです。Terminology Web サイトには、<http://www.ibm.com/software/globalization/terminology> からアクセスできます。

---

## アクセシビリティ

アクセシビリティ機能は、運動障害または視覚障害など身体に障害を持つユーザーがソフトウェア・プロダクトを快適に使用できるようにサポートします。この製品では、音声による支援テクノロジーを使用してインターフェースをナビゲートすることができます。また、マウスの代わりにキーボードを使用して、グラフィカル・ユーザー・インターフェースのすべての機能を操作できます。

詳しくは、「*IBM Security Directory Server 製品概要*」の付録の『アクセシビリティ』を参照してください。

---

## 技術研修

技術研修の情報については、IBM Education Web サイト (<http://www.ibm.com/software/tivoli/education>) を参照してください。

---

## サポート情報

IBM サポートは、コード関連の問題、および短時間のインストールや使用方法の定型的質問に対する支援を提供します。IBM ソフトウェア・サポート・サイトには、<http://www.ibm.com/software/support/probsub.html> から直接アクセスできます。

「*IBM Security Directory Server Troubleshooting Guide*」には、次のことに関する詳細が記述されています。

- IBM サポートに連絡する前に収集する情報。
- IBM サポートに連絡するためのさまざまな方法。
- IBM Support Assistant の利用方法。
- 問題を自分で特定して修正するための説明および問題判別リソース。

注: 製品のインフォメーション・センターの「コミュニティおよびサポート」タブに、追加のサポート・リソースがある場合があります。

---

## 適切なセキュリティの実施について

IT システム・セキュリティには、企業内外からの不正アクセスの防止、検出、および対応によって、システムや情報を保護することが求められます。不正アクセスにより、情報の改ざん、破壊、悪用を招くおそれがあり、またシステムが損傷したり誤用されたりして、他のシステムへの攻撃に使用されるおそれがあります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティ対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、包括的なセキュリティの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、システム、製品、サービス、および企業がいかなる第三者による悪意のある行為または不正行為からも保護されることを保証するものではありません。

---

## 第 1 章 インストールの計画

IBM Security Directory Server をインストールする前に、ディレクトリー・サーバー環境のハードウェア、ソフトウェア、ユーザーの役割、セキュリティー、およびその他の要件を決定する必要があります。

### 計画ロードマップ

このセクションのチェックリストを使用してサーバーをインストールします。

以前のリリースからアップグレードする場合は、このチェックリストは使用しないでください。代わりに、97 ページの『第 14 章 前バージョンのインスタンスのアップグレード』の説明を参照してください。

サーバーをインストールするには、以下の手順を実行します。

1. 概略を読んで、インストールする IBM Security Directory Server のコンポーネントについて学習します。
2. 最小限の必須ハードウェアおよびソフトウェアがあることを確認します。要件については、3 ページの『ディスク・スペース要件』を参照してください。
3. IBM Installation Manager を使用して、IBM Security Directory Server をインストールします。
4. Windows システムでシステムを再始動した場合、インストール時にログオンしていたユーザーとしてログオンします。
5. インスタンス管理ツールを使用して、ディレクトリー・サーバー・インスタンスを管理します。
6. オプションで、データベースにサンプル LDIF ファイルをロードし、インストールおよび構成を検証します。詳細については、281 ページの『付録 B. サンプル・データベースのロードおよびサーバーの始動』を参照してください。
7. ディレクトリー・サーバー・インスタンスを始動します。Web 管理ツールをインストールしている場合は、それを始動します。
8. サーバーおよび Web 管理ツールのセットアップおよび使用については、IBM Security Directory Server 資料の『管理』セクションを参照してください。

フル・ディレクトリー・サーバーをインストール済みで、データベースの編成を計画する場合は、137 ページの『構成の計画』の情報を参照してください。



## 第 2 章 インストールの概要

コンピューターを準備し、ご使用の環境に適用できる適切な IBM Security Directory Server のインストール・モードを選択する必要があります。

Windows、Linux64、および AIX 向けに、IBM Installation Manager ベースのインストーラーが用意されています。また、UNIX システム (Linux 64 および AIX を除く) 上では、IBM Security Directory Server のラッパー・インストーラーが使用可能です。Installation Manager ベースのインストーラーでは、IBM Security Directory Server V6.3.1 の GUI によるインストールとサイレント・インストールがサポートされています。

### ディスク・スペース要件

IBM Security Directory Server および相互前提条件ソフトウェアの正常なインストールのために、コンピューターには必要なディスク・スペースが確保されている必要があります。ディスク・スペース要件は、オペレーティング・システム、IBM Security Directory Server の機能、およびインストールで選択した相互前提条件ソフトウェアに基づいて異なります。

#### Windows のディスク・スペース要件

注: インストールでプロキシ・サーバー機能または完全な Directory Server 機能を選択した場合は、クライアント SDK、IBM Java Development Kit、および Java クライアントのサイズを一度追加します。

表 1. Windows での IBM Security Directory Server 機能および相互前提条件ソフトウェアのディスク・スペース要件

インストール可能な機能	インストール用のディスク・スペース (MB 単位)
クライアント・ソフトウェア開発キット	25 MB
IBM Java Development Kit	200 MB
Java クライアント	124 MB
デプロイされた Web 管理ツール (WebSphere® Application Server 組み込みバージョンおよび WebSphere Application Server 組み込みバージョンにデプロイされた Web 管理ツールを含む)	440 MB
既存の WebSphere Application Server 組み込みバージョンまたは WebSphere Application Server 内の Web 管理ツールのデプロイメント	260 MB
Base Server	23 MB
プロキシ・サーバー (クライアント SDK、Java クライアント、および Base Server のサイズを追加してください)	40 MB

表 1. Windows での IBM Security Directory Server 機能および相互前提条件ソフトウェアのディスク・スペース要件 (続き)

インストール可能な機能	インストール用のディスク・スペース (MB 単位)
完全な Directory Server (クライアント SDK、Java クライアント、および Base Server のサイズを追加してください)	8 MB
IBM DB2®	763 MB
IBM Global Security Kit	11 MB

## AIX のディスク・スペース要件

注: インストールでプロキシ・サーバー機能または完全な Directory Server 機能を選択した場合は、クライアント SDK、IBM Java Development Kit、および Java クライアントのサイズを一度追加します。

表 2. AIX での IBM Security Directory Server 機能および相互前提条件ソフトウェアのディスク・スペース要件

インストール可能な機能	インストール用のディスク・スペース (MB 単位)
クライアント・ソフトウェア開発キット	8 MB
IBM Java Development Kit	200 MB
Java クライアント	91 MB
デPLOYされた Web 管理ツール (WebSphere Application Server 組み込みバージョンおよび WebSphere Application Server 組み込みバージョンにデPLOYされた Web 管理ツールを含む)	443 MB
既存の WebSphere Application Server 組み込みバージョンまたは WebSphere Application Server 内の Web 管理ツールのデPLOYメント	500 MB
SSL Web 管理ツール	51 MB
Base Server	39 MB
プロキシ・サーバー (クライアント SDK、Java クライアント、および Base Server のサイズを追加してください)	4 MB
完全な Directory Server (クライアント SDK、Java クライアント、および Base Server のサイズを追加してください)	12 MB
IBM DB2	1250 MB
IBM Global Security Kit	16 MB

## Linux のディスク・スペース要件

注: インストールでプロキシ・サーバー機能または完全な Directory Server 機能を選択した場合は、クライアント SDK、IBM Java Development Kit、および Java クライアントのサイズを一度追加します。

表 3. Linux での IBM Security Directory Server 機能および相互前提条件ソフトウェアのディスク・スペース要件

インストール可能な機能	インストール用のディスク・スペース (MB 単位)
クライアント・ソフトウェア開発キット	9 MB
IBM Java Development Kit	200 MB
Java クライアント	166 MB
デプロイされた Web 管理ツール (WebSphere Application Server 組み込みバージョンおよび WebSphere Application Server 組み込みバージョンにデプロイされた Web 管理ツールを含む)	443 MB
既存の WebSphere Application Server 組み込みバージョンまたは WebSphere Application Server 内の Web 管理ツールのデプロイメント	375 MB
Base Server	32 MB
プロキシ・サーバー (クライアント SDK、Java クライアント、および Base Server のサイズを追加してください)	40 MB
完全な Directory Server (クライアント SDK、Java クライアント、および Base Server のサイズを追加してください)	8 MB
IBM DB2 (System x Linux)	460 MB
IBM DB2 (System zLinux)	670 MB
IBM DB2 (System i および System p Linux)	520 MB
IBM DB2 (AMD64/EM64T Linux)	1300 MB
IBM Global Security Kit	40 MB

注: (Installation Manager ベースのインストーラーに適用されます。) 共有リソース・ディレクトリーに、200 MB のハード・ディスク・スペースが必要です。IBM Security Directory Server のインストール・ディレクトリーに、さらに 200 MB のハード・ディスク・スペースが必要です。

システムのデフォルトの temp ディレクトリーのスペース所要量: DB2 をインストール対象として選択した場合は、temp ディレクトリーに 2048 MB + 500 MB のフリー・スペースが必要です。DB2 をインストールしない場合は、temp ディレクトリーに 500 MB のフリー・スペースが必要です。

## Solaris のディスク・スペース要件

注: サーバーとプロキシ・サーバー機能をインストール対象として選択した場合は、C クライアント、IBM Java Development Kit、および Java クライアントのサイズを一度追加してください。

表 4. Solaris での IBM Security Directory Server 機能および相互前提条件ソフトウェアのディスク・スペース要件

インストール可能な機能	インストール用のディスク・スペース (MB 単位)	注釈
C クライアント	11 MB	
IBM Java Development Kit		
Java クライアント	145 MB	
サーバー	47 MB	C クライアントおよび Java クライアントのサイズを追加
プロキシ・サーバー	40 MB	C クライアントおよび Java クライアントのサイズを追加
Web 管理ツール	470 MB	WebSphere Application Server 組み込みバージョン、および WebSphere Application Server 組み込みバージョンにデプロイされた Web 管理ツールを含む
IBM DB2	1155 MB	
IBM Global Security Kit	34 MB	

## HP-UX のディスク・スペース要件

表 5. HP-UX での IBM Security Directory Server 機能および相互前提条件ソフトウェアのディスク・スペース要件

インストール可能な機能	インストール用のディスク・スペース (MB 単位)
C クライアント	26 MB
IBM Java Development Kit	
Java クライアント	172 MB
IBM Global Security Kit	41 MB

## インストール・メディアの準備

IBM Security Directory Server 製品パッケージには、IBM Security Directory Server、相互前提条件ソフトウェア、およびインストール・プログラムが含まれています。インストール・メディアは、インストール DVD またはパスポート・アドバンテージ Web サイトから入手できます。

IBM Security Directory Server 製品は、.zip、.tar、および .iso の 3 つのファイル・タイプで入手できます。.iso ファイルには、複数の .zip または .tar ファイルに対応する複数のファイルが含まれています。

表 6. 様々なオペレーティング・システムにおいて以下の形式で入手できる IBM Security Directory Server 製品

AIX、Linux、Solaris および Windows	AIX、Linux、Solaris および HP-UX	Windows
ISO イメージ (.iso ファイル)	テープ・アーカイブ・ファイル (.tar ファイル)	アーカイブ・ファイル (.zip ファイル)

インストール・メディアとして DVD を使用する場合、以下のいずれかのタスクを実行する必要があります。

- ご使用のオペレーティング・システム用の IBM Security Directory Server 製品イメージから DVD イメージを作成します。
- コンピューターのハード・ディスク上に IBM Security Directory Server 製品イメージを保管し、必要な場合にこれをマウントします。

製品のアーカイブ・ファイルをダウンロードするには、以下の要件を満たしている必要があります。

1. 必要なすべてのアーカイブ・ファイルを、同一のディレクトリーにダウンロードします。パス名にスペースが含まれているディレクトリー・ロケーションにアーカイブ・ファイルをダウンロードすることは避けてください。
2. ディレクトリー・パスにスペースを含まない同一のディレクトリーに、すべてのアーカイブ・ファイルを圧縮解除します。インストール可能ファイルのディレクトリー・パスは、スペースを含んではいけません。

IBM Security Directory Server 製品をパスポート・アドバンテージからダウンロードするには、『パスポート・アドバンテージからのソフトウェアのダウンロード』を参照してください。

インストール・メディアの準備ができれば、ご使用のオペレーティング・システムのための前提ソフトウェア要件を満たす必要があります。16 ページの『インストールの前提条件』を参照してください。

## パスポート・アドバンテージからのソフトウェアのダウンロード

IBM Security Directory Server をインストールするには、IBM パスポート・アドバンテージからソフトウェアをダウンロードする必要があります。

### 始める前に

IBM パスポート・アドバンテージにアクセスするには、登録してお客様番号とパスワードを取得する必要があります。

### 手順

1. IBM パスポート・アドバンテージの Web サイト ([http://www.ibm.com/software/howtobuy/passportadvantage/pao\\_customers.htm](http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm)) にアクセスします。
2. 「Customer sign in」をクリックします。
3. 「IBM ID」フィールドに IBM ID を入力します。
4. 「Password」フィールドにパスワードを入力します。
5. 「Sign in」をクリックします。

- 指示に従って、IBM Security Directory Server ソフトウェアをダウンロードします。

## ダウンロードしたファイルのディレクトリー構造

IBM Security Directory Server のインストール・ファイルをダウンロードした後で、ディレクトリー構造を検証する必要があります。

### Windows パッケージのディレクトリー構造

Windows パッケージの Security Directory Server 6.3.1 のファイル名は、以下のとおりです。

DVD イメージ: sds631-win.iso

.zip ファイル:

- sds631-win-base.zip (Security Directory Server 6.3.1 クライアントおよびサーバー)
- sds631-win-db2.zip (DB2 V9.7)
- sds631-win-ewas.zip (WebSphere Application Server 7.0.0.29 組み込みバージョン)
- sds631-win-gskit.zip (GSKit 8.0)
- sds631-win-jdk.zip (IBM Java Development Kit)
- sds631-win-IM.zip (IBM Installation Manager)

DVD を作成、または .zip ファイルを解凍すると、ディレクトリー構造は次のようになります。

¥sdsV6.3.1 (unzip されたファイルの最上位ディレクトリー)

- ibm\_gskit¥ (GSKit)
- license¥ (Security Directory Server およびその他の提供される製品のライセンス)
- quickstart¥ (英語またはその他の言語のクイック・スタート・ガイド)
- entitlement¥ (プロキシ・サーバーの資格ファイル)
- entitlement.txt
- tools¥ (migbkup などのツール)
- migbkup.bat
- ibm\_db2\_32bit¥ (DB2)
- ibm\_db2\_64bit¥ (DB2)
- ibm\_ewas\_32bit¥ (WebSphere Application Server 組み込みバージョン)
- ibm\_ewas\_64bit¥ (WebSphere Application Server 組み込みバージョン)
- ibm\_im\_32bit¥ (IBM Installation Manager)
- ibm\_im\_64bit¥ (IBM Installation Manager)
- ibm\_jdk¥ (IBM Java Development Kit)
- ibm\_sds¥ (インストーラー・ファイル)
- atoc
- files
- native
- Offerings
- plugins
- ShareableEntities
- build.properties
- repository.config
- repository.xml

- launchpad¥
- SilentInstallScripts¥ (サイレント・インストールで使用される応答ファイル)
- autorun.inf
- imLauncherWindows.bat
- launchpad.exe
- launchpad.ini
- launchpad64.exe
- launchpad64.ini
- sds\_install.xml
- write\_sds\_path.bat

## Windows クライアントのみのパッケージ

.zip ファイル:

- sds631-win-client.zip (Security Directory Server 6.3.1 クライアント)

.zip ファイルを解凍すると、ディレクトリー構造は次のようになります。

¥sdsV6.3.1 (unzip されたファイルの最上位ディレクトリー)

- ibm\_gskit¥ (GSKit 8)
- jdk¥ (IBM Java Development Kit)
- ibm\_im\_32bit (IBM Installation Manager)
- ibm\_im\_64bit (IBM Installation Manager)
- ibm\_sds¥ (インストーラー・ファイル)
- launchpad¥
- SilentInstallScripts¥
- autorun.inf
- license¥ (Security Directory Server およびその他の提供される製品のライセンス)
- quickstart¥ (英語またはその他の言語のクイック・スタート・ガイド)
- 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

## AIX パッケージのディレクトリー構造

AIX パッケージの Security Directory Server 6.3.1 のファイル名は、以下のとおりです。

DVD イメージ: sds631-aix-ppc64.iso

.tar ファイル:

- tds63-aix-ppc64-base.tar (Security Directory Server 6.3.1 クライアントおよびサーバー)
- sds631-aix-ppc64-db2.tar (DB2 V9.7)
- sds631-aix-ppc64-ewas.tar (WebSphere Application Server 7.0.0.29 組み込みバージョン)
- 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)

DVD を作成、または .tar ファイルを解凍すると、ディレクトリー構造は次のようになります。

- /sdsV6.3.1 (untar されたファイルの最上位ディレクトリー)
  - license/ (Security Directory Server およびその他の提供される製品のライセンス)
  - quickstart/ (英語またはその他の言語のクイック・スタート・ガイド)
  - ibm\_im (IBM Installation Manager)
  - ibm\_db2/ (DB2)
  - ibm\_ewas/ (WebSphere Application Server 組み込みバージョン)
  - ibm\_gskit/ (GSKit 8)
  - ibm\_jdk/ (IBM Java Development Kit)
  - ibm\_sds/ (インストーラー・ファイル)
  - atoc/
  - files/
  - native/
  - Offerings/
  - plugins/
  - ShareableEntities
  - build.properties
  - repository.config
  - repository.xml
- tools/ (migbkup などのツール)
- launchpad/
- SilentInstallScripts/
- launchpad.sh
- sds\_install.xml
- write\_sds\_path.sh
- entitlement/ (プロキシ・サーバーの資格ファイル)
- native / (ネイティブ・パッケージ)

## AIX クライアントのみのパッケージ

.zip ファイル:

- sds631-aix-ppc64-client.tar (Security Directory Server 6.3.1 クライアント)

.zip ファイルを解凍すると、ディレクトリー構造は次のようになります。

- ¥sdsV6.3.1 (unzip されたファイルの最上位ディレクトリー)
  - ibm\_gskit¥ (GSKit 8)
  - ibm\_jdk¥ (IBM Java Development Kit)
  - ibm\_im¥ (IBM Installation Manager)
  - ibm\_sds¥ (インストーラー・ファイル)
  - launchpad¥
  - SilentInstallScripts¥
  - autorun.inf
  - license¥ (Security Directory Server およびその他の提供される製品のライセンス)

- quickstart¥ (英語またはその他の言語のクイック・スタート・ガイド)
- ibm\_im¥ (IBM Installation Manager)
- imLauncherWindows.bat
- launchpad.exe
- launchpad.ini
- sds\_install.xml
- write\_sds\_path.bat

## Linux x86\_64 サーバー・パッケージのディレクトリー構造

Linux x86\_64 サーバー・パッケージの Security Directory Server 6.3.1 のファイル名は、以下のとおりです。

DVD イメージ: sds631-linux-x86-64.iso

.tar ファイル:

- sds631-linux-x86-64-base.tar (IBM Security Directory Server 6.3.1 クライアントおよびサーバー)
- sds631-linux-x86-64-IM.tar (IBM Installation Manager)
- sds631-linux-x86-64-gskit.tar (GSKit 8)
- sds631-linux-x86-64-db2.tar (DB2 vV9.7)
- sds631-linux-x86-64-ewas.tar (WebSphere Application Server 7.0.0.29 組み込みバージョン)
- sds631-linux-x86-64-jdk.tar (IBM Java Development Kit)

DVD を作成、または .tar ファイルを解凍すると、ディレクトリー構造は次のようになります。

/sdsV6.3.1 (untar されたファイルの最上位ディレクトリー)

- license/ (Security Directory Server およびその他の提供される製品のライセンス)
- quickstart/ (英語またはその他の言語のクイック・スタート・ガイド)
- ibm\_im (IBM Installation Manager)
- ibm\_db2/ (DB2)
- ibm\_ewas/ (WebSphere Application Server 組み込みバージョン)
- ibm\_gskit/ (GSKit 8)
- ibm\_jdk/ (IBM Java Development Kit)
- ibm\_sds/ (インストーラー・ファイル)
- atoc/
- files/
- native/
- Offerings/
- plugins/
- ShareableEntities
- build.properties
- repository.config
- repository.xml
- tools/ (migbkup などのツール)
- launchpad/
- SilentInstallScripts/
- launchpad.sh
- sds\_install.xml

- write\_sds\_path.sh
- entitlement/ (プロキシ・サーバーの資格ファイル)
- native/ (ネイティブ・パッケージ)

## Linux x86\_64 クライアントのみのパッケージ

.zip ファイル:

- sds631-linux-x86-64-client.tar (Security Directory Server 6.3.1 クライアント)

.zip ファイルを解凍すると、ディレクトリー構造は次のようになります。

¥sdsV6.3.1 (unzip されたファイルの最上位ディレクトリー)

- ibm\_jdk¥ (IBM Java Development Kit)
- ibm\_im (IBM Installation Manager)
- ibm\_sds¥ (インストーラー・ファイル)
- launchpad¥
- SilentInstallScripts¥
- autorun.inf
- license¥ (Security Directory Server およびその他の提供される製品のライセンス)
- quickstart¥ (英語またはその他の言語のクイック・スタート・ガイド)
- ibm\_im¥ (IBM Installation Manager)
- imLauncherWindows.bat
- launchpad.exe
- launchpad.ini
- sds\_install.xml
- write\_sds\_path.bat

## Linux x86 サーバー・パッケージのディレクトリー構造

Linux x86 サーバー・パッケージの Security Directory Server 6.3.1 のファイル名は、以下のとおりです。

DVD イメージ: sds631-linux-x86.iso

.tar ファイル:

- sds631-linux-x86-base.tar (IBM Security Directory Server 6.3.1 クライアントおよびサーバー)
- sds631-linux-x86-gskit.tar (GSKit 8)
- sds631-linux-x86-db2.tar (DB2 v9.7)
- sds631-linux-x86-ewas.tar (WebSphere Application Server 7.0.0.29 組み込みバージョン)
- sds631-linux-x86-jdk.tar (IBM Java Development Kit)

DVD を作成、または .tar ファイルを解凍すると、ディレクトリー構造は次のようになります。

/sdsV6.3.1 (untar されたファイルの最上位ディレクトリー)

- appsrv/ (WebSphere Application Server 組み込みバージョン)
- db2 (DB2)
- gskit/ (GSKit 8)
- jdk/ (IBM Java Development Kit)
- ids\_detectGskitVersion
- idsinstall\_i
- idsNativeInstall.sh

- images/ (ネイティブ・イメージ)
- license (Security Directory Server およびその他の製品のライセンス)
- responseFile.txt (応答ファイル)

## Linux x86 クライアントのみのパッケージ

.zip ファイル:

- sds631-linux-x86-client.tar (Security Directory Server 6.3.1 クライアント)

.zip ファイルを解凍すると、ディレクトリー構造は次のようになります。

¥sdsV6.3.1 (unzip されたファイルの最上位ディレクトリー)

- gskit/(GSKit 8)
- image/
- license/ (Security Directory Server およびその他の製品のライセンス)
- jdk (IBM Java Development Kit)

## Linux ppc サーバー・パッケージのディレクトリー構造

Linux ppc サーバー・パッケージの Security Directory Server 6.3.1 のファイル名は、以下のとおりです。

DVD イメージ: sds631-linux-ppc64.iso

.tar ファイル:

- sds631-linux-ppc64-base.tar (IBM Security Directory Server 6.3.1 クライアントおよびサーバー)
- sds631-linux-ppc64-gskit.tar (GSKit 8)
- sds631-linux-ppc64-db2.tar (DB2 V9.7)
- sds631-linux-ppc64-ewas.tar (WebSphere Application Server 7.0.0.29 組み込みバージョン)
- sds631-linux-ppc64-jdk.tar (IBM Java Development Kit)

DVD を作成、または .tar ファイルを解凍すると、ディレクトリー構造は次のようになります。

/sdsV6.3.1 (untar されたファイルの最上位ディレクトリー)

- appsrv/ (WebSphere Application Server 組み込みバージョン)
- db2 (DB2)
- gskit/ (GSKit 8)
- jdk/ (IBM Java Development Kit)
- ids\_detectGskitVersion
- idsinstall\_i
- idsNativeInstall.sh
- images/ (ネイティブ・イメージ)
- license (Security Directory Server およびその他の製品のライセンス)
- responseFile.txt (応答ファイル)

## Linux ppc クライアントのみのパッケージ

.zip ファイル:

- sds631-linux-ppc64-client.tar (Security Directory Server 6.3.1 クライアント)

.zip ファイルを解凍すると、ディレクトリー構造は次のようになります。

- ¥sdsV6.3.1 (unzip されたファイルの最上位ディレクトリー)
- gskit/(GSKit 8)
- image/
- license/ (Security Directory Server およびその他の製品のライセンス)
- jdk (IBM Java Development Kit)

## Linux s390 サーバー・パッケージのディレクトリー構造

Linux s390 サーバー・パッケージの Security Directory Server 6.3.1 のファイル名は、以下のとおりです。

DVD イメージ: sds631-linux-s390x.iso

.tar ファイル:

- sds631-linux-s390x-base.tar (IBM Security Directory Server 6.3.1 クライアントおよびサーバー)
- sds631-linux-s390x-gskit.tar (GSKit 8)
- sds631-linux-s390x-db2.tar (DB2 V9.7)
- sds631-linux-s390x-ewas.tar (WebSphere Application Server 7.0.0.29 組み込みバージョン)
- sds631-linux-s390x-jdk.tar (IBM Java Development Kit)

DVD を作成、または .tar ファイルを解凍すると、ディレクトリー構造は次のようになります。

- /sdsV6.3.1 (untar されたファイルの最上位ディレクトリー)
- appsrv/ (WebSphere Application Server 組み込みバージョン)
- db2 (DB2)
- gskit/ (GSKit 8)
- jdk/ (IBM Java Development Kit)
- ids\_detectGskitVersion
- idsinstall\_i
- idsNativeInstall.sh
- images/ (ネイティブ・イメージ)
- license (Security Directory Server およびその他の製品のライセンス)
- responseFile.txt (応答ファイル)

## Linux s390 クライアントのみのパッケージ

.zip ファイル:

- sds631-linux-s390x-client.tar (Security Directory Server 6.3.1 クライアント)

.zip ファイルを解凍すると、ディレクトリー構造は次のようになります。

- ¥sdsV6.3.1 (unzip されたファイルの最上位ディレクトリー)
- gskit/(GSKit 8)
- image/
- license/ (Security Directory Server およびその他の製品のライセンス)
- jdk (IBM Java Development Kit)

## Solaris x86\_64 サーバー・パッケージのディレクトリー構造

Solaris x86\_64 サーバー・パッケージの Security Directory Server 6.3.1 のファイル名は、以下のとおりです。

DVD イメージ: sds631-solaris-x86-64.iso

.tar ファイル:

- sds631-solaris-x86-64-base.tar (IBM Security Directory Server 6.3.1 クライアントおよびサーバー)
- sds631-solaris-x86-64-gskit.tar (GSKit 8)
- sds631-solaris-x86-64-db2.tar(DB2 v9.7)
- sds631-solaris-x86-64-ewas.tar (WebSphere Application Server 7.0.0.29 組み込みバージョン)
- sds631-solaris-x86-64-jdk.tar (IBM Java Development Kit)

DVD を作成、または .tar ファイルを解凍すると、ディレクトリー構造は次のようになります。

/sdsV6.3.1 (untar されたファイルの最上位ディレクトリー)

- appsrv/ (WebSphere Application Server 組み込みバージョン)
- db2 (DB2)
- gskit/ (GSKit 8)
- jdk/ (IBM Java Development Kit)
- ids\_detectGskitVersion
- idsinstall\_i
- idsNativeInstall.sh
- images/ (ネイティブ・イメージ)
- license (Security Directory Server およびその他の製品のライセンス)
- responseFile.txt (応答ファイル)

## **Solaris x86\_64 クライアントのみのパッケージ**

.zip ファイル:

- sds631-solaris-x86-64-client.tar (Security Directory Server 6.3.1 クライアント)

.zip ファイルを解凍すると、ディレクトリー構造は次のようになります。

¥sdsV6.3.1 (unzip されたファイルの最上位ディレクトリー)

- gskit/(GSKit 8)
- image/
- license/ (Security Directory Server およびその他の製品のライセンス)
- jdk (IBM Java Development Kit)

## **Solaris Sparc サーバー・パッケージのディレクトリー構造**

Solaris Sparc サーバー・パッケージの Security Directory Server 6.3.1 のファイル名は、以下のとおりです。

DVD イメージ:

.tar ファイル:

- sds631-solaris-sparc.iso
- sds631-solaris-sparc-base.tar (IBM Security Directory Server 6.3.1 クライアントおよびサーバー)
- sds631-solaris-sparc-gskit.tar (GSKit 8)
- sds631-solaris-sparc-db2.tar (DB2 v9.7)
- sds631-solaris-sparc-ewas.tar (WebSphere Application Server 7.0.0.29 組み込みバージョン)
- sds631-solaris-sparc-jdk.tar (IBM Java Development Kit)

DVD を作成、または .tar ファイルを解凍すると、ディレクトリー構造は次のようになります。

```
/sdsV6.3.1 (untar されたファイルの最上位ディレクトリー)
- appsrv/ (WebSphere Application Server 組み込みバージョン)
- db2 (DB2)
- gskit/ (GSKit 8)
- jdk/ (IBM Java Development Kit)
- ids_detectGskitVersion
- idsinstall_i
- idsNativeInstall.sh
- images/ (ネイティブ・イメージ)
- license (Security Directory Server およびその他の製品のライセンス)
- responseFile.txt (応答ファイル)
```

### Solaris Sparc クライアントのみのパッケージ

.zip ファイル:  
- sds631-solaris-sparc-client.tar (Security Directory Server 6.3.1 クライアント)

.zip ファイルを解凍すると、ディレクトリー構造は次のようになります。

```
¥sdsV6.3.1 (unzip されたファイルの最上位ディレクトリー)
- gskit/ (GSKit 8)
- image/
- license/ (Security Directory Server およびその他の製品のライセンス)
- jdk (IBM Java Development Kit)
```

---

## インストールの前提条件

IBM Security Directory Server およびその相互前提条件ソフトウェアをインストールするには、オペレーティング・システムの前提条件のインストールが必要な場合があります。前提ソフトウェアは、IBM Security Directory Server およびその相互前提条件ソフトウェアをインストールする前にインストールする必要があります。

### 各種オペレーティング・システムに必要な前提条件パッケージ

IBM Security Directory Server およびその相互前提条件製品のインストールに必要な前提条件パッケージを使用して、コンピューターを更新する必要があります。

AIX、Linux、Solaris、および HP-UX (Itanium) オペレーティング・システムでは、Korn シェルが必要です。SuSE Linux Enterprise Server では、PDKSH が必要です。

IBM Security Directory Server を以下のオペレーティング・システムにインストールするには、以下の前提条件パッケージが必要です。

**AIX** rpm パッケージを AIX にインストールするには、AIX システム用の rpm パッケージ・マネージャーを <ftp://public.dhe.ibm.com/aix/freeSoftware/aixtoolbox/INSTALLPPC/rpm.rte> の Web サイトからダウンロードします。

表 7. AIX オペレーティング・システムに必要な前提条件パッケージ

パッケージ	理由	ダウンロード・アドレス
AIX 用 Mozilla Firefox Web ブラウザー	AIX 上でランチパッドを開くには、サポートされるバージョンのブラウザが存在する必要があります。	AIX 用の Web ブラウザーについて詳しくは、 <a href="http://www.ibm.com/systems/power/software/aix/browsers/">http://www.ibm.com/systems/power/software/aix/browsers/</a> の Web サイトを参照してください。
gtk+ RPM (gtk2-2.10.6-4.aix5.2.ppc.rpm)	Eclipse では、UNIX オペレーティング・システムでのウィンドウ・システム要件が motif から gtk に変更されました。AIX の場合、この Eclipse ウィンドウ・システムの変更により、GUI をサポートするために gtk ライブラリーをインストールすることが必要になりました。IBM Installation Manager の場合、GUI はウィザードの操作モードです。	gtk ライブラリーのインストールについて詳しくは、『Required gtk libraries for Installation Manager on AIX』技術情報 Web サイト ( <a href="http://www.ibm.com/support/docview.wss?uid=swg21631478">http://www.ibm.com/support/docview.wss?uid=swg21631478</a> ) を参照してください。
GNU tar	AIX システム上で IBM Security Directory Server で提供されたアーカイブ・ファイルを圧縮解除するには、GNU ファイル・アーカイブ・プログラムが必要です。オペレーティング・システムに tar プログラムが提供される前に、GNU tar プログラムのパスを設定しておく必要があります。GNU tar プログラムは /opt/freeware/bin ディレクトリーにインストールされ、オペレーティング・システムで提供される tar プログラムは /usr/bin ディレクトリーにインストールされます。/opt/freeware/bin パスを設定するには、 <code>export PATH=/opt/freeware/bin:\$PATH</code> コマンドを実行します。	GNU tar アーカイブ・ファイル (tar) をダウンロードするには、 <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> の Web サイトを参照してください。
X11.adt.lib ファイル・セット	X11.adt.lib ファイル・セットは、idsldap.cljtjava631 および idsldap.webadmin631 パッケージを AIX システムにインストールするための前提条件です。	

表 7. AIX オペレーティング・システムに必要な前提条件パッケージ (続き)

パッケージ	理由	ダウンロード・アドレス
x1C.rte 8.0.0.6 および x1C.aix50.rte 8.0.0.6 以降 のレベル	IBM C++ Runtime Environment Components for AIX では、x1C.rte 8.0.0.6 および x1C.aix50.rte 8.0.0.6 ランタイム・レベル 以降が必要です。	
bos.loc.iso.en_US 5.3.0.0	IBM Security Directory Server バージョン 6.3.1 では、最小 の基本レベルのシステム・ロ ケール・ファイル・セット・ レベル bos.loc.iso.en_US 5.3.0.0 が必要です。	

## PowerPC LE での LDAP クライアントの前提条件

PowerPC LE (リトル・エンディアン) 上で IBM Security Directory Server クライアントを実行するには、PowerPC LE システムに IBM Advance Toolchain バージョン 7.1 をインストールする必要があります。

LDAP クライアントを実行する予定であるか、あるいは提供されたライブラリーにリンクして独自のクライアントを作成するにかかわらず、IBM Advance Toolchain バージョン 7.1 をインストールする必要があります。

ご使用のオペレーティング・システムに対応する IBM Advanced Toolchain バージョン 7.1 をダウンロードしてインストールするには、IBM Advance Toolchain 資料を参照してください。

## idsldap ユーザーおよびグループ

サーバーまたはプロキシ・サーバー機能をインストール対象として選択すると、インストール・プログラムによって idsldap ユーザーおよびグループを作成することができます。

インストール・プログラムは、idsldap ユーザーおよびグループを作成します (これらが存在しない場合)。

**注:** AIX、Linux、および Solaris の場合、オペレーティング・システムのユーティリティーを使用したインストールにより、idsldap ユーザーが作成されます (存在しない場合)。ただし、/home/idsldap ディレクトリー (Linux および AIX の場合) または /export/home/idsldap ディレクトリー (Solaris の場合) が既に存在すると、idsldap ユーザーを作成できない場合があります。したがって、idsldap ユーザーが存在しない場合、idsldap のホーム・ディレクトリーが確実に存在しないようにする必要があります。

idsldap ユーザーおよびグループを制御することが必要な環境の場合、インストール前にこれらを作成することができます。idsldap ユーザーとグループは、以下の要件を満たしている必要があります。

- idsldap ユーザーが idsldap グループのメンバーである必要があります。

- AIX、Linux、および Solaris の場合は、root ユーザーが idsldap グループのメンバーである必要があります。Windows の場合は、管理者が idsldap グループのメンバーである必要があります。
- idsldap ユーザーがホーム・ディレクトリーを持っている必要があります。
- AIX、Linux、および Solaris の場合は、idsldap ユーザーのデフォルト・シェルが Korn シェルである必要があります。
- idsldap ユーザーはパスワードを持つことができますが、必須ではありません。
- idsldap ユーザーは、ディレクトリー・サーバー・インスタンス所有者になることができます。

すべての要件を満たしてから IBM Security Directory Server のインストールを行う必要があります。idsldap ユーザーが存在していても、要件を満たさない場合、プロキシー・サーバー機能のインストールが失敗することもあります。

**注:** インスタンス、ディレクトリー・インスタンス、データベース所有者のユーザー ID 要件について詳しくは、133 ページの『ディレクトリー・サーバー・インスタンスに関連付けられたユーザーとグループ』を参照してください。

ディレクトリー・サーバー・インスタンスを作成する際に、インスタンス管理ツールを使用して、ユーザーとグループを作成できます。また、オペレーティング・システムのユーティリティーを使用して、idsldap ユーザーおよびグループを作成し、これらを正しく設定することもできます。

## 例

以下のオペレーティング・システムのユーティリティーを実行して、idsldap グループ、idsldap ユーザー、パスワードを作成し、idsldap グループのメンバーとして root を追加します。

### AIX システムの場合:

idsldap グループを作成するには、以下のコマンドを実行します。

```
mkgroup idsldap
```

idsldap ユーザー ID を idsldap グループのメンバーとして作成し、Korn シェルをデフォルト・シェルとして設定するには、以下のコマンドを実行します。

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

idsldap ユーザーのパスワードを設定するには、以下のコマンドを実行します。

```
passwd idsldap
```

root ユーザー ID を idsldap グループのメンバーとして追加するには、以下のコマンドを実行します。

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

### Linux システムの場合:

idsldap グループを作成するには、以下のコマンドを実行します。

```
groupadd idsldap
```

idsldap ユーザー ID を idsldap グループのメンバーとして作成し、Korn シェルをデフォルト・シェルとして設定するには、以下のコマンドを実行します。

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

idsldap ユーザーのパスワードを設定するには、以下のコマンドを実行します。

```
passwd idsldap
```

root ユーザー ID を idsldap グループのメンバーとして追加するには、以下のコマンドを実行します。

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

groups root コマンドを使用して、ご使用のコンピューターの *rootgroups* の値を取得することができます。

#### **Solaris システムの場合:**

idsldap グループを作成するには、以下のコマンドを実行します。

```
groupadd idsldap
```

idsldap ユーザー ID を idsldap グループのメンバーとして作成し、Korn シェルをデフォルト・シェルとして設定するには、以下のコマンドを実行します。

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

idsldap ユーザーのパスワードを設定するには、以下のコマンドを実行します。

```
passwd idsldap
```

root ユーザー ID を idsldap グループのメンバーとして追加するには、以下のコマンドを実行します。

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

root が idsldap グループのメンバーになるように root ユーザー ID を変更するには、該当するツールを使用します。

ユーザーおよびグループを追加するコマンドについて詳しくは、オペレーティング・システムの資料を参照してください。

---

## インストール方法

IBM Security Directory Server およびその相互前提条件ソフトウェアのインストールについて、ご使用の環境に最も適した該当のインストール方法を選択する必要があります。

IBM Security Directory Server およびその相互前提条件ソフトウェアをインストールするには、以下の方法を使用できます。

- IBM Installation Manager を使用したインストール
- オペレーティング・システム・コマンド行ユーティリティーを使用したインストール

**注意:**

- 同じコンピューター上で異なるインストール・モードを使用しないでください。  
**IBM Security Directory Server** のインストールの実行は、**IBM Installation Manager** またはオペレーティング・システムのコマンド行ユーティリティーのいずれかを使用する必要がありますが、両方を使用してはいけません。2 つのインストール・モードを混用すると、特定の機能についてのすべての適切なパッケージがインストールに含まれないことがあります。
- **DB2** および **WebSphere Application Server** 組み込みバージョンを、**IBM Installation Manager** によって使用されているそれらのデフォルトのインストール・パスに手動インストールすることは避けてください。そのような手動インストールを行うと、**IBM Installation Manager** を使用してインストール、変更、またはアンインストールを実行した場合に、これらの操作に失敗することがあります。デフォルトのインストール・パスについて詳しくは、30 ページの『デフォルトのインストール・ロケーション』を参照してください。



---

## 第 3 章 IBM Installation Manager を使用したインストール

IBM Installation Manager は、IBM Security Directory Server およびその相互前提条件ソフトウェアをインストールおよび保守するために使用できるツールです。

---

### IBM Installation Manager の概要

IBM Installation Manager は、IBM 製品をインストール、変更、更新、ロールバック、またはアンインストールするための手順を導くインストール・ウィザードです。インストールには、リモートまたはローカルのソフトウェア・リポジトリを使用できます。

IBM Installation Manager は、コンピューター上にインストールした IBM アプリケーションまたはパッケージを、以下の方法で管理する際にも役立ちます。

- インストール内容の記録を保持する
- インストール可能なパッケージを判別して表示する
- 前提条件および相互依存関係を検査する

IBM Installation Manager には、パッケージの保持を容易にする、以下の 6 つのウィザードが含まれます。

- 「インストール」ウィザードは、インストール・プロセスを導きます。一度に 1 つ以上のパッケージをインストールすることが可能です。デフォルト設定を受け入れたり、可能な場合は、設定を変更してカスタムのインストール済み環境を作成したりすることもできます。インストールする前に、ウィザード全体の選択内容の完全な要約が表示されます。
- 「更新」ウィザードは、システムにインストールされたパッケージに適用可能な更新を検索します。ウィザードには更新内容の詳細が表示されます。更新を適用するかどうかが選択することができます。
- 「変更」ウィザードは、インストール済みのパッケージの特定の要素を変更するのに役立ちます。パッケージの初回インストール時に、インストールする機能を選択します。後で他の機能が必要になった場合は、パッケージの変更ウィザードを使用して、その機能をパッケージに追加できます。機能を削除することもできます。
- 「ライセンスの管理」ウィザードは、パッケージのライセンスをセットアップする際に役立ちます。このウィザードを使用して、試用ライセンスを完全なライセンスに変更できます。また、フローティング・ライセンス用にサーバーをセットアップしたり、それぞれのパッケージにどのライセンス・タイプを使用するかを選択したりすることができます。
- 「ロールバック」ウィザードを使用すると、パッケージを前のバージョンに戻す際に役立ちます。
- 「アンインストール」ウィザードは、コンピューターからパッケージを除去します。一度に複数のパッケージをアンインストールできます。

---

## サポートされるオペレーティング・システム

IBM Installation Manager を使用して、IBM Security Directory Server を AIX (ppc64)、Linux (AMD64/EM64T アーキテクチャー)、および Microsoft Windows にインストールすることができます。

以下のセクションでは、IBM Installation Manager を使用して、IBM Security Directory Server をインストールするためにサポートされているオペレーティング・システムのバージョンのリストを示します。

以下のセクションにリストされていないオペレーティング・システムに IBM Security Directory Server をインストールする場合、以下のようになります。

1. オペレーティング・システムのバージョンが、IBM Security Directory Server についてサポートされているかどうか確認します。すべてのサポートされるオペレーティング・システムのリストについては、「*IBM Security Directory Server* 製品概要」を参照してください。
2. サポートされている場合、オペレーティング・システムのコマンド行ユーティリティを使用して、IBM Security Directory Server をインストールできます。

### AIX (ppc64)

- AIX バージョン 6.1
- AIX バージョン 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

---

## IBM Security Directory Server のインストール・パッケージ・タイプ

IBM Security Directory Server のインストール・パッケージを正しく選択するには、選択可能なインストール・パッケージ・タイプを知っておく必要があります。

IBM Installation Manager を使用してインストール可能な IBM Security Directory Server のインストール・パッケージ・タイプは、以下のとおりです。

表 8. IBM Security Directory Server のインストール・パッケージ・タイプとインストール可能な機能

すべての機能	完全版製品インストーラー内の機能	クライアント専用インストーラー内の機能
IBM DB2	はい	いいえ
IBM Global Security Kit	はい	はい
C クライアント	はい	はい
IBM Java Development Kit	はい	はい
Java クライアント	はい	はい
サーバー	はい	いいえ
プロキシ・サーバー	はい	いいえ
Web 管理ツール	はい	いいえ

注: Web 管理ツールをインストールすることを選択した場合、IBM Installation Manager には、WebSphere Application Server 組み込みバージョンをインストールするオプションがあります。

## インストールに関するガイドライン

IBM Installation Manager を使用して IBM Security Directory Server のインストールを開始する前に、いくつかの制限事項について検討する必要があります。

### インストール方法

IBM Security Directory Server のインストール時に、IBM Installation Manager を使用してインストールするか、またはオペレーティング・システムのコマンド行ユーティリティーを使用してインストールするかを選択できます。IBM Security Directory Server パッケージ、機能、およびフィックスパックを今後インストールまたはアンインストールする場合は、システム上で同じインストール方法を使用する必要があります。例えば、IBM Installation Manager を使用して IBM Security Directory Server をインストールする場合、コマンド行ユーティリティーを使用して機能をインストールしたり、製品をアンインストールしたりしないでください。これを行うと、IBM Security Directory Server のセットアップが破損したり使用できなくなったりする場合があります。

### IBM Installation Manager のバージョン

IBM Security Directory Server のインストール用に IBM Installation Manager バージョン 1.7.0 以降がサポートされています。以下のシナリオの場合、IBM Installation Manager の「パッケージのインストール」ページにエラー・メッセージが表示され、インストールを進めることができません。

- 以前のバージョンの IBM Installation Manager を使用して、IBM Security Directory Server のインストールを開始しようとした。
- IBM Security Directory Server のインストールをランチパッド・プログラムから開始したとき、以前のバージョンの IBM Installation Manager が検出された。

### 複数のインストール

同じバージョンの IBM Security Directory Server の複数のコピーを同じシステム上にインストールすることはできません。同じバージョンのインストール・パッケージを再選択すると、IBM Installation Manager から警告メッセージが生成され、インストールを進めることができなくなります。ただし、異なるバージョンの IBM Security Directory Server は、同じシステムに共存できます。

#### AIX および Linux システム上のインストール・ロケーション:

AIX および Linux システムでは、IBM Security Directory Server は事前定義されたロケーションにのみインストールできます。デフォルトでは、このパスは IBM Installation Manager の「インストール・ディレクトリー」フィールドに指定されています。このフィールドは IBM Installation Manager 内で編集可能ですが、デフォルトで指定されているパスを変更すると、「次へ」をクリックしてインストールを進めることができなくなります。IBM Security Directory Server のデフォルト・インストール・パスに戻す必要があります。

この制約事項は Microsoft Windows オペレーティング・システムには適用されません。IBM Security Directory Server は、Microsoft Windows オペレーティング・システム上のあらゆるカスタム・ロケーションにインストールできます。IBM Security Directory Server のカスタム・インストール・ロケーションを選択した場合も、idsinstinfo ディレクトリーと、そこに格納される idsinstances.ldif ファイルは、%SystemDrive% で指定される区画に常に作成されます。IBM Security Directory Server が E: ドライブにインストールされ、オペレーティング・システムが C: ドライブにある場合、以下の変化にご注意ください。

- idsinstinfo ディレクトリーは、E:¥Program Files¥IBM¥ldap ディレクトリーではなく、C: ドライブ (C:¥idsinstinfo) に作成されます。

デフォルトのインストール・ロケーションについては、30 ページの『デフォルトのインストール・ロケーション』を参照してください。

---

## IBM Security Directory Server のコンポーネント

IBM Installation Manager を使用して IBM Security Directory Server をインストールする場合、インストールするコンポーネントを選択できます。IBM Installation Manager には、選択した各コンポーネントの依存関係が表示されます。

以下の IBM Security Directory Server コンポーネントをインストール用に選択できます。

### IBM DB2

IBM DB2 を機能としてインストールできます。サポートされるバージョンの IBM DB2 がインストールされている場合、IBM Security Directory Server パッケージで提供される DB2 をインストールする必要はありません。各種オペレーティング・システムに対してサポートされる DB2 のバージョンについては、「*IBM Security Directory Server 製品概要*」を参照してください。

フル・ディレクトリー・サーバーの場合、DB2 データベースにディレクトリー・データが保管されるため、IBM DB2 が必要です。プロキシー・サーバーには、IBM DB2 は不要です。

### IBM Global Security Kit

IBM Global Security Kit (GSKit) は、IBM Security Directory Server の他の機能と一緒に機能としてインストールできます。GSKit は、Secure Sockets Layer (SSL) または Transport Layer Security (TLS) 通信プロトコルを使用する場合にのみ必要なオプションの機能です。セキュア接続を確立して使用するためには、GSKit をサーバー・システムとクライアント・システムの両方にインストールする必要があります。

### C クライアント

C クライアントは、それ単独か、IBM Security Directory Server の他の機能と一緒に機能としてインストールできます。C クライアント機能には、他の機能に対する依存関係はありません。ただし、サーバーとプロキシー・サーバーの機能は C クライアントに依存しています。サーバーまたはプロキシー・サーバーの機能をインストールすると、C クライアント機能はインストール対象として自動的に選択されます。

C クライアントは、C 言語 LDAP アプリケーションの開発に必要なツールを提供するクライアント・ソフトウェア開発キット (SDK) です。C クライアント・パッケージには、以下のファイルおよびアプリケーションが格納されています。

- 一連の C 言語アプリケーション・プログラミング・インターフェース (API) を提供するクライアント・ライブラリー
- LDAP アプリケーションを構築およびコンパイルするための C ヘッダー・ファイル
- C サーバーおよびクライアント・ユーティリティー
- ソース形式のサンプル・プログラム

### IBM Java Development Kit

IBM Java Development Kit は、それ単独か、IBM Security Directory Server の他の機能と一緒に機能としてインストールできます。IBM Java Development Kit をインストールすることを選択した場合、IBM Installation Manager は、圧縮ファイルを IBM Security Directory Server のインストール・ロケーション内の java サブディレクトリーに解凍します。IBM Java Development Kit は、IBM Java SDK および Java 1.6 SR 14 を提供します。Java サンプル・プログラムをコンパイルしたり、インスタンス管理ツール (`idsxinst`) や構成ツール (`idsxcfg`) などの Java プログラムを実行したりするには、IBM Java Development Kit が必要です。

### Java クライアント

Java クライアントは、それ単独か、IBM Security Directory Server の他の機能と一緒に機能としてインストールできます。Java クライアント機能には、他の機能に対する依存関係はありません。ただし、サーバーとプロキシー・サーバーの機能は Java クライアントに依存しています。サーバーまたはプロキシー・サーバーの機能をインストールすると、Java クライアント機能はインストール対象として自動的に選択されます。

Java クライアントには、IBM Security Directory Server JNDI ツールキットと、Java クライアント・ユーティリティーが含まれています。

### サーバー

サーバーは、IBM Security Directory Server の他の機能と一緒に機能としてインストールできます。サーバー機能は、C クライアント機能および Java クライアント機能に依存しています。サーバー機能をインストール対象として選択すると、C クライアント機能および Java クライアント機能がインストール対象として選択されます。

サーバーは、フル・ディレクトリー・サーバーまたは LDAP サーバーを作成するために必要です。データベース・インスタンスを使用して、フル・ディレクトリー・サーバーを構成する必要があります。これは、データベースに保管されている項目へのアクセスを必要とするクライアント要求を処理します。フル・ディレクトリー・サーバーには、DB2 が必要です。

### プロキシ・サーバー

プロキシ・サーバーは、IBM Security Directory Server の他の機能と一緒に機能としてインストールできます。プロキシ・サーバー機能は、C クライアント機能および Java クライアント機能に依存しています。プロキシ・サーバー機能をインストール対象として選択すると、C クライアント機能および Java クライアント機能がインストール対象として選択されます。

プロキシ・サーバーは、ディレクトリーのフロントエンドとして機能する LDAP サーバーです。これは、ディレクトリー全体に対するクライアント要求を認証し、フル・ディレクトリー・サーバーに要求を送付します。プロキシ・サーバーはサーバー・クラスターまたは分散ディレクトリーのフロントエンドで使用することもでき、これにより、フェイルオーバーおよびロード・バランシングを行うことができます。

### Web 管理ツール

Web 管理ツールは、それ単独か、IBM Security Directory Server の他の機能と一緒に機能としてインストールできます。Web 管理ツールは、Directory Server をリモートで管理する場合に必要なオプションの機能です。Web 管理ツールを使用するには、これをサポート対象バージョンの WebSphere Application Server 組み込みバージョンまたは WebSphere Application Server にデプロイする必要があります。

Web 管理ツールをインストールするときに、Directory Services Markup Language (DSML) ファイルもコンピューターにコピーされます。DSML について詳しくは、279 ページの『付録 A. Directory Services Markup Language (DSML)』を参照してください。

コンソールとして Web 管理ツールを使用すると、次のタイプのディレクトリー・サーバーを管理できます。

- IBM Security Directory Server バージョン 6.3.1
- IBM Security Directory Server バージョン 6.3
- IBM Security Directory Server バージョン 6.2
- IBM Security Directory Server バージョン 6.1
- IBM Security Directory Server バージョン 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

**重要:** z/OS の場合は、ディレクトリー・データの管理がサポートされ、サーバー管理はサポートされません。

#### WebSphere Application Server 組み込みバージョン

Web 管理ツールをインストールすることを選択した場合、WebSphere Application Server 組み込みバージョンをインストールできます。WebSphere Application Server 組み込みバージョンは、Web 管理ツールをデプロイして実行する場合にのみ必要です。サポート対象バージョンの WebSphere Application Server がシステムにインストール済みの場合、WebSphere Application Server 組み込みバージョンをインストールしなくてもかまいません。Web 管理ツールは、システムにインストール済みの既存の WebSphere Application Server または WebSphere Application Server 組み込みバージョンにデプロイできます。

---

## IBM Security Directory Server のインストールのカスタマイズ

製品の使用方法に合わせて IBM Security Directory Server のインストールをカスタマイズできます。

IBM Security Directory Server のインストールは、以下の目的に沿って分類できます。

- 完全な製品
- フル・ディレクトリー・サーバー
- プロキシ・サーバー
- クライアント
- Web 管理ツールを使用したリモート・サーバー管理

表 9. 製品の使用方法に基づいてインストールする IBM Security Directory Server 機能

すべての機能	フル・ディレクトリー・サーバー	プロキシ・サーバー	クライアント	Web 管理ツールを使用したリモート・サーバー管理
IBM DB2	はい	いいえ	いいえ	いいえ
IBM Global Security Kit	はい	はい	はい	いいえ
C クライアント	はい	はい	はい	いいえ
IBM Java Development Kit	はい	はい	はい	いいえ
Java クライアント	はい	はい	はい	いいえ
サーバー	はい	いいえ	いいえ	いいえ

表9. 製品の使用方法に基づいてインストールする IBM Security Directory Server 機能 (続き)

すべての機能	フル・ディレクトリー・サーバー	プロキシ・サーバー	クライアント	Web 管理ツールを使用したりリモート・サーバー管理
プロキシ・サーバー	いいえ	はい	いいえ	いいえ
Web 管理ツール	オプション	オプション	いいえ	はい

注: Web 管理ツールをインストールすることを選択した場合、IBM Installation Manager には、WebSphere Application Server 組み込みバージョンをインストールするオプションがあります。

フル・ディレクトリー・サーバーおよびプロキシ・サーバーとともに、WebSphere Application Server 組み込みバージョンと Web 管理ツールをオプションでインストールすることを選択できます。

## デフォルトのインストール・ロケーション

インストールのために IBM Installation Manager を実行した場合、IBM Security Directory Server およびその相互前提条件ソフトウェアは、事前定義されたインストール・ロケーションにインストールされます。

表10. IBM Security Directory Server、IBM DB2、WebSphere Application Server 組み込みバージョン、および IBM Java Development Kit のデフォルトのインストール・ロケーション。

オペレーティング・システム	IBM Security Directory Server	IBM DB2	WebSphere Application Server 組み込みバージョン	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

AIX および Linux システムでは、IBM Security Directory Server は事前定義されたロケーションにのみインストールできます。デフォルトでは、このパスは IBM Installation Manager の「インストール・ディレクトリー」フィールドに指定されています。このフィールドは IBM Installation Manager 内で編集可能ですが、デフォルトで指定されているパスを変更すると、「次へ」をクリックしてインストールを進めることができなくなります。IBM Security Directory Server のデフォルト・インストール・パスに戻す必要があります。

この制約事項は Microsoft Windows オペレーティング・システムには適用されません。IBM Security Directory Server は、Microsoft Windows オペレーティング・システム上のあらゆるカスタム・ロケーションにインストールできます。IBM Security Directory Server のカスタム・インストール・ロケーションを選択した場合も、idsinstinfo ディレクトリーと、そこに格納される idsinstances.ldif ファイルは、%SystemDrive% で指定される区画に常に作成されます。IBM Security Directory Server が E: ドライブにインストールされ、オペレーティング・システムが C: ドライブにある場合、以下の変化にご注意ください。

- idsinstinfo ディレクトリーは、E:¥Program Files¥IBM¥ldap ディレクトリーではなく、C: ドライブ (C:¥idsinstinfo) に作成されます。

---

## インストール・リポジトリー

インストール・リポジトリーは、インストール用に IBM Security Directory Server パッケージが利用可能なロケーションです。

IBM Security Directory Server は、以下のいずれかのロケーションからインストールできます。

- 製品のセットアップ・ディスク
- インストール・パッケージの電子イメージが格納されているリモート共有ドライブまたはローカル・ディレクトリー

リポジトリーを使用して、以下の方法でインストールを開始できます。

- ランチパッドを使用して、以下の場所からインストールを開始します。
  - 製品のセットアップ・ディスク
  - リモート共有ドライブまたはローカル・ディレクトリーにあるインストール・パッケージの電子イメージ

ランチパッドを使用する場合、インストール・プロセスは、インストール・パッケージを含むリポジトリーのロケーションを使用して既に構成されています。

- IBM Installation Manager を直接開始し、リポジトリー設定を手動で指定します。以下に例を示します。
  - Web サーバー上のリポジトリーの URL
  - 製品パッケージを含むリモート共有ドライブのパス

---

## インストールの開始

IBM Security Directory Server のインストールは、ランチパッドを使用するか、またはリポジトリー設定で設定された IBM Installation Manager を使用して開始することができます。

### ランチパッドを使用したインストールの開始

ランチパッドを使用して、インストール・プロセスを 1 カ所から開始することができます。

## このタスクについて

ランチパッドは、以下のシナリオでインストールを開始する場合に使用できます。

- 製品のセットアップ・ディスクからのインストール
- 製品パッケージの電子イメージが置かれているローカル・ディレクトリーまたはリモート共有ドライブからのインストール

ランチパッドを使用してインストールを開始すると、IBM Installation Manager が自動的にインストールされます (サポート対象バージョンがシステムにインストールされていない場合)。

## 手順

1. インストール・パッケージのルート・ディレクトリーに移動します。
  - IBM Security Directory Server の製品セットアップ・ディスクを使用する場合は、ディスク・ドライブにディスクを挿入します。
  - 製品インストール・パッケージの電子イメージからインストールする場合は、イメージが置かれているディレクトリーに変更します。
2. ランチパッドを開始します。

注: Windows オペレーティング・システムの場合、launchpad の .exe ファイルを右クリックして「管理者として実行」を選択します。

オペレーティング・システム	実行するコマンド:
Windows 32 ビット	launchpad.exe
Windows 64 ビット	launchpad64.exe
AIX および Linux	./launchpad.sh

IBM Security Directory Server のランチパッドが開始され、ウェルカム・ページが表示されます。

3. ウェルカム・ページで、「言語の選択」リストから言語を選択し、「OK」をクリックします。
4. 左側のナビゲーション領域で、「IBM Security Directory Server のインストール」をクリックします。
5. 「インストール」ページで、「IBM Security Directory Server インストーラーの起動」リンクをクリックします。IBM Installation Manager が始動します。
6. 以下のパッケージがインストール対象として選択されていることを確認します。
  - IBM Installation Manager (サポート対象バージョンがシステムにインストールされていない場合にのみリストされます)
  - IBM Security Directory Server
7. IBM Security Directory Server をインストールするための手順を進めます。35 ページの『IBM Installation Manager を使用したインストール』を参照してください。
8. インストールが完了したら、「終了」をクリックします。

## タスクの結果

ランチパッドを使用して IBM Security Directory Server のインストールを開始すると、メディア・パス名を含んだ一時ファイル `sds631.temp` が作成されます。`sds631.temp` ファイルは、オペレーティング・システムに応じて以下のロケーションに作成されます。

### AIX および Linux

`/tmp`

### Microsoft Windows

`TEMP` 変数で設定されるシステムのデフォルトの一時ディレクトリー。

同じバージョンの IBM Security Directory Server の複数のコピーを同じシステム上にインストールすることはできません。同じバージョンのインストール・パッケージを再選択すると、IBM Installation Manager から警告メッセージが生成され、インストールを進めることができなくなります。ただし、異なるバージョンの IBM Security Directory Server は、同じシステムに共存できます。

## 次のタスク

IBM Security Directory Server をインストールするための手順を進めます。 35 ページの『IBM Installation Manager を使用したインストール』を参照してください。

## リポジトリ設定を設定することによるインストールの開始

サポート対象バージョンの IBM Installation Manager がシステムにインストールされている場合は、これを直接始動して、リポジトリ設定を指定することができます。

### 始める前に

IBM Security Directory Server のインストール用に IBM Installation Manager バージョン 1.7.0 以降がサポートされています。以下のシナリオの場合、IBM Installation Manager の「パッケージのインストール」ページにエラー・メッセージが表示され、インストールを進めることができません。

- 以前のバージョンの IBM Installation Manager を使用して、IBM Security Directory Server のインストールを開始しようとした。
- IBM Security Directory Server のインストールをランチパッド・プログラムから開始したとき、以前のバージョンの IBM Installation Manager が検出された。

システムにバージョン 1.7.0 より前の IBM Installation Manager がインストールされている場合は、バージョン 1.7.0 以降にアップグレードする必要があります。以下のいずれかの方法で、必要なバージョンの IBM Installation Manager をインストールできます。

- ランチパッドを使用して IBM Installation Manager のインストールを開始します。詳細については、31 ページの『ランチパッドを使用したインストールの開始』を参照してください。
- 該当するオペレーティング・システム用の IBM Installation Manager バージョン 1.7.0 以降をダウンロードします。IBM Installation Manager のサイレント・モー

ド・インストールについて詳しくは、IBM Installation Manager 資料 (<http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome>) を参照してください。

## このタスクについて

以下のインストール・シナリオでは、リポジトリ設定を設定することでインストールを開始できます。

- IBM Passport Advantage®からダウンロードした製品パッケージが格納されているローカル・ディレクトリまたはリモート共有ドライバーからのインストール。
- Web サーバー上のリポジトリの URL からのインストール。

## 手順

1. IBM Installation Manager を始動します。

### Windows

「スタート」メニューで、「すべてのプログラム」 > 「IBM Installation Manager」 > 「IBM Installation Manager」をクリックします。

### AIX および Linux

コマンド・プロンプトで、以下のコマンドを入力します。IBM Installation Manager が別のロケーションにインストールされている場合は、以下のデフォルト・パスを変更します。

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

2. IBM Installation Manager の「開始」ページで、「ファイル」 > 「設定」をクリックします。
3. 「リポジトリ」ページで、「リポジトリの追加」をクリックします。
4. 「リポジトリの追加」ページで、リポジトリ・ロケーションの URL を入力するか、あるいはそのロケーションを参照してファイル・パスを設定します。
5. 「OK」をクリックします。HTTPS または制限付きリポジトリ・ロケーションを指定した場合は、ユーザー ID とパスワードの入力を求めるプロンプトが表示されます。新規リポジトリ・ロケーションまたは変更されたリポジトリ・ロケーションがリストされます。
6. リポジトリへのアクセスを確認するには、「接続のテスト」をクリックします。
7. 「OK」をクリックして「リポジトリ」ページを終了します。

## タスクの結果

同じバージョンの IBM Security Directory Server の複数のコピーを同じシステム上にインストールすることはできません。同じバージョンのインストール・パッケージを再選択すると、IBM Installation Manager から警告メッセージが生成され、インストールを進めることができなくなります。ただし、異なるバージョンの IBM Security Directory Server は、同じシステムに共存できます。

## 次のタスク

IBM Security Directory Server をインストールするための手順を進めます。『IBM Installation Manager を使用したインストール』を参照してください。

---

## IBM Installation Manager を使用したインストール

IBM Installation Manager を使用して IBM Security Directory Server をインストールします。

### 始める前に

インストールを開始します。

### 手順

1. IBM Installation Manager の「始動」ページで、「インストール」をクリックします。
2. 「パッケージのインストール」ページで、インストール対象の IBM Security Directory Server パッケージを選択します。
3. 「次へ」をクリックします。IBM Installation Manager によって、コンピューターに前提条件のパッケージがあるかどうかチェックされます。
4. コンピューターが前提条件を満たしていない場合は、「検証結果」ページに前提条件が表示されます。
  - a. 前提条件のパッケージをインストールした後に前提条件が満たされているかどうかを確認するには、「ステータスの再チェック (Recheck Status)」をクリックします。前提条件について詳しくは、16 ページの『各種オペレーティング・システムで必要な前提条件パッケージ』を参照してください。
  - b. すべての前提条件が満たされている場合は、「次へ」をクリックします。
5. 「使用条件の条項に同意します」をクリックしてから、「次へ」をクリックします。共有リソース・ディレクトリーのロケーションが表示されます。
6. オプション: デフォルトのパスを使用するか、「共有リソース・ディレクトリー」フィールドでパスを指定します。共有リソース・ディレクトリーは、1 つ以上の製品パッケージ・グループで使用できるようにインストール成果物を保管するディレクトリーです。共有リソース・ディレクトリーは、パッケージの初回インストール時にのみ指定できます。
7. 「次へ」をクリックします。パッケージ・グループ名とデフォルトのインストール・ロケーションが表示されます。「新規パッケージ・グループの作成」オプションがデフォルトで選択されます。IBM Security Directory Server のインストールでは、このオプションのみがサポートされます。パッケージ・グループとは、各パッケージが同じグループに属する他のパッケージとリソースを共用するディレクトリーを表します。パッケージ・グループには、自動的に名前が割り当てられます。

### 制約事項:

AIX および Linux システムでは、IBM Security Directory Server は事前定義されたロケーションにのみインストールできます。デフォルトでは、このパスは IBM Installation Manager の「インストール・ディレクトリー」フィールドに指

定されています。このフィールドは IBM Installation Manager 内で編集可能ですが、デフォルトで指定されているパスを変更すると、「次へ」をクリックしてインストールを進めることができなくなります。IBM Security Directory Server のデフォルト・インストール・パスに戻す必要があります。

各種オペレーティング・システムのデフォルトのインストール・ロケーションについては、30 ページの『デフォルトのインストール・ロケーション』を参照してください。

この制約事項は Microsoft Windows オペレーティング・システムには適用されません。IBM Security Directory Server は、Microsoft Windows オペレーティング・システム上のあらゆるカスタム・ロケーションにインストールできます。IBM Security Directory Server のカスタム・インストール・ロケーションを選択した場合も、idsinstinfo ディレクトリーと、そこに格納される idsinstances.ldif ファイルは、%SystemDrive% で指定される区画に常に作成されます。IBM Security Directory Server が E: ドライブにインストールされ、オペレーティング・システムが C: ドライブにある場合、以下の変化にご注意ください。

- idsinstinfo ディレクトリーは、E:%Program Files%IBM%ldap ディレクトリーではなく、C: ドライブ (C:%idsinstinfo) に作成されます。

8. 「次へ」をクリックします。
9. 「パッケージのインストール」ページで、必要な機能を選択します。選択した機能の従属、または他の機能への依存関係を表示するには、「依存関係の表示」チェック・ボックスを選択します。

表 11. 完全版製品パッケージまたはクライアント専用パッケージでインストール対象として選択できる IBM Security Directory Server の機能

すべての機能	インストールの依存関係	完全版製品パッケージ内の機能	クライアント専用パッケージ内の機能
IBM DB2	なし	はい	いいえ
IBM Global Security Kit	なし	はい	はい
C クライアント	なし	はい	はい
IBM Java Development Kit	なし	はい	はい
Java クライアント	なし	はい	はい
サーバー	C クライアント Java クライアント	はい	いいえ
プロキシ・サーバー	C クライアント Java クライアント	はい	いいえ
Web 管理ツール	なし	はい	いいえ

10. 「次へ」をクリックします。
11. IBM DB2 機能をインストール対象として選択する場合は、「**IBM DB2**」をクリックし、以下のいずれかのアクションを実行します。
  - IBM DB2 をインストールするには、以下のアクションを実行します。
    - a. 「**DB2 のインストール**」をクリックします。

- b. 「**DB2 インストール可能ファイルのパス**」フィールドに、DB2 インストール可能ファイルのパス名を指定します。「参照」をクリックして、パスを指定することもできます。
  - c. Windows の場合は、「**ユーザー名**」フィールドに、DB2ADMNS グループまたは DB2USERS グループに必要なシステム・ユーザー ID を入力します。このユーザー ID を使用して、ローカルの DB2 アプリケーションとツールをコンピューターで実行することができます。このユーザー ID が存在しない場合は、インストール・プログラムによってユーザー・アカウントが作成されます。
  - d. Windows の場合は、「**パスワード**」フィールドにこのユーザー ID のパスワードを入力します。このパスワードがコンピューターで設定されているパスワード・ポリシーに適合しない場合は、インストールが失敗することがあります。
  - e. Windows の場合は、「**確認パスワード**」フィールドにユーザー ID のパスワードを入力します。
  - f. 「**次へ**」をクリックします。
- サポートされるバージョンの IBM DB2 がコンピューターにインストールされている場合は、以下のいずれかのアクションを実行します。
    - a. 既存の IBM DB2 バージョンを使用して続行する場合は、「**既存の DB2 を使用して続行**」をクリックします。

**重要:** インストール中に既存の DB2 を使用して続行するように指定すると、IBM Installation Manager によって、そのレジストリーが DB2 機能項目で更新されます。
    - b. リストから、IBM Security Directory Server で使用する DB2 のサポート対象のバージョンを選択します。
    - c. 「**次へ**」をクリックします。
12. IBM Global Security Kit 機能をインストール対象として選択する場合は、「**IBM Global Security Kit**」をクリックし、以下のいずれかのアクションを実行します。
- コンピューターに GSKit バージョン 8.0 以降がインストールされていない場合は、以下のアクションを実行します。
    - a. 「**GSKit のインストール**」をクリックします。
    - b. 「**GSKit インストール可能ファイルのパス**」フィールドに、GSKit インストール可能ファイルのパス名を指定します。「参照」をクリックして、パスを指定することもできます。

**注:** 指定するパスには、64 ビットと 32 ビットの両方の GSKit インストール可能ファイルが含まれている必要があります。
    - c. 「**次へ**」をクリックします。
  - コンピューターに GSKit バージョン 8.0 以降がインストールされている場合は、以下のアクションを実行します。
    - a. 既存の GSKit バージョンを使用して続行する場合は、「**既存の GSKit を使用して続行**」をクリックします。

**重要:** インストール中に既存の GSKit を使用して続行するように指定すると、IBM Installation Manager によって、そのレジストリーが GSKit 機能項目で更新されます。

- b. 「次へ」をクリックします。
13. IBM Java Development Kit 機能をインストール対象として選択する場合は、「**IBM Java Development Kit**」をクリックし、以下の手順を実行します。
    - a. 「**IBM Java Development Kit**」フィールドで、JDK 圧縮ファイルのファイル名をパス名とともに指定します。「参照」をクリックして、パスを指定することもできます。
    - b. 「次へ」をクリックします。
  14. Web 管理ツール機能をインストール対象として選択する場合は、「**Web 管理ツール**」をクリックし、以下の手順を実行します。
    - a. WebSphere Application Server 組み込みバージョンをインストールするには、以下のアクションを実行します。
      - 1) 「**WebSphere Application Server 組み込みバージョンのインストール**」を選択します。
      - 2) 「**WebSphere Application Server 組み込みバージョンのインストール可能ファイルのパス**」フィールドに、WebSphere Application Server 組み込みバージョンのインストール可能ファイルのパス名を指定します。「参照」をクリックして、パスを指定することもできます。
    - b. Web 管理ツールをデプロイするには、以下のアクションのいずれかを実行します。
      - デフォルトのインストール・パスにある WebSphere Application Server 組み込みバージョンにデプロイする場合は、「**デフォルトの WebSphere Application Server 組み込みバージョンにデプロイ**」をクリックします。
- 注:** 前バージョンの Web 管理ツールが存在する場合は、以下の条件が満たされていれば、インストール・プログラムによってそのバージョンが現行バージョンに移行されます。
- 1) 前バージョンの Web 管理ツールおよび WebSphere Application Server 組み込みバージョンがデフォルトのインストール・パスにインストールされている。
  - 2) 前バージョンの Web 管理ツールが、デフォルトのインストール・パスにある WebSphere Application Server 組み込みバージョンにデプロイされている。
  - 3) IBM Security Directory Server バージョン 6.1、6.2、または 6.3 で提供されている Web 管理ツールが移行の対象としてサポートされている。
- カスタム・インストール・パスにある WebSphere Application Server または WebSphere Application Server 組み込みバージョンにデプロイする場合は、「**既存の WebSphere Application Server にデプロイ**」をクリックします。

- 1) 「**WebSphere Application Server または WebSphere Application Server 組み込みバージョンのインストール・パス**」フィールドで、既存の Web アプリケーション・サーバーのインストール・パスを指定します。
  - サポートされる Web アプリケーション・サーバーに後から Web 管理ツールをデプロイする場合は、「**後で手動でデプロイ**」をクリックします。
15. 「**次へ**」をクリックします。インストール前の要約情報として、インストール・ロケーション、パッケージのリスト、リポジトリ情報などが表示されます。
16. 要約情報を確認して、「**インストール**」をクリックします。インストールが開始し、進行状況表示バーが表示されます。インストールが完了すると、インストール後の要約ページが表示されます。
17. 「**ログ・ファイルの表示**」リンクをクリックして、インストールが正常に終了したことを確認します。詳細については、49 ページの『第 5 章 IBM Installation Manager のログ・ファイル』を参照してください。
18. プログラムの始動に関して、以下のいずれかのアクションを実行します。
  - インスタンス管理ツールを始動するには、「**インスタンス管理ツール (idsxinst)**」をクリックします。
  - どのプログラムも始動しない場合は、「**なし**」をクリックします。
19. 「**完了**」をクリックします。
20. 「**ファイル**」 > 「**終了**」をクリックします。

## タスクの結果

インストールが正常に終了すると、IBM Security Directory Server がインストール・ロケーションにインストールされます。デフォルトのインストール・ロケーションについては、30 ページの『デフォルトのインストール・ロケーション』を参照してください。選択した機能でインストールが失敗した場合は、IBM Security Directory Server パッケージのインストールがロールバックされます。

## 次のタスク

IBM Security Directory Server がインストールされたら、以下のアクションを実行する必要があります。

- IBM Security Directory Server を完全なディレクトリー・サーバーとして使用する場合は、ディレクトリー・サーバー・インスタンスを作成してください。詳細については、149 ページの『デフォルトのディレクトリー・サーバー・インスタンスの作成』を参照してください。
- IBM Security Directory Server をプロキシ・サーバーとして使用するには、プロキシ・サーバー・インスタンスを作成してください。詳細については、160 ページの『カスタム設定を使用したプロキシ・サーバー・インスタンスの作成』を参照してください。

---

## サイレント・モード・インストール

サイレント・モード・インストールを使用して、手操作による介入を行うことなく IBM Security Directory Server を複数のシステムにインストールできます。

サイレント・モード・インストールを実行するには、以下の作業を行う必要があります。

1. IBM Installation Manager をインストールします (存在しない場合)。
2. デフォルトの応答ファイルを使用するか、カスタマイズされた応答ファイルを記録します。
3. パッケージをインストールします。

## サイレント・インストールの応答ファイル

サイレント・モード・インストールでは、ユーザー・インターフェースは使用できません。応答ファイルをインストールの入力として使用します。応答ファイルは、サイレント・インストールを実行するために必要なデータを含む XML ファイルです。

### カスタマイズされた応答ファイルの記録

以下のタスクのための応答ファイルを記録することができます。

- パッケージのインストール
- パッケージの変更
- パッケージのアンインストール

応答ファイルを記録するには、IBM Installation Manager を使用して、ユーザー・インターフェース・モードで設定およびインストール・アクションを記録する必要があります。サイレント・インストール用の応答ファイルを最初に記録するときに、**-skipInstall agentDataLocation** パラメーターを使用して、パッケージをインストールしないことを選択できます。

*agentDataLocation* ロケーションには、製品をインストールするためのデータが保管されます。製品のサイレント変更またはアンインストールのための応答ファイルを記録するには、**-skipInstall** パラメーターとともに、同じ *agentDataLocation* ロケーションを使用する必要があります。

複数のインストール・シナリオがある場合、シナリオごとに別の *agentDataLocation* ロケーションを使用して、異なる応答ファイルを記録する必要があります。

サイレント・インストール用の応答ファイルの記録について詳しくは、IBM Installation Manager 資料 (<http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome>) を参照してください。

## サイレント・インストールの検証

インストールが完了したら、サイレント・インストールを検証する必要があります。以下の方法のいずれかを使用して、インストールを検証できます。

- 戻りコードの検査
- ログ・ファイルの検査
- パッケージの検査

## 応答ファイルを使用したサイレント・インストール

IBM Security Directory Server のサイレント・インストールを使用して、手操作による介入なしに必要なパッケージをインストールします。

## 始める前に

IBM Security Directory Server パッケージのサイレント・インストールには、IBM Installation Manager バージョン 1.7.0 以降が必要です。

## このタスクについて

デフォルトの応答ファイルを使用するか、またはカスタマイズした応答ファイルを記録し、サイレント・インストールの入力ファイルとして使用できます。

## 手順

1. 管理者としてシステムにログインします。
2. IBM Installation Manager のインストール・ロケーションにある **IBMIM** コマンドにアクセスします。

オペレーティング・システム	IBMIM コマンドのデフォルト・ロケーション:
Microsoft Windows	C:\Program Files\IBM\InstallationManager\eclipse
AIX および Linux	/opt/IBM/InstallationManager/eclipse

3. オプション: **IBMIM** コマンドを実行して、インストール用の応答ファイルを記録します。

**ヒント:** サンプルのインストール用応答ファイルを使用することもできます。サンプル応答ファイルのデフォルトのロケーションについては、39 ページの『サイレント・モード・インストール』を参照してください。

- a. 製品をインストールせずにインストール・ステップを記録するには、各種オペレーティング・システムで以下のコマンドを実行します。

### Microsoft Windows

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

### AIX および Linux

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

このコマンドによって、IBM Installation Manager が開きます。

- b. IBM Security Directory Server リポジトリを設定します。詳細については、2 (34 ページ)を参照してください。
  - c. IBM Security Directory Server のインストールの記録を実行します。詳細については、35 ページの『IBM Installation Manager を使用したインストール』を参照してください。
4. **imcl** コマンドを実行して、応答ファイルを入力とするサイレント・インストールを開始します。**imcl** コマンドは、<IBM\_Installation\_Manager\_install\_dir>/eclipse/tools にあります。

オペレーティング・システム	実行するコマンド:
Microsoft Windows	<code>imcl.exe input path_name%responseFile.xml -acceptLicense -showProgress</code>
AIX および Linux	<code>./imcl input path_name/responseFile.xml -acceptLicense -showProgress</code>

注: **imcl** コマンドとともに使用できるパラメーターは、他にも多数あります。詳しくは、**imcl** コマンドのヘルプを参照してください。

5. インストールの要約およびログ・ファイルを確認します。

オペレーティング・システム	デフォルトのログ・パス:
Microsoft Windows	<code>C:\ProgramData\IBM\InstallationManager\logs</code>
AIX および Linux	<code>/var/ibm/InstallationManager/logs/</code>

6. IBM Security Directory Server パッケージが必要なレベルであるかどうかを確認します。

オペレーティング・システム	パッケージの確認:
Microsoft Windows	91 ページの『IBM Installation Manager を使用した IBM Security Directory Server 機能の検証』を参照してください。
AIX および Linux	91 ページの『IBM Installation Manager を使用した IBM Security Directory Server 機能の検証』を参照してください。

## タスクの結果

インストールが正常に終了すると、IBM Security Directory Server のインストール・ロケーションに IBM Security Directory Server がインストールされます。デフォルトのインストール・ロケーションについては、30 ページの『デフォルトのインストール・ロケーション』を参照してください。選択した機能でインストールが失敗した場合は、IBM Security Directory Server パッケージのインストールがロールバックされます。

## 次のタスク

注: インストール用の応答ファイルを記録するときにインスタンス管理ツールを開くように選択しても、IBM Security Directory Server のサイレント・インストール後にインスタンス管理ツールは開きません。

サーバー・フィーチャーまたはプロキシ・サーバー・フィーチャーのインストールを選択した場合は、インスタンス管理ツールを開いて、ディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスを作成します。146 ページの『インスタンス管理ツールの始動』を参照してください。

---

## 第 4 章 IBM Installation Manager を使用した変更

IBM Installation Manager を使用して、以前インストールしなかった IBM Security Directory Server の機能をインストールしたり、既にインストールされている機能をアンインストールしたり、それらの両方を実行できます。

インストールされている他の機能の前提条件である機能は、削除できません。従属するすべての機能を削除するよう選択した場合や、それらが削除済みである場合に限り、依存関係を削除できます。

**重要:** インストール中に既存のバージョンの DB2 または GSKit を使用して続行することを選択した場合、IBM Installation Manager は機能項目を使用して、レジストリーを更新します。「**既存の DB2/GSKit を使用して続行 (Continue with the existing)**」オプションを使用してインストールされた機能を削除する場合、Installation Manager は以下のアクションを実行します。

- IBM Installation Manager レジストリーから機能項目を削除します。
- コンピューターから機能をアンインストールしません。

---

### IBM Installation Manager を使用した機能変更

IBM Installation Manager を使用して、IBM Security Directory Server の機能を変更します。

#### 始める前に

全てのIBM Security Directory Server クライアントとサーバーのプロセスを停止する必要があります。

- ディレクトリー・サーバー
- 管理サーバー
- LDAP トレース
- カスタム LDAP アプリケーション

使用中のプロセスがある場合は、プログラムやライブラリーを削除できません。

#### 手順

1. IBM Installation Manager を始動します。
  - AIX および Linux:
    - a. コマンド行ウィンドウを開き、IBM Installation Manager が置かれているディレクトリーに変更します。IBM Installation Manager のデフォルトのインストール・ロケーションは、以下のディレクトリーです。

```
opt/IBM/InstallationManager/eclipse
```
    - b. 以下のコマンドを実行します。

```
./IBMIM
```
  - Microsoft Windows:

- a. 「スタート」 > 「すべてのプログラム」 > 「IBM Installation Manager」 > 「IBM Installation Manager」をクリックします。
2. 「変更」をクリックします。
3. 「IBM Security Directory Server」を選択してから、「次へ」をクリックします。
4. 「パッケージの変更」ページで、以下のアクションを実行する必要があります。
  - a. インストールする機能を選択します。
  - b. アンインストールする機能の選択を解除します。

表 12. 完全版製品パッケージまたはクライアント専用パッケージで変更対象として選択できる IBM Security Directory Server の機能

すべての機能	インストールの依存関係	完全版製品パッケージ内の機能	クライアント専用パッケージ内の機能
IBM DB2	なし	はい	いいえ
IBM Global Security Kit	なし	はい	はい
C クライアント	なし	はい	はい
IBM Java Development Kit	なし	はい	はい
Java クライアント	なし	はい	はい
サーバー	C クライアント Java クライアント	はい	いいえ
プロキシサーバー	C クライアント Java クライアント	はい	いいえ
Web 管理ツール	なし	はい	いいえ

**重要:** インストール中に既存のバージョンの DB2 または GSKit を使用して続行することを選択した場合、IBM Installation Manager は機能項目を使用して、レジストリーを更新します。「既存の DB2/GSKit を使用して続行 (Continue with the existing)」オプションを使用してインストールされた機能を削除する場合、Installation Manager は以下のアクションを実行します。

- IBM Installation Manager レジストリーから機能項目を削除します。
- コンピューターから機能をアンインストールしません。

IBM Installation Manager でインストールされた DB2 コピーを使用して作成した DB2 インスタンスが存在する場合は、IBM DB2 を削除できません。このような場合は、DB2 インスタンスを手動で削除してからやり直す必要があります。DB2 インスタンスを削除する前に、データベースのバックアップを行うことをお勧めします。

- c. 「次へ」をクリックします。
5. IBM DB2 機能をインストール対象として選択する場合は、「IBM DB2」をクリックし、以下のいずれかのアクションを実行します。
  - IBM DB2 をインストールするには、以下のアクションを実行します。
    - a. 「DB2 のインストール」をクリックします。

- b. 「**DB2 インストール可能ファイルのパス**」フィールドに、DB2 インストール可能ファイルのパス名を指定します。「参照」をクリックして、パスを指定することもできます。
- c. Windows の場合は、「**ユーザー名**」フィールドに、DB2ADMNS グループまたは DB2USERS グループに必要なシステム・ユーザー ID を入力します。このユーザー ID を使用して、ローカルの DB2 アプリケーションとツールをコンピューターで実行することができます。このユーザー ID が存在しない場合は、インストール・プログラムによってユーザー・アカウントが作成されます。
- d. Windows の場合は、「**パスワード**」フィールドにこのユーザー ID のパスワードを入力します。このパスワードがコンピューターで設定されているパスワード・ポリシーに適合しない場合は、インストールが失敗することがあります。
- e. Windows の場合は、「**確認パスワード**」フィールドにユーザー ID のパスワードを入力します。
- f. 「**次へ**」をクリックします。
- サポートされるバージョンの IBM DB2 がコンピューターにインストールされている場合は、以下の手順を実行します。
  - a. 既存の IBM DB2 バージョンを使用して続行する場合は、「**既存の DB2 を使用して続行**」をクリックします。

**重要:** インストール中に既存の DB2 を使用して続行するように指定すると、IBM Installation Manager によって、そのレジストリーが DB2 機能項目で更新されます。
  - b. リストから、IBM Security Directory Server で使用する DB2 のサポート対象のバージョンを選択します。
  - c. 「**次へ**」をクリックします。
- 6. IBM Global Security Kit 機能をインストール対象として選択する場合は、「**IBM Global Security Kit**」をクリックし、以下のいずれかのアクションを実行します。
  - コンピューターに GSKit バージョン 8.0 以降がインストールされていない場合は、以下の手順を実行します。
    - a. 「**GSKit のインストール**」をクリックします。
    - b. 「**GSKit インストール可能ファイルのパス**」フィールドに、GSKit インストール可能ファイルのパス名を指定します。「参照」をクリックして、パスを指定することもできます。

**注:** 指定するパスには、64 ビットと 32 ビットの両方の GSKit インストール可能ファイルが含まれている必要があります。
    - c. 「**次へ**」をクリックします。
  - コンピューターに GSKit バージョン 8.0 以降がインストールされている場合は、以下の手順を実行します。
    - a. 既存の GSKit バージョンを使用して続行する場合は、「**既存の GSKit を使用して続行**」をクリックします。

**重要:** インストール中に既存の GSKit を使用して続行するように指定すると、IBM Installation Manager によって、そのレジストリーが GSKit 機能項目で更新されます。

- b. 「次へ」をクリックします。
7. IBM Java Development Kit 機能をインストール対象として選択する場合は、「**IBM Java Development Kit**」をクリックし、以下の手順を実行します。
    - a. 「**IBM Java Development Kit**」フィールドで、JDK 圧縮ファイルのファイル名をパス名とともに指定します。「参照」をクリックして、パスを指定することもできます。
    - b. 「次へ」をクリックします。
  8. Web 管理ツール機能をインストール対象として選択する場合は、「**Web 管理ツール**」をクリックし、以下の手順を実行します。
    - a. WebSphere Application Server 組み込みバージョンをインストールするには、以下のアクションを実行します。
      - 1) 「**WebSphere Application Server 組み込みバージョンのインストール**」を選択します。
      - 2) 「**WebSphere Application Server 組み込みバージョンのインストール可能ファイルのパス**」フィールドに、WebSphere Application Server 組み込みバージョンのインストール可能ファイルのパス名を指定します。「参照」をクリックして、パスを指定することもできます。
    - b. Web 管理ツールをデプロイするには、以下のアクションのいずれかを実行します。
      - デフォルトのインストール・パスにある WebSphere Application Server 組み込みバージョンにデプロイする場合は、「**デフォルトの WebSphere Application Server 組み込みバージョンにデプロイ**」をクリックします。
- 注:** 前バージョンの Web 管理ツールが存在する場合は、以下の条件が満たされていれば、インストール・プログラムによってそのバージョンが現行バージョンに移行されます。
- 1) 前バージョンの Web 管理ツールおよび WebSphere Application Server 組み込みバージョンがデフォルトのインストール・パスにインストールされている。
  - 2) 前バージョンの Web 管理ツールが、デフォルトのインストール・パスにある WebSphere Application Server 組み込みバージョンにデプロイされている。
  - 3) IBM Security Directory Server バージョン 6.1、6.2、または 6.3 で提供されている Web 管理ツールが移行の対象としてサポートされている。
- カスタム・インストール・パスにある WebSphere Application Server または WebSphere Application Server 組み込みバージョンにデプロイする場合は、「**既存の WebSphere Application Server にデプロイ**」をクリックします。

- 1) 「WebSphere Application Server または WebSphere Application Server 組み込みバージョンのインストール・パス」フィールドで、既存の Web アプリケーション・サーバーのインストール・パスを指定します。
  - サポートされる Web アプリケーション・サーバーに後から Web 管理ツールをデプロイする場合は、「**後で手動でデプロイ**」をクリックします。
9. 「次へ」をクリックします。

**重要:** インストール中に既存のバージョンの DB2 または GSKit を使用して続行することを選択した場合、IBM Installation Manager は機能項目を使用して、レジストリーを更新します。「**既存の DB2/GSKit を使用して続行 (Continue with the existing)**」オプションを使用してインストールされた機能を削除する場合、Installation Manager は以下のアクションを実行します。

  - IBM Installation Manager レジストリーから機能項目を削除します。
  - コンピューターから機能をアンインストールしません。
10. 要約情報を確認し、「**変更**」をクリックします。
11. オプション: 変更中にエラーが発生した場合は、「**ログ・ファイルの表示**」をクリックして、詳細を表示します。詳細については、49 ページの『第 5 章 IBM Installation Manager のログ・ファイル』を参照してください。
12. 「完了」をクリックします。
13. 「ファイル」 > 「終了」をクリックします。

## タスクの結果

変更が正常に終了した場合は、以下の変更を確認できます。

- 追加するように選択した IBM Security Directory Server の機能がインストール・ロケーションにインストールされます。デフォルトのインストール・ロケーションについては、30 ページの『デフォルトのインストール・ロケーション』を参照してください。
- 削除するように選択した IBM Security Directory Server の機能がアンインストールされます。



---

## 第 5 章 IBM Installation Manager のログ・ファイル

IBM Security Directory Server およびそのコンポーネントのインストール、変更、またはアンインストールは、IBM Installation Manager が作成するログ・ファイルを確認することによって検証できます。

IBM Security Directory Server およびそのコンポーネントのインストール、変更、またはアンインストール中にエラーが発生した場合、ログ・ファイルを確認する必要があります。IBM Installation Manager は、ログ・ファイルをデフォルト・ロケーションに作成します。

表 13. 各種オペレーティング・システム上での IBM Installation Manager ログ・ファイルのデフォルト・ロケーション

オペレーティング・システム	IBM Installation Manager のデフォルト・ログ・ロケーション
AIX および Linux	/var/ibm/InstallationManager/logs
Microsoft Windows	C:\ProgramData\IBM\InstallationManager\logs

デフォルト・ロケーションは、サポートされるすべてのバージョンの AIX、Linux、および Microsoft Windows に適用できます。



---

## 第 6 章 IBM Security Directory Server パッケージの照会

サポート対象プラットフォームで IBM Security Directory Server パッケージを照会して、IBM Security Directory Server パッケージを検証します。

### このタスクについて

IBM Security Directory Server パッケージのインストール後は、すべてのパッケージが必須レベルであることを確認する必要があります。このタスクは、インストールされている IBM Security Directory Server パッケージのバージョン番号を照会するときに役立ちます。

### 手順

IBM Security Directory Server パッケージをインストールしたシステムにログオンし、root 特権で以下のコマンドを実行します。

- AIX システムの場合: **lslpp** コマンドを実行します。以下に例を示します。

```
lslpp -l 'idsldap*'
```

- Linux システムの場合: **rpm** コマンドを実行します。以下に例を示します。

```
rpm -qa | grep idsldap
```

- Solaris システムの場合:

1. インストールされているパッケージをリストするには、**pkginfo** コマンドを実行します。以下に例を示します。

```
pkginfo | grep IDS1
```

2. 特定の IBM Security Directory Server パッケージのバージョンを照会するには、**pkgparam** コマンドを実行します。以下に例を示します。

```
pkgparam IDS1bc63 VERSION
```

- HP-UX (Itanium) システムの場合: **swlist** コマンドを実行します。以下に例を示します。

```
swlist | grep idsldap
```



---

## 第 7 章 スクリプトを使用したネイティブ・インストールおよび構成

スクリプトを使用して IBM Security Directory Server をインストールしたり構成したりすることができます。

---

### インストール・ロードマップ

ロードマップを使用して、Linux x86、Linux i/pSeries、Linux s390、Solaris、および HP-UX システムに IBM Security Directory Server をインストールします。

1. ご使用のシステムが最小限の必須ハードウェアおよびソフトウェアを満たしていることを確認します。詳しくは、IBM Security Directory Server 資料の『製品概要』セクションで『システム要件』を参照してください。
2. DB2 などの前提ソフトウェアをインストールします。インストール済みではない場合は、DB2 インストール可能ファイルへのパスにアクセス可能であり、必要なアクセス権があることを確認します。
3. 以下のいずれかの機能を使用する計画がある場合は、オプションの前提ソフトウェアをインストールする必要があります。インストール済みではない場合は、オプションの前提ソフトウェアへのパスにアクセス可能であり、必要なアクセス権があることを確認します。
  - Web 管理ツールを使用するには、サポート対象の WebSphere Application Server 組み込みバージョンまたは WebSphere Application Server が必要です。また、サポート対象バージョンのブラウザーも必要です。
  - Secure Socket Layer (SSL) または Transport Layer Security (TLS) 暗号化については、サポート対象バージョンの IBM Global Security Kit (GSKit) が必要です。
4. Linux x86、Linux i/pSeries、Linux s390、Solaris、および HP-UX システム上で、**idsNativeInstall** インストール・プログラムを使用して、IBM Security Directory Server パッケージおよびその他の必須ソフトウェアをインストールします。
5. IBM Security Directory Server をインストールした後に、**idsdefinst** コマンドを使用してディレクトリー・サーバー・インスタンスの作成および構成を行います。
6. ディレクトリー・サーバー・インスタンスを開始します。
7. サンプル LDIF ファイルをデータベースにロードします。ディレクトリー・サーバー・インスタンスの使用については、IBM Security Directory Server 資料の『管理』セクションを参照してください。

注: Windows、AIX、および Linux x86\_64 (64 ビット) オペレーティング・システムの場合、ネイティブ・インストール・スクリプト **idsNativeInstall** は提供されません。IBM Installation Manager または オペレーティング・システムのコマンド行ユーティリティーを使用すると、これらのオペレーティング・システムに手動でインストールできます。

---

## Linux、Solaris、および HP-UX の各プラットフォームへの IBM Security Directory Server パッケージのインストール

以下の手順を使用して、Linux x86、Linux i/pSeries、Linux s390、Solaris、および HP-UX システム上で IBM Security Directory Server パッケージをインストールまたはアップグレードします。

### 始める前に

IBM Security Directory Server パッケージのインストールを始める前に、以下のステップを実行する必要があります。

1. root 特権でシステムにログオンします。
2. IBM Security Directory Server バージョン 6.3.1 のアーカイブ・ファイルを、十分なディスク・スペースがあるディレクトリーに抽出します (例: /sdsV6.3.1)。
3. IBM Security Directory Server クライアントおよびサーバーのすべてのプロセス (ディレクトリー・サーバー、管理サーバー、カスタムの LDAP アプリケーションを含む) を停止します。使用中のプログラムおよびライブラリーは置換できません。トレースが設定されている場合は、ldtrc off を実行してトレース・プロセスを停止します。ディレクトリー・サーバー・インスタンスおよび管理サーバーを停止するための手順については、IBM Security Directory Server 資料の『管理』セクションにある、『基本的なサーバー管理タスク』および『ディレクトリー管理サーバー』の各セクションを参照してください。

### このタスクについて

**idsNativeInstall** コマンドを使用して、Linux x86、Linux i/pSeries、Linux s390、Solaris、および HP-UX システム上で IBM Security Directory Server パッケージをインストールまたはアップグレードできます。必要に応じ、

**idsNativeInstall** コマンドを使用して、DB2、GSKit、および WebSphere Application Server 組み込みバージョンをインストールすることもできます (まだシステムにインストールされていない場合)。

#### 注:

- Windows、AIX、および Linux x86\_64 (64 ビット) オペレーティング・システムの場合、ネイティブ・インストール・スクリプト **idsNativeInstall** は提供されません。IBM Installation Manager または オペレーティング・システムのコマンド行ユーティリティーを使用すると、これらのオペレーティング・システムに手動でインストールできます。
- HP-UX システムでは、IBM Security Directory Server クライアントのみのパッケージを使用して、インストールまたはアップグレードを行うことができます。

### 手順

1. **idsNativeInstall** インストール・プログラムと responseFile.txt ファイルがあるディレクトリーに存在します。idsNativeInstall と responseFile.txt ファイルは同じディレクトリーに存在している必要があります。
2. responseFile.txt ファイルの以下の項目を更新します。デフォルトでは、機能インストール変数の値は false に設定されており、それに対応するパス変数は設定されていません。

- DB2 をインストールするには、*db2FeatureInstall* 変数を true に設定し、*db2InstallImagePath* 変数を DB2 インストール可能ファイルの絶対パスに更新します。以下に例を示します。

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

**重要:** 完全な Directory Server を使用する場合は、DB2 がシステムにインストールされている必要があります。DB2 変数 *db2FeatureInstall* および *db2InstallImagePath* を設定すると、DB2 が /opt/ibm/sdsV6.3.1db2 (Linux の場合) または /opt/IBM/sdsV6.3.1db2 (Solaris の場合) にインストールされます。DB2 の特定のバージョンが上記のロケーションに既にインストールされている場合は、インストールによって既存のファイルが上書きされます。

- GSKit をインストールするには、*gskitFeatureInstall* 変数を true に設定し、*gskitInstallImagePath* 変数を GSKit インストール可能ファイルの絶対パスに更新します。以下に例を示します。

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

**重要:** SSL または TLS 経由で通信するようにディレクトリー・サーバー・インスタンスを構成するには、GSKit の必須バージョンがシステムにインストールされている必要があります。

- IBM Java Development Kit をインストールするには、*JDKFeatureInstall* 変数を true に設定し、*JDKInstallImagePath* 変数を IBM Java Development Kit インストール可能ファイルの絶対パスに更新します。以下に例を示します。

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

IBM Java Development Kit は、Linux および Solaris システムでは /opt/ibm/ldap/V6.3.1/java にインストールされます。

- WebSphere Application Server 組み込みバージョンをインストールするには、*eWasFeatureInstall* 変数を true に設定し、*eWasInstallImagePath* 変数を WebSphere Application Server 組み込みバージョンのインストール可能ファイルの絶対パスに更新します。以下に例を示します。

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

組み込みバージョンの WebSphere Application Server は、Linux および Solaris システムでは /opt/ibm/ldap/V6.3/appsrv にインストールされます。

- IBM Security Directory Server バージョン 6.3.1 一般出荷版 (GA) をインストールするには、*tdsInstallImagePath* 変数を IBM Security Directory Server バージョン 6.3.1 GA インストール可能ファイルの絶対パスに更新します。以下に例を示します。

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

IBM Security Directory Server バージョン 6.3.1 のインストール可能ファイルのロケーションとして /sdsV6.3.1 を指定する場合は、/sdsV6.3.1 ディレクトリーに以下のファイルが存在することを確認してください。

```
idsinstall
idsinstall_i
ids_detectGskitVersion
```

IBM Security Directory Server バージョン 6.3.1 パッケージは、/sdsV6.3.1/tdsfiles ディレクトリーに存在する必要があります。

3. コマンド・プロンプトで **idsNativeInstall** コマンドを実行します。

## タスクの結果

**idsNativeInstall** コマンドを実行すると、IBM Security Directory Server 6.3.1 パッケージがインストールされます。**idsNativeInstall** コマンドは、応答ファイルの値に応じて、DB2、GSKit、IBM Java Development Kit、または WebSphere Application Server 組み込みバージョンもインストールします。

注: IBM Security Directory Server バージョン 6.3.1 がシステムにインストールされていない場合は、IBM Security Directory Server バージョン 6.3.1 のすべてのコンポーネントがインストールされます。IBM Security Directory Server バージョン 6.3.1 は、Linux、Solaris、および HP-UX システムでは、/opt/ibm/ldap/V6.3.1/ にインストールされます。

## 次のタスク

IBM Security Directory Server のインストール後は、IBM Security Directory Server パッケージがインストールされているかどうか検証する必要があります。ログの検証について詳しくは、『インストール・ログの検証』を参照してください。

---

## インストール・ログの検証

Linux x86、Linux iSeries、Linux s390、Solaris、および HP-UX システム上でのインストール状況を検証するために確認する必要があるログ・ファイルを判別します。

インストールの後に、**idsNativeInstall** コマンドにより、インストールが成功したかどうかを示す適切なメッセージが表示されます。IBM Security Directory Server パッケージがインストールされたかどうかを検証するには、インストール・ログについてログ・ファイルを確認します。

ログ・ファイルは /var/idsldap/V6.3/idsNativeInstall\_timestamp.log です。

インストール・ログの検証後に、すべてのパッケージが正常にインストールされており、必要なレベルにあることを確認してください。インストール済みパッケージのバージョン番号の照会について詳しくは、51 ページの『第 6 章 IBM Security Directory Server パッケージの照会』を参照してください。

---

## 第 8 章 IBM DB2 のインストール

IBM Security Directory Server インスタンスを作成して、インスタンスとともに DB2 データベースを構成するには、サポートされるバージョンの IBM DB2 がコンピューターにインストールされている必要があります。

IBM Security Directory Server のインストール・メディアでは、サポートされるバージョンの IBM DB2 が提供されます。IBM Security Directory Server のインストールのためにオペレーティング・システムのユーティリティーを使用している場合、IBM DB2 のインストールを完了する必要があります。IBM Security Directory Server のインストールを実行すると、プロパティー・ファイルは、サポートされる IBM DB2 バージョンの詳細情報で更新されます。サポートされるバージョンの IBM DB2 がコンピューターにインストールされている場合、DB2 を使用して、ディレクトリー・サーバー・インスタンスとともに構成することができます。ldapdb.properties ファイルの更新について詳しくは、283 ページの『付録 C. 手動による ldapdb.properties ファイルの更新』を参照してください。

IBM DB2 をインストールするには、IBM Security Directory Server のインストール・メディアにアクセスし、IBM DB2 インストール可能ファイルが格納されているディレクトリーに移動します。

IBM DB2 のインストールを実行する前に、DB2 の前提条件を満たしておく必要があります。コンピューターが DB2 の前提条件検査に適合しているかどうかを検証するには、**db2prereqcheck** コマンドを実行します。何らかのパッケージがコンピューターから欠落している場合、必要なパッケージについてコンピューターを更新する必要があります。

AIX、Linux、および Solaris の場合は、**db2\_install** コマンドを使用して IBM DB2 をインストールできます。Windows の場合、**setup.exe** コマンドを使用して、IBM DB2 をインストールします。

Intel 32 ビット・アーキテクチャー上の System x Linux の場合、WSE と入力して、Workspace Server Edition を選択する必要があります。サポートされるその他のオペレーティング・システムの場合、ESE と入力して、Enterprise Server Edition を選択します。

IBM DB2 をインストールした後、/tmp/db2\_install\_log.XXXXX ファイルを確認して、インストールが成功したかどうかを確認します。XXXXX は、インストールに関連付けられたランダムな数です。

DB2 の前提条件および IBM DB2 のインストールについて詳しくは、IBM DB2 製品資料 (<http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome>)を参照してください。

### Solaris システムのカーネル・パラメーター

Solaris システムでは、IBM DB2 のインストールを行う前に、/etc/system ファイル内のカーネル・パラメーターの更新が必要になる場合があります。 **db2osconf** コ

マンドを使用して、コンピューターの正しいカーネル・パラメーター値を調べることができます。**projmod** コマンドを使用して、Solaris で DB2 のインストールを行う前に、Solaris のカーネル・パラメーター値を構成することができます。

Solaris システムでゾーンが構成されている場合、**db2osconf** コマンドは、Solaris のグローバル・ゾーンからのみ実行できます。

**db2osconf** コマンドについて詳しくは、IBM DB2 製品資料 (<http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome>) で **db2osconf** を検索してください。

## 第 9 章 IBM Security Directory Server 用の IBM Java Development Kit

Java サンプル・プログラムをコンパイルしたり、インスタンス管理ツールや構成ツールなどの Java プログラムを実行したりするには、IBM Security Directory Server のインストール・ロケーションに IBM Java Development Kit を圧縮解除する必要があります。

IBM Security Directory Server のインストール・メディアでは、サポートされるバージョンの IBM Java Development Kit、IBM Java 1.6 SR 14 が提供されます。IBM Security Directory Server のインストールのためにオペレーティング・システムのユーティリティーを使用する場合、IBM Java Development Kit のインストールを完了する必要があります。

IBM Java Development Kit をインストールするには、IBM Security Directory Server のインストール・メディアにアクセスし、IBM Java Development Kit の圧縮ファイルが格納されているディレクトリーに移動します。

IBM Java Development Kit アーカイブ・ファイルを IBM Security Directory Server のインストール・ロケーションに圧縮解除する必要があります。IBM Java Development Kit アーカイブ・ファイルは java ディレクトリーに圧縮解除されます。IBM Security Directory Server のインストール・ロケーションについて詳しくは、30 ページの『デフォルトのインストール・ロケーション』を参照してください。

AIX では、GNU tar を使用して、IBM Java Development Kit アーカイブ・ファイルを IBM Security Directory Server のインストール・ロケーションに圧縮解除することができます。それ以外の場合は、圧縮解除した java ディレクトリーを、IBM Security Directory Server のインストール・ロケーションに移動することが必要な場合もあります。前提条件パッケージについて詳しくは、16 ページの『各種オペレーティング・システムに必要な前提条件パッケージ』を参照してください。

表 14. 様々なオペレーティング・システムで使用できる IBM Java Development Kit パッケージ

オペレーティング・システム	パッケージ名
AIX	ibm-java-16sr14-aix-ppc-64.tar
System x Linux (Intel 32 ビット)	ibm-java-16sr14-linux-i386.tar
System i and System p Linux	ibm-java-16sr14-linux-ppc-64.tar
System z Linux	ibm-java-16sr14-linux-s390-64.tar
Linux (AMD64/EM64T)	ibm-java-16sr14-linux-64.tar
HP-UX (Itanium)	ibm-java-16sr14-hp-itanium-64.tar
Solaris (AMD64/EM64T)	ibm-java-16sr14-solaris-amd-64.tar
Solaris SPARC	ibm-java-16sr14-solaris-sparc-64.tar
Windows 32 ビット	ibm-java-16sr14-win-i386.zip
Windows (AMD64/EM64T)	ibm-java-16sr14-win-x86_64.zip

## 例

**例 1:** IBM Java Development Kit アーカイブ・ファイルを、Linux システム上の IBM Security Directory Server のインストール・ロケーションに圧縮解除するには、以下のコマンドを実行します。

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

---

## 第 10 章 IBM Global Security Kit のインストール

Secure Sockets Layer (SSL) および Transaction Layer Security (TLS) を IBM Security Directory Server で使用するには、サポートされるバージョンの IBM Global Security Kit (GSKit) がコンピューターに含まれている必要があります。

ご使用のオペレーティング・システムが、IBM Installation Manager によるインストールをサポートしていない場合、IBM Global Security Kit のインストールのためにオペレーティング・システムのユーティリティーを使用することができます。セキュア接続を確立して使用するためには、GSKit をサーバー・システムとクライアント・システムの両方にインストールする必要があります。

低レベルの暗号化サポートには、GSKit crypt パッケージが必要です。セキュア通信のハンドシェイク操作には、GSKit SSL パッケージが必要です。GSKit crypt パッケージは、GSKit SSL パッケージの前提条件です。

IBM Security Directory Server のインストール・メディアでは、各種オペレーティング・システム用の以下の GSKit パッケージが提供されます。

注: Solaris x64 アーキテクチャーと SPARC アーキテクチャーについては、GSKit パッケージ名は同じです。

### AIX

#### GSKit (64 ビット) のパッケージ名

GSKit8.gskcrypt64.ppc.rte

GSKit8.gskssl64.ppc.rte

#### GSKit (32 ビット) のパッケージ名

GSKit8.gskcrypt32.ppc.rte

GSKit8.gskssl32.ppc.rte

### System x Linux

#### GSKit (32 ビット) のパッケージ名

gskcrypt32-8.0.14.26.linux.x86.rpm

gskssl32-8.0.14.26.linux.x86.rpm

### System z Linux

#### GSKit (64 ビット) のパッケージ名

gskcrypt64-8.0.14.26.linux.s390x.rpm

gskssl64-8.0.14.26.linux.s390x.rpm

#### GSKit (32 ビット) のパッケージ名

gskcrypt31-8.0.14.26.linux.s390.rpm

gskssl31-8.0.14.26.linux.s390.rpm

### System i and System p Linux

**GSKit (64 ビット) のパッケージ名**  
gskcrypt64-8.0.14.26.linux.ppc.rpm  
gskssl64-8.0.14.26.linux.ppc.rpm

**GSKit (32 ビット) のパッケージ名**  
gskcrypt32-8.0.14.26.linux.ppc.rpm  
gskssl32-8.0.14.26.linux.ppc.rpm

**Linux IA64 (Itanium) および AMD64/EM64T Linux**

**GSKit (64 ビット) のパッケージ名**  
gskcrypt64-8.0.14.26.linux.x86\_64.rpm  
gskssl64-8.0.14.26.linux.x86\_64.rpm

**GSKit (32 ビット) のパッケージ名**  
gskcrypt32-8.0.14.26.linux.x86.rpm  
gskssl32-8.0.14.26.linux.x86.rpm

**Solaris**

**GSKit (64 ビット) のパッケージ名**  
gsk8cry64.pkg  
gsk8ssl64.pkg

**GSKit (32 ビット) のパッケージ名**  
gsk8cry32.pkg  
gsk8ssl32.pkg

**HP-UX (Itanium)**

**GSKit (64 ビット) のパッケージ名**  
gskcrypt64  
gskssl64

**GSKit (32 ビット) のパッケージ名**  
gskcrypt32  
gskssl32

**Microsoft Windows**

**GSKit (64 ビット) のパッケージ名**  
gsk8crypt64.exe  
gsk8ssl64.exe

**GSKit (32 ビット) のパッケージ名**  
gsk8crypt32.exe  
gsk8ssl32.exe

---

## **installp を使用した IBM Global Security Kit のインストール**

**installp** コマンドを使用して、AIX システムで IBM Global Security Kit のインストールを実行することができます。

## 始める前に

IBM Security Directory Server インストール・メディアにアクセスして、IBM Global Security Kit インストール可能ファイルを取得します。6 ページの『インストール・メディアの準備』を参照してください。

## このタスクについて

**installp** インストール・プログラムは、AIX システムに IBM Global Security Kit (GSKit) をインストールします。

## 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを、IBM Global Security Kit のインストール可能ファイルが保管されている `gskit` ディレクトリーに変更します。
4. **installp** コマンドを実行して IBM Global Security Kit パッケージをインストールします。

- a. GSKit 64 ビット・パッケージをインストールするには、以下のコマンドを実行します。

```
installp -acgXd . GSKit8.gskcrypt64.ppc.rte  
installp -acgXd . GSKit8.gskssl64.ppc.rte
```

- b. GSKit 32 ビット・パッケージをインストールするには、以下のコマンドを実行します。

```
installp -acgXd . GSKit8.gskcrypt32.ppc.rte  
installp -acgXd . GSKit8.gskssl32.ppc.rte
```

5. 以下のコマンドを実行して、IBM Global Security Kit のインストールが正常に終了したかどうかを確認します。

```
ls1pp -aL GSKit8*
```

## タスクの結果

インストール・プログラムによって、IBM Global Security Kit が AIX システムの以下のロケーションにインストールされます。

### GSKit 64 ビット

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

### GSKit 32 ビット

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

---

## Linux ユーティリティーを使用した IBM Global Security Kit のインストール

**rpm** コマンドを使用して、Linux システムで IBM Global Security Kit のインストールを実行します。

## 始める前に

IBM Security Directory Server インストール・メディアにアクセスして、IBM Global Security Kit インストール可能ファイルを取得します。6 ページの『インストール・メディアの準備』を参照してください。

## このタスクについて

`rpm` コマンドは、Linux システムに IBM Global Security Kit (GSKit) をインストールします。例では、AMD64 Opteron/EM64T Linux に IBM Global Security Kit をインストールしています。System z、System i、System p、または System x の Linux の場合は、該当するパッケージ名で置き換える必要があります。

## 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを、IBM Global Security Kit のインストール可能ファイルが保管されている `gskit` ディレクトリーに変更します。
4. `rpm` コマンドを実行して IBM Global Security Kit パッケージをインストールします。
  - a. GSKit 64 ビット・パッケージをインストールするには、以下のコマンドを実行します。

```
rpm -ivh gskcrypt64-8.0.14.26.linux.x86_64.rpm
rpm -ivh gskssl64-8.0.14.26.linux.x86_64.rpm
```
  - b. GSKit 32 ビット・パッケージをインストールするには、以下のコマンドを実行します。

```
rpm -ivh gskcrypt32-8.0.14.26.linux.x86.rpm
rpm -ivh gskssl32-8.0.14.26.linux.x86.rpm
```
5. 以下のコマンドを実行して、IBM Global Security Kit のインストールが正常に終了したかどうかを確認します。

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

## タスクの結果

インストール・プログラムによって、IBM Global Security Kit が Linux システムの以下のロケーションにインストールされます。

### GSKit 64 ビット

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

### GSKit 32 ビット

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

---

## Solaris ユーティリティーを使用した IBM Global Security Kit のインストール

`pkgadd` コマンドを使用して、Solaris システムで IBM Global Security Kit のインストールを実行します。

## 始める前に

IBM Security Directory Server インストール・メディアにアクセスします。6 ページの『インストール・メディアの準備』を参照してください。

## このタスクについて

**pkgadd** コマンドは、Solaris システムに IBM Global Security Kit (GSKit) をインストールします。パッケージ名とファイル名は、Solaris SPARC オペレーティング・システムと Solaris X64 オペレーティング・システムで同じです。

## 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを、IBM Global Security Kit のインストール可能ファイルが保管されている **gskit** ディレクトリーに変更します。
4. **pkgadd** コマンドを実行して IBM Global Security Kit パッケージをインストールします。

- a. GSKit 64 ビット・パッケージをインストールするには、以下のコマンドを実行します。

```
pkgadd -d gsk8cry64.pkg  
pkgadd -d gsk8ssl64.pkg
```

- b. GSKit 32 ビット・パッケージをインストールするには、以下のコマンドを実行します。

```
pkgadd -d gsk8cry32.pkg  
pkgadd -d gsk8ssl32.pkg
```

5. 以下のコマンドを実行して、IBM Global Security Kit のインストールが正常に終了したかどうかを確認します。

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

`package_name` を GSKit パッケージ名で置き換えてバージョンを確認します。

---

## HP-UX ユーティリティーを使用した IBM Global Security Kit のインストール

**swinstall** コマンドを使用して、HP-UX システムで IBM Global Security Kit のインストールを実行します。

## 始める前に

IBM Security Directory Server インストール・メディアにアクセスして、IBM Global Security Kit インストール可能ファイルを取得します。6 ページの『インストール・メディアの準備』を参照してください。

## 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。

3. 現在の作業ディレクトリーを、IBM Global Security Kit のインストール可能ファイルが保管されている `gskit` ディレクトリーに変更します。
4. `swinstall` コマンドを実行して IBM Global Security Kit パッケージをインストールします。
  - a. GSKit 64 ビット・パッケージをインストールするには、以下のコマンドを実行します。

```
swinstall -s path_to_gskit_installable/gskcrypt64 gskcrypt64
swinstall -s path_to_gskit_installable/gskssl64 gskssl64
```

`-s` パラメーターには、GSKit インストール可能ファイルの絶対パス名を指定する必要があります。
  - b. GSKit 32 ビット・パッケージをインストールするには、以下のコマンドを実行します。

```
swinstall -s path_to_gskit_installable/gskcrypt32 gskcrypt32
swinstall -s path_to_gskit_installable/gskssl32 gskssl32
```
5. 以下のコマンドを実行して、IBM Global Security Kit のインストールが正常に終了したかどうかを確認します。

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

---

## Windows での IBM Global Security Kit のインストール

IBM Global Security Kit インストール・プログラムを実行して、Windows システムで IBM Global Security Kit のインストールを実行します。

### 始める前に

IBM Security Directory Server インストール・メディアにアクセスして、IBM Global Security Kit インストール可能ファイルを取得します。6 ページの『インストール・メディアの準備』を参照してください。

### このタスクについて

例では、GSKit crypt 64 ビットおよび GSKit SSL 64 ビットをインストールしています。GSKit 32 ビットをインストールする場合は、該当するパッケージを使用してください。Windows 64 ビット・オペレーティング・システムには、64 ビットと 32 ビットの両方の GSKit パッケージをインストールできます。

### 手順

1. 管理者グループのメンバーとしてログインします。
2. 現在の作業ディレクトリーを、IBM Global Security Kit のインストール可能ファイルが保管されている `gskit` ディレクトリーに変更します。
3. GSKit 64 ビット・パッケージをインストールするには、GSKit インストール・プログラムを実行します。
  - a. GSKit8 crypt インストール・パッケージ `gsk8crypt64.exe` を実行します。
  - b. GSKit8 crypt のインストール・ウィンドウで、以下の手順を実行します。
    - 1) GSKit8 crypt のインストール・パスを指定します。
    - 2) 「次へ」をクリックします。

- 3) 「インストール」をクリックします。
- 4) 「完了」をクリックします。
- c. GSKit8 SSL インストール・パッケージ `gsk8ssl64.exe` を実行します。
- d. GSKit8 SSL のインストール・ウィンドウで、以下の手順を実行します。
  - 1) GSKit8 SSL のインストール・パスを指定します。
  - 2) 「次へ」をクリックします。
  - 3) 「インストール」をクリックします。
  - 4) 「完了」をクリックします。
4. GSKit コマンドをコマンド行から実行するには、`PATH` 変数で Windows x86\_64 システム上の `bin` ディレクトリーと `lib64` ディレクトリーを設定します。

注: Windows 32 ビットでは、`PATH` 変数で `bin` ディレクトリーと `lib` ディレクトリーを設定します。

GSKit のインストール・ロケーションが `C:\Program Files\IBM\gsk8` である場合は、`PATH` 変数で以下の値を設定します。

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

---

## Windows での IBM Global Security Kit のサイレント・インストール

IBM Global Security Kit インストール・プログラムをコマンド・プロンプトから実行して、Windows システムで IBM Global Security Kit のインストールをサイレントに実行します。

### 始める前に

IBM Security Directory Server インストール・メディアにアクセスして、IBM Global Security Kit インストール可能ファイルを取得します。6 ページの『インストール・メディアの準備』を参照してください。

### このタスクについて

例では、GSKit crypt 64 ビットおよび GSKit SSL 64 ビットをインストールしています。GSKit 32 ビットをインストールする場合は、該当するパッケージを使用してください。Windows 64 ビット・オペレーティング・システムには、64 ビットと 32 ビットの両方の GSKit パッケージをインストールできます。

### 手順

1. 管理者グループのメンバーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを、IBM Global Security Kit のインストール可能ファイルが保管されている `gskit` ディレクトリーに変更します。
4. GSKit 64 ビット・パッケージをサイレント・インストールするには、以下のコマンドを実行します。

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

5. GSKit コマンドをコマンド行から実行するには、*PATH* 変数で Windows x86\_64 システム上の bin ディレクトリーと lib64 ディレクトリーを設定します。

**注:** Windows 32 ビットでは、*PATH* 変数で bin ディレクトリーと lib ディレクトリーを設定します。

GSKit のインストール・ロケーションが C:\Program Files\IBM\gsk8 である場合は、*PATH* 変数で以下の値を設定します。

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

## 第 11 章 言語パックのインストール

英語以外の言語でディレクトリー・サーバーのメッセージを生成するには、使用する言語の言語パックをインストールする必要があります。

IBM Installation Manager では、フル・インストーラーからのインストール機能を選択した場合、オペレーティング・システムで使用可能なすべての言語パックをインストールできます。言語パックは、IBM Security Directory Server のインストール・ロケーションの nls サブディレクトリーにインストールされます。

注: クライアントに対して言語パックをインストールする必要はありません。

**idslink** および **idsrmlink** コマンドについて、英語以外の言語でメッセージを生成する場合は、クライアントに対して言語パックをインストールすることができます。**idslink** および **idsrmlink** コマンドについて詳しくは、「*Command Reference*」を参照してください。

言語パックは、AIX および Linux システム上でオペレーティング・システムのユーティリティーを使用するか IBM Installation Manager を使用してインストールできます。IBM Installation Manager を使用した言語パックのインストールは、IBM Security Directory Server の完全な製品インストーラーで提供されます。

**要確認:** IBM Installation Manager を使用した言語パックのインストールは、AMD64/EM64T アーキテクチャーの AIX、Linux と、Microsoft Windows コンピューターでのみサポートされます。IBM Installation Manager を使用した IBM Security Directory Server のインストールをサポートするオペレーティング・システムでは、オペレーティング・システムのユーティリティーを使用して言語パックを手動でインストールしないでください。IBM Installation Manager を使用して言語パックをインストールすることがオペレーティング・システムでサポートされていない場合、オペレーティング・システムのユーティリティーを使用して、言語パックをインストールしてください。

表 15. AIX、Linux、Solaris、および Windows オペレーティング・システムでサポートされる言語のリスト

言語	AIX	Linux	Solaris	Microsoft Windows
チェコスロバキア語	✓			
フランス語	✓	✓	✓	✓
ドイツ語	✓	✓	✓	✓
ハンガリー語	✓			
イタリア語	✓	✓	✓	✓
日本語	✓	✓	✓	✓
韓国語	✓	✓	✓	✓
ポーランド語	✓			
ポルトガル語 (ブラジル)	✓	✓	✓	✓
ロシア語	✓			

表 15. AIX、Linux、Solaris、および Windows オペレーティング・システムでサポートされる言語のリスト (続き)

言語	AIX	Linux	Solaris	Microsoft Windows
スロバキア語	✓			
スペイン語	✓	✓	✓	✓
中国語 (簡体字)	✓	✓	✓	✓
中国語 (繁体字)	✓	✓	✓	✓

## インストール用の各言語パックのパッケージ

言語パックをインストールする前に、サポートされるオペレーティング・システムの各言語に関連付けられているパッケージ名を特定する必要があります。

### 言語名および言語パック名

**要確認:** Linux 用の言語パックは、次のアーキテクチャーでサポートされます。

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

**要確認:** Solaris 用の言語パックは、次のアーキテクチャーでサポートされます。

- Solaris SPARC
- Solaris X64

表 16. AIX、Linux、および Solaris の各オペレーティング・システム上でサポートされる言語の言語パック名付きリスト

言語	AIX	Linux	Solaris
チェコスロバキア語	idsldap.msg631.cs_CZ		
フランス語	idsldap.msg631.fr_FR	idsldap-msg631-fr-6.3.1-0.noarch.rpm	idsldap.msg631.fr.pkg
ドイツ語	idsldap.msg631.de_DE	idsldap-msg631-de-6.3.1-0.noarch.rpm	idsldap.msg631.de.pkg
ハンガリー語	idsldap.msg631.hu_HU		
イタリア語	idsldap.msg631.it_IT	idsldap-msg631-it-6.3.1-0.noarch.rpm	idsldap.msg631.it.pkg
日本語	idsldap.msg631.ja_JP	idsldap-msg631-ja-6.3.1-0.noarch.rpm	idsldap.msg631.ja.pkg
韓国語	idsldap.msg631.ko_KO	idsldap-msg631-ko-6.3.1-0.noarch.rpm	idsldap.msg631.ko.pkg
ポーランド語	idsldap.msg631.pl_PL		
ポルトガル語 (ブラジル)	idsldap.msg631.pt_BR	idsldap-msg631-pt_BR-6.3.1-0.noarch.rpm	idsldap.msg631.pt_BR.pkg
ロシア語	idsldap.msg631.ru_RU		
スロバキア語	idsldap.msg631.sk_SK		

表 16. AIX、Linux、および Solaris の各オペレーティング・システム上でサポートされる言語の言語パック名付きリスト (続き)

言語	AIX	Linux	Solaris
スペイン語	idsldap.msg631.es_ES	idsldap-msg631-es-6.3.1-0.noarch.rpm	idsldap.msg631.es.pkg
中国語 (簡体字)	idsldap.msg631.zh_CN	idsldap-msg631-zh_CN-6.3.1-0.noarch.rpm	idsldap.msg631.zh_CN.pkg
中国語 (繁体字)	idsldap.msg631.zh_TW	idsldap-msg631-zh_TW-6.3.1-0.noarch.rpm	idsldap.msg631.zh_TW.pkg

## オペレーティング・システムのユーティリティーを使用した言語パックのインストール

オペレーティング・システムが IBM Installation Manager によるインストールをサポートしていない場合は、オペレーティング・システムのユーティリティーを使用して言語パックをインストールします。

### 始める前に

IBM Security Directory Server インストール・メディアを準備する必要があります。6 ページの『インストール・メディアの準備』を参照してください。

### このタスクについて

英語以外の言語でディレクトリー・サーバーのメッセージを生成するには、使用する言語の言語パックをインストールする必要があります。

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを、IBM Security Directory Server のインストール可能ファイルが保管されているディレクトリーに変更します。
4. tdsLangpack サブディレクトリーに移動します。
5. 特定言語の言語パックをインストールするには、パッケージ・インストール・コマンドを実行します。以下の例は、フランス語の言語パックのインストールを示しています。各オペレーティング・システムでの適切なパッケージ名に置き換えることで、任意の言語パックをインストールできます。

オペレーティング・システム	実行するコマンド:
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. 言語パックのインストールが正常に終了したかを検証します。詳細については、93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。

## タスクの結果

インストール・プログラムによって、言語パックが以下のディレクトリーにインストールされます。

表 17. IBM Security Directory Server の言語パックのデフォルト・インストール・ロケーション

オペレーティング・システム	言語パックのインストール・ロケーション
Linux	/opt/ibm/ldap/V6.3.1/nls/msg
AIX および Solaris	/opt/IBM/ldap/V6.3.1/nls/msg

---

## 第 12 章 オペレーティング・システム・コマンド行ユーティリティーを使用したインストール

X11 サポートが提供されていないシステムでは、オペレーティング・システムのコマンド行ユーティリティーを使用して、IBM Security Directory Server のインストールを実行できます。

注意:

- 同じコンピューター上で異なるインストール・モードを使用しないでください。**IBM Security Directory Server** のインストールの実行は、**IBM Installation Manager** またはオペレーティング・システムのコマンド行ユーティリティーのいずれかを使用する必要がありますが、両方を使用してはいけません。2 つのインストール・モードを混用すると、特定の機能についてのすべての適切なパッケージがインストールに含まれないことがあります。
- **DB2** および **WebSphere Application Server** 組み込みバージョンを、**IBM Installation Manager** によって使用されているそれらのデフォルトのインストール・パスに手動インストールすることは避けてください。そのような手動インストールを行うと、**IBM Installation Manager** を使用してインストール、変更、またはアンインストールを実行した場合に、これらの操作に失敗することがあります。デフォルトのインストール・パスについては、30 ページの『デフォルトのインストール・ロケーション』を参照してください。

製品をインストールする前に、IBM Security Directory Server のインストール・ソースを取得する必要があります。IBM Security Directory Server 製品は、アーカイブ・ファイルか、インストール可能イメージとして入手できます。インストール可能イメージからインストール DVD を作成できます。

インストール・メディアを準備する必要があります。詳細については、6 ページの『インストール・メディアの準備』を参照してください。

**重要:** IBM Security Directory Server をフル・ディレクトリー・サーバーとして使用するには、サポートされるバージョンの **IBM DB2** をコンピューターにインストールしてください (まだインストールされていない場合)。IBM DB2 のパス名およびバージョンを使用して、`ldapdb.properties` ファイルを構成する必要があります。

---

### AIX ユーティリティーを使用したインストール

AIX コマンド行ユーティリティーを使用して、AIX システムに IBM Security Directory Server をインストールできます。

IBM Security Directory Server をインストールするには、以下のいずれかのユーティリティーを使用できます。

**SMIT** 望ましいインストール方法は、このユーティリティーを使用する方法です。詳細については、76 ページの『SMIT を使用したインストール』を参照してください。

## installp

詳細については、78 ページの『installp を使用したインストール』を参照してください。

## AIX システムへのインストール用パッケージ

IBM Security Directory Server を AIX システム上のフル・ディレクトリー・サーバー、プロキシ・サーバー、またはクライアントとして使用するには、適切なパッケージをインストールする必要があります。

### パッケージおよびファイル・セット

IBM Security Directory Server には、AIX システム用の各種パッケージが用意されています。各パッケージには、1 つ以上のファイル・セットが含まれています。

表 18. パッケージおよびパッケージに含まれているファイル・セット

パッケージ	パッケージに関連付けられているファイル・セット
idsldap.license631	idsldap.license631.rte - ライセンス
idsldap.cltbase631	• idsldap.cltbase631.rte - 基本クライアントのランタイム • idsldap.cltbase631.adt - 基本クライアント SDK
idsldap.clt32bit631	• idsldap.clt32bit631.rte - 32 ビット C クライアント (SSL および TLS なし)
idsldap.clt64bit631	• idsldap.clt64bit631.rte - 64 ビット C クライアント (SSL および TLS なし)
idsldap.clt_max_crypto32bit631	• idsldap.clt_max_crypto32bit631.rte - 32 ビット C クライアント (SSL および TLS あり)
idsldap.clt_max_crypto64bit631	• idsldap.clt_max_crypto64bit631.rte - 64 ビット C クライアント (SSL および TLS あり)
idsldap.cltjava631	• idsldap.cltjava631.rte - Java クライアント
idsldap.srvbase64bit631	• idsldap.srvbase64bit631.rte - 基本サーバー
idsldap.srv_max_cryptobase64bit631	• idsldap.srv_max_cryptobase64bit631.rte - 基本サーバー (SSL)
idsldap.srvproxy64bit631	• idsldap.srvproxy64bit631.rte - プロキシ・サーバー (64 ビット)
idsldap.srv64bit631	• idsldap.srv64bit631.rte - ディレクトリー・サーバー (64 ビット)
idsldap.webadmin631	• idsldap.webadmin631.rte - Web 管理ツール (SSL および TLS なし)
idsldap.webadmin_max_crypto631	• idsldap.webadmin_max_crypto631.rte - Web 管理ツール (SSL および TLS あり)
idsldap.msg631.en_US	使用不可
idsldap.ent631	• idsldap.ent631.rte - IBM Directory Server Entitlement (パスポート・アドバンテージでのみ提供される)

### インストール・シーケンス

これらの機能はすべて同時にインストールすることができます。これらの機能を別々にインストールする場合は、それらを特定の順番でインストールする必要があります。

#### 重要:

- Secure Socket Layer (SSL) または Transport Layer Security (TLS) を使用する場合、サポートされているバージョンの IBM Global Security Kit をインストールする必要があります。

- AIX システム上での Kerberos のサポートについては、サポート対象バージョンの Network Authentication Service が必要です。

**注:** コンピューターで X11 をサポートしない場合、IBM JDK で用意されている JDK コンポーネントのインストールをスキップできます。JDK コンポーネントがインストールされていない場合、インスタンス管理ツールまたは構成ツールを使用できない場合があります。

表 19. クライアント機能のインストール・シーケンス

32 ビット・クライアント (SSL および TLS なし)	32 ビット・クライアント (SSL および TLS あり)	64 ビット・クライアント (SSL および TLS なし)	64 ビット・クライアント (SSL および TLS あり)
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

**注:** IBM Security Directory Server のインストール用にライセンス付き ISO イメージまたはライセンスのアーカイブされたファイル付きクライアント/サーバーを使用する場合、最初にライセンス条項に同意してから idsldap.license631 パッケージをインストールする必要があります。

表 20. フル・ディレクトリー・サーバー機能のインストール・シーケンス

フル・ディレクトリー・サーバー 64 ビット (SSL および TLS なし)	フル・ディレクトリー・サーバー 64 ビット (SSL および TLS あり)
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

表 21. プロキシ・サーバー機能のインストール・シーケンス

プロキシ・サーバー 64 ビット (SSL および TLS なし)	プロキシ・サーバー 64 ビット (SSL および TLS あり)
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

注: Web 管理ツールを使用するには、このツールを Web アプリケーション・サーバーにデプロイする必要があります。WebSphere Application Server 組み込みバージョンのインストールについて詳しくは、121 ページの『手動による WebSphere Application Server 組み込みバージョンのインストール』を参照してください。

表 22. Web 管理ツールのインストール・パッケージ

Web 管理ツール (SSL および TLS なし)	Web 管理ツール (SSL および TLS あり)
1. idsldap.license631	1. idsldap.license631
2. idsldap.webadmin631	2. idsldap.webadmin_max_crypto631

Web 管理ツールをインストールするときに、Directory Services Markup Language (DSML) ファイルもコンピューターにコピーされます。DSML について詳しくは、279 ページの『付録 A. Directory Services Markup Language (DSML)』を参照してください。

## SMIT を使用したインストール

**smit** コマンドを使用して、AIX システムで IBM Security Directory Server のインストールを実行します。

### 始める前に

IBM Security Directory Server インストール・メディアを準備する必要があります。6 ページの『インストール・メディアの準備』を参照してください。

### このタスクについて

**smit** インストール・プログラムは、AIX システムに IBM Security Directory Server をインストールします。サポート対象バージョンの IBM DB2 がシステムにインストールされている場合は、インストール・プロセスが DB2 のパス名とバージョンを使用して `ldapdb.properties` ファイルを更新します。

## 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. **idsLicense** コマンドを実行します。  
./idsLicense
4. ソフトウェアのご使用条件に同意する場合は、1 を入力します。以下から選択することができます。
  - 1: ご使用条件に同意する。
  - 2: ご使用条件を拒否し、インストールを終了する。
  - 3: ご使用条件を印刷する。
  - 4: ご使用条件の IBM 以外の条項を見る。
  - 99: 前の画面に戻る。

ご使用条件に同意すると、IBM Security Directory Server のインストール・ローテーションに Lapid ファイルと license フォルダが作成されます。ライセンス・フォルダには、サポートされるすべての言語の IBM Security Directory Server ライセンス・ファイルが含まれています。

**重要:** Lapid ファイルおよびライセンス・フォルダ内のライセンス・ファイルは、変更または削除しないでください。

5. **smit install** コマンドを実行します。「ソフトウェアのインストールおよび保守」ウィンドウが開きます。
6. 「ソフトウェアのインストールおよび更新」 > 「すべての使用可能なソフトウェアのインストールおよび更新」をクリックします。
7. インストール・メディアを選択します。
  - DVD からインストールしている場合は、以下のアクションを実行します。
    - a. 「リスト」をクリックして、IBM Security Directory Server イメージが保管されているデバイスにアクセスします。
  - 解凍アーカイブ・ファイルからインストールする場合は、「ソフトウェアの入力デバイス/ディレクトリー」フィールドに . と入力します。
8. 「OK」をクリックします。
9. カーソルを「インストールするソフトウェア」に移動し、以下のアクションを実行します。
  - a. idsldap ファイル・セットをインストールするには、idsldap と入力します。
  - b. 「リスト」をクリックしてファイル・セットをすべてリストし、インストールするファイル・セットを選択します。
  - c. 「OK」をクリックします。
10. インストールを開始するには、「OK」をクリックします。
11. 出力の最後にあるインストールの要約をチェックして、ファイルセットのインストールが正常に終了したかどうかを確認してください。
12. インストールが完了したら、「完了」をクリックします。
13. **SMIT** プログラムを終了するには、F12 キーを押します。

14. IBM Security Directory Server インストールが正常に終了したかを検証します。詳細については、93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。

## タスクの結果

インストール・プログラムによって、IBM Security Directory Server が AIX システム上の /opt/IBM/ldap/V6.3.1 ディレクトリーにインストールされます。サポート対象バージョンの IBM DB2 がシステムにインストールされている場合は、インストール・プロセスが DB2 のパス名とバージョンを使用して ldapdb.properties ファイルを更新します。

## 次のタスク

IBM Security Directory Server がインストールされたら、以下のアクションを実行する必要があります。

- IBM Security Directory Server を完全なディレクトリー・サーバーとして使用する場合は、ディレクトリー・サーバー・インスタンスを作成してください。149 ページの『デフォルトのディレクトリー・サーバー・インスタンスの作成』を参照してください。
- IBM Security Directory Server をプロキシ・サーバーとして使用するには、プロキシ・サーバー・インスタンスを作成してください。160 ページの『カスタム設定を使用したプロキシ・サーバー・インスタンスの作成』を参照してください。

## installp を使用したインストール

**installp** コマンドを使用して、AIX システムで IBM Security Directory Server のインストールを実行します。

### 始める前に

IBM Security Directory Server インストール・メディアを準備する必要があります。6 ページの『インストール・メディアの準備』を参照してください。

### このタスクについて

**installp** インストール・プログラムは、AIX システムに IBM Security Directory Server をインストールします。サポート対象バージョンの IBM DB2 がシステムにインストールされている場合は、インストール・プロセスが DB2 のパス名とバージョンを使用して ldapdb.properties ファイルを更新します。

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを、IBM Security Directory Server のインストール可能ファイルが保管されているディレクトリーに変更します。
4. **idsLicense** コマンドを実行します。  
./idsLicense

5. ソフトウェアのご使用条件に同意する場合は、1 を入力します。以下から選択することができます。

- 1: ご使用条件に同意する。
- 2: ご使用条件を拒否し、インストールを終了する。
- 3: ご使用条件を印刷する。
- 4: ご使用条件の IBM 以外の条項を見る。
- 99: 前の画面に戻る。

ご使用条件に同意すると、IBM Security Directory Server のインストール・ロケーションに LAPIID ファイルと license フォルダが作成されます。ライセンス・フォルダには、サポートされるすべての言語の IBM Security Directory Server ライセンス・ファイルが含まれています。

**重要:** LAPIID ファイルおよびライセンス・フォルダ内のライセンス・ファイルは、変更または削除しないでください。

6. インストールする IBM Security Directory Server パッケージを決定します。

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

インストール可能なすべての IBM Security Directory Server パッケージのリストが表示されます。

7. 以下のコマンドを実行して、パッケージをインストールします。

```
installp -acgXd . package_names
```

すべての IBM Security Directory Server パッケージを現在のパスからインストールするには、以下のコマンドを実行します。

```
installp -acgXd . idsldap
```

8. インストールが完了すると、システムはインストールの要約を生成します。
9. IBM Security Directory Server インストールが正常に終了したかを検証します。詳細については、93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。

## タスクの結果

インストール・プログラムによって、IBM Security Directory Server が AIX システム上の /opt/IBM/ldap/V6.3.1 ディレクトリーにインストールされます。サポート対象バージョンの IBM DB2 がシステムにインストールされている場合は、インストール・プロセスが DB2 のパス名とバージョンを使用して ldapdb.properties ファイルを更新します。

## 次のタスク

IBM Security Directory Server がインストールされたら、以下のアクションを実行する必要があります。

- IBM Security Directory Server を完全なディレクトリー・サーバーとして使用する場合は、ディレクトリー・サーバー・インスタンスを作成してください。詳細については、149 ページの『デフォルトのディレクトリー・サーバー・インスタンスの作成』を参照してください。

- IBM Security Directory Server をプロキシ・サーバーとして使用するには、プロキシ・サーバー・インスタンスを作成してください。詳細については、160ページの『カスタム設定を使用したプロキシ・サーバー・インスタンスの作成』を参照してください。

## Linux ユーティリティを使用したインストール

Linux コマンド行ユーティリティを使用して、Linux システムに IBM Security Directory Server をインストールできます。

IBM Security Directory Server では、オペレーティング・システムおよびアーキテクチャが異なるコンピューターに対して別々のパッケージが提供されています。ご使用のコンピューターにインストールする適切なパッケージを選択する必要があります。パッケージ名について詳しくは、『Linux システムへのインストール用パッケージ』を参照してください。

## Linux システムへのインストール用パッケージ

IBM Security Directory Server を Linux システム上のフル・ディレクトリー・サーバー、プロキシ・サーバー、またはクライアントとして使用するには、適切なパッケージをインストールする必要があります。

### 各種 Linux システムに用意されているパッケージ

表 23. 各種 Linux システム用の IBM Security Directory Server が付属しているパッケージ

IBM Security Directory Server のパッケージ	AMD64 Opteron/EM64T Linux	System i または System p	System x	System z
IBM Directory Server - ライセンス	idsldap-license631-6.3.1-0.x86_64.rpm	idsldap-license631-6.3.1-0.ppc.rpm	idsldap-license631-6.3.1-0.i386.rpm	idsldap-license631-6.3.1-0.s390.rpm
IBM Directory Server - 基本クライアント	idsldap-cltbase631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.ppc.rpm	idsldap-cltbase631-6.3.1-0.i386.rpm	idsldap-cltbase631-6.3.1-0.s390.rpm
IBM Directory Server - 32 ビット・クライアント	idsldap-clt32bit631-6.3.1-0.x86_64.rpm	idsldap-clt32bit631-6.3.1-0.ppc.rpm	idsldap-clt32bit631-6.3.1-0.i386.rpm	idsldap-clt32bit631-6.3.1-0.s390.rpm
IBM Directory Server - 64 ビット・クライアント	idsldap-clt64bit631-6.3.1-0.x86_64.rpm	idsldap-clt64bit631-6.3.1-0.ppc64.rpm	使用不可	idsldap-clt64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Java クライアント	idsldap-cltjava631-6.3.1-0.x86_64.rpm	idsldap-cltjava631-6.3.1-0.ppc.rpm	idsldap-cltjava631-6.3.1-0.i386.rpm	idsldap-cltjava631-6.3.1-0.s390.rpm
IBM Directory Server - 基本サーバー	idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm	idsldap-srvbase64bit631-6.3.1-0.ppc64.rpm	idsldap-srvbase32bit631-6.3.1-0.i386.rpm	idsldap-srvbase64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - プロキシ・サーバー	idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm	idsldap-srvproxy64bit631-6.3.1-0.ppc64.rpm	idsldap-srvproxy32bit631-6.3.1-0.i386.rpm	idsldap-srvproxy64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - 32 ビット・サーバー	使用不可	使用不可	idsldap-srv32bit631-6.3.1-0.i386.rpm	使用不可
IBM Directory Server - 64 ビット・サーバー	idsldap-srv64bit631-6.3.1-0.x86_64.rpm	idsldap-srv64bit631-6.3.1-0.ppc64.rpm	使用不可	idsldap-srv64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Web 管理ツール	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

表 23. 各種 Linux システム用の IBM Security Directory Server が付属しているパッケージ (続き)

IBM Security Directory Server のパッケージ	AMD64 Opteron/EM64T Linux	System i または System p	System x	System z
IBM Directory Server - メッセージ (米国英語)	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 Entitlement (パスポート・アドバンテージでのみ提供される)	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

## パッケージ依存関係

特定のパッケージのインストールについては、まず従属先パッケージをインストールする必要があります。

**注:** IBM Security Directory Server のインストール用にライセンス付き ISO イメージまたはライセンスのアーカイブされたファイル付きクライアント/サーバーを使用する場合、最初にライセンス条項に同意してから `idsldap-license631-6.3.1-0.arch.rpm` パッケージをインストールする必要があります。

次の表では、AMD64 Opteron/EM64T Linux でのパッケージの依存関係が示されています。System z、System i、System p、または System x の Linux の場合は、該当するパッケージ名で置き換えてください。

表 24. パッケージおよびその従属先パッケージ

パッケージ名	従属先
<code>idsldap-clt32bit631-6.3.1-0.x86_64.rpm</code>	<code>idsldap-cltbase631-6.3.1-0.x86_64.rpm</code>
<code>idsldap-clt64bit631-6.3.1-0.x86_64.rpm</code>	<code>idsldap-cltbase631-6.3.1-0.x86_64.rpm</code>
<code>idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm</code>	<ol style="list-style-type: none"> <li><code>idsldap-license631-6.3.1-0.x86_64.rpm</code></li> <li><code>idsldap-cltbase631-6.3.1-0.x86_64.rpm</code></li> <li><code>idsldap-clt64bit631-6.3.1-0.x86_64.rpm</code></li> </ol>
<code>idsldap-srv64bit631-6.3.1-0.x86_64.rpm</code>	<ol style="list-style-type: none"> <li><code>idsldap-license631-6.3.1-0.x86_64.rpm</code></li> <li><code>idsldap-cltbase631-6.3.1-0.x86_64.rpm</code></li> <li><code>idsldap-clt64bit631-6.3.1-0.x86_64.rpm</code></li> <li><code>idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm</code></li> </ol>
<code>idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm</code>	<ol style="list-style-type: none"> <li><code>idsldap-license631-6.3.1-0.x86_64.rpm</code></li> <li><code>idsldap-cltbase631-6.3.1-0.x86_64.rpm</code></li> <li><code>idsldap-clt64bit631-6.3.1-0.x86_64.rpm</code></li> <li><code>idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm</code></li> </ol>

## インストール・シーケンス

これらの機能はすべて同時にインストールすることができます。これらの機能を別々にインストールする場合は、それらを特定の順番でインストールする必要があります。

**重要:** Secure Socket Layer (SSL) または Transport Layer Security (TLS) を使用する  
場合、サポートされているバージョンの IBM Global Security Kit をインストールする  
必要があります。

インストール・シーケンスの例では、AMD64 Opteron/EM64T Linux が使用されて  
います。System z、System i、System p、または System x の Linux の場合は、該  
当するパッケージ名で置き換えてください。

表 25. クライアント機能のインストール・シーケンス

32 ビット・クライアント	64 ビット・クライアント
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

表 26. フル・ディレクトリー・サーバーおよびプロキシ・サーバー機能のインストール・  
シーケンス

フル・ディレクトリー・サーバー 64 ビット	プロキシ・サーバー 64 ビット
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

**注:** Web 管理ツールを使用するには、このツールを Web アプリケーション・サー  
バーにデプロイする必要があります。WebSphere Application Server 組み込みバー  
ジョンのインストールについて詳しくは、121 ページの『手動による WebSphere  
Application Server 組み込みバージョンのインストール』を参照してください。

表 27. Web 管理ツールのインストール・パッケージ

Web 管理ツール
1. idsldap-license631-6.3.1-0.x86_64.rpm
2. idsldap-webadmin631-6.3.1-0.x86_64.rpm

Web 管理ツールをインストールするときに、Directory Services Markup Language  
(DSML) ファイルもコンピューターにコピーされます。DSML について詳しくは、  
279 ページの『付録 A. Directory Services Markup Language (DSML)』を参照してく  
ださい。

## Linux ユーティリティーを使用したインストール

`rpm` コマンドを使用して、Linux システムで IBM Security Directory Server のインストールを実行します。

### 始める前に

IBM Security Directory Server インストール・メディアを準備する必要があります。6 ページの『インストール・メディアの準備』を参照してください。

### このタスクについて

`rpm` インストール・プログラムは、Linux システムに IBM Security Directory Server をインストールします。サポート対象バージョンの IBM DB2 がシステムにインストールされている場合は、インストール・プロセスが DB2 のパス名とバージョンを使用して `ldapdb.properties` ファイルを更新します。

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを、IBM Security Directory Server のインストール可能ファイルが保管されているディレクトリーに変更します。
4. `idsLicense` コマンドを実行します。

```
./idsLicense
```

5. ソフトウェアのご使用条件に同意する場合は、1 を入力します。以下から選択することができます。
  - 1: ご使用条件に同意する。
  - 2: ご使用条件を拒否し、インストールを終了する。
  - 3: ご使用条件を印刷する。
  - 4: ご使用条件の IBM 以外の条項を見る。
  - 99: 前の画面に戻る。

ご使用条件に同意すると、IBM Security Directory Server のインストール・ロケーションに Lapid ファイルと license フォルダが作成されます。ライセンス・フォルダには、サポートされるすべての言語の IBM Security Directory Server ライセンス・ファイルが含まれています。

**重要:** Lapid ファイルおよびライセンス・フォルダ内のライセンス・ファイルは、変更または削除しないでください。

6. 以下のコマンドを実行して、パッケージをインストールします。

```
rpm -ivh package_name
```

すべての IBM Security Directory Server パッケージをインストールするには、以下のコマンドを実行します。

```
rpm -ivh idsldap*
```

7. IBM Security Directory Server インストールが正常に終了したかを検証します。詳細については、93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。

## タスクの結果

インストール・プログラムによって、IBM Security Directory Server が Linux システム上の `opt/ibm/ldap/V6.3.1` ディレクトリーにインストールされます。サポート対象バージョンの IBM DB2 がシステムにインストールされている場合は、インストール・プロセスが DB2 のパス名とバージョンを使用して `ldapdb.properties` ファイルを更新します。

## 次のタスク

IBM Security Directory Server がインストールされたら、以下のアクションを実行する必要があります。

- IBM Security Directory Server を完全なディレクトリー・サーバーとして使用する場合は、ディレクトリー・サーバー・インスタンスを作成してください。詳細については、149 ページの『デフォルトのディレクトリー・サーバー・インスタンスの作成』を参照してください。
- IBM Security Directory Server をプロキシ・サーバーとして使用するには、プロキシ・サーバー・インスタンスを作成してください。詳細については、160 ページの『カスタム設定を使用したプロキシ・サーバー・インスタンスの作成』を参照してください。

---

## Solaris ユーティリティーを使用したインストール

Solaris コマンド行ユーティリティーを使用して、Solaris システムに IBM Security Directory Server をインストールできます。

IBM Security Directory Server では、異なるアーキテクチャーのコンピューターに対して同じパッケージのセットが提供されます。Sun SPARC Solaris および AMD64 Opteron/EM64T Solaris オペレーティング・システムで使用可能なパッケージがあります。パッケージ名およびファイル名は、どちらのオペレーティング・システムでも同じです。パッケージ名について詳しくは、『Solaris システムへのインストール用パッケージ』を参照してください。

IBM Security Directory Server パッケージをインストールするときは、システム・デフォルトの「ALL (すべて)」を使用しないでください。「ALL (すべて)」のパッケージの選択を使用すると、システムはパッケージの順序を正しく処理できないため、インストールは失敗します。

## Solaris システムへのインストール用パッケージ

IBM Security Directory Server を Solaris システム上のフル・ディレクトリー・サーバー、プロキシ・サーバー、またはクライアントとして使用するには、適切なパッケージをインストールする必要があります。

### Solaris システムに用意されているパッケージ

**重要:** パッケージ名およびファイル名は、Solaris SPARC および AMD64 Opteron/EM64T Solaris のオペレーティング・システムで同じです。

表 28. 各種 Solaris システム用の IBM Security Directory Server が付属しているパッケージ

IBM Security Directory Server のパッケージ	パッケージ名	ファイル名
IBM Directory Server - ライセンス	IDS1license631	idsldap-license631.pkg
IBM Directory Server - 基本クライアント	IDS1bc631	idsldap.cltbody631.pkg
IBM Directory Server - 32 ビット・クライアント	IDS132c631	idsldap.cltbody32bit631.pkg
IBM Directory Server - 64 ビット・クライアント	IDS164c631	idsldap.cltbody64bit631.pkg
IBM Directory Server - Java クライアント	IDS1jc631	idsldap.cltbodyjava631.pkg
IBM Directory Server - 基本サーバー	IDS1bs631	idsldap.srvbase64bit631.pkg
IBM Directory Server - プロキシ・サーバー	IDS164p631	idsldap.srvproxy64bit631.pkg
IBM Directory Server - 64 ビット・サーバー	IDS164s631	idsldap.srv64bit631.pkg
IBM Directory Server - Web 管理ツール	IDS1web631	idsldap.webadmin631.pkg
IBM Directory Server - メッセージ (米国英語)	IDS1en631	idsldap.msg631.en.pkg
IBM Directory Server Entitlement (パ スポート・アドバンテージでのみ提供 される)	IDS1ent631	idsldap.ent631.pkg

## パッケージ依存関係

特定のパッケージのインストールについては、まず従属先パッケージをインストールする必要があります。

表 29. パッケージおよびその従属先パッケージ

パッケージ名	従属先
idsldap.cltbody32bit631.pkg	idsldap.cltbody631.pkg
idsldap.cltbody64bit631.pkg	idsldap.cltbody631.pkg
idsldap.srvbase64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbody631.pkg 3. idsldap.cltbody64bit631.pkg
idsldap.srv64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbody631.pkg 3. idsldap.cltbody64bit631.pkg 4. idsldap.srvbase64bit631.pkg
idsldap.srvproxy64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbody631.pkg 3. idsldap.cltbody64bit631.pkg 4. idsldap.srvbase64bit631.pkg

## インストール・シーケンス

各パッケージを Solaris システムにインストールする際は、それらのパッケージを特定の順番でインストールする必要があります。

**重要:** Secure Socket Layer (SSL) または Transport Layer Security (TLS) を使用する  
場合、サポートされているバージョンの IBM Global Security Kit をインストールする  
必要があります。

表 30. クライアント機能のインストール・シーケンス

32 ビット・クライアント	64 ビット・クライアント
1. idsldap.cltbase631.pkg	1. idsldap.cltbase631.pkg
2. idsldap.clt32bit631.pkg	2. idsldap.clt64bit631.pkg
3. idsldap.cltjava631.pkg	3. idsldap.cltjava631.pkg

**注:** IBM Security Directory Server のインストール用にライセンス付き ISO イメージ  
またはライセンスのアーカイブされたファイル付きクライアント/サーバーを使用  
する場合、最初にライセンス条項に同意してから idsldap-license631.pkg パッケージ  
をインストールする必要があります。

表 31. フル・ディレクトリー・サーバーおよびプロキシ・サーバー機能のインストール・  
シーケンス

フル・ディレクトリー・サーバー 64 ビット	プロキシ・サーバー 64 ビット
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

**注:** Web 管理ツールを使用するには、このツールを Web アプリケーション・サー  
バーにデプロイする必要があります。WebSphere Application Server 組み込みバー  
ジョンのインストールについて詳しくは、121 ページの『手動による WebSphere  
Application Server 組み込みバージョンのインストール』を参照してください。

表 32. Web 管理ツールのインストール・パッケージ

Web 管理ツール
1. idsldap-license631.pkg
2. idsldap.webadmin631.pkg

Web 管理ツールをインストールするときに、Directory Services Markup Language  
(DSML) ファイルもコンピューターにコピーされます。DSML について詳しくは、  
279 ページの『付録 A. Directory Services Markup Language (DSML)』を参照してく  
ださい。

## Solaris ユーティリティーを使用したインストール

**pkgadd** コマンドを使用して、Solaris システムで IBM Security Directory Server の  
インストールを実行します。

## 始める前に

IBM Security Directory Server インストール・メディアにアクセスします。6 ページの『インストール・メディアの準備』を参照してください。

## このタスクについて

**pkgadd** インストール・プログラムは、Solaris システムに IBM Security Directory Server をインストールします。サポート対象バージョンの IBM DB2 がシステムにインストールされている場合は、インストール・プロセスが DB2 のパス名とバージョンを使用して `ldapdb.properties` ファイルを更新します。

## 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを、IBM Security Directory Server のインストール可能ファイルが保管されているディレクトリーに変更します。
4. **idsLicense** コマンドを実行します。

```
./idsLicense
```

5. ソフトウェアのご使用条件に同意する場合は、1 を入力します。以下から選択することができます。
  - 1: ご使用条件に同意する。
  - 2: ご使用条件を拒否し、インストールを終了する。
  - 3: ご使用条件を印刷する。
  - 4: ご使用条件の IBM 以外の条項を見る。
  - 99: 前の画面に戻る。

ご使用条件に同意すると、IBM Security Directory Server のインストール・ロケーションに Lapid ファイルと `license` フォルダが作成されます。ライセンス・フォルダには、サポートされるすべての言語の IBM Security Directory Server ライセンス・ファイルが含まれています。

**重要:** Lapid ファイルおよびライセンス・フォルダ内のライセンス・ファイルは、変更または削除しないでください。

6. 以下のコマンドを実行して、パッケージをインストールします。

**注:** Solaris システムでは、IBM Security Directory Server パッケージを特定の順序でインストールする必要があります。詳細については、84 ページの『Solaris システムへのインストール用パッケージ』を参照してください。

```
pkgadd -d package_name
```

7. IBM Security Directory Server インストールが正常に終了したかを検証します。詳細については、93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。

## タスクの結果

インストール・プログラムによって、IBM Security Directory Server が Solaris システム上の `/opt/IBM/ldap/V6.3.1` ディレクトリーにインストールされます。サポー

ト対象バージョンの IBM DB2 がシステムにインストールされている場合は、インストール・プロセスが DB2 のパス名とバージョンを使用して `ldapdb.properties` ファイルを更新します。

## 次のタスク

IBM Security Directory Server がインストールされたら、以下のアクションを実行する必要があります。

- IBM Security Directory Server を完全なディレクトリー・サーバーとして使用する場合は、ディレクトリー・サーバー・インスタンスを作成してください。詳細については、149 ページの『デフォルトのディレクトリー・サーバー・インスタンスの作成』を参照してください。
- IBM Security Directory Server をプロキシ・サーバーとして使用するには、プロキシ・サーバー・インスタンスを作成してください。詳細については、160 ページの『カスタム設定を使用したプロキシ・サーバー・インスタンスの作成』を参照してください。

---

## HP-UX ユーティリティーを使用したインストール

HP-UX コマンド行ユーティリティーを使用して、HP-UX システムに IBM Security Directory Server をインストールできます。

IBM Security Directory Server は、Itanium システム (Intel IA64 プロセッサベースのサーバー) 上の HP-UX に対してクライアントのみのパッケージを提供します。詳細については、『HP-UX Itanium システムへのインストール用パッケージ』を参照してください。

## HP-UX Itanium システムへのインストール用パッケージ

IBM Security Directory Server を HP-UX システム上のクライアントとして使用するには、適切なパッケージをインストールする必要があります。

### HP-UX システムに用意されているパッケージ

IBM Security Directory Server では、HP-UX on Itanium システム (Intel IA64 プロセッサ・ベースのサーバー) 用のクライアントのみのパッケージを提供しています。

表 33. HP-UX システム用の IBM Security Directory Server が付属しているパッケージ

IBM Security Directory Server のパッケージ	パッケージ名
IBM Directory Server - 基本クライアント	<code>idsldap.clbase631.depot</code>
IBM Directory Server - 32 ビット・クライアント	<code>idsldap.clt32bit631.depot</code>
IBM Directory Server - 64 ビット・クライアント	<code>idsldap.clt64bit631.depot</code>
IBM Directory Server - Java クライアント	<code>idsldap.cltjava631.depot</code>
IBM Directory Server - ライセンス	<code>idsldap.license631.depot</code>

### パッケージ依存関係

特定のパッケージのインストールについては、まず従属先パッケージをインストールする必要があります。

表 34. パッケージおよびその従属先パッケージ

パッケージ名	従属先
idsldap.clt32bit631.depot	idsldap.cltbase631.depot
idsldap.clt64bit631.depot	idsldap.cltbase631.depot

## インストール・シーケンス

各パッケージを HP-UX システムにインストールする際は、それらのパッケージを特定の順番でインストールする必要があります。

**重要:** Secure Socket Layer (SSL) または Transport Layer Security (TLS) を使用する場合、サポートされているバージョンの IBM Global Security Kit をインストールする必要があります。

表 35. クライアント機能のインストール・シーケンス

32 ビット・クライアント	64 ビット・クライアント
1. idsldap.cltbase631.depot	1. idsldap.cltbase631.depot
2. idsldap.clt32bit631.depot	2. idsldap.clt64bit631.depot
3. idsldap.cltjava631.depot	3. idsldap.cltjava631.depot

## HP-UX ユーティリティーを使用したインストール

`swinstall` コマンドを使用して、HP-UX システムで IBM Security Directory Server のインストールを実行することができます。

### 始める前に

IBM Security Directory Server インストール・メディアを準備する必要があります。6 ページの『インストール・メディアの準備』を参照してください。

### このタスクについて

`swinstall` インストール・プログラムは、HP-UX システムに IBM Security Directory Server をインストールします。サポート対象バージョンの IBM DB2 がシステムにインストールされている場合は、インストール・プロセスが DB2 のパス名とバージョンを使用して `ldapdb.properties` ファイルを更新します。

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを、IBM Security Directory Server のインストール可能ファイルが保管されているディレクトリーに変更します。
4. 以下のコマンドを実行して、パッケージをインストールします。

```
swinstall -s sds_installable_path/idsldap.cltbase631.depot ¥*
swinstall -s sds_installable_path/idsldap.clt32bit631.depot ¥*
swinstall -s sds_installable_path/idsldap.clt64bit631.depot ¥*
swinstall -s sds_installable_path/idsldap.cltjava631.depot ¥*
```

5. IBM Security Directory Server インストールが正常に終了したかを検証します。  
詳細については、93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。

### **タスクの結果**

インストール・プログラムによって、IBM Security Directory Server が HP-UX システム上の /opt/IBM/ldap/V6.3.1 ディレクトリーにインストールされます。

---

## 第 13 章 IBM Security Directory Server の機能の検証

IBM Security Directory Server のインストール、変更、またはアンインストール後に、IBM Security Directory Server の各機能が正しくインストール、変更、またはアンインストールされたかどうかを検証する必要があります。

インストール、変更、またはアンインストールが正常に完了したかどうかを検証するために、IBM Installation Manager またはオペレーティング・システムのユーティリティーを使用することができます。

---

### IBM Installation Manager を使用した IBM Security Directory Server 機能の検証

IBM Installation Manager を使用して、IBM Installation Manager によってインストールした IBM Security Directory Server の機能および相互前提条件製品を検証します。

#### 手順

1. IBM Installation Manager を始動します。

##### Windows

「スタート」メニューで、「すべてのプログラム」 > 「IBM Installation Manager」 > 「IBM Installation Manager」をクリックします。

##### AIX および Linux

コマンド・プロンプトで、以下のコマンドを入力します。IBM Installation Manager が別のロケーションにインストールされている場合は、以下のデフォルト・パスを変更します。

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

2. 「IBM Installation Manager」ページで、「ファイル」 > 「インストール済みパッケージの表示」をクリックします。
3. 「インストール済みパッケージ」ページ内の「インストール済みパッケージおよびフィックス」のリストで、「IBM Security Directory Server」を展開します。
4. 「インストール済みパッケージおよびフィックス」のリストで、機能を確認する IBM Security Directory Server のバージョンをクリックします。
5. 「詳細」エリアの下で、機能と相互前提条件製品のインストールを検証します。
6. 「インストール済みパッケージ」ページを閉じるには、「閉じる」をクリックします。
7. 「IBM Installation Manager」を閉じるには、「ファイル」 > 「終了」をクリックします。

## IBM Security Directory Server 機能の Windows 上での検証

Microsoft Windows レジストリーを確認することによって、IBM Security Directory Server のインストール、変更、またはアンインストールが正常に完了したかどうかを検証することができます。

### このタスクについて

Microsoft Windows では、Windows システム上に存在するソフトウェアを追跡するためにレジストリー項目が維持されます。IBM Security Directory Server 機能が正常にインストール、変更、またはアンインストールされた後に、システムに対する最新の更新を記録するためにレジストリー項目が変更されます。IBM Security Directory Server 機能が正常にインストールの後にレジストリー項目の例が示されます。IBM Security Directory Server 機能を変更またはアンインストールすると、これらの機能を追跡するレジストリー項目が、最新の状況を示すように変更されます。レジストリー項目は、AMD64/EM64T アーキテクチャー上の Microsoft Windows に対して表示されます。

### 手順

1. 管理者特権で Windows システムにログオンします。
2. コマンド・プロンプトにアクセスして、以下のコマンドを実行します。

```
regedit
```

3. 「レジストリ エディタ」ウィンドウで、「マイ コンピュータ」 > 「HKEY\_LOCAL\_MACHINE」 > 「SOFTWARE」 > 「Wow6432NODE」 > 「IBM」 > 「IDSLDAP」 > 「6.3.1」をクリックします

注: IBM Security Directory Server のインストールを Intel x86 (IA32) アーキテクチャー上の Microsoft Windows システムで検証するには、「マイ コンピュータ」 > 「HKEY\_LOCAL\_MACHINE」 > 「SOFTWARE」 > 「IBM」 > 「IDSLDAP」 > 「6.3.1」と展開します。

My Computer¥HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Wow6432NODE¥IBM¥IDSLDAP¥6.3.1 は、システムにインストールされている IBM Security Directory Server 機能のメジャー・バージョンを示しています。

```
BaseServerMajorVersion    6.3.1
BitMode                    64
ClientMajorVersion        6.3.1
JavaClientMajorVersion    6.3.1
LDAPHome                   installation_location
ProxyServerMajorVersion   6.3.1
ServerMajorVersion        6.3.1
WebadminMajorVersion      6.3.1
WebSphereAppSrvMajorVersion 7.0
```

システムにインストールされていて、My

Computer¥HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Wow6432NODE¥IBM¥IDSLDAP¥6.3.1 の下に表示される IBM Security Directory Server 機能のマイナー・バージョン。以下に例を示します。

```
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. 「レジストリ エディタ」ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックします。

---

## IBM Security Directory Server パッケージの検証

IBM Security Directory Server パッケージのシステムを確認することによって、IBM Security Directory Server のインストールが正常に完了しているかどうかを検証することができます。

### このタスクについて

IBM Security Directory Server のインストール後に、各パッケージが必要なレベルにあることを確認する必要があります。IBM Security Directory Server パッケージのバージョン番号を照会できます。

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスして、以下のコマンドを実行します。

オペレーティング・システム	パッケージを照会するコマンド:
AIX	lsllpp -l 'idsldap*'
Linux	rpm -qa   grep -i idsldap
Solaris	pkginfo   grep IDS1 pkgparam package_name VERSION
HP-UX	swlist   grep -i idsldap

### タスクの結果

このコマンドでは、システムにインストールされている IBM Security Directory Server パッケージをリストします。

---

## Web 管理ツールのバージョンの検証

Web 管理ツールのインストールまたはアップグレードが正常に完了したかどうかを検証するには、Web 管理ツールのバージョンを検証する必要があります。

## 手順

1. 管理者特権でログインします。
2. `ds_install_location/idstools` ディレクトリーに移動します。  
`ds_install_location` は IBM Security Directory Server のインストール・ロケーションです。以下のロケーションが、各オペレーティング・システムのデフォルトのロケーションです。

表 36. 各オペレーティング・システム上のデフォルトの IBM Security Directory Server のインストール・ロケーション

オペレーティング・システム	デフォルトのインストール・ロケーション:
Microsoft Windows	c:\Program Files\IBM\ldap\6.3.1
AIX および Solaris	/opt/IBM/ldap/V6.3.1
Linux	/opt/ibm/ldap/V6.3.1

3. 以下のコマンドを実行します。

オペレーティング・システム	実行するコマンド:
Microsoft Windows	deploy_IDSWebApp.bat -v
AIX、Linux、および Solaris	deploy_IDSWebApp -v

このコマンドには以下の情報が表示されます。

- `deploy_IDSWebApp` コマンドのバージョンと日付の値。
- インストール済みの `IDSWebApp.war` ファイルのバージョンと日付の値。
- 現在デプロイ済みの `IDSWebApp.war` ファイルのバージョンと日付の値。

## 次のタスク

次の各値を確認する必要があります。

1. インストール済みの `IDSWebApp.war` ファイルのバージョンと日付の値が、現在デプロイ済みの `IDSWebApp.war` ファイルのバージョンと日付の値と異なるかどうか。
2. これらの値が異なる場合、最新の Web 管理ツールを Web アプリケーション・サーバーにデプロイします。

---

## IBM Global Security Kit の Windows へのインストールの検証

IBM Global Security Kit (GSKit) のインストール状況を検証して、Windows へのインストールが正常に完了したかどうかを確認します。

### 手順

1. `gskitinst.log` ファイルにアクセスします。

オペレーティング・システム	デフォルト・パス:
Windows	C:\Program Files\IBM\ldap\6.3.1\var

2. 以下のディレクトリーが作成されたかどうかを確認します。 `C:\Program Files\IBM\gsk8`

3. gskitinst.log ファイルに値の EXIT 0 が含まれているかどうかを確認します。  
IBM Global Security Kit のインストールが正常に完了した場合は 0 が設定され、そうでない場合はゼロ以外の値が設定されます。
4. オプション: IBM Global Security Kit のインストールが正常に完了しなかった場合は、エラーの詳細が C:\Program Files\IBM\dap\6.3.1\var\gskitinsterr.log ファイル内に格納されます。

---

## IBM Global Security Kit の AIX、Linux、Solaris、および HP-UX へのインストールの検証

IBM Global Security Kit (GSKit) のインストールを検証して、インストールが正常に完了したかどうかを確認します。

### このタスクについて

IBM Global Security Kit のインストール後に、各パッケージが必要なレベルにあることを確認する必要があります。IBM Global Security Kit のバージョン番号を照会できます。

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスして、以下のコマンドを実行します。

オペレーティング・システム	実行するコマンド:
AIX	lslpp -a   grep -i gsk
Linux	rpm -qa   grep -i gsk
Solaris	pkginfo   grep gsk pkgparam package_name VERSION
HP-UX	swlist   grep -i gsk



---

## 第 14 章 前バージョンのインスタンスのアップグレード

既存のインスタンスを最新リリースの機能を持つインスタンスに変換し、既存の構成ファイルを使用して続行するには、インスタンスをアップグレードする必要があります。

アップグレード処理では、スキーマ定義に対する変更内容、構成ファイルに対する変更内容、および Directory Server インスタンスのデータが保持されます。

インスタンスを前のバージョンからアップグレードするには、以下のプロセスを実行する必要があります。

1. IBM Security Directory Server のインストールを完了します。
2. 既存のインスタンスを前バージョンからアップグレードします。

IBM Security Directory Server バージョン 6.3.1 のサーバーおよびクライアントは、バージョン 6.0、6.1、6.2、および 6.3 のサーバーおよびクライアントと共存できます。

以下のバージョンのディレクトリー・サーバー・インスタンスは、IBM Security Directory Server バージョン 6.3.1 に直接アップグレードできます。

- IBM Security Directory Server バージョン 6.3
- IBM Security Directory Server バージョン 6.2
- IBM Security Directory Server バージョン 6.1

**重要:** IBM Security Directory Server バージョン 6.0 のインスタンスから IBM Security Directory Server バージョン 6.3.1 への直接アップグレードは、サポートされません。6.0 インスタンスを 6.1、6.2、または 6.3 にアップグレードしてから 6.3.1 にアップグレードすることはできます。

前のバージョンのインスタンスは、以下の方法でアップグレードできます。

- ローカル・コンピューター上の既存のインスタンスを、IBM Security Directory Server インスタンス管理ツール (`idsxinst`) または `idsimigr` コマンドを使用してアップグレードします。アップグレードするディレクトリー・サーバー・インスタンスは除去しないでください。フル・ディレクトリー・サーバー・インスタンスの場合は、データベースを構成解除しないでください。ディレクトリー・サーバー・インスタンスが除去されたり、そのデータベースが構成解除されたりした場合、アップグレードはサポートされません。
- リモート・コンピューター上のインスタンスを、`migbkup` および `idsimigr` コマンドでアップグレードします。詳細については、103 ページの『`idsimigr` コマンドを使用した前のバージョンのリモート・インスタンスのアップグレード』を参照してください。

**重要:** アップグレード障害から復旧するために、インスタンスのスキーマ、構成ファイル、およびデータベースをバックアップする必要があります。

## DB2 データベースのアップグレード

インスタンスをアップグレードするときに、その関連付けられた DB2 データベースも、DB2 バージョンが IBM Security Directory Server バージョン 6.3.1 によってサポートされているバージョンよりも低い場合はアップグレードされます。DB2 データベースをアップグレードするために、`idsdbmigr` コマンドが内部で実行されます。

**重要:** DB2 バージョン 9.1 で構成したディレクトリー・サーバー・インスタンスを DB2 バージョン 10.1.0.2 以上で構成したインスタンスに直接アップグレードする操作はサポートされていません。DB2 バージョン 9.1 で構成したインスタンスを DB2 バージョン 10.1.0.2 以上で構成したインスタンスにアップグレードするには、以下のいずれかの方法を使用します。

- DB2 バージョン 9.1 を使用したインスタンスを、DB2 バージョン 9.5 を使用したインスタンスにアップグレードした後、DB2 バージョン 10.1.0.2 以上を使用したインスタンスにアップグレードする。
- DB2 バージョン 9.1 を使用したインスタンスを、DB2 バージョン 9.7 を使用したインスタンスにアップグレードした後、DB2 バージョン 10.1.0.2 以上を使用したインスタンスにアップグレードする。

## クライアント・インストールのアップグレード

IBM Security Directory Server クライアント・インストーラーを使用して、クライアント専用機能をインストールした場合、アップグレードは必要ありません。バージョン 6.0、6.1、6.2、および 6.3 のクライアントは、6.3.1 のサーバーおよびクライアントと共存できます。

---

## インスタンスをアップグレードする前の環境の設定

既存のインスタンスをアップグレードする前に、ディレクトリー・サーバー環境をセットアップする必要があります。

### 始める前に

環境を設定する前に、以下のタスクを実行する必要があります。

- IBM Security Directory Server インストール・メディアにアクセスします。
- IBM Security Directory Server バージョン 6.3.1 のインストールを完了します。31 ページの『インストールの開始』を参照してください。
- AIX、Linux、または Solaris オペレーティング・システムでは root ユーザーとしてログインし、Windows オペレーティング・システムでは管理者グループのメンバーとしてログインします。

### 手順

1. アップグレードするインスタンスが存在するオペレーティング・システムが、IBM Security Directory Server バージョン 6.3.1 でサポートされていることを確認します。
2. アップグレードする前バージョンのインスタンスが正常に始動することを確認します。ディレクトリー・サーバー・インスタンスをアップグレードする場合は、データベースを構成する必要があります (まだ構成されていない場合)。

**重要:** サーバーを正常に始動できない場合は、プロキシ・サーバーまたはディレクトリー・サーバーのアップグレードがサポートされません。

- アップグレードするインスタンスのオフライン・バックアップを実行します。ディレクトリー・サーバー・インスタンスの場合は、DB2 データベースと DB2 設定をバックアップします。**idsdbback** コマンドについて詳しくは、「*Command Reference*」を参照してください。
- スキーマ・ファイルおよび構成ファイルをバックアップするには、以下の **migbkup** コマンドを実行します。

オペレーティング・システム	実行するコマンド:
Microsoft Windows	<b>migbkup.bat</b> drive_name%idsslapped-instance_name backup_directory
AIX、Linux、および Solaris	<b>migbkup</b> user_home_dir/idsslapped-instance_name backup_directory

**migbkup** コマンドは、IBM Security Directory Server インストール・メディアの tools サブディレクトリーにあります。IBM Security Directory Server のインストールが完了している場合は、**migbkup** コマンドが IBM Security Directory Server インストール・ロケーションの sbin フォルダーにあります。各種オペレーティング・システムでのデフォルトのインストール・ロケーションは、以下のディレクトリーです。

#### Microsoft Windows

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

#### AIX および Solaris

/opt/IBM/ldap/V6.3.1

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

**migbkup** コマンドは、以下のファイルをバックアップします。

- 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` (Windows の場合)
- `ibmslapdService.cmd` (Windows の場合)

**migbkup** コマンドは、以下のファイルを作成します。

- `db2info` には、ディレクトリー・サーバー・インスタンスが使用する DB2 のパス名とバージョン情報が含まれています。ディレクトリー・サーバー・インスタンスをアップグレードすると、**idsimigr** コマンドまたはインスタンス管理ツールが、このファイルを使用して DB2 インスタンスとデータベースをアップグレードします。プロキシー・サーバー・インスタンスの場合は、このファイルを使用できません。
  - `platforminfo` には、オペレーティング・システムおよびプロセス・タイプに関する情報が含まれています。
5. アップグレードするインスタンスの `V3.modifiedschema` ファイルを手動で変更した場合は、このファイルでオブジェクト・クラスまたは属性のオブジェクト ID (OID) が重複しないようにする必要があります。このファイルで OID が重複していると、アップグレード時にそれらの ID が保持されません。スキーマ・ファイルで OID が重複している場合は、`V3.modifiedschema` 内の OID が保持されます。スキーマ・ファイルに属性またはオブジェクト・クラスが含まれていない場合は、管理サーバーと `idsslapd` プロセスを始動できない可能性があります。このような場合にサーバーを始動するには、不足している属性またはオブジェクト・クラスをスキーマ・ファイルに手動で追加する必要があります。
  6. カスタム・スキーマ・ファイルを使用してインスタンスを構成した場合は、それらのファイルを手動でバックアップ・ディレクトリーにコピーします。スキーマ・ファイルと構成ファイルをバックアップすると、**migbkup** コマンドによってカスタム・スキーマ・ファイルがバックアップされます。ただし、インスタンスをアップグレードすると、これらのスキーマ・ファイルが使用されなくなる場合があります。

## 次のタスク

環境をセットアップしたら、**idsimigr** コマンドまたはインスタンス管理ツールを実行して、インスタンスを前バージョンからアップグレードします。インスタンスをアップグレードするには、以下の方法のいずれかを使用します。

- 『**idsimigr** コマンドを使用した前のバージョンのインスタンスのアップグレード』
- 165 ページの『インスタンス管理ツールを使用した前のバージョンのインスタンスのアップグレード』

---

## idsimigr コマンドを使用した前のバージョンのインスタンスのアップグレード

**idsimigr** コマンドを使用して、前のバージョンのディレクトリー・サーバー・インスタンスまたはプロキシー・サーバー・インスタンスを現在のバージョンにアップグレードします。

## 始める前に

**idsimigr** コマンドを使用してインスタンスをアップグレードする前に、以下のタスクを完了する必要があります。

- IBM Security Directory Server インストールを完了します。31 ページの『インストールの開始』を参照してください。
- インスタンスをアップグレードする前に、環境をセットアップします。98 ページの『インスタンスをアップグレードする前の環境の設定』を参照してください。
- AIX、Linux、または Solaris オペレーティング・システムでは root ユーザーとしてログインし、Windows オペレーティング・システムでは管理者グループのメンバーとしてログインします。

インスタンス管理ツールを使用して、コンピューター上に存在するインスタンスをアップグレードすることもできます。詳細については、165 ページの『インスタンス管理ツールを使用した前のバージョンのインスタンスのアップグレード』を参照してください。

## このタスクについて

前のバージョンのインスタンスをアップグレードした後、そのインスタンスは IBM Security Directory Server の現行バージョンバージョンの完全に機能するインスタンスに変換されます。

## 手順

1. コマンド・プロンプトにアクセスします。
2. 現在の作業ディレクトリーを `sbin` に変更します。次のデフォルトのロケーションが、各オペレーティング・システム上のデフォルトです。

### Microsoft Windows

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

### AIX および Solaris

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

### Linux

```
/opt/ibm/ldap/V6.3.1/sbin
```

3. アップグレードを計画しているインスタンスの `ibmslapd` プロセスと管理サーバーを停止します。

```
ibmslapd -I instance_name -k  
ibmdiradm -I instance_name -k
```

4. アップグレードを計画しているインスタンスに関連付けられている IBM Security Directory Server 製品バージョンをアンインストールしないでください。

5. **idsimigr** コマンドを実行して、インスタンスを前のバージョンから現行バージョンの IBM Security Directory Server にアップグレードします。

```
idsimigr -I instance_name
```

6. インスタンスの `ibmslapd` プロセスと管理サーバーを始動します。

```
ibmslapd -I instance_name -n  
ibmdiradm -I instance_name
```

7. インスタンスのオフライン・バックアップを実行します。212 ページの『ディレクトリー・サーバーのバックアップ』を参照してください。

## 別のコンピューターに対する前のバージョンのインスタンスのアップグレード

あるコンピューター上にある前のバージョンの既存のインスタンスを、別のコンピューター上で後のバージョンにアップグレードできます。

以下のいずれかの理由で、既存のインスタンスをリモート側でアップグレードした方がよい場合もあります。

- 前のバージョンのインスタンスが存在するコンピューター上のオペレーティング・システムが、IBM Security Directory Server バージョン 6.3.1 によってサポートされているオペレーティング・システムではない場合があります。そのコンピューター上でオペレーティング・システムをアップグレードまたは変更しない方がよい場合もあります。
- IBM Security Directory Server バージョン 6.3.1 を、前のバージョンが存在するオペレーティング・システムとは異なるオペレーティング・システムを使用するコンピューターにインストールしたい場合があります。ただし、前のバージョンの既存のインスタンスとしての情報を持つインスタンスを作成する必要があります。例えば、AMD64/EM64T Linux システム上に前のバージョンの既存のインスタンスがあるが、AIX システム上に 6.3.1 サーバーを配置するとします。そのような場合、2 つのオペレーティング・システムのエンディアン・タイプが同じである必要があります。最初のコンピューターがリトル・エンディアンである場合、2 番目のシステムもリトル・エンディアンである必要があります。エンディアン・タイプは、メモリー内でデータを表現するときに使用されるビットの配列に関わります。オペレーティング・システムのエンディアン・タイプが同じでない場合、インスタンスのアップグレードはサポートされません。

リモート・アップグレードの手順は同じコンピューター上でのアップグレードの手順と似ています。例外となる点は、コンピューターにあるバックアップ・ファイルを、IBM Security Directory Server バージョン 6.3.1 をインストールしたコンピューターにコピーする必要があるということです。

**注:** 複製に参加するコンピューターからリモート・インスタンスをアップグレードするには、以下のアクションを実行します。

- ソース・システムをサプライヤーとして複製を有効にします。
- ターゲット・システムをコンシューマーとして複製を有効にします。

複製を使用すると、更新情報はキューに入れられ、ターゲット・システムがオンラインになったときに複製できます。ソース・システム上のインスタンスをバックアップする前に、複製を使用可能にする必要があります。

### リモート・インスタンスのアップグレード用にサポートされるオペレーティング・システム

リモート・インスタンスを適切なターゲット・オペレーティング・システムでアップグレードするには、インスタンスのソースとターゲットのオペレーティング・システムを特定する必要があります。

表 37. リモート・インスタンス・アップグレード用にサポートされるソースおよびターゲットのオペレーティング・システム

	オペレーティング・システム: ターゲット・システム (IBM Security Directory Server バージョン 6.3.1)								
オペレーティング・システム: ソース・システム (IBM Security Directory Server 6.3 以前) ↓	Intel 32 ビット Windows	AMD64/EM64T Windows	System x Linux (32 ビット)	AMD64/EM64T Linux	System i and System p Linux	System z Linux	AIX	Solaris SPARC	Solaris X64
Intel 32 ビット Windows	✓	✓	✓	✓					✓
AMD/EM64T Windows	✓	✓	✓	✓					✓
System x Linux (32 ビット)	✓	✓	✓	✓					✓
AMD/EM64T Linux	✓	✓	✓	✓					✓
System i and System p Linux					✓	✓	✓	✓	
System z Linux					✓	✓	✓	✓	
AIX					✓	✓	✓	✓	
Solaris SPARC					✓	✓	✓	✓	
Solaris X64	✓	✓	✓	✓					✓

## idsimigr コマンドを使用した前のバージョンのリモート・インスタンスのアップグレード

-u パラメーターを指定した **idsimigr** コマンドを使用して、前のバージョンのリモートのディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスをバージョン 6.3.1 にアップグレードします。

### 始める前に

-u パラメーターを指定した **idsimigr** コマンドを使用してインスタンスをアップグレードする前に、以下のタスクを完了する必要があります。

- インスタンスをアップグレードする前に、環境をセットアップします。98 ページの『インスタンスをアップグレードする前の環境の設定』を参照してください。

- AIX、Linux、または Solaris オペレーティング・システムでは root ユーザーとしてログインし、Windows オペレーティング・システムでは管理者グループのメンバーとしてログインします。

リモート・インスタンスは、インスタンス管理ツールを使用してバックアップ・ファイルでアップグレードすることもできます。詳細については、167 ページの『インスタンス管理ツールを使用した前のバージョンのリモート・インスタンスのアップグレード』を参照してください。

## このタスクについて

アップグレード処理の完了後に、**idsimigr** コマンドでは、リモート・インスタンスからの情報を使用してコンピューター上に 6.3.1 のインスタンスを作成します。

## 手順

1. **idsdb2ldif** コマンドを使用して、リモート・コンピューター上に存在するディレクトリー・サーバー・インスタンスのデータベースをバックアップします。

**重要:** プロキシ・サーバー・インスタンスをアップグレードしている場合は、データベースをバックアップしないでください。プロキシ・サーバーには、それに関連付けられたデータベースは含まれていません。

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

**idsdb2ldif** コマンドについて詳しくは、「*Command Reference*」を参照してください。

2. リモート・インスタンスのアップグレード対象のコンピューターへの IBM Security Directory Server のインストールを完了させます。31 ページの『インストールの開始』を参照してください。
3. リモート・インスタンスのスキーマ・ファイルおよび構成ファイルをバックアップするには、アップグレード先バージョンの次の **migbkup** コマンドを実行します。

オペレーティング・システム	実行するコマンド:
Microsoft Windows	<b>migbkup.bat</b> drive_name%idsslapped-instance_name backup_directory
AIX、Linux、および Solaris	<b>migbkup</b> user_home_dir/idsslapped-instance_name backup_directory

**migbkup** コマンドは、IBM Security Directory Server インストール・メディアの tools サブディレクトリーにあります。

4. **migbkup** を使用して作成したバックアップ・ディレクトリー backup\_directory を、リモート・コンピューターから IBM Security Directory Server がインストールされたコンピューターにコピーします。
5. オプション: データベース・バックアップ・ファイル inst\_out.ldif を、リモート・コンピューターから IBM Security Directory Server がインストールされたコンピューターにコピーします。
6. **-u** パラメーターを指定した **idsimigr** コマンドを実行して、リモート・インスタンスのバックアップ・データによってインスタンスを作成します。

```
idsimigr -u backup_directory
```

7. ディレクトリー・サーバー・インスタンス用のデータベース、サフィックス、および管理者 DN とパスワードを構成します。

**重要:** プロキシ・サーバー・インスタンスをアップグレードしている場合は、**idscfgdb** コマンドを実行してデータベースを構成しないでください。

```
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. オプション: **idsldif2db** コマンドを実行して、データベース・バックアップ・ファイルの `inst_out.ldif` を、アップグレードされたディレクトリー・サーバー・インスタンスにインポートします。
9. インスタンスの `ibmslapd` プロセスと管理サーバーを始動します。

```
ibmslapd -I instance_name -n
ibmdiradm -I instance_name
```

10. インスタンスのバックアップを実行します。詳細については、212 ページの『ディレクトリー・サーバーのバックアップ』を参照してください。

---

## クライアントおよびサーバー・ユーティリティーへのリンク

**idslink** コマンドを使用して、ディレクトリー・サーバーのコマンド行ユーティリティーおよびライブラリーへのリンクを設定できます。

IBM Security Directory Server をインストールした後で、クライアントおよびサーバー・ユーティリティーのためのリンクを設定できます。これらのリンクは、インストール中に自動的に設定されません。

以前のバージョンの IBM Security Directory Server のユーティリティーへのリンクが構成されている場合、変更しない限り、これらのリンクは残ります。**idslink** コマンドで設定されたリンクを除去するには、**idsrmlink** コマンドを使用します。

**idslink** コマンドを使用して、**idsldapmodify** や **idsldapadd** などのコマンド行ユーティリティーへのリンクや、`libibmldap.so` などのライブラリーへのリンクを設定できます。これらのリンクは、IBM Security Directory Server ユーティリティーおよびライブラリーが格納されているロケーションを指します。

**idslink** および **idsrmlink** コマンドについて詳しくは、「*Command Reference*」を参照してください。



---

## 第 15 章 前バージョンのインスタンスからのデータおよびソリューションの移行

前バージョンのインスタンスで構成されたディレクトリー・データ、ソリューション、またはその両方を、6.3.1 インスタンスで使用するために移行することができます。

### IBM DB2 Enterprise Server Edition (ESE) から IBM DB2 Workspace Server Edition (WSE) への DB2 データの移行

System x Linux (Intel 32 ビット・アーキテクチャー) では、IBM DB2 ESE バージョン 9.7 以降はサポートされません。System x Linux の場合、IBM Security Directory Server は IBM DB2 WSE バージョン 9.7、フィックスパック 6 以降を使用してデータベースの作成および構成を行います。

データを持つ 6.1 または 6.2 のインスタンスを 6.3.1 にアップグレードするとき、インスタンスのリモート・アップグレードを実行することが必要な場合があります。DB2 WSE バージョン 9.7 以降を持つ 6.3 インスタンスを DB2 WSE バージョン 9.7 以降を持つ 6.3.1 インスタンスにアップグレードすることができます。System x Linux の場合、DB2 ESE バージョン 9.1 以降を持つ 6.1 または 6.2 インスタンスから、DB2 WSE バージョン 9.7 以降を持つ 6.3.1 インスタンスへの直接アップグレードは失敗することがあります。DB2 WSE への DB2 ESE データベースの移行方法については詳しくは、108 ページの『DB2 ESE データベースを使用するインスタンスから DB2 WSE データベースを使用するインスタンスへの移行』を参照してください。

### IBM Security Directory Integrator に基づくディレクトリー・サーバー・ソリューションの移行

前のバージョンのインスタンスで構成されたソリューションを、6.3.1 インスタンスと一緒に使用するには、これらのソリューションを移行する必要があります。

以下のソリューションがサポートされています。

- ログ管理ツール
- Simple Network Management Protocol (SNMP)
- Active Directory との同期

ディレクトリー・サーバー・ソリューションについては詳しくは、IBM Security Directory Server 製品資料の『管理』トピックを参照してください。

ソリューションを機能させるには、IBM Security Directory Integrator バージョン 7.1 がコンピューター上になければなりません。IBM Security Directory Integrator のインストールおよび管理については、製品資料 (<http://www-01.ibm.com/support/knowledgecenter/SSCQGF/welcome>) の『インストールと管理』セクションを参照してください。

IBM Security Directory Integrator のインストール・パスが、デフォルトのインストール・パスと異なる場合、IBM Security Directory Integrator のインス

ツール・ロケーションを使用して、*IDS\_LDAP\_TDI\_HOME* 変数を設定します。以下のインストール・パスは、様々なオペレーティング・システム上の IBM Security Directory Integrator バージョン 7.1 に対するデフォルトです。

**AIX、Linux、および Solaris**

/opt/IBM/TDI/V7.1

**Windows**

C:\Program Files\IBM\TDI\V7.1

---

## DB2 ESE データベースを使用するインスタンスから DB2 WSE データベースを使用するインスタンスへの移行

DB2 ESE を使用する 6.1 または 6.2 インスタンスを、DB2 WSE を使用する 6.3.1 インスタンスにアップグレードするには、DB2 ESE データベースから DB2 WSE データベースへとデータを移行します。

### 始める前に

前バージョンのインスタンスから 6.3.1 インスタンスへとデータを移行するには、事前に以下のタスクを実行する必要があります。

- IBM DB2 WSE を使用して IBM Security Directory Server バージョン 6.3.1 のインストールを完了します。31 ページの『インストールの開始』を参照してください。
- インスタンスをアップグレードする前に、環境をセットアップします。98 ページの『インスタンスをアップグレードする前の環境の設定』を参照してください。
- AIX、Linux、または Solaris オペレーティング・システムでは root ユーザーとしてログインし、Windows オペレーティング・システムでは管理者グループのメンバーとしてログインします。

### 手順

1. ディレクトリー・データの移行元となるディレクトリー・サーバー・インスタンスを停止します。
2. IBM Security Directory Server バージョン 6.3.1 で提供されている **migbkup** コマンドを実行して、インスタンスをバックアップします。98 ページの『インスタンスをアップグレードする前の環境の設定』を参照してください。**migbkup** コマンドについて詳しくは、「*Command Reference*」を参照してください。
3. データの移行元となるディレクトリー・サーバー・インスタンスのデータベースをバックアップします。インスタンスのデータベース **dsrdbm01** をバックアップするには、以下の手順を実行します。
  - a. ユーザー・コンテキストを DB2 インスタンス所有者に切り替えます。

```
su - dsrdbm01
```
  - b. このユーザーに対して **db2profile** を実行します。

```
sqllib/db2profile
```
  - c. インスタンスの DB2 データベースをバックアップします。

```
db2 backup database dsrdbm01 to database_backup_directory
```

データベース所有者には、データベース・バックアップ・ディレクトリー `database_backup_directory` に対する読み取り、書き込み、および実行のアクセス権が必要です。

- d. ディレクトリー・サーバー・インスタンスに対して変更ログ・データベースが構成されている場合は、そのデータベースをバックアップします。

```
db2 backup db ldaplog to changelog_backup_directory
```

データベース所有者には、変更ログ・バックアップ・ディレクトリー `database_backup_directory` に対する読み取り、書き込み、および実行のアクセス権が必要です。

- e. `exit` コマンドを実行して、ユーザー・コンテキストを終了します。
4. ディレクトリー・サーバー・インスタンスをデータベースと共に削除します。インスタンスをデータベースと共に削除する方法については、184 ページの『コマンド行ユーティリティーを使用したインスタンスの削除』を参照してください。

5. 現在の作業ディレクトリーを IBM Security Directory Server バージョン 6.3.1 のインストール・ロケーション内の `sbin` サブディレクトリーに変更します。
6. インスタンスのリモート・アップグレードにインスタンス・バックアップ・ディレクトリーを使用するには、`idsimigr` コマンドを以下の形式で実行します。

```
idsimigr -I dsrdbm01 -u instance_backup_location -l instance_home_directory -n
```

7. インスタンスを構成するには、以下の形式で `idscfgdb` コマンドを実行します。

```
idscfgdb -I dsrdbm01 -a database_owner -w passwd  
-t dsrdbm01 -l instance_home_directory -n
```

8. インスタンスに対して変更ログ・データベースが構成されていた場合は、そのインスタンスに対して変更ログ・データベースを構成します。

```
idscfgchglg -I dsrdbm01 -n
```

9. バックアップ・イメージからデータベースを復元します。インスタンスのデータベース `dsrdbm01` を復元するには、以下の手順を実行します。

- a. ユーザー・コンテキストを DB2 インスタンス所有者に切り替えます。

```
su - dsrdbm01
```

- b. インスタンスの DB2 データベースを復元します。

```
db2 restore database dsrdbm01 from database_backup_directory replace existing
```

- c. ディレクトリー・サーバー・インスタンスに対して変更ログ・データベースが構成されている場合は、そのデータベースを復元します。

```
db2 restore db ldaplog from changelog_backup_directory
```

- d. `exit` コマンドを実行して、ユーザー・コンテキストを終了します。

10. 復元されたデータベースをカタログするには、以下のコマンドを実行します。

```
su - dsrdbm01  
db2 uncatalog database dsrdbm01  
db2 catalog database dsrdbm01 as dsrdbm01 authentication server  
exit
```

11. 復元された変更ログ・データベースをカタログするには、以下のコマンドを実行します。

```
su - dsrdbm01
db2 uncatalog database ldapclog
db2 catalog database ldapclog as ldapclog authentication server
exit
```

12. ディレクトリー・サーバーおよび管理サーバーを始動します。

```
ibmslapd -I dsrdbm01 -n -t
ibmdiradm -I dsrdbm01
```

---

## ログ管理ソリューションの移行

前バージョンのインスタンスで構成されているログ管理ソリューションを、6.3.1 のインスタンスに移行することができます。

### 始める前に

ログ管理ソリューションを前バージョンのインスタンスから 6.3.1 のインスタンスへと移行するには、事前に以下のタスクを実行する必要があります。

- IBM Security Directory Server バージョン 6.3.1 のインストールを完了します。31 ページの『インストールの開始』を参照してください。
- IBM Security Directory Integrator バージョン 7.1 のインストールを実行します (コンピューターにインストールされていない場合)。
- AIX、Linux、または Solaris オペレーティング・システムでは root ユーザーとしてログインし、Windows オペレーティング・システムでは管理者グループのメンバーとしてログインします。

### 手順

1. 既存のディレクトリー・サーバー・インスタンスの *DS\_instance\_home/idsslapd-instance\_name/etc/logmgmt* ディレクトリーにある *solution.properties* ファイルをバックアップします。
2. 前バージョンのインスタンスを 6.3.1 のインスタンスにアップグレードします。97 ページの『第 14 章 前バージョンのインスタンスのアップグレード』を参照してください。
3. アップグレードしたインスタンスの *DS\_instance\_home/idsslapd-instance\_name/etc/logmgmt* ディレクトリーから、すべてのファイルとサブディレクトリーを削除します。
4. IBM Security Directory Integrator のバージョンが 7.1 より前である場合は、IBM Security Directory Integrator バージョン 7.1 のインストールを実行します。
5. ユーザー・コンテキストをディレクトリー・サーバー・インスタンス所有者に切り替えます。

```
su - instance_owner
```
6. 以下のファイルをコピーします。
  - a. *Directory\_Integrator\_v7.1\_installation\_location/etc* から *DS\_instance\_home/idsslapd-instance\_name/etc/logmgmt* にファイルとディレクトリーをコピーします。

- b. *Directory\_Integrator\_v7.1\_installation\_location/serverapi* から *DS\_instance\_home/idsslapd-instance\_name/etc/logmngmt* にファイルとディレクトリーをコピーします。
- c. *Directory\_Integrator\_v7.1\_installation\_location/idisrv.sth* を *DS\_instance\_home/idsslapd-instance\_name/etc/logmngmt* にコピーします。
- d. *Directory\_Integrator\_v7.1\_installation\_location/testserver.jks* を *DS\_instance\_home/idsslapd-instance\_name/etc/logmngmt* にコピーします。
7. *DS\_instance\_home/idsslapd-instance\_name/etc/logmngmt* に、logs という名前のディレクトリーを作成します。
8. *DS\_instance\_home/idsslapd-instance\_name/etc/logmngmt/solutions.properties* ファイルの末尾に `systemqueue.on=false` 項目を追加します。
9. IBM Security Directory Integrator バージョン 7.1 のインストール・パスがデフォルト・パスと異なる場合は、*IDS\_LDAP\_TDI\_HOME* 変数でインストール・ロケーションを設定します。
10. ログ管理ソリューションを実行します。

---

## SNMP ソリューションの移行

前バージョンのインスタンスで構成されている Simple Network Management Protocol (SNMP) ソリューションを、6.3.1 のインスタンスに移行することができます。

### 始める前に

SNMP ソリューションを前バージョンのインスタンスから 6.3.1 のインスタンスへと移行するには、事前に以下のタスクを実行する必要があります。

- IBM Security Directory Server バージョン 6.3.1 のインストールを完了します。31 ページの『インストールの開始』を参照してください。
- IBM Security Directory Integrator バージョン 7.1 のインストールを実行します (コンピューターにインストールされていない場合)。
- AIX、Linux、または Solaris オペレーティング・システムでは root ユーザーとしてログインし、Windows オペレーティング・システムでは管理者グループのメンバーとしてログインします。

### 手順

1. 前バージョンの既存のインスタンスに関連付けられた、IBM Security Directory Server インストール・ロケーション内の `snmp` ディレクトリーをバックアップします。
2. 前バージョンのインスタンスを 6.3.1 のインスタンスにアップグレードします。97 ページの『第 14 章 前バージョンのインスタンスのアップグレード』を参照してください。
3. IBM Security Directory Server バージョン 6.3.1 のインストール・パスにある `/idstools/snmp/idssnmp.conf` ファイルを、前バージョンの IBM Security Directory Server のインストール・パスにある `/idstools/snmp/idssnmp.conf` ファイルで置き換えます。

4. IBM Security Directory Server バージョン 6.3.1 のインストール・パスにある `/idstools/snmp/idssnmp.properties` ファイルを、前バージョンの IBM Security Directory Server のインストール・パスにある `/idstools/snmp/idssnmp.properties` ファイルで置き換えます。
5. IBM Security Directory Server バージョン 6.3.1 のインストール・パスにある `/idstools/snmp/IBM-DIRECTORYSERVER-MIB` ファイルを、前バージョンの IBM Security Directory Server のインストール・パスにある `/idstools/snmp/IBM-DIRECTORYSERVER-MIB` ファイルで置き換えます。
6. IBM Security Directory Server バージョン 6.3.1 のインストール・パスにある `/idstools/snmp/INET-ADDRESS-MIB` ファイルを、前バージョンの IBM Security Directory Server のインストール・パスにある `/idstools/snmp/INET-ADDRESS-MIB` ファイルで置き換えます。
7. IBM Security Directory Integrator バージョン 7.1 のインストール・パスがデフォルト・パスと異なる場合は、`IDS_LDAP_TDI_HOME` 変数でインストール・ロケーションを設定します。
8. SNMP ソリューションを実行します。

---

## Active Directory との同期ソリューションの移行

前バージョンのインスタンスで構成されている Active Directory との同期ソリューションを、6.3.1 のインスタンスに移行することができます。

### 始める前に

Active Directory との同期ソリューションを前バージョンのインスタンスから 6.3.1 のインスタンスへと移行するには、事前に以下のタスクを実行する必要があります。

- IBM Security Directory Server バージョン 6.3.1 のインストールを完了します。31 ページの『インストールの開始』を参照してください。
- IBM Security Directory Integrator バージョン 7.1 のインストールを実行します (コンピューターにインストールされていない場合)。
- AIX、Linux、または Solaris オペレーティング・システムでは root ユーザーとしてログインし、Windows オペレーティング・システムでは管理者グループのメンバーとしてログインします。

IBM Security Directory Server バージョン 6.3.1 より、Active Directory との同期ソリューションは推奨されなくなりました。代わりに、LDAPSync ソリューションを使用してください。

### 手順

1. 前バージョンのインスタンスを 6.3.1 のインスタンスにアップグレードします。97 ページの『第 14 章 前バージョンのインスタンスのアップグレード』を参照してください。
2. ディレクトリー・サーバー・インスタンスを作成します。149 ページの『インスタンス管理ツールを使用したインスタンス作成』を参照してください。

3. ディレクトリー・サーバー・インスタンスを、Active Directory との同期に対応するように構成します。241 ページの『Active Directory との同期』を参照してください。
4. インスタンスをアップグレードする前に、`DS_instance_home/idsslapd-instance_name/etc/tdisoldir/solution.properties` ファイルに加えた変更を復元します。

注: 新規に作成した `solution.properties` ファイルを以前のファイルで置き換えると、Active Directory との同期が失敗する場合があります。`idsadscfg` コマンドを実行して作成された `solution.properties` ファイルの形式は、以前のファイルと異なります。

5. Active Directory との同期ソリューションを実行します。`idsadsrun` コマンドについて詳しくは、「*Command Reference*」を参照してください。

---

## 前のバージョンの Web 管理ツール構成の移行

前のバージョンの Web 管理ツール構成を移行して、後のバージョンの Web 管理ツールで同じ設定を使用し続けられるようにします。

前のバージョンの既存の Web 管理ツール構成を、`idswmigr` コマンドを使用して移行するには、以下の条件を満たす必要があります。

1. 前のバージョンの Web 管理ツールがコンピューターにインストールされている。
2. 前のバージョンの WebSphere Application Server 組み込みバージョンがコンピューターにインストールされている。
3. 前のバージョンの Web 管理ツールが前のバージョンの WebSphere Application Server 組み込みバージョンにデプロイされている。
4. IBM Security Directory Server バージョン 6.3.1 と一緒に提供されている Web 管理ツールをインストールする。
5. IBM Security Directory Server バージョン 6.3.1 と一緒に提供されている WebSphere Application Server 組み込みバージョンをインストールする。
6. 6.3.1 と一緒に提供されている Web 管理ツールを、WebSphere Application Server 組み込みバージョンにデプロイしない。

以下に示すバージョンの WebSphere Application Server 組み込みバージョンにデプロイされている、以下のバージョンの IBM Security Directory Server の Web 管理ツールが、移行用にサポートされています。

- IBM Security Directory Server バージョン 6.1 および WebSphere Application Server 組み込みバージョンのバージョン 6.1.0.7 以降
- IBM Security Directory Server バージョン 6.2 および WebSphere Application Server 組み込みバージョンのバージョン 6.1.0.13 以降 (UNIX の場合) または WebSphere Application Server 組み込みバージョンのバージョン 6.1.0.17 以降 (Windows の場合)
- IBM Security Directory Server バージョン 6.3 および WebSphere Application Server 組み込みバージョンのバージョン 7.0.0.7 以降

**idswmigr** コマンドを使用して、前のバージョンの Web 管理ツールの構成設定を移行する場合、コマンドによって以下の操作が実行されます。

1. 前のバージョンの Web 管理ツールの構成ファイルを保存する
2. 前のバージョンの Web 管理ツールを、前のバージョンの WebSphere Application Server 組み込みバージョンからアンデプロイする。
3. 前のバージョンの WebSphere Application Server 組み込みバージョンの構成を、指定した一時ロケーションにバックアップする。
4. 前のバージョンの WebSphere Application Server 組み込みバージョンの構成を、あるロケーションにリストアする。
5. IBM Security Directory Server バージョン 6.3.1 と一緒に提供されている現行バージョンの WebSphere Application Server 組み込みバージョン内で Web 管理ツールをデプロイする。
6. Web 管理ツールの以前の構成ファイルを移行し、これらのファイルを後のバージョンの WebSphere Application Server 組み込みバージョンにリストアする。

注: IBM Installation Manager を使用して Web 管理ツールを移行できるのは、移行対象の WebSphere Application Server 組み込みバージョンのメジャー・バージョンが、新規インストール対象の WebSphere Application Server 組み込みバージョンのメジャー・バージョンよりも小さい場合に限られます。

## idswmigr

**idswmigr** コマンドを使用して、前のバージョンの既存の Web 管理ツール構成を新しいバージョンの Web 管理ツールに移行します。

### 説明

前のバージョンの既存の Web 管理ツール構成を、**idswmigr** コマンドを使用して移行するには、以下の条件を満たす必要があります。

1. 前のバージョンの Web 管理ツールがコンピューターにインストールされている。
2. 前のバージョンの WebSphere Application Server 組み込みバージョンがコンピューターにインストールされている。
3. 前のバージョンの Web 管理ツールが前のバージョンの WebSphere Application Server 組み込みバージョンにデプロイされている。
4. Web 管理ツールの新しいバージョンをインストールする。
5. WebSphere Application Server 組み込みバージョンの新しいバージョンをインストールする。
6. 新しいバージョンの Web 管理ツールを WebSphere Application Server 組み込みバージョンにデプロイしない。

### 構文

```
idswmigr -l temp_path [-s source_path -t target_path  
-r profile_name -a app_name -v -o ports_path]
```

### オプション

**idswmigr** コマンドは、以下のパラメーターをとります。

- a *app\_name***  
アプリケーション名を指定します。指定しない場合、デフォルトの `IDSWebApp.war` が使用されます。
  - l *temp\_path***  
一時ファイルを保管するロケーションを指定します。
  - o *ports\_path***  
ポート定義ファイルの完全修飾パスを指定します。指定しない場合は、以下のデフォルト・パスが使用されます。
- Windows**  
C:\Program Files\IBM\ldap\V6.3.1\idstools\TDSWEBPortDef.props
- AIX および Solaris**  
/opt/IBM/ldap/V6.3.1/idstools/TDSWEBPortDef.props
- Linux** /opt/ibm/ldap/V6.3.1/idstools/TDSWEBPortDef.props
- r *profile\_name***  
アプリケーションに関連付けられたプロファイル名を指定します。指定しない場合は、デフォルトの `TDSWebAdminProfile` が使用されます。
  - s *source\_path***  
前バージョンの WebSphere Application Server 組み込みバージョンのソース・ロケーションを指定します。
  - t *target\_path***  
新しいバージョンの WebSphere Application Server 組み込みバージョンのインストール・ロケーションを指定します。
  - v** バージョン情報を表示します。

## 例

**例 1** バージョン 6.2 の既存の Web 管理ツール構成をバージョン 6.3.1 に移行するには、次のコマンドを実行します。

```
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
```

## Web 管理ツールの手動での移行

Web 管理ツールを手動で移行することができます。

### 始める前に

Web 管理ツールを手動で移行するには、あらかじめ Web 管理ツールがインストールされている必要があります。ステップに従って、Web 管理ツールを手動で移行してください。ここで示した例では、IBM Security Directory Server V6.3 上の Web 管理ツールを、IBM Security Directory Server V6.3.1 に移行します。

AIX の移行コマンドは、Linux のコマンドと似ていますが、パス `/opt/ibm/ldap` を `/opt/IBM/ldap` に置き換える必要があります。

## 手順

1. Windows の場合は、以下のコマンドを使用して、WebSphere Application Server サービスを追加します。

```
"C:%Program Files%IBM%ldap%V6.3%appsrv%bin%WASService.exe" -add
TDSWebAdmin-V6.3.1 -serverName server1 -profilePath
"C:%Program Files%IBM%ldap%V6.3%appsrv%profiles%TDSWebAdminProfile"
-startType automatic
```

2. 以前のリリースの Web 管理ツールのファイルをバックアップします。

- Windows では、これらのファイルが以下のディレクトリーにあります。

```
C:%Program Files%IBM%LDAP%V6.3%appsrv%profiles%TDSWebAdminProfile%
installedApps%DefaultNode%IDSWebApp.war.ear%IDSWebApp.war%
WEB-INF%classes%
```

または

```
C:%Program Files%IBM%LDAP%V6.3%appsrv%installedApps%DefaultNode
%IDSWebApp.war.ear%IDSWebApp.war%WEB-INF%classes
```

- Linux では、これらのファイルが以下のディレクトリーにあります。

```
/opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/installedApps
/DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
```

または

```
/opt/ibm/ldap/V6.3/appsrv/installedApps/DefaultNode
/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
```

各ディレクトリーから以下の 5 ファイルのみコピーします。

```
security%console_passwd
IDSSConfig%IDSSessionConfig%IDSSessionMgmt.xml
IDSSConfig%IDSServersConfig%IDSServersInfo.xml
IDSSConfig%IDSSAppReg%IDSSAppReg.xml
IDSSConfig%IDSSearchSettings%IDSSearchMgmt.xml
```

以下に例を示します。

```
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%
IDSSConfig%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%
IDSSConfig%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%
IDSSConfig%IDSSAppReg%IDSSAppReg.xml" c:%BackUp
copy "C:%Program Files%IBM%LDAP%V6.3%appsrv%profiles%TDSWebAdminProfile%
installedApps%DefaultNode%IDSWebApp.war.ear%IDSWebApp.war%WEB-INF%classes%
IDSSConfig%IDSSearchSettings%IDSSearchMgmt.xml" c:%BackUp
```

3. 以前のリリースの WAR ファイルをアンインストールします。

- Windows では、以下のディレクトリーにコマンドがあります。

```
C:%Program Files%IBM%LDAP%V6.3%appsrv%profiles%TDSWebAdminProfile%bin%wsadmin.bat
```

または

```
C:%Program Files%IBM%LDAP%V6.3%appsrv%bin%wsadmin.bat
```

- Linux では、以下のディレクトリーにコマンドがあります。  
/opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh

または

```
/opt/ibm/ldap/V6.3/appsrv/bin/wsadmin.sh
wsadmin.bat -conntype NONE -c "$AdminApp uninstall IDWebApp.war"
```

以下に例を示します。

```
"C:%Program Files%IBM%LDAP%V6.3%appsrv%profiles%TDSWebAdminProfile%bin%wsadmin.bat"
-conntype NONE -c "$AdminApp uninstall IDWebApp.war"
```

4. 以前の WebSphere Application Server 組み込みバージョンのサーバーが実行中である場合は、アプリケーション・サーバーを停止します。

- Windows では、以下のディレクトリーにコマンドがあります。

```
C:%Program Files%IBM%LDAP%V6.3%appsrv%profiles%TDSWebAdminProfile%bin%
stopServer.bat
```

または

```
C:%Program Files%IBM%LDAP%V6.3%appsrv%bin%stopServer.bat
```

- Linux では、以下のディレクトリーにコマンドがあります。

```
/opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/stopServer.sh
```

または

```
/opt/ibm/ldap/V6.3/appsrv/bin/stopServer.sh
```

以下に例を示します。

```
"C:%Program Files%IBM%LDAP%V6.3%appsrv%profiles%TDSWebAdminProfile%bin%
stopServer.bat" server1
```

5. 新しい WebSphere Application Server 組み込みバージョンにプロファイルがあるかどうか確認します。プロファイルがない場合は、新しいプロファイルを作成します。

- Windows では、以下のコマンドを実行して、新しいプロファイルを作成します。

```
"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"
```

- Linux では、以下のコマンドを実行して、新しいプロファイルを作成します。

```
/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. 新しい WAR ファイルを新しい WebSphere Application Server ディレクトリーにコピーします。

- Windows では、以下のコマンドを実行します。

```
copy "C:\Program Files\IBM\LDAP\6.3.1\idstools\IDSWebApp.war"
"C:\Program Files\IBM\LDAP\6.3.1\appsrv\profiles\TDSWebAdminProfile\
installableApps"
```

- Linux では、以下のコマンドを実行します。

```
cp "/opt/ibm/ldap/V6.3.1/idstools/IDSWebApp.war"
"/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installableApps"
```

7. 新しい WAR ファイルを、新しい WebSphere Application Server 製品にインストールします。

- Windows では、以下のコマンドを実行します。

```
"C:\Program Files\IBM\LDAP\6.3.1\appsrv\profiles\TDSWebAdminProfile\bin
\wsadmin.bat" -conntype NONE -c "$AdminApp install {C:\Program Files\
IBM\LDAP\6.3.1\appsrv\profiles\TDSWebAdminProfile\installableApps\
IDSWebApp.war} {-configroot %"C:\Program Files\IBM\LDAP\6.3.1\
appsrv\config%" -node DefaultNode -usedefaultbindings -nodeployejb
-appname IDSWebApp.war -contextroot %"IDSWebApp%"}"
```

- Linux では、以下のコマンドを実行します。

```
"/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. 前の手順で保存した Web 管理ツールの構成ファイルをリストアします。

- Windows では、以下のファイルをバックアップ・コピーのファイルに置き換えます。

```
C:\Program Files\IBM\LDAP\6.3.1\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
classes\security\console_passwd
C:\Program Files\IBM\LDAP\6.3.1\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
classes\IDSSessionConfig\IDSSessionMgmt.xml
C:\Program Files\IBM\LDAP\6.3.1\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
classes\IDSServersConfig\IDSServersInfo.xml
C:\Program Files\IBM\LDAP\6.3.1\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
classes\IDSSessionConfig\IDSAppReg\IDSAppReg.xml
C:\Program Files\IBM\LDAP\6.3.1\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
classes\IDSSessionConfig\IDSSearchSettings\IDSSearchMgmt.xml
```

- Linux では、以下のファイルをバックアップ・コピーのファイルに置き換えます。

```
/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/IDSSessionConfig/
IDSSessionMgmt.xml
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSSessionConfig/
IDSServersInfo.xml
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSSessionConfig/
IDSAppReg/IDSAppReg.xml
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSSessionConfig/
IDSSearchSettings/IDSSearchMgmt.xml
```

9. Windows では、追加したサービスを開始します。

```
"C:¥Program Files¥IBM¥ldap¥V6.3.1¥appsrv¥bin¥WASService.exe"  
-start TDSWebAdmin-V6.3.1
```

10. Linux では、サーバーを始動します。

```
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin/startServer.sh server1
```



---

## 第 16 章 手動による Web 管理ツールのデプロイメント

Web 管理ツールを使用して、ディレクトリー・サーバー・インスタンスを管理するには、サポートされる Web アプリケーション・サーバーに Web 管理ツールをデプロイする必要があります。

Web 管理ツールをデプロイするには、サポートされるバージョンの Web アプリケーション・サーバーがコンピューターに含まれている必要があります。IBM Security Directory Server のインストール・メディアには、WebSphere Application Server 組み込みバージョン バージョン 7.0.0.25 が提供されています。IBM Installation Manager を使用して Web 管理ツールのインストールを実行し、これを WebSphere Application Server 組み込みバージョンにデプロイすることができます。

IBM Installation Manager を使用した IBM Security Directory Server のインストールが、オペレーティング・システムでサポートされない場合、WebSphere Application Server 組み込みバージョンを手動でインストールします。WebSphere Application Server 組み込みバージョンのインストールが終わったら、WebSphere Application Server 組み込みバージョンに Web 管理ツールをデプロイする必要があります。

サポートされるバージョンの WebSphere Application Server がコンピューター上にある場合、そこに Web 管理ツールをデプロイできます。

WebSphere Application Server は、Java ベースのアプリケーション用の IBM ランタイム環境です。詳しくは、WebSphere Application Server 製品資料 (<http://www-01.ibm.com/support/knowledgecenter/SSEQTP/welcome>) を参照してください。

---

### 手動による WebSphere Application Server 組み込みバージョンのインストール

Web 管理ツールをデプロイするには、WebSphere Application Server 組み込みバージョンをご使用のコンピューターにインストールする必要があります。

#### 始める前に

WebSphere Application Server 組み込みバージョンのインストールの場合は、以下の手順を実行します。

1. WebSphere Application Server 組み込みバージョンのインストール可能ファイルが収録された IBM Security Directory Server インストール・メディアにアクセスします。6 ページの『インストール・メディアの準備』を参照してください。

#### このタスクについて

deploy\_IDSWebApp コマンドをパラメーターなしで使用して Web 管理ツール をデプロイするには、以下の値を指定する必要があります。

1. IBM Security Directory Server インストール・パスの appsrv ディレクトリーを、WebSphere Application Server 組み込みバージョンのインストール・ロケー

ションとして指定します。デフォルトの IBM Security Directory Server のインストール・パスについて詳しくは、30 ページの『デフォルトのインストール・ロケーション』を参照してください。

WebSphere Application Server 組み込みバージョンには、それ以外に任意のインストール・ロケーションを指定することができます。その場合、Web 管理ツールをデプロイするための `deploy_IDSWebApp` コマンドに、`-w`、`-p`、`-r`、および `-o` の各パラメーターと値を指定する必要があります。

## 手順

1. 管理者特権でログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを、WebSphere Application Server 組み込みバージョンのインストール可能ファイルが含まれているディレクトリーに変更します。
4. WebSphere Application Server 組み込みバージョンを IBM Security Directory Server のデフォルトのインストール・パスにインストールするには、以下のコマンドを実行します。

オペレーティング・システム	実行するコマンド:
Microsoft Windows	<code>install.bat -installRoot c:%ProgramFiles%IBM\ldap\V6.3.1\appsrv</code>
AIX および 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>

## 次のタスク

Web 管理ツールがコンピューターにインストールされていない場合は、Web 管理ツールのインストールを実行します。73 ページの『第 12 章 オペレーティング・システム・コマンド行ユーティリティーを使用したインストール』を参照してください。

Web 管理ツールがコンピューターにインストールされている場合は、Web 管理ツールのデプロイメントを実行します。124 ページの『WebSphere Application Server 組み込みバージョンへの Web 管理ツールのデプロイ』を参照してください。

---

## Web 管理ツールのデフォルト・ポート

Web 管理ツールと他のアプリケーションのポート間におけるポート競合を防ぐために、Web 管理ツールによって使用されるデフォルト・ポートを知っておく必要があります。

WebSphere Application Server 組み込みバージョン では、Web 管理ツールに対して以下のデフォルト・ポート設定を使用します。

- HTTP トランスポート (ポート 1): 12100
- HTTPS トランスポート (ポート 2): 12101
- 管理コンソール (WebSphere Application Server 管理用) ポート: 12104

- セキュア管理コンソール (WebSphere Application Server 管理用) ポート: 12105

WebSphere Application Server 組み込みバージョン では、他のアプリケーションに対して以下のデフォルト・ポート設定を使用します。

- ブートストラップ/rmi ポート: 12102
- Soap コネクタ・ポート: 12103

WebSphere Application Server 組み込みバージョンによって使用される可能性がある他のポート番号: 9405、9406、9407、9375、9105、7276、7286、5558、5577、5075、5076。

別のアプリケーションとの間でポート競合が存在し、そのアプリケーションが 1 つ以上のデフォルト・ポートを使用している場合、環境に適した以下のいずれかのアクションを実行してください。

- デフォルト・ポートを未使用ポートに変更し、未使用ポートでアプリケーションを開始します。
- デフォルト・ポートを使用しているアプリケーションが重要なサービスまたはサーバーではない場合、そのポート番号を変更してデフォルト・ポートを解放します。

WebSphere Application Server 組み込みバージョンがアプリケーションのために初期化するデフォルトのポート番号を変更するには、`portdef.props` ファイルに適切なポート番号を設定する必要があります。`portdef.props` ファイルは IBM Security Directory Server のインストール・ロケーションの `¥appsrv¥profiles¥TDSWebAdminProfile¥properties¥` ディレクトリにあります。デフォルトの IBM Security Directory Server のインストール・ロケーションについて詳しくは、30 ページの『デフォルトのインストール・ロケーション』を参照してください。

#### **HTTP トランスポート (ポート 1)**

HTTP トランスポート (ポート 1) 用のポートを変更するには、ポート番号 12100 の項目を、使用中でないポート番号に変更します。

#### **HTTPS トランスポート (ポート 2)**

HTTPS トランスポート (ポート 2) 用のポートを変更するには、ポート番号 12101 の項目を、使用中でないポート番号に変更します。

#### **ブートストラップ/rmi ポート**

ブートストラップ/rmi ポート用のポートを変更するには、ポート番号 12102 の項目を、使用中でないポート番号に変更します。

#### **Soap コネクタ・ポート**

Soap コネクタ・ポート用のポートを変更するには、ポート番号 12103 の項目を、使用中でないポート番号に変更します。

#### **管理コンソール・ポート**

管理コンソール・ポート用のポートを変更するには、ポート番号 12104 の項目を、使用中でないポート番号に変更します。

#### **セキュア管理コンソール・ポート**

セキュア管理コンソール・ポート用のポートを変更するには、ポート番号 12105 の項目を、使用中でないポート番号に変更します。

# WebSphere Application Server 組み込みバージョンへの Web 管理ツールのデプロイ

Web 管理ツールを使用するには、このツールを Web アプリケーション・サーバーにデプロイする必要があります。

## 始める前に

Web 管理ツールをデプロイする前に、以下のアクションを実行する必要があります。

1. ご使用のオペレーティング・システムに対応した Web 管理ツール・パッケージをインストールします。
2. サポート対象バージョンの Web アプリケーション・サーバーをインストールします。
3. 既にある前バージョンの Web 管理ツール構成を移行する予定の場合は、それより後のバージョンの Web 管理ツールをデプロイしないでください。

## このタスクについて

Web 管理ツールをデプロイすると、コマンドが以下のアクションを実行します。

1. 前バージョンの Web 管理ツールを削除します。
2. Web アプリケーション・サーバーに Web 管理ツールをデプロイします。
3. Web アプリケーション・サーバーを始動します。

## 手順

1. 管理者特権でログインします。
2. `DS_install_location/idstools` ディレクトリーに移動します。  
`DS_install_location` は IBM Security Directory Server のインストール・ロケーションです。以下のロケーションが、各オペレーティング・システムのデフォルトのロケーションです。

オペレーティング・システム	デフォルトのインストール・ロケーション:
Microsoft Windows	<code>c:\Program Files\IBM\ldap\6.3.1</code>
AIX および Solaris	<code>/opt/IBM/ldap/V6.3.1</code>
Linux	<code>/opt/ibm/ldap/V6.3.1</code>

3. 以下のコマンドを実行します。

注: WebSphere Application Server 組み込みバージョンをデフォルトの IBM Security Directory Server インストール・ロケーションにインストールした場合は、`deploy_IDSWebApp` コマンドにパラメーターを一切指定しないでください。`deploy_IDSWebApp` コマンドについて詳しくは、`deploy_IDSWebApp -h` でこのコマンドの使用法を参照してください。

オペレーティング・システム	実行するコマンド:
Microsoft Windows	<code>deploy_IDSWebApp.bat -w path_to_war_file -p was_installation_path -r profile -o ports_file</code>

オペレーティング・システム	実行するコマンド:
AIX、Linux、および Solaris	<pre>deploy_IDSWebApp -w path_to_war_file -p was_installation_path -r profile -o ports_file</pre>

## タスクの結果

このコマンドにより、*was\_installation\_path* で指定された Web アプリケーション・サーバーに Web 管理ツールがデプロイされます。

## 次のタスク

Web 管理ツールにアクセスするには、ブラウザ・ウィンドウを開き、`http://host_name:12100/IDSWebApp` と入力します。 *host\_name* 変数は、Web 管理ツールをインストールしたコンピューターのホスト名または IP アドレスを示します。

---

## WebSphere Application Server への Web 管理ツールのデプロイ

コンピューター上のアプリケーションを WebSphere Application Server で管理したい場合は、WebSphere Application Server に Web 管理ツールをデプロイすることができます。

### 始める前に

WebSphere Application Server に Web 管理ツールをデプロイするには、以下の要件を満たしている必要があります。

1. ご使用のオペレーティング・システムに対応した Web 管理ツール・パッケージをインストールします。35 ページの『IBM Installation Manager を使用したインストール』を参照してください。
2. サポート対象バージョンの WebSphere Application Server がコンピューターにインストールされている必要があります。

### このタスクについて

IBM Security Directory Server インストール・メディアには、Web 管理ツールおよび WebSphere Application Server 組み込みバージョンが収録されています。コンピューターに WebSphere Application Server がインストールされている場合は、WebSphere Application Server に Web 管理ツールをデプロイできます。Web 管理ツールをデプロイするには、IBM Security Directory Server インストール・ロケーションの `idstools` ディレクトリーにある `IDSWebApp.war` ファイルをデプロイする必要があります。

### 手順

1. URL `http://hostname_WAS_server:9060/ibm/console` を使用して WebSphere 管理コンソールにログインします。 *hostname\_WAS\_server* 変数は、WebSphere Application Server がインストールされているコンピューターのホスト名または

IP アドレスに置き換えてください。カスタム・ポートを指定して WebSphere 管理コンソールにアクセスする場合は、デフォルト・ポート 9060 をご使用のポート番号で置き換えてください。

2. ユーザーのユーザー ID およびパスワードを入力します。このユーザーは、WebSphere Application Server で操作を実行するために必要な権限を持っている必要があります。
3. 左側のナビゲーション・ペインで、「アプリケーション」 > 「新規アプリケーション」をクリックします。
4. 「新規アプリケーション」ページで、「新規エンタープライズ・アプリケーション」をクリックします。
5. 「新規アプリケーションへのパス」ページで、WebSphere 管理コンソールにどこからアクセスしたかに応じて、以下のいずれかのオプションを選択します。
  - ローカル・コンピューターから WebSphere 管理コンソールにアクセスした場合は、「ローカル・ファイル・システム」を選択し、「絶対パス」フィールドに IDSSWebApp.war ファイルのパスを入力します。「参照」をクリックして、パスを指定することもできます。
  - リモート・コンピューターから WebSphere 管理コンソールにアクセスした場合は、「リモート・ファイル・システム」を選択し、「絶対パス」フィールドに IDSSWebApp.war ファイルのパスを入力します。「参照」をクリックして、パスを指定することもできます。
6. 「アプリケーションをどのようにインストールしますか」ページで、「ファスト・パス」オプションを選択し、「次へ」をクリックします。
7. 「インストール・オプションの選択」ページでは、デフォルトのオプションが選択されています。
8. 「次へ」をクリックします。
9. 「モジュールをサーバーにマップ」ページで、「クラスターおよびサーバー」フィールドに指定されているサーバーにモジュールをマップできます。
  - a. 必要なモジュールのチェック・ボックスを選択し、「適用」をクリックします。
  - b. マッピングが完了したら、「次へ」をクリックします。
10. 「Web モジュールの仮想ホストをマップ」ページで、Web アプリケーションを特定の仮想サーバーにマップすることができます。仮想ホストが複数ある場合は、サーバーが正しいモジュールを選択できるように WebSphere 環境に関する情報が必要になります。この例では、default\_host オプションを選択できます。
11. 「次へ」をクリックします。
12. 「Web モジュールのコンテキスト・ルートをマップ」ページで、フィールドにコンテキスト・ルートとして /IDSSWebApp を入力します。
13. 選択した内容の要約が表示されます。
14. 「完了」をクリックします。アプリケーションのインストールが開始されます。インストールの要約が表示されます。
15. 変更をマスター構成に保存するには、「保存」をクリックします。

16. 左側のナビゲーション・ペインで、「アプリケーション」 > 「アプリケーション・タイプ」 > 「WebSphere エンタープライズ・アプリケーション」をクリックします。
17. 「エンタープライズ・アプリケーション」ページで、IDSWebApp\_war の横にあるチェック・ボックスを選択し、「開始」をクリックします。
18. Web 管理ツールを始動します。
19. Web 管理ツールにアクセスするには、ブラウザを開いて以下のアドレスを入力します。
  - 非セキュア・アクセス (HTTP) の場合は、`http://WAS_server_hostname:9080/IDSWebApp` と入力します。
  - セキュア・アクセス (HTTPS) の場合は、`https://WAS_server_hostname:9443/IDSWebApp` と入力します。

WebSphere Application Server のデフォルトの HTTP ポートは 9080、デフォルトの HTTPS ポートは 9443 です。これらのポートが WebSphere Application Server 用に構成されたポートでない場合は、適切なポート番号を指定してください。WebSphere Application Server でグローバル・セキュリティまたは管理セキュリティが構成されている場合は、以下の要件を満たしている必要があります。

- a. Web 管理ツール を WebSphere Application Server に新規プロファイルとしてデプロイします。
- b. Web 管理ツールに対して SSL を構成します。
- c. Web 管理ツールをプロファイルにデプロイできない場合は、ディレクトリー・サーバーの証明書をプロファイルのトラストストアに追加します。サーバー・クライアント認証を行う場合は、WebSphere Application Server プロファイル証明書をディレクトリー・サーバーのトラストストアに追加します。

---

## Web 管理ツールを使用するための WebSphere Application Server 組み込みバージョンの始動

Web 管理ツールに関連付けられている Web アプリケーション・サーバーを始動して、ディレクトリー・サーバー・インスタンスの追加および管理を行います。

### 始める前に

Web 管理ツールに関連付けられている Web アプリケーション・サーバーを始動する前に、以下のタスクを完了させる必要があります。

1. Web 管理ツールのインストールを完了します。
2. サポートされる Web アプリケーション・サーバーに Web 管理ツールをデプロイします。

**注:** WebSphere Application Server 組み込みバージョンへの Web 管理ツールのインストールとデプロイメントに IBM Installation Manager を使用する場合は、Web 管理ツールのデプロイメントの完了後にアプリケーション・サーバーが始動します。

## 手順

1. Web 管理ツールに関連付けられているアプリケーション・サーバーを始動するには、各オペレーティング・システム上で以下のコマンドを実行します。

### Windows

アプリケーション・サーバーが始動していない場合は、以下のコマンドを実行してください。

```
installation_path%idstools%bin%startWebadminApp.bat
```

デフォルトのインストール・パスは C:%Program Files%IBM%ldap%V6.3.1 です。

### AIX および Solaris

```
/opt/IBM/ldap/V6.3.1/idstools/bin/startWebadminApp
```

### Linux

```
/opt/ibm/ldap/V6.3.1/idstools/bin/startWebadminApp
```

2. Web ブラウザーを開きます。
3. Web ブラウザーのアドレス・バーに以下の URL を入力します。

注: Web 管理ツールをリモート・システムにインストールおよびデプロイしていた場合、localhost をシステムのホスト名または IP アドレスで置換します。

```
http://localhost:12100/IDSWebApp
```

## 次のタスク

ディレクトリー・サーバー・インスタンスを管理するには、Web 管理ツール・コンソールでサーバーを追加します。『Web 管理ツールへのアクセス』を参照してください。

---

## Web 管理ツールへのアクセス

ディレクトリー・サーバー・インスタンスをリモートで管理するには、「Web 管理ツール」を開き、ディレクトリー・サーバー・インスタンスをリモート管理できるように構成します。

### 始める前に

Web 管理ツールにアクセスするには、以下のタスクを完了する必要があります。

1. Web 管理ツールのインストールを完了します。
2. サポートされる Web アプリケーション・サーバーに Web 管理ツールをデプロイします。
3. Web 管理ツールに関連付けられた Web アプリケーション・サーバーを始動します。

### 手順

1. Web 管理ツールにアクセスするには、以下のオプションのいずれかを使用します。
  - Web ブラウザーを開いて以下の URL を入力します。

- 非セキュア・アクセスの場合は、`http://hostname:12100/IDSWebApp` と入力します。
  - セキュア・アクセスの場合は、`https://hostname:12101/IDSWebApp` と入力します。
- Web ブラウザーで以下のファイルを開きます。

#### Windows

非セキュア・アクセスの場合は、  
`ds_installation_path\idstools\bin\idswebadmin.html` を開きます。  
「スタート」 > 「すべてのプログラム」 > 「IBM Security  
**Directory Server 6.3.1**」 > 「Web 管理ツール」をクリックする方法  
もあります。

セキュア・アクセスの場合は、  
`ds_installation_path\idstools\bin\idswebadminssl.html` を開き  
ます。「スタート」 > 「すべてのプログラム」 > 「IBM Security  
**Directory Server 6.3.1**」 > 「Web 管理ツール (セキュア)」をクリッ  
クする方法もあります。

#### AIX、Linux、および Solaris

非セキュア・アクセスの場合は、`ds_installation_path/idstools/  
bin/idswebadmin.html` を開きます。

セキュア・アクセスの場合は、`ds_installation_path/idstools/bin/  
idswebadminssl.html` を開きます。

`ds_installation_path` 変数は、IBM Security Directory Server のインストール・  
ロケーションを表します。デフォルト・ロケーションについては、30  
ページの『デフォルトのインストール・ロケーション』を参照してください。

2. Web 管理ツール・コンソールに、コンソール管理者としてログインします。
  - a. 「ユーザー ID」フィールドに `superadmin` と入力します。
  - b. 「パスワード」フィールドに `secret` と入力します。

注: 初回ログインの後にコンソール管理者パスワードを変更する必要があります。

  - c. 「ログイン」をクリックします。
3. ディレクトリー・サーバーをコンソールに追加するには、以下の手順を実行しま  
す。
  - a. 「概要」ページで、「コンソール・サーバーの管理」をクリックします。
  - b. 「コンソール・サーバーの管理」ページで、「追加」をクリックします。
  - c. 「サーバー名」フィールドに、サーバーを識別する固有の名前を入力しま  
す。値を指定しない場合は、アプリケーションによって `hostname:port` 値  
または `IP_address:port` 値が割り当てられます。
  - d. 「ホスト名」フィールドに、ディレクトリー・サーバーのホスト名または IP  
アドレスを入力します。
  - e. 「ポート」フィールドに、サーバーのポート番号を入力します。
  - f. コンソールがサーバーとセキュアに通信する必要があるかどうかを指定する  
には、「SSL 暗号化を使用可能にする」を選択します。

- g. 管理ポートの制御を使用可能にするには、「サポートされる管理サーバー」を選択します。
  - h. 「管理ポート」フィールドに、管理サーバーのポート番号を入力します。
  - i. 変更を適用するには、「OK」をクリックします。
4. Web 管理ツール・コンソールからログアウトするには、「ログアウト」をクリックします。

## Web アプリケーション・サーバーの停止

Web 管理ツールのアンインストールの前に、Web 管理ツールからログアウトして、Web 管理ツールに関連付けられている Web アプリケーション・サーバーを停止する必要があります。

### 始める前に

Web 管理ツールに関連付けられている Web アプリケーション・サーバーを停止できるようにするには、その前に以下のタスクを完了させる必要があります。

1. サポートされる Web アプリケーション・サーバーに Web 管理ツールをデプロイします。
2. Web 管理ツールに関連付けられた Web アプリケーション・サーバーを始動します。

### 手順

1. 各 UNIX システムには root で、Windows には管理者グループのメンバーでログインします。
2. コマンド・プロンプトにアクセスします。
3. 「Web 管理ツール」のプロファイル内の bin サブディレクトリーに移動します。以下のロケーションが Web 管理ツールがデプロイされる、WebSphere Application Server 組み込みバージョンのデフォルトのインストール・パスです。WebSphere Application Server 組み込みバージョンにカスタムのインストール・パスを指定していた場合、適切な変更を行う必要があります。

オペレーティング・システム	パス
<b>Windows</b>	C:\Program Files\IBM\1dap\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin
<b>AIX および Solaris</b>	/opt/IBM/1dap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin
<b>Linux</b>	/opt/ibm/1dap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin

4. Web 管理ツールに関連付けられている Web アプリケーション・サーバーを停止するには、次のコマンドを実行します。

オペレーティング・システム	実行するコマンド:
<b>Windows</b>	stopServer.bat server1
<b>AIX、Linux、および Solaris</b>	./stopServer server1

注: Windows では、Web アプリケーション・サーバーに関連付けられているサービスを「サービス」ウィンドウから停止することもできます。

---

## WebSphere Application Server 組み込みバージョンでの HTTPS

アプリケーションへの Web アクセスを保護するために、アプリケーションを構成して HTTPS モードで開始することができます。

Web 管理ツールを WebSphere Application Server 組み込みバージョンにデプロイすると、アプリケーションを開始することができます。Web 管理ツールには、HTTPS の Web アドレスとセキュア・ポートを指定することによって安全に接続することができます。

HTTPS を使用するには、Web 管理ツールにアクセスするための次の Web アドレスを指定します。

```
https://hostname:12101/IDSWebApp
```

非 HTTPS 接続を使用するには、Web 管理ツールにアクセスするための次の Web アドレスを指定します。

```
http://hostname:12100/IDSWebApp
```

デフォルトの JKS ファイルは、SSL/TLS セキュア通信用に Web アプリケーション・サーバーで提供されている証明書と変更することもできます。WebSphere Application Server 組み込みバージョン内にデプロイされたアプリケーションで使用するための、新規の鍵データベース・ファイルとトラストストア・データベース・ファイルを作成することができます。デフォルトの鍵データベース・ファイルとトラストストア・データベース・ファイルは別個のファイルで、`WAS_HOME/profiles/TDSWebAdminProfile/etc/` ディレクトリーにあります。`WAS_HOME` 変数は、WebSphere Application Server 組み込みバージョンのインストール・ロケーションです。デフォルトの鍵データベース・ファイルは `DummyServerKeyFile.jks` で、デフォルトのトラストストア・データベース・ファイルは `DummyServerTrustFile.jks` です。

独自の JKS ファイルを作成した場合、鍵データベース・ファイルとトラストストア・データベース・ファイルを変更できます。独自の JKS ファイル、パスワード、およびファイル形式を構成するには、`WAS_HOME/profiles/TDSWebAdminProfile/config/cells/DefaultNode/security.xml` ファイル内の (太字で強調表示された) 次の各エントリーを追加または変更します。

```
<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"/>

```

## Web 管理ツールの WebSphere Application Server 組み込みバージョンからのアンデプロイ

既存の Web 管理ツール (IDSWebApp.war ファイル) を新しいバージョンに置き換えるには、既存の Web 管理ツールをアンデプロイする必要があります。

### 手順

1. Web 管理ツールに関連付けられている Web アプリケーション・サーバーが停止状態の場合、それを始動します。127 ページの『Web 管理ツールを使用するための WebSphere Application Server 組み込みバージョンの始動』を参照してください。
2. `DS_install_location/idstools` ディレクトリに移動します。  
`DS_install_location` は IBM Security Directory Server のインストール・ロケーションです。以下のロケーションが、各オペレーティング・システムのデフォルトのロケーションです。

オペレーティング・システム	デフォルトのインストール・ロケーション:
Microsoft Windows	c:\Program Files\IBM\ldap\6.3.1
AIX および Solaris	/opt/IBM/ldap/V6.3.1
Linux	/opt/ibm/ldap/V6.3.1

3. 以下のコマンドを実行します。

注: WebSphere Application Server 組み込みバージョンをカスタム・ロケーションにインストールしていた場合、パラメーターの `-a`、`-w`、`-p`、および `-r` を `deploy_IDSWebApp` コマンドに指定する必要もあります。`deploy_IDSWebApp` コマンドについて詳しくは、`deploy_IDSWebApp -h` でこのコマンドの使用法を参照してください。

オペレーティング・システム	実行するコマンド:
Microsoft Windows	deploy_IDSWebApp.bat -u
AIX、Linux、および Solaris	deploy_IDSWebApp -u

---

## 第 17 章 インスタンス構成の計画

LDAP 環境を作成および構成する前に、コンピューターの構成設定を決定する必要があります。

ディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスを作成するには、インスタンスを所有するシステム・ユーザー ID をまず作成する必要があります。ディレクトリー・サーバー・インスタンスにディレクトリー・データを格納するには、使用するコード・ページを決定する必要があります。

IBM Security Directory Server および相互前提条件ソフトウェア製品のインストールと、ディレクトリー・サーバー・インスタンスの作成を行うには、コンピューターにユーザーおよびグループを作成する必要があります。IBM Security Directory Server 相互前提条件ソフトウェア製品 (IBM DB2 など) をインストールするには、DB2 管理者用のシステム・ユーザー ID の作成が必要です。

---

### ディレクトリー・サーバー・インスタンスに関連付けられたユーザーとグループ

ディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスを作成するには、必要な許可を持つユーザーおよびグループを作成する必要があります。

コンピューター上にインスタンスを作成するには、インスタンスをシステム・ユーザー ID と関連付ける必要があります。このユーザー ID は、ディレクトリー・サーバー・インスタンスの所有者です。インスタンスに対するシステム・ユーザー ID が存在しない場合、コンピューター上にユーザー ID を作成する必要があります。ディレクトリー・サーバー・インスタンス所有者、データベース・インスタンス所有者、およびデータベース所有者のユーザー ID を作成するには、命名規則に従う必要があります。命名規則について詳しくは、134 ページの『命名規則』を参照してください。

フル・ディレクトリー・サーバーの場合は、システム・ユーザー ID を、データベース・インスタンスおよびデータベースの所有者として関連付ける必要もあります。3 つの役割すべてに対して同じユーザー ID を使用できます。同じユーザー ID を使用した場合、ディレクトリー・サーバー・インスタンス、データベース・インスタンス、およびデータベース所有者は、すべて同じ所有者名を含むことになります。

インスタンス管理ツールを使用してディレクトリー・サーバー・インスタンスを作成する場合は、このツールによってディレクトリー・サーバー・インスタンス所有者のユーザー ID を作成できます。また、`idsadduser` コマンドを使用して、ディレクトリー・サーバー・インスタンス所有者のユーザー ID を作成することもできます。このコマンドは、すべての要件を満たすユーザー ID を作成します。

ディレクトリー・サーバー・インスタンス所有者、データベース・インスタンス所有者、およびデータベース所有者に関連付けるユーザー ID には、以下の役割が含まれています。

#### ディレクトリー・サーバー・インスタンス所有者

ディレクトリー・サーバー・インスタンス所有者として機能するシステム・ユーザー ID が、コンピューター上に存在する必要があります。ディレクトリー・サーバー・インスタンス所有者のユーザー ID は、ディレクトリー・サーバー・インスタンスの名前にもなります。このユーザーには、ディレクトリー・サーバー・インスタンスを管理する権限が割り当てられます。

Windows の場合は、管理者グループのメンバーも、ディレクトリー・サーバー・インスタンスを管理する権限を持ちます。AIX、Linux、および Solaris の場合は、ディレクトリー・サーバー・インスタンス所有者の 1 次グループも、ディレクトリー・サーバー・インスタンスを管理する権限を持ちます。

注: AIX、Linux、および Solaris では、インスタンス所有者名は大文字と小文字が区別されます。ディレクトリー・サーバー・インスタンスの名前と所有者は、常に、ユーザー ID を指定するのと全く同様に指定する必要があります。例えば、JoeSmith と joesmith は、2 つの異なる所有者名です。

#### データベース・インスタンス所有者

データベース・インスタンス所有者として機能するユーザー ID は、ディレクトリー・サーバー・インスタンスのために構成されたデータベース・インスタンスを所有します。データベース・インスタンスとデータベース・インスタンス所有者の名前は同じです。このユーザーは、データベース・インスタンスを管理します。ディレクトリー・サーバー・インスタンス所有者は、データベース・インスタンスを管理することもできます。デフォルトでは、このユーザー ID は、ディレクトリー・サーバー・インスタンスを所有するユーザー ID と同じです。

#### データベース所有者

このユーザー ID は、ディレクトリー・データを保管するためにディレクトリー・サーバー・インスタンスが使用するデータベースを所有します。このデータベースは、データベース・インスタンス所有者が所有するデータベース・インスタンス内に格納されます。ディレクトリー・サーバー・インスタンスは、データベース所有者のユーザー ID とそのパスワードを使用してデータベースに接続します。

## 命名規則

ディレクトリー・サーバー・インスタンスのユーザー ID および 1 次グループは、命名規則の指針に合致する必要があります。

命名規則要件は、以下のユーザー ID に適用されます。

- ディレクトリー・サーバー・インスタンス名 (ディレクトリー・サーバー・インスタンスを所有するユーザー ID)。
- データベース・インスタンス名 (データベース・インスタンスを所有するユーザー ID)。このユーザー ID は、通常ディレクトリー・サーバー・インスタンス名と同じです。

- AIX、Linux、および Solaris の場合は、ディレクトリー・サーバー・インスタンス所有者のユーザー ID とデータベース・インスタンス所有者のユーザー ID の 1 次グループ。

**注:** ユーザー ID およびグループを作成するときは、適切な許可を割り当てる必要があります。『ユーザーとグループ作成の要件』を参照してください。

ユーザー ID とグループ ID は、以下の要件を満たしている必要があります。

- 8 文字以下でなければなりません。
- 以下のいずれの名前も使用できません。
  - USERS
  - ADMINS
  - GUESTS
  - PUBLIC
  - LOCAL
  - idsldap
- 以下のプレフィックスのいずれかで開始することはできません。
  - IBM
  - SQL
  - SYS
- アクセント付き文字を含むことはできません。
- 以下の文字を含むことができます。
  - A から Z
  - a から z
  - 0 から 9
  - \_ (下線)
- 以下のいずれかの文字で開始しなければなりません。
  - A から Z
  - a から z

## ユーザーとグループ作成の要件

インスタンス用のユーザーとグループを作成する際に、ユーザーとグループに適切な許可を割り当て、適切なグループのメンバーとして追加する必要があります。

インスタンス用に必要なユーザーとグループを作成した後、適切な許可を割り当て、ユーザーを適切なグループに追加する必要があります。ユーザーとグループの ID については、以下の要件を満たしている必要があります。

### Windows

- ディレクトリー・サーバー・インスタンス所有者およびデータベース・インスタンス所有者を、管理者グループのメンバーとして追加します。
- データベース・インスタンス所有者に対して有効なロケールを、サーバーでメッセージを生成する際に使用する言語に設定します。必要に応じて、このユーザーでログインし、ロケールを適切な値に変更します。

## AIX、Linux、および Solaris

- root ID を、ディレクトリー・サーバー・インスタンス所有者およびデータベース・インスタンス所有者の 1 次グループのメンバーとして追加します。
- root ID を、idsldap グループのメンバーとして追加します。
- ディレクトリー・サーバー・インスタンス所有者およびデータベース・インスタンス所有者を、idsldap グループのメンバーとして追加します。
- ディレクトリー・サーバー・インスタンス所有者およびデータベース・インスタンス所有者のホーム・ディレクトリーを作成します。
- ディレクトリー・サーバー・インスタンス所有者のホーム・ディレクトリーに対する適切な許可を割り当てます。
  - インスタンスのユーザー所有権はディレクトリー・サーバー・インスタンス所有者です。
  - インスタンスのグループ所有権はディレクトリー・サーバー・インスタンス所有者の 1 次グループです。
  - ディレクトリー・サーバー・インスタンス所有者およびその 1 次グループのホーム・ディレクトリーに対する読み取り、書き込み、および実行の許可を割り当てる必要があります。
- ディレクトリー・サーバー・インスタンス所有者およびその 1 次グループに対して、データベースが作成されたロケーションでの読み取り、書き込み、および実行のアクセス権を割り当てます。
- あるディレクトリー・サーバー・インスタンスについてのディレクトリー・サーバー・インスタンス所有者およびデータベース・インスタンス所有者は、異なるユーザーであってもかまいません。このような場合、ディレクトリー・サーバー・インスタンス所有者は、データベース・インスタンス所有者の 1 次グループのメンバーである必要があります。
- ディレクトリー・サーバー・インスタンス所有者、DB2 インスタンス所有者、およびデータベース所有者が異なる場合、これらはすべて同じグループのメンバーである必要があります。
- Korn シェル・スクリプト (/usr/bin/ksh) を、ディレクトリー・サーバー・インスタンス所有者、データベース・インスタンス所有者、およびデータベース所有者のログイン・シェルとして設定します。

ディレクトリー・サーバー・インスタンス所有者、データベース・インスタンス所有者、およびデータベース所有者のパスワードが正しく設定されて、使用できるようになっている必要があります。有効期限が切れているパスワードや、いかなる種類であっても初回の妥当性検査が済んでいないパスワードであってはなりません。パスワードが正しく設定されているかどうかについては、コンピューター上で Telnet にアクセスし、ユーザー ID およびパスワードでログインすることによって検証できます。

データベースの構成時には、必須ではありませんが、データベース・ロケーションとしてデータベース・インスタンス所有者のホーム・ディレクトリーを指定するのが一般的です。他の場所を指定する場合は、データベース・インスタンス所有者のホーム・ディレクトリーに、3 MB から 4 MB の使用可能スペースが必要です。データベース自体を他の場所に置く場合でも、DB2 はリンクを作成し、データベー

ス・インスタンス所有者のホーム・ディレクトリーにファイルを追加します。データベース・インスタンス所有者のホーム・ディレクトリーに必要なスペースがコンピューターにない場合、スペースを追加するか、ホーム・ディレクトリーを変更することができます。

## 例

ディレクトリー・サーバー・インスタンス所有者の要件を満たすインスタンス所有者を作成するために、**idsadduser** コマンドを実行することができます。**idsadduser** コマンドは、IBM Security Directory Server のインストール・ロケーション内の `sbin` サブディレクトリーにあります。

**例 1:** 以下の値を持つユーザー・アカウントを AIX、Linux、または Solaris に作成するには、**idsadduser** コマンドを実行します。

- ユーザー名: JoeSmith
- 1 次グループ: employees
- ホーム・ディレクトリー: /home/joe (Solaris の場合は /export/home/joe を使用する)
- パスワード: joespw

```
idsadduser -u JoeSmith -g employees -l /home/joe -w joespw
```

**例 2:** 以下の値を持つユーザー・アカウントを、Windows 上の管理者グループのメンバーとして作成するには、**idsadduser** コマンドを実行します。

- ユーザー名: JoeSmith
- パスワード: joespw

```
idsadduser -u JoeSmith -w joespw
```

---

## 構成の計画

ご使用のディレクトリー・サーバー環境について、格納する予定のデータ型、データ構造、および設定するデータ・セキュリティを決定する必要があります。

データベースを構成してデータを取り込む前に、以下のことを決定する必要があります。

### ディレクトリー・サーバーに保管するデータ型

ディレクトリー・サーバーに対して使用するスキーマと、ディレクトリー・サーバーに保管するデータ型を決定する必要があります。ディレクトリー・サーバーには、属性タイプ定義とオブジェクト・クラス定義の標準セットが含まれています。データをカスタマイズするには、カスタムの属性タイプ定義とオブジェクト・クラス定義を追加してから、ディレクトリー・サーバーに項目を追加することをお勧めします。

ディレクトリーにデータを取り込んだ後に、スキーマに対して追加または変更を行うことができます。状況によっては、スキーマを変更するためにデータのアンロードと再ロードが必要な場合があります。

### 使用するコード・ページ

ローカル・コード・ページを使用してデータベースを作成するか、汎用文字セット (UTF-8) を使用してデータベースを作成するかを決定してください。ローカル・コード・ページを選択すると、IBM Security Directory Server

アプリケーションおよびユーザーは、言語の照合順序について予期したとおりの検索結果を得ることができます。ただし、ローカル・コード・ページを使用すると、その特定のコード・ページのデータがディレクトリーに格納されます。UTF-8 を使用すると、UTF-8 の文字データをディレクトリーに保管することができます。UTF-8 の詳細については、『UTF-8 サポート』を参照してください。

**注:** 言語タグを使用する場合は、データベースのコード・ページとして UTF-8 を使用する必要があります。

#### ディレクトリー・データを保管するための階層構造を定義する

IBM Security Directory Server は、ディレクトリー・データを階層ツリー構造で保管します。ディレクトリー内の項目名は、ツリー構造内での項目の相対位置に基づいています。LDAP 環境に適したディレクトリーに対する論理的編成を定義することが重要です。論理的編成により、クライアントは必要な情報を見つけるためにツリーのどの枝を検索すればよいか容易に判別できるようになります。

#### データ・セキュリティの要件を定義する

非セキュア・ポートを経由したディレクトリー・データへのアクセスを防止するために、セキュア通信用にディレクトリー・サーバーを構成できます。データの保護について詳しくは、IBM Security Directory Server 資料の『管理』セクションを参照してください。

#### ディレクトリー・データに対して必要なアクセス権限を定義する

アクセス権限の使用については、IBM Security Directory Server 資料の『管理』セクションでアクセス制御リストを参照してください。

#### プロキシ・サーバーが必要かどうかを評価する

ディレクトリー・データ量が多く、書き込み中心型の環境である場合は、プロキシ・サーバーを使用するかどうかを検討する必要があります。大規模なディレクトリー環境で読み込みに負荷がかかる場合は、複製を構成することにより、必要なスケーリングを実現できる可能性があります。プロキシ・サーバーの使用を決定する前に、IBM Security Directory Server 資料の『管理』セクションで、プロキシ・サーバーでサポートされる機能のリストを参照してください。

---

## UTF-8 サポート

UTF-8 で表すことが可能な各国語文字を保管するように、ディレクトリー・サーバーを構成することができます。

IBM Security Directory Server は、UTF-8 (UCS 変換形式) 文字セットにより、多くの言語の文字をサポートします。LDAP バージョン 3 のプロトコルでは、LDAP クライアントとサーバーが通信する文字データはすべて UTF-8 です。

サーバーでは、データベースの構成に使用されるコード・ページに基づいて、保管および検索できる文字のタイプを判別します。データベースの文字セットを UTF-8 と指定したり、サーバーが存在するシステムのローカル文字セットを使用するように設定したりすることができます。ローカル文字セットは、システム上のローカル、言語、およびコード・ページ環境に基づきます。

UTF-8 を使用すると、UTF-8 の文字データをディレクトリーに保管することができます。UTF-8 がサポートされる任意の言語をサポートするシステム上の LDAP クライアントは、ディレクトリーへのアクセスと検索を正常に行うことができます。LDAP クライアントがローカル文字セットを保持するシステム上に存在する場合、このクライアントは特定の文字セットのサーバーから取得された結果を正しく表示しない場合があります。

UTF-8 データベースを使用すると、データベースに対するデータの保管時や検索時のデータ変換が不要になるため、データベースのパフォーマンスが向上します。

注: 言語タグを使用する場合は、データベースが UTF-8 データベースである必要があります。

## ディレクトリー・サーバーでの UTF-8 の使用

使用するコード・ページを決定するには、ディレクトリー・データの保管とそのデータへのアクセスを行うために、ディレクトリー・サーバーがコード・ページをどのように使用するかについて理解しておく必要があります。

UTF-8 データベースには固定の照合順序があり、この順序は UTF-8 文字のバイナリー順です。UTF-8 データベースで言語依存の照合の実行はできません。

LDAP アプリケーションまたはユーザーが次の結果を取得するためには、UTF-8 はデータベースの適切な文字セットでない可能性があります。

- "name >= SMITH" のような順序付けフィルターを使用する検索で、ご使用のロケールと同様の順序を期待する場合。
- 結果をソートするコントロールを使用する検索で、ご使用のロケールと同様の順序を期待する場合。

このような状態では、LDAP サーバー・システムとすべてのクライアント・システムを、同じ文字セットとロケールを使用して実行する必要があります。

例えば、スペイン語のロケールで構成された LDAP サーバーのデータベースでは、スペイン語のクライアントが期待するような文字の順序に基づいて検索結果を返します。このような構成では、ディレクトリー・ユーザー・コミュニティはそのロケールでの単一の文字セットと照合順序に限定されます。

## サーバー・ユーティリティーの使用による UTF-8 値を持つ LDIF ファイルの作成

charset 拡張機能を使用して、UTF-8 値を持つ LDIF 形式を作成できます。

UTF-8 値を含む LDIF ファイルを手作業で作成するのは困難です。LDIF ファイル・ヘッダーに、Internet Assigned Numbers Authority (IANA) 文字セット名をサポートする拡張機能とバージョン番号を指定できます。サポートされる IANA 文字セットについて詳しくは、141 ページの『サポートされる IANA 文字セット』を参照してください。

### 例

**例 1:** サーバー・ユーティリティーで、指定された文字セットが UTF-8 に自動的に変換されるようにするために、charset タグを使用できます。

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, ou=University of New Mexico, o=sample
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcVhZGVyIHlvd
title: Associate Dean
title: [title in Spanish]
jpegPhoto:< file:///usr/local/photos/jgriego.jpg
```

以下の例で、単一コロンの区切られているすべての属性名と値は、ISO-8859-1 文字セットから UTF-8 に変換されます。二重コロンの区切られたすべての属性名と値 (description:: V2hhdCBhIGNhcmVmdWwgcVhZGVyIHlvd など) は、ベース 64 エンコードで、バイナリーまたは UTF-8 文字ストリングのいずれかである必要があります。ファイルから読み取られた値 (jpegPhoto 属性など、Web アドレスで指定されたもの) も、バイナリーまたは UTF-8 のいずれかである必要があります。このような属性値については、指定された charset から UTF-8 への変換は行われません。

**例 2:** 以下の例に示す charset タグのない LDIF ファイルの場合、内容は UTF-8 と考えられます。

```
# 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
```

IBM Security Directory Server では、version: 1 ヘッダー情報を持たない以下の内容を持つ LDIF ファイルを使用できます。

```
# 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
```

## サポートされる IANA 文字セット

Internet Assigned Number Authority (IANA) 文字セット名を LDIF ファイル内で使用したり、C クライアント・インターフェースで使用したりすることで、ディレクトリー・データの文字セットを識別することができます。

IBM Security Directory Server は、Internet Assigned Number Authority (IANA) 文字セット名をオペレーティング・システム別にサポートしています。

IANA に登録済みの文字セットについては、「Character Sets」の Web サイト ([www.iana.org/assignments/character-sets](http://www.iana.org/assignments/character-sets)) を参照してください。

表 38. IANA 定義の文字セット

文字 セット名	ロケール					DB2 コード・ページ	
	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
ISO-8859-9	X	X	X	X	X	920	1254
ISO-8859-15	X	適用外	X	X	X		
IBM437	適用外	適用外	X	適用外	適用外	437	437
IBM850	適用外	適用外	X	X	適用外	850	850
IBM852	適用外	適用外	X	適用外	適用外	852	852
IBM857	適用外	適用外	X	適用外	適用外	857	857
IBM862	適用外	適用外	X	適用外	適用外	862	862
IBM864	適用外	適用外	X	適用外	適用外	864	864
IBM866	適用外	適用外	X	適用外	適用外	866	866
IBM869	適用外	適用外	X	適用外	適用外	869	869
IBM1250	適用外	適用外	X	適用外	適用外		
IBM1251	適用外	適用外	X	適用外	適用外		
IBM1253	適用外	適用外	X	適用外	適用外		
IBM1254	適用外	適用外	X	適用外	適用外		
IBM1255	適用外	適用外	X	適用外	適用外		
IBM1256	適用外	適用外	X	適用外	適用外		
TIS-620	適用外	適用外	X	X	適用外	874	874
EUC-JP	X	X	適用外	X	X	954	適用外
EUC-KR	適用外	適用外	適用外	X	X	970	適用外
EUC-CN	適用外	適用外	適用外	X	X	1383	適用外
EUC-TW	X	適用外	適用外	X	X	964	適用外
Shift-JIS	適用外	X	X	X	X	932	943
KSC	適用外	適用外	X	適用外	適用外	適用外	949

表 38. IANA 定義の文字セット (続き)

文字 セット名	ロケール					DB2 コード・ページ	
	HP-UX	Linux、 Linux_390	Windows	AIX	Solaris	UNIX	Windows
GBK	適用外	適用外	X	X	適用外	1386	1386
Big5	X	適用外	X	X	X	950	950
GB18030	適用外	X	X	X	X		
HP15CN	X (非 GB18030 の場合)						

注:

- 中国語文字セット標準 GB18030 は、www.oracle.com および www.microsoft.com から入手できる適切なパッチによってサポートされます。
- Windows オペレーティング・システムでは、zhCNGB18030 環境変数を TRUE に設定する必要があります。

### 33 番から 126 番までの ASCII 文字

ASCII 文字の表を使用して、ディレクトリー・サーバー・インスタンスの暗号化シードと暗号化ソルトに使用する文字を判断します。

暗号化シード・ストリングと暗号化ソルトでは、33 から 126 までの ASCII 文字を使用することができます。

表 39. 33 番から 126 番までの ASCII 文字

ASCII コード	文字	ASCII コード	文字	ASCII コード	文字
33	! 感嘆符	34	" 二重引用符	35	# 番号記号
36	\$ ドル記号	37	% % 記号	38	& アンバーサンド
39	' アポストロフィ	40	( 左括弧	41	) 右括弧
42	* アスタリスク	43	+ 正符号	44	, コンマ
45	- ハイフン	46	. ピリオド	47	/ スラッシュ
48	0	49	1	50	2
51	3	52	4	53	5
54	6	55	7	56	8
57	9	58	: コロン	59	; セミコロン
60	< LT 記号	61	= 等号	62	> より大記号
63	? 疑問符	64	@ アットマーク	65	A 大文字の a
66	B 大文字の b	67	C 大文字の c	68	D 大文字の d
69	E 大文字の e	70	F 大文字の f	71	G 大文字の g
72	H 大文字の h	73	I 大文字の i	74	J 大文字の j
75	K 大文字の k	76	L 大文字の l	77	M 大文字の m
78	N 大文字の n	79	O 大文字の o	80	P 大文字の p

表 39. 33 番から 126 番までの ASCII 文字 (続き)

ASCII コード	文字	ASCII コード	文字	ASCII コード	文字
81	Q 大文字の q	82	R 大文字の r	83	S 大文字の s
84	T 大文字の t	85	U 大文字の u	86	V 大文字の v
87	W 大文字の w	88	X 大文字の x	89	Y 大文字の y
90	Z 大文字の z	91	[ 左大括弧	92	¥ 円記号
93	] 右大括弧	94	^ 脱字記号	95	_ 下線
96	` 抑音符号	97	a 小文字の a	98	b 小文字の b
99	c 小文字の c	100	d 小文字の d	101	e 小文字の e
102	f 小文字の f	103	g 小文字の g	104	h 小文字の h
105	i 小文字の i	106	j 小文字の j	107	k 小文字の k
108	l 小文字の l	109	m 小文字の m	110	n 小文字の n
111	o 小文字の o	112	p 小文字の p	113	q 小文字の q
114	r 小文字の r	115	s 小文字の s	116	t 小文字の t
117	u 小文字の u	118	v 小文字の v	119	w 小文字の w
120	x 小文字の x	121	y 小文字の y	122	z 小文字の z
123	{ 左中括弧	124	垂直バー	125	} 右中括弧
126	~ 波形記号				



---

## 第 18 章 インスタンスの作成および管理

ID インフラストラクチャー内でディレクトリー・サーバーを使用するには、要件に従ってディレクトリー・サーバー・インスタンスを作成する必要があります。

IBM Security Directory Server のインストールの完了後に、ディレクトリー・サーバー・インスタンスを作成し、インスタンスの管理者 DN およびパスワードを設定する必要があります。フル・ディレクトリー・サーバーまたはプロキシー・サーバーを作成できます。ディレクトリー・サーバー・インスタンスまたはプロキシー・サーバー・インスタンスを作成するには、コンピューター上にシステム・ユーザー ID を作成する必要があります。システム・ユーザー ID は、ディレクトリー・サーバー・インスタンスまたはプロキシー・サーバー・インスタンスの所有者です。

フル・ディレクトリー・サーバーの場合は、DB2 データベースを作成し、ディレクトリー・サーバー・インスタンスを使用してデータベースを構成する必要があります。DB2 データベースを作成するには、サポートされる DB2 バージョンをコンピューターにインストールする必要があります。ldapdb.properties ファイルが DB2 インストール・パスおよびバージョンを使用して更新されていることを確認する必要があります。詳細については、283 ページの『付録 C. 手動による ldapdb.properties ファイルの更新』を参照してください。

注: IBM Security Directory Server インスタンス管理ツール (**idsxinst**) を使用して、フル・ディレクトリー・サーバー・インスタンスを作成する際に、インスタンスのホーム・ディレクトリーに ldapdb.properties ファイルも作成されます。Windows の場合、ldapdb.properties ファイルは *instance\_home%idsslapd-instance\_name%etc* ディレクトリーにあります。AIX、Linux、または Solaris の場合、ファイルは *instance\_home/idsslapd-instance\_name/etc* ディレクトリーにあります。

プロキシー・サーバー・インスタンスの場合、プロキシー・サーバー・インスタンスを使用して DB2 データベースを作成および構成しないでください。

インスタンス管理ツールは、ディレクトリー・サーバー・インスタンスの作成や管理に使用できるグラフィカル・ユーザー・インターフェース (GUI) です。インスタンス管理ツールを使用するには、IBM Java Development Kit が必要です。インスタンス管理ツールを使用すると、タスクの実行に役立つウィザードがツールから提供されます。

インスタンス管理ツールを使用して、インスタンスを作成、表示、コピー、削除したり、インスタンスに関する情報を変更したりできます。また、このツールを使用して、ディレクトリー・サーバー・インスタンスを所有するユーザーを作成または編集したり、IBM Security Directory Server の以前のバージョンからインスタンスをアップグレードしたりできます。インスタンス管理ツールを使用して、インスタンスのサーバーや管理サーバーを始動したり停止したりできます。さらに、インスタンス管理ツールから構成ツールを開くことができます。

また、コマンド行ユーティリティを使用して、ディレクトリー・サーバー・インスタンスを作成および管理することもできます。

---

## インスタンス管理ツールの始動

インスタンス管理ツールを始動して、ディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスを作成および管理します。

### 始める前に

インスタンス管理ツールを使用するには、サーバー、プロキシ・サーバー、または両方の機能を持つ IBM Security Directory Server をインストールする必要があります。インスタンス管理ツールを実行するには、次の資格情報でログインします。

#### AIX、Linux、および Solaris

root ユーザーとしてログインします。

#### Windows

管理者グループのメンバーとしてログインします。

IBM Security Directory Server のインストール・パスに、IBM Java Development Kit が存在している必要があります。デフォルトの IBM Security Directory Server のインストール・パスについては、30 ページの『デフォルトのインストール・ロケーション』を参照してください。

### 手順

インスタンス管理ツールを始動するには、以下のオプションのいずれかを使用します。

インスタンス管理ツールを開くためのオプション	実行するコマンド:
IBM Security Directory Server のサーバー機能のインストール	「要約」ページで、「インスタンス管理ツール (idsxinst)」をクリックします。詳しくは、35 ページの『IBM Installation Manager を使用したインストール』を参照してください。

<p>インスタンス管理ツールを開くためのオプション</p>	<p>実行するコマンド:</p>
<p><b>idsxinst</b> コマンド</p>	<p><b>Windows</b></p> <ol style="list-style-type: none"> <li>現在のディレクトリーを IBM Security Directory Server インストール・ロケーション内の <code>sbin</code> ディレクトリーに変更します。</li> <li><b>idsxinst</b> コマンドを実行します。</li> </ol> <p><b>注:</b> 「スタート」 &gt; 「すべてのプログラム」 &gt; 「IBM Security Directory Server 6.3.1」 &gt; 「インスタンス管理ツール」をクリックすることもできます。</p> <p><b>AIX、Linux および Solaris</b></p> <ol style="list-style-type: none"> <li>現在のディレクトリーを IBM Security Directory Server インストール・ロケーション内の <code>sbin</code> ディレクトリーに変更します。</li> <li><b>idsxinst</b> コマンドを実行します。</li> </ol> <p>IBM Security Directory Server のインストール・パスについて詳しくは、30 ページの『デフォルトのインストール・ロケーション』を参照してください。</p>

## インスタンスをアップグレードするためのインスタンス管理ツールの始動

インスタンス管理ツールを開いてバックアップ・データを含んだリモート・インスタンスをアップグレードするために、パラメーターを指定してインスタンス管理ツールを実行します。

### 始める前に

リモート・インスタンスをアップグレードするには、以下の要件を満たしている必要があります。

- コンピューターに、**migbkup** コマンドで作成されたバックアップ・データが格納されている必要があります。リモート・インスタンスをアップグレードするバージョンの **migbkup** コマンドを使用する必要があります。
- AIX、Linux、および Solaris システムでは、`root` ユーザーとしてログインします。Windows では、管理者グループのメンバーとしてログインします。

### 手順

1. コマンド・プロンプトにアクセスします。

- 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` ディレクトリーに変更します。 デフォルトのインストール・パスについて詳しくは、30 ページの『デフォルトのインストール・ロケーション』を参照してください。

- 以下の形式で `idsxinst` コマンドを実行します。

```
idsxinst -migrate backup_directory
```

`backup_directory` 変数は、`migbkup` コマンドで作成されたインスタンスのバックアップ・データを保管したロケーションで置き換えてください。

---

## ディレクトリー・サーバー・インスタンス作成

LDAP 環境でディレクトリー・サーバー・インスタンスを使用するには、最適なパフォーマンスを得るために、既存のインスタンスと暗号的に同期されたインスタンスを作成します。

ディレクトリー・サーバー・インスタンスを既存のディレクトリー・サーバー・インスタンスのコピーとして作成する場合は、2 つのディレクトリー・サーバー・インスタンスは暗号的に同期されます。それらを同期する必要はありません。

既存のインスタンスのコピーでないインスタンスを作成する場合、このインスタンスと既存のインスタンスを暗号的に同期します。以下の環境で最高のパフォーマンスを得るには、サーバー・インスタンスを暗号的に同期させる必要があります。

- レプリカ生成
- 分散ディレクトリー
- サーバー・インスタンス間での LDIF データのインポートおよびエクスポート

以下のいずれかの操作を行う前に、サーバー・インスタンスを同期する必要があります。

- 新規サーバー・インスタンスを開始する。
- サーバー・インスタンス上で `idsbulkload` コマンドを実行する。
- サーバー・インスタンス上で `idsldif2db` コマンドを実行する。

ディレクトリー・サーバーの同期について詳しくは、IBM Security Directory Server 資料の『管理』セクションを参照してください。

ディレクトリー・サーバー・インスタンスを作成して、DB2 データベースを使用してこれを構成した後、ディレクトリー・サーバー・インスタンスをバックアップします。構成、スキーマ、DB2 データベース、およびディレクトリー鍵 `stash` ファイルをバックアップする必要があります。 `idsdbback` コマンドを使用して、ディレクトリー・サーバー・インスタンスのバックアップを作成できます。必要な場合は、`idsdbrestore` コマンドを使用して、鍵 `stash` ファイルを復元できます。コマンドのバックアップおよび復元について詳しくは、「*Command Reference*」を参照してください。

---

## インスタンス管理ツールを使用したインスタンス作成

ご使用の環境の要件を評価して、環境に適した段階でディレクトリー・サーバー・インスタンスを作成する必要があります。

インスタンス管理ツールを使用して、複数の異なる方法でインスタンスを作成できます。

- デフォルトの名前およびその他の設定でデフォルト・インスタンスを作成する。『デフォルトのディレクトリー・サーバー・インスタンスの作成』を参照してください。
- カスタム設定を使用してインスタンスを作成する。151 ページの『カスタム設定を使用したディレクトリー・サーバー・インスタンスの作成』を参照してください。
- IBM Security Directory Server の以前のバージョンからインスタンスをアップグレードする。100 ページの『idsimigr コマンドを使用した前のバージョンのインスタンスのアップグレード』または 165 ページの『インスタンス管理ツールを使用した前のバージョンのインスタンスのアップグレード』を参照してください。
- このコンピューターまたは別のコンピューター上の既存のインスタンスのコピーであるインスタンスを作成する。172 ページの『インスタンス管理ツールを使用した既存のインスタンスのコピーの作成』を参照してください。

## デフォルトのディレクトリー・サーバー・インスタンスの作成

デフォルトのインスタンス作成オプションを使用して、定義済みのインスタンス名およびデフォルトの設定でディレクトリー・サーバー・インスタンスを作成します。

### 始める前に

デフォルト・インスタンスを作成するには、以下のタスクを実行する必要があります。

1. IBM Security Directory Server をサーバー機能とともにインストールします。35 ページの『IBM Installation Manager を使用したインストール』を参照してください。
2. IBM DB2 をインストールします。35 ページの『IBM Installation Manager を使用したインストール』を参照してください。
3. ldapdb.properties ファイルに、DB2 のインストール・パスおよびバージョン情報が含まれているかどうかを確認します。283 ページの『付録 C. 手動による ldapdb.properties ファイルの更新』を参照してください。

### このタスクについて

コンピューターにデフォルトのインスタンス名を持つディレクトリー・サーバー・インスタンスが存在する場合は、デフォルトのディレクトリー・サーバー・インスタンスを作成できません。

デフォルトのディレクトリー・サーバー・インスタンスには以下の設定が含まれています。これらの設定は変更できません。

表 40. デフォルトのディレクトリー・サーバー・インスタンスの設定

設定	Microsoft Windows	AIX および Linux	Solaris
名前	dsrdbm01	dsrdbm01	dsrdbm01
インスタンス・ロケーション	c:\%idsslappd-dsrdbm01	/home/dsrdbm01	/export/home/dsrdbm01
グループ名	Administrators	grrdbm01	grrdbm01
管理者 DN	cn=root	cn=root	cn=root
データベース名	dsrdbm01	dsrdbm01	dsrdbm01

デフォルト・ディレクトリー・サーバー・インスタンスの DB2 テーブル・スペースは、データベース管理ストレージ (DMS) です。

デフォルト・ディレクトリー・サーバー・インスタンスには、インスタンス管理ツールによって o=sample サフィックスが作成されます。後で構成ツールまたは **idscfgsuf** コマンドを使用して、サフィックスを追加することができます。詳細については、228 ページの『サフィックス構成』を参照してください。

## 手順

1. インスタンス管理ツール の始動 146 ページの『インスタンス管理ツールの始動』を参照してください。
2. 「**インスタンスの作成**」をクリックします。
3. 「**新規 Directory Server インスタンスの作成**」ウィンドウで、以下の手順を実行します。
  - a. 「**デフォルト・インスタンスの作成**」をクリックします。
  - b. 「**次へ**」をクリックします。
  - c. 「**ユーザー・パスワード**」フィールドに、ディレクトリー・サーバー・インスタンスを所有するユーザー・アカウントのパスワードを入力します。
  - d. 「**確認パスワード**」フィールドに、ディレクトリー・サーバー・インスタンスを所有するユーザー・アカウントのパスワードをもう一度入力します。
  - e. 「**暗号化シード**」フィールドに、ディレクトリー・サーバー・インスタンスの暗号化シードを入力します。

**要確認:** ディレクトリー・サーバー・インスタンスの暗号化シードは、他の構成タスクで必要となる場合があるため、忘れないようにしてください。

暗号化シードに含める文字は、33 から 126 の範囲の値の印刷可能な ISO-8859-1 ASCII 文字のみでなければなりません。暗号化シードの長さは、12 文字以上 1016 文字以下でなければなりません。使用する文字については、142 ページの『33 番から 126 番までの ASCII 文字』を参照してください。ディレクトリー・サーバーは、暗号化シードを使用して Advanced Encryption Standard (AES) 共通鍵の値セットを生成します。鍵の値は、ディレクトリー・サーバー・インスタンスの鍵 stash ファイルに格納され、パスワードと属性の暗号化および暗号化解除に使用されます。

- f. 「**暗号化シードの確認**」フィールドに、ディレクトリー・サーバー・インスタンスの暗号化シードを入力します。

- g. 「管理者 DN パスワード」フィールドに、ディレクトリー・サーバー・インスタンス管理者のパスワードを入力します。
  - h. 「確認パスワード」フィールドに、ディレクトリー・サーバー・インスタンス管理者のパスワードを入力します。
  - i. 「次へ」をクリックします。
  - j. デフォルトのディレクトリー・サーバー・インスタンスに関する情報を確認します。および
  - k. デフォルトのディレクトリー・サーバー・インスタンスの作成を開始するには、「完了」をクリックします。 ログ情報を含んだ「結果」ウィンドウが表示されます。
4. 「結果」ウィンドウに表示されたログ情報を確認します。
  5. 「結果」ウィンドウを閉じるには、「閉じる」をクリックします。
  6. インスタンス管理ツールを閉じるには、「閉じる」をクリックします。

## タスクの結果

インスタンス管理ツールによって、コンピューター上にデフォルトのディレクトリー・サーバー・インスタンス dsrdbm01 が作成されます。

## 次のタスク

ディレクトリー・サーバー・インスタンスに関連付けられた `ibmslapd` プロセスおよび管理サーバーを始動する必要があります。 176 ページの『ディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

# カスタム設定を使用したディレクトリー・サーバー・インスタンスの作成

インスタンス管理サーバーを使用して、要件に従ったカスタム値でディレクトリー・サーバー・インスタンスを作成します。

## 始める前に

ディレクトリー・サーバー・インスタンスを作成するには、以下のタスクを実行する必要があります。

1. IBM Security Directory Server をサーバー機能とともにインストールします。 35 ページの『IBM Installation Manager を使用したインストール』を参照してください。
2. RDBM バックエンドを使用するフル・ディレクトリー・サーバーを作成する場合は、IBM DB2 をインストールします。 35 ページの『IBM Installation Manager を使用したインストール』を参照してください。
3. `ldapdb.properties` ファイルに、DB2 のインストール・パスおよびバージョン情報が含まれているかどうかを確認します。 283 ページの『付録 C. 手動による `ldapdb.properties` ファイルの更新』を参照してください。

## 手順

1. インスタンス管理ツールの始動 146 ページの『インスタンス管理ツールの始動』を参照してください。

2. 「**インスタンスの作成**」をクリックします。
3. 「**新規 Directory Server インスタンスの作成**」ウィンドウの「**作成または移行**」パネルで、「**新規 Directory Server インスタンスの作成**」をクリックします。
4. 「**次へ**」をクリックします。
5. 「**新規 Directory Server インスタンスの作成**」ウィンドウの「**インスタンスの詳細**」パネルで、以下の値を指定します。
  - a. 「**ユーザー名**」リストから、ディレクトリー・サーバー・インスタンスを所有するユーザー名を選択します。このユーザー名と同じ名前がディレクトリー・サーバー・インスタンスに割り当てられます。
  - b. このインスタンスに新規ユーザー・アカウントを関連付ける場合は、「**ユーザーの作成**」をクリックします。「**Directory Server インスタンスの新規ユーザーの作成**」ウィンドウで、以下の手順を実行します。
    - 1) 「**ユーザー名**」フィールドに、ユーザー名を入力します。
    - 2) 「**パスワード**」フィールドに、ユーザー・アカウントのパスワードを入力します。
    - 3) 「**確認パスワード**」フィールドに、ユーザー・アカウントのパスワードを入力します。
    - 4) 「**ホーム・ディレクトリー**」フィールドに、ユーザー・アカウント用に構成するホーム・ディレクトリーを入力します。「**参照**」をクリックして、ホーム・ディレクトリーを指定することができます。
    - 5) 「**1 次グループ**」フィールドに、ユーザーの 1 次グループ名を入力します。
    - 6) ユーザー・アカウントを作成するには、「**作成**」をクリックします。
  - c. 既存のユーザー・アカウントを変更するには、「**ユーザー名**」リストでユーザー名を選択し、「**ユーザーの編集**」をクリックします。「**Directory Server インスタンスのユーザーの編集**」ウィンドウで、以下の手順を実行します。
    - 1) 「**ユーザー名**」フィールドにはユーザー名が取り込まれます。
    - 2) 「**パスワード**」フィールドに、ユーザー・アカウントのパスワードを入力します。
    - 3) 「**確認パスワード**」フィールドに、ユーザー・アカウントのパスワードを入力します。
    - 4) 「**ホーム・ディレクトリー**」フィールドに、ユーザー・アカウント用に構成するホーム・ディレクトリーを入力します。「**参照**」をクリックして、ホーム・ディレクトリーを指定することができます。
    - 5) 「**1 次グループ**」フィールドに、ユーザーの 1 次グループ名を入力します。
    - 6) ユーザー・アカウントを編集するには、「**編集**」をクリックします。
6. 「**インスタンス・ロケーション**」フィールドに、ディレクトリー・サーバー・インスタンスのロケーションを入力します。「**参照**」をクリックして、インスタンス・ホーム・ディレクトリーを指定することができます。このロケーションには、30 MB 以上の空きディスク・スペースが必要です。Windows システムの場合、このロケーションは C: などのディスク・ドライブです。ディレク

トリー・インスタンス・ファイルは、指定したディスク・ドライブ上の `#{dsslapd-instance_name}` ディレクトリーに格納されます。`instance_name` 変数は、ディレクトリー・サーバー・インスタンスの名前です。AIX、Linux、および Solaris システムの場合は、ディレクトリー・サーバー・インスタンス所有者のホーム・ディレクトリーがデフォルトのインスタンス・ロケーションとなりますが、別のパスを指定することができます。

7. 「暗号化シード・ストリング」フィールドに、ディレクトリー・サーバー・インスタンスの暗号化シードを入力します。

**要確認:** ディレクトリー・サーバー・インスタンスの暗号化シードは、他の構成タスクで必要となる場合があるため、忘れないようにしてください。

暗号化シードに含める文字は、33 から 126 の範囲の値の印刷可能な ISO-8859-1 ASCII 文字のみでなければなりません。暗号化シードの長さは、12 文字以上 1016 文字以下でなければなりません。使用する文字については、142 ページの『33 番から 126 番までの ASCII 文字』を参照してください。ディレクトリー・サーバーは、暗号化シードを使用して Advanced Encryption Standard (AES) 共通鍵の値セットを生成します。鍵の値は、ディレクトリー・サーバー・インスタンスの鍵 `stash` ファイルに格納され、パスワードと属性の暗号化および暗号化解除に使用されます。

8. 「暗号化シードの確認」フィールドに、ディレクトリー・サーバー・インスタンスの暗号化シードを入力します。
9. 暗号化ソルト値を指定する場合は、「暗号化ソルト値の使用」をクリックします。
  - a. 「暗号化ソルト・ストリング」フィールドに、ディレクトリー・サーバー・インスタンスの暗号化ソルト値を入力します。暗号化ソルトに含める文字は、33 から 126 の範囲の値の印刷可能な ISO-8859-1 ASCII 文字のみでなければなりません。暗号化ソルトは 12 文字で指定する必要があります。使用する文字については、142 ページの『33 番から 126 番までの ASCII 文字』を参照してください。ディレクトリー・サーバーの暗号化を別のディレクトリー・サーバー・インスタンスと同期させるには、同じ暗号化シードとソルト値を使用する必要があります。
  - b. 「暗号化ソルトの確認」フィールドに、ディレクトリー・サーバー・インスタンスの暗号化ソルト値を入力します。
10. オプション: 「インスタンスの説明」フィールドに、ディレクトリー・サーバー・インスタンスの説明を入力します。この説明はインスタンスの識別に役立ちます。
11. 「次へ」をクリックします。
12. 「DB2 インスタンスの詳細」パネルの「DB2 インスタンス名」フィールドで、ディレクトリー・サーバー・インスタンスの DB2 インスタンス名を指定します。

**注:** ディレクトリー・サーバー・インスタンスの DB2 インスタンスは、他のプログラムまたは製品によって構成または使用されていないことが必要です。

デフォルトでは、DB2 インスタンス名はディレクトリー・サーバー・インスタンス名と同じになります。ただし、DB2 インスタンスには別の名前を指定することができます。別の名前を指定する場合は、同じ名前のシステム・ユーザー

ID がコンピューターに存在していなければなりません。このユーザー・アカウント名を別のディレクトリー・サーバー・インスタンスに関連付けることはできません。

13. 「次へ」をクリックします。
14. 「マルチホーム・ホストの場合の TCP/IP 設定」パネルで、以下のいずれかのオプションを選択します。
  - ディレクトリー・サーバー・インスタンスにすべての IP アドレスを listen させる場合は、「すべての構成済み IP アドレスを listen する」を選択します。
  - コンピューター上で構成された特定の IP アドレス・セットをインスタンスに listen させる場合は、以下の手順を実行します。
    - a. 「すべての構成済み IP アドレスを listen する」をクリアします。
    - b. 「listen する特定の IP アドレスの選択」リストから、インスタンスが listen する IP アドレスを選択します。
15. 「次へ」をクリックします。
16. 「TCP/IP ポートの設定」パネルで、以下の値を指定します。

注: ディレクトリー・サーバーのポートには、コンピューターで使用されている既存のポートと競合しない固有のポート番号を割り当てる必要があります。AIX、Linux、および Solaris の各システムでは、1 から 1000 の範囲のポート番号を root のみが使用できます。

- a. 「サーバー・ポート」フィールドに、サーバーが非セキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - b. 「サーバーのセキュア・ポート」フィールドに、サーバーがセキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - c. 「管理サーバー・ポート」フィールドに、管理サーバーが非セキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - d. 「管理サーバー・セキュア・ポート」フィールドに、管理サーバーがセキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - e. 「次へ」をクリックします。
17. 「オプションのステップ」パネルで、以下の手順を実行します。
    - a. ディレクトリー・サーバー・インスタンスの管理者 DN とパスワードを構成するには、「管理者 DN とパスワードの構成」を選択します。管理者 DN とパスワードは、プロキシ・サーバーとフル・ディレクトリー・サーバーに対して設定する必要があります。
    - b. ディレクトリー・サーバー・インスタンスのデータベースを構成するには、「データベースの構成」を選択します。
    - c. 「次へ」をクリックします。
  18. 「管理者 DN とパスワードの構成」パネルで、以下の手順を実行します。

- a. 「管理者 DN」フィールドに有効な DN を入力するか、デフォルト DN の `cn=root` をそのまま使用します。管理者 DN の値には大/小文字の区別はありません。管理者 DN ユーザーには、ディレクトリー・サーバー・インスタンス内のすべてのデータに対する全アクセス権限が与えられます。
  - b. 「管理者パスワード」フィールドに、管理者 DN のパスワードを入力します。パスワードでは、大文字と小文字が区別されます。2 バイト文字セット (DBCS) の文字はパスワード内で使用できません。
  - c. 「確認パスワード」フィールドに、管理者 DN のパスワードを入力します。パスワードは今後も使用するため、忘れないようにしてください。
  - d. 「次へ」をクリックします。
19. 「データベースの構成」パネルで、以下のタスクを実行してディレクトリー・サーバー・インスタンスのデータベースを構成します。インスタンス管理ツールによって、ディレクトリー・サーバー・インスタンスの構成ファイル (`ibmslapd.conf`) にデータベース情報が追加されます。データベースが存在しない場合は、インスタンス管理ツールによってデータベースが作成されます。
- a. 「データベース・ユーザー名」フィールドに、有効な DB2 管理者 ID を入力します。データベースを構成するには、DB2 管理者 ID がコンピューターに存在していること、および必要なアクセス権を持っていることが必要です。

注: サーバーを始動する前に、DB2 管理者 ID によってサーバー・メッセージを表示する言語のロケールが適切に設定されている必要があります。

- b. 「パスワード」フィールドに、DB2 管理者のパスワードを入力します。パスワードでは、大文字と小文字が区別されます。

注: DB2 管理者のシステム・パスワードを変更する場合、インスタンス管理ツールではそのパスワードを更新できません。構成ツールまたは `w-` パラメーター付きの `idscfgdb` コマンドを使用する必要があります。詳細については、204 ページの『DB2 データベース管理者パスワードの管理』を参照してください。

- c. 「データベース名」フィールドに、DB2 データベース名を入力します。この名前は、1 から 8 文字の範囲でなければなりません。
- d. オプション: 以下の DB2 構成設定を設定する場合は、「拡張テーブル・スペース・オプションの表示」を選択します。

注: DB2 は、テーブル・スペースを作成するときに、データ・ストレージ・タイプとしてシステム管理ストレージ (SMS) またはデータベース管理ストレージ (DMS) を使用できます。IBM Security Directory Server のデフォルトはデータベース管理ストレージ (DMS) です。6.2 以前のバージョンの IBM Security Directory Server は、すべてのデータベースに SMS を使用します。「拡張テーブル・スペース・オプションの表示」をクリアした場合は、デフォルトのサイズとロケーションの `USERSPACE1` および `LDAPSPACE` テーブル・スペースが、DMS を使用して作成されます。AIX、Linux、および Solaris での `USERSPACE1` テーブル・スペースのデフォルトのパスとファイル名は、`database_location/instance_name/NODE0000/SQL00001/USPACE` です。Windows での `USERSPACE1` テーブル・スペースのデフォルトのパスとファイル名は、

`database_location¥instance_name¥NODE0000¥SQL00001¥USPACE` です。  
AIX、Linux、および Solaris での LDAPSPACE テーブル・スペースのデフォルトのパスとファイル名は、`database_location/  
ldap32kcont_instance_name/ldapspace` です。Windows での LDAPSPACE テーブル・スペースのデフォルトのパスとファイル名は、  
`database_location¥ldap32kcont_instance_name¥ldapspace` です。

- データベースで DB2 テーブル・スペースにシステム管理ストレージ (SMS) データ・ストレージを使用する場合。SMS が使用される場合は、オペレーティング・システムのファイル・システム・マネージャーによって、DB2 テーブルを保管するテーブル・スペースの割り振りと管理が行われます。
- データベースで DB2 テーブル・スペースにデータベース管理ストレージ (DMS) データ・ストレージを使用し、さらに USERSPACE1 テーブル・スペースと LDAPSPACE テーブル・スペース、サイズ、およびロケーションを指定してデータベースを構成する場合。DMS が使用される場合には、テーブル・スペースはデータベース・マネージャーによって管理されます。データベース管理者が、使用するデバイスおよびファイルを決定的と、DB2 がこれらのデバイスとファイルでスペースを管理します。

e. 「次へ」をクリックします。

20. 「データベース・オプション」パネルで、以下の手順を実行します。

- a. 「データベースのインストール・ロケーション」フィールドに、データベース・ロケーション・パスを入力します。「参照」をクリックして、ディレクトリーを指定します。Windows では、ディスク・ドライブのロケーション C: を指定する必要があります。AIX、Linux、および Solaris では、ロケーションが `/home/ldapdb` などのディレクトリー名でなければなりません。

注: DMS データベースに必要な最小のディスク・スペースは 1 GB です。SMS データベースの場合は、最小で 150 MB のディスク・スペースが必要です。これらの要件は、空のデータベースの場合です。データベースにデータを保管すると、さらにディスク・スペースが必要になってきます。

- b. ディレクトリー・サーバーでデータベースのオンライン・バックアップを構成するには、以下の手順を実行します。

- 1) 「オンライン・バックアップの構成」を選択します。
- 2) 「データベースのバックアップ・ロケーション」フィールドに、バックアップ・イメージを保管するロケーションを入力します。「参照」をクリックすると、ロケーションを指定できます。

注: バックアップ操作の実行中にインスタンス管理ツールを終了しないでください。

データベースの構成が完了した後にデータベースのオンライン・バックアップを構成すると、データベースのオフライン・バックアップが実行されます。オフライン・バックアップ操作が完了すると、管理サーバーが再始動します。 `idscfgdb` コマンドを使用して、ディレクトリー・サーバー・インスタンスでのオンライン・バックアップを構成することもできます。ただし、`idscfgdb` コマンドに `-c` パラメーターを指定してオンライン・バックアップを構成解除することはできません。インスタンス管理ツールまたは構成ツ

ールを使用してインスタンスでのオンライン・バックアップを構成した場合は、構成ツールまたは **idscfgdb** コマンドを使用してその構成を解除できます。

- c. 「**文字セット・オプション**」領域で、以下のいずれかのオプションを選択してデータベース・タイプを作成します。

注: データを複数の言語でディレクトリー・サーバーに保管する場合は、ユニバーサル DB2 データベースを作成します。ユニバーサル DB2 データベースはデータ変換が少ないため、最も効率的でもあります。言語タグを使用する場合は、データベースが UTF-8 データベースである必要があります。UTF-8 の詳細については、138 ページの『UTF-8 サポート』を参照してください。

- LDAP クライアントが UTF-8 文字データを保管できる UCS Transformation Format (UTF-8) データベースを作成する場合は、「**ユニバーサル DB2 データベースの作成**」をクリックします。
- ローカル・コード・ページでデータベースを作成する場合は、「**ローカル・コード・ページ DB2 データベースの作成**」をクリックします。

- d. 「**次へ**」をクリックします。

21. 「**データベースの構成**」パネルで「**拡張テーブル・スペース・オプションの表示**」を選択した場合は、「**データベース・テーブル・スペースの構成**」パネルで以下の値を入力する必要があります。

- a. 「**データベース・テーブル・スペース・タイプの選択**」リストから、データベース・タイプを選択します。DMS データベースのテーブル・スペース・タイプがデフォルトです。SMS データベースのテーブル・スペース・タイプを選択すると、他のすべてのフィールドが使用不可になります。DMS テーブル・スペース・サポートは、USERSPACE1 および LDAPSPACE テーブル・スペースに対してのみ使用されます。その他すべてのテーブル・スペース(カタログ・テーブル・スペース、一時テーブル・スペースなど)のタイプは SMS です。

- a. 「**USERSPACE1 テーブル・スペースの詳細**」領域で、以下の詳細を指定します。

- 1) 「**テーブル・スペース・コンテナ**」リストから、コンテナ・タイプを選択します。USERSPACE1 テーブル・スペースのロケーションをファイル・システムにする場合は、「**ファイル**」を選択します。データベース・テーブル・スペース・コンテナのロケーションがファイル・システム内にある場合、DMS クックド・テーブル・スペースが作成されます。テーブル・スペースの初期サイズおよび拡張可能な単位のサイズを指定すると、テーブル・スペースを必要に応じて自動的に拡張することができます。USERSPACE1 テーブル・スペースをロー・デバイスに作成する場合は、「**ロー・デバイス**」を選択します。ロー・デバイスとは、ファイル・システムがインストールされていないデバイスのこと(ファイル・システムが含まれていないハード・ディスクなど)。データベース・テーブル・スペース・コンテナのロケーションがロー・デバイス内にある場合、DMS ロー・テーブル・スペースが作成されます。この場合、データベース・テーブル・スペース・コンテナのサイズは固定

され、拡張できません。「ロー・デバイス」を選択する場合は、デフォルト値を受け入れる代わりに、コンテナ・ロケーションと併せてサイズを指定してください。

- 2) 「テーブル・スペース・コンテナ」リストで「ファイル」を選択した場合は、以下の詳細を指定します。
  - a) 「ディレクトリー・パス」フィールドで、USERSPACE1 テーブル・スペースを作成するディレクトリー・パスを指定します。「参照」をクリックすると、ディレクトリーを選択できます。
  - b) 「ファイル名」フィールドで、作成するテーブル・スペースのファイル名を入力するか、デフォルトのファイル名 (USPACE) を受け入れます。
  - c) 「初期サイズ」フィールドで、USERSPACE1 テーブル・スペースの初期サイズ (ページ数) を入力するか、デフォルト値を受け入れます。ファイル・タイプのテーブル・スペース・コンテナの場合、USERSPACE1 テーブル・スペース・コンテナは自動増分タイプです。「初期サイズ」フィールドに初期サイズを指定し、「拡張可能サイズ」フィールドに拡張可能な単位のサイズを指定できます。初期サイズのデフォルト値は 16 K ページ、デフォルトの拡張可能な単位サイズは 8 K ページです。USERSPACE1 テーブル・スペース・コンテナのページ・サイズは、1 ページあたり 4 KB です。
- 3) 「テーブル・スペース・コンテナ」リストで「ロー・デバイス」を選択した場合は、以下の詳細を指定します。
  - a) 「デバイス・パス」フィールドに、ロー・デバイスのロケーションを入力します。Windows では、パスが ¥¥.¥ で始まっている必要があります。例えば、デバイス名を含むパスの場合は ¥¥.¥device\_name となります。AIX、Linux、および Solaris では、デバイス・パスが有効なパスでなければなりません。
  - b) 「初期サイズ」フィールドで、USERSPACE1 テーブル・スペースの初期サイズを入力するか、デフォルト値を受け入れます。ロー・デバイス・タイプのテーブル・スペース・コンテナの場合、USERSPACE1 テーブル・スペース・コンテナのサイズは固定です。デフォルトのサイズは 16 K ページです。よりよい結果が得られるように、必要なサイズを指定してください。
- b. 「LDAPSPACE テーブル・スペースの詳細」領域で、以下の詳細を指定します。
  - 1) 「テーブル・スペース・コンテナ」リストから、コンテナ・タイプを選択します。LDAPSPACE テーブル・スペースのロケーションをファイル・システムにする場合は、「ファイル」を選択します。LDAPSPACE テーブル・スペースをロー・デバイスに作成する場合は、「ロー・デバイス」を選択します。ロー・デバイスとは、ファイル・システムがインストールされていないデバイスのことです (ファイル・システムが含まれていないハード・ディスクなど)。
  - 2) 「テーブル・スペース・コンテナ」リストで「ファイル」を選択した場合は、以下の詳細を指定します。

- a) 「ディレクトリー・パス」フィールドで、LDAPSPACE テーブル・スペースを作成するディレクトリー・パスを指定します。「参照」をクリックすると、ディレクトリーを選択できます。
  - b) 「ファイル名」フィールドで、作成するテーブル・スペースのファイル名を入力するか、デフォルトのファイル名 (ldapSPACE) を受け入れます。
  - c) 「初期サイズ」フィールドで、LDAPSPACE テーブル・スペースの初期サイズ (ページ数) を入力するか、デフォルト値を受け入れます。ファイル・タイプのテーブル・スペース・コンテナの場合、LDAPSPACE テーブル・スペース・コンテナは自動増分タイプです。「初期サイズ」フィールドに初期サイズを指定し、「拡張可能サイズ」フィールドに拡張可能な単位のサイズを指定できます。初期サイズのデフォルト値は 16 K ページ、デフォルトの拡張可能な単位サイズは 8 K ページです。LDAPSPACE テーブル・スペース・コンテナのページ・サイズは、1 ページあたり 32 KB です。
- 3) 「テーブル・スペース・コンテナ」リストで「ロー・デバイス」を選択した場合は、以下の詳細を指定します。
    - a) 「デバイス・パス」フィールドに、ロー・デバイスのロケーションを入力します。Windows では、パスが ¥¥.¥ で始まっている必要があります。例えば、デバイス名を含むパスの場合は ¥¥.¥device\_name となります。AIX、Linux、および Solaris では、デバイス・パスが有効なパスでなければなりません。
    - b) 「初期サイズ」フィールドで、LDAPSPACE テーブル・スペースの初期サイズを入力するか、デフォルト値を受け入れます。ロー・デバイス・タイプのテーブル・スペース・コンテナの場合、LDAPSPACE テーブル・スペース・コンテナのサイズは固定です。デフォルトのサイズは 16 K ページです。よりよい結果が得られるように、必要なサイズを指定してください。
    - c) 「テーブル・スペース・コンテナ」リストのいずれか、または両方で「ファイル」を選択した場合は、「拡張可能サイズ」フィールドでテーブル・スペース・コンテナを拡張するページ数を指定します。
    - d) 「次へ」をクリックします。
  22. 「設定の確認」パネルで、生成された要約を確認します。
  23. ディレクトリー・サーバー・インスタンスの作成を開始するには、「完了」をクリックします。
  24. 「結果」ウィンドウで、インスタンス作成操作に関して生成されたログ・メッセージを確認します。
  25. 「結果」ウィンドウを閉じるには、「閉じる」をクリックします。
  26. インスタンス管理ツールを閉じるには、「閉じる」をクリックします。

## タスクの結果

インスタンス管理ツールによって、コンピューター上にディレクトリー・サーバー・インスタンスが作成されます。

## 次のタスク

ディレクトリー・サーバー・インスタンスに関連付けられた `ibmslapd` プロセスおよび管理サーバーを始動する必要があります。176 ページの『ディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## カスタム設定を使用したプロキシ・サーバー・インスタンスの作成

インスタンス管理サーバーを使用して、要件に従ったカスタム値でプロキシ・サーバー・インスタンスを作成します。

### 始める前に

プロキシ・サーバー・インスタンスを作成するには、以下のタスクを実行する必要があります。

1. IBM Security Directory Server をプロキシ・サーバー機能とともにインストールします。35 ページの『IBM Installation Manager を使用したインストール』を参照してください。

### 手順

1. インスタンス管理ツールの始動 146 ページの『インスタンス管理ツールの始動』を参照してください。
2. 「インスタンスの作成」をクリックします。
3. 「新規 Directory Server インスタンスの作成」ウィンドウの「作成または移行」パネルで、以下の手順を実行してプロキシ・サーバー・インスタンスを作成します。
  - a. 「新規 Directory Server インスタンスの作成」をクリックします。
  - b. 「プロキシとしてセットアップ」をクリックします。
4. 「次へ」をクリックします。
5. 「新規 Directory Server インスタンスの作成」ウィンドウの「インスタンスの詳細」パネルで、以下の値を指定します。
  - a. 「ユーザー名」リストから、インスタンスを所有するユーザー名を選択します。このインスタンスにはユーザー名と同じ名前が割り当てられています。
  - b. このインスタンスに新規ユーザー・アカウントを関連付ける場合は、「ユーザーの作成」をクリックします。「Directory Server インスタンスの新規ユーザーの作成」ウィンドウで、以下の手順を実行します。
    - 1) 「ユーザー名」フィールドに、ユーザー名を入力します。
    - 2) 「パスワード」フィールドに、ユーザー・アカウントのパスワードを入力します。
    - 3) 「確認パスワード」フィールドに、ユーザー・アカウントのパスワードを入力します。
    - 4) 「ホーム・ディレクトリー」フィールドに、ユーザー・アカウント用に構成するホーム・ディレクトリーを入力します。「参照」をクリックして、ホーム・ディレクトリーを指定することができます。

- 5) 「1 次グループ」フィールドに、ユーザーの 1 次グループ名を入力します。
- 6) ユーザー・アカウントを作成するには、「作成」をクリックします。
- c. 既存のユーザー・アカウントを変更するには、「ユーザー名」リストでユーザー名を選択し、「ユーザーの編集」をクリックします。「**Directory Server インスタンスのユーザーの編集**」ウィンドウで、以下の手順を実行します。
  - 1) 「ユーザー名」フィールドにはユーザー名が取り込まれます。
  - 2) 「パスワード」フィールドに、ユーザー・アカウントのパスワードを入力します。
  - 3) 「確認パスワード」フィールドに、ユーザー・アカウントのパスワードを入力します。
  - 4) 「ホーム・ディレクトリー」フィールドに、ユーザー・アカウント用に構成するホーム・ディレクトリーを入力します。「参照」をクリックして、ホーム・ディレクトリーを指定することができます。
  - 5) 「1 次グループ」フィールドに、ユーザーの 1 次グループ名を入力します。
  - 6) ユーザー・アカウントを編集するには、「編集」をクリックします。
  - 7) 「**Directory Server インスタンスのユーザーの編集**」確認ウィンドウで、「はい」をクリックします。
6. 「インスタンス・ロケーション」フィールドに、プロキシ・サーバー・インスタンスのロケーションを入力します。「参照」をクリックして、インスタンス・ホーム・ディレクトリーを指定することができます。このロケーションには、30 MB 以上の空きディスク・スペースが必要です。Windows システムの場合、このロケーションは C: などのディスク・ドライブです。ディレクトリー・インスタンス・ファイルは、指定したディスク・ドライブ上の `%dsslapd-instance_name` ディレクトリーに格納されます。`instance_name` 変数は、プロキシ・サーバー・インスタンスの名前です。AIX、Linux、および Solaris システムの場合は、プロキシ・サーバー・インスタンス所有者のホーム・ディレクトリーがデフォルトのインスタンス・ロケーションとなりますが、別のパスを指定することができます。
7. 「暗号化シード・ストリング」フィールドに、インスタンスの暗号化シードを入力します。

**要確認:** インスタンスの暗号化シードは、他の構成タスクで必要となる場合があるため、忘れないようにしてください。

暗号化シードに含める文字は、33 から 126 の範囲の値の印刷可能な ISO-8859-1 ASCII 文字のみでなければなりません。暗号化シードの長さは、12 文字以上 1016 文字以下でなければなりません。使用する文字については、142 ページの『33 番から 126 番までの ASCII 文字』を参照してください。ディレクトリー・サーバーは、暗号化シードを使用して Advanced Encryption Standard (AES) 共通鍵の値セットを生成します。鍵の値は、ディレクトリー・サーバー・インスタンスの鍵 `stash` ファイルに格納され、パスワードと属性の暗号化および暗号解除に使用されます。

8. 「暗号化シードの確認」フィールドに、インスタンスの暗号化シードを入力します。

9. 暗号化ソルト値を指定する場合は、「**暗号化ソルト値の使用**」をクリックします。
  - a. 「**暗号化ソルト・ストリング**」フィールドに、インスタンスの暗号化ソルト値を入力します。暗号化ソルトに含める文字は、33 から 126 の範囲の値の印刷可能な ISO-8859-1 ASCII 文字のみでなければなりません。暗号化ソルトは 12 文字で指定する必要があります。使用する文字については、142 ページの『33 番から 126 番までの ASCII 文字』を参照してください。
  - b. 「**暗号化ソルトの確認**」フィールドに、インスタンスの暗号化ソルト値を入力します。
10. オプション: 「**インスタンスの説明**」フィールドに、インスタンスの説明を入力します。この説明はインスタンスの識別に役立ちます。
11. 「**次へ**」をクリックします。
12. 「**マルチホーム・ホストの場合の TCP/IP 設定**」パネルで、以下のいずれかのオプションを選択します。
  - インスタンスがすべての IP アドレスを listen するようにするには、「**すべての構成済み IP アドレスを listen する**」を選択します。
  - コンピューター上で構成された特定の IP アドレス・セットをインスタンスに listen させる場合は、以下の手順を実行します。
    - a. 「**すべての構成済み IP アドレスを listen する**」をクリアします。
    - b. 「**listen する特定の IP アドレスの選択**」リストから、インスタンスが listen する IP アドレスを選択します。
13. 「**次へ**」をクリックします。
14. 「**TCP/IP ポートの設定**」パネルで、以下の値を指定します。

注: ディレクトリー・サーバーのポートには、コンピューターで使用されている既存のポートと競合しない固有のポート番号を割り当てる必要があります。AIX、Linux、および Solaris の各システムでは、1 から 1000 の範囲のポート番号を root のみが使用できます。

- a. 「**サーバー・ポート**」フィールドに、サーバーが非セキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - b. 「**サーバーのセキュア・ポート**」フィールドに、サーバーがセキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - c. 「**管理サーバー・ポート**」フィールドに、管理サーバーが非セキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - d. 「**管理サーバー・セキュア・ポート**」フィールドに、管理サーバーがセキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - e. 「**次へ**」をクリックします。
15. 「**オプションのステップ**」パネルで、以下の手順を実行します。

- a. インスタンスの管理者 DN とパスワードを構成するには、「**管理者 DN とパスワードの構成**」を選択します。 管理者 DN とパスワードは、プロキシ・サーバー・インスタンスに対して設定する必要があります。
  - b. 「**次へ**」をクリックします。
16. 「**管理者 DN とパスワードの構成**」パネルで、以下の手順を実行します。
- a. 「**管理者 DN**」フィールドに有効な DN を入力するか、デフォルト DN の `cn=root` をそのまま使用します。 管理者 DN の値には大/小文字の区別はありません。 管理者 DN ユーザーには、インスタンス内のすべてのデータに対する全アクセス権限が与えられます。
  - b. 「**管理者パスワード**」フィールドに、管理者 DN のパスワードを入力します。 パスワードでは、大文字と小文字が区別されます。 2 バイト文字セット (DBCS) の文字はパスワード内で使用できません。
  - c. 「**確認パスワード**」フィールドに、管理者 DN のパスワードを入力します。 パスワードは今後も使用するため、忘れないようにしてください。
  - d. 「**次へ**」をクリックします。
17. 「**設定の確認**」パネルで、生成された要約を確認します。
18. プロキシ・サーバー・インスタンスの作成を開始するには、「**完了**」をクリックします。
19. 「**結果**」ウィンドウで、インスタンス作成操作に関して生成されたログ・メッセージを確認します。
20. 「**結果**」ウィンドウを閉じるには、「**閉じる**」をクリックします。
21. インスタンス管理ツールを閉じるには、「**閉じる**」をクリックします。

## タスクの結果

インスタンス管理ツールによって、コンピューター上にプロキシ・サーバー・インスタンスが作成されます。

## 次のタスク

管理サーバーと `ibmslapd` プロセスを構成専用モードで始動し、バックエンド・サーバーを構成する必要があります。 IBM Security Directory Server 資料の『**管理**』セクションを参照してください。

## コマンド行ユーティリティーを使用したインスタンスの作成

コマンド行ユーティリティー `idsicrt` を使用して、インスタンスを作成します。

### 始める前に

コマンド行ユーティリティーを使用してインスタンスを作成するには、以下の条件を満たしている必要があります。

1. IBM Security Directory Server を、サーバー、プロキシ・サーバー、またはその両方の機能とともにインストールします。 35 ページの『**IBM Installation Manager を使用したインストール**』を参照してください。

2. インスタンスを所有するシステム・ユーザー ID が存在している必要があります。システム・ユーザー ID の作成について詳しくは、133 ページの『ディレクトリー・サーバー・インスタンスに関連付けられたユーザーとグループ』を参照してください。

## このタスクについて

**idsicrt** コマンドを実行すると、インスタンスおよびフル・ディレクトリー・サーバー・インスタンスの DB2 データベース・インスタンスが作成されます。

### 手順

1. AIX、Linux、または Solaris では root ユーザーとしてログインし、Windows では管理者メンバーとしてログインします。
2. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ローション内の sbin サブディレクトリーに変更します。
3. インスタンスを作成するには、以下のコマンドを実行します。 *instance\_name* 変数は、有効なシステム・ユーザー ID の名前で置き換えてください。

完了するタスク	実行するコマンド:
ディレクトリー・サーバー・インスタンスの作成	<code>idsicrt -I instance_name -e mysecretkey! -l instance_home</code>
プロキシ・サーバー・インスタンスの作成	<code>idsicrt -I instance_name -e mysecretkey! -l instance_home -x</code>

**idsicrt** コマンドについて詳しくは、「*Command Reference*」を参照してください。

### 例

**例 1:** AIX、Linux、または Solaris で、次の値を指定してディレクトリー・サーバー・インスタンスを作成するには、以下のコマンドを実行します。

- インスタンス名: `myinst`
- 非セキュア・ポート: 389
- セキュア・ポート: 636
- 暗号化シード: `mysecretkey!`
- 暗号化ソルト: `mysecretsalt`
- インスタンスのホーム: `/home/myinst` (AIX および Linux) または `/export/home/myinst` (Solaris)

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!¥  
-g mysecretsalt -l /home/myinst
```

Windows で次の値を指定してディレクトリー・サーバー・インスタンスを作成するには、以下のコマンドを実行します。

- インスタンス名: `myinst`
- 非セキュア・ポート: 389
- セキュア・ポート: 636
- 暗号化シード: `mysecretkey!`
- 暗号化ソルト: `mysecretsalt`

- インスタンスのホーム: C:

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!  
-g mysecretsalt -l C:
```

**例 2:** AIX、Linux、または Solaris で、次の値を指定してプロキシ・サーバー・インスタンスを作成するには、以下のコマンドを実行します。

- インスタンス名: myproxy
- 非セキュア・ポート: 389
- セキュア・ポート: 636
- 暗号化シード: mysecretkey!
- 暗号化ソルト: mysecretsalt
- インスタンスのホーム: /home/myproxy (AIX および Linux) または /export/home/myproxy (Solaris)

```
idsicrt -I myproxy -p 389 -s 636 -e mysecretkey!  
-g mysecretsalt -l /home/myproxy -x
```

Windows で次の値を指定してプロキシ・サーバー・インスタンスを作成するには、以下のコマンドを実行します。

- インスタンス名: myproxy
- 非セキュア・ポート: 389
- セキュア・ポート: 636
- 暗号化シード: mysecretkey!
- 暗号化ソルト: mysecretsalt
- インスタンスのホーム: C:

```
idsicrt -I myproxy -p 389 -s 636 -e mysecretkey!  
-g mysecretsalt -l C: -x
```

## 次のタスク

以下の構成を実行して、機能するインスタンスを作成します。

1. フル・ディレクトリー・サーバー・インスタンス用に DB2 データベース・インスタンスを構成します。
2. インスタンスの管理者 DN およびパスワードを構成します。
3. インスタンスのサフィックスを構成します。

## インスタンス管理ツールを使用した前のバージョンのインスタンスのアップグレード

インスタンス管理ツールを使用して、前のバージョンのディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスをバージョン 6.3.1 にアップグレードします。

### 始める前に

インスタンス管理ツールを使用してインスタンスをアップグレードする前に、以下のタスクを完了させる必要があります。

- IBM Security Directory Server バージョン 6.3.1 のインストールを完了します。31 ページの『インストールの開始』を参照してください。

- インスタンスをアップグレードする前に、環境をセットアップします。98 ページの『インスタンスをアップグレードする前の環境の設定』を参照してください。
- AIX、Linux、または Solaris オペレーティング・システムでは root ユーザーとしてログインし、Windows オペレーティング・システムでは管理者グループのメンバーとしてログインします。

## このタスクについて

前のバージョンのインスタンスをアップグレードした後、そのインスタンスは IBM Security Directory Server バージョン 6.3.1 の完全に機能するインスタンスに変換されます。

## 手順

1. コマンド・プロンプトにアクセスします。
2. 現在の作業ディレクトリーを sbin に変更します。次のロケーションが、各オペレーティング・システム上のデフォルトのロケーションです。

### Microsoft Windows

```
C:¥Program Files¥IBM¥ldap¥V6.3.1¥sbin
```

### AIX および Solaris

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

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

3. インスタンス管理ツールを始動するには、以下のコマンドを実行します。

注: Windows システムでは、「スタート」メニューから開始することができます。「スタート」 > 「すべてのプログラム」 > 「IBM Security Directory Server 6.3.1」 > 「インスタンス管理ツール」をクリックします。

```
idsxinst
```

4. アップグレードするインスタンスの前のバージョンを選択します。
5. 「マイグレーション」をクリックします。
6. 「Directory Server インスタンスのマイグレーション」ウィンドウで、「マイグレーション」をクリックします。
7. アップグレード操作の完了後にインスタンス管理ツールでプロンプトが表示された場合は、「OK」をクリックします。
8. 要約情報を検証します。
9. 「Directory Server インスタンスのマイグレーション」ウィンドウを閉じるには、「閉じる」をクリックします。
10. インスタンスのオフライン・バックアップを実行します。詳細については、212 ページの『ディレクトリー・サーバーのバックアップ』を参照してください。
11. インスタンス管理ツールを閉じるには、「閉じる」をクリックします。

## タスクの結果

インスタンス管理ツールによって、前のバージョンのディレクトリー・サーバー・インスタンスが 6.3.1 にアップグレードされます。

## 次のタスク

ディレクトリー・サーバー・インスタンスに関連付けられた `ibmslapd` プロセスおよび管理サーバーを始動する必要があります。176 ページの『ディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## インスタンス管理ツールを使用した前のバージョンのリモート・インスタンスのアップグレード

インスタンス管理ツールを使用して、前のバージョンのリモートのディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスをバージョン 6.3.1 にアップグレードします。

### 始める前に

インスタンス管理ツールを使用してインスタンスをアップグレードする前に、以下のタスクを完了させる必要があります。

- インスタンスをアップグレードする前に、環境をセットアップします。98 ページの『インスタンスをアップグレードする前の環境の設定』を参照してください。
- AIX、Linux、または Solaris オペレーティング・システムでは `root` ユーザーとしてログインし、Windows オペレーティング・システムでは管理者グループのメンバーとしてログインします。

### このタスクについて

アップグレード処理の完了後に、インスタンス管理ツールでは、リモート・インスタンスの情報を使用してコンピューター上に 6.3.1 のインスタンスを作成します。

### 手順

1. `idsdb2ldif` コマンドを使用して、リモート・コンピューター上に存在するディレクトリー・サーバー・インスタンスのデータベースをバックアップします。

**重要:** プロキシ・サーバー・インスタンスをアップグレードしている場合は、データベースをバックアップしないでください。プロキシ・サーバーには、それに関連付けられたデータベースは含まれていません。

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

`idsdb2ldif` コマンドについて詳しくは、「*Command Reference*」を参照してください。

2. リモート・インスタンスのアップグレード対象のコンピューターへの IBM Security Directory Server バージョン 6.3.1 のインストールを完了させます。31 ページの『インストールの開始』を参照してください。
3. リモート・インスタンスのスキーマ・ファイルおよび構成ファイルをバックアップするには、アップグレード先バージョンの 6.3.1 の次の `migbkup` コマンドを実行します。

オペレーティング・システム	実行するコマンド:
Microsoft Windows	<code>migbkup.bat drive_name%idsldapd-instance_name backup_directory</code>

オペレーティング・システム	実行するコマンド:
AIX、Linux、および Solaris	<code>migbkup user_home_dir/idsslapd-instance_name backup_directory</code>

**migbkup** コマンドは、IBM Security Directory Server インストール・メディアの `tools` サブディレクトリーにあります。

4. **migbkup** を使用して作成したバックアップ・ディレクトリーの `backup_directory` をリモート・コンピューターから、IBM Security Directory Server バージョン 6.3.1 がインストールされたコンピューターにコピーします。
5. オプション: データベース・バックアップ・ファイルの `inst_out.ldif` をリモート・コンピューターから、IBM Security Directory Server バージョン 6.3.1 がインストールされたコンピューターにコピーします。
6. インスタンス管理ツールの始動 146 ページの『インスタンス管理ツールの始動』を参照してください。
7. 「インスタンスの作成」をクリックします。
8. 「作成または移行」パネルで、以下のタスクを実行します。
  - a. 「前のバージョンのディレクトリー・サーバーからの移行」をクリックします。
  - b. 「バックアップ・ファイルのパスの入力」フィールドに、リモート・インスタンスの構成ファイルとスキーマ・ファイルのバックアップをコピーしたパスを入力します。「参照」をクリックして、バックアップ・ロケーションを指定できます。
  - c. 「次へ」をクリックします。
9. 「新規 Directory Server インスタンスの作成」ウィンドウの「インスタンスの詳細」パネルで、次の各値を指定します。

注: インスタンスをアップグレードしている場合、既存のユーザー情報を編集することはできません。

- a. 「ユーザー名」のリストから、ディレクトリー・サーバー・インスタンスを所有する必要があるユーザー名を選択します。このユーザー名と同じ名前がディレクトリー・サーバー・インスタンスに割り当てられます。
- b. このインスタンスに新規ユーザー・アカウントを関連付ける場合は、「ユーザーの作成」をクリックします。「Directory Server インスタンスの新規ユーザーの作成」ウィンドウで、以下の手順を実行します。
  - 1) 「ユーザー名」フィールドに、ユーザー名を入力します。
  - 2) 「パスワード」フィールドに、ユーザー・アカウントのパスワードを入力します。
  - 3) 「確認パスワード」フィールドに、ユーザー・アカウントのパスワードを入力します。
  - 4) 「ホーム・ディレクトリー」フィールドに、ユーザー・アカウント用に構成するホーム・ディレクトリーを入力します。「参照」をクリックして、ホーム・ディレクトリーを指定することができます。
  - 5) 「1 次グループ」フィールドに、ユーザーの 1 次グループ名を入力します。

- 6) ユーザー・アカウントを作成するには、「作成」をクリックします。
10. 「**インスタンス・ロケーション**」フィールドに、ディレクトリー・サーバー・インスタンスのロケーションを入力します。「参照」をクリックして、インスタンス・ホーム・ディレクトリーを指定することができます。このロケーションには、30 MB 以上の空きディスク・スペースが必要です。Windows システムの場合、このロケーションは C: などのディスク・ドライブです。ディレクトリー・インスタンス・ファイルは、指定したディスク・ドライブ上の `%idsslapd-instance_name` ディレクトリーに格納されます。`instance_name` 変数は、ディレクトリー・サーバー・インスタンスの名前です。AIX、Linux、および Solaris システムの場合は、ディレクトリー・サーバー・インスタンス所有者のホーム・ディレクトリーがデフォルトのロケーションとなりますが、別のパスを指定することができます。
  11. オプション: 「**インスタンスの説明**」フィールドに、ディレクトリー・サーバー・インスタンスの説明を入力します。この説明はインスタンスの識別に役立ちます。
  12. 「次へ」をクリックします。
  13. リモートのディレクトリー・サーバー・インスタンスを DB2 データベースの詳細でアップグレードする場合は、「**DB2 インスタンスの詳細**」パネルで「次へ」をクリックします。バックアップ・ファイルがリモートのプロキシ・サーバー・インスタンスのものである場合、「**DB2 インスタンスの詳細**」パネルが表示されない場合があります。
  14. 「**マルチホーム・ホストの場合の TCP/IP 設定**」パネルで、以下のいずれかのオプションを選択します。
    - ディレクトリー・サーバー・インスタンスにすべての IP アドレスを listen させる場合は、「**すべての構成済み IP アドレスを listen する**」を選択します。
    - コンピューター上で構成された特定の IP アドレス・セットをディレクトリー・サーバー・インスタンスで listen させるには、「**すべての構成済み IP アドレスを listen する**」をクリアします。ディレクトリー・サーバー・インスタンスで listen させる IP アドレスをリストから 1 つ以上選択します。
  15. 「次へ」をクリックします。
  16. 「**TCP/IP ポートの設定**」パネルで、以下の値を指定します。

注: ディレクトリー・サーバーのポートには、コンピューターで使用されている既存のポートと競合しない固有のポート番号を割り当てる必要があります。AIX、Linux、および Solaris の各システムでは、1 から 1000 の範囲のポート番号を root のみが使用できます。

- a. 「**サーバー・ポート**」フィールドに、サーバーが非セキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
- b. 「**サーバーのセキュア・ポート**」フィールドに、サーバーがセキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
- c. 「**管理サーバー・ポート**」フィールドに、管理サーバーが非セキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。

- d. 「管理サーバー・セキュア・ポート」フィールドに、管理サーバーがセキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - e. 「次へ」をクリックします。
17. 「設定の確認」パネルで、生成された要約を確認します。
  18. バックアップされた構成ファイルとスキーマ・ファイルを使用して、ディレクトリー・サーバー・インスタンスの作成を開始するには、「完了」をクリックします。
  19. 「結果」ウィンドウで、インスタンス作成操作に関して生成されたログ・メッセージを確認します。
  20. 「結果」ウィンドウを閉じるには、「閉じる」をクリックします。
  21. インスタンス管理ツールを閉じるには、「閉じる」をクリックします。

## タスクの結果

インスタンス管理ツールによって、コンピューター上にディレクトリー・サーバー・インスタンスが作成されます。

## 次のタスク

ディレクトリー・サーバー・インスタンスに関連付けられた `ibmslapd` プロセスおよび管理サーバーを始動する必要があります。176 ページの『ディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

インスタンスのバックアップを実行します。ディレクトリー・サーバー・インスタンスのバックアップについては、212 ページの『ディレクトリー・サーバーのバックアップ』を参照してください。

---

## 既存のインスタンスからのインスタンス作成

インスタンス管理ツールを使用して、ローカル・コンピューターまたはリモート・コンピューターにある既存のインスタンスからディレクトリー・サーバー・インスタンスを作成できます。ソース・ディレクトリー・サーバーは、ターゲット・ディレクトリー・サーバー・インスタンスのテンプレートとして役立ちます。

IBM Security Directory Server インスタンス管理ツールは、ツールおよびインスタンスが同じバージョンの場合に限り、ソース・ディレクトリー・サーバー・インスタンスのコピーをサポートします。ターゲット・ディレクトリー・サーバーは、インスタンス管理ツールが実行されているコンピューター上に作成されます。ソース・ディレクトリー・サーバーが別のコンピューター上にある場合、2 つのコンピューターのオペレーティング・システムは異なっていてもかまいません。例えば、Linux システム上のインスタンスのコピーであるディレクトリー・サーバー・インスタンスを Windows システム上に作成できます。

このツールを使用してソース・インスタンスをコピーするとき、入力に基づいてツールで以下の操作を実行できます。

- ソース・ディレクトリー・サーバー・インスタンスと同じ構成設定およびスキーマ・ファイルを持つターゲット・ディレクトリー・サーバーを作成できます。また、ソース・サーバーからターゲット・サーバー上のディレクトリー鍵 stash ファイルを同期できます。
- ソース・ディレクトリー・サーバー・インスタンスがフル・ディレクトリー・サーバーの場合は、作成されるターゲット・ディレクトリー・サーバー・インスタンスもフル・ディレクトリー・サーバーです。既存のディレクトリー・サーバー・インスタンスからデータをコピーすることを選択できます。ソース・ディレクトリー・サーバーがオンライン・バックアップ用に構成されている場合、そのデータベース内の項目を使用して、機能するターゲット・ディレクトリー・サーバーを作成できます。
- ソース・ディレクトリー・サーバー・インスタンスがプロキシ・サーバーの場合は、作成されるターゲット・ディレクトリー・サーバー・インスタンスもプロキシ・サーバーです。
- ソース・ディレクトリー・サーバーが複製環境にある場合、ターゲット・インスタンスをソース・サーバーのレプリカ・サーバーまたはピア・サーバーとして構成することができます。
- ソース・ディレクトリー・サーバーが分散環境にある場合、ターゲット・ディレクトリー・サーバー・インスタンスをプロキシ・サーバーとして構成できます。
- ソース・ディレクトリー・サーバー・インスタンスがセキュア通信に構成されている場合、インスタンス管理ツールは鍵データベース・ファイルをターゲット・ディレクトリー・サーバーにコピーします。

ソース・ディレクトリー・サーバーからディレクトリー・サーバーを作成する前に、ソース・ディレクトリー・サーバーが以下の条件を満たすようにする必要があります。

- ソース・ディレクトリー・サーバーは IBM Security Directory Server バージョン 6.3.1 である必要があります。ソース・ディレクトリー・サーバーは、前のバージョンのインスタンスであってはなりません。
- ソース・ディレクトリー・サーバーは、通常モードで実行している必要があります。構成モードで実行中のインスタンスのコピーはサポートされません。
- ソース・ディレクトリー・サーバーは、インスタンス管理ツールが稼働しているコンピューターからアクセス可能である必要があります。
- ターゲット・ディレクトリー・サーバーをレプリカまたはピアとして作成するには、ソース・ディレクトリー・サーバー・インスタンス上に複製コンテキストが存在する必要があります。複製トポロジーに最初にレプリカまたはピアを設定する場合、インスタンス管理ツールを使用することはできません。ソース・ディレクトリー・サーバー・インスタンスに、少なくとも 1 つの複製コンテキスト、複製グループ、および複製サブエントリーが定義されている必要があります。インスタンスをレプリカとして構成する場合、ソース・インスタンスには、少なくとも 1 つの別のサーバーへの合意を含む、初期複製トポロジーが含まれている必要があります。インスタンスをピアとして構成する場合は、複製構成の 1 つ以上のサブエントリーについて、そのソース・サーバーがマスターとして定義されていなければなりません。

- インスタンスをピアまたはレプリカとして作成する場合、新しい複製サブエントリーが `ibm-replicaGroup=default,replicationContext` DN の下に作成されません。DN がない場合は、インスタンスをコピーできません。

ソース・ディレクトリー・サーバー・インスタンスからターゲット・ディレクトリー・サーバー・インスタンスにデータをコピーする場合、以下の要件を満たす必要があります。

- DB2 バージョンは、両方のディレクトリー・サーバー・インスタンスで異なってもかまいません。オペレーティング・システム上でのデータベース・バックアップは、オペレーティング・システム・タイプが同じであれば、どのコンピューター上にも復元できます。例えば、Windows システム上の DB2 UDB バージョン 9 に作成されたデータベースを、DB2 バージョン 10 を持つシステムに復元できます。AIX、Linux、および Solaris システムの場合、DB2 UDB バージョン 9 で作成されたバックアップは、バックアップ用および復元用のオペレーティング・システムのエンディアン (ビッグ・エンディアンまたはリトル・エンディアン) が同じであれば、DB2 バージョン 10 に復元できます。
- オンライン・バックアップについてソース・ディレクトリー・サーバー・インスタンスを構成する必要があります。オンライン・バックアップは、初回のデータベース構成中に構成できます。インスタンス管理ツールまたは構成ツールを使用して、オンライン・バックアップを構成できます。
- インスタンス管理ツールを使用してディレクトリー・サーバー・インスタンスをコピーする前に、ソース・ディレクトリー・サーバー・インスタンスの初期オフライン・バックアップを取っておく必要があります。バックアップ用に指定するパスには、1 つのバックアップ・イメージのみを含む必要があります。
- バックアップ・イメージが含まれるパスは、ソース・ディレクトリー・サーバー・インスタンスとターゲット・ディレクトリー・サーバー・インスタンスの両方からアクセス可能でなければなりません。

## インスタンス管理ツールを使用した既存のインスタンスのコピーの作成

インスタンス管理ツールを使用して、既存のインスタンスのコピーを作成します。

### 始める前に

既存のインスタンスのコピーを作成するには、以下の要件を満たしている必要があります。

- インスタンスの `ibmslapd` プロセスおよび管理サーバーを通常モードで始動します。
- ソース・ディレクトリー・サーバーがインスタンス管理ツールからアクセス可能であることを確認します。

### 手順

1. インスタンス管理ツールの始動 146 ページの『インスタンス管理ツールの始動』を参照してください。
2. 以下のオプションのいずれかを選択して、既存のインスタンスのコピーを作成します。

- ローカル・コンピューター上にある既存のインスタンスのコピーを作成するには、「ローカル・インスタンスのコピー」をクリックします。
  - リモート・コンピューター上にある既存のインスタンスのコピーを作成するには、「リモート・インスタンスのコピー」をクリックします。
3. 「**Directory Server インスタンスのコピー**」パネルで、以下の値を指定します。
- a. ソース・ディレクトリー・サーバーがリモート・コンピューター上にある場合は、「**ホスト**」フィールドに IP アドレスまたはホスト名を入力します。ソース・ディレクトリー・サーバーがローカル・コンピューター上にある場合は、このフィールドに localhost が入力されます。この値は編集できません。
  - b. 「**ポート**」フィールド内のポート番号が有効でない場合は、このフィールドにディレクトリー・サーバーのポート番号を入力します。セキュア接続を使用する場合は、ソース・ディレクトリー・サーバー・インスタンスのセキュア・ポート番号を指定する必要があります。
  - c. インスタンスがリモート・コンピューター上にある場合は、「**管理者 DN**」フィールドにソース・ディレクトリー・サーバーの管理者 DN を入力します。ソース・ディレクトリー・サーバーがローカル・コンピューター上にある場合は、このフィールドに管理者 DN の値が入力されます。この値は編集できません。
  - d. 「**パスワード**」フィールドに、管理者 DN のパスワードを入力します。
  - e. 「**暗号化シード**」フィールドに、ソース・ディレクトリー・サーバー・インスタンスの暗号化シードを入力します。
  - f. ソース・ディレクトリー・サーバーがセキュア接続用に構成されている場合に、セキュア接続に対応するようにターゲット・ディレクトリー・サーバーを構成するには、「**SSL 接続の使用**」をクリックします。
    - 1) 「**鍵ファイル**」フィールドに、鍵データベース・ファイルのファイル名をパスとともに入力します。「**参照**」をクリックして、ロケーションを指定します。
    - 2) 「**鍵名**」フィールドに、ソース・ディレクトリー・サーバーの鍵ファイルから使用する秘密鍵名を入力します。
    - 3) 「**鍵パスワード**」フィールドに、鍵ファイルの鍵データベース・パスワードを入力します。
  - g. 「**次へ**」をクリックします。
4. 「**インスタンス・セットアップ - ステップ 1**」パネルで、以下の手順を実行します。
- a. 「**ソース URL**」および「**ソース・インスタンス・タイプ**」フィールドで、ソース・ディレクトリー・サーバーに関する情報を確認します。「**ソース・インスタンス・タイプ**」は、フル・ディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスのいずれかです。
  - b. ターゲット・ディレクトリー・サーバーを既存の複製トポロジーのピアまたはレプリカとして構成するには、「**ピアまたはレプリカ・サーバーとして構成**」を選択し、以下のいずれかのオプションを選択します。
    - ターゲット・ディレクトリー・サーバーをレプリカとして構成する場合は、「**レプリカ**」をクリックします。

- ターゲット・ディレクトリー・サーバーをピアとして構成する場合は、「ピア」をクリックします。
- c. 「**ユーザー名**」フィールドに、ターゲット・ディレクトリー・サーバー・インスタンスを所有するシステム・ユーザー ID を入力します。名前は 8 文字以下でなければなりません。同じ名前が、ディレクトリー・サーバー・インスタンス名、DB2 管理者 ID、データベース・インスタンス名、およびデータベース名にも設定されます。このユーザー ID はコンピューター上に存在している必要があり、コンピューター上の他のディレクトリー・サーバー・インスタンスに関連付けることはできません。ユーザー ID の詳細については、133 ページの『ディレクトリー・サーバー・インスタンスに関連付けられたユーザーとグループ』を参照してください。
  - d. 「**パスワード**」フィールドに、ユーザー ID のパスワードを入力します。
  - e. 「**インスタンス・ロケーション**」フィールドに、ディレクトリー・サーバー・インスタンスのロケーションを入力します。「**参照**」をクリックして、インスタンス・ホーム・ディレクトリーを指定することができます。このロケーションには、30 MB 以上の空きディスク・スペースが必要です。Windows システムの場合、このロケーションは C: などのディスク・ドライブです。ディレクトリー・インスタンス・ファイルは、指定したディスク・ドライブ上の `%idsslapd-instance_name` ディレクトリーに格納されます。`instance_name` 変数は、ディレクトリー・サーバー・インスタンスの名前です。AIX、Linux、および Solaris システムの場合は、ディレクトリー・サーバー・インスタンス所有者のホーム・ディレクトリーがデフォルトのロケーションとなりますが、別のパスを指定することができます。
  - f. 「**次へ**」をクリックします。
5. 「**インスタンス・セットアップ - ステップ 2**」パネルで、以下の手順を実行します。
    - a. 「**管理者 DN**」フィールドに、ターゲット・ディレクトリー・サーバー・インスタンスの有効な DN を入力します。管理者 DN の値には大/小文字の区別はありません。管理者 DN ユーザーには、ディレクトリー・サーバー・インスタンス内のすべてのデータに対する全アクセス権限が与えられません。
    - b. 「**パスワード**」フィールドに、管理者 DN のパスワードを入力します。パスワードでは、大文字と小文字が区別されます。2 バイト文字セット (DBCS) の文字はパスワード内で使用できません。
    - c. 「**確認パスワード**」フィールドに、管理者 DN のパスワードを入力します。パスワードは今後も使用するため、忘れないようにしてください。
    - d. ソース・サーバーのデータベースからターゲット・サーバーにデータをコピーするには、「**ソース・インスタンスから新規インスタンスにデータをコピー**」を選択し、以下の手順を実行します。
 

**注:** ターゲット・ディレクトリー・サーバーをピアまたはレプリカとして作成することを選択した場合は、このチェック・ボックスが選択されてクリアできないようになっています。

      - 1) 「**バックアップ・イメージのパス**」フィールドに、ソース・サーバーのバックアップ・イメージのパス名を入力します。「**参照**」をクリックすると、ロケーションを指定できます。ソース・インスタンスがリモー

ト・コンピューター上にある場合は、このバックアップ・パスがソース・コンピューターとターゲット・コンピューターの両方で共有され、両方からアクセス可能であることが必要です。共有パスの例には、読み取り/書き込み NFS ファイル・システムなどがあります。

- e. 「次へ」をクリックします。
6. 「設定の確認」パネルで、生成された要約を確認します。
7. ソース・ディレクトリー・サーバーのコピーの作成を開始するには、「完了」をクリックします。
8. 「結果」ウィンドウで、インスタンス作成操作に関して生成されたログ・メッセージを確認します。
9. 「結果」ウィンドウを閉じるには、「閉じる」をクリックします。
10. インスタンス管理ツールを閉じるには、「閉じる」をクリックします。

## タスクの結果

インスタンス管理ツールによって、コンピューター上にソース・ディレクトリー・サーバー・インスタンスのコピーが作成されます。

## 次のタスク

ディレクトリー・サーバー・インスタンスに関連付けられた `ibmslapd` プロセスおよび管理サーバーを始動する必要があります。176 ページの『ディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

インスタンスのバックアップを実行します。ディレクトリー・サーバー・インスタンスのバックアップについては、212 ページの『ディレクトリー・サーバーのバックアップ』を参照してください。

## コマンド行ユーティリティーを使用した既存のインスタンスのコピーの作成

コマンド行ユーティリティー `idsideploy` を使用して、インスタンスのコピーを作成します。

### 始める前に

既存のインスタンスのコピーを作成するには、以下の要件を満たしている必要があります。

- ソース・インスタンスの `ibmslapd` プロセスおよび管理サーバーを通常モードで始動します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。
- ソース・ディレクトリー・サーバーが、インスタンスのコピーを作成するコンピューターからアクセス可能であることを確認します。

### 手順

1. AIX、Linux、または Solaris では root ユーザーとしてログインし、Windows では管理者メンバーとしてログインします。
2. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。

3. 既存のディレクトリー・サーバー・インスタンスからデータなしでインスタンスのコピーを作成するには、以下のコマンドを実行します。

```
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
```

**idsideploy** コマンドについて詳しくは、「*Command Reference*」を参照してください。

---

## ディレクトリー・サーバーおよび管理サーバーの始動または停止

ディレクトリー・サーバー・インスタンスを使用するには、インスタンスに関連付けられた管理サーバーおよび **ibmslapd** プロセスを開始する必要があります。

ディレクトリー・サーバーの構成を変更した場合は、変更内容を適用するために、サーバーおよび管理サーバーを停止して再始動することが必要な場合があります。ディレクトリー・サーバーおよび管理サーバーを停止できるのは、これが通常モードまたは構成モードで稼働中の場合に限られます。

インスタンス管理サーバーや、**ibmslapd** あるいは **ibmdiradm** などのサーバー・ユーティリティを使用して、サーバーを始動および停止できます。**ibmslapd** プロセスは、ディレクトリー・サーバーに関連付けられています。ディレクトリー・サーバー・インスタンスは、インスタンス管理ツールを使用して通常モードでのみ始動できます。ディレクトリー・サーバーを構成専用モードで始動するには、コマンド行オプションを使用してください。

ディレクトリー・サーバーは、以下のいずれかの状態になります。

- 始動
- 停止
- 始動 (構成専用)

管理サーバーは、以下のいずれかの状態になります。

- 始動
- 停止

## ディレクトリー・サーバーおよび管理サーバーの始動または停止

インスタンス管理ツールを使用して、インスタンスに関連付けられているディレクトリー・サーバー、管理サーバー、または両方を始動または停止します。

### 始める前に

インスタンスのディレクトリー・サーバーと管理サーバーを始動または停止するには、以下の条件を満たしている必要があります。

1. インスタンス管理ツールと同じバージョンのインスタンスが存在している必要があります。
2. インスタンスが存在しない場合は、インスタンスを作成してください。149 ページの『デフォルトのディレクトリー・サーバー・インスタンスの作成』または 151 ページの『カスタム設定を使用したディレクトリー・サーバー・インスタンスの作成』を参照してください。

## 手順

1. インスタンス管理ツールの始動 146 ページの『インスタンス管理ツールの始動』を参照してください。
2. 「コンピューターにインストールされている **Directory Server** インスタンスのリスト」リストから、インスタンス管理ツールと同じバージョンのインスタンスを選択します。
3. ディレクトリー・サーバー、管理サーバー、または両方を始動または停止するには、「始動/停止」をクリックします。
4. 「サーバー状態の管理」ウィンドウで、以下のアクションを実行します。
  - インスタンスのディレクトリー・サーバー、管理サーバー、またはその両方を始動する場合は、以下の手順を実行します。
    - ディレクトリー・サーバーを始動するには、「サーバーの始動」をクリックします。
    - 管理サーバーを始動するには、「管理サーバーの始動」をクリックします。
    - 「OK」をクリックします。
  - ディレクトリー・サーバー、管理サーバー、またはその両方を停止する場合は、以下の手順を実行します。
    - ディレクトリー・サーバーを停止するには、「サーバーの停止」をクリックします。
    - 管理サーバーを停止するには、「管理サーバーの停止」をクリックします。
    - 「OK」をクリックします。
5. 「サーバー状態の管理」ウィンドウを閉じるには、「閉じる」をクリックします。
6. インスタンス管理ツールを閉じるには、「閉じる」をクリックします。

## コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止

コマンド行ユーティリティーを使用して、インスタンスに関連付けられているディレクトリー・サーバー、管理サーバー、または両方を始動または停止します。

### 始める前に

インスタンスのディレクトリー・サーバーと管理サーバーを始動または停止するには、以下の条件を満たしている必要があります。

- コマンド行ユーティリティーと同じバージョンのインスタンスが存在している必要があります。インスタンスが存在しない場合は、インスタンスを作成してください。149 ページの『デフォルトのディレクトリー・サーバー・インスタンスの作成』または 151 ページの『カスタム設定を使用したディレクトリー・サーバー・インスタンスの作成』を参照してください。

### 手順

1. 必要なアクセス権でコンピューターにログインします。189 ページの『第 20 章 インスタンス構成』を参照してください。

2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
4. インスタンス `instance_name` のサーバーと管理サーバーを始動するには、次のコマンドを実行します。 `instance_name` の値をご使用のインスタンス名で置換します。

```
ibmslapd -I instance_name  
ibmdiradm -I instance_name
```

5. インスタンスのサーバーと管理サーバーを停止するには、次のコマンドを実行します。 `instance_name` の値をご使用のインスタンス名で置換します。

```
ibmslapd -I instance_name -k  
ibmdiradm -I instance_name -k
```

---

## ディレクトリー・サーバー・インスタンス構成の管理

構成ツールを使用して、ディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスの状況の検査や、構成の管理および変更を行うことができます。

構成ツールを使用して、同じバージョンのディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスの構成を管理および変更することができます。IBM Security Directory Server バージョンで提供されている構成ツールを使用して、前のバージョンまたは後のバージョンのディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスを管理することはできません。

インスタンス用の構成ツールは、以下のオプションのいずれかを使用して開くことができます。

- インスタンス管理ツールを使用する。
- インスタンス名をパラメーター値として `idsxcfg` コマンドを実行する。

構成ツールについて詳しくは、189 ページの『第 20 章 インスタンス構成』を参照してください。

## インスタンス管理ツールから構成ツールを開く

IBM Security Directory Server の構成ツールを開いて、ディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスの構成を管理または変更します。

### 始める前に

構成ツールを使用してインスタンスを管理するには、以下の条件を満たしている必要があります。

- 構成ツールと同じバージョンのインスタンスが存在している必要があります。インスタンスが存在しない場合は、インスタンスを作成してください。149 ページの『デフォルトのディレクトリー・サーバー・インスタンスの作成』または 151 ページの『カスタム設定を使用したディレクトリー・サーバー・インスタンスの作成』を参照してください。

## 手順

1. インスタンス管理ツールの始動 146 ページの『インスタンス管理ツールの始動』を参照してください。
2. 「コンピューターにインストールされている Directory Server インスタンスのリスト」リストから、インスタンス管理ツールと同じバージョンのインスタンスを選択します。
3. 構成ツールを使用してインスタンスを管理するには、「管理」をクリックします。 インスタンスに対して IBM Security Directory Server の構成ツール・ウィンドウが開きます。
4. 構成ツールを閉じるには、「ファイル」 > 「終了」をクリックします。
5. 構成ツールの確認ウィンドウで、「はい」をクリックします。

---

## インスタンスの TCP/IP 設定の変更

インスタンス管理ツールまたはコマンド行ユーティリティーを使用して、ディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスの TCP/IP 設定を変更することができます。

インスタンスの TCP/IP 設定を変更するには、インスタンスと、インスタンス管理ツールのバージョンが同じである必要があります。

## インスタンス管理ツールを使用したインスタンスの TCP/IP 設定の変更

インスタンス管理ツールを使用して、既存のインスタンスの TCP/IP 設定を変更します。

### 始める前に

インスタンス管理ツールを使用してインスタンスの TCP/IP 設定を変更するには、以下の条件を満たしている必要があります。

1. インスタンス管理ツールと同じバージョンのインスタンスが存在している必要があります。
2. インスタンスのディレクトリー・サーバーと管理サーバーを停止する必要があります。 176 ページの『ディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. インスタンス管理ツールの始動 146 ページの『インスタンス管理ツールの始動』を参照してください。
2. 「コンピューターにインストールされている Directory Server インスタンスのリスト」リストから、インスタンス管理ツールと同じバージョンのインスタンスを選択します。
3. インスタンスの TCP/IP 設定を変更するには、「TCP/IP 設定の編集」をクリックします。 インスタンスに対して「TCP/IP 設定の編集」ウィンドウが開きます。

4. 「TCP/IP 設定の編集」ウィンドウで、以下のいずれかのオプションを選択します。
  - コンピューター上で構成されているすべての IP アドレスをインスタンスに listen させる場合は、「すべての構成済み IP アドレスを listen する」を選択します。
  - コンピューター上で構成された特定の IP アドレス・セットをインスタンスに listen させる場合は、以下の手順を実行します。
    - a. 「すべての構成済み IP アドレスを listen する」をクリアします。
    - b. 「listen する特定の IP アドレスの選択」リストから、インスタンスが listen する IP アドレスを選択します。
5. 「次へ」をクリックします。
6. 「ポートの詳細」パネルで、以下の値を指定します。

注: ディレクトリー・サーバーのポートには、コンピューターで使用されている既存のポートと競合しない固有のポート番号を割り当てる必要があります。AIX、Linux、および Solaris の各システムでは、1 から 1000 の範囲のポート番号を root のみが使用できます。

- a. 「サーバー・ポート」フィールドに、サーバーが非セキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - b. 「サーバーのセキュア・ポート」フィールドに、サーバーがセキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - c. 「管理サーバー・ポート」フィールドに、管理サーバーが非セキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - d. 「管理サーバー・セキュア・ポート」フィールドに、管理サーバーがセキュア・ポートとして使用するポート番号を入力します。この数は、1 から 65535 の範囲でなければなりません。
  - e. 「完了」をクリックします。
7. 「TCP/IP 結果の編集」ウィンドウで、TCP/IP 設定編集操作に関して生成されたログ・メッセージを確認します。
  8. 「TCP/IP 結果の編集」ウィンドウを閉じるには、「閉じる」をクリックします。
  9. インスタンス管理ツールを閉じるには、「閉じる」をクリックします。

## コマンド行ユーティリティーを使用したインスタンスの TCP/IP 設定の変更

**idssethost** および **idssetport** コマンドを使用して、既存のインスタンスの TCP/IP 設定とポート設定を変更します。

### 始める前に

コマンド行ユーティリティーを使用してインスタンスの TCP/IP 設定を変更するには、以下の条件を満たしている必要があります。

1. コマンド行ユーティリティと同じバージョンのインスタンスが存在している必要があります。
2. インスタンスのディレクトリー・サーバーと管理サーバーを停止する必要があります。177 ページの『コマンド行ユーティリティを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. AIX、Linux、または Solaris では root ユーザーとしてログインし、Windows では管理者メンバーとしてログインします。
2. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の sbin サブディレクトリーに変更します。
3. ディレクトリー・サーバー *instance\_name* の IP アドレスを更新するには、以下のいずれかのオプションを選択します。 *instance\_name* 変数はインスタンス名で置き換えてください。

バインドする IP アドレス	実行するコマンド:
コンピューター上の特定の IP アドレス xx.xx.xx.xx	<code>idssethost -I instance_name -i xx.xx.xx.xx</code>
コンピューター上で構成されているすべての IP アドレス	<code>idssethost -I instance_name -i all</code>

4. ディレクトリー・サーバー *instance\_name* のポート番号を更新するには、以下のコマンドを実行します。 *instance\_name* 変数はインスタンス名で置き換えてください。

注: ディレクトリー・サーバーのポートには、コンピューターで使用されている既存のポートと競合しない固有のポート番号を割り当てる必要があります。

AIX、Linux、および Solaris の各システムでは、1 から 1000 の範囲のポート番号を root のみが使用できます。

構成するポート	実行するコマンド:
サーバー・ポート	<code>idssetport -I instance_name -p port_no</code>
サーバーのセキュア・ポート	<code>idssetport -I instance_name -s secure_port</code>
管理サーバー・ポート	<code>idssetport -I instance_name -a adm_port</code>
管理サーバー・セキュア・ポート	<code>idssetport -I instance_name -c adm_secure_port</code>

**idssethost** および **idssetport** コマンドについて詳しくは、「*Command Reference*」を参照してください。

5. ディレクトリー・サーバーおよび管理サーバーを始動します。177 ページの『コマンド行ユーティリティを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## インスタンスに関する情報の表示

インスタンスのホーム・ディレクトリー、IP アドレス、ポートなどのインスタンスの詳細を表示するために、インスタンス管理ツールまたはコマンド行ユーティリティーを使用することができます。

コンピューター上の既存のすべてのインスタンスに関する情報を表示することができます。インスタンスの状況は、「停止」状態または「始動」状態です。

**idsilist** コマンドによっても、コンピューター上の 1 つのインスタンスまたは使用可能なすべてのインスタンスについての同様の情報が提供されます。**idsilist** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## インスタンス管理ツールを使用したインスタンスに関する情報の表示

インスタンス管理ツールを使用して、既存のインスタンスの詳細を表示します。

### 手順

1. インスタンス管理ツールの始動 146 ページの『インスタンス管理ツールの始動』を参照してください。
2. 「システムにインストールされている **Directory Server** インスタンスのリスト」というリストから、詳細を表示するインスタンスを選択します。
3. 「表示」をクリックします。選択したインスタンスに関する一般情報と TCP/IP の詳細が示された「インスタンスの詳細の表示」ウィンドウが表示されます。
4. 「インスタンスの詳細の表示」ウィンドウを閉じるには、「閉じる」をクリックします。
5. インスタンス管理ツールを閉じるには、「閉じる」をクリックします。

## コマンド行ユーティリティーを使用したインスタンスに関する情報の表示

**idsilist** コマンドを使用して、既存のインスタンスに関する情報を表示します。

### 手順

1. AIX、Linux、または Solaris では root ユーザーとしてログインし、Windows では管理者メンバーとしてログインします。
2. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の **sbin** サブディレクトリーに変更します。
3. コンピューター上のインスタンスに関する情報を表示するには、適切な **idsilist** コマンドを実行します。

完了するタスク	実行するコマンド:
すべてのインスタンスをリストする	<code>idsilist</code>
すべてのインスタンスをすべての情報と説明付きでリストする	<code>idsilist -a</code>
すべてのインスタンスを未加工フォーマットのすべての情報付きでリストする	<code>idsilist -r</code>

完了するタスク	実行するコマンド:
特定のインスタンスをリストする	<code>idsilist -I instance_name</code>
特定のインスタンスをすべての情報と説明付きでリストする	<code>idsilist -I instance_name -a</code>
特定のインスタンスを未加工フォーマットのすべての情報付きでリストする	<code>idsilist -I instance_name -r</code>

**idsilist** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## ディレクトリー・サーバー・インスタンスの削除

インスタンス管理ツールまたはコマンド行ユーティリティーを使用して、ディレクトリー・サーバー・インスタンスやプロキシ・サーバー・インスタンスを削除することができます。

インスタンスを別のコンピューターに移行したか、インスタンスが不要になったときに、インスタンスをコンピューターから削除したい場合があります。

DB2 データベースを使用するディレクトリー・サーバーを削除する場合、インスタンスを削除する前にバックアップを取っておくことをお勧めします。プロキシ・サーバー・インスタンスを削除する場合、インスタンスのバックアップを取っておくことをお勧めします。

**注:** プロキシ・サーバー・インスタンスの場合、インスタンスの削除のみが有効なオプションです。

インスタンス管理ツールでは、以下のオプションを選択できます。

- ディレクトリー・サーバー・インスタンスを削除し、データベース・インスタンスを保持する
- ディレクトリー・サーバー・インスタンスを削除し、関連付けられた DB2 データベース・インスタンスを除去する

**idsidrop** コマンドでは、以下のオプションを選択できます。

- ディレクトリー・サーバー・インスタンスを削除し、データベース・インスタンスを保持する
- ディレクトリー・サーバー・インスタンスを削除し、関連付けられた DB2 データベース・インスタンスを除去する
- DB2 データベース・インスタンスからディレクトリー・サーバー・インスタンスを構成解除し、ディレクトリー・サーバー・インスタンスを削除しない

**idsidrop** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## インスタンス管理ツールを使用したインスタンスの削除

インスタンス管理ツールを使用して、ディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスを削除します。

## 始める前に

インスタンス管理ツールを使用してインスタンスの TCP/IP 設定を変更するには、以下の条件を満たしている必要があります。

1. インスタンス管理ツールと同じバージョンのインスタンスが存在している必要があります。
2. インスタンスのディレクトリー・サーバーと管理サーバーを停止する必要があります。176 ページの『ディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. インスタンス管理ツールの始動 146 ページの『インスタンス管理ツールの始動』を参照してください。
2. 「コンピューターにインストールされている **Directory Server** インスタンスのリスト」リストから、インスタンス管理ツールと同じバージョンのインスタンスを選択します。
3. 削除操作を開始するには、「**削除**」をクリックします。
4. 「**Directory Server インスタンスの削除**」ウィンドウで、以下の手順を実行します。
  - a. 以下の削除方法のいずれかを選択します。
    - 関連する DB2 データベース・インスタンスを削除せずにディレクトリー・サーバー・インスタンスを削除するには、「**Directory Server インスタンスのみの削除**」をクリックします。

注: プロキシ・サーバー・インスタンスの場合は、「**Directory Server インスタンスのみの削除**」が唯一の有効なオプションとなります。
    - ディレクトリー・サーバー・インスタンスを関連する DB2 データベース・インスタンスと共に削除するには、「**Directory Server インスタンスの削除と、関連するデータベース・インスタンスの破棄**」をクリックします。
  - b. 「**削除**」をクリックします。
  - c. 「警告」ウィンドウで「はい」をクリックして、インスタンス削除を確認します。
  - d. 「情報」ウィンドウで「OK」をクリックします。
  - e. 「**Directory Server インスタンスの削除**」ウィンドウを閉じるには、「閉じる」をクリックします。
  - f. インスタンス管理ツールを閉じるには、「閉じる」をクリックします。

## コマンド行ユーティリティーを使用したインスタンスの削除

`idsidrop` コマンドを使用して、既存のインスタンスを削除します。

## 始める前に

コマンド行ユーティリティーを使用してインスタンスを削除するには、以下の条件を満たしている必要があります。

1. コマンド行ユーティリティーと同じバージョンのインスタンスが存在している必要があります。
2. インスタンスのディレクトリー・サーバーと管理サーバーを停止する必要があります。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. AIX、Linux、または Solaris では root ユーザーとしてログインし、Windows では管理者メンバーとしてログインします。
2. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の sbin サブディレクトリーに変更します。
3. インスタンス *instance\_name* を削除するには、以下のいずれかのオプションを選択します。 *instance\_name* 変数はインスタンス名で置き換えてください。

完了するタスク	実行するコマンド:
ディレクトリー・サーバー・インスタンスを削除し、関連するデータベース・インスタンスを保持する。	<code>idsidrop -I instance_name</code>
ディレクトリー・サーバー・インスタンスを削除し、関連するデータベース・インスタンスを削除する。	<code>idsidrop -I instance_name -r</code>
ディレクトリー・サーバー・インスタンスを削除せずに、関連するデータベース・インスタンスを構成解除する。	<code>idsidrop -I instance_name -R</code>

**idsidrop** コマンドについて詳しくは、「*Command Reference*」を参照してください。



---

## 第 19 章 ディレクトリー構造の検証

IBM Security Directory Server をインストールした後でディレクトリー構造を検証する必要があります。

### Windows 32 ビットおよび 64 ビット・システム

IBM Security Directory Server を Windows オペレーティング・システムにインストールした後、インストール・ロケーション (C:\Program Files\IBM\LDAP\6.3.1 など) で以下のディレクトリーおよびファイルを確認できます (インストール・ロケーションは変更できます)。

```
appsrv
etc
java
lib
messages
bin
examples
javalib
lib64
nls
var
codeset
idstools
jre
license
properties
config
include
ldapcfg.ico
logs
sbin
```

### Linux 64 ビット・システム

IBM Security Directory Server を Linux オペレーティング・システムにインストールした後、インストール・ロケーション (/opt/ibm/ldap/6.3.1 など) で以下のディレクトリーおよびファイルを確認できます (インストール・ロケーションは変更できません)。

```
bin
codeset
config
etc
examples
idstools
```

include  
javalib  
LAPID  
lib  
lib64  
nls  
properties  
sbin  
tmp  
web

---

## 第 20 章 インスタンス構成

構成ツールまたはコマンド行ユーティリティーを使用して、要件に従ってディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスを構成することができます。

IBM Security Directory Server 構成ツール (**idsxcfg**) は、インスタンスを構成するために使用できる、グラフィカル・ユーザー・インターフェース (GUI) です。構成ツールを使用するには、IBM Java Development Kit が必要です。

構成ツールを開始するには、以下の資格情報を使用してログインする必要があります。

### AIX、Linux、または Solaris

- root ユーザー
- ディレクトリー・サーバー・インスタンス所有者
- ディレクトリー・サーバー・インスタンス所有者の 1 次グループ内にあるユーザー ID

### Windows

- デフォルトの管理者グループ内にあるユーザー ID

また、構成ツールを使用して、既存のディレクトリー・サーバー構成を変更することもできます。

フル・ディレクトリー・サーバー・インスタンス上での以下のタスクについて、構成ツールを使用できます。

- サーバーの始動または停止
- 1 次管理者 DN およびパスワードの管理
- ディレクトリー・サーバー・インスタンスの DB2 データベースの構成および構成解除
- インスタンスに関連付けられたデータベースの最適化
- DB2 索引の編成または DB2 の行の圧縮による DB2 データベースの保守
- データベースのバックアップおよび復元
- ディレクトリー・サーバー・インスタンスのパフォーマンス調整
- 変更ログの使用可能化と使用不能化
- サフィックスの追加または削除
- スキーマ・ファイルの追加または削除
- LDIF データのインポートまたはエクスポート
- Active Directory との同期の構成

プロキシ・サーバー・インスタンス上での以下のタスクについて、構成ツールを使用できます。

- サーバーの始動または停止

- 1 次管理者 DN およびパスワードの管理
- サフィックスの追加または削除
- スキーマ・ファイルの追加または削除
- インスタンスのバックアップおよび復元

---

## 構成ツールの開始

インスタンスに対して IBM Security Directory Server の構成ツールを開始して、ディレクトリー環境の要件に応じてインスタンスを構成します。

### 始める前に

構成ツールを使用してインスタンスを管理するには、以下の条件を満たしている必要があります。

- 構成ツールと同じバージョンのインスタンスが存在している必要があります。インスタンスが存在しない場合は、インスタンスを作成してください。151 ページの『カスタム設定を使用したディレクトリー・サーバー・インスタンスの作成』または 160 ページの『カスタム設定を使用したプロキシ・サーバー・インスタンスの作成』を参照してください。
- IBM Security Directory Server のインストール・パスに、IBM Java Development Kit が存在している必要があります。デフォルトの IBM Security Directory Server のインストール・パスについては、30 ページの『デフォルトのインストール・ロケーション』を参照してください。

### 手順

1. 必要なアクセス権でコンピューターにログインします。189 ページの『第 20 章 インスタンス構成』を参照してください。
2. コマンド・プロンプトを開きます。
3. 現在のディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
4. 以下の形式で `idsxcfg` コマンドを実行します。 `instance_name` 変数はインスタンス名で置き換えてください。

```
idsxcfg -I instance_name
```

指定したインスタンスに対して IBM Security Directory Server の構成ツール・ウィンドウが開きます。

5. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
6. 構成ツールの確認ウィンドウで、「はい」をクリックします。

---

## 構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止

構成ツールを使用して、インスタンスに関連付けられた管理サーバーや `ibmslapd` プロセスを開始することができます。

ディレクトリー・サーバーの構成を変更した場合は、変更内容を適用するために、サーバーおよび管理サーバーを停止して再始動することが必要な場合があります。ディレクトリー・サーバーおよび管理サーバーを停止できるのは、これが通常モードまたは構成モードで稼働中の場合に限られます。

構成ツールまたは **ibmslapd** や **ibmdiradm** などのサーバー・ユーティリティーを使用して、サーバーおよび管理サーバーを始動および停止することができます。**ibmslapd** プロセスは、ディレクトリー・サーバーに関連付けられています。ディレクトリー・サーバー・インスタンスは、構成ツールを使用して、通常モードでのみ始動できます。ディレクトリー・サーバーを構成専用モードで始動するには、コマンド行オプションを使用してください。

ディレクトリー・サーバーは、以下のいずれかの状態になります。

- 始動
- 停止
- 始動 (構成専用)

管理サーバーは、以下のいずれかの状態になります。

- 始動
- 停止

## 構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止

構成ツールを使用して、インスタンスに関連付けられたディレクトリー・サーバー、管理サーバー、またはその両方の始動または停止を行います。

### 手順

1. インスタンス用の構成ツールを開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「サーバー状態の管理」をクリックします。
3. 「現在の状態」ページで、サーバーおよび管理サーバーの現在の状態を確認します。
4. 「現在の状態」ページで、以下のアクションを実行します。
  - インスタンスのディレクトリー・サーバー、管理サーバー、またはその両方を始動する場合は、以下の手順を実行します。
    - ディレクトリー・サーバーを始動するには、「サーバーの始動」をクリックします。
    - 管理サーバーを始動するには、「管理サーバーの始動」をクリックします。
    - 「情報」ウィンドウで「OK」をクリックします。
  - ディレクトリー・サーバー、管理サーバー、またはその両方を停止する場合は、以下の手順を実行します。
    - ディレクトリー・サーバーを停止するには、「サーバーの停止」をクリックします。

- 管理サーバーを停止するには、「管理サーバーの停止」をクリックします。
  - 「情報」ウィンドウで「OK」をクリックします。
5. 「現在の状態」ページを閉じるには、「閉じる」をクリックします。
  6. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
  7. 構成ツールの確認ウィンドウで、「はい」をクリックします。

## コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止

コマンド行ユーティリティーを使用して、インスタンスに関連付けられているディレクトリー・サーバー、管理サーバー、または両方を始動または停止します。

### 始める前に

インスタンスのディレクトリー・サーバーと管理サーバーを始動または停止するには、以下の条件を満たしている必要があります。

- コマンド行ユーティリティーと同じバージョンのインスタンスが存在している必要があります。インスタンスが存在しない場合は、インスタンスを作成してください。149 ページの『デフォルトのディレクトリー・サーバー・インスタンスの作成』または 151 ページの『カスタム設定を使用したディレクトリー・サーバー・インスタンスの作成』を参照してください。

### 手順

1. 必要なアクセス権でコンピューターにログインします。189 ページの『第 20 章 インスタンス構成』を参照してください。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
4. インスタンス `instance_name` のサーバーと管理サーバーを始動するには、次のコマンドを実行します。 `instance_name` の値をご使用のインスタンス名で置換します。

```
ibmslapd -I instance_name
ibmdiradm -I instance_name
```

5. インスタンスのサーバーと管理サーバーを停止するには、次のコマンドを実行します。 `instance_name` の値をご使用のインスタンス名で置換します。

```
ibmslapd -I instance_name -k
ibmdiradm -I instance_name -k
```

---

## インスタンスの 1 次管理者 DN の管理

インスタンスの構成データおよびすべてのディレクトリー・データにアクセスするには、インスタンスの 1 次管理者識別名 (DN) を作成して構成する必要があります。

管理者 DN は、インスタンスの 1 次管理者が使用する DN です。1 つのインスタンスについて 1 つの 1 次管理者のみ作成できます。

デフォルトの DN は cn=root です。DN 値には大/小文字の区別はありません。

DN には attribute:value のペアが含まれており、コンマで区切られています。DN 値の例を以下に示します。

```
cn=Ben Gray,ou=dept_audit,o=sample
```

構成ツールまたはコマンド行ユーティリティー **idsdnpw** を使用して、1 次管理者 DN を設定または変更することができます。1 次管理者 DN を設定または変更するには、インスタンスに関連付けられている **ibmslapd** プロセスを停止する必要があります。

## 構成ツールを使用した 1 次管理者 DN の管理

構成ツールを使用して、インスタンスの 1 次管理者 DN を構成します。

### 始める前に

インスタンスの 1 次管理者 DN を構成するには、以下の要件を満たしている必要があります。

- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用した ディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### 手順

1. インスタンス用の構成ツール を開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「**管理者 DN の管理**」をクリックします。
3. 「**管理者 DN**」フィールドに 1 次管理者の DN を入力するか、デフォルト DN の cn=root をそのまま使用します。
4. 「**OK**」をクリックします。
5. アクションを確認するには、「**OK**」をクリックします。
6. 構成ツール ウィンドウを閉じるには、「**ファイル**」 > 「**終了**」をクリックしてください。
7. アクションを確認するには、「**はい**」をクリックします。

### 次のタスク

ディレクトリー・サーバーを始動します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## コマンド行ユーティリティーを使用した 1 次管理者 DN の管理

コマンド行ユーティリティー **idsdnpw** を使用して、インスタンスの 1 次管理者 DN を管理します。

## 始める前に

インスタンスの 1 次管理者 DN を構成するには、以下の要件を満たしている必要があります。

- ディレクトリー・サーバーを停止します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## このタスクについて

管理者 DN の値を指定しない場合は、ディレクトリー・サーバー・インスタンスの `ibmslapd.conf` ファイルにデフォルト値 `cn=root` が設定されます。インスタンスの 1 次管理者パスワードは指定する必要があります。

パスワードを指定しないと、`idsdnpw` コマンドからパスワードを要求するプロンプトが出されます。パスワードを入力するときに、コマンド・プロンプトでパスワードが表示されることはありません。

## 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
4. インスタンスの管理者 DN を設定するには、以下のコマンドを実行します。  
`instance_name`、`adminDN`、および `adminPWD` の値を、要件に従って置き換えてください。

```
idsdnpw -I instance_name -u adminDN -p adminPWD
```

`idsdnpw` コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 次のタスク

ディレクトリー・サーバーを始動します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

---

## インスタンスの 1 次管理者パスワードの管理

インスタンスに対して認証を行い、構成データおよびすべてのディレクトリー・データにアクセスするには、インスタンスの 1 次管理者パスワードを作成して構成する必要があります。

管理者パスワードでは大文字と小文字が区別されます。2 バイト文字セット (DBCS) の文字はサポートされていないため、パスワードには使用できません。今後の参照用に、管理者パスワードを保存しておく必要があります。

構成ツールまたはコマンド行ユーティリティー `idsdnpw` を使用して、1 次管理者パスワードを構成することができます。管理者パスワードを構成するには、インスタンスに関連付けられている `ibmslapd` プロセスを停止する必要があります。

管理パスワード・ポリシーを使用可能にしている場合、1 次管理者のパスワードは、管理パスワード・ポリシーの要件に従っている必要があります。パスワード・ポリシーについては、IBM Security Directory Server 資料の『管理』セクションを参照してください。

## 構成ツールを使用した 1 次管理者パスワードの管理

構成ツールを使用して、インスタンスの 1 次管理者のパスワードを構成します。

### 始める前に

インスタンスの 1 次管理者 DN のパスワードを構成するには、以下の要件を満たしている必要があります。

- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用した ディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### 手順

1. インスタンス用の構成ツール を開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「管理者パスワードの管理」 をクリックします。
3. 「管理者パスワード」フィールドに、1 次管理者のパスワードを入力します。
4. 「確認パスワード」フィールドに、1 次管理者のパスワードを入力します。
5. 「OK」をクリックします。
6. アクションを確認するには、「OK」をクリックします。
7. 「管理者パスワードの管理」ページを閉じるには、「OK」をクリックします。
8. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
9. アクションを確認するには、「はい」をクリックします。

### 次のタスク

ディレクトリー・サーバーを始動します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## コマンド行ユーティリティーを使用した 1 次管理者パスワードの管理

コマンド行ユーティリティー `idsdnpw` を使用して、インスタンスの 1 次管理者パスワードを管理します。

### 始める前に

インスタンスの 1 次管理者パスワードを構成するには、以下の要件を満たしている必要があります。

- ディレクトリー・サーバーを停止します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ローション内の `sbin` サブディレクトリーに変更します。
4. インスタンスの管理者パスワードを設定するには、以下のコマンドを実行します。 `instance_name`、`adminDN`、および `adminPWD` の値を、要件に従って置き換えてください。

```
idsdnpw -I instance_name -u adminDN -p adminPWD
```

**idsdnpw** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 次のタスク

ディレクトリー・サーバーを始動します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

---

## ディレクトリー・サーバー・インスタンスのデータベース構成

インスタンスをディレクトリー・サーバーとして使用して、ディレクトリー・データを保管するには、インスタンス用の DB2 データベースを構成する必要があります。

インスタンス管理ツール、構成ツール、または **idscfgdb** コマンドを使用して、DB2 データベースを作成および構成できます。ディレクトリー・サーバーは、データベースを構成または構成解除する前に停止する必要があります。**idscfgdb** コマンドについて詳しくは、「*Command Reference*」を参照してください。

インスタンス管理ツールを使用してデフォルト・インスタンスを作成するを選択した場合、そのインスタンスについての DB2 データベース・インスタンスも作成および構成されます。プロキシ・サーバー・インスタンスの場合、DB2 データベースの構成は不要です。

インスタンスについての DB2 データベースを構成すると、インスタンスの構成ファイルは DB2 データベース情報を使用して更新されます。ツールによって、データベースおよびローカル・ループバック設定も作成されます。

データベースおよびローカル・ループバックの設定が存在しない場合は、それらが作成されます。データベースをローカル・コード・ページ・データベースとして作成するのか、それとも UTF-8 データベースとして作成するのかを指定できます。DB2 データベースの作成に使用されるデフォルト・コード・ページは UTF-8 です。

## 構成ツールを使用したインスタンスのデータベースの構成

構成ツールを使用して、ディレクトリー・サーバー・インスタンスの DB2 データベースを構成します。

### 始める前に

ディレクトリー・サーバー・インスタンスの DB2 データベースを構成するには、以下のタスクを実行する必要があります。

- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。
- DB2 データベース・インスタンスを所有するには、システム・ユーザー ID が存在している必要があります。システム・ユーザー ID の要件について詳しくは、133 ページの『ディレクトリー・サーバー・インスタンスに関連付けられたユーザーとグループ』を参照してください。

### 手順

1. インスタンス用の構成ツールを開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「データベース・タスク」 > 「データベースの構成」をクリックします。
3. 「データベースの構成」ページで、以下のオプションのいずれかを選択します。
  - インスタンスのデータベースを構成するには、以下の手順を実行します。
    - a. 「データベース・ユーザー名」フィールドに、データベースを所有するシステム・ユーザー ID を入力します。ディレクトリー・サーバー・インスタンスは、このシステム・ユーザーを使用してデータベースに接続します。
    - b. 「パスワード」フィールドに、データベース管理者のパスワードを入力します。
    - c. 「データベース名」フィールドに、データベース名を入力します。
    - d. 以下の DB2 構成設定を設定する場合は、「拡張テーブル・スペース・オプションの表示」を選択します。
      - データベースで DB2 テーブル・スペースにシステム管理ストレージ (SMS) データ・ストレージを使用する場合。SMS が使用される場合は、オペレーティング・システムのファイル・システム・マネージャーによって、DB2 テーブルを保管するテーブル・スペースの割り振りと管理が行われます。
      - データベースで DB2 テーブル・スペースにデータベース管理ストレージ (DMS) データ・ストレージを使用し、さらに USERSPACE1 テーブル・スペースと LDAPSPACE テーブル・スペース、サイズ、およびロケーションを指定してデータベースを構成する場合。DMS が使用される場合には、テーブル・スペースはデータベース・マネージャーによって管理されます。データベース管理者が、使用するデバイスおよびファイルを決めると、DB2 がこれらのデバイスとファイルでスペースを管理します。

「**拡張テーブル・スペース・オプションの表示**」を選択しない場合は、デフォルトのサイズとロケーションの `USERSPACE1` および `LDAPSPACE` テーブル・スペースを使用する `DB2` データベースが、`DMS` を使用して作成されます。既存のデータベースを使用するインスタンスを構成する場合は、「**データベース名**」フィールドに既存のデータベースの名前を入力すると、「**拡張テーブル・スペース・オプションの表示**」が使用不可になります。

- e. 「**次へ**」をクリックします。
- データベース管理者パスワードを再度構成するには、以下の手順を実行します。
  - a. 「**パスワードのリセット**」をクリックします。
  - b. 「**パスワード**」フィールドに、データベース管理者のパスワードを入力します。
  - c. 「**確認パスワード**」フィールドに、データベース管理者のパスワードを入力します。
  - d. 「**次へ**」をクリックします。
- 4. `DB2` データベースを作成および構成する場合は、以下の手順を実行します。
  - a. 「**データベースのインストール・ロケーション**」フィールドに、データベース・ロケーション・パスを入力します。「**参照**」をクリックして、ディレクトリを指定します。Windows では、ディスク・ドライブのロケーション (`C:` など) を指定する必要があります。AIX、Linux、および Solaris では、ロケーションが `/home/ldapdb` などのディレクトリ名でなければなりません。

**注:** `DMS` データベースに必要な最小のディスク・スペースは `1 GB` です。`SMS` データベースの場合は、最小で `150 MB` のディスク・スペースが必要です。これらの要件は、空のデータベースの場合です。データベースにデータを保管すると、さらにディスク・スペースが必要になってきます。

- b. ディレクトリー・サーバーでデータベースのオンライン・バックアップを構成するには、以下の手順を実行します。
  - 1) 「**オンライン・バックアップの構成**」を選択します。
  - 2) 「**データベースのバックアップ・ロケーション**」フィールドに、バックアップ・イメージを保管するロケーションを入力します。「**参照**」をクリックすると、ロケーションを指定できます。

**注:** バックアップ操作の実行中に構成ツールを終了したり、操作をキャンセルしたりしないでください。

データベースの構成が完了した後にデータベースのオンライン・バックアップを構成すると、データベースのオフライン・バックアップが実行されます。オフライン・バックアップ操作が完了すると、管理サーバーが再始動します。`idscfgdb` コマンドを使用して、ディレクトリー・サーバー・インスタンスでのオンライン・バックアップを構成することもできます。ただし、`idscfgdb` コマンドに `-c` パラメーターを指定してオンライン・バックアップを構成解除することはできません。インスタンス管理ツールまたは構成ツ

ールを使用してインスタンスでのオンライン・バックアップを構成した場合は、構成ツールまたは **idscfgdb** コマンドを使用してその構成を解除できません。

- c. 「**文字セット・オプション**」領域で、以下のいずれかのオプションを選択してデータベース・タイプを作成します。

注: データを複数の言語でディレクトリー・サーバーに保管する場合は、ユニバーサル DB2 データベースを作成します。ユニバーサル DB2 データベースはデータ変換が少ないため、最も効率的でもあります。言語タグを使用する場合は、データベースが UTF-8 データベースである必要があります。UTF-8 の詳細については、138 ページの『UTF-8 サポート』を参照してください。

- LDAP クライアントが UTF-8 文字データを保管できる UCS Transformation Format (UTF-8) データベースを作成する場合は、「**ユニバーサル DB2 データベースの作成**」をクリックします。
- ローカル・コード・ページでデータベースを作成する場合は、「**ローカル・コード・ページ DB2 データベースの作成**」をクリックします。

- d. 「**次へ**」をクリックします。

5. 「**拡張テーブル・スペース・オプションの表示**」を選択した場合は、以下の手順を実行する必要があります。

- a. 「**データベース・テーブル・スペース・タイプの選択**」リストから、データベース・タイプを選択します。DMS データベースのテーブル・スペース・タイプがデフォルトです。SMS データベースのテーブル・スペース・タイプを選択すると、他のすべてのフィールドが使用不可になります。DMS テーブル・スペース・サポートは、USERSPACE1 および LDAPSPACE テーブル・スペースに対してのみ使用されます。その他すべてのテーブル・スペース(カタログ・テーブル・スペース、一時テーブル・スペースなど)のタイプは SMS です。

- a. 「**USERSPACE1 テーブル・スペースの詳細**」領域で、以下の詳細を指定します。

- 1) 「**テーブル・スペース・コンテナ**」リストから、コンテナ・タイプを選択します。USERSPACE1 テーブル・スペースのロケーションをファイル・システムにする場合は、「**ファイル**」を選択します。データベース・テーブル・スペース・コンテナのロケーションがファイル・システム内にある場合、DMS クックド・テーブル・スペースが作成されます。テーブル・スペースの初期サイズおよび拡張可能な単位のサイズを指定すると、テーブル・スペースを必要に応じて自動的に拡張することができます。USERSPACE1 テーブル・スペースをロー・デバイスに作成する場合は、「**ロー・デバイス**」を選択します。ロー・デバイスとは、ファイル・システムがインストールされていないデバイスのこと(ファイル・システムが含まれていないハード・ディスクなど)。データベース・テーブル・スペース・コンテナのロケーションがロー・デバイス内にある場合、DMS ロー・テーブル・スペースが作成されます。この場合、データベース・テーブル・スペース・コンテナのサイズは固定され、拡張できません。「**ロー・デバイス**」を選択する場合は、デフォルト値を受け入れる代わりに、コンテナ・ロケーションと併せてサイズを指定してください。

- 2) 「**テーブル・スペース・コンテナ**」リストで「**ファイル**」を選択した場合は、以下の詳細を指定します。
  - a) 「**ディレクトリー・パス**」フィールドで、USERSPACE1 テーブル・スペースを作成するディレクトリー・パスを指定します。「**参照**」をクリックすると、ディレクトリーを選択できます。
  - b) 「**ファイル名**」フィールドで、作成するテーブル・スペースのファイル名を入力するか、デフォルトのファイル名 (USPACE) を受け入れます。
  - c) 「**初期サイズ**」フィールドで、USERSPACE1 テーブル・スペースの初期サイズ (ページ数) を入力するか、デフォルト値を受け入れます。**ファイル・タイプ**の**テーブル・スペース・コンテナ**の場合、USERSPACE1 テーブル・スペース・コンテナは自動増分タイプです。「**初期サイズ**」フィールドに初期サイズを指定し、「**拡張可能サイズ**」フィールドに拡張可能な単位のサイズを指定できます。初期サイズのデフォルト値は 16 K ページ、デフォルトの拡張可能な単位サイズは 8 K ページです。USERSPACE1 テーブル・スペース・コンテナの**ページ・サイズ**は、1 ページあたり 4 KB です。
- 3) 「**テーブル・スペース・コンテナ**」リストで「**ロー・デバイス**」を選択した場合は、以下の詳細を指定します。
  - a) 「**デバイス・パス**」フィールドに、ロー・デバイスのロケーションを入力します。Windows では、パスが ¥¥.¥ で始まっている必要があります。例えば、デバイス名を含むパスの場合は ¥¥.¥device\_name となります。AIX、Linux、および Solaris では、デバイス・パスが有効なパスでなければなりません。
  - b) 「**初期サイズ**」フィールドで、USERSPACE1 テーブル・スペースの初期サイズを入力するか、デフォルト値を受け入れます。**ロー・デバイス・タイプ**の**テーブル・スペース・コンテナ**の場合、USERSPACE1 テーブル・スペース・コンテナの**サイズ**は固定です。デフォルトの**サイズ**は 16 K ページです。よりよい結果が得られるように、必要な**サイズ**を指定してください。
- b. 「**LDAPSPACE テーブル・スペースの詳細**」領域で、以下の詳細を指定します。
  - 1) 「**テーブル・スペース・コンテナ**」リストから、**コンテナ・タイプ**を選択します。LDAPSPACE テーブル・スペースのロケーションを**ファイル・システム**にする場合は、「**ファイル**」を選択します。LDAPSPACE テーブル・スペースを**ロー・デバイス**に作成する場合は、「**ロー・デバイス**」を選択します。ロー・デバイスとは、**ファイル・システム**がインストールされていない**デバイス**のことです (**ファイル・システム**が含まれていない**ハード・ディスク**など)。
  - 2) 「**テーブル・スペース・コンテナ**」リストで「**ファイル**」を選択した場合は、以下の詳細を指定します。
    - a) 「**ディレクトリー・パス**」フィールドで、LDAPSPACE テーブル・スペースを作成するディレクトリー・パスを指定します。「**参照**」をクリックすると、ディレクトリーを選択できます。

- b) 「**ファイル名**」フィールドで、作成するテーブル・スペースのファイル名を入力するか、デフォルトのファイル名 (ldapSPACE) を受け入れます。
  - c) 「**初期サイズ**」フィールドで、LDAPSPACE テーブル・スペースの初期サイズ (ページ数) を入力するか、デフォルト値を受け入れます。ファイル・タイプのテーブル・スペース・コンテナーの場合、LDAPSPACE テーブル・スペース・コンテナーは自動増分タイプです。「**初期サイズ**」フィールドに初期サイズを指定し、「**拡張可能サイズ**」フィールドに拡張可能な単位のサイズを指定できます。初期サイズのデフォルト値は 16 K ページ、デフォルトの拡張可能な単位サイズは 8 K ページです。LDAPSPACE テーブル・スペース・コンテナーのページ・サイズは、1 ページあたり 32 KB です。
- 3) 「**テーブル・スペース・コンテナー**」リストで「**ロー・デバイス**」を選択した場合は、以下の詳細を指定します。
    - a) 「**デバイス・パス**」フィールドに、ロー・デバイスのロケーションを入力します。Windows では、パスが ¥¥.¥ で始まっている必要があります。例えば、デバイス名を含むパスの場合は ¥¥.¥device\_name となります。AIX、Linux、および Solaris では、デバイス・パスが有効なパスでなければなりません。
    - b) 「**初期サイズ**」フィールドで、LDAPSPACE テーブル・スペースの初期サイズを入力するか、デフォルト値を受け入れます。ロー・デバイス・タイプのテーブル・スペース・コンテナーの場合、LDAPSPACE テーブル・スペース・コンテナーのサイズは固定です。デフォルトのサイズは 16 K ページです。よりよい結果が得られるように、必要なサイズを指定してください。
    - c) 「**テーブル・スペース・コンテナー**」リストのいずれか、または両方で「**ファイル**」を選択した場合は、「**拡張可能サイズ**」フィールドでテーブル・スペース・コンテナーを拡張するページ数を指定します。
  6. 「**完了**」をクリックします。
  7. タスクの完了を受け入れるには、「**OK**」をクリックします。
  8. データベース構成操作に関して生成されたログを確認します。
  9. 「**データベースの構成**」ページを閉じるには、「**閉じる**」をクリックします。
  10. 構成ツール ウィンドウを閉じるには、「**ファイル**」 > 「**終了**」をクリックしてください。
  11. アクションを確認するには、「**はい**」をクリックします。

## 次のタスク

データベースを構成した後に、インスタンスに対して以下の構成を実行する必要があります。

- 1 次管理者 DN およびパスワードを構成します。193 ページの『構成ツールを使用した 1 次管理者 DN の管理』および 195 ページの『構成ツールを使用した 1 次管理者パスワードの管理』を参照してください。
- 必要なサフィックスを構成します。228 ページの『サフィックス構成』を参照してください。

## コマンド行ユーティリティーを使用したインスタンスのデータベースの構成

コマンド行ユーティリティー **idscfgdb** を使用して、ディレクトリー・サーバー・インスタンスの DB2 データベースを構成します。

### 始める前に

ディレクトリー・サーバー・インスタンスの DB2 データベースを構成するには、以下のタスクを実行する必要があります。

- データベースを構成するときに、**DB2COMM** 環境変数を設定しないでください。
- ディレクトリー・サーバーを停止します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。
- DB2 データベース・インスタンスを所有するには、システム・ユーザー ID が存在している必要があります。システム・ユーザー ID の要件について詳しくは、133 ページの『ディレクトリー・サーバー・インスタンスに関連付けられたユーザーとグループ』を参照してください。

### このタスクについて

**idscfgdb** コマンドを実行して、以下の操作を実行できます。

- データベースをディレクトリー・サーバー・インスタンスに作成して構成します。ローカル・ループバック設定が存在しない場合は作成されます。
- ディレクトリー・サーバー・インスタンスの **ibmslapd.conf** ファイルに、データベースに関する情報を追加します。

データベースを作成するときは、ローカル・コード・ページ・データベースとして作成するのか、それとも UTF-8 データベース (デフォルト) として作成するのかを指定できます。

### 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の **sbin** サブディレクトリーに変更します。
4. 次の値を使用してディレクトリー・サーバー・インスタンスの DB2 データベースを構成するには、以下のコマンドを実行します。
  - インスタンス名: **ldapdb**
  - データベース名: **ldapdb**
  - DB2 データベース管理者 ID: **ldapdb**
  - DB2 データベース管理者パスワード: **ldapdb123**
  - データベース・ロケーション: **/home/ldapdb**

```
idscfgdb -I ldapdb -a ldapdb -w ldapdb123 -t ldapdb  
-l /home/ldapdb
```

Windows では、データベース・ロケーションのディスク・ドライブ名を指定します。Solaris では、適切なデータベース・ロケーションを指定します。**idscfgdb** コマンドについて詳しくは、「*Command Reference*」を参照してください。このコマンドによって、デフォルト・サイズの DMS テーブル・スペースを使用するデータベースが構成されます。

## 例

**例 1:** ファイル・システム上にある特定サイズの DMS テーブル・スペースを使用するデータベースを構成するには、以下の値を指定して **idscfgdb** コマンドを実行します。

- インスタンス名: ldapdb
- データベース名: ldapdb
- DB2 データベース管理者 ID: dbadmin
- DB2 データベース管理者パスワード: ldapdb123
- データベース・ロケーション: c:%dblocation
- USERSPACE1 テーブル・スペースのロケーション:  
c:%dblocation%ldapinst%tablespace%loc%USPACE
- USERSPACE1 テーブル・スペースのコンテナ・サイズ: 10000 ページ
- 拡張サイズ: 16 ページ

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb  
-w ldapdb123 -n -l c:%dblocation  
-u c:%dblocation%ldapinst%tablespace%loc%USPACE -U 10000 -z 16
```

**例 2:** SMS テーブル・スペースを使用する同じデータベースを構成するには、以下の値を指定して **idscfgdb** コマンドを実行します。

- インスタンス名: ldapdb
- データベース名: ldapdb
- DB2 データベース管理者 ID: dbadmin
- DB2 データベース管理者パスワード: ldapdb123
- データベース・ロケーション: c:%dblocation

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb  
-w ldapdb123 -n -l c:%dblocation  
-m SMS
```

## 次のタスク

データベースを構成した後に、インスタンスに対して以下の構成を実行する必要があります。

- 1 次管理者 DN およびパスワードを構成します。193 ページの『コマンド行ユーティリティを使用した 1 次管理者 DN の管理』および 195 ページの『コマンド行ユーティリティを使用した 1 次管理者パスワードの管理』を参照してください。
- 必要なサフィックスを構成します。228 ページの『サフィックス構成』を参照してください。

---

## DB2 データベース管理者パスワードの管理

DB2 インスタンス所有者のシステム・パスワードを変更する場合は、このパスワードを使用して、ディレクトリー・サーバー・インスタンス構成ファイルを更新する必要があります。

インスタンスを使用して構成されるデータベースの DB2 インスタンス所有者について、システム・パスワードを変更する場合、パスワードはインスタンス構成ファイル内で更新されません。インスタンスの構成ファイル内のデータベース管理者パスワードが、データベースに関連付けられている DB2 インスタンス所有者のシステム・パスワードに一致しない場合、インスタンスは通常モードで開始されないことがあります。最新の DB2 インスタンス所有者パスワードを使用して、インスタンス構成ファイルを更新する必要があります。

構成ツール、`idscfgdb` コマンド、または `idsldapmodify` コマンドを使用して、DB2 データベース管理者パスワードを更新できます。

構成ツールまたは `idscfgdb` コマンドを使用してデータベース管理者パスワードを変更する場合、パスワードを変更する前にディレクトリー・サーバーを停止する必要があります。 `idsldapmodify` コマンドを使用してデータベース管理者パスワードを変更するには、ディレクトリー・サーバーを構成モードで始動する必要があります。 `idsldapmodify` コマンドは、プライマリー・ディレクトリー・サーバー管理者か、`dirdata` 役割を持つローカル管理者グループ・メンバーとして実行します。

`idscfgdb` および `idsldapmodify` コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 構成ツールを使用した DB2 データベース管理者パスワードの変更

構成ツールを使用して、ディレクトリー・サーバー・インスタンス構成ファイル内の DB2 データベース管理者パスワードを更新します。

### 始める前に

インスタンス構成ファイル内の DB2 データベース管理者パスワードを更新するには、以下のタスクを実行する必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。197 ページの『構成ツールを使用したインスタンスのデータベースの構成』を参照してください。
- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### このタスクについて

構成ツールによって、ディレクトリー・サーバー・インスタンス構成ファイル内の DB2 データベース管理者パスワードが更新されます。インスタンスに対して変更ログが構成されている場合は、構成ファイル内の変更ログ・データベース所有者のパスワードもツールによって更新されます。

## 手順

1. インスタンス用の構成ツール を開始します。 190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「データベース・タスク」 > 「データベースの構成」をクリックします。
3. 「データベースの構成」 ページで、以下の手順を実行します。
  - a. 「パスワードのリセット」を選択します。
  - b. 「パスワード」 フィールドに、データベース管理者のパスワードを入力します。
  - c. 「確認パスワード」 フィールドに、データベース管理者のパスワードを入力します。
  - d. 「次へ」をクリックします。
4. 「完了」をクリックします。
5. タスクの完了を受け入れるには、「OK」をクリックします。
6. データベース・パスワード構成操作に関して生成されたログを確認します。
7. 「データベースの構成」 ページを閉じるには、「閉じる」をクリックします。
8. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
9. アクションを確認するには、「はい」をクリックします。

## 次のタスク

ディレクトリー・サーバーを始動します。 191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## コマンド行ユーティリティーを使用した DB2 データベース管理者パスワードの変更

`idscfgdb` または `idsldapmodify` コマンド行ユーティリティーを使用して、ディレクトリー・サーバー・インスタンス構成ファイル内の DB2 データベース管理者パスワードを更新します。

### 始める前に

インスタンス構成ファイル内の DB2 データベース管理者パスワードを更新するには、以下のタスクを実行する必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。 202 ページの『コマンド行ユーティリティーを使用したインスタンスのデータベースの構成』を参照してください。

### このタスクについて

`idscfgdb` コマンドを実行して、インスタンス構成ファイル内の DB2 データベース管理者パスワードを更新することができます。`idscfgdb` コマンドを実行する前に、ディレクトリー・サーバーを停止する必要があります。

ディレクトリー・サーバー・インスタンスの実行時にパスワードを変更するには、**idsldapmodify** コマンドを使用することができます。**idsldapmodify** コマンドは、プライマリー・ディレクトリー・サーバー管理者か、`dirdata` 役割を持つローカル管理者グループ・メンバーとして実行します。

**idscfgdb** および **idsldapmodify** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. DB2 データベース管理者パスワードを変更するには、以下の方法のいずれかを選択します。
  - **idscfgdb** コマンドで DB2 データベース管理者パスワードを変更するには、以下の手順を実行します。
    - a. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
    - b. ディレクトリー・サーバーを停止します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。
    - c. 以下の形式で **idscfgdb** コマンドを実行します。

```
idscfgdb -I instance_name -w db2adminPWD
```
    - d. ディレクトリー・サーバーを始動します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。
  - **idsldapmodify** コマンドで DB2 データベース管理者パスワードを変更するには、以下の手順を実行します。
    - a. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `bin` サブディレクトリーに変更します。
    - b. 以下の形式で **idsldapmodify** コマンドを実行します。

```
idscfgdb -h IP_address -p port -D adminDN -w adminPWD -i file1.ldif
```

`file1.ldif` には、以下の項目が含まれています。

```
dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas,
   cn=Configuration
changetype: modify
replace: ibm-slapdDbUserPW
ibm-slapdDbUserPW: db2adminPWD
```
    - c. `directory server` を再始動します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

---

## ディレクトリー・サーバー・インスタンスからのデータベース構成解除

既存のディレクトリー・サーバー・インスタンスを別の DB2 データベースと一緒に使用するには、インスタンスから既存の DB2 データベースを構成解除する必要があります。

ディレクトリー・サーバー・インスタンスの場合は、データベースを構成解除できるのは、そのインスタンスに DB2 データベースが構成されている場合に限られます。

構成ツールまたは `idsucfgdb` コマンドを使用して、以下の操作を選択して実行できます。

- ディレクトリー・サーバー・インスタンスの構成ファイルから DB2 データベース情報を削除します。この操作では、ユーティリティーは DB2 データベースをインスタンスから構成解除し、DB2 データベースを削除しません。
- ディレクトリー・サーバー・インスタンスの構成ファイルから DB2 データベース情報を削除し、DB2 データベースを削除します。この操作では、DB2 データベースが削除され、すべてのデータが失われます。

ディレクトリー・サーバー・インスタンスから DB2 データベースを構成解除した後は、データベースはインスタンスにアクセスできません。

プロキシ・サーバー・インスタンスについては、データベースの構成解除操作はサポートされていません。

`idsucfgdb` コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 構成ツールを使用したインスタンスからの DB2 データベースの構成解除

構成ツールを使用して、ディレクトリー・サーバー・インスタンスから DB2 データベースを構成解除します。

### 始める前に

インスタンスから DB2 データベースを構成解除するには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。197 ページの『構成ツールを使用したインスタンスのデータベースの構成』を参照してください。
- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### 手順

1. インスタンス用の構成ツールを開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「データベース・タスク」 > 「データベースの構成解除」をクリックします。
3. 「データベースの構成解除」ページで、以下の手順を実行します。
  - a. 「オプション」エリアから、次のオプションの 1 つを選択します。
    - DB2 データベースを削除せずに、DB2 データベースをインスタンスから構成解除するには、「データベースの構成解除」をクリックします。

- DB2 データベースをインスタンスから構成解除し、DB2 データベースを削除するには、「データベースの構成解除と破棄」をクリックします。
- b. データベースがオンライン・バックアップ用に構成されている場合に、インスタンスのデータベース・バックアップ・コピーを削除するには、「データベースのバックアップ・コピーを除去」を選択します。
- c. 構成解除を開始するには、「構成解除」をクリックします。
- d. 確認ウィンドウで、「はい」をクリックします。
- 4. タスクの完了を受け入れるには、「OK」をクリックします。
- 5. データベース構成解除操作に対して生成されたログを確認します。
- 6. 「データベースの構成解除」ページを閉じるには、「キャンセル」をクリックします。
- 7. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
- 8. アクションを確認するには、「はい」をクリックします。

## コマンド行ユーティリティーを使用したインスタンスからの DB2 データベースの構成解除

コマンド行ユーティリティー **idsucfgdb** を使用して、ディレクトリー・サーバー・インスタンスから DB2 データベースを構成解除します。

### 始める前に

インスタンスから DB2 データベースを構成解除するには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。202 ページの『コマンド行ユーティリティーを使用したインスタンスのデータベースの構成』を参照してください。
- ディレクトリー・サーバーを停止します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の **sbin** サブディレクトリーに変更します。
4. インスタンスから DB2 データベースを構成解除するには、以下のオプションのいずれかを選択します。
  - ディレクトリー・サーバー・インスタンスからデータベースを構成解除するには、以下の形式で **idsucfgdb** コマンドを実行します。
 

```
idsucfgdb -I instance_name
```
  - ディレクトリー・サーバー・インスタンスからデータベースを構成解除および削除するには、以下の形式で **idsucfgdb** コマンドを実行します。
 

```
idsucfgdb -I instance_name -r
```

---

## データベースの最適化

DB2 データベースの検索パフォーマンスを向上させるために、データベースを最適化し、データベース表についての DB2 統計を更新することができます。

構成ツールを使用するか、**idsrunstats** コマンドを使用して、DB2 データベースを最適化できます。DB2 最適化操作は定期的に行うか、データ・インポート操作後などのデータベース更新後に実行する必要があります。

データベース最適化を実行すると、ツールによって、表に定義されているすべての索引に関する統計が収集され、更新されます。DB2 照会最適化プログラムでは、これらの統計を使用して、データにアクセスするための最適のパスを決定します。

インスタンスがプロキシ・サーバーの場合や、インスタンスが DB2 データベースを使用して構成されていない場合、DB2 最適化を実行することはできません。

**idsrunstats** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 構成ツールを使用したデータベースの最適化

構成ツールを使用して、インスタンスに関連付けられた DB2 データベースを最適化します。

### 始める前に

インスタンスの DB2 データベースを最適化するには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。197 ページの『構成ツールを使用したインスタンスのデータベースの構成』を参照してください。

### 手順

1. インスタンス用の構成ツールを開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「データベース・タスク」 > 「データベースの最適化」をクリックします。
3. 「データベースの最適化」ページで、以下の手順を実行します。
  - a. データベースの最適化操作を開始するには、「最適化」をクリックします。
  - b. タスクの完了を受け入れるには、「OK」をクリックします。
  - c. データベース最適化操作に関して生成されたログを確認します。
  - d. ログをクリアするには、「結果のクリア」をクリックします。
4. 「データベースの最適化」ページを閉じるには、「閉じる」をクリックします。
5. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
6. アクションを確認するには、「はい」をクリックします。

## コマンド行ユーティリティーを使用したデータベースの最適化

コマンド行ユーティリティー **idsrunstats** を使用して、インスタンスに関連付けられた DB2 データベースを最適化します。

### 始める前に

インスタンスの DB2 データベースを最適化するには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。202 ページの『コマンド行ユーティリティーを使用したインスタンスのデータベースの構成』を参照してください。

### 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の **sbin** サブディレクトリーに変更します。
4. DB2 データベースを最適化するには、以下の形式で **idsrunstats** コマンドを実行します。

```
idsrunstats -I instance_name
```

**idsrunstats** コマンドについて詳しくは、「*Command Reference*」を参照してください。

---

## データベース保守

インスタンスに対する検索または更新の操作を向上させるために、DB2 索引の再編成または DB2 の行の圧縮を実行することができます。

構成ツールまたは **idsdbmaint** コマンドを使用して、DB2 索引の再編成または DB2 の行の圧縮を行うことができます。

データベースの DB2 表を、多くの挿入および削除によって更新した場合、データベースの検索操作および更新操作が遅くなります。DB2 索引を再編成すると、検索操作および更新操作のパフォーマンスが向上します。

DB2 の行の圧縮を実行すると、ツールは反復するパターンを検索し、そのパターンを短い記号ストリングで置き換えます。ツールは行の圧縮を分析し、圧縮による性能の向上が 30 パーセントを超える場合に限り、行の圧縮を実行します。

**idsdbmaint** コマンドを使用して、SMS テーブル・スペースを DMS テーブル・スペースに変換することも、DMS テーブル・スペースを SMS テーブル・スペースに変換することもできます。テーブル・スペースの変換は、構成ツールによってサポートされません。**idsdbmaint** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 構成ツールを使用したデータベース保守の実行

構成ツールを使用して、インスタンスに関連付けられた DB2 データベースを保守します。

### 始める前に

インスタンスの DB2 データベースを保守するには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。197 ページの『構成ツールを使用したインスタンスのデータベースの構成』を参照してください。
- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### 手順

1. インスタンス用の構成ツール を開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「データベース・タスク」 > 「保守」をクリックします。
3. 「保守」ページで、以下の手順を実行します。
  - a. 実行する DB2 データベースの保守操作を選択します。
    - DB2 索引の再編成を実行するには、「索引の再編成の実行」をクリックします。
    - DB2 の行の圧縮を実行するには、「テーブルを調べて行の圧縮を実行」をクリックします。
  - b. 「OK」をクリックします。
  - c. タスクの完了ウィンドウで、「OK」をクリックします。
  - d. データベース保守操作に関して生成されたログを確認します。
  - e. ログをクリアするには、「結果のクリア」をクリックします。
4. 「保守」ページを閉じるには、「閉じる」をクリックします。
5. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
6. アクションを確認するには、「はい」をクリックします。

### 次のタスク

ディレクトリー・サーバーを始動します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## コマンド行ユーティリティーを使用したデータベース保守の実行

コマンド行ユーティリティー `idsdbmaint` を使用して、インスタンスに関連付けられた DB2 データベースの保守操作を実行します。

## 始める前に

DB2 データベース保守操作を実行するには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。202 ページの『コマンド行ユーティリティーを使用したインスタンスのデータベースの構成』を参照してください。
- ディレクトリー・サーバーを停止します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
4. DB2 の索引の再編成を実行するには、以下の形式で `idsdbmaint` コマンドを実行します。

```
idsdbmaint -I instance_name -i
```

`idsdbmaint` コマンドについて詳しくは、「*Command Reference*」を参照してください。

5. DB2 の行の圧縮を実行するには、以下の形式で `idsdbmaint` コマンドを実行します。

```
idsdbmaint -I instance_name -r
```

## 次のタスク

ディレクトリー・サーバーを始動します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

---

## ディレクトリー・サーバーのバックアップ

ディレクトリー・サーバー・インスタンス障害から復旧するには、ディレクトリー・サーバー・インスタンスを頻繁にバックアップする必要があります。

構成ツールまたは `idsdbback` コマンドを使用して、インスタンスをバックアップできます。プロキシー・サーバーにはデータベースが関連付けられていないため、`idsdbback` コマンドを使用してプロキシー・サーバー・インスタンスをバックアップすることはできません。

オンライン・バックアップ用のインスタンスに関連付けられているデータベースを、`idscfgdb` コマンドを使用して構成できます。ただし、`-c` パラメーターを指定した `idscfgdb` コマンドを使用して、オンライン・バックアップを構成解除することはできません。インスタンス管理ツールまたは構成ツールを使用して、インスタンスのオンライン・バックアップを構成した場合、構成ツールまたは `idscfgdb` コマンドを使用してこれを構成解除できます。最も信頼性の高い結果を得るには、イ

インスタンス管理ツールまたは構成ツールを使用して、データベースを持つインスタンスのオンライン・バックアップを構成してください。

また、**idsdb21dif** コマンドを使用して、ディレクトリー・サーバー内の項目を LDIF ファイルにエクスポートすることもできます。**migbkup** コマンドを使用して、ディレクトリー・サーバー・インスタンスおよびプロキシ・サーバー・インスタンスのスキーマ・ファイルおよび構成ファイルをバックアップすることができます。**idsdbback**、**idsdb21dif**、**migbkup** コマンドについて詳しくは、「*Command Reference*」を参照してください。ご使用の環境で使用する最適なコマンドについては、IBM Security Directory Server 資料の『パフォーマンス・チューニングとキャパシティー計画 (*Performance Tuning and Capacity Planning*)』セクションを参照してください。

構成ツールを使用して、以下のアクションを実行できます。

- ディレクトリー・サーバー・インスタンスやプロキシ・サーバー・インスタンスの構成設定をバックアップします。
- ディレクトリー・サーバー・インスタンスとそのデータベースを一緒にバックアップします。
- ディレクトリー・サーバー・インスタンスと変更ログ・データベース (インスタンス用に構成されている場合) をバックアップします。

バックアップおよびリストア操作について詳しくは、IBM Security Directory Server 資料の『管理』セクションを参照してください。

## 構成ツールを使用したディレクトリー・サーバー・インスタンスのデータベースのバックアップ

障害からリカバリーできるように、構成ツールを使用してディレクトリー・サーバー・インスタンスをそのデータベースとともにバックアップします。

### 始める前に

ディレクトリー・サーバー・インスタンスをそのデータベースとともにバックアップするには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。197 ページの『構成ツールを使用したインスタンスのデータベースの構成』を参照してください。

### 手順

1. インスタンス用の構成ツールを開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「バックアップ/復元」> 「データベースのバックアップ」をクリックします。
3. 「データベースのバックアップ」ページで、以下の手順を実行します。
  - a. 「バックアップ・ディレクトリー」フィールドに、すべてのディレクトリー・データと構成ファイルをバックアップするディレクトリー・パスを入力します。「参照」をクリックして、ディレクトリー・パスを指定することもできます。

- b. オンライン・バックアップの場合は、以下のオプションのいずれかを選択します。
    - オンライン・バックアップがまだ構成されていないディレクトリー・サーバーとそのデータベースでオンライン・バックアップを構成するには、「データベース構成を更新してオンライン・バックアップをサポートする」を選択します。
    - サーバーでオンライン・バックアップが構成されている場合に、ディレクトリー・サーバー・インスタンスのオンライン・バックアップを実行するには、「オンライン・バックアップの実行」を選択します。
  - c. 変更ログが構成されている場合に、インスタンスの変更ログ・データベースをバックアップするには、「変更ログ・データをバックアップに組み込む」を選択します。
  - d. データベース・ファイルをバックアップから除外するには、「データベース・ファイルをバックアップしない」を選択します。「データベース・ファイルをバックアップしない」を選択すると、ディレクトリー・サーバー・インスタンスのデータベースおよび変更ログ・データベースがバックアップされなくなります。ツールは、ディレクトリー・サーバー・インスタンスのファイル（鍵 stash ファイル、スキーマ、構成ファイルなど）をバックアップします。
  - e. バックアップ・ディレクトリーの有無によってバックアップを続行するかどうかを決定するには、以下のいずれかのオプションを選択します。
    - バックアップ・ディレクトリーが存在しないときにバックアップ・ディレクトリーを作成する場合は、「必要に応じてバックアップ・ディレクトリーを作成する」をクリックします。
    - バックアップ・ディレクトリーが存在しないときにバックアップ・ディレクトリーを作成しない場合は、「バックアップ・ディレクトリーが見つからない場合は打ち切る」をクリックします。バックアップ・ディレクトリーが存在しない場合にこのオプションを選択すると、データベースはバックアップされません。
- 注: バックアップ操作の実行中に構成ツールを終了しないでください。
- f. バックアップ操作を開始するには、「バックアップ」をクリックします。
  - g. バックアップ操作でディレクトリー・サーバーを停止する必要がある場合は、「はい」をクリックします。
  - h. タスクの完了を確認するには、「OK」をクリックします。
  - i. バックアップ操作に関して生成されたログを確認します。
  - j. ログをクリアするには、「結果のクリア」をクリックします。
  - k. 「データベースのバックアップ」ページを閉じるには、「閉じる」をクリックします。
- 4. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
  - 5. アクションを確認するには、「はい」をクリックします。

## 構成ツールを使用したプロキシ・サーバー・インスタンスのバックアップ

構成ツールを使用してプロキシ・サーバー・インスタンスをバックアップして、障害からリカバリーできるようにします。

### 始める前に

プロキシ・サーバー・インスタンスをバックアップするには、プロキシ・サーバー・インスタンスが存在している必要があります。160 ページの『カスタム設定を使用したプロキシ・サーバー・インスタンスの作成』を参照してください。

### 手順

1. インスタンス用の構成ツールを開始します。190 ページの『構成ツールの開始』を参照してください。
  2. 左側のナビゲーション・ペインのタスク・リストから、「バックアップ/復元」 > 「インスタンスのバックアップ」をクリックします。
  3. 「インスタンスのバックアップ」ページで、以下の手順を実行します。
    - a. 「バックアップ・ディレクトリー」フィールドに、スキーマと構成ファイルをバックアップするディレクトリー・パスを入力します。「参照」をクリックして、ディレクトリー・パスを指定することもできます。
    - b. プロキシ・サーバー・インスタンスに対しては、「データベース・ファイルをバックアップしない」チェック・ボックスが選択されています。
    - c. バックアップ・ディレクトリーの有無によってバックアップを続行するかどうかを決定するには、以下のいずれかのオプションを選択します。
      - バックアップ・ディレクトリーが存在しないときにバックアップ・ディレクトリーを作成する場合は、「必要に応じてバックアップ・ディレクトリーを作成する」をクリックします。
      - バックアップ・ディレクトリーが存在しないときにバックアップ・ディレクトリーを作成しない場合は、「バックアップ・ディレクトリーが見つからない場合は打ち切る」をクリックします。バックアップ・ディレクトリーが存在しない場合にこのオプションを選択すると、プロキシ・インスタンスはバックアップされません。
- 注: バックアップ操作の実行中に構成ツールを終了しないでください。
- d. バックアップ操作を開始するには、「バックアップ」をクリックします。
  - e. この操作でインスタンスを停止する必要がある場合は、「はい」をクリックします。
  - f. タスクの完了を確認するには、「OK」をクリックします。
  - g. バックアップ操作に関して生成されたログを確認します。
  - h. ログをクリアするには、「結果のクリア」をクリックします。
  - i. 「インスタンスのバックアップ」ページを閉じるには、「閉じる」をクリックします。
4. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
  5. アクションを確認するには、「はい」をクリックします。

---

## ディレクトリー・サーバーの復元

ディレクトリー・サーバー・インスタンスに障害が発生した場合、インスタンスを最新のバックアップ・イメージに復元できます。

構成ツールまたは **idsdbestore** コマンドを使用して、以前にバックアップされたディレクトリー・データと構成設定 (オプション) を復元することができます。ディレクトリー・サーバーは、データベースまたは構成設定、あるいはその両方を復元する前に停止する必要があります。

プロキシー・サーバーの場合、構成設定を復元できます。プロキシー・サーバーの場合、**idsdbestore** コマンドに **-x** パラメーターを指定して実行する必要があります。

DB2 データベースを使用するインスタンスの場合、データベース・バックアップに使用された名前と同じ名前のデータベースおよびデータベース・インスタンスにデータベースを復元できます。DB2 データベースを使用するディレクトリー・サーバーの場合、データベースがディレクトリー・サーバー・インスタンスに対して構成されている場合のみ復元できます。**idsdbestore** コマンドにより、現在構成されているデータベースにバックアップ・データベースが復元されます。バックアップされたデータベース・インスタンスおよびデータベースが、構成されているデータベース・インスタンスおよびデータベースと一致しない場合、コマンドは失敗します。データベースを復元するには、バックアップされたデータベースと、コマンドで復元するデータベースのロケーションが同じでなければなりません。

**idsdbestore** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 構成ツールを使用したディレクトリー・サーバーのデータベースの復元

構成ツールを使用して、ディレクトリー・サーバー・インスタンスとそのデータベースをバックアップされたイメージから復元します。

### 始める前に

ディレクトリー・サーバー・インスタンスとそのデータベースを復元するには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。197 ページの『構成ツールを使用したインスタンスのデータベースの構成』を参照してください。
- ディレクトリー・サーバー・インスタンスのバックアップ・イメージが存在している必要があります。213 ページの『構成ツールを使用したディレクトリー・サーバー・インスタンスのデータベースのバックアップ』を参照してください。
- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. インスタンス用の構成ツール を開始します。 190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「バックアップ/復元」 > 「データベースの復元」をクリックします。
3. 「データベースの復元」 ページで、以下の手順を実行します。
  - a. 「復元ディレクトリー」 フィールドに、インスタンスのバックアップ・イメージが置かれているディレクトリー・パスを入力します。「参照」をクリックして、ディレクトリー・パスを指定することもできます。
  - b. バックアップ・イメージからディレクトリー・データのみを復元して構成設定を復元しない場合は、「現在の構成設定を保存する」を選択します。 データベースと構成設定の両方を復元する場合は、「現在の構成設定を保存する」をクリアする必要があります。
  - c. インスタンスに対して変更ログが構成されている場合に、変更ログ・データを復元するには、「変更ログ・データを復元に組み込む」を選択します。
  - d. 復元操作を開始するには、「復元」をクリックします。
  - e. この操作でディレクトリー・サーバーを停止する必要がある場合は、「はい」をクリックします。
  - f. タスクの完了を確認するには、「OK」をクリックします。
  - g. 復元操作に関して生成されたログを確認します。
  - h. ログをクリアするには、「結果のクリア」をクリックします。
  - i. 「データベースの復元」 ページを閉じるには、「閉じる」をクリックします。
4. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
5. アクションを確認するには、「はい」をクリックします。

## 構成ツールを使用したプロキシ・サーバー・インスタンスの復元

障害からリカバリーするために、構成ツールを使用してプロキシ・サーバー・インスタンスを復元します。

### 始める前に

プロキシ・サーバー・インスタンスを復元するには、プロキシ・サーバー・インスタンスが以下の要件を満たしている必要があります。

- プロキシ・サーバー・インスタンスが存在している必要があります。 160 ページの『カスタム設定を使用したプロキシ・サーバー・インスタンスの作成』を参照してください。
- プロキシ・サーバー・インスタンスのバックアップ・イメージが存在している必要があります。 215 ページの『構成ツールを使用したプロキシ・サーバー・インスタンスのバックアップ』を参照してください。
- ディレクトリー・サーバーを停止します。 191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. インスタンス用の構成ツール を開始します。 190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「バックアップ/復元」 > 「インスタンスの復元」をクリックします。
3. 「インスタンスの復元」 ページで、以下の手順を実行します。
  - a. 「復元ディレクトリー」フィールドに、インスタンスのバックアップ・イメージが置かれているディレクトリー・パスを入力します。「参照」をクリックして、ディレクトリー・パスを指定することもできます。
  - b. バックアップ・イメージから構成設定を復元しない場合は、「現在の構成設定を保存する」を選択します。
  - c. 復元操作を開始するには、「復元」をクリックします。
  - d. この操作でディレクトリー・サーバーを停止する必要がある場合は、「はい」をクリックします。
  - e. タスクの完了を確認するには、「OK」をクリックします。
  - f. 復元操作に関して生成されたログを確認します。
  - g. ログをクリアするには、「結果のクリア」をクリックします。
  - h. 「インスタンスの復元」 ページを閉じるには、「閉じる」をクリックします。
4. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
5. アクションを確認するには、「はい」をクリックします。

---

## ディレクトリー・サーバーのパフォーマンス・チューニング

検索および更新のパフォーマンスを向上させるために、ディレクトリー・サーバー・インスタンスを調整する必要があります。

構成ツールまたは **idsperftune** コマンドを実行して、ディレクトリー・サーバー・インスタンスを調整することができます。ツールにより、ディレクトリー・サーバー・キャッシュおよび DB2 バッファー・プールについてのパフォーマンス・チューニング設定値が生成されます。ツールでは、ディレクトリー・サーバー・インスタンスについてユーザーから提供された値に基づくチューニング設定が生成されます。また、ツールはインスタンスのチューニング設定を更新することもできます。ツールは **ibmslapd.conf** ファイルをバックアップし、ディレクトリー・サーバー・インスタンスのホーム・ディレクトリーの **logs/ibmslapd.conf.save** ファイルに保存します。

ツールは、ユーザーが **logs/perftune\_input.conf** ファイルに提供した情報を、ディレクトリー・サーバー・インスタンスのホーム・ディレクトリーに保存します。

構成ツールまたは **idsperftune** コマンドは、ユーザーから提供された値を使用して、以下に示すインスタンスのチューニング設定を計算します。

- 項目キャッシュのサイズ
- フィルター・キャッシュのサイズ
- グループ・メンバー・キャッシュのサイズ

- グループ・メンバー・キャッシュ・バイパスの制限
- DB2 LDAPDB バッファ・プール・サイズ
- DB2 IBMDEFAULTDB バッファ・プール・サイズ

ディレクトリー・サーバー・インスタンスが実行中の場合、ツールはインスタンスのパフォーマンスをモニターし、データベースの正常性チェック情報を提供します。データベースの正常性チェック情報には、以下の DB2 パラメーターが含まれています。

- DB2 NUM\_IOSERVERS
- DB2 NUM\_IOCLEANERS
- CATALOGCACHE\_SZ
- PCKCACHESZ
- LOGFILSIZ
- LOCKLIST

インスタンスに関する拡張チューニングを実行する場合、ツールはディレクトリー・サーバー・インスタンスについてのデータを収集して分析します。インスタンスをしばらく実行して、データベースの正常性チェック分析を実行している間の DB2 チューニング・データを収集する必要があります。ツールは以下の DB2 パラメーターについてのチューニング値を生成し、インスタンス用の logs/perftune\_stat.log ファイルにこれらの値を保存します。

- SORTHEAP
- MAXFILOP
- DBHEAP
- CHNGPGS\_THRESH
- NUM\_IOSERVERS
- NUM\_IOCLEANERS

DB2 パラメーターについて表示される正常性ステータスの値は、以下のいずれかです。

- OK
- 増加
- 減少
- 未収集

分析されない DB2 パラメーターの正常性ステータスには、「未収集」という値が割り当てられます。表示された値を使用して、より良いパフォーマンスを得るために調整可能な DB2 パラメーターがどれかを判別することができます。

より良いパフォーマンスを得るためには、初期のディレクトリー・データをロードした直後にインスタンスに対してツールを実行する必要があります。初期チューニングの後は定期的にツールを実行し、特に、多くの項目を追加したり項目の内容を変更したりした場合に実行するようにします。ディレクトリー・サーバー・インスタンスのチューニングについて詳しくは、IBM Security Directory Server 資料の『パフォーマンス・チューニングとキャパシティー計画 (Performance Tuning and Capacity Planning)』セクションを参照してください。

構成ツールまたは `idsperftune` コマンドを使用して、データベースを使用して構成されていないインスタンスおよびプロキシ・サーバー・インスタンスを調整することはできません。

## 構成ツールを使用したパフォーマンス・チューニングのためのディレクトリー・サーバーの構成

構成ツールを使用して、検索操作と更新操作のパフォーマンスが向上するようにディレクトリー・サーバーをチューニングします。

### 始める前に

ディレクトリー・サーバー・インスタンスをチューニングするには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。197 ページの『構成ツールを使用したインスタンスのデータベースの構成』を参照してください。

### 手順

1. インスタンス用の構成ツールを開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「データベース・タスク」 > 「パフォーマンス・チューニング」をクリックします。
3. 「パフォーマンス・チューニング」ページで、以下の手順を実行します。
  - a. 「このディレクトリー・インスタンスに割り振る使用可能システム・メモリーのパーセンテージ」フィールドに、インスタンスに割り振るシステム・メモリーのパーセンテージを入力します。使用可能なシステム・メモリーは、複数のディレクトリー・サーバー・インスタンス間、またはインスタンスとシステムで実行するその他のサーバー間で分配されます。ユーザーが指定した値を使用して、ツールが項目キャッシュとフィルター・キャッシュのサイズを計算します。
  - b. 「計画したグループの数」フィールドに、インスタンスに追加する予定のグループ数を入力します。ユーザーが指定した値を使用して、ツールがディレクトリー・サーバー・キャッシュのサイズを計算します。
  - c. 頻繁に参照されるグループの平均メンバー数を「参照頻度が高いグループ内のメンバーの最大数」フィールドに入力します。
  - d. 「項目数および平均項目サイズ」領域で、以下のいずれかのオプションを選択します。
    - ディレクトリー内の項目数と項目の平均サイズを見積もる場合は、以下の手順を実行します。
      - 1) 「計画した項目の数」フィールドに、インスタンスに対して計画した項目の総数を入力します。ツールは、ディレクトリー・サーバー・インスタンス内の項目数を決定しようとします。できない場合は、デフォルトの 10,000 項目を使用します。ツールは、この値を使用してディレクトリー・サーバー・キャッシュのサイズを計算します。
      - 2) 「項目の平均サイズ」フィールドに、インスタンス内の項目の平均サイズをバイト単位で入力します。このツールは、ディレクトリー・サ

サーバー・インスタンスの項目サイズの計算を試みます。できなかった場合は、デフォルトの 2,650 バイトを使用します。ツールは、この値を使用してディレクトリー・サーバー・キャッシュのサイズを計算します。

- 項目の総数と平均項目サイズをツールで決定する場合は、「サーバー・インスタンス・データベースからのロード」をクリックします。ツールによって、「計画した項目の数」フィールドと「項目の平均サイズ」フィールドに値が取り込まれます。
- e. 「更新頻度」領域で、以下のいずれかのオプションを選択します。
- インスタンスを頻繁に更新することが予想される場合は、「高頻度の更新」をクリックします。(目安として、平均して 500 回検索するごとに 2 回以上更新される場合は、更新が頻繁であるとみなすことができます。)
  - 更新頻度が低いことが予想される場合、または更新をグループ化して 1 日のうちの特定の時間に実行する場合は「バッチ更新」をクリックします。

この情報を使用して、ツールがフィルター・キャッシュのサイズを設定します。フィルター・キャッシュが役立つのは、インスタンスの更新頻度が低く、同じ検索が複数回実行される場合に限られます。頻繁な更新が予想される場合は、フィルター・キャッシュが 0 に設定されます。更新頻度が低いと予想される場合またはバッチ更新が予想される場合は、フィルター・キャッシュが 1024 フィルター・キャッシュ項目に設定されます。

- f. ツールを使用してパフォーマンス分析値を得る場合は、「拡張チューニングのための追加のシステム・データの収集を使用可能にする」を選択します。
- このチェック・ボックスを選択すると、DB2 モニター・スイッチ BUFFERPOOL と SORTHEAP が使用可能になります。ツールが DB2 モニター・スイッチを使用可能にしてデータを収集すると、ディレクトリー・サーバー・インスタンスのパフォーマンスが低下することがあります。
  - ディレクトリー・サーバー・インスタンスを最適にチューニングするための正確なデータを得るには、ご使用の環境で標準的なディレクトリー・アクティビティが実行されているときにこのチェック・ボックスを選択します。サーバーが通常に比べてビジーでないときにデータベース正常性チェックを実行しても、最適なパフォーマンス値は得られません。
- g. 「次へ」をクリックします。「パフォーマンス・チューニング: 検証」ページが開きます。
4. 「パフォーマンス・チューニング: 検証」ページで、以下の手順を実行します。
- a. 「データベースの正常性ステータス」リストで、ツールが生成したパフォーマンス・チューニングの設定を確認します。インスタンスにデータベース・アクティビティがない場合は、「データベースの正常性ステータス」リストが空になる可能性があります。このリストには、ツールが 1 つ以上の DB2 関連パラメーターに関する情報を収集した場合のみデータが取り込まれます。チューニング設定は、perftune\_stat.log ファイルにも記録されます。

- b. データベース・パラメーター値を変更するには、「データベース・パラメーターの調整」をクリックします。「データベース・パラメーター」ウィンドウが開きます。
- c. 「データベース・パラメーター」ウィンドウで、以下のデータベース・パラメーターの値を指定します。
  - 1) 「データベース・ヒープ」フィールドに、データベース・ヒープに対して設定する最大メモリー (ページ数) を入力します。データベース・ヒープには、テーブル、索引、テーブル・スペース、およびバッファークール・プールの制御ブロック情報が含まれます。また、ログ・バッファークールや、ユーティリティで使用される一時メモリーも含まれます。
  - 2) 「パッケージ・キャッシュ・サイズ」フィールドに、データベース上の静的 SQL と動的 SQL および XQuery ステートメントのセクションをキャッシュするためのサイズ (ページ数) を入力します。
  - 3) 「ログ・バッファークール・サイズ」フィールドに、ログ・レコードに割り振る必要があるバッファークールのサイズ (ページ数) を入力します。ログ・レコードのバッファークールとして使用するデータベース・ヒープの量を指定する必要があります。
  - 4) 「アプリケーションごとに開くデータベース・ファイルの最大数」フィールドに、データベース・エージェントごとに開くことができるファイル・ハンドルの最大数を入力します。
  - 5) 「変更されたページ数のしきい値」フィールドに、変更されたページ数の割合を入力します。
  - 6) 「ソート・ヒープ・サイズ」フィールドに、ソート・ヒープの最大サイズ (ページ数) を入力します。ソート・ヒープは、プライベート・ソートでの専用メモリー・ページ、または共有ソートでの共用メモリー・ページとして使用できます。
  - 7) 「ログ・ファイル・サイズ」フィールドに、ログ・ファイルのサイズ (KB 単位) を入力します。このパラメーターは、1 次ログ・ファイルと 2 次ログ・ファイルのそれぞれのサイズを定義します。
  - 8) 「データベース・ログ・パス」フィールドに、ログ・ファイルを保管するロケーションを入力します。「参照」をクリックすると、ロケーションを指定できます。
  - 9) 設定した値を保存し、その値でデータベース・パラメーターを更新するには、「OK」をクリックします。パラメーターの値を指定しない場合は、デフォルト値が設定されます。
5. ディレクトリーとデータベースの設定をチューニング値で更新するかどうかを確定するには、以下のいずれかのオプションを選択します。
  - ディレクトリー・サーバー・インスタンスのチューニング設定を更新する場合は、「はい、推奨値を使用してディレクトリーおよびデータベースの構成設定を更新します」をクリックします。
  - チューニング設定を使用しない場合は、「いいえ、現行の設定を保持します。構成設定を更新しません」をクリックします。
6. 変更を適用するには、「完了」をクリックします。
7. タスクの完了を確認するには、「OK」をクリックします。
8. チューニング設定が更新されるときに生成されたログを確認します。

9. ログをクリアするには、「結果のクリア」をクリックします。
10. 「パフォーマンス・チューニング」ページを閉じるには、「閉じる」をクリックします。
11. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
12. アクションを確認するには、「はい」をクリックします。

## コマンド行ユーティリティーを使用したパフォーマンス・チューニングのためのディレクトリー・サーバーの構成

コマンド行ユーティリティー **idsperftune** を使用して、検索操作と更新操作のパフォーマンスが向上するようにディレクトリー・サーバーをチューニングします。

### 始める前に

ディレクトリー・サーバー・インスタンスをチューニングするには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。202 ページの『コマンド行ユーティリティーを使用したインスタンスのデータベースの構成』を参照してください。

### 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
4. ディレクトリー・サーバーとそのデータベースをチューニングするには、**idsperftune** コマンドを実行します。

- ディレクトリー・サーバーの基本チューニングを実行するには、**idsperftune** コマンドを以下の形式で実行します。

```
idsperftune -I instance_name -i property_file -B -u
```

**-u** パラメーターを指定すると、LDAP キャッシュと DB2 バッファー・プールの設定がサーバーおよびデータベース内で更新されます。**-u** パラメーターを指定しない場合は、チューニング設定が `perftune_stat.log` ファイルにのみ記録されます。

- インスタンスとそのデータベースから項目数と平均項目サイズを取得するには、**idsperftune** コマンドを以下の形式で実行します。

```
idsperftune -I instance_name -s
```

- ディレクトリー・サーバーの拡張チューニングを実行するには、**idsperftune** コマンドを以下の形式で実行します。

```
idsperftune -I instance_name -i property_file -A -m
```

**-m** パラメーターを指定すると、BUFFERPOOL と SORT のモニター・スイッチがオンになります。インスタンスを最適にチューニングするための正確なデータを得るには、ご使用の環境で標準的なディレクトリー・アクティビティーが実行されているときにこのコマンドを実行します。

**idsperftune** コマンドについて詳しくは、「*Command Reference*」を参照してください。

---

## ディレクトリー・サーバー・インスタンスのための変更ログ管理

インスタンスのスキーマまたはディレクトリー項目への変更を記録するように変更ログ・データベースを構成できます。

変更ログは、ディレクトリー・サーバー・インスタンスに対するすべての更新操作 (add、delete、modify、modrdrn など) を記録します。クライアント・ユーティリティーを使用して、ディレクトリー・サーバー・データベースが変更されたときに記録された変更ログ・データを取得することができます。

構成ツールまたはコマンド行ユーティリティーを使用して、変更ログ・データベースを使用可能または使用不可にすることができます。ディレクトリー・サーバーは、変更ログ・データベースを構成または構成解除する前に停止する必要があります。

ディレクトリー・サーバーの変更ログを構成するには、**idscfgchglg** コマンドを使用します。ディレクトリー・サーバーの変更ログを構成解除するには、**idsucfgchglg** コマンドを使用します。プロキシ・サーバー・インスタンスの変更ログ・データベースは構成できません。

ディレクトリー・サーバー・インスタンスの変更ログを構成するには、以下の基準を満たしている必要があります。

1. ディレクトリー・サーバー・インスタンスと同じ名前の DB2 インスタンスが存在している必要があります。
2. ディレクトリー・サーバー・インスタンスのデータベースを構成する必要があります。
3. AIX、Linux、および Solaris の場合は、ローカル・ループバック・サービスが `/etc/services` ファイルに登録されている必要があります。

変更ログ・データベースを構成すると、それがディレクトリー・サーバー・インスタンス・データベースと同じデータベース・インスタンス内に作成されます。変更ログ・データベースについては、ハード・ディスクのスペースとして、さらに 30 MB が必要になります。変更ログを構成すると、変更ログの項目がディレクトリー・サーバー・インスタンスの構成ファイルに追加されます。

### 構成ツールを使用した変更ログの構成

構成ツールを使用して、ディレクトリー・サーバー・インスタンスの変更ログ・データベースを構成します。

#### 始める前に

インスタンスの変更ログを構成するには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。197 ページの『構成ツールを使用したインスタンスのデータベースの構成』を参照してください。

- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. インスタンス用の構成ツール を開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「**変更ログの管理**」をクリックします。
3. 「**変更ログの管理**」ページで、以下の手順を実行します。
  - a. 変更ログを構成するには、「**変更ログ・データベースを使用可能にする**」を選択します。
  - b. 「**ログの最大項目数**」領域で、変更ログ・データベースに記録する項目の最大数を指定します。
    - 変更ログに記録する項目数を制限しない場合は、「**無制限**」をクリックします。
    - 特定の数の項目を記録する場合は、「**項目**」をクリックし、項目の数を入力します。デフォルトの項目数は 1,000,000 です。
  - c. 「**最大存続期間**」領域で、変更ログ・データベースに項目を保管する期間の上限を指定します。
    - 変更ログに無期限に項目を保管する場合は、「**無制限**」をクリックします。
    - 特定の期間にわたって項目を保管する場合は、「**存続期間 (Age)**」をクリックし、日数と時間数を入力します。
  - d. 変更を適用するには、「**更新**」をクリックします。
  - e. タスクの完了を確認するには、「**OK**」をクリックします。
  - f. 変更ログ・データベースの構成に関して生成されたログを確認します。
  - g. ログをクリアするには、「**結果のクリア**」をクリックします。
  - h. 「**変更ログの管理**」ページを閉じるには、「**閉じる**」をクリックします。
4. 構成ツール ウィンドウを閉じるには、「**ファイル**」 > 「**終了**」をクリックしてください。
5. アクションを確認するには、「**はい**」をクリックします。

## 次のタスク

ディレクトリー・サーバーを始動します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## コマンド行ユーティリティーを使用した変更ログの構成

コマンド行ユーティリティー `idscfgchg1g` を使用して、ディレクトリー・サーバー・インスタンスの変更ログ・データベースを構成します。

## 始める前に

インスタンスの変更ログを構成するには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。202 ページの『コマンド行ユーティリティーを使用したインスタンスのデータベースの構成』を参照してください。
- ディレクトリー・サーバーを停止します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
4. ディレクトリー・サーバー・インスタンスの変更ログを構成するには、**idscfgchglg** コマンドを実行します。

- 経過時間の制限またはサイズ制限なしでインスタンスの変更ログを構成するには、次の **idscfgchglg** コマンドを実行します。

```
idscfgchglg -I instance_name -m 0
```

- サイズ制限を 1,000,000、経過時間を 25 時間に設定してインスタンスの変更ログを構成するには、次の **idscfgchglg** コマンドを実行します。

```
idscfgchglg -I instance_name -m 1000000 -y 1 -h 1
```

**idscfgchglg** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 次のタスク

ディレクトリー・サーバーを始動します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 構成ツールを使用した変更ログの構成解除

構成ツールを使用して、ディレクトリー・サーバー・インスタンスから変更ログ・データベースを構成解除します。

## 始める前に

インスタンスから変更ログを構成解除するには、インスタンスが以下の要件を満たしている必要があります。

- インスタンスの変更ログが構成されている必要があります。224 ページの『構成ツールを使用した変更ログの構成』を参照してください。
- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. インスタンス用の構成ツール を開始します。 190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「**変更ログの管理**」をクリックします。
3. 「**変更ログの管理**」ページで、以下の手順を実行します。
  - a. 変更ログを構成解除するには、「**変更ログ・データベースを使用可能にする**」をクリアします。
  - b. 変更を適用するには、「**更新**」をクリックします。
  - c. 「**変更ログの管理**」ウィンドウで「**はい**」をクリックして、アクションを確認します。
  - d. 変更ログ・データベースを構成解除する際に生成されたログを確認します。
  - e. ログをクリアするには、「**結果のクリア**」をクリックします。
  - f. 「**変更ログの管理**」ページを閉じるには、「**閉じる**」をクリックします。
4. 構成ツール ウィンドウを閉じるには、「**ファイル**」 > 「**終了**」をクリックしてください。
5. アクションを確認するには、「**はい**」をクリックします。

## 次のタスク

ディレクトリー・サーバーを始動します。 191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## コマンド行ユーティリティーを使用した変更ログの構成解除

コマンド行ユーティリティー `idsucfgchglg` を使用して、ディレクトリー・サーバー・インスタンスから変更ログ・データベースを構成解除します。

### 始める前に

インスタンスから変更ログを構成解除するには、インスタンスが以下の要件を満たしている必要があります。

- インスタンスの変更ログが構成されている必要があります。 225 ページの『コマンド行ユーティリティーを使用した変更ログの構成』を参照してください。
- ディレクトリー・サーバーを停止します。 177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
4. ディレクトリー・サーバー・インスタンスの変更ログを構成解除するには、以下の形式で `idsucfgchglg` コマンドを実行します。

```
idsucfgchglg -I instance_name
```

**idsucfgchglg** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 次のタスク

ディレクトリー・サーバーを始動します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

---

## サフィックス構成

ディレクトリー階層を作成するには、ディレクトリー・サーバー・インスタンスに必要なサフィックスを構成する必要があります。

サフィックスは、命名コンテキストとして知られています。これは、ディレクトリー階層内の最上部の項目を識別する識別名 (DN) です。LDAP では相対命名方式が使用されています。したがって、DN は、ディレクトリー階層内のすべての項目のサフィックスでもあります。ディレクトリー・サーバーでは複数のサフィックスを追加でき、各サフィックスがディレクトリー階層を識別します。サフィックスを追加すると、ディレクトリー・サーバー・インスタンスの構成ファイルに項目が追加されます。サフィックス項目の例を次に示します。o=sample。

構成ツールを使用してサフィックスを追加したり削除したりできます。また、**idscfgsuf** コマンドを使用してサフィックスを追加したり、**idsucfgsuf** コマンドを使用してサフィックスを削除したりできます。サフィックスを追加または削除する前に、ディレクトリー・サーバーを停止する必要があります。**idscfgsuf** または **idsucfgsuf** コマンドについて詳しくは、「*Command Reference*」を参照してください。

システムで定義されたサフィックスをディレクトリー・サーバー・インスタンスから削除することはできません。これらのサフィックスは、プロキシ・サーバー・インスタンスでは使用できません。以下のサフィックスがシステムで定義されています。

- cn=localhost
- cn=configuration
- cn=ibmpolicies
- cn=Deleted Objects

項目をディレクトリー・サーバーに追加する場合は、以下の点を考慮してください。

- サフィックス項目は、サフィックス DN 用のディレクトリー・サーバー内に追加する必要があります。
- ディレクトリー・サーバーに追加する項目 DN は、サフィックス DN 値に一致するサフィックスを含んでいる必要があります。サフィックス DN を含む項目の例を次に示します。ou=Marketing,o=sample。
- DB2 データベースを使用して構成されていないプロキシ・サーバー・インスタンスやディレクトリー・サーバーには、項目を追加できません。

照会に含まれたサフィックスがローカル・データベース用に構成されたいずれのサフィックスにも一致しない場合は、その照会は、デフォルト参照によって識別される LDAP サーバーを対象とします。LDAP デフォルト参照が指定されていない場合、「オブジェクトは存在していません」というメッセージが生成されます。

## 構成ツールを使用したサフィックスの追加

構成ツールを使用して、インスタンスにサフィックスを追加します。

### 始める前に

インスタンスにサフィックスを追加するには、以下の手順を実行する必要があります。

- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### このタスクについて

インスタンスにサフィックスを追加すると、インスタンスの構成ファイルにサフィックス項目が追加されます。

### 手順

1. インスタンス用の構成ツール を開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「サフィックス管理」をクリックします。
3. 「サフィックス管理」ページで、以下の手順を実行します。
  - a. 「サフィックス DN」フィールドに、インスタンスに追加するサフィックスを入力します。
  - b. 「追加」をクリックします。
  - c. 変更を適用するには、「OK」をクリックします。
4. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
5. アクションを確認するには、「はい」をクリックします。

### 次のタスク

ディレクトリー・サーバーを始動します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## コマンド行ユーティリティーを使用したサフィックスの追加

コマンド行ユーティリティー `idscfgsuf` を使用して、インスタンスにサフィックスを追加します。

## 始める前に

インスタンスにサフィックスを追加するには、以下の手順を実行する必要があります。

- ディレクトリー・サーバーを停止します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## このタスクについて

インスタンスにサフィックスを追加すると、インスタンスの構成ファイルにサフィックス項目が追加されます。

## 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
4. インスタンスに `o=sample` サフィックスを追加するには、以下の形式で **idscfgsuf** コマンドを実行します。

```
idscfgsuf -I instance_name -s "o=sample"
```

**idscfgsuf** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 次のタスク

ディレクトリー・サーバーを始動します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 構成ツールを使用したサフィックスの削除

構成ツールを使用して、ディレクトリー・サーバー・インスタンスからサフィックスを削除します。

## 始める前に

ディレクトリー・サーバー・インスタンスからサフィックスを削除するには、以下の手順を実行する必要があります。

- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## このタスクについて

インスタンスからサフィックスを削除すると、インスタンスの構成ファイルからサフィックス項目が削除されます。

## 手順

1. インスタンス用の構成ツール を開始します。 190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「サフィックス管理」をクリックします。
3. 「サフィックス管理」ページで、以下の手順を実行します。
  - a. 「現在のサフィックス DN」リストから、削除するサフィックスを選択します。フル・ディレクトリー・サーバーの場合は、以下のシステム定義サフィックスを削除できません。
    - cn=localhost
    - cn=configuration
    - cn=ibmpolicies
    - cn=Deleted Objects
  - b. 「除去」をクリックします。
  - c. 「サフィックス管理」の確認ウィンドウで、「OK」をクリックします。
  - d. 変更を適用するには、「OK」をクリックします。
4. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
5. アクションを確認するには、「はい」をクリックします。

## 次のタスク

ディレクトリー・サーバーを始動します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## コマンド行ユーティリティーを使用したサフィックスの削除

コマンド行ユーティリティー `idsucfgsuf` を使用して、インスタンスからサフィックスを削除します。

### 始める前に

インスタンスからサフィックスを削除するには、以下の手順を実行する必要があります。

- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### このタスクについて

インスタンスからサフィックスを削除すると、インスタンスの構成ファイルからサフィックス項目が削除されます。フル・ディレクトリー・サーバーの場合は、以下のシステム定義サフィックスを削除できません。

- cn=localhost
- cn=configuration
- cn=ibmpolicies

- cn=Deleted Objects

## 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
4. インスタンスから `o=sample` サフィックスを削除するには、`idsucfgsuf` コマンドを実行します。

```
idsucfgsuf -I instance_name -s "o=sample"
```

`idsucfgsuf` コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 次のタスク

ディレクトリー・サーバーを始動します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

---

## スキーマ管理

インスタンスがカスタム・オブジェクト・クラスおよび属性をサポートするには、カスタム・オブジェクト・クラスおよび属性を定義するスキーマ・ファイルを追加する必要があります。

構成ツールまたは `idscfgsch` や `idsucfgsch` などのコマンド行ユーティリティーを使用して、スキーマ・ファイルを管理することができます。スキーマ・ファイルはコンピューター上に存在する必要があります。`idscfgsch` コマンドまたは `idsucfgsch` コマンドについて詳しくは、「*Command Reference*」を参照してください。

スキーマ・ファイルを追加または削除する前に、ディレクトリー・サーバーを停止する必要があります。

スキーマ・ファイルを追加または削除すると、インスタンスの構成ファイルが更新されます。以下のスキーマ管理操作を実行できます。

- サーバー始動時にロードするスキーマ・ファイルのリストにスキーマ・ファイルを追加する。
- サーバー始動時に更新されるスキーマ・ファイルのリストからスキーマ・ファイルを削除する。
- スキーマ・ファイルに対して行う妥当性検査のタイプを変更する。

以下のシステム定義スキーマ・ファイルは削除できません。

- 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

また、構成ツールを使用して、項目がスキーマ・ルールを満たしているかどうかを検査するスキーマ妥当性検査規則を指定することもできます。デフォルトのスキーマ妥当性検査規則はバージョン 3 (厳密でない) です。ディレクトリー・サーバーでは以下のスキーマ妥当性検査規則がサポートされています。

#### バージョン 3 (厳密な)

サーバーは項目に対して LDAP バージョン 3 の厳密な妥当性検査を実行します。このタイプの妥当性検査では、項目の追加時にすべての親オブジェクト・クラスが存在している必要があります。

#### バージョン 3 (厳密でない)

サーバーは項目に対して LDAP バージョン 3 の厳密でない妥当性検査を実行します。このタイプの妥当性検査では、項目の追加時にすべての親オブジェクト・クラスが存在している必要はありません。LDAP バージョン 3 (厳密でない) は、デフォルトのスキーマ妥当性検査規則です。

#### バージョン 2

サーバーは項目に対して LDAP バージョン 2 の検査を実行します。

なし サーバーは妥当性検査を実行しません。

## 構成ツールを使用したスキーマ・ファイルの管理

構成ツールを使用して、インスタンスのスキーマ・ファイルを管理します。

### 始める前に

インスタンスのスキーマ・ファイルを管理するには、以下の手順を実行する必要があります。

- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### このタスクについて

スキーマ・ファイルを追加または削除すると、インスタンスの構成ファイルがスキーマ項目で更新されます。

### 手順

1. インスタンス用の構成ツール を開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「スキーマ・ファイルの管理」をクリックします。

3. 「スキーマ・ファイルの管理」 ページで、実行する操作を選択します。
  - インスタンスの構成ファイルにスキーマ・ファイルを追加するには、以下の手順を実行します。
    - a. 「パスおよびファイル名」 フィールドに、スキーマ・ファイルの名前をパスとともに入力します。「参照」 をクリックすると、スキーマ・ファイル名およびロケーションを指定できます。
    - b. 「追加」 をクリックします。
  - インスタンスの構成ファイルのスキーマ・ファイルを削除するには、以下の手順を実行します。
    - a. 「現在のスキーマ・ファイル」 リストから、削除するスキーマ・ファイル名を選択します。
    - b. 「除去」 をクリックします。
    - c. 「スキーマ・ファイルの管理」 の確認ウィンドウで、「OK」 をクリックします。
4. 変更を適用するには、「OK」 をクリックします。
5. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」 をクリックしてください。
6. アクションを確認するには、「はい」 をクリックします。

## 次のタスク

ディレクトリー・サーバーを始動します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## コマンド行ユーティリティーを使用したスキーマ・ファイルの管理

コマンド行ユーティリティーを使用して、ディレクトリー・サーバー・インスタンスのスキーマ・ファイルを管理します。

### 始める前に

インスタンスのスキーマ・ファイルを管理するには、以下の手順を実行する必要があります。

- ディレクトリー・サーバーを停止します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### このタスクについて

スキーマ・ファイルを追加または削除すると、インスタンスの構成ファイルがスキーマ項目で更新されます。

### 手順

1. ディレクトリー・サーバー・インスタンス所有者としてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。

4. インスタンスのスキーマ・ファイルを管理するには、実行する操作を選択します。
  - インスタンスのスキーマ・ファイルを追加するには、以下の形式で **idscfgsch** コマンドを実行します。

```
idscfgsch -I instance_name -s schema_file.oc
```

- インスタンスのスキーマ・ファイルを削除するには、以下の形式で **idsucfgsch** コマンドを実行します。

```
idsucfgsch -I instance_name -s schema_file.oc
```

**idscfgsch** コマンドと **idsucfgsch** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 次のタスク

ディレクトリー・サーバーを始動します。177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 構成ツールを使用したスキーマ妥当性検査の構成

構成ツールを使用して、インスタンスのスキーマ妥当性検査を構成します。

### 始める前に

インスタンスに対してスキーマ妥当性検査規則を構成するには、以下の手順を実行する必要があります。

- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### このタスクについて

スキーマ妥当性検査を構成すると、その値でインスタンスの構成ファイルが更新されます。

### 手順

1. インスタンス用の構成ツールを開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「スキーマ・ファイルの管理」をクリックします。
3. 「スキーマ・ファイルの管理」ページの「スキーマ妥当性検査規則」領域で、以下のいずれかのスキーマ妥当性検査規則を構成対象として選択します。
  - LDAP バージョン 3 の厳密な妥当性検査を構成する場合は、「バージョン 3 (厳密な)」をクリックします。
  - LDAP バージョン 3 の厳密でない妥当性検査を構成する場合は、「バージョン 3 (厳密でない)」をクリックします。
  - LDAP バージョン 2 の検査を構成する場合は、「バージョン 2」をクリックします。
  - 妥当性検査が不要であることを指定する場合は、「なし」をクリックします。

4. 変更を適用するには、「OK」をクリックします。
5. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
6. アクションを確認するには、「はい」をクリックします。

## 次のタスク

ディレクトリー・サーバーを始動します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

---

## LDIF データ管理

ディレクトリー・データを使用するには、既存のインスタンスか、LDAP データ交換フォーマット (LDIF) ファイルから、ディレクトリー・サーバー・インスタンスにデータを追加する必要があります。

構成ツールを使用して、LDIF ファイルからデータをインポートしたり、データベースから LDIF ファイルへデータをエクスポートしたりすることができます。LDIF は、LDAP 項目をテキスト・フォームで表示するために使用されます。データをインポートすると、空のディレクトリー・データベースまたは項目が入っているデータベースに項目を追加できます。また、構成ツールを使用すると、データをディレクトリーに追加せずに LDIF ファイル内のデータを検証することができます。

DB2 データベースを使用して構成されたインスタンスにデータを追加することができます。ディレクトリー・データをプロキシ・サーバー・インスタンスに追加することはサポートされていないため、実行しないでください。

別のサーバー・インスタンスから LDIF データをインポートする場合は、サーバー・インスタンスを暗号的に同期する必要があります。サーバー通信におけるデータの暗号化および復号に必要な時間を削減するために、ディレクトリー・サーバー・インスタンス間での両方向の暗号化を同期する必要があります。暗号的に同期されていない LDIF データをインポートした場合、ファイル内の AES で暗号化された項目はインポートされません。両方向の暗号化の同期については「*Command Reference*」を参照してください。

サーバー・インスタンスが暗号的に同期されない場合、ソース・サーバーから LDIF ファイルをエクスポートするときに、ターゲット・サーバーの暗号化シードと暗号化ソルトを提供します。AES で暗号化されたデータはソース・サーバーの AES 鍵を使用して復号され、その後、ターゲット・サーバーの暗号化シード値および暗号化ソルト値を使用して暗号化されます。暗号化されたデータは、LDIF ファイルに保管されます。

データをインポートするには、プロセスを開始する前に、以下の要件を満たしている必要があります。

- LDIF データのインポートまたはエクスポートは、プロキシ・サーバー・インスタンスや、DB2 データベースを使用して構成されていないインスタンスではサポートされません。

- データのインポート先とするターゲット・サーバーに必要なサフィックスを追加します。228 ページの『サフィックス構成』を参照してください。
- データのインポート先とするターゲット・サーバーを停止する必要があります。

大量のデータをロードした場合 (**idsbulkload** を使用してデータベースにデータを取り込んだ場合など) は、データベースを最適化する必要があります。この操作により、データベースのパフォーマンスが向上する可能性があります。

以下のコマンド行ユーティリティーを使用して、LDIF データをインポート、エクスポート、または検証することもできます。

- LDIF ファイルからデータをインポートするには、**idsldif2db** または **idsbulkload** ユーティリティーを使用します。
- LDIF ファイルにデータをエクスポートするには、**idsdb2ldif** ユーティリティーを使用します。
- LDIF ファイルのデータの検証を行うには、**idsbulkload** ユーティリティーを使用します。

コマンド行ユーティリティーについて詳しくは、「*Command Reference*」を参照してください。

## 例

サーバーの暗号化ソルト値を取得するには、以下の形式で **idsldapsearch** コマンドを実行します。

```
idsldapsearch -h host_name -p port -D adminDN -w adminPWD ¥
-b "cn=crypto,cn=localhost" objectclass=* ibm-slapdCryptoSalt
```

```
ibm-slapdCryptoSalt=:SxaQ+.qdKor
```

`ibm-slapdCryptoSalt` 属性の等号 (=) の後にあるストリングが暗号化ソルトです。この例では、`:SxaQ+.qdKor` が暗号化ソルトです。

## 構成ツールを使用した LDIF データのインポート

構成ツールを使用して、LDIF ファイルからディレクトリー・サーバー・インスタンスにデータをインポートします。

### 始める前に

データを LDIF ファイルからインスタンスにインポートするには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。197 ページの『構成ツールを使用したインスタンスのデータベースの構成』を参照してください。
- 必要なサフィックス項目が構成されている必要があります。229 ページの『構成ツールを使用したサフィックスの追加』を参照してください。
- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 手順

1. インスタンス用の構成ツール を開始します。 190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「**LDIF タスク**」 > 「**LDIF データのインポート**」をクリックします。
3. 「**LDIF データのインポート**」ページで、以下の手順を実行します。
  - a. 「パスと **LDIF ファイル名**」フィールドに、データのインポート元となる LDIF ファイルのパスとファイル名を入力します。「参照」をクリックして、パス付きの LDIF ファイル名を指定することもできます。
  - b. データから後続スペースを除去する場合は、「**標準インポートまたは Bulkload の後続スペースの除去**」を選択します。
  - c. インポートする項目の数に基づいて適切なオプションを選択します。
    - **idsldif2db** ユーティリティを使用してデータをインポートする場合は、「**標準インポート**」をクリックします。このオプションは、LDIF ファイルに含まれている項目の数が少ない場合に使用します。
    - **idsbulkload** ユーティリティを使用してデータをインポートする場合は、「**Bulkload**」をクリックします。LDIF ファイル内の項目数が多い場合は、**idsbulkload** ユーティリティの方が **idsldif2db** ユーティリティよりも速くデータをインポートできます。
  - d. データをインポートするためのオプションとして「**Bulkload**」を選択した場合は、LDIF データに対して実行する妥当性検査のタイプを指定します。
    - 1) LDIF データがスキーマに従っているかどうかを確認する場合は、「**スキーマの検査を使用可能にする**」を選択します。
    - 2) LDIF データに適切な ACL が含まれているかどうかを確認する場合は、「**ACL 検査を使用可能にする**」を選択します。
  - e. インポート操作を開始するには、「**インポート**」をクリックします。
  - f. タスクの完了を確認するには、「**OK**」をクリックします。
  - g. LDIF ファイルのインポート操作に関して生成されたログを確認します。
  - h. ログをクリアするには、「**結果のクリア**」をクリックします。
  - i. 「**LDIF データのインポート**」ページを閉じるには、「**閉じる**」をクリックします。
4. 構成ツール ウィンドウを閉じるには、「**ファイル**」 > 「**終了**」をクリックしてください。
5. アクションを確認するには、「**はい**」をクリックします。

## 次のタスク

ディレクトリー・サーバーを始動します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。大量のデータをロードした場合 (**idsbulkload** を使用してデータベースにデータを取り込んだ場合など) は、データベースを最適化する必要があります。データベースの最適化について詳しくは、209 ページの『構成ツールを使用したデータベースの最適化』を参照してください。

## 構成ツールを使用した LDIF データの検証

構成ツールを使用して、データをデータベースに追加せずに LDIF ファイルをディレクトリー・サーバー・スキーマに対して検証します。

### 始める前に

LDIF ファイル内のデータをディレクトリー・サーバー・スキーマと検証するには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。197 ページの『構成ツールを使用したインスタンスのデータベースの構成』を参照してください。
- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### 手順

1. インスタンス用の構成ツール を開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「LDIF タスク」 > 「LDIF データのインポート」をクリックします。
3. 「LDIF データのインポート」ページで、以下の手順を実行します。
  - a. 「パスと LDIF ファイル名」フィールドに、データのインポート元となる LDIF ファイルのパスとファイル名を入力します。「参照」をクリックして、パス付きの LDIF ファイル名を指定することもできます。
  - b. 「データ妥当性検査のみ」をクリックします。
  - c. データ妥当性検査操作を開始するには、「インポート」をクリックします。
  - d. タスクの完了を確認するには、「OK」をクリックします。
  - e. データ妥当性検査操作に対して生成されたログを確認します。
  - f. ログをクリアするには、「結果のクリア」をクリックします。
  - g. 「LDIF データのインポート」ページを閉じるには、「閉じる」をクリックします。
4. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
5. アクションを確認するには、「はい」をクリックします。

### 次のタスク

ディレクトリー・サーバーを始動します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

## 構成ツールを使用した LDIF データのエクスポート

構成ツールを使用して、インスタンスから LDIF ファイルにディレクトリー・データをエクスポートします。

## 始める前に

インスタンスから LDIF ファイルにデータをエクスポートするには、インスタンスが以下の要件を満たしている必要があります。

- DB2 データベースにより構成されている Directory Server インスタンスが存在している必要があります。197 ページの『構成ツールを使用したインスタンスのデータベースの構成』を参照してください。
- インスタンスにディレクトリー項目が含まれている必要があります。

## 手順

1. インスタンス用の構成ツール を開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「LDIF タスク」 > 「LDIF データのエクスポート」をクリックします。
3. 「LDIF データのエクスポート」ページで、以下の手順を実行します。
  - a. 「パスと LDIF ファイル名」フィールドに、データのエクスポート先となる LDIF ファイルのパスとファイル名を入力します。「参照」をクリックして、パス付きの LDIF ファイル名を指定することもできます。
  - b. ファイルが存在する場合にファイルをデータで上書きするには、「ファイルが存在する場合に上書き」を選択します。
  - c. 運用属性 (creatorsName、createTimestamp、modifiersName、modifyTimestamp など) をエクスポートする場合は、「運用属性のエクスポート」を選択します。運用属性は、ディレクトリー項目の作成時または変更時にサーバーによって作成または変更されます。この属性には、項目を作成または変更したユーザーおよび項目を作成または変更した時刻に関する情報が含まれます。これらの項目は、ベース 64 エンコード・コントロールとして LDIF ファイルに保管されます。
  - d. Advanced Encryption Standard (AES) 対応の宛先サーバーにデータをインポートする場合に、そのサーバーとソース・サーバーの暗号が同期されていないときは、「AES 対応宛先サーバーにデータをエクスポート」を選択します。
  - e. 削除されてはいるがトゥームストーン・サブツリーにまだ保管されている項目をエクスポートする場合は、「削除された項目のエクスポート」を選択します。トゥームストーン・サブツリーについて詳しくは、IBM Security Directory Server 資料の『管理』セクションを参照してください。
  - f. 「AES 対応宛先サーバーにデータをエクスポート」を選択した場合、以下の値を指定します。
    - 「暗号化シード」フィールドに、宛先サーバーの暗号化シードを入力します。
    - 「暗号化ソルト」フィールドに、宛先サーバーの暗号化ソルトを入力します。暗号化ソルトの取得方法について詳しくは、236 ページの『LDIF データ管理』を参照してください。
  - g. LDIF ファイルにエクスポートする項目のフィルターを指定するには、「フィルター項目 DN」フィールドに有効な複製フィルターの DN を入力します。フィルターにより、基準を満たしている特定のデータベース項目が LDIF ファイルにエクスポートされます。複製フィルターについて詳しくは、IBM Security Directory Server 資料の『管理』セクションを参照してください。

- h. LDIF ファイルにコメントを追加する場合は、「コメント」フィールドにコメントを入力します。
  - i. 特定のサブツリーの下にある項目をエクスポートする場合は、「サブツリー DN」フィールドにサブツリーの DN を入力します。サブツリー DN は、LDIF ファイルに書き込まれるサブツリーの最上部の項目を識別します。このサブツリーとディレクトリー階層内でそれより下にあるすべての項目が、ファイルに書き込まれます。サブツリー DN を指定しない場合は、データベースに保管されているすべてのディレクトリー項目が出力ファイルに書き込まれます。これらの項目は、ディレクトリー・サーバー・インスタンスの構成ファイルに指定されているサフィックスに基づいて特定されます。
  - j. エクスポート操作を開始するには、「エクスポート」をクリックします。
  - k. タスクの完了を確認するには、「OK」をクリックします。
  - l. LDIF データのエクスポート操作に関して生成されたログを確認します。
  - m. ログをクリアするには、「結果のクリア」をクリックします。
  - n. 「LDIF データのエクスポート」ページを閉じるには、「閉じる」をクリックします。
4. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
  5. アクションを確認するには、「はい」をクリックします。

---

## Active Directory との同期

Microsoft Active Directory のユーザーとグループ・コンテナ内の項目を、IBM Security Directory Server インスタンスと同期することができます。データ同期は Active Directory からディレクトリー・サーバー・インスタンスへの片方向です。

注: IBM Security Directory Server バージョン 6.3.1 より、Active Directory との同期ソリューションは推奨されなくなりました。代わりに、LDAPSync ソリューションを使用してください。

構成ツールあるいは `idsadscfg` や `idsadsrun` などのコマンド行ユーティリティーを使用して、Active Directory との同期を構成して実行することができます。

注: IBM Security Directory Proxy Server 経由での Active Directory から IBM Security Directory Server インスタンスへのユーザーとグループの同期はサポートされません。

Active Directory との同期では、ユーザーおよびグループ・コンテナを同期するために IBM Security Directory Integrator を使用します。Active Directory との同期を使用する前に IBM Security Directory Integrator をインストールする必要があります。

以下のアクションを行うには、IBM Security Directory Integrator が必要です。

- 構成の実行
- 操作の開始、停止、再始動、およびモニター

Active Directory との同期を構成する際に以下の点について考慮する必要があります。

- Active Directory との同期アプリケーションと、IBM Security Directory Integrator は、ディレクトリー・サーバー・インスタンスと同じコンピューター上にある必要があります。
- Active Directory との同期では、ユーザーとグループ・コンテナーのみが同期されます。このツールでは、他のオブジェクトやコンテナーをディレクトリー・サーバー・インスタンスに同期することは行いません。
- このソリューションでは、ユーザー項目のグループ・メンバーシップも検査され、ユーザー項目は、Active Directory と同期されるインスタンス内のすべてのグループに追加されます。既存のユーザー項目がユーザー・コンテナーから除外されると、そのユーザー項目はインスタンスから削除されます。そのユーザー項目は、インスタンス内のすべてのグループからも削除されます。
- Active Directory との同期では、ネストされた組織単位 (ou) は同期されません。
- Active Directory の複数の属性をディレクトリー・サーバー・インスタンスの単一属性にマップすることはできません。
- Active Directory の userpassword 属性をディレクトリー・サーバー・インスタンスにマップすることはできません。ユーザー・パスワードは、このソリューションでは同期されません。
- Active Directory との同期では、Active Directory の 1 つ以上のユーザー・コンテナーからのユーザーおよびグループをディレクトリー・サーバーの単一の組織単位 (ou) に同期させることができます。ただし、このツールが Active Directory の複数のユーザー・コンテナーおよびグループ・コンテナーをディレクトリー・サーバーの複数の組織単位 (ou) に同期させることはありません。
- 分離文字としてセミコロン (;) を使用することにより、複数のユーザー・コンテナーが、ディレクトリー・サーバー内の単一の組織単位 (ou) と同期するように指定できます。別の文字を分離文字として使用することはサポートされません。分離文字としてセミコロン (;) を使用する場合、引数を引用符 (") で囲んでください。分離文字としてセミコロン (;) を使用する例を次に示します。  
"ou=SWUGroups,dc=adsync,dc=com;ou=STGGroups,dc=adsync,dc=com"。
- Active Directory の SAMAccountName 属性は、IBM Security Directory Server の \$dn 属性を構成するために使用されます。SAMAccountName 属性はドメインで固有であるため、複数の Active Directory ユーザー・コンテナーをディレクトリー・サーバーの単一の組織単位に同期させても競合は発生しません。
- このソリューションでは Active Directory とのセキュア接続がサポートされていますが、ディレクトリー・サーバー・インスタンスへのセキュア接続はサポートされません。
- Active Directory との同期を構成した後に、ディレクトリー・サーバー・インスタンスの管理者 DN、パスワード、またはその両方を変更した場合、Active Directory との同期を再構成する必要があります。
- Active Directory との同期の実行中に、Active Directory からのユーザー・コンテナーまたはグループ・コンテナーが変更された場合、変更された名前で Active Directory との同期を再構成する必要があります。再構成しないと、Active Directory との同期プログラムが実行されない場合があります。
- Active Directory との同期以外のツールを使用して IBM Security Directory Server ユーザーとグループを変更した場合、Active Directory との同期が正しく機能しないことがあります。

## Active Directory との同期の構成および実行

Active Directory のユーザー・コンテナーとグループ・コンテナーを IBM Security Directory Server インスタンスに同期させるには、Active Directory との同期を構成して実行します。

### 始める前に

Active Directory との同期を構成して実行するには、以下のソフトウェアをインストールする必要があります。

- IBM Security Directory Server
- IBM Security Directory Integrator

### 手順

1. IBM Security Directory Integrator をカスタム・パスにインストールした場合は、`IDS_LDAP_TDI_HOME` 環境変数にこのインストール・パスを設定します。

**注:** Windows システムでは、この環境変数にスペースと引用符を含まないインストール・パスを設定する必要があります。パスを指定するときは、短縮名を使用してください。

以下のパスは、IBM Security Directory Integrator のデフォルトのインストール・パスです。

#### AIX および Solaris

`/opt/IBM/TDI/V7.1`

**Linux** `/opt/ibm/TDI/V7.1`

#### Windows

`C:%Program Files%IBM%TDI%V7.1`

2. オプション: サンプルの `users.ldif` ファイルと `groups.ldif` ファイルを Active Directory にロードします。
3. **idsadscfg** コマンドを実行して、Active Directory との同期を構成します。構成ツールを実行して Active Directory との同期を構成することもできます。このコマンドによって `adsync_private.prop` ファイルと `adsync_public.prop` ファイルが作成されます。
4. `adsync_public.prop` ファイルを変更して、オプションの属性および SSL パラメーターをカスタマイズします。これらのファイルおよびセキュア通信については、IBM Security Directory Server 資料の『管理』セクションを参照してください。
5. **idsadsrun** コマンドを実行して、Active Directory との同期を開始します。コマンドから、完全同期を実行した後にリアルタイム同期を実行するか、またはリアルタイム同期を開始するかを尋ねるプロンプトが出されます。Active Directory との同期ツールによって、Active Directory 項目に対する変更が特定され、IBM Security Directory Server 内の項目と同期されます。
6. オプション: IBM Security Directory Integrator の「管理およびモニター・コンソールの開始」を実行して、同期の管理とモニターを行います。

## 構成ツールを使用した Active Directory との同期の構成

構成ツールを使用して、ディレクトリー・サーバー・インスタンスと Active Directory との同期を構成します。

### 始める前に

Active Directory との同期を構成するには、以下の要件を満たしている必要があります。

- IBM Security Directory Integrator のインストール。
- ディレクトリー・サーバーを停止します。191 ページの『構成ツールを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### 手順

1. インスタンス用の構成ツールを開始します。190 ページの『構成ツールの開始』を参照してください。
2. 左側のナビゲーション・ペインのタスク・リストから、「**Active Directory との同期**」をクリックします。
3. 「**Active Directory との同期: インスタンスの詳細**」ページで、IBM Security Directory Server インスタンスの構成の詳細を指定します。指定した情報は、`adsync_private.properties` ファイルと `adsync_public.properties` ファイルに保存されます。これらのファイルは、インスタンス・ホーム・ディレクトリーの `etc/tdisoldir` サブディレクトリーに保管されます。
4. 「**ディレクトリー・サフィックス**」フィールドに、Active Directory との同期に使用するディレクトリー・サーバー・サフィックスを入力します。「**LDAP URL**」フィールドには、ディレクトリー・サーバー・インスタンスの URL が取り込まれます。このフィールドは編集できません。
5. 「**グループ・コンテナ項目 DN**」フィールドに、Active Directory からグループをコピーする既存のコンテナの DN を入力します。グループおよびグループ内のユーザーのメンバーシップが Active Directory と IBM Security Directory Server の間で同期されます。Active Directory でユーザーをグループに追加したりグループから削除したりすると、IBM Security Directory Server インスタンス内の対応するグループに対して項目の追加または削除が行われます。
6. 「**ユーザー・コンテナ項目 DN**」フィールドに、Active Directory からユーザーをコピーする既存のコンテナの DN を入力します。
7. Active Directory に対して SSL 接続を使用する場合は、「**Active Directory に SSL 接続を使用**」を選択します。IBM Security Directory Server との SSL 接続はサポートされていません。Active Directory への SSL 接続を構成する手順については、IBM Security Directory Server 資料の『管理』セクションを参照してください。
8. 「**次へ**」をクリックします。「**Active Directory との同期: Active Directory の詳細**」ページが開きます。
9. 「**ホスト・アドレス**」フィールドに、Active Directory ドメイン・コントローラーのホスト名または IP アドレスを入力します。

10. 「ホスト・ポート」フィールドに、Active Directory が使用するポートを入力します。
11. 「ログイン名」フィールドに、IBM Security Directory Integrator が Active Directory へのバインドに使用するログイン名を入力します。 ログイン ID には、ディレクトリー・サーバー・インスタンスに伝搬する Active Directory 項目を読み取るために必要なアクセス権がなければなりません。
12. 「ログイン・パスワード」フィールドに、IBM Security Directory Integrator が Active Directory へのバインドに使用するパスワードを入力します。
13. 「検索ベース」フィールドに、インスタンスに対する変更の伝搬元となる Active Directory 内のサブツリーを入力します。 このサブツリーでのユーザー項目の変更が、ディレクトリー・サーバー・インスタンスに伝搬されます。 Active Directory グループ内の全ユーザーをインスタンスに伝搬する場合は、検索ベースを Active Directory 内の階層の最上位に設定します。
14. 「グループ・コンテナ項目 DN」フィールドに、インスタンスと同期させるグループが含まれている Active Directory コンテナ DN を入力します。
15. 「ユーザー・コンテナ項目 DN」フィールドに、インスタンスと同期させるユーザーが含まれている Active Directory コンテナ DN を入力します。
16. 「完了」をクリックします。「Active Directory との同期: 結果」ウィンドウが開きます。
17. Active Directory との同期の構成に関して生成されたログ・メッセージを確認します。
18. ログをクリアするには、「結果のクリア」をクリックします。
19. 「Active Directory との同期」ページを閉じるには、「閉じる」をクリックします。
20. 構成ツール ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックしてください。
21. アクションを確認するには、「はい」をクリックします。

## コマンド行ユーティリティーを使用した Active Directory との同期の構成

コマンド行ユーティリティー `idsadscfg` を使用して、ディレクトリー・サーバー・インスタンスと Active Directory との同期を構成します。

### 始める前に

Active Directory との同期を構成するには、以下の要件を満たしている必要があります。

- IBM Security Directory Integrator のインストール。
- ディレクトリー・サーバーを停止します。 177 ページの『コマンド行ユーティリティーを使用したディレクトリー・サーバーおよび管理サーバーの始動または停止』を参照してください。

### 手順

1. AIX、Linux、または Solaris では root としてログインし、Windows では管理者グループ・メンバーとしてログインします。

2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを IBM Security Directory Server インストール・ロケーション内の `sbin` サブディレクトリーに変更します。
4. インスタンスと Active Directory との同期を構成するには、以下の形式で **idsadscfg** コマンドを実行します。

```
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
```

**idsadscfg** コマンドについて詳しくは、「*Command Reference*」を参照してください。

## 次のタスク

**idsadsrun** コマンドを実行して、Active Directory との同期を開始します。

**idsadsrun** コマンドについて詳しくは、「*Command Reference*」を参照してください。

---

## 第 21 章 オペレーティング・システムの始動時におけるディレクトリー・サーバー・インスタンスの自動始動

コンピューターが保守またはアップグレードのためにシャットダウンされた後で再始動する際に、ディレクトリー・サーバー・インスタンスが自動的に始動するように構成できます。

ディレクトリー・サーバー・インスタンスの作成時に、インスタンスの作成に成功すると、管理サーバーが始動します。DB2 データベースを使用するディレクトリー・サーバーを始動するには、インスタンスの `ibmslapd` または `idsslapd` プロセスを開始する必要があります。

コンピューターを再始動するときは、インスタンスに関連付けている管理サーバーと `ibmslapd` プロセスの両方を開始する必要があります。ただし、インスタンスに関連付けられたサービスおよびプロセスが、オペレーティング・システム上で自動的に開始するように構成することができます。

オペレーティング・システムの始動時に AIX、Linux、または Solaris 上でディレクトリー・サーバー・インスタンスを始動するには、サーバー情報を使用して `/etc/inittab` ファイルを更新する必要があります。`inittab` ファイルは、システム始動時と通常操作中に開始する必要があるプロセスを指定します。ディレクトリー・サーバーに対する項目を、以下の形式で `inittab` ファイルに追加する必要があります。

```
id:runlevels:action:process
```

`inittab` ファイル内の属性は、以下の値を必要とします。

**id** この属性は、1 から 4 桁のファイル内の固有 ID を指定します。

### **runlevels**

`runlevels` 属性は、プロセスを自動的に始動させるオペレーティング・システムの `runlevel` モードを示します。AIX、Linux、または Solaris オペレーティング・システムの操作モードを示します。`runlevels` 属性の構成は、オペレーティング・システムによって異なります。特定の `runlevel` 構成の詳細については、オペレーティング・システムのマニュアルを参照してください。

**action** `action` はアクション・タイプを指定します。

### **process**

`process` 属性は、開始するプロセスを指定します。

---

## Windows でのディレクトリー・サーバー・インスタンスの自動始動の構成

Windows で、「サービス」ウィンドウを使用してディレクトリー・サーバーの自動始動を構成します。

## 始める前に

オペレーティング・システムを始動した後にディレクトリー・サーバー・インスタンスの自動始動を構成するには、コンピューターが以下の要件を満たしている必要があります。

- 通常モードで稼働可能なディレクトリー・サーバー・インスタンスがコンピューターに存在している必要があります。

## このタスクについて

Windows では、「サービス」ウィンドウまたは `idsslapd` コマンドを使用してディレクトリー・サーバー (`idsslapd` プロセス) を始動することができます。DB2 データベースを使用するディレクトリー・サーバー・インスタンスの場合は、ディレクトリー・サーバーに関連付けられたサービスが DB2 インスタンス・サービスに依存することを設定する必要があります。DB2 データベースを使用するディレクトリー・サーバー・インスタンスの場合は、DB2 を開始しないと `idsslapd` プロセスを開始できません。依存関係を設定しないまま、サーバーに関連付けられたサービスに対して「スタートアップの種類」フィールドを「自動」に設定すると、コンピューターを再始動したときにエラーが発生する可能性があります。プロキシ・サーバー・インスタンスの場合は、DB2 インスタンスに関連付けられたサービスとの依存関係を構成する必要はありません。

プロキシ・サーバー・インスタンスの場合は、ステップ 1、2、4、5、6 (249 ページ) を使用してください。

## 手順

1. 管理者グループ・メンバーとしてログインします。
2. 「サービス」ウィンドウを開くには、以下の手順を実行します。
  - a. 「スタート」 > 「ファイル名を指定して実行」をクリックします。
  - b. 「名前」フィールドに `services.msc` と入力します。
  - c. 「OK」をクリックします。
3. 自動始動させるディレクトリー・サーバー・インスタンスに関連付けられた DB2 サービス名を見つけます。サービス名は、DB2 - SDSV631DB2 - で開始されています。DB2 インスタンス名が DSRDBM01 である場合、項目は DB2 - SDSV631DB2 - DSRDBM01 です。このサービスをダブルクリックし、「表示名」フィールドで DB2 - SDSV631DB2 - の後に表示されている値を記録します。この例では、値は DSRDBM01 です。
4. 自動始動するディレクトリー・サーバー・インスタンスのサービスを見つけます。サービス名は、IBM Security Directory Server Instance 6.3.1 で始まります。インスタンス名が `dsrdbm01` である場合、項目は IBM Security Directory Server Instance 6.3.1 - `dsrdbm01` です。このサービスをダブルクリックし、「表示名」フィールドで IBM Security Directory Server Instance 6.3.1 - の後に表示されている値を記録します。この例では、インスタンス `dsrdbm01` に対するこの値が `idsslapd-dsrdbm01` となります。
5. 「IBM Security Directory Server Instance 6.3.1 - `dsrdbm01`」プロパティ・ウィンドウで、「スタートアップの種類」リストから「自動」を選択します。

6. 「OK」をクリックします。
7. 「サービス」ウィンドウを閉じるには、「ファイル」 > 「終了」をクリックします。
8. Windows レジストリーを開くには、以下の手順を実行します。
  - a. 「スタート」 > 「ファイル名を指定して実行」をクリックします。
  - b. 「名前」フィールドに `regedit` と入力します。
  - c. 「OK」をクリックします。
9. 左側のナビゲーション・ペインで、「マイ コンピューター」 > 「HKEY\_LOCAL\_MACHINE」 > 「SYSTEM」 > 「CurrentControlSet」 > 「Services」の順に移動します。
10. ディレクトリー・サーバー・インスタンスに関連付けられたサービスを見つけます。この例では、`idsslapd-dsrdm01` です。
11. インスタンスに関連付けられたサービスをクリックします。
12. ウィンドウの右側のペインで、`DependOnService` 属性をダブルクリックします。
13. 「複数行文字列の編集」ウィンドウで、**LanmanServer** の下にインスタンスに関連付けられた `DB2` サービス名を追加します。この例では、`DSRDBM01` です。
14. 「OK」をクリックします。これにより、`DB2` サービスへの依存関係が作成されます。
15. Windows レジストリーを閉じるには、「ファイル」 > 「終了」をクリックします。

## タスクの結果

コンピューターを再始動すると、ディレクトリー・サーバー・インスタンスが自動的に始動します。

---

## UNIX でのディレクトリー・サーバー・インスタンスの自動始動の構成

AIX、Linux、または Solaris でディレクトリー・サーバー・インスタンスの自動始動を構成するには、`/etc/inittab` ファイルのディレクトリー・サーバー項目を更新します。

### 始める前に

オペレーティング・システムを始動した後にディレクトリー・サーバー・インスタンスの自動始動を構成するには、コンピューターが以下の要件を満たしている必要があります。

- 通常モードで稼働可能なディレクトリー・サーバー・インスタンスがコンピューターに存在している必要があります。

### 手順

1. `root` ユーザーとしてログインします。

2. ディレクトリー・サーバー・インスタンスまたはプロキシ・サーバー・インスタンスの自動始動を構成するには、`/etc/inittab` ファイルに以下の項目を追加します。

- a. ディレクトリー・サーバー・インスタンスに関連付けられた `idsslapd` プロセスおよび管理サーバーを追加するには、以下の項目を追加します。

```
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
        Administration Server
```

`instance_name` 変数はインスタンス名で置き換えてください。

- b. プロキシ・サーバー・インスタンスに関連付けられた `idsslapd` プロセスおよび管理サーバーを追加するには、まずディレクトリー・サーバー・インスタンスを始動する必要があります。プロキシ・サーバーを始動する前に、DB2 データベースを使用するすべてのディレクトリー・サーバーを始動する必要があります。コンピューターにフル・ディレクトリー・サーバーとプロキシ・サーバーがある場合は、フル・ディレクトリー・サーバーの始動からプロキシ・サーバーの始動の間に遅延を追加します。以下の例では、`id:2345:wait` という形式の項目を `/etc/inittab` ファイルに追加することで遅延を導入しています。

```
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
        Administration 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
```

*instance\_name1* 変数と *instance\_name2* 変数は、ディレクトリー・サーバー・インスタンス名で置き換えてください。*proxy\_instance1* 変数は、プロキシ・サーバー・インスタンス名で置き換えてください。

## タスクの結果

これらの項目を `/etc/inittab` ファイルに追加すると、システム再始動後にディレクトリー・サーバー・インスタンス (フルまたはプロキシ) の自動始動が可能になります。



---

## 第 22 章 フィックスパックの計画

IBM Security Directory Server のフィックスパックおよびパッチについての情報を調べます。

AIX、Linux、Solaris、および HP-UX のパッチまたはフィックスパックは、ネイティブ・スクリプト・ベースのインストールで使用できます。

Windows の場合は、IBM Installation Manager ベースのパッチとフィックスパックを利用できます。

IBM Installation Manager ベースのパッチやフィックスパックは、GUI およびサイレント・インストール・モードでインストールできます。

IBM Installation Manager を使用して、以下の方法でインストール済みのパッチまたはフィックスパックのバージョンを判別できます。

- 「ファイル」 > 「インストール済みパッケージの表示」を選択します。
- IBM Installation Manager のインストール・ディレクトリーのツール・ディレクトリーから **imcl** コマンドを使用します。

UNIX システムの場合は、ネイティブ・パッケージのバージョンを調べて、インストール済みのパッチやフィックスパックのバージョンを判断します。

**注:** ネイティブ・ベースのフィックスパックをベース・バージョンに適用した後に、IBM Installation Manager で変更やアンインストールを行ってはなりません。ネイティブ・フィックスパックを適用した後は、追加の操作にはネイティブ・メソッドのみを使用してください。

---

### IBM Installation Manager を使用したフィックスパックのインストール

IBM Installation Manager を使用して、Microsoft Windows オペレーティング・システム上で、フィックスパックを適用したり、サービス・ストリーム機能拡張をインストールしたりします。

#### 始める前に

- フィックスパック戦略に関する情報を確認します。
- IBM Installation Manager バージョン 1.7.0 以降がインストールされていることを確認します。IBM Installation Manager の資料を確認してください。
- フィックスパックのインストールを開始する前に、IBM Security Directory Server のすべての実行中のプロセスおよびサービスを停止します。これは、手動で行うか、Installation Manager の「**ブロッキング・プロセスをすべて停止**」をクリックします。

## このタスクについて

フィックスパックは、既にインストールされているフィーチャーのみを更新します。まだシステムにインストールされていないフィーチャーをインストールするには、「変更」ウィザードを使用する前に、製品を更新する必要があります。

フィックスパックは、IBM DB2、IBM GSKit、IBM 組み込み WebSphere Application Server、および IBM Java Development Kit は更新しません。これらのソフトウェアを更新するには、「変更」ウィザードを使用します。

## 手順

1. フィックスパックを <http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631> からダウンロードします。
2. リポジトリ設定を IBM Installation Manager で設定します。
  - a. IBM Installation Manager を、「スタート」メニューから開始するには、「すべてのプログラム」 > 「IBM Installation Manager」 > 「IBM Installation Manager」をクリックします。
  - b. IBM Installation Manager の「開始」ページで、「ファイル」 > 「設定」をクリックします。
  - c. 「リポジトリ」ページで、「リポジトリの追加」をクリックします。
  - d. 「リポジトリの追加」ページで、以下のリポジトリ・ロケーションのいずれかを指定します。
    - IBM サポート Web サイトからダウンロードした製品パッケージが含まれているローカル・ディレクトリまたはリモート共有ドライブのファイル・パス。
    - Web サーバー上のリポジトリの URL。
  - e. 「OK」をクリックします。HTTPS または制限付きリポジトリ・ロケーションを指定した場合は、ユーザー ID とパスワードの入力を求めるプロンプトが表示されます。新規リポジトリ・ロケーションまたは変更されたリポジトリ・ロケーションがリストされます。
  - f. リポジトリへのアクセスを確認するには、「接続のテスト」をクリックします。
  - g. 「OK」をクリックして「リポジトリ」ページを終了します。
3. インストールを開始します。
  - IBM Security Directory Server バージョン 6.3.1 がシステムにインストールされていない場合、以下の手順を実行します。
    - a. IBM Installation Manager の「始動」ページで、「インストール」をクリックします。「インストール」ウィザードは、インストール・プロセスを導きます。
    - b. 35 ページの『IBM Installation Manager を使用したインストール』に説明されているインストール手順を最後まで行います。
  - IBM Security Directory Server バージョン 6.3.1 がシステムにインストールされている場合、フィックスパックを適用するために、以下の手順を実行します。

- a. IBM Installation Manager の「始動」ページで、「更新」をクリックします。「更新」ウィザードは、システムにインストールされたパッケージに適用可能な更新を検索します。
- b. 「IBM Security Directory Server」を選択します。インストール・ディレクトリーは、バージョン 6.3.1 がインストールされた場所であり、これは変更できません。「次へ」をクリックします。
- c. 更新対象の製品「IBM Security Directory Server」を選択し、適用する更新「バージョン 6.3.1.5」を選択します。「次へ」をクリックします。
- d. フィックスパックのライセンスに同意し、「次へ」をクリックします。
- e. 更新対象のフィーチャーがデフォルトで選択されています。システムに以前にインストールされているフィーチャーのみが、更新対象として表示されます。「次へ」をクリックします。

注: 選択内容のいずれかをクリアすると、そのフィーチャーにアンインストールのマークが付けられます。

**制約事項:** IBM DB2 がこのページにフィーチャーとしてリストされており、デフォルトで更新対象として選択されていますが、これは更新されません。IBM Installation Manager で「更新」ウィザードを選択した場合、前提条件ソフトウェアは更新されません。サーバーのフィーチャーがクリアされてしまうため、IBM DB2 の選択をクリアしないでください。

- f. 要約ページで、情報を確認し、「次へ」をクリックしてインストールを開始します。
4. インストールを検証します。IBM Installation Manager を使用した検証および該当するオペレーティング・システムの検証については、『91 ページの『第 13 章 IBM Security Directory Server の機能の検証』』のセクションを参照してください。

## 次のタスク

フィックスパックをアンインストールするには、パッケージを前のバージョンに戻す「ロールバック」ウィザードを使用します。

## フィックスパックのサイレント・モード・インストール

IBM Installation Manager を使用して、フィックスパックをサイレント・モードでインストールできます。

注: 更新用の応答ファイルに、まだインストールされていないフィーチャーを指定することはできません。指定すると、フィックスパックの更新プロセスが失敗します。

### フィックスパックをインストールするための新規応答ファイルの生成

製品のインストールに使用された応答ファイルがない場合、新しい応答ファイルを記録します。

1. IBM Installation Manager をシミュレーション・インストール・モードで開始します。以下に例を示します。

```
C:\Program Files\IBM\Installation Manager\ eclipse\IBMIM.exe
-record c:\SDS_6310\install_resp.xml -skipInstall agentDataLocation
```

ここで、

*agentDataLocation* ロケーションには、製品をインストールするためのデータが保管されます。

2. リポジトリ設定をバージョン 6.3.1.0 に設定します。
3. シミュレーション・インストール・プロセスを完了します。
4. IBM Installation Manager を閉じます。インストール・プロセスの応答ファイルが、製品をインストールせずに作成されます。
5. 以下のセクションのステップを完了します。

## 製品のインストール中に使用した応答ファイルによるインストール

1. `install_resp.xml` 応答ファイルを編集し、以下の変更を行います。
  - a. リポジトリのパスを、バージョン 6.3.1.5 のリポジトリ・パスで更新します。

```
<repository location='C:\SDS_6315\ibm_sds' />
```
  - b. オファリング・バージョンを 6.3.1.5 に更新します。

```
<offering id='com.ibm.security.directoryserver.v631' version='6.3.1.5' profile=.....
```
2. インストールをサイレント・モードで開始して、フィックスパックを適用します。以下に例を示します。

```
C:\Program Files\IBM\Installation Manager\ eclipse\tools\imcl.exe
input c:\SDS_6310\install_resp.xml -acceptLicense -showProgress
```

このコマンドでは、必要に応じて `-stopBlockingProcesses` オプションを使用し、フィックスパックのインストール前に、ブロック中のプロセスをすべてサイレントに停止することができます。

---

## ネイティブ・スクリプトを使用したフィックスパックのインストール

提供されているスクリプトをコマンド行から実行して、AIX、Linux、および Solaris システムでフィックスパックの適用またはサービス・ストリーム機能拡張のインストールを実行します。

### 始める前に

フィックスパック戦略に関する情報を確認します。

### 手順

1. フィックスパックを <http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631> からダウンロードします。
2. 十分な空きスペースがあるディレクトリーに、フィックス・アーカイブを解凍します。ディレクトリー名およびファイル名を含む、フィックスパックに関する詳細は、フィックスパックに含まれている *README* ファイルに記載されています。
3. IBM Security Directory Server に関連するすべてのクライアント・プロセスおよびサーバー・プロセスを停止します。デーモン・プロセス・セットには、ディ

レクトリー・サーバー、管理サーバー、プロキシ・サーバー (使用している場合)、およびすべてのカスタム LDAP アプリケーションが含まれます。使用中のプログラムおよびライブラリーは置換できません。トレースが有効になっている場合、**ldtrc off** を実行してオフにします。ディレクトリー・サーバー・インスタンスおよび管理プロセスの停止方法については、IBM Security Directory Server の資料の基本サーバー管理タスクを参照してください。

4. コマンド行で、フィックス・アーカイブを解凍したフォルダーへとディレクトリーを移動します。
5. 次のコマンドを **root** として実行します。

```
idsinstall -u -f
```

インストール・プログラムにより、システムに既にインストールされているコンポーネントの更新がインストールされます。

6. インストールを検証します。
  - a. インストール・プログラムが、インストールが成功したかどうかを示すメッセージを表示します。`/tmp/idsinstall_timestamp` にあるインストール・ログを確認します。
  - b. インストールが失敗した場合、または一部のパッケージがインストールされなかったことを示すメッセージが表示された場合、ログに示されているエラー (例えば、ディスク・スペースの不足) を解決します。その後、インストール・プログラムを再実行し、すべてのパッケージが正しくインストールされることを確認します。
  - c. パッケージのバージョン番号を確認して、すべてが正しいレベルであることを検証します。手順については、51 ページの『第 6 章 IBM Security Directory Server パッケージの照会』を参照してください。



---

## 第 23 章 IBM Security Directory Server のアンインストール: 概要

IBM Security Directory Server 製品のアンインストールについての概要、およびアンインストール前に考慮すべき重要な点について説明します。

### 始める前に

IBM Security Directory Server をアンインストールするには、AIX、Linux、Solaris、または HP-UX システムでは root 特権でログオンし、Windows システムでは管理者グループ・メンバーとしてログオンする必要があります。

### このタスクについて

IBM Security Directory Server をアンインストールしても、インスタンスおよびその構成ファイルは削除されません。

### 手順

1. IBM Security Directory Server クライアントまたはサーバーのすべてのプロセス (ディレクトリー・サーバー、管理デーモン、カスタムの LDAP アプリケーションを含む) を停止します。使用中のプログラムおよびライブラリーは置換できません。トレースが設定されている場合は、**ldtrc off** コマンドを実行してトレースをオフにします。
2. IBM Security Directory Server のインストールのモードおよびオペレーティング・システムに基づいて、同じモードを使用して IBM Security Directory Server をアンインストールしてください。IBM Security Directory Server パッケージのアンインストールで使用可能な方法は、以下のとおりです。
  - a. GUI アンインストール・プログラム。
  - b. オペレーティング・システムのユーティリティー。Linux システム上のパッケージ名は、GA バージョンと更新では若干の違いがあります。例えば、xSeries Linux 上の GA バージョンのベース・クライアントのパッケージ名は、`idsldap-cltbase63-6.3.0-0.i386.rpm` です。**rpm -qa** コマンドを使用するとすべてのパッケージをリスト表示できます。
3. IBM Security Directory Server のアンインストール後に、すべての IBM Security Directory Server パッケージが正常に削除されたかどうかを照会します。詳細については、51 ページの『第 6 章 IBM Security Directory Server パッケージの照会』を参照してください。

### 関連情報:



<http://www-01.ibm.com/support/knowledgecenter/SSVJJU/welcome>

詳しくは、IBM Security Directory Server 製品資料の『インストールと構成』セクションにある『IBM Security Directory Server のアンインストール』トピックを参照してください。



---

## 第 24 章 IBM Security Directory Server および相互要件ソフトウェアのアンインストール

コンピューターを他の目的で使用するか、コンピューターを廃止することを計画している場合、IBM Security Directory Server およびその相互前提条件ソフトウェアの削除が必要になることがあります。

IBM Security Directory Server のアンインストールには、IBM Installation Manager またはオペレーティング・システムのユーティリティを使用することができます。アンインストールでは、インストールで使用したのと同じモードを使用する必要があります。インストールとアンインストールの両方について IBM Installation Manager を使用するか、インストールとアンインストールの両方についてオペレーティング・システムのユーティリティを使用する必要があります。インストールとアンインストールを行う際に、両方のモードを混用しないでください。

IBM Security Directory Server をコンピューターから削除する場合、アンインストール前に以下の条件について考慮してください。

1. 全てのIBM Security Directory Server クライアントとサーバーのプロセスを停止する必要があります。
  - ディレクトリー・サーバー
  - 管理サーバー
  - LDAP トレース
  - Web 管理ツールおよびそれに関連付けられているアプリケーション・サーバー
  - カスタム LDAP アプリケーション
2. コンピューター上で IBM Security Directory Server のインストールを再実行する計画がある場合、ディレクトリー・サーバー・インスタンスを削除したり、DB2 データベースをインスタンスから構成解除したりする必要はありません。IBM Security Directory Server をコンピューターから削除する場合、ディレクトリー・サーバー・インスタンスはユーザーが手動で削除するか構成解除しない限り、そのままの状態が残されます。
3. IBM Security Directory Server のインストール中に作成された `idsldap` ユーザーとグループは、アンインストール後にシステムに残されます。AIX、Linux、または Solaris から IBM Security Directory Server をアンインストールする前に、追加の条件を考慮する必要があります。
  - 定義された `idsldap` ユーザーとグループが必要ない場合、オペレーティング・システムのユーティリティを使用して、これらを削除してください。`idsldap` ユーザーとグループは、プロキシ・サーバーとフル・ディレクトリー・サーバーの両方で必要であり、IBM Security Directory Server をインストールしている場合は、これらがコンピューター上に存在する必要があります。
  - `idsldap` ユーザーを削除して、ユーザーのホーム・ディレクトリーを削除しない場合、IBM Security Directory Server のインストール中に `idsldap` ユーザーが作成されるときに問題が発生することがあります。したがって、`idsldap` ユ

ユーザーを削除する場合は、`idsldap` ユーザーのホーム・ディレクトリーを必ず削除してください。`userdel` コマンドを使用して `idsldap` ユーザーを削除する場合は、`-r` パラメーターを使用して、ホーム・ディレクトリーを必ず削除してください (`userdel -r idsldap`)。

4. Windows の場合、IBM Security Directory Server のアンインストール中に管理サーバー・サービスおよびディレクトリー・サーバー・サービスが除去されます。これらのサービスは IBM Security Directory Server のインストール中に置き換えられません。`idsslapd` コマンドを使用してサーバー・サービスを追加し、`idsdiradm` コマンドを使用して管理サーバー・サービスを追加することができます。`idsslapd` および `idsdiradm` コマンドについては、「*IBM Security Directory Server Command Reference*」を参照してください。

---

## IBM Installation Manager を使用したアンインストール

IBM Security Directory Server のインストールに IBM Installation Manager を使用した場合、IBM Security Directory Server およびそのコンポーネントのアンインストールには、IBM Installation Manager を使用します。

IBM Installation Manager を使用して IBM Security Directory Server をアンインストールするとき、インストールされている IBM Security Directory Server およびそのすべての相互前提条件ソフトウェアがプログラムによって削除されます。IBM Installation Manager を使用してアンインストールするとき、IBM Security Directory Server の機能を選択的に削除することはできません。

IBM Security Directory Server で提供されている IBM DB2 をインストールした場合、IBM DB2 を正しくアンインストールするには、DB2 のコピーで作成されたすべての DB2 インスタンスを削除する必要があります。DB2 のコピーで作成された DB2 インスタンスがコンピューターに残っていると、IBM Security Directory Server のアンインストール中に、DB2 が削除されません。IBM Installation Manager は、そのログ・ファイルにエラー・メッセージを記録します。

IBM Security Directory Server およびそのコンポーネントをインストール、変更、またはアンインストールするには、IBM Installation Manager またはオペレーティング・システムのユーティリティーのいずれかを使用する必要があります。IBM Security Directory Server およびそのコンポーネントをインストール、変更、またはアンインストールするときに、IBM Installation Manager とオペレーティング・システムのユーティリティーの両方を使用してはいけません。

## IBM Installation Manager を使用したアンインストール

IBM Security Directory Server のインストールに IBM Installation Manager を使用していた場合、IBM Security Directory Server のアンインストールには IBM Installation Manager を使用します。

### 始める前に

全てのIBM Security Directory Server クライアントとサーバーのプロセスを停止する必要があります。

- ディレクトリー・サーバー
- 管理サーバー

- LDAP トレース
- カスタム LDAP アプリケーション

使用中のプロセスがある場合は、プログラムやライブラリーを削除できません。

## 手順

1. IBM Installation Manager を始動します。
  - AIX および Linux:
    - a. コマンド行ウィンドウを開き、IBM Installation Manager が置かれているディレクトリーに変更します。IBM Installation Manager のデフォルトのインストール・ロケーションは、以下のディレクトリーです。  
`opt/IBM/InstallationManager/eclipse`
    - b. 以下のコマンドを実行します。  
`./IBMIM`
  - Microsoft Windows:
    - a. 「スタート」 > 「すべてのプログラム」 > 「IBM Installation Manager」 > 「IBM Installation Manager」をクリックします。
2. 「アンインストール」をクリックします。
3. 該当のバージョンの「IBM Security Directory Server」を選択してから、「次へ」をクリックします。
4. 「パッケージのアンインストール」ウィンドウで、アンインストール対象として選択したパッケージを確認します。

**重要:** インストール中に既存のバージョンの DB2 または GSKit を使用して続行することを選択した場合、IBM Installation Manager は機能項目を使用して、レジストリーを更新します。「既存の DB2/GSKit を使用して続行 (Continue with the existing)」オプションを使用してインストールされた機能を削除する場合、Installation Manager は以下のアクションを実行します。

- IBM Installation Manager レジストリーから機能項目を削除します。
- コンピューターから機能をアンインストールしません。

IBM Installation Manager でインストールされた DB2 コピーで作成した DB2 インスタンスが存在する場合は、IBM Security Directory Server をアンインストールすることはできません。このような場合は、DB2 インスタンスを手動で削除してからやり直す必要があります。DB2 インスタンスを削除する前に、データベースのバックアップを行うことをお勧めします。

5. 「アンインストール」をクリックします。アンインストールが終了すると、IBM Installation Manager では、アンインストールが成功したか失敗したかを示します。
6. オプション: アンインストール中にエラーが発生した場合は、「ログ・ファイルの表示」をクリックして、詳細を表示します。詳細については、49 ページの『第 5 章 IBM Installation Manager のログ・ファイル』を参照してください。
7. 「完了」をクリックします。
8. 「ファイル」 > 「終了」をクリックします。

## タスクの結果

IBM Installation Manager によって、IBM Security Directory Server とそのコンポーネントがアンインストールされます。

## 応答ファイルを使用したサイレント・アンインストール

応答ファイルを使用して、IBM Security Directory Server のコンポーネントをサイレントにアンインストールします。

### 始める前に

IBM Security Directory Server パッケージのサイレント・アンインストールには、IBM Installation Manager バージョン 1.7.0 以降が必要です。

### このタスクについて

デフォルトの応答ファイルを使用するか、またはカスタマイズした応答ファイルを記録し、サイレント・アンインストールの入力ファイルとして使用できます。

### 手順

1. 管理者としてシステムにログインします。
2. IBM Installation Manager のインストール・ロケーションにある **IBMIM** コマンドにアクセスします。

オペレーティング・システム	IBMIM コマンドのデフォルト・ロケーション:
Microsoft Windows	C:\Program Files\IBM\InstallationManager\ eclipse
AIX および Linux	/opt/IBM/InstallationManager/eclipse

3. オプション: **IBMIM** コマンドを実行して、サイレント・アンインストール用の応答ファイルを記録します。
  - a. 各種オペレーティング・システムで、以下のコマンドを実行します。

#### Microsoft Windows

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

#### AIX および Linux

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

このコマンドによって、IBM Installation Manager が開きます。

- b. IBM Security Directory Server のアンインストールの記録を実行します。詳細については、2 (263 ページ)を参照してください。
4. **IBMIM** コマンドを実行して、応答ファイルを入力とするサイレント・アンインストールを開始します。

オペレーティング・システム	実行するコマンド:
Microsoft Windows	IBMIM.exe -silent -input <i>path_name</i> uninstsll_responseFile.xml -noSplash
AIX および Linux	./IBMIM -silent -input <i>path_name</i> /uninstall_responseFile.xml -noSplash

5. アンインストールの要約およびログ・ファイルを確認します。

オペレーティング・システム	デフォルトのログ・パス:
Microsoft Windows	C:\ProgramData\IBM\InstallationManager\logs
AIX および Linux	/var/ibm/InstallationManager/logs/

6. IBM Security Directory Server パッケージがアンインストールされたかどうかを検証します。

オペレーティング・システム	パッケージの確認:
Microsoft Windows	92 ページの『IBM Security Directory Server 機能の Windows 上での検証』を参照してください。
AIX および Linux	93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。

## タスクの結果

IBM Installation Manager によって、IBM Security Directory Server コンポーネントがサイレントにアンインストールされます。

## imcl uninstall コマンドを使用したサイレント・アンインストール

**imcl uninstall** コマンドを使用して IBM Security Directory Server コンポーネントのサイレント・アンインストール手順を実行します。

### 始める前に

IBM Security Directory Server パッケージのサイレント・インストールには、IBM Installation Manager バージョン 1.7.0 以降が必要です。

### このタスクについて

**imcl uninstall** コマンドを使用して、サイレント・モードで IBM Security Directory Server をアンインストールできます。

### 手順

1. 管理者としてシステムにログインします。
- 2.

3. <IBM\_Installation\_Manager\_install\_dir>/eclipse/tools ディレクトリーから **imcl listInstalledPackages** コマンドを実行します。

オペレーティング・システム	実行するコマンド
Microsoft Windows	imcl.exe listInstalledPackages
AIX および Linux	./imcl listInstalledPackages

このコマンドは、IBM Installation Manager によってインストールされるすべてのパッケージをリストします。

4. **imcl uninstall com.ibm.security.directoryserver.v631\_6.3.1.0** を実行します。上記のコマンド **imcl listInstalledPackages** の出力として表示される Security Directory Server 項目を使用します。

オペレーティング・システム	実行するコマンド:
Microsoft Windows	imcl.exe uninstall com.ibm.security.directoryserver.v631_6.3.1.0
AIX および Linux	./imcl uninstall com.ibm.security.directoryserver.v631_6.3.1.0

## タスクの結果

IBM Installation Manager によって、IBM Security Directory Server コンポーネントがサイレントにアンインストールされます。

## オペレーティング・システムのユーティリティーを使用した IBM Security Directory Server のアンインストール

IBM Security Directory Server のインストールにオペレーティング・システムのユーティリティーを使用した場合、IBM Security Directory Server のアンインストールにはオペレーティング・システムのユーティリティーを使用します。

AIX、Linux、Solaris、および HP-UX オペレーティング・システムを使用するコンピューターから IBM Security Directory Server をアンインストールするには、オペレーティング・システムのユーティリティーを使用することができます。Windows の場合、IBM Security Directory Server のインストールおよびアンインストールには、IBM Installation Manager を使用する必要があります。262 ページの『IBM Installation Manager を使用したアンインストール』を参照してください。

オペレーティング・システムのユーティリティーを使用して IBM Security Directory Server をアンインストールするとき、IBM Security Directory Server はプログラムによって削除されます。オペレーティング・システムのユーティリティーを使用してアンインストールする場合は、IBM Security Directory Server の各機能を選択的に削除することができます。

IBM Security Directory Server をアンインストールする前に、IBM Security Directory Server のクライアントとサーバーのプロセスをすべて停止する必要があります。

- ディレクトリー・サーバー
- 管理サーバー

- LDAP トレース
- Web 管理ツールおよびそれに関連付けられているアプリケーション・サーバー
- カスタム LDAP アプリケーション

DB2 データベースを使用するディレクトリー・サーバー・インスタンスが作成および構成されている場合、IBM Security Directory Server をアンインストールするためにオペレーティング・システムのユーティリティを使用するとき、これらは削除されません。

## AIX ユーティリティを使用したアンインストール

AIX コマンド行ユーティリティを使用して、AIX システムから IBM Security Directory Server をアンインストールできます。

IBM Security Directory Server をアンインストールするには、以下のいずれかのユーティリティを使用できます。

**SMIT** 望ましいアンインストール方法は、このユーティリティを使用する方法です。詳細については、『SMIT を使用したアンインストール』を参照してください。

### **installp**

詳細については、268 ページの『installp を使用したアンインストール』を参照してください。

## SMIT を使用したアンインストール

**smit** コマンドを使用して、IBM Security Directory Server の AIX システムからのアンインストールを実行します。

### 始める前に

全てのIBM Security Directory Server クライアントとサーバーのプロセスを停止する必要があります。

- ディレクトリー・サーバー
- 管理サーバー
- LDAP トレース
- Web 管理ツールおよびそれに関連付けられているアプリケーション・サーバー
- カスタム LDAP アプリケーション

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. **smit** コマンドを実行します。「ソフトウェアのインストールおよび保守」ウィンドウが開きます。
4. 「ソフトウェアのインストールおよび保守」 > 「ソフトウェアの保守およびユーティリティ」を選択します。
5. 「インストールされたソフトウェアの除去」を選択します。

6. 「ソフトウェア名」フィールドで、**F4** を押してインストールされているソフトウェアのリストを表示します。このフィールドに `idsldap` という値を指定して、すべての IBM Security Directory Server パッケージをリストすることができます。
7. 削除するパッケージを選択して、Enter キーを押します。

## タスクの結果

SMIT ユーティリティーによって、IBM Security Directory Server が AIX システムから削除されます。すべての IBM Security Directory Server パッケージの削除を選択していた場合、このユーティリティーによって IBM Security Directory Server のインストール・ディレクトリーの `/opt/IBM/ldap/V6.3.1` も AIX システムから削除されます。

## 次のタスク

IBM Security Directory Server のアンインストールが正常に終了したかを検証します。詳細については、93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。

## installp を使用したアンインストール

`installp` コマンドを使用して、IBM Security Directory Server の AIX システムからのアンインストールを実行します。

## 始める前に

全てのIBM Security Directory Server クライアントとサーバーのプロセスを停止する必要があります。

- ディレクトリー・サーバー
- 管理サーバー
- LDAP トレース
- Web 管理ツールおよびそれに関連付けられているアプリケーション・サーバー
- カスタム LDAP アプリケーション

## 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 次のコマンドを実行して、削除する IBM Security Directory Server パッケージを決定します。

```
lslpp -l 'idsldap*'
```

4. IBM Security Directory Server パッケージを削除するには、以下のコマンドを実行します。

```
installp -u package_name
```

IBM Security Directory Server を完全に削除するには、すべての IBM Security Directory Server パッケージを削除してください。IBM Security Directory Server のアンインストールの場合、インストールの逆順でパッケージを指定する必要があります。シーケンスについて詳しくは、74 ページの『AIX システムへのイン

ストール用パッケージ』を参照してください。 `idsldap.ent631` パッケージを削除するには、次のコマンドを実行します。

```
installp -u idsldap.ent631
```

## 次のタスク

IBM Security Directory Server のアンインストールが正常に終了したかを検証します。詳細については、93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。

## Linux ユーティリティを使用したアンインストール

Linux コマンド行ユーティリティを使用して、Linux システムから IBM Security Directory Server をアンインストールできます。

IBM Security Directory Server パッケージの名前は、さまざまなオペレーティング・システムおよびアーキテクチャーのコンピューターごとに異なります。アンインストールする前に、インストールされている IBM Security Directory Server パッケージを確認する必要があります。

## Linux ユーティリティを使用したアンインストール

`rpm` コマンドを使用して、IBM Security Directory Server の Linux システムからのアンインストールを実行します。

### 始める前に

全ての IBM Security Directory Server クライアントとサーバーのプロセスを停止する必要があります。

- ディレクトリー・サーバー
- 管理サーバー
- LDAP トレース
- Web 管理ツールおよびそれに関連付けられているアプリケーション・サーバー
- カスタム LDAP アプリケーション

### このタスクについて

次の例は、IBM Security Directory Server パッケージの AMD64 Opteron/EM64T Linux システムからのアンインストールを示しています。System z、System i、System p、または System x の Linux の場合は、該当するパッケージ名で置き換える必要があります。

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 次のコマンドを実行して、削除する IBM Security Directory Server パッケージを決定します。

```
rpm -qa | grep -i idsldap
```

4. IBM Security Directory Server パッケージを削除するには、以下のコマンドを実行します。

```
rpm -ev package_name
```

IBM Security Directory Server を完全に削除するには、すべての IBM Security Directory Server パッケージを削除してください。IBM Security Directory Server のアンインストールの場合、インストール・シーケンスの逆順でパッケージを指定する必要があります。シーケンスについて詳しくは、80 ページの『Linux システムへのインストール用パッケージ』を参照してください。

idsldap-srv64bit631-6.3.1-0.x86\_64.rpm パッケージを削除するには、以下のコマンドを実行します。

```
rpm -ev idsldap-srv64bit631-6.3.1-0.x86_64.rpm
```

## 次のタスク

IBM Security Directory Server のアンインストールが正常に終了したかを検証します。詳細については、93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。

## Solaris ユーティリティーを使用したアンインストール

Solaris コマンド行ユーティリティーを使用して、Solaris システムから IBM Security Directory Server をアンインストールできます。

Solaris SPARC システムと Solaris X64 システムでは、IBM Security Directory Server のパッケージ名は同じです。

## Solaris ユーティリティーを使用したアンインストール

**pkgrm** コマンドを使用して、IBM Security Directory Server の Solaris システムからのアンインストールを実行します。

## 始める前に

全てのIBM Security Directory Server クライアントとサーバーのプロセスを停止する必要があります。

- ディレクトリー・サーバー
- 管理サーバー
- LDAP トレース
- Web 管理ツールおよびそれに関連付けられているアプリケーション・サーバー
- カスタム LDAP アプリケーション

## 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 次のコマンドを実行して、削除する IBM Security Directory Server パッケージを決定します。

```
pkginfo | grep -i IDS1
```

4. IBM Security Directory Server パッケージを削除するには、以下のコマンドを実行します。

```
pkgrm package_name
```

IBM Security Directory Server を完全に削除するには、すべての IBM Security Directory Server パッケージを削除してください。IBM Security Directory Server のアンインストールの場合、インストール・シーケンスの逆順でパッケージを指定する必要があります。シーケンスについて詳しくは、84 ページの『Solaris システムへのインストール用パッケージ』を参照してください。IDS1ent631 パッケージを削除するには、以下のコマンドを実行します。

```
pkgrm IDS1ent631
```

### 次のタスク

IBM Security Directory Server のアンインストールが正常に終了したかを検証します。詳細については、93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。

## HP-UX ユーティリティーを使用したアンインストール

HP-UX コマンド行ユーティリティーを使用して、HP-UX システムから IBM Security Directory Server をアンインストールできます。

HP-UX (Itanium) コンピューター上では、IBM Security Directory Server クライアント・パッケージのみがサポートされています。

### HP-UX ユーティリティーを使用したアンインストール

**swremove** コマンドを使用して、IBM Security Directory Server の HP-UX システムからのアンインストールを実行します。

### 始める前に

すべての IBM Security Directory Server クライアント・プロセスを停止する必要があります。

- LDAP トレース
- カスタム LDAP アプリケーション

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 次のコマンドを実行して、削除する IBM Security Directory Server パッケージを決定します。

```
swlist | grep -i idsldap
```

4. IBM Security Directory Server パッケージを削除するには、以下のコマンドを実行します。

```
swremove package_name
```

IBM Security Directory Server を完全に削除するには、すべての IBM Security Directory Server パッケージを削除してください。IBM Security Directory Server のアンインストールの場合、インストール・シーケンスの逆順でパッケージを指定する必要があります。シーケンスについて詳しくは、88 ページの『HP-UX

Itanium システムへのインストール用パッケージ』を参照してください。  
idsldap.cltjava631.depot パッケージを削除するには、以下のコマンドを実行  
します。

```
swremove idsldap.cltjava631.depot
```

## 次のタスク

IBM Security Directory Server のアンインストールが正常に終了したかを検証しま  
す。詳細については、93 ページの『IBM Security Directory Server パッケージの検  
証』を参照してください。

---

## DB2 コマンドを使用した IBM DB2 のアンインストール

IBM Security Directory Server で提供された IBM DB2 のコピーを手動でインスト  
ールした場合、IBM DB2 をコンピューターから削除するには DB2 コマンドを使用  
してください。

IBM Security Directory Server のインストール中に IBM Installation Manager を使用  
して IBM DB2 のコピーをインストールした場合、IBM DB2 は事前定義されたロ  
ケーションにインストールされます。デフォルト・ロケーションについて詳しく  
は、30 ページの『デフォルトのインストール・ロケーション』を参照してくださ  
い。IBM Installation Manager を使用して IBM DB2 のコピーをインストールした場  
合、IBM DB2 のアンインストールには IBM Installation Manager を使用する必要が  
あります。

IBM DB2 のコピーに対する DB2 インスタンスがコンピューターにある場合、IBM  
DB2 をアンインストールする前に DB2 インスタンスを手動でドロップする必要が  
あります。アンインストールの前に DB2 データベースおよびデータをバックアッ  
プすることをお勧めします。

DB2 コマンドを使用して IBM DB2 をカスタム・ロケーションに手動インストール  
した場合、IBM DB2 をアンインストールするには DB2 コマンドを使用してくださ  
い。AIX、Linux、および Solaris の場合、IBM DB2 をアンインストールするには、  
*DB2\_installation\_location/install/* ディレクトリーにある **db2\_deinstall** コマ  
ンドを実行します。Windows の場合、IBM DB2 をアンインストールするには、  
*DB2\_instalaton\_location\bin* ディレクトリーにある **db2unins** コマンドを実行し  
てください。IBM DB2 のアンインストールについて詳しくは、IBM DB2 製品資料  
(<http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome>) を参照してくださ  
い。

---

## オペレーティング・システムのユーティリティーを使用した IBM Global Security Kit のアンインストール

IBM Global Security Kit (GSKit) のインストールにオペレーティング・システムの  
ユーティリティーを使用した場合、GSKit のアンインストールにはオペレーティ  
ング・システムのユーティリティーを使用します。

AIX、Linux、Solaris、および HP-UX オペレーティング・システムを使用するコンピューターから GSKit をアンインストールするには、オペレーティング・システムのユーティリティーを使用することができます。

Windows では、インストール済みバージョンの GSKit を IBM Installation Manager と一緒にインストール中に使用することを選択した場合に限り、GSKit の手動アンインストールを実行できます。IBM Security Directory Server がコンピューターにインストールされている場合、これが使用されている間に GSKit を削除しないでください。最新バージョンの GSKit を使用する場合、IBM Installation Manager を使用して GSKit 機能を変更し、レジストリーからこれを削除する必要があります。その後、GSKit のアンインストールを実行できます。

## SMIT を使用した IBM Global Security Kit のアンインストール

**smit** コマンドを使用して、IBM Global Security Kit (GSKit) の AIX システムからのアンインストールを実行します。

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. **smit** コマンドを実行します。「ソフトウェアのインストールおよび保守」ウィンドウが開きます。
4. 「ソフトウェアのインストールおよび保守」 > 「ソフトウェアの保守およびユーティリティー」を選択します。
5. 「インストールされたソフトウェアの除去」を選択します。
6. 「ソフトウェア名」フィールドで、**F4** を押してインストールされているソフトウェアのリストを表示します。このフィールドに GSKit という値を指定して、すべての GSKit パッケージをリストすることができます。
7. 「従属ソフトウェアを除去する」の値を「YES」に設定して、除去する製品に依存する更新とソフトウェア製品を除去します。
8. 削除するパッケージを選択して、Enter キーを押します。
9. GSKit のアンインストールが正常に終了したかを検証します。

```
lslpp -l 'GSK*'
```

## installp を使用した IBM Global Security Kit のアンインストール

**installp** コマンドを使用して、IBM Global Security Kit (GSKit) の AIX システムからのアンインストールを実行します。

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 次のコマンドを実行して、削除する GSKit パッケージを決定します。

```
lslpp -l 'GSK*'
```

4. GSKit パッケージを削除するには、以下のコマンドを実行します。

```
installp -u package_name
```

GSKit を完全に除去するには、同じバージョンのすべての GSKit を除去してください。GSKit のアンインストールの場合、まず GSKit SSL パッケージを削除し、その後 GSKit crypt パッケージを削除する必要があります。パッケージの GSKit8.gskssl64.ppc.rte と GSKit8.gskcrypt64.ppc.rte を削除するには、次のコマンドを実行します。

```
installp -u GSKit8.gskssl64.ppc.rte  
installp -u GSKit8.gskcrypt64.ppc.rte
```

5. GSKit のアンインストールが正常に終了したかを検証します。

```
ls1pp -l 'GSK*'
```

## Linux ユーティリティーを使用した IBM Global Security Kit のアンインストール

**rpm** コマンドを使用して、IBM Global Security Kit (GSKit) の Linux システムからのアンインストールを実行します。

### このタスクについて

次の例は、GSKit パッケージの AMD64 Opteron/EM64T Linux システムからのアンインストールを示しています。System z、System i、System p、または System x の Linux の場合は、該当するパッケージ名で置き換える必要があります。

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 次のコマンドを実行して、削除する GSKit パッケージを決定します。

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

4. GSKit パッケージを削除するには、以下のコマンドを実行します。

```
rpm -ev package_name
```

GSKit を完全に除去するには、同じバージョンのすべての GSKit を除去してください。GSKit のアンインストールの場合、まず GSKit SSL パッケージを削除し、その後 GSKit crypt パッケージを削除する必要があります。パッケージの gskssl64-8.0-14.26.x86\_64 と gskcrypt64-8.0-14.26.x86\_64 を削除するには、次のコマンドを実行します。

```
rpm -ev gskssl64-8.0-14.26.x86_64  
rpm -ev gskcrypt64-8.0-14.26.x86_64
```

5. GSKit のアンインストールが正常に終了したかを検証します。

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

## Solaris ユーティリティーを使用した IBM Global Security Kit のアンインストール

**pkgrm** コマンドを使用して、IBM Global Security Kit (GSKit) の Solaris システムからのアンインストールを実行します。

## 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 次のコマンドを実行して、削除する GSKit パッケージを決定します。

```
pkginfo | grep -i gsk
```

4. GSKit パッケージを削除するには、以下のコマンドを実行します。

```
pkgrm package_name
```

GSKit を完全に除去するには、同じバージョンのすべての GSKit を除去してください。GSKit のアンインストールの場合、まず GSKit SSL パッケージを削除し、その後 GSKit crypt パッケージを削除する必要があります。パッケージの gsk8ss164 と gsk8cry64 を削除するには、次のコマンドを実行します。

```
pkgrm gsk8ss164  
pkgrm gsk8cry64
```

5. GSKit のアンインストールが正常に終了したかを検証します。

```
pkginfo | grep -i gsk
```

## HP-UX ユーティリティーを使用した IBM Global Security Kit のアンインストール

**swremove** コマンドを使用して、IBM Global Security Kit (GSKit) の HP-UX システムからのアンインストールを実行します。

### 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 次のコマンドを実行して、削除する GSKit パッケージを決定します。

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

4. GSKit パッケージを削除するには、以下のコマンドを実行します。

```
swremove package_name
```

GSKit を完全に除去するには、同じバージョンのすべての GSKit を除去してください。GSKit のアンインストールの場合、まず GSKit SSL パッケージを削除し、その後 GSKit crypt パッケージを削除する必要があります。パッケージの gskss164 と gskcrypt64 を削除するには、次のコマンドを実行します。

```
swremove gskss164  
swremove gskcrypt64
```

5. GSKit のアンインストールが正常に終了したかを検証します。

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

## Windows での IBM Global Security Kit のアンインストール

IBM Global Security Kit (GSKit) コマンドを使用して、GSKit の Windows システムからのアンインストールを実行します。

## このタスクについて

次の例では、パッケージの GSKit SSL 64 ビットと GSKit crypt 64 ビットの、AMD64/EM64T アーキテクチャー上の Windows システムからのサイレント・アンインストールが示されています。IA32/x86 アーキテクチャー上の Windows オペレーティング・システムの場合、GSKit のパッケージ名は異なります。GSKit パッケージ名については、61 ページの『第 10 章 IBM Global Security Kit のインストール』を参照してください。

注: 「スタート」 > 「コントロール パネル」 > 「プログラムの追加と削除」を使用して、GSKit パッケージを削除することもできます。

### 手順

1. 管理者グループのメンバーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 現在の作業ディレクトリーを、IBM Global Security Kit のインストール可能ファイルが保管されている gskit ディレクトリーに変更します。
4. GSKit 64 ビット・パッケージをサイレントに削除するには、以下のコマンドを実行します。GSKit を完全に除去するには、同じバージョンのすべての GSKit を除去してください。GSKit のアンインストールの場合、まず GSKit SSL パッケージを削除し、その後 GSKit crypt パッケージを削除する必要があります。

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

---

## 言語パックのアンインストール

IBM Security Directory Server のアンインストールを完了するには、コンピューターにインストールした言語パックをアンインストールする必要があります。

IBM Installation Manager を使用して、IBM Security Directory Server および言語パックをコンピューターにインストールした場合、IBM Installation Manager を使用して言語パックをアンインストールする必要があります。

言語パックのインストールにオペレーティング・システムのユーティリティーを使用した場合、言語パックのアンインストールにはオペレーティング・システムのユーティリティーを使用します。

インストールについてプロキシ・サーバーまたはサーバー機能を選択しない場合、すべての言語パックがシステムからアンインストールされます。

## オペレーティング・システムのユーティリティーを使用した言語パックのアンインストール

言語パックをオペレーティング・システムのユーティリティーを使用してインストールしていた場合、オペレーティング・システムのユーティリティーを使用して、その言語パックのアンインストールを実行します。

## 始める前に

IBM Security Directory Server の言語パックのアンインストールの前に、すべての IBM Security Directory Server クライアントとサーバーのプロセスを停止する必要があります。

- ディレクトリー・サーバー
- 管理サーバー
- LDAP トレース
- カスタム LDAP アプリケーション

## 手順

1. root ユーザーとしてログインします。
2. コマンド・プロンプトにアクセスします。
3. 以下のように、コンピューター上の削除する言語パックを決定します。

オペレーティング・システム	実行するコマンド:
AIX	<code>lslpp -l 'idsldap.msg631*'</code>
Linux	<code>rpm -qa   grep -i idsldap-msg631</code>
Solaris	<code>pkginfo   grep IDS1</code>

4. 特定の言語の言語パックをアンインストールするには、そのパッケージのアンインストール・コマンドを実行します。次の例では、フランス語の言語パックのアンインストールが示されています。対象のオペレーティング・システムの適切なパッケージ名で置換することによって、任意の言語パックをアンインストールできます。

オペレーティング・システム	実行するコマンド:
AIX	<code>installp -u idsldap.msg631.fr_FR</code>
Linux	<code>rpm -ev idsldap-msg631-fr-6.3.1-0.noarch.rpm</code>
Solaris	<code>pkgrm IDS1fr631</code>

5. 言語パックのインストールが正常に終了したかを検証します。詳細については、93 ページの『IBM Security Directory Server パッケージの検証』を参照してください。



---

## 付録 A. Directory Services Markup Language (DSML)

Directory Services Markup Language を使用して、ディレクトリー構造情報、ディレクトリーの照会と更新、およびディレクトリー操作の結果を XML 形式で表すことができます。

IBM Security Directory Server Web 管理ツールのインストールが完了すると、Directory Services Markup Language (DSML) ファイルのアーカイブ・ファイル DSML.zip がコンピューターに格納されます。DSML.zip は、IBM Security Directory Server のインストール・ロケーションの idstools サブディレクトリーに保管されます。デフォルトの IBM Security Directory Server のインストール・ロケーションについて詳しくは、30 ページの『デフォルトのインストール・ロケーション』を参照してください。

DSML.zip ファイルには、DSML のインストール、構成、使用方法を説明する資料および DSML インストール可能ファイルが含まれています。DSML.zip ファイルには、以下のファイルが含まれます。

### **DSMLReadme.txt**

DSMLReadme.txt ファイルには、パッケージ内のファイルのリストと、DSML をインストールおよび構成するための説明が記載されています。

### **dsm1.pdf**

dsm1.pdf ファイルは PDF 形式で、DSML の使用方法が説明されています。

### **dsm1.htm**

dsm1.htm ファイルは HTML 形式で、DSML の使用方法が説明されています。



---

## 付録 B. サンプル・データベースのロードおよびサーバーの始動

サンプル・データベースをロードしてディレクトリー・サーバーを始動し、項目の追加、更新、および検索を行います。

### 始める前に

ディレクトリー・サーバー・インスタンスを作成します。148 ページの『ディレクトリー・サーバー・インスタンス作成』を参照してください。

### このタスクについて

構成ツールを使用して LDIF データをディレクトリー・サーバーにロードし、サーバーを始動することができます。

### 手順

1. 構成ツールを開始するには、以下のコマンドを実行します。

```
idsxcfg -I instance_name
```
2. 左側のナビゲーション領域で、「**LDIF タスク**」 > 「**LDIF データのインポート**」をクリックします。
3. 「**パスと LDIF ファイル名**」フィールドで、LDIF データ・ファイルをパス付きで指定します。「参照」をクリックして、LDIF データ・ファイルを指定することもできます。各種オペレーティング・システムでのデフォルトのパス名と LDIF データ・ファイルは以下のとおりです。

#### Windows

```
installation_path\examples\sample.ldif
```

#### AIX および Solaris

```
/opt/IBM/ldap/V6.3.1/examples/sample.ldif
```

**Linux** /opt/ibm/ldap/V6.3.1/examples/sample.ldif

4. 「**標準インポート**」をクリックします。
5. 「**インポート**」をクリックします。
6. ディレクトリー・サーバー・インスタンスを始動するには、以下のアクションを実行します。
  - a. 左側のナビゲーション領域で、「**サーバー状態の管理**」をクリックします。
  - b. 「**サーバーの始動**」をクリックします。



---

## 付録 C. 手動による ldapdb.properties ファイルの更新

サポートされているバージョンの IBM DB2 が含まれていないコンピューターに IBM Security Directory Server をインストールした場合、ldapdb.properties ファイルにはインストール中にデータが取り込まれません。このような状態の場合、サポートされているバージョンの IBM DB2 をインストールしてから、ldapdb.properties ファイルを手動で更新する必要があります。

### 始める前に

フル・ディレクトリー・サーバーのパッケージを必ずインストールしておく必要があります。

### 手順

1. サポートされているバージョンの IBM DB2 がまだインストールされていない場合、それをインストールします。
2. **db21s** コマンドを実行して、コンピューターにインストールされている DB2 のバージョン、およびそれらのインストール・パスをリストします。
3. サポートされている DB2 のバージョンとインストール・パスで ldapdb.properties ファイルを更新します。各オペレーティング・システム用のサンプルの値を用いた ldapdb.properties ファイルのデフォルトのロケーション:

#### 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 および 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. ldapdb.properties ファイルを保存します。



---

## 付録 D. Security Directory Server のアクセシビリティ機能

アクセシビリティ機能は、運動障害または視覚障害など身体に障害を持つユーザーが情報技術製品を快適に使用できるようにサポートします。

この製品の主要なアクセシビリティ機能により、ユーザーは以下の操作を行うことができます。

- スクリーン・リーダー・ソフトウェアなどの支援テクノロジーを使用して、画面の表示内容を音声として聞く。本製品でのこれらのテクノロジーの使用についての詳細は、支援テクノロジーの製品資料を参照してください。
- キーボードのみを使用して、特定の機能または同等の機能を操作する。
- 画面の表示内容を拡大する。

加えて、製品資料が変更され、アクセシビリティを支援する以下の機能が含まれました。

- すべての資料が HTML 形式で利用可能となり、ユーザーがスクリーン・リーダー・ソフトウェアを最大限に活用できるようになりました。
- 資料内のすべての画像に代替テキストが提供され、視覚障害のあるユーザーが画像の内容を理解できるようになりました。

### アクセシビリティ

以下のリストに、IBM Security Directory Server の主なアクセシビリティ機能を示します。

- キーボードのみの操作のサポート
- スクリーン・リーダーで一般的に使用されるインターフェースのサポート
- キーは触ることで識別可能であり、単に触っただけでは有効になりません

IBM Security Directory Server の資料はアクセシビリティ対応です。資料のアクセシビリティ機能はオンラインの資料セットに記載されています。

### キーボードによるナビゲーション

本製品では、標準的なショートカット・キーとアクセラレーター・キーが使用されており、それらはオペレーティング・システムで文書化されています。詳しくは、オペレーティング・システム付属の資料を参照してください。

本製品では、標準的な Microsoft Windows ナビゲーション・キーを使用します。

### 画面の表示内容の拡大

製品が稼働中のオペレーティング・システムで提供される機能を使用することで、製品ウィンドウの情報を拡大できます。例えば、Microsoft Windows 環境では、画面の解像度を低くすると、画面上のテキストのフォント・サイズを拡大することができます。詳しくは、オペレーティング・システム付属の資料を参照してください。

## IBM およびアクセシビリティ

IBM のアクセシビリティに対する取り組みについて詳しくは、IBM Human Ability and Accessibility Center (<http://www.ibm.com/able>) を参照してください。

# 索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

## [ア行]

- アクセシビリティ ix, 285
- アクセス, Web 管理ツール
  - 構成 128
- アップグレード, インスタンス
  - 一般情報 97
- アップグレード, ディレクトリー・インスタンス
  - idsimigr コマンド 101
- アップグレード, プロキシ・インスタンス
  - idsimigr コマンド 101
- アプリケーション・サーバーの停止, Web アプリケーション・サーバー
  - 構成 130
- アンインストール, 言語パック
  - 一般情報 276
  - AIX ユーティリティ 277
  - Linux ユーティリティ 277
  - Solaris ユーティリティ 277
- アンインストール, ディレクトリー・サーバー
  - 一般情報 261
- アンインストール, AIX ユーティリティ
  - 一般情報 267
- アンインストール, DB2
  - 一般情報 272
- アンインストール, GSKit コマンド
  - GSKit 276
- アンインストール, HP-UX ユーティリティ
  - 一般情報 271
- アンインストール, IBM Installation Manager
  - IBM Security Directory Server 262
- アンインストール, installp コマンド
  - ディレクトリー・サーバー 268
  - GSKit 273
- アンインストール, Linux ユーティリティ
  - 一般情報 269
- アンインストール, pkgrm コマンド
  - ディレクトリー・サーバー 270
- アンインストール, pkgrm コマンド (続き)
  - GSKit 275
- アンインストール, rpm コマンド
  - ディレクトリー・サーバー 269
  - GSKit 274
- アンインストール, SMIT ユーティリティ
  - ディレクトリー・サーバー 267
  - GSKit 273
- アンインストール, Solaris ユーティリティ
  - 一般情報 270
- アンインストール, swremove コマンド
  - ディレクトリー・サーバー 271
  - GSKit 275
- アンデプロイメント, Web 管理ツール
  - 構成 132
- インスタンス, 作成
  - 一般情報 148
- インスタンス, ユーザーとグループ
  - 許可, 一般情報 135
  - 作成, 一般情報 135
- インスタンス, Web 管理ツール
  - リモート管理, 構成 128
- インスタンス管理サーバー, インスタンス作成
  - カスタム設定 151
  - デフォルト・インスタンス 149
- インスタンス管理サーバー, プロキシ・インスタンス作成
  - カスタム設定 160
- インスタンス管理ツール
  - インスタンスのアップグレード 165
- インスタンス管理ツール, アップグレード
  - リモート・インスタンス 167
- インスタンス管理ツール, インスタンス削除
  - 構成 184
- インスタンス管理ツール, インスタンスの開始または停止
  - 一般情報 176
- インスタンス管理ツール, インスタンスのコピー
  - 構成 172
- インスタンス管理ツール, インスタンスの削除
  - 一般情報 183
- インスタンス管理ツール, インスタンスの詳細の表示
  - 一般情報 182
- インスタンス管理ツール, インスタンスの詳細の表示 (続き)
  - 構成 182
- インスタンス管理ツール, 管理サーバーの開始または停止
  - 構成 176
- インスタンス管理ツール, 構成
  - インスタンスのコピー 172
  - 管理サーバーの始動または停止 176
  - サーバーの始動または停止 176
- インスタンス管理ツール, 始動
  - 構成 146
- インスタンス管理ツール, ディレクトリー・サーバーの開始または停止
  - 構成 176
- インスタンス管理ツール, 開く
  - 構成 146
  - 構成ツール 178
- インスタンス管理ツール, リモート・アップグレード
  - バックアップ・データを含んだインスタンス 147
- インスタンス管理ツール, TCP/IP 設定の変更
  - インスタンス 179
  - 構成 179
- インスタンス作成, オプション
  - インスタンス管理ツール 149
- インスタンス作成, システム構成
  - 一般情報 133
- インスタンス作成, 方法
  - 一般情報 145
- インスタンスのアップグレード
  - インスタンス管理ツール 165
  - 環境のセットアップ 98
  - リモート, サポートされるオペレーティング・システム 103
- インスタンスのアップグレード, 構成
  - リモート側, インスタンス管理ツール 167
  - リモート側, idsimigr -u 103
  - idsimigr コマンド, -u 103
- インスタンスのアップグレード, リモート側
  - 一般情報 102
- インストール
  - 手動
    - HP-UX 88
    - HP-UX ユーティリティ 88
    - pkgadd コマンド 87

- インストール (続き)
  - Solaris へのディレクトリー・サーバー・パッケージ 84
- インストール、概要
  - IBM Installation Manager 23
- インストール、環境の要件
  - 一般情報 1
- インストール、計画
  - 一般情報 1
- インストール、言語パック
  - 一般情報 69
  - AIX ユーティリティ 71
  - Linux ユーティリティ 71
  - Solaris ユーティリティ 71
- インストール、手動
  - WebSphere Application Server 組み込みバージョン 121
- インストール、ツール
  - IBM Installation Manager 23
- インストール、ディレクトリー・サーバーオペレーティング・システムのユーティリティ 73
  - ランチパッド、構成 32
  - リポジトリ 33
  - IBM Installation Manager 35
  - swinstall コマンド 89
- インストール、リポジトリ構成
  - ディレクトリー・サーバー 33
- インストール、ロケーション
  - ディレクトリー構造 187
- インストール、AIX へのディレクトリー・サーバー・パッケージ
  - 一般情報 74
- インストール、AIX ユーティリティ
  - 一般情報 73
- インストール、DB2
  - 一般情報 57
- インストール、GSKit
  - 一般情報 61
  - パッケージ名 61
- インストール、IBM Global Security Kit
  - Windows 66
- インストール、IBM Installation Manager
  - 一般情報 23
  - 概要 23
- インストール、IBM JDK
  - 一般情報 59
- インストール、installp コマンド
  - ディレクトリー・サーバー 78
  - IBM Global Security Kit 63
- インストール、Linux へのディレクトリー・サーバー・パッケージ
  - 一般情報 80
- インストール、Linux ユーティリティ
  - 一般情報 80
- インストール、pkgadd コマンド
  - IBM Global Security Kit 65
- インストール、rpm コマンド
  - ディレクトリー・サーバー 83
  - IBM Global Security Kit 64
- インストール、SMIT ユーティリティ
  - ディレクトリー・サーバー 76
- インストール、Solaris ユーティリティ
  - ディレクトリー・サーバー 84
- インストール、swinstall コマンド
  - IBM Global Security Kit 65
- インストール、Windows
  - IBM Global Security Kit 66
- インストールの概要、ディレクトリー・サーバー
  - 一般情報 3
- インストールの検証、GSKit
  - UNIX 95
- インストールの方法
  - 一般情報 20
- インストールの前提条件
  - 一般情報 16
- インストール方法
  - 一般情報 20
- インストール要件、IBM Security
  - Directory Server
    - 一般情報 25
- インストール用のパッケージ、ディレクトリー・サーバー
  - HP-UX 88
- インストール・コンポーネント、IBM Security
  - Directory Server
    - 一般情報 26
- インストール・シナリオ、IBM Security
  - Directory Server
    - 一般情報 29
- インストール・パッケージ、タイプ
  - 一般情報 24
- インストール・メディア、IBM Security
  - Directory Server
    - 一般情報 6
- インストール・リポジトリ
  - 一般情報 31
- インストール・ロケーション
  - デフォルト、一般情報 30
- オペレーティング・システム、言語パック
  - パッケージ名 70
- オペレーティング・システム、更新
  - 前提条件パッケージ 16
- オペレーティング・システムのユーティリティ、ディレクトリー・サーバーのアンインストール
  - 一般情報 266
- オペレーティング・システムのユーティリティ、ディレクトリー・サーバーのインストール
  - 一般情報 73
- オペレーティング・システムのユーティリティ、GSKit アンインストール
  - 一般情報 273
- オペレーティング・システムのユーティリティを使用したアンインストール、ディレクトリー・サーバー
  - 一般情報 266
- オペレーティング・システムのユーティリティを使用したアンインストール、GSKit
  - 一般情報 273
- オンライン
  - 資料 vii
  - 用語 vii

## [力行]

- 開始、Web 管理ツール
  - 構成 128
- 各国語文字
  - UTF-8 138
- 環境のセットアップ
  - インスタンスのアップグレード 98
- 管理サーバー、始動または停止
  - 一般情報 176, 191
- 機能、アンインストール
  - IBM Security Directory Server 262
- 機能、検証
  - IBM Security Directory Server 91
- 機能、変更
  - IBM Security Directory Server の機能 43
- クライアント・ユーティリティ、リンク
  - 一般情報 105
- クライアント・ユーティリティ、DB2
  - データベース管理者
    - パスワード、構成 205
- クライアント・ユーティリティ、LDIF
  - データ管理
    - 一般情報 236
- 言語パック、アンインストール
  - 一般情報 276
- 言語パック、インストール
  - 一般情報 69
- 言語パック、オペレーティング・システム
  - サポートされる言語 69
- 言語パック、パッケージ名
  - オペレーティング・システム 70
- 研修 ix
- 検証、ディレクトリー・サーバー
  - 一般情報 91

- 検証、バージョン
    - Web 管理ツール 94
  - コード・ページ、違い
    - UTF-8、ロケール 139
  - コード・ページ、DB2
    - 文字セット、IANA 141
  - 構成、データベースの計画
    - 一般情報 137
  - 構成ツール
    - 一般情報 178, 189
  - 構成ツール、インスタンスの開始または停止
    - 一般情報 191
  - 構成ツール、開始
    - 構成 190
  - 構成ツール、管理
    - 管理者 DN、構成 193
    - 管理者パスワード、構成 195
  - 構成ツール、管理サーバーの始動または停止
    - 構成 191
  - 構成ツール、管理者 DN の管理
    - 構成 193
  - 構成ツール、管理者パスワードの管理
    - 構成 195
  - 構成ツール、構成
    - 管理サーバーの始動または停止 191
    - サーバーの始動または停止 191
  - 構成ツール、サーバー構成
    - 一般情報 178
  - 構成ツール、サフィックス
    - 一般情報 228
  - 構成ツール、スキーマ管理
    - 一般情報 232
  - 構成ツール、データベース管理者パスワード
    - 一般情報 204
  - 構成ツール、データベース構成
    - 一般情報 196
  - 構成ツール、データベース構成解除
    - 一般情報 207
  - 構成ツール、データベースの最適化
    - 一般情報 209
  - 構成ツール、データベースのバックアップ
    - 構成 213
  - 構成ツール、データベースの復元
    - 構成 216
  - 構成ツール、データベース保守
    - 一般情報 210
  - 構成ツール、ディレクトリー・サーバー
    - サフィックスの削除、構成 230
    - サフィックスの追加、構成 229
    - スキーマ妥当性検査、構成 235
    - スキーマの管理、構成 233
    - データベースの最適化、構成 209
    - データベースの保守、構成 211
  - 構成ツール、ディレクトリー・サーバーの始動または停止
    - 構成 191
  - 構成ツール、バックアップ
    - 一般情報 212
  - 構成ツール、パフォーマンス・チューニング
    - ディレクトリー・サーバー 220, 223
  - 構成ツール、開く
    - 構成 190
  - 構成ツール、復元
    - 一般情報 216
  - 構成ツール、プロキシ・サーバーのバックアップ
    - 構成 215
  - 構成ツール、プロキシ・サーバーの復元
    - 構成 217
  - 構成ツール、変更ログ
    - 一般情報 224
    - 構成 224
  - 構成ツール、変更ログを使用不可にする
    - 構成 226
  - 構成ツール、Active Directory との同期
    - 構成 244
  - 構成ツール、DB2 データベース
    - 構成 197
    - 構成解除 207
  - 構成ツール、DB2 データベース管理者パスワード、構成 204
  - 構成ツール、LDIF データ管理
    - 一般情報 236
  - 構成ツール、LDIF データのインポート
    - 構成 237
  - 構成ツール、LDIF データのエクスポート
    - 構成 240
  - 構成ツール、LDIF データの検証
    - 構成 239
  - コマンド、移行
    - Web 管理ツール、idswmigr 114
- ## [サ行]
- サーバー・ユーティリティー
    - インスタンス管理ツール 165
    - idsimigr コマンド 101
    - idsimigr コマンド、-u 103
  - サーバー・ユーティリティー、インスタンス削除
    - 構成 184
  - サーバー・ユーティリティー、インスタンス作成
    - 構成 163
  - サーバー・ユーティリティー、インスタンスのコピー
    - 構成 175
  - サーバー・ユーティリティー、インスタンスの詳細の表示
    - 構成 182
  - サーバー・ユーティリティー、管理
    - 管理者 DN、構成 194
    - 管理者パスワード、構成 195
  - サーバー・ユーティリティー、管理サーバーの開始または停止
    - 構成 177, 192
  - サーバー・ユーティリティー、管理者 DN の管理
    - 構成 194
  - サーバー・ユーティリティー、管理者パスワードの管理
    - 構成 195
  - サーバー・ユーティリティー、構成
    - インスタンスのコピー 175
    - 管理サーバーの始動または停止 177, 192
    - サーバーの始動または停止 177, 192
  - サーバー・ユーティリティー、コマンド行
    - サーバーの始動または停止 176
  - サーバー・ユーティリティー、作成
    - LDIF ファイル、UTF-8 値 139
  - サーバー・ユーティリティー、サフィックス
    - 一般情報 228
  - サーバー・ユーティリティー、スキーマ管理
    - 一般情報 232
  - サーバー・ユーティリティー、データベース管理者パスワード
    - 一般情報 204
  - サーバー・ユーティリティー、データベース構成
    - 一般情報 196
  - サーバー・ユーティリティー、データベース構成解除
    - 一般情報 207
  - サーバー・ユーティリティー、データベースの最適化
    - 一般情報 209
    - 構成 210
  - サーバー・ユーティリティー、データベース保守
    - 一般情報 210
    - 構成 212
  - サーバー・ユーティリティー、ディレクトリー・サーバー
    - サフィックスの削除、構成 231
    - サフィックスの追加、構成 230
    - スキーマの管理、構成 234
    - DB2 データベースの構成解除 208
  - サーバー・ユーティリティー、ディレクトリー・サーバーの開始または停止
    - 構成 177, 192

サーバー・ユーティリティ、バックアップ  
     一般情報 212  
 サーバー・ユーティリティ、復元  
     一般情報 216  
 サーバー・ユーティリティ、変更ログ  
     一般情報 224  
     構成 226  
 サーバー・ユーティリティ、変更ログを  
 使用不可にする  
     構成 227  
 サーバー・ユーティリティ、リンク  
     一般情報 105  
 サーバー・ユーティリティ、1 次管理者  
     一般情報 192  
 サーバー・ユーティリティ、1 次管理者  
 パスワード  
     一般情報 194  
 サーバー・ユーティリティ、Active  
 Directory との同期  
     構成 245  
 サーバー・ユーティリティ、DB2 デー  
 タベース  
     構成 202  
 サーバー・ユーティリティ、DB2 デー  
 タベース管理者  
     パスワード、 構成 205  
 サーバー・ユーティリティ、LDIF デー  
 タ管理  
     一般情報 236  
 サーバー・ユーティリティ、LDIF ファ  
 イル作成  
     idsbulkload 139  
     idsdb2ldif 139  
     idsldif2db 139  
 サーバー・ユーティリティ、TCP/IP 設  
 定の変更  
     構成 180  
 サイレント変更、応答ファイル  
     一般情報 40  
     構成 41  
 サイレント・アンインストール  
     GSKit 276  
 サイレント・アンインストール、応答ファ  
 イル  
     一般情報 40  
     構成 41, 264  
 サイレント・アンインストール、imcl コ  
 マンド  
     構成 265  
 サイレント・インストール、応答ファイル  
     一般情報 40  
     構成 41  
 サイレント・インストール、IBM Global  
 Security Kit  
     Windows 67

サイレント・インストール、Windows  
     IBM Global Security Kit 67  
 サポートされるオペレーティング・システ  
 ム  
     インスタンスのアップグレード、リモ  
     ート 103  
 自動始動、ディレクトリー・サーバー  
     一般情報 247  
 自動始動ディレクトリー・サーバー、AIX  
     構成 249  
 自動始動ディレクトリー・サーバー、  
 Linux  
     構成 249  
 自動始動ディレクトリー・サーバー、  
 Solaris  
     構成 249  
 自動始動ディレクトリー・サーバー、  
 Windows  
     構成 248  
 手動、インストール  
     WebSphere Application Server 組み込み  
     バージョン 121  
 手動アンインストール、AIX ユーティリ  
 ティー  
     一般情報 267  
 手動アンインストール、HP-UX ユーティ  
 リティ  
     一般情報 271  
 手動アンインストール、Linux ユーティリ  
 ティー  
     一般情報 269  
 手動アンインストール、Solaris ユーティ  
 リティ  
     一般情報 270  
 手動インストール、AIX ユーティリテ  
 ー  
     一般情報 73  
 手動インストール、Linux ユーティリテ  
 ー  
     一般情報 80  
 資料  
     アクセス、オンライン vii  
     本製品用のリスト vii

## [夕行]

データおよびソリューションの移行  
     一般情報 107  
 データベース、構成計画  
     アクセス権 137  
     一般情報 137  
     階層構造 137  
     コード・ページ 137  
 ディスク・スペース要件  
     ディレクトリー・サーバー、コンポー  
     ネント 3

ディレクトリー構造  
     インストール、ロケーション 187  
 ディレクトリー構造、ダウンロードしたフ  
 ァイル  
     AIX 8  
     Linux 8  
     Solaris 8  
     Windows 8  
 ディレクトリー情報、Directory Services  
 Markup Language  
     一般情報 279  
 ディレクトリー・インスタンス  
     アップグレード 101  
 ディレクトリー・インスタンス、リモー  
 ト・アップグレード  
     構成、idsimigr -u 103  
 ディレクトリー・サーバー  
     インスタンス作成 148  
     サーバーの始動 281  
     始動、Web アプリケーション・サーバ  
     ー 127  
     データのロード 281  
     DB2 データベースの構成解除 207  
     Solaris へのインストール用パッケージ  
     84  
 ディレクトリー・サーバー、アンインスト  
 ール  
     一般情報 261, 262  
 ディレクトリー・サーバー、インスタンス  
 管理  
     一般情報 145  
 ディレクトリー・サーバー、インスタンス  
 管理ツール  
     一般情報 145  
 ディレクトリー・サーバー、インスタンス  
 構成  
     一般情報 189  
 ディレクトリー・サーバー、インスタンス  
 削除  
     構成 184  
 ディレクトリー・サーバー、インスタンス  
 作成  
     一般情報 145, 148  
     インスタンス管理ツール 149  
     カスタム設定 151  
     構成 163, 175  
     デフォルト・インスタンス 149  
 ディレクトリー・サーバー、インスタンス  
 追加  
     構成 172  
     複製トポロジー 170  
 ディレクトリー・サーバー、インスタンス  
 のアップグレード  
     一般情報 97

- ディレクトリー・サーバー、インスタンスの削除
  - 一般情報 183
- ディレクトリー・サーバー、インスタンスの詳細の表示
  - 一般情報 182
  - 構成 182
- ディレクトリー・サーバー、インストールオペレーティング・システムのユーティリティ
  - 73
  - 前提条件、一般情報 16
  - 要件、一般情報 1
  - ランチパッド、構成 32
  - リポジトリ 33
  - IBM Installation Manager 35
- ディレクトリー・サーバー、インストールの概要
  - 一般情報 3
- ディレクトリー・サーバー、インストールの前提条件
  - 一般情報 16
- ディレクトリー・サーバー、管理者 DN の管理
  - 構成 193, 194
- ディレクトリー・サーバー、管理者パスワードの管理
  - 構成 195
- ディレクトリー・サーバー、クライアントおよびサーバー・ユーティリティ
  - リンク、一般情報 105
- ディレクトリー・サーバー、検証
  - 一般情報 91
  - Web 管理ツールのバージョン 94
- ディレクトリー・サーバー、構成ツール
  - パフォーマンス・チューニング 220, 223
- ディレクトリー・サーバー、構成の管理
  - 一般情報 178
- ディレクトリー・サーバー、構成の変更
  - 一般情報 178
- ディレクトリー・サーバー、コピー
  - 一般情報 170
- ディレクトリー・サーバー、コンポーネント
  - ディスク・スペース要件 3
- ディレクトリー・サーバー、サーバー・ユーティリティ
  - インスタンス削除、構成 184
  - インスタンスの詳細の表示、構成 182
  - TCP/IP 設定の変更、構成 180
- ディレクトリー・サーバー、サイレント変更
  - 一般情報 40
  - 構成 41
- ディレクトリー・サーバー、サイレント・アンインストール
  - 一般情報 40
  - 構成 41, 264, 265
- ディレクトリー・サーバー、サイレント・インストール
  - 一般情報 40
  - 構成 41
- ディレクトリー・サーバー、作成
  - 一般情報 170
  - システム構成 133
- ディレクトリー・サーバー、サフィックス
  - 一般情報 228
- ディレクトリー・サーバー、サフィックスの削除
  - 構成 230, 231
- ディレクトリー・サーバー、サフィックスの追加
  - 構成 229, 230
- ディレクトリー・サーバー、始動または停止
  - 一般情報 176, 191
- ディレクトリー・サーバー、手動インストール
  - Solaris 84
- ディレクトリー・サーバー、状況
  - 一般情報 178
- ディレクトリー・サーバー、スキーマ管理
  - 一般情報 232
- ディレクトリー・サーバー、スキーマ妥当性検査
  - 構成 235
- ディレクトリー・サーバー、スキーマの管理
  - 構成 233, 234
- ディレクトリー・サーバー、ソリューションの移行
  - 一般情報 107
- ディレクトリー・サーバー、チューニング
  - 一般情報 218
  - パフォーマンス、一般情報 218
- ディレクトリー・サーバー、データベース管理者パスワード
  - 一般情報 204
- ディレクトリー・サーバー、データベース構成
  - 一般情報 196
- ディレクトリー・サーバー、データベース構成解除
  - 一般情報 207
- ディレクトリー・サーバー、データベースの移行
  - 構成 108
- ディレクトリー・サーバー、データベースの最適化
  - 一般情報 209
- ディレクトリー・サーバー、データベースのバックアップ
  - 構成 213
- ディレクトリー・サーバー、データベースの復元
  - 構成 216
- ディレクトリー・サーバー、データベース保守
  - 一般情報 210
- ディレクトリー・サーバー、デプロイメント
  - Web 管理ツール 124
- ディレクトリー・サーバー、同期
  - 一般情報 18, 241
- ディレクトリー・サーバー、バックアップ
  - 一般情報 212
- ディレクトリー・サーバー、パフォーマンス
  - チューニング、一般情報 218
- ディレクトリー・サーバー、開く
  - 構成ツール 178
- ディレクトリー・サーバー、復元
  - 一般情報 216
- ディレクトリー・サーバー、変更
  - 一般情報 43
- ディレクトリー・サーバー、変更ログ
  - 一般情報 224
  - 構成 224, 226
- ディレクトリー・サーバー、変更ログを使用不可にする
  - 構成 226, 227
- ディレクトリー・サーバー、命名規則
  - 一般情報 134
  - ユーザー ID、1 次グループ 134
- ディレクトリー・サーバー、ユーザーとグループ
  - 一般情報 133
  - 許可、一般情報 135
  - 作成、一般情報 135
  - 要件 133
- ディレクトリー・サーバー、ログ管理ソリューションの移行
  - 構成 110
- ディレクトリー・サーバー、1 次管理者
  - 一般情報 192
- ディレクトリー・サーバー、1 次管理者パスワード
  - 一般情報 194
- ディレクトリー・サーバー、Active Directory
  - 同期、一般情報 18, 241
- ディレクトリー・サーバー、Active Directory との同期
  - 構成 244, 245

- ディレクトリー・サーバー、Active Directory との同期ソリューションの移行
  - 構成 112
- ディレクトリー・サーバー、AIX 上での検証
  - 構成 93
- ディレクトリー・サーバー、AIX へのインストール用パッケージ
  - 一般情報 74
- ディレクトリー・サーバー、AIX ユーティリティーを使用したアンインストール
  - 一般情報 267
- ディレクトリー・サーバー、AIX ユーティリティーを使用したインストール
  - 一般情報 73
- ディレクトリー・サーバー、DB2
  - 一般情報 57
- ディレクトリー・サーバー、DB2 データベース
  - 構成解除 208
  - 最適化 209, 210
  - 保守 211, 212
- ディレクトリー・サーバー、DB2 データベース管理者
  - パスワード、構成 204, 205
- ディレクトリー・サーバー、DB2 データベースの構成
  - 構成 197, 202
- ディレクトリー・サーバー、DB2 プロパティ・ファイル
  - 構成 283
- ディレクトリー・サーバー、HP-UX 上での検証
  - 構成 93
- ディレクトリー・サーバー、IBM Installation Manager を使用したインストール
  - サポートされるオペレーティング・システム、一般情報 24
- ディレクトリー・サーバー、IBM JDK
  - 一般情報 59
- ディレクトリー・サーバー、LDIF データ管理
  - 一般情報 236
- ディレクトリー・サーバー、LDIF データのインポート
  - 構成 237
- ディレクトリー・サーバー、LDIF データのエクスポート
  - 構成 240
- ディレクトリー・サーバー、LDIF データの検証
  - 構成 239
- ディレクトリー・サーバー、Linux 上での検証
  - 構成 93
- ディレクトリー・サーバー、Linux へのインストール用パッケージ
  - 一般情報 80
- ディレクトリー・サーバー、SNMP ソリューションの移行
  - 構成 111
- ディレクトリー・サーバー、Solaris pkgadd を使用したインストール
  - 87
- ディレクトリー・サーバー、Solaris 上での検証
  - 構成 93
- ディレクトリー・サーバー、TCP/IP 設定の変更
  - 一般情報 179
  - 構成 179
- ディレクトリー・サーバー、Windows 上での検証
  - 構成 92
- ディレクトリー・サーバーのアンインストール、オペレーティング・システムのユーティリティー
  - 一般情報 266
- ディレクトリー・サーバー・インスタンス、作成
  - インスタンス管理サーバー 151
  - 構成 163
- ディレクトリー・サーバー・パッケージ、HP-UX
  - 一般情報 88
- デフォルトのインストール・ロケーション
  - 一般情報 30
- デフォルト・インスタンス、作成
  - インスタンス管理サーバー 149
- デフォルト・ポート、Web 管理ツール
  - 一般情報 122
- デプロイメント
  - Web 管理ツール 124
- デプロイメント、Web 管理ツール
  - 一般情報 121
- WebSphere Application Server 125
  - 同期
    - Active Directory から Security Directory Server への 18, 241
  - トラブルシューティング ix

## [ハ行]

- パスポート・アドバンテージ、ダウンロード
  - IBM Security Directory Server 7
- パスポート・アドバンテージ、IBM Security Directory Server
  - 製品のダウンロード 7

- パッケージ名
  - 言語パック 70
- 開く、Web 管理ツール
  - 構成 128
- フィックスパック 253
- プロキシー・インスタンス
  - アップグレード 101
- プロキシー・インスタンス、リモート・アップグレード
  - 構成、idsimigr -u 103
- プロキシー・サーバー、インスタンス構成
  - 一般情報 189
- プロキシー・サーバー、インスタンス削除
  - 構成 184
- プロキシー・サーバー、インスタンス作成
  - カスタム設定 160
- プロキシー・サーバー、インスタンスの削除
  - 一般情報 183
- プロキシー・サーバー、インスタンスの詳細の表示
  - 一般情報 182
  - 構成 182
- プロキシー・サーバー、管理者 DN の管理
  - 構成 193, 194
- プロキシー・サーバー、管理者パスワードの管理
  - 構成 195
- プロキシー・サーバー、構成の管理
  - 一般情報 178
- プロキシー・サーバー、構成の変更
  - 一般情報 178
- プロキシー・サーバー、サーバー・ユーティリティー
  - インスタンス削除、構成 184
  - インスタンスの詳細の表示、構成 182
  - TCP/IP 設定の変更、構成 180
- プロキシー・サーバー、作成
  - システム構成 133
- プロキシー・サーバー、サフィックスの削除
  - 構成 230, 231
- プロキシー・サーバー、サフィックスの追加
  - 構成 229, 230
- プロキシー・サーバー、状況
  - 一般情報 178
- プロキシー・サーバー、スキーマ妥当性検査
  - 構成 235
- プロキシー・サーバー、スキーマの管理
  - 構成 233, 234
- プロキシー・サーバー、バックアップ
  - 一般情報 212
  - 構成 215

プロキシ・サーバー、開く  
構成ツール 178  
プロキシ・サーバー、復元  
一般情報 216  
構成 217  
プロキシ・サーバー、1 次管理者  
一般情報 192  
プロキシ・サーバー、1 次管理者パスワード  
一般情報 194  
プロキシ・サーバー、TCP/IP 設定の変更  
一般情報 179  
構成 179  
プロキシ・サーバー・インスタンス、作成  
インスタンス管理サーバー 160

## [マ行]

命名規則、ディレクトリー・サーバー・インスタンス  
ユーザー ID、1 次グループ 134  
文字、各国語  
UTF-8 138  
文字セット、IANA  
コード・ページ、DB2 141  
問題判別 ix

## [ヤ行]

ユーザーおよびグループ、idsldap  
一般情報 18  
要件 18  
ユーザーとグループ、データベース所有者  
一般情報 133  
ユーザーとグループ、データベース・インスタンス所有者  
一般情報 133  
ユーザーとグループ、ディレクトリー・サーバー  
一般情報 133  
ユーザーとグループ、ディレクトリー・サーバー・インスタンス所有者  
一般情報 133  
用語 vii

## [ラ行]

ランチパッド、インストール  
ディレクトリー・サーバー 32  
リモート管理、インスタンス  
Web 管理ツール、構成 128

リモート・アップグレード、インスタンス管理ツール  
バックアップ・データを含んだインスタンス 147  
リモート・インスタンスのアップグレード、構成  
インスタンス管理ツール 167  
ログ管理ソリューション、移行  
構成 110  
ログ・ロケーション  
IBM Installation Manager 49

## [数字]

1 次管理者、管理  
一般情報 192  
1 次管理者パスワード、管理  
一般情報 194

## A

Active Directory  
同期の開始 243  
Active Directory との同期  
構成 243  
Active Directory との同期ソリューション、移行  
構成 112  
AIX  
SMIT を使用したインストール 76  
AIX 上での検証、ディレクトリー・サーバー  
構成 93  
AIX ユーティリティー、アンインストール  
言語バック 277  
AIX ユーティリティー、インストール  
言語バック 71  
AIX、ディスク・スペース要件  
ディレクトリー・サーバー、コンポーネント 3  
AIX、ディレクトリー・サーバー  
SMIT を使用したアンインストール 267  
AIX、ディレクトリー・サーバーの自動始動  
一般情報 247  
構成 249  
AIX、GSKit  
SMIT を使用したアンインストール 273  
AIX、installp を使用したアンインストール  
ディレクトリー・サーバー 268  
GSKit 273

AIX、installp を使用したインストール  
ディレクトリー・サーバー 78  
IBM Global Security Kit 63  
ASCII 文字  
サポートされる暗号化シード・ストリング 142  
33 から 126 142

## D

DB2 アンインストール、DB2 コマンド  
一般情報 272  
DB2 コード・ページ  
ロケール、IANA 141  
DB2 データベース、オンライン・バックアップ  
インスタンス管理ツール 151  
DB2 データベース、構成  
インスタンス管理ツール 151  
DB2 データベース、構成ツール  
構成 197  
構成解除 207  
パスワード、構成 204  
DB2 データベース、サーバー・ユーティリティー  
構成 202  
DB2 プロパティ・ファイル、ディレクトリー・サーバー  
構成 283  
DB2、データの移行  
一般情報 107  
構成 108  
DB2、ディレクトリー・サーバー  
一般情報 57  
Directory Services Markup Language (DSML)  
一般情報 279

## G

GSKit アンインストール、オペレーティング・システムのユーティリティー  
一般情報 273  
GSKit、インストールの検証  
UNIX 95  
GSKit、検証  
Windows 94

## H

HP-UX 上での検証、ディレクトリー・サーバー  
構成 93

HP-UX、ディスク・スペース要件  
ディレクトリー・サーバー、コンポ  
ネント 3

HP-UX、swinstall を使用したインストー  
ル  
ディレクトリー・サーバー 89  
IBM Global Security Kit 65

HP-UX、swremove を使用したアンインス  
トール  
ディレクトリー・サーバー 271  
GSKit 275

HTTPS、WebSphere Application Server 組  
み込みバージョン  
一般情報 131

## I

IBM  
ソフトウェア・サポート ix  
Support Assistant ix

IBM Installation Manager、インストールの  
開始  
ディレクトリー・サーバー 35

IBM Installation Manager、ディレクトリ  
ー・サーバーのアンインストール  
一般情報 262

IBM Installation Manager、ディレクトリ  
ー・サーバーのインストール  
サポートされるオペレーティング・シ  
ステム、一般情報 24

IBM Installation Manager、ディレクトリ  
ー・サーバー変更  
一般情報 43

IBM Installation Manager、ログ  
一般情報 49  
ロケーション 49

IBM JDK、ディレクトリー・サーバー  
一般情報 59

IBM Security Directory Server  
インストール・シナリオ 29

IBM Security Directory Server、アンイン  
ストール  
フィーチャー 262

IBM Security Directory Server、インスト  
ール  
一般情報 25  
前提条件パッケージ 16

IBM Security Directory Server、インスト  
ール・シナリオ  
一般情報 29

IBM Security Directory Server、インスト  
ール・パッケージ  
タイプ、一般情報 24

IBM Security Directory Server、インスト  
ール・メディア  
一般情報 6

IBM Security Directory Server、インスト  
ール・リポジトリー  
一般情報 31

IBM Security Directory Server、検証  
相互前提条件製品、DB2 91  
相互前提条件製品、GSKit 91  
相互前提条件製品、WebSphere  
Application Server 組み込みバージョ  
ン 91  
フィーチャー 91

IBM Security Directory Server、コンポー  
ネント  
一般情報 26

IBM Security Directory Server、パスポー  
ト・アドバンテージ  
製品のダウンロード 7

IBM Security Directory Server、変更  
フィーチャー 43

IBM Security Directory Server、IBM  
Installation Manager  
インストールの開始、構成 31  
インストールの開始、方法 31

installp によるアンインストール  
ディレクトリー・サーバー 268  
GSKit 273

installp によるインストール  
ディレクトリー・サーバー 78  
IBM Global Security Kit 63

## L

LDIF ファイル、作成  
UTF-8 値 139

Linux 上での検証、ディレクトリー・サー  
バー  
構成 93

Linux ユーティリティ、アンインストー  
ル  
言語パック 277

Linux ユーティリティ、インストール  
言語パック 71

Linux、ディスク・スペース要件  
ディレクトリー・サーバー、コンポー  
ネント 3

Linux、ディレクトリー・サーバーの自動  
始動  
一般情報 247  
構成 249

Linux、rpm を使用したアンインストール  
ディレクトリー・サーバー 269  
GSKit 274

Linux、rpm を使用したインストール  
ディレクトリー・サーバー 83  
IBM Global Security Kit 64

## P

pkgadd によるインストール  
ディレクトリー・サーバー 87  
IBM Global Security Kit 65

pkgrm によるアンインストール  
ディレクトリー・サーバー 270  
GSKit 275

## R

rpm によるアンインストール  
ディレクトリー・サーバー 269  
GSKit 274

rpm によるインストール  
ディレクトリー・サーバー 83  
IBM Global Security Kit 64

## S

SMIT によるアンインストール  
ディレクトリー・サーバー 267  
GSKit 273

SMIT によるインストール  
ディレクトリー・サーバー 76

SNMP ソリューション、移行  
構成 111

Solaris 上での検証、ディレクトリー・サー  
バー  
構成 93

Solaris ユーティリティ、アンインスト  
ール  
言語パック 277

Solaris ユーティリティ、インストール  
言語パック 71

Solaris、ディスク・スペース要件  
ディレクトリー・サーバー、コンポー  
ネント 3

Solaris、ディレクトリー・サーバーの自動  
始動  
一般情報 247  
構成 249

Solaris、pkgadd を使用したインストール  
IBM Global Security Kit 65

Solaris、pkgrm を使用したアンインストー  
ル  
ディレクトリー・サーバー 270  
GSKit 275

swinstall によるインストール  
IBM Global Security Kit 65

swinstall、インストール  
ディレクトリー・サーバー 89

swremove によるアンインストール  
ディレクトリー・サーバー 271  
GSKit 275

## U

UTF-8

各国語文字 138

## W

Web アドレス、HTTPS

一般情報 131

Web アプリケーション・サーバー、アプリケーション・サーバーの停止

構成 130

Web アプリケーション・サーバー、始動

構成 127

Web 管理ツール

移行、一般情報 113

移行、idswmigr コマンド 114

構成の移行 113

Web 管理ツール、アンデプロイメント

構成 132

Web 管理ツール、デフォルト・ポート

一般情報 122

Web 管理ツール、デプロイメント

一般情報 121

WebSphere Application Server 125

WebSphere Application Server 組み込みバージョン

インストール 121

WebSphere Application Server 組み込みバージョン、HTTPS

一般情報 131

WebSphere Application Server、Web 管理ツールのデプロイメント

構成 125

Windows 上での検証、ディレクトリー・サーバー

構成 92

Windows、アンインストール

GSKit 276

Windows、インストール

IBM Global Security Kit 66

Windows、サイレント・インストール

IBM Global Security Kit 67

Windows、ディスク・スペース要件

ディレクトリー・サーバー、コンポーネント 3

Windows、ディレクトリー・サーバーの自動始動

一般情報 247

構成 248

Windows、GSKit

検証 94



---

## 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510  
東京都中央区日本橋箱崎町19番21号  
日本アイ・ビー・エム株式会社  
法務・知的財産  
法的財産権ライセンス渉外

**以下の保証は、国または地域の法律に沿わない場合は、適用されません。**

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。

国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation  
2Z4A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのもと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラット

フォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。お客様は、IBM のアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. \_年を入れる\_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

## 商標

IBM、IBM ロゴおよび [ibm.com](http://www.ibm.com)<sup>®</sup> は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、<http://www.ibm.com/legal/copytrade.shtml> をご覧ください。

Adobe、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

IT Infrastructure Library は英国 Office of Government Commerce の一部である the Central Computer and Telecommunications Agency の登録商標です。

インテル、Intel、Intel ロゴ、Intel Inside、Intel Inside ロゴ、Centrino、Intel Centrino ロゴ、Celeron、Xeon、Intel SpeedStep、Itanium、および Pentium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

ITIL は英国 The Minister for the Cabinet Office の登録商標および共同体登録商標であって、米国特許商標庁にて登録されています。

UNIX は The Open Group の米国およびその他の国における登録商標です。



Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Cell Broadband Engine は、Sony Computer Entertainment, Inc. の米国およびその他の国における商標であり、同社の許諾を受けて使用しています。

Linear Tape-Open, LTO、LTO ロゴ、Ultrium、および Ultrium ロゴは、HP、IBM Corp. および Quantum の米国およびその他の国における商標です。





Printed in Japan

SA88-4191-02



**日本アイ・ビー・エム株式会社**  
〒103-8510 東京都中央区日本橋箱崎町19-21