

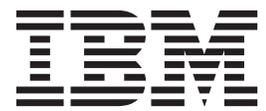
IBM Security Directory Server
バージョン 6.3.1.5

管理ガイド



IBM Security Directory Server
バージョン 6.3.1.5

管理ガイド



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、795 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: SC27-2749-02
IBM Security Directory Server
Version 6.3.1.5
Administration 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 2007, 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 ディレクトリーの概要	1
ディレクトリーの概要	1
ディレクトリー・クライアントとディレクトリー・サーバー	2
ディレクトリーのセキュリティ	2
IBM Security Directory Server の概要	3
識別名 (DN)	10
識別名の構文	10
DN エスケープ規則	12
拡張された DN の処理	12
第 2 章 サーバー管理	13
ディレクトリー管理サーバー	13
ディレクトリー管理サーバーのインスタンスの始動	14
ディレクトリー管理サーバーのインスタンスの停止	14
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・インスタンスの始動	15
構成専用モード	17
構成専用モードの最低要件	18
構成専用モードで始動する方法	18
サーバーが構成専用モードで実行中かどうかを確認する方法	19
Web 管理ツールのグラフィカル・ユーザー・インターフェース (GUI)	19
Web 管理ツールを使用するための Web アプリケーション・サーバーの始動	20
Web 管理ツールの始動	21
コンソールのレイアウト	23
コンソールのログオフ	24
Web 管理ツールでのテーブルの使用	24
Web 管理ツールのセットアップ	28
コンソール管理	28
Web 管理ツールでのシナリオ・ベースのヘルプ・ファイルの表示	32
IBM Security Directory スキーマ	32
共通スキーマ・サポート	34
オブジェクト ID (OID)	35
オブジェクト・クラス	35
属性の処理	46
サブスキーマ項目	67
IBMsubschema オブジェクト・クラス	67
スキーマの照会	67

動的スキーマ	68
許可されないスキーマの変更	69
スキーマの検査	80
iPlanet との互換性	82
一般化時刻および UTC 時刻	83
基本的なサーバー管理タスク	84
1 次管理者の識別名およびパスワードの変更	85
サーバーの開始と停止	86
サーバー状況の検査	88
キャッシュ・ステータスの表示	104
サーバー機能 (ルート DSE) 情報の表示	108
サーバー接続の管理	111
接続プロパティの管理	113
サーバー・プロパティの設定	116
サーバー・ポートの変更および言語タグの使用可能化	117
パフォーマンスの設定	118
最小 ulimit	120
検索設定	122
ページングとソートを使用したディレクトリーの検索	125
仮想リスト・ビュー	130
永続検索	131
イベント通知	132
トランザクション・サポート	135
サフィックスの追加または除去	137
トゥームストーンによる削除された項目の記録	140
キャッシュ・プロパティの管理	142
DB2 のパスワード・モニター	149
ディレクトリー通信のセキュリティ	151
セキュリティ設定の構成	151
鍵データベースの設定	179
PKCS#11	180
SSL 通信と TLS 通信の暗号化レベルの設定	182
NIST SP 800-131A のサポート	184
鍵データベースからの証明書のインポート	227
JKS 鍵データベースからの証明書のエクスポート	229
証明書取り消し検査	230
ディレクトリー・アクセス権限のセキュリティ	231
パスワード暗号化	232
パスワード・ポリシー設定	235
Kerberos のセットアップ	254
DIGEST-MD5 構成	259
固有の属性値によるバインド	261
属性 - 値の固有の組み合わせによるバインド	263
「固有の属性値によるバインド」と「属性 - 値の固有の組み合わせによるバインド」の違い	266
パスルー認証	266
管理グループ作成	291
参照	301
他の LDAP ディレクトリーへの参照の設定	302

デフォルト参照の作成	306
参照の変更	308
参照の除去	309
レプリカ生成	310
複製に関連する用語	313
複製トポロジー	315
複製の概要	316
複製合意	325
複製を構成する前に考慮する事項	326
スキーマ更新およびパスワード・ポリシー更新の複製	327
マスター - レプリカ・トポロジーの作成	328
パスワード・ポリシー運用属性の複製	339
ピア複製を持つ単純なトポロジーのセットアップ	349
マスター - 転送 - レプリカ・トポロジーの作成	356
ピア複製を持つ複雑なトポロジーのセットアップ	362
マスターレプリカ構成の構成解除	368
ゲートウェイ・トポロジーのセットアップ	370
部分複製	380
複製トポロジー情報の除外	387
リカバリ手順	388
マルチスレッド複製	392
複製エラー・テーブル	393
複製を管理するための Web 管理タスク	394
複製を管理するためのコマンド行タスク	421
分散ディレクトリー	425
プロキシ・サーバー	425
サブツリー内のデータの分割	430
情報の同期化	434
区画項目	435
プロキシ・サーバーを持つ分散ディレクトリーのセットアップ	435
分散ディレクトリーでのスキーマの更新	448
分散ディレクトリーのパスワード・ポリシー	450
フェイルオーバーおよびロード・バランシング	450
バックエンド・サーバーの重みによる優先順位付け	454
プロキシ・サーバー間のフェイルオーバー	454
プロキシ・サーバーを使用した分散ディレクトリーのバックアップ複製の設定	455
ディレクトリー・サーバーをバックアップおよびリストアする	466
ディレクトリー・サーバー・インスタンス情報全体のバックアップ	466
データベース情報のみのバックアップ	468
拡張バックアップ	468
Web 管理の使用	469
コマンド・ラインの使用	475
ロギングのユーティリティー	476
デフォルト・ログのパス	477
ログ管理ツール	478
デフォルトのログ管理	479
グローバル・ログ設定の変更	480
管理サーバー・ログ設定の変更	481
管理サーバー監査ログの使用可能化と管理監査ログ設定の変更	484

管理サーバー監査ログの使用不可化	487
事前監査レコードの構成	488
サーバーの監査ログ設定	488
監査ログを使用不可にする	496
パフォーマンスのプロファイル作成	496
Bulkload ログ設定の変更	499
構成ツール・ログ設定の変更	501
DB2 ログ設定の変更	503
逸失および検出ログ設定の変更	504
サーバー・ログの変更	506
サーバー・トレースの開始と終了	508
IBM Security Directory Server ログの表示	509
CBE および CARS フォーマットへのログの統合	515

第 3 章 ディレクトリー管理 525

ディレクトリー項目	525
ツリーのブラウズ	525
項目の追加	526
属性の複数値の追加	528
属性のバイナリー・データ	528
言語タグ	530
項目の削除	534
項目の変更	535
項目の再作成	537
項目のアクセス・コントロール・リストの編集	538
補助オブジェクト・クラスの追加	539
補助オブジェクト・クラスの削除	540
ディレクトリー項目の検索	541
アクセス制御リスト	546
概説	546
ACL タイプの使用法のシナリオ	548
アクセス制御属性の構文	549
伝搬の概要	555
アクセス評価	556
ACL の処理	558
サブツリー複製に関する考慮事項	569
グループと役割	569
グループ (Groups)	570
静的グループ項目の作成	578
動的グループ項目の作成	580
ネストされたグループ項目の作成	581
グループ・タスクの確認	582
グループ項目のメンバーの管理	583
項目のメンバーシップの管理	585
動的グループの memberURL の編集	587
役割	588
検索制限グループ	588
検索制限グループの作成	589
検索制限グループの変更	591
検索制限グループの再作成	592
検索制限グループの除去	592
プロキシ許可グループ	593
プロキシ許可グループの作成	594
プロキシ許可グループの変更	596
プロキシ許可グループの再作成	597

プロキシー許可グループの除去	598	パスワード・ポリシー照会	670
第 4 章 ユーザー関連のタスク	599	パスワード・ポリシーのオーバーライドおよびア カウントのアンロック	671
レルム、テンプレート、ユーザー、およびグループ	599	複数のパスワード・ポリシー属性の複製	672
レルムの作成	599	パスワード・ポリシー運用属性の複製	672
レルム管理者の作成	599	項目に対する強制追加または強制更新	674
テンプレートの作成	602	付録 I. IBM Security Directory Server	
レルムへのテンプレートの追加	604	の必須属性定義	675
グループの作成	604	付録 J. サーバー・インスタンス間の両	
レルムへのユーザーの追加	605	方向の暗号化の同期	703
レルムの管理	605	付録 K. フィルターに掛けられた ACL	
テンプレートの管理	607	およびフィルターに掛けられていない	
ユーザー管理	611	ACL – サンプル LDIF ファイル	705
グループ管理	613	付録 L. 動的に変更される属性	713
付録 A. エラー・コード	617	付録 M. IBM Security Directory	
付録 B. ルート DSE 内部のオブジェク ト ID (OID) および属性	623	Server のバックアップおよび復元	717
ルート DSE 内の属性	623	Security Directory Server のディレクトリー・スキ マおよびデータベース定義	717
サポートされ、使用可能になっている機能の OID	625	Security Directory Server のディレクトリー・ス キーマ	718
ACI 機構の OID	636	Security Directory Server ディレクトリー・デー タベースおよびテーブル・スペース	718
拡張操作の OID	636	Security Directory Server の変更ログ・デー タベースおよびテーブル・スペース	721
コントロールの OID	638	LDAP のバックアップと復元の手順の概要	722
付録 C. LDAP データ交換フォーマット (LDIF).	641	ディレクトリー・データベースのオフライン・バ ックアップおよびリストアの手順の例	723
LDIF の例	641	複製に関する考慮事項	724
バージョン 1 LDIF サポート	642	Security Directory Server のオンライン・バックアッ プと復元の手順の概要	724
バージョン 1 LDIF の例	642	ログの管理	724
プラットフォームでサポートされている IANA 文 字セット	643	DB2 のバックアップおよび復元の使用	727
付録 D. 33 番から 126 番までの ASCII 文字	647	付録 N. SSL セキュリティーのセットア ップ – SSL シナリオ	739
付録 E. IPv6 サポート	649	組み込み WebSphere Application Server バージョン 7.x での HTTPS の使用	739
付録 F. Simple Network Management Protocol エージェント	651	IBM Security Directory Server および IBM Security Directory Server Web 管理ツール間でのセキュア接 続の作成	740
SNMP ロギング	656	IBM Security Directory Server C ベース・クライア ントと IBM Security Directory Server 間の SSL 接 続のセットアップ	747
コマンド行の使用 – idssnmp	656	付録 G. Active Directory との同期	659
付録 H. パスワード・ポリシーに関する 追加情報	669	Active Directory との同期を使用する場合の手順	660
パスワード・ポリシー運用属性	669	Active Directory との同期で使用されるファイル	661
パスワード・ポリシーの応答制御の相互運用性サポ ート	670	Active Directory との同期の実行	665
		Active Directory への SSL 接続を使用するための Active Directory との同期の構成	665

付録 O. 高可用性のシナリオ	753
付録 P. 参照整合性プラグイン	755
付録 Q. IBM Security Directory Server と z/OS IBM Security Directory Server との間の相互運用性の ガイドライン	757
スキーマに関する考慮事項	757
ディレクトリー項目のインポートまたはエクスポート	759
機能に関する考慮事項	760

付録 R. LDAPSync	761
LDAPSync の概念	761
LDAPSync のインストール	762
LDAPSync の構成	763
LDAPSync の実行	767
LDAPSync 操作	769
LDAPSync プロパティ	770
LDAPSync ログ・ファイル	778
索引	783
特記事項	795

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 管理ガイド*」では、Web 管理ツールおよびコマンド行を使用して管理者タスクを実行する方法について説明します。

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、SA88-4191-01

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ーの実施について

IT システム・セキュリティーには、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ー対策が、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ー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 ディレクトリーの概要

ここで提供されている情報を使用して、ディレクトリーの概要についての詳細を知ることができます。さらに、ディレクトリーの定義、識別名、および IBM Security Directory Server についてもここで説明します。

ディレクトリーの概要

ディレクトリーは、階層構造に配置されるオブジェクトに関する情報のコレクションです。ディレクトリーは、特定のタスクに必要とされる特性を持つリソースをユーザーやアプリケーションが検索できるようにするためのデータ・リポジトリーです。

オブジェクトの名前がわかっている場合は、その特性の検索が可能です。個々のオブジェクトの名前がわからない場合は、特定の要件を満たす一連のオブジェクトをディレクトリーから検索できます。一般にディレクトリーは、事前定義された一連の特性によってだけでなく、特定の基準によっても検索できます。

ディレクトリーは、汎用のリレーショナル・データベースとは異なる特性を持つデータ・リポジトリーです。ディレクトリーの特徴は、更新（書き込み）されるよりも、アクセス（読み取りまたは検索）される回数の方が圧倒的に多いということです。ディレクトリーは、大量の読み取り要求に対応できなければならないため、通常は、読み取りアクセス性能が最適化されています。ディレクトリーは、汎用データベースと同等の機能を提供することが目的ではありません。最適化することにより、より多くのアプリケーションが、大規模な分散環境に配置されたディレクトリー・データに対し高速かつ経済的にアクセスできるようになります。

ディレクトリーは、1 個所にまとめて配置することもできますし、分散して配置することもできます。ディレクトリーを 1 個所に配置する場合は、ディレクトリー・アクセスを提供する 1 つのディレクトリー・サーバーを 1 つの場所に配置する必要があります。ディレクトリーを分散して配置する場合は、通常は地理的に分散した複数のサーバーがディレクトリーへのアクセスを提供します。

ディレクトリーを分散して配置する場合は、ディレクトリーに保管される情報を分割、または複製します。情報を分割する場合、それぞれのディレクトリー・サーバーには、他のサーバーとは重複しない、全体の情報の一部が保管されます。つまり、各ディレクトリー項目は 1 台のサーバーのみで保管されます。ディレクトリーを区画化するために使用する技法の 1 つが、LDAP 参照です。LDAP 参照は、クライアントに指示するサーバーから返されるものであり、Lightweight Directory Access Protocol (LDAP) 要求に、別個（または同一）のサーバーに保管された同一（または別個）の名前空間を参照させるようにします。またプロキシ・サーバーを使用すれば、参照を使用せずに分割を行えます。情報を複製する場合は、複数のサーバーに同じディレクトリー項目が保管されます。分散ディレクトリーでは、一部の情報が区画化され、一部の情報が複製される、ということもあります。

ディレクトリー・クライアントとディレクトリー・サーバー

クライアントとサーバーに関連したディレクトリーへのアクセス方法について説明します。

ディレクトリーには、クライアント/サーバー型の通信モデルを使用してアクセスします。ディレクトリー・クライアントとディレクトリー・サーバーは、同じマシン上に存在しない場合があります。サーバーは、複数のクライアントにサービスを提供することができます。ディレクトリーの情報を読み取り/書き込みする場合、アプリケーションは、そのディレクトリーに直接アクセスするのではなく、メッセージを別のプロセスに送る関数またはアプリケーション・プログラミング・インターフェース (API) を呼び出します。この 2 番目のプロセスが、要求を出したアプリケーションに代わって、ディレクトリーの情報にアクセスします。このプロセスによって読み取り/書き込みされた結果が、要求を出したアプリケーションに戻されます。

API は、特定のプログラミング言語がサービスにアクセスする際に使用するプログラミング・インターフェースを定義します。クライアントとサーバーとの間で交換されるメッセージの形式と内容は、同意されたプロトコルに従っている必要があります。LDAP は、ディレクトリー・クライアントとディレクトリー・サーバーが使用するメッセージ・プロトコルを定義します。C 言語向けに関連付けられた LDAP API もあります。Java Naming and Directory Interface (JNDI) を使用して、Java アプリケーションからディレクトリーにアクセスする方法もあります。

ディレクトリーのセキュリティー

ディレクトリーは、セキュリティー・ポリシーをインプリメントするのに必要な基本的な機能をサポートしている必要があります。

ディレクトリーは、基盤となるセキュリティー機能を直接には提供していない場合があります。とはいえディレクトリーは、基本的なセキュリティー・サービスを提供するトラステッド・ネットワーク・セキュリティー・サービスと統合できる場合があります。その場合、最初に必要となるのは、ユーザー認証方式です。認証では、ユーザーが偽りのない本人であるかどうかを検査されます。ユーザー名とパスワードは、基本的な認証方式の 1 つです。ユーザーが認証されたら、要求された操作を特定のオブジェクトに対して実行する権限や許可がそのユーザーに付与されているかどうかを判断する必要があります。

一般に許可は、アクセス・コントロール・リスト (ACL) に基づいて判断されます。ACL は、ディレクトリー内のオブジェクトや属性に付加できる許可を記述したリストです。ACL には、ディレクトリー項目およびディレクトリー・オブジェクトで各ユーザーやグループに対して許可または禁止されているアクセスのタイプがリストされています。ACL をコンパクトにして管理しやすくするため、多くの場合、同じアクセス権を持つユーザー同士をグループ化します。または、ACL にフィルターを適用します。詳細については、546 ページの『アクセス制御リスト』を参照してください。

IBM Security Directory Server の概要

Security Directory Server には、Internet Engineering Task Force (IETF) LDAP V3 仕様がインプリメントされています。また、IBM により追加された、関数やパフォーマンスに関する機能強化も組み込まれています。

本バージョンでは、IBM DB2® をバックキング・ストアとして使用することにより、LDAP 操作単位のトランザクション整合性、パフォーマンスに優れた操作、およびオンラインによるバックアップ/復元機能を提供しています。IBM Security Directory Server は、IETF LDAP V3 ベースのクライアントと相互に運用されます。

本製品の主要な機能を以下に示します。

- 動的拡張可能なディレクトリー・スキーマ – 管理者は新しい属性やオブジェクト・クラスを定義して、ディレクトリー・スキーマを拡張することができます。ディレクトリー・スキーマに変更を加えることもでき、この変更は整合性検査の対象になります。ユーザーは、ディレクトリー・サーバーを再始動せずに、スキーマの内容を動的に変更できます。スキーマ自体もディレクトリーの一部であるため、スキーマの更新は、標準 LDAP API を介して行われます。LDAPv3 動的拡張可能スキーマで提供される主要機能を以下に示します。
 - LDAP API を介した検索可能なスキーマ情報
 - LDAP API を介した動的なスキーマ変更
 - サーバーのルート DSE
- ネイティブ言語サポート – IBM Security Directory Server は、UTF-8 (Universal Character Set Transformation Format) 文字セットをサポートしています。この Unicode (または UCS) 変換フォーマットは 8 ビットのエンコード方式で、既存の ASCII ベースのシステムで簡単に使用できるように設計されています。IBM Security Directory Server は、複数言語のデータもサポートしており、ネイティブ言語のコード・ページで情報を保管、取得、および管理することができます。
- 複製 – この機能により、ディレクトリーのコピーが、より多く作成できるようになり、ディレクトリー・サービスのパフォーマンスと信頼性が向上します。複製トポロジーでは、転送サーバーとゲートウェイ・サーバーもサポートされます。
- セキュリティー機能 – IBM Security Directory Server は、豊富なセキュリティー機能セットを提供します。

識別および認証

識別および認証は、LDAP クライアントの身元確認に使用されます。つまり、ユーザーが自身が申告しているユーザー自身であるか検査する際に使用されます。ユーザー名とパスワードは、基本的な認証方式の 1 つです。このユーザー ID を使用することで、アクセス権が決定され、ユーザーのアカウントビリティが確保されます。

Simple Authentication and Security Layer (SASL)

このサポートにより、認証メカニズムが強化されます。詳しくは、151 ページの『Web 管理の使用』 および 259 ページの『DIGEST-MD5 構成』を参照してください。

Secure Sockets Layer (SSL) および Transaction Layer Security (TLS)

このサポートでは、データの暗号化と X.509v3 公開鍵証明書を使用した認証を行うことができます。サーバーでの実行は、SSL サポートと TLS

サポートのどちらか一方をオン、両方をオン、両方オフのいずれにも構成することができます。詳しくは、154 ページの『Secure Sockets Layer』および 154 ページの『Transaction Layer Security』を参照してください。

アクセス制御

ユーザーが認証されたら、要求された操作を特定のオブジェクトに対して実行する権限や許可がそのユーザーに付与されているかどうかを判断する必要があります。一般に許可は、アクセス・コントロール・リスト (ACL) に基づいて判断されます。ACL は、ディレクトリー内のオブジェクトや属性に付加できる許可を記述したリストです。ACL には、各ユーザーやユーザー・グループに対して許可または禁止されているアクセスのタイプがリストされています。ACL をコンパクトにしてより管理しやすくするために、同じアクセス権を持つユーザーをグループ化したり、ACL にフィルターを適用したりすることがよくあります。ディレクトリー管理者は、個々のユーザーまたはグループのオブジェクトに対するアクセス権を指定することで、アクセス・コントロールを管理できます。ユーザーそれぞれのアクセス権が異なっても、委任された権限を使用すると操作を実行できます。委任された権限の場合、ユーザーには、委任されたユーザー ID と、その委任されたユーザー ID の ACL 制限が適用されます。詳細については、546 ページの『アクセス制御リスト』を参照してください。

監査 IBM Security Directory Server は、ユーザー認証や、ディレクトリー・ツリーの変更といった、セキュリティー関連のイベントを監査できます。この監査機能により、時刻、ユーザー ID、操作に関する詳細情報を含む監査記録が生成されることで、アカウントビリティーを確保するための手段が提供されます。ディレクトリー管理者は、監査可能イベントの選択など、監査機能の動作を管理します。管理者は、監査のレビューおよび監査ファイルの消去も管理します。詳細については、488 ページの『サーバーの監査ログ設定』を参照してください。

セキュリティー役割

IBM Security Directory Server は、5 つの異なるセキュリティー役割をサポートしています。

プライマリー・ディレクトリー管理者

プライマリー・ディレクトリー管理者は特定のユーザー・アカウントに関連付けられます。LDAP サーバーのプライマリー・ディレクトリー管理者アカウントは 1 つだけ作成できます。プライマリー・ディレクトリー管理者は、LDAP サーバーを管理するためのすべての権限を持ちます。プライマリー・ディレクトリー管理者は、製品のインストールおよび構成中に作成されます。プライマリー・ディレクトリー管理者は、ユーザー ID、パスワード、およびディレクトリー全体を操作するための定義済みの権限から構成されます。プライマリー・ディレクトリー管理者は、ユーザーのセキュリティー役割を作成します。これは、特定の識別名 (DN)、ユーザー・パスワード、およびその特定のユーザーを表す他の属性を含む LDAP 項目です。またプライマリー・ディレクトリー管理者は、ユーザーが項目に対して所有する権限のレベルを定義します。

管理グループ・メンバー

管理グループ・メンバーは、管理特権のサブセットを割り当てられたユーザーです。管理グループは、ディレクトリー管理者が限定的な一連の管理用タスクを委任するために使用できる方法です。タスクは、1 つ以上の個別ユーザー・アカウントに委任することができます。サーバー管理グループ・メンバーにはさまざまな役割が明示的に割り当てられ、その役割により、グループ・メンバーに実行の権限があるタスクが定義されます。これらの管理役割には、パスワード管理者やサーバー始動/停止管理者などの特殊な役割が含まれています。詳細については、291 ページの『管理グループ作成』を参照してください。

グローバル管理グループ・メンバー

グローバル管理グループを使用すると、ディレクトリー管理者は、データベース・バックエンドに対する管理権限を分散環境で委任することができます。グローバル管理グループ・メンバーは、管理グループと同じ特権セットが割り当てられたユーザーです。このメンバーには、データベース・バックエンドの項目に対するアクセス権があります。グローバル管理グループ・メンバーは、ディレクトリー・サーバー・バックエンドにアクセスできません。グローバル管理グループ・メンバーは、監査ログにアクセスできません。監査ログは、ローカル管理者がグローバル管理グループ・メンバーのアクティビティをモニターするために使用できます。

グローバル管理グループ・メンバーには、ディレクトリー・サーバーの構成設定に関連するデータまたは操作に対するアクセス権はありません。ディレクトリー・サーバーの構成設定は一般に、構成バックエンドと呼ばれます。すべてのグローバル管理グループ・メンバーは同じ特権セットを所有します。

注: グローバル管理グループ・メンバーには、管理制御権を送る権限があります。

LDAP ユーザー

LDAP ユーザーは、ACL によって決定される特権を所有するユーザーです。各 LDAP ユーザーは、そのユーザーの認証情報および権限情報を含む LDAP 項目により識別されます。またこの認証および権限情報により、ユーザーは他の項目を照会したり、更新したりできます。使用されている認証のタイプに応じて、ユーザーの資格情報が検証に合格すれば、そのユーザーは、自身に権限が付与されている項目の属性にアクセスできるようになります。

マスター・サーバー DN

マスター・サーバー DN は、複製で使用される役割です。この役割では、マスター・サーバー DN として DN が定義されているレプリカまたは転送レプリカの複製コンテキストの下の項目を更新できます。マスター・サーバー DN は、レプリカまたは転送レプリカに複製コンテキスト項目を作成できます。DN が特定の複製コンテキストに対するマスター・サーバー DN として定義され

ている場合、または汎用マスター・サーバー DN として定義されている場合、マスター・サーバー DN はその複製コンテキストを作成できます。

マスター・サーバー DN は、AES バインド・コントロールを送信することで、AES で暗号化されたデータをレプリカに送信できます。

以下は、マスター・サーバー DN に関する重要事項です。

- サーバーの構成ファイルで複数のマスター・サーバー DN を定義できます。デフォルトの、または汎用の `ibm-slappedMasterDN` を含むことのできる `ibm-slappedReplication` オブジェクトが 1 つあります。また、複数の `ibm-slappedSupplier` オブジェクトがあって、それぞれで特定の複製コンテキストの (つまり、特定のサブツリーに限定される) `ibm-slappedMasterDN` を定義している、という場合もあります。管理パスワード・ポリシーはこれらのすべてに適用されます。
- これらのマスター・サーバー DN はすべてディレクトリーにバインドできます。
- これらすべてのマスター・サーバー DN には、サーバーの構成ファイル内の項目

```
cn=Directory, cn=RDBM Backends, cn=IBM Directory,  
cn=schemas, cn=Configuration
```

の `ibm-slappedSuffix` 属性を更新する権限があります。マスター・サーバー DN は、構成ファイルのその他の項目には読み取りアクセスまたは書き込みアクセスできません。

- マスター・サーバー DN は、構成ファイルのその他の部分にはアクセスできません。
- 汎用マスター・サーバー DN または `cn=IBMPOLICIES` コンテキストのマスター・サーバー DN がスキーマに更新アクセスできます。
- 特定コンテキストのマスター・サーバー DN は、そのコンテキスト内のすべての項目に完全読み取りアクセスおよび完全書き込みアクセスできます。
- 汎用マスター・サーバー DN は、すべてのコンテキスト内のすべての項目に完全読み取りアクセスおよび完全書き込みアクセスできます。

パスワード・ポリシー

IBM Security Directory Server が提供するパスワード・ポリシー機能を使用すると、管理者は、管理者パスワードおよびユーザー・パスワードに使用するポリシーを定義できます。管理者は、パスワード・ポリシーで構文、検証、およびロックアウトに関するルールを指定することで、パスワードに制限事項を設けることができます。管理者パスワード・ポリシーの構成は、構成バックエンドに保管され、1 次管理者のみが変更できます。ユーザー・パスワード・ポリシーの構成は、LDAP ツリー内に保管され、1 次管理者または管理グループのメンバーのみ変更できます。属性値を変

更できるのは、管理者として IBM Security Directory Server にバインドした場合のみです。Security Directory Server には、3 つのタイプのパスワード・ポリシー (個別、グループ、およびグローバルのパスワード・ポリシー) があります。詳細については、235 ページの『パスワード・ポリシー設定』を参照してください。

パスワード暗号化

IBM Security Directory Server は、ユーザー・パスワードに対する無許可アクセスを防止するのに役立ちます。

管理者は、片方向暗号化形式または両方向暗号化形式のいずれかで userPassword 属性値を暗号化するようにサーバーを構成することができます。

片方向暗号化形式は以下のとおりです。

- crypt
- MD5
- SHA-1
- Salted SHA-1
- SHA-2 (SHA 224、SHA 256、SHA 384、および SHA 512)
- Salted SHA-2 (SSHA 224、SSHA 256、SSHA 384、および SSHA 512)

サーバーを構成すると、新規パスワードや変更パスワードは暗号化されます。これらのパスワードは、暗号化してからディレクトリー・データベースに保管されます。

パスワードを指定するときは、パスワードの先行文字として > 文字を、終了文字として < 文字を使用しないでください。パスワードでこれらの文字が指定されると、パスワードは間違っ暗号化され、保存されて、認証障害が発生する可能性があります。

クリア・パスワードを取得する必要があるアプリケーション (中間層認証エージェントなど) の場合、ディレクトリー管理者は、ユーザー・パスワードを両方向暗号化するかあるいは暗号化を実行しないようにサーバーを構成する必要があります。

両方向暗号化形式は以下のとおりです。

- AES

Web 管理を使用してサーバーを構成すると、以下の暗号化オプションのいずれかを選択することができます。

なし 暗号化を行いません。パスワードは平文形式で格納されます。

crypt パスワードを UNIX crypt 暗号化アルゴリズムによって暗号化してからディレクトリーに格納します。

MD5 パスワードを MD5 メッセージ・ダイジェスト・アルゴリズムによって暗号化してからディレクトリーに格納します。

SHA-1 パスワードを SHA-1 暗号化アルゴリズムによって暗号化してからディレクトリーに格納します。

Salted SHA-1

パスワードを Salted SHA-1 暗号化アルゴリズムによって暗号化してからディレクトリーに格納します。

SHA-2 パスワードを SHA-2 ファミリーの暗号化アルゴリズムによって暗号化してからディレクトリーに格納します。SHA-2 ファミリーの暗号化アルゴリズムでサポートされる暗号化スキームは、以下のとおりです。

- SHA-224
- SHA-256
- SHA-384
- SHA-512

Salted SHA-2

パスワードを Salted SHA-2 ファミリーの暗号化アルゴリズムによって暗号化してからディレクトリーに格納します。Salted SHA-2 ファミリーの暗号化アルゴリズムでサポートされる暗号化スキームは、以下のとおりです。

- SSHA-224
- SSHA-256
- SSHA-384
- SSHA-512

AES128

パスワードを AES128 アルゴリズムによって暗号化してからディレクトリーに格納します。パスワードは、項目の一部として、元のクリアな形式で取得されます。

AES192

パスワードを AES192 アルゴリズムによって暗号化してからディレクトリーに格納します。パスワードは、項目の一部として、元のクリアな形式で取得されます。

AES256

パスワードを AES256 アルゴリズムによって暗号化してからディレクトリーに格納します。パスワードは、項目の一部として、元のクリアな形式で取得されます。

デフォルト・オプションは AES256 です。変更内容は、サーバー構成ファイルのパスワード暗号化ディレクティブに登録されます。

```
ibm-SlapdPwEncryption: AES256
```

サーバー構成ファイルは以下の場所にあります。

```
<instance_directory>\etc\ibmslapd.conf
```

注:

1. UNIX の crypt 方式を使用する場合は、先頭から 8 文字のみが有効となります。
2. 片方向暗号化されたパスワードは、パスワードの比較に使用することはできませんが、暗号化解除することはできません。ログイン・パスワード

ードは、ユーザー・ログイン時に暗号化され、格納されているパスワードと比較され、一致するかどうか検証されます。

- 変更ログ – LDAP データに対する変更を記録します。これらは、ディレクトリーの更新をモニターするために、メタ・ディレクトリーまたはクライアント照会をサポートする LDAP サーバーで、別個のデータベースに記録されます。
- 動的構成 – LDAP API を使用して変更することにより、ディレクトリーにバインドし、拡張操作値を構成するデータを使用して単一の拡張操作を実行する機能が提供されます。これは、すべての LDAP クライアント・ユーティリティーで使用される標準のホスト、ポート、SSL、および認証オプションをサポートしています。さらに、実行される操作と、各拡張操作の引数を指定するための一連のオプションも定義されます。
- Web 管理ツール – IBM Security Directory Server を管理および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)。このインターフェースの管理/構成機能により、管理者は以下のアクションを実行できます。
 - ディレクトリーの初期設定
 - 構成パラメーターとオプションの変更
 - オブジェクト、オブジェクト・クラス、属性、および項目を追加したり編集したりするなど、ディレクトリーの日常操作の管理
- プロキシ・サーバー – プロキシ・サーバーは、分散ディレクトリーのフロントエンドに位置しています。プロキシ・サーバーは、ユーザー要求を効率的にルーティングし、特定の状況でのパフォーマンスを改善し、クライアントでのディレクトリー・ビューを統合します。プロキシ・サーバーは、フェイルオーバーおよびロード・バランシングを提供するサーバー・クラスターのフロントエンドとして使用することもできます。
- 管理サーバー (idsdiradm) – IBM Security Directory Server のインスタンスのリモート管理を可能にします。これは必ず IBM Security Directory Server をインストールしたマシンにインストールし、また常時実行している必要があります。
- 構成専用モード – 管理者は、始動時にエラーが発生した場合でも、サーバーへのリモート・アクセスが可能です。サーバーは、データベース・バックエンドの初期化が成功したかどうかには依存しません。管理者は、LDAP プロトコルを使用してサーバーの構成を照会したり更新したりできます。
- 属性固有制御 – この機能を構成すると、指定した属性は、単一のディレクトリー・サーバーのディレクトリー内で常に固有な値を持つようになります。
- 言語タグ – これにより、ディレクトリーは、自然言語コードを、ディレクトリーで扱われる値に関連付けることができます。また、これによりクライアントは、ディレクトリーに照会を行って、特定の自然言語要件を満たす値を取得することができます。
- 検索結果のソート – 検索で検出した項目を、指定した属性値の最初の 240 バイトを使用してソートします。
- ページ付け結果 – リスト全体ではなく、検索結果のサブセット (ページ) のみを受け取るページング機能を LDAP クライアントに提供します。
- トランザクション – アプリケーションは、一連の項目更新を 1 つのトランザクションにまとめることができます。
- 複数インスタンス – ユーザーは、サーバーに複数のディレクトリー・インスタンスを持つことができます。

- 参照 – 複数の LDAP サーバーにわたってディレクトリーを分散配置できます。その各サーバーには、ディレクトリーの全データから 1 サブセットのみが格納されます。
- 属性暗号化 - DirDataAdmin 役割および SchemaAdmin 役割が割り当てられたローカルの管理グループ・メンバーが、パスワード情報用にサポートされている暗号化スキームのサブセットを使用してディレクトリー・データベースで暗号化される属性を指定できるようになります。詳細については、60 ページの『暗号化属性』を参照してください。
- パススルー認証 - クライアントがディレクトリー・サーバーへのバインドを試行し、ユーザー資格情報がローカルにない場合に、クライアントの代理でサーバーが別の外部ディレクトリー・サーバーから、またはパススルー・サーバーから資格情報の検査を試行するメカニズムです。詳細については、266 ページの『パススルー認証』を参照してください。
- サーバー管理の SNMP - SNMP エージェントは、IBM Security Directory Integrator アセンブリー・ラインと併用できます。これにより、ディレクトリー・サーバーのパフォーマンスおよび正常性の情報をモニターおよびレポートできます。
- Active Directory との同期 - ユーザーおよびグループを既存の Microsoft Active Directory と IBM Security Directory Server インスタンスとの間で同期化するツールです。この機能は、IBM Security Directory Server 6.1 リリース以降でサポートされます。

識別名 (DN)

ディレクトリー内のすべての項目には、識別名 (DN) が付いています。DN は、ディレクトリー内の項目を一意に識別するための名前です。

例えば、DN は attribute=value の組をコンマで区切ったものから構成されます。

```
cn=Ben Gray,ou=editing,o=New York Times,c=US
cn=Lucille White,ou=editing,o=New York Times,c=US
cn=Tom Brown,ou=reporting,o=New York Times,c=US
```

ディレクトリー・スキーマ内に定義された、システム属性または制限付き属性以外の属性はいずれも DN を作成するために使用できます。コンポーネントの属性と値のペアの順序は重要です。DN は、ルートを基点として、項目が存在するレベルまでの各ディレクトリー階層レベルごとに、1 つのコンポーネントを含みます。LDAP DN は、最も特定の属性 (通常、ある種の名前) から始まります。その後属性は徐々に広範になり、最後は一般に国属性で終わります。DN の先頭のコンポーネントは、相対識別名 (RDN) と呼ばれます。RDN は項目を、同じ親を持つ他の項目と明確に区別します。上記の例では、RDN cn=Ben Gray によって、1 番目の項目を 2 番目の項目 (RDN cn=Lucille White を持つ) と区別しています。これら 2 つの DN は、それ以外は同じものです。項目の RDN を構成している attribute:value のペアは、その項目の中にも存在している必要があります。これは、DN のその他のコンポーネントには当てはまりません。

識別名の構文

このサーバーでサポートされる識別名 (DN) の構文は、RFC 2253 に基づいています。

バックス正規形式 (BNF) の構文は、以下のように定義されます。

```
<name> ::= <name-component> ( <spaced-separator> )
| <name-component> <spaced-separator> <name>

<spaced-separator> ::= <optional-space>
<separator>
<optional-space>

<separator> ::= ", " | ";"

<optional-space> ::= ( <CR> ) * ( " " )

<name-component> ::= <attribute>
| <attribute> <optional-space> "+"
<optional-space> <name-component>

<attribute> ::= <string>
| <key> <optional-space> "=" <optional-space> <string>

<key> ::= 1*( <keychar> ) | "OID." <oid> | "oid." <oid>
<keychar> ::= letters, numbers, and space

<oid> ::= <digitstring> | <digitstring> "." <oid>
<digitstring> ::= 1*<digit>
<digit> ::= digits 0-9

<string> ::= *( <stringchar> | <pair> )
| "'" *( <stringchar> | <special> | <pair> ) "'"
| "#" <hex>

<special> ::= ", " | "=" | <CR> | "+" | "<" | ">"
| "#" | ";"

<pair> ::= "¥" ( <special> | "¥" | "'" )
<stringchar> ::= any character except <special> or "¥" or "'"

<hex> ::= 2*<hexchar>
<hexchar> ::= 0-9, a-f, A-F
```

セミコロン (;) 文字は、識別名内の RDN を区切るために使用できますが、通常の表記ではコンマ (,) 文字が使用されます。

コンマまたはセミコロンの両側に、空白文字 (スペース) を付けることができます。空白文字は無視されます。また、セミコロンはコンマで置き換えられます。

'+' または '=' の前後には、スペース (' ASCII 32) 文字を付けることができます。これらの空白文字は、構文解析のときには無視されます。

値は二重引用符 ("" ACSII 34) 文字で囲まれますが、二重引用符は値の一部ではありません。引用符に囲まれた値の内部では、以下の文字を指定することができます (これらの文字は、エスケープ文字とは解釈されません)。

- スtringの先頭のスペース文字または "#" 文字
- Stringの最後のスペース文字
- ""、"="、"+", "¥", "<", ">", または ";" のいずれかの文字

もう 1 つの方法としてエスケープされる単一文字の先頭には、バックスラッシュまたは円記号 (¥ ASCII 92) を付けることができます。この方法を使用すると、上にリストされた文字、および二重引用符 ("" ACSII 34) 文字をエスケープすることができます。

この表記は、名前の共通形式に対して便利なように設計されています。以下の例は、この表記を使用して記述した識別名です。先頭は、3 つのコンポーネントを含む名前です。これらのコンポーネントの先頭は、複数値の RDN です。複数値の RDN には、複数の属性と値のペアが含まれています。複数値の RDN を使用すると、単純 CN 値が不明確な場合に、特定の項目を明確に識別することができます。

DN エスケープ規則

識別名 (DN) の文字およびその使用方法について説明します。

DN には、特殊文字を含めることができます。含めることができる特殊文字は、`,` (コンマ)、`=` (等号)、`+` (正符号)、`<` (より小)、`>` (より大)、`#` (番号記号)、`;` (セミコロン)、`¥` (円記号)、および `"` (引用符) です。

これらの特殊文字やその他の文字を DN スtringの属性値の中でエスケープするには、以下の方法を使用します。

- 方法 1: エスケープする文字が特殊文字の 1 つである場合は、その前に円記号 (`¥` ASCII 92) を付けます。以下の例は、組織名のコンマをエスケープする方法を示しています。

```
CN=L. Eagle,O=Sue¥, Grabbit and Runn,C=GB
```

これは、よく使用される方法です。

- 方式 2: エスケープする文字をバックスラッシュまたは円記号と、その文字のコードを形成する単一バイトに該当する 2 桁の 16 進数で置き換えます。文字コードは、UTF-8 コード・セットのものを使用する**必要があります**。

```
CN=L. Eagle,O=Sue¥2C Grabbit and Runn,C=GB
```

- 方式 3: 属性値全体を `"` (引用符) (ASCII 34) で囲みます。これは値の一部ではありません。引用符で囲まれた文字は、`¥` (円記号) を除き、すべてそのまま解釈されます。`¥` (円記号) を使用すると、文字をエスケープできます。エスケープできる文字は、円記号 (ASCII 92)、引用符 (ASCII 34)、前述した特殊文字、上記の 2 番目の方法にある 16 進数のペアです。例えば、`cn=xyz"qrs"abc` で引用符をエスケープするには、`cn=xyz¥"qrs¥"abc` のようにします。また、`¥` をエスケープするには以下のようにします。

```
"you need to escape a single backslash this way ¥¥"
```

`"¥Zoo"` は正しくありません。このコンテキストでは、`'Z'` をエスケープできないからです。

この形式の DN をサーバー・エンドで受け取ると、サーバーは、1 番と 2 番のエスケープ・メカニズムで DN を再フォーマットして、内部処理を行います。

拡張された DN の処理

識別名 (DN) の複合 RDN は、`+` 演算子で結合された複数のコンポーネントからなります。サーバーでは、そのような DN を持つ項目の検索サポートが強化されています。

複合 RDN は、検索操作のベースとして、任意の順序で指定できます。

```
idsldapsearch cn=mike+ou=austin,o=sample
```

サーバーは、DN 正規化の拡張操作を受け入れます。DN 正規化の拡張操作は、サーバー・スキーマを使用して DN を正規化します。この拡張操作は、DN を使用するアプリケーションに役立つ場合があります。詳細については、「*IBM Security Directory Server Version 6.3 Programming Reference*」を参照してください。

第 2 章 サーバー管理

ここで提供されている情報を使用して、サーバー管理についての詳細を知ることができます。さらに、ディレクトリー管理、構成モード、Web 管理ツール、IBM Directory スキーマ、その他さまざまな事項についてもここで説明します。

ディレクトリー管理サーバー

ディレクトリー管理サーバー `idsdiradm` により、IBM Security Directory Server のインスタンスのリモート管理が可能になります。これは、IBM Security Directory Server をインストールしたシステムにインストールし、常時実行していなければなりません。

ディレクトリー管理サーバーは、LDAP 拡張操作によって要求を受け入れ、IBM Security Directory Server の始動、停止、再始動、および状況モニターをサポートします。

ディレクトリー管理サーバーでは、構成ファイルまたは構成バックエンドへのアクセスはサポートされていません。ただし、動的更新要求はサポートされています。動的更新要求をサポートすることにより、サーバーのメモリー内の構成とサーバーの構成が継続して同期されます。例えば、管理サーバーおよびディレクトリー・サーバーの両方に影響を与える更新が構成ファイルに対して行われた場合、動的更新要求が管理サーバーとディレクトリー・サーバーの両方に送信されます。

管理サーバーでは、バインド要求のたびに構成ファイルに対してバインド DN およびパスワードを検査することはありません。代わりに、管理 DN およびパスワードのすべての変更に対して構成更新要求を発行し、有効にします。

注: すべての管理グループ・メンバーが、管理サーバーにバインドできます。

デフォルトでは、IBM ディレクトリー管理サーバーの最初のインスタンスは、以下の 2 つのポートを `listen` します。

- 非 SSL 接続用のポート 3538
- SSL 接続用のポート 3539 (SSL 通信が使用可能な場合)

ディレクトリー管理サーバーは、ルート DSE 検索の実行にも使用されます。

ディレクトリー管理サーバーを始動するには、コマンド・プロンプトからプログラム `idsdiradm` を実行します。14 ページの『ディレクトリー管理サーバーのインスタンスの始動』を参照してください。

注:

- 管理サーバーは、バージョン 3 の監査のみサポートしています。
- 管理サーバーの監査は、デフォルトですべての操作に対して有効になっていません。

- SSL 通信を使用可能にする場合は、SSL を有効にするため、ディレクトリー管理サーバーを停止して再始動する必要があります。151 ページの『Web 管理の使用』を参照してください。
- Windows システムでタイム・ゾーンを変更する場合、時間の変更を認識させるために、サーバーおよび管理サーバーを再始動します。サーバーの再始動によって、管理サーバーのログのタイム・スタンプは、サーバーのログのタイム・スタンプと一致するようになります。
- 管理サーバーでは、すべてのログ読み取りアクセスの拡張操作がサポートされています。ディレクトリー・サーバーが稼働していない場合にも、ログ・ファイルをリモート側で読み取ることができます。

ディレクトリー管理サーバーのインスタンスの始動

管理サーバーのインスタンスを開始するには、以下の手順を実行します。

このタスクについて

注: デフォルトでは、管理サーバーは、ディレクトリー・サーバー・インスタンスの作成時に始動されます。

- UNIX または Linux ベースのシステムと Windows ベースのシステムの場合は、以下のコマンドを発行します。

```
idsdiradm -I <instancename>
```

- Windows ベースのシステムの場合は、「コントロール パネル」->「管理ツール」->「サービス」を選択し、「IBM Security Directory Server Instance V6.3 -<インスタンス名> Admin Server」を選択して「開始」をクリックすることもできます。

注: Linux SLES システムの場合、管理サーバーは inittab から始動させてはいけません。その代わりに、コマンド行から手動で管理サーバーを始動させます。詳しくは、「IBM Security Directory Server Version 6.3 Command Reference」の `idsdiradm` コマンド情報を参照してください。

ディレクトリー管理サーバーのインスタンスの停止

以下に示すいずれかの方法で、管理サーバーのインスタンスを停止することができます。

このタスクについて

- ディレクトリー管理サーバーの管理 DN とパスワードをすでに構成している場合は、`ibmdirctl` コマンドを使用して管理サーバーを停止できます。このコマンドは、プラットフォームに固有のものではありません。詳しくは、「IBM Security Directory Server Version 6.3 Command Reference」の `ibmdirctl` コマンド情報を参照してください。

以下のコマンドのいずれかを発行します。

```
ibmdirctl -D <adminDN> -w <adminPW> -h <hostname>
-p <port> admstop
```

ibmdirctl コマンドはローカル側でもリモート側でも発行できます。

```
idsdiradm -I <instancename> -k
```

idsdiradm コマンドはローカル側で発行する必要があります。

- Windows ベースのシステムの場合は「サービス」パネルで、「**IBM Security Directory Server Instance V6.3 - <instancename> Admin Server**」を選択し、「停止」をクリックすることもできます。

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・インスタンスの始動

この機能により、オペレーティング・システムの始動時にディレクトリー・サーバー・インスタンスを始動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ディレクトリー・サーバー・インスタンスを自動的に始動するように設定するには、以下のいずれかのセクションを参照してください。

- 『Windows システムでの自動始動』
- 16 ページの『AIX、Linux、および Solaris システムでの自動始動』

Windows システムでの自動始動

以下に示す手順を使用して、サーバーを自動的に始動することができます。

このタスクについて

Windows システムでは、サーバー (**idsslapd** プロセス) は「サービス」ウィンドウまたは **idsslapd** コマンドを使用して、手動で始動します。「サービス」ウィンドウの「**スタートアップの種類**」を「**自動**」に更新してサーバーを自動で始動しようとすると、コンピューターの再始動時にエラーが発生します。これは、**idsslapd** プロセスを開始する前に **DB2** が実行されている必要があるからです。

手順

1. 以下のいずれかの方法で「サービス」ウィンドウを開きます。
 - 「スタート」 -> 「ファイル名を指定して実行」をクリックし、「名前」フィールドに **services.msc** と入力します。「**OK**」をクリックします。
 - 「スタート」 -> 「設定」 -> 「コントロール パネル」をクリックします。「コントロール パネル」で「管理ツール」をダブルクリックしてから「サービス」をダブルクリックします。
2. 自動始動させるディレクトリー・サーバー・インスタンスの **DB2** サービス名を見つけます。このサービス名は **DB2 - TDSV63DB2 -** から始まります (例: **DB2 - TDSV63DB2 - DSRDBM01**)。サービスをダブルクリックし、「表示名」フィールドを確認します。 **DB2 - TDSV63DB2 -** の後の名前を書き留めます。(この例では **DSRDBM01** を書き留めます。)この **DB2** の名前は後で使用します。
3. 自動始動させるディレクトリー・サーバー・インスタンスのサービスを見つけます。このサービスは **IBM Security Directory Server Instance 6.3 -** で始まっています (例えば、**IBM Security Directory Server Instance 6.3 - dsrdbm01** のようになります)。サービスをダブルクリックし、「表示名」フィールドを確認します。 **IBM Security Directory Server Instance 6.3 -** の後に続く、**idsslapd-** が先頭に付いている名前を書き留めます。(この例では **idsslapd-dsrdbm01** を書き留めます。) このインスタンス名は後で使用します。

4. 「IBM Security Directory Server Instance V6.3 - *instance_name*」ウィンドウで、「スタートアップの種類」フィールドを「自動」に変更し、次に「OK」をクリックします。システム始動時にこのサービスが自動的に始動するように設定されます。
5. 「サービス」ウィンドウを閉じます。
6. Windows レジストリーを開くため、「スタート」->「ファイル名を指定して実行」をクリックします。「名前」フィールドに `regedit` と入力します。「OK」をクリックします。「レジストリ エディタ」ウィンドウが表示されます。
7. ウィンドウの左側で、「マイ コンピューター」->「HKEY_LOCAL_MACHINE」->「SYSTEM」->「CurrentControlSet」->「Services」の順に移動します。
8. ディレクトリー・サーバー・インスタンスに対応するサービスを検索します。(この例では `idsslapd-dsrdm01` です。) サービスをクリックします。
9. ウィンドウの右側で、**DependOnService** 属性をダブルクリックします。
10. 「複数行文字列の編集」ウィンドウで、**LanmanServer** の下に DB2 サービス名 (この例では `DSRDBM01`) を追加し、「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追加されます。)
11. レジストリー・エディターを終了します。

タスクの結果

システムを再始動すると、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。

注: プロキシ・サーバーには DB2 は必要ありません。そのため、システムの始動時にプロキシ・サーバーを自動的に始動させるには、ステップ 1 (15 ページ)、3 (15 ページ)、および 4 の操作のみを実行します。

AIX、Linux、および Solaris システムでの自動始動

AIX、Linux、および Solaris システムでオペレーティング・システムの始動時にディレクトリー・サーバー・インスタンスを始動するには、`/etc/inittab` ファイルを編集して 1 行を追加する必要があります。

このタスクについて

`inittab` ファイルには、システムの始動時および通常の動作時に開始されるプロセスが指定されています。`inittab` ファイルの項目は以下の形式になっています。

```
id:runlevels:action:process
```

説明:

- `id` は、1 から 4 桁のファイル内の固有 ID です。
- `runlevels` は、そのプロセスが自動的に開始される、オペレーティング・システムのラン・レベル・モードを表しています。`runlevel` は、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。ラン・レベルの構成は、オペレーティング・システムによって異なります。特定のラン・レベル構成について詳しくは、ご使用のオペレーティング・システムのマニュアルを参照してください。

- *action* は、実行されるアクションを示しています。この場合は、プロセスがシステムの始動時に開始されることを示す値である *boot* に設定されます。
- *process* は、開始するプロセスです。

以下のいずれかの行を *inittab* ファイルに追加します。

AIX システムの場合

```
srv1:2:once:/opt/IBM/ldap/V6.3/sbin/idsslapd -I server_name > /dev/null 2>&1
#Autostart IBM LDAP Directory Server Instance
```

Linux システムの場合

```
srv1:2345:once:/opt/ibm/ldap/V6.3/sbin/ibmslapd -I server_name > /dev/null 2>&1
#Autostart IBM LDAP Directory Server Instance
```

Solaris システムの場合

```
srv1:234:once:/opt/IBM/ldap/V6.3/sbin/ibmslapd -I server_name > /dev/null 2>&1
#Autostart IBM LDAP Directory Server Instance
```

server_name は、自動的に始動させるディレクトリー・サーバー・インスタンスの名前です。

/etc/inittab ファイルに項目が追加されると、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ー) は、システムが再始動してから自動始動可能になります。

プロキシー・サーバーの始動前にすべてのフル・ディレクトリー・サーバーが稼働しているようにしてください。フル・サーバーとプロキシー・サーバーが同じコンピュータにある場合は、フル・サーバーの開始後に遅延を挿入してプロキシー・サーバーを開始します。以下の例では、*srv3:2345:wait:* および *srv4:2345:wait:* で始まる行において、これを実行しています。

```
#Autostart IBM LDAP Directory Server Instance
srv1:2345:wait:/opt/IBM/ldap/V6.3/sbin/idsslapd -I server1 > /dev/null 2>&1
#Autostart IBM LDAP Directory Server Instance
srv2:2345:wait:/opt/IBM/ldap/V6.3/sbin/idsslapd -I server2 > /dev/null 2>&1
#Autostart IBM LDAP Directory Server proxy instance
srv3:2345:wait:/opt/IBM/ldap/V6.3/sbin/idsslapd -I proxy -k > /dev/null 2>&1
#Autostart IBM LDAP Directory Server proxy instance
srv4:2345:wait:/opt/IBM/ldap/V6.3/sbin/idsslapd -I proxy > /dev/null 2>&1
```

ここで、*server1* および *server2* はフル・ディレクトリー・サーバー・インスタンス、*proxy* はプロキシー・サーバー・インスタンスです。

構成専用モード

この機能により、サーバーを構成モードのみで始動することができます。

IBM Security Directory Server は、サーバーの構成設定への LDAP アクセスをサポートしています。管理者は、LDAP プロトコルを使用してサーバーの構成を照会したり更新したりできます。この機能によって、リモート管理を使用できます。さらに堅固となり信頼性を高めるため、サーバーは、データベース・バックエンドの初期化が正常に終了しているかどうかには依存しないようになっています。

cn=configuration サフィックスがアクティブな場合のみ、サーバーを構成専用モードで始動することができます。すなわち、構成バックエンドが使用可能な限り、サーバーを開始して LDAP 要求は受け入れられます。構成専用モードを使用すると、管理者は、始動時にエラーが発生した場合でも、サーバーへのリモート・アクセスが可能です。

構成専用モードでは、以下の機能がサポートされています。

- 構成ファイルとログ・ファイルへのアクセス
- 監査
- イベント通知
- Kerberos
- SASL
- SSL

構成専用モードでは、以下の機能はサポートされていません。

- データベースへのアクセス
- 変更ログ
- パスワード・ポリシー
- レプリカ生成
- スキーマの変更
- トランザクション

構成専用モードの最低要件

この機能により、構成モードを設定するための最小要件を知ることができます。

以下の要件は、構成モードを設定するための最小要件です。

- 構成ファイルが正しい LDIF 形式になっており、サーバーはファイルを検出して読み取ることができなければなりません。
- サーバーは、構成ファイルに従ってスキーマを読み取ってロードする必要があります。
- サーバーは構成プラグインをロードする必要があります。

構成専用モードで始動する方法

構成専用モードで始動する方法については、以下の情報を参照してください。

サーバーの始動時に障害が発生した場合に、サーバーを構成専用モードで始動する必要があります。

Web 管理の使用

Web 管理ツールを使用して構成モードを開始する場合は、以下の情報を参照してください。

このタスクについて

Web 管理ナビゲーション領域の「サーバー管理」をクリックし、展開されたリストの「サーバーの始動/停止/再始動」をクリックします (この操作をまだ実行していない場合)。サーバーを構成専用モードで始動するには、「構成専用モードで始動/再始動」チェック・ボックスを選択します。

コマンド・ラインの使用

構成モードを開始するには、以下のコマンドを使用します。

このタスクについて

サーバーの始動時に `-a` または `-A` を指定します。

```
idsslapd -a -I <instancename>
```

または

```
ibmdirctl -h <hostname> -D <adminDN> -w <adminpw> -p <portnumber>  
start -- -a
```

注: `-n` または `-N` オプションを使用すると、データベース・バックエンドを使用してサーバーを指導できない場合、サーバーは始動されません (構成専用モードにはなりません)。詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の `ibmdirctl` コマンド情報を参照してください。

サーバーが構成専用モードで実行中かどうかを確認する方法

サーバーが構成専用モードで稼働しているかどうかを確認するには、**Web 管理ツール**またはコマンド行インターフェースを使用します。

Web 管理の使用

サーバーが構成専用モードで始動されている場合、停止アイコンと始動アイコンの間にある  アイコンが強調表示されます。

このタスクについて

コマンド・ラインの使用

管理サーバーが構成モードで稼働しているかどうかを確認するには、以下のコマンドを実行します。

このタスクについて

属性 `ibm-slappedisconfigurationmode` のルート DSE の検索を発行します。true に設定されている場合、サーバーは構成専用モードで実行されています。

```
idsldapsearch -s base -b " " objectclass=* ibm-slappedisconfigurationmode
```

Web 管理ツールのグラフィカル・ユーザー・インターフェース (GUI)

IBM Security Directory Server Web 管理ツールのグラフィカル・ユーザー・インターフェースを使用する場合は、以下の情報を参照してください。

IBM Security Directory Server Web 管理ツールは、Web アプリケーション・サーバーにインストールされます。例えば、IBM Security Directory Server と共に提供される組み込みバージョンの IBM WebSphere® Application Server - Express® (WAS) などです (コンソール経由で管理されます)。コンソールに追加されたサーバーは、Web 管理ツール経由で管理することができます。各サーバーにこのツールをインストールする必要はありません。

サーバーの管理では、Web 管理ツールがよく使用されます。

注: 最新バージョンの Web 管理ツールを使用して古いバージョンのディレクトリー・サーバー・インスタンスを管理する場合、一部のパネルが表示されないことがあります。

サーバーに対して Web 管理ツールの使用を開始するには、そのサーバーを構成する際に以下のタスクを実行しておく必要があります。

- サーバーを開始できるように管理 DN とパスワードを設定します。
- サーバーがプロキシ・サーバーとして構成されていない場合、構成専用モード以外の状態でサーバーを開始できるようにデータベースを構成します。
- サーバーまたは管理サーバーのいずれかが実行中であることを確認してください。

これらのタスクの詳細については、IBM Security Directory Server の資料の『インストールと構成』セクションと、13 ページの『ディレクトリー管理サーバー』を参照してください。

注: 他のアプリケーション・サーバーが稼働している場合は、Web 管理ツールがインストールされているアプリケーション・サーバーが、他のアプリケーション・サーバーと同じポート上で稼働していないことを確認してください。

Web 管理ツールを使用するための Web アプリケーション・サーバーの始動

Web 管理ツールがインストールされているアプリケーション・サーバーを始動することにより、Web 管理ツールを開始することができます。

このタスクについて

Web アプリケーション・サーバーとして WebSphere Application Server 組み込みバージョンを使用している場合、Web アプリケーション・サーバーを開始するには、以下のいずれかのファイルを使用します。これらのファイルには、Web アプリケーション・サーバーを開始するコマンドが組み込まれています。

- Windows システムの場合、`installpath\%dstools%\bin\startWebadminApp.bat`
- AIX, Linux、および Solaris システムの場合、`installpath/ldstools/bin/startWebadminApp`

ここで、`installpath` は Security Directory Server がインストールされているパスです。このパスは、以下のとおりです。

- Windows の場合 (デフォルト): `c:\Program Files\IBM\LDAP\V6.3`
- AIX および Solaris の場合: `/opt/IBM/ldap/V6.3`
- Linux の場合: `/opt/ibm/ldap/V6.3`

注: Directory White Pages のための Web アプリケーション・サーバー始動コマンドが記述されたファイルもあります。そのファイルを以下に示します。

Directory White Pages

Windows システムの場合: `installpath\%idsapps%\bin\startWpgsApp`

AIX, Linux, Solaris システムの場合: `installpath/idsapps/bin/startWpgsApp`

Web 管理ツールの始動

Web 管理ツールを開始するには、以下の手順を実行します。

このタスクについて

1. Web アプリケーション・サーバーが開始した後、以下の複数の方法で Web 管理ツールを開始できます。

- Web ブラウザーから、以下のアドレスを入力します。

`http://localhost:12100/IDSWebApp/`

- Windows システムで、以下のオプションのいずれかをクリックします。
 - 非 SSL の場合: 「スタート」->「すべてのプログラム」->「IBM Security Directory Server 6.3」->「Web 管理ツール」
 - SSL の場合: 「スタート」->「すべてのプログラム」->「IBM Security Directory Server 6.3」->「Web 管理ツール (セキュア)」
- 以下のファイルを Web ブラウザーにロードします。

- Windows システムの場合:

- `installpath\idstools\bin\idswebadmin.html` (非 SSL)
- SSL の場合、`installpath\idstools\bin\idswebadminssl.html`

`installpath` は、IBM Security Directory Server がインストールされているパスです。デフォルトでは、これは `C:\Program Files\IBM\LDAP\6.3` です。

- AIX、Linux、または Solaris システムの場合:

- `installpath/idstools/bin/idswebadmin.html` (非 SSL の場合)
- `installpath/idstools/bin/idswebadminssl.html` (SSL の場合)

`installpath` は、AIX および Solaris システムの場合は `/opt/IBM/ldap/V6.3`、Linux システムの場合は `/opt/ibm/ldap/V6.3` です。

このファイルはローカル・ホストを指し示します。必要に応じて変更できません。

Web 管理ツールのログイン・ページが表示されます。

注: Web 管理ツールがインストールされているコンピューターでブラウザーを実行している場合に限り、このアドレスが使用できます。Web 管理ツールが別のコンピューターにインストールされている場合は、**localhost** を、Web 管理ツール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。**ipconfig** コマンドを使用して、コンピューターの IP アドレスを検索することができます。

2. 以下の手順により、コンソール管理者としてコンソールにログインします。
 - 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。
 - c. 「ログイン」をクリックします。

「IBM Security Directory Server Web 管理ツール」コンソールが表示されます。

3. 以下の指示に従い、サーバーをコンソールに追加します。

- a. 以下のステップのいずれかを実行します。
 - ウィンドウの右側で「**コンソール・サーバーの管理**」をクリックします。
 - ナビゲーション領域で「**コンソール管理**」を展開し、「**コンソール・サーバーの管理**」をクリックします。サーバー・ホスト名およびポート番号の表が表示されます。
 - b. 「**追加**」をクリックします。
 - c. 「**サーバー名**」フィールドに、特定のホスト名または IP アドレスおよびサーバー・ポートで実行されている登録済み IBM Security Directory Server インスタンスを識別する、固有の名前を入力します。
 - d. 「**ホスト名**」フィールドに、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・ポート番号を指定します。
 - f. コンソールとサーバーとの通信に Secure Sockets Layer (SSL) を使用するかどうかを指定します。「**SSL 暗号化を使用可能にする**」チェック・ボックスは、SSL 対応のバージョンの IBM(R) Security Directory Server Web 管理ツールをインストールした場合にのみ表示されます。
 - g. 「**サポートされる管理サーバー**」チェック・ボックスを選択して、管理ポートの制御を使用可能にします。
 - h. 「**管理ポート**」フィールドに管理サーバー・ポート番号を指定します。
 - i. 変更を適用する場合は「**OK**」をクリックします。変更を行わずにパネルを終了する場合は「**キャンセル**」をクリックします。
4. ナビゲーション領域で「**ログアウト**」をクリックします。

「Web 管理ツール」によるディレクトリー・サーバーへのログオン

「Web 管理ツール」を使用するには、以下に示す点を考慮する必要があります。

始める前に

- 「Web 管理ツール」をインストールします。
- 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。
- ディレクトリー・サーバーにログインするには、コンソール管理ページでサーバーを登録する必要があります。

このタスクについて

必要な特権が付与されていれば、「Web 管理ツール」を使用してディレクトリー・サーバーを構成および管理することができます。ディレクトリー・サーバーには、以下のいずれかのユーザーとしてログインできます。

- 1 次管理者
- ローカル管理グループ・メンバー
- グローバル管理者グループ・メンバー
- ディレクトリー・ユーザー

注:

- バインド操作向けの固有値を持つ属性を構成した場合は、その値を DN 値の代わりに使用できます。

- 「Web 管理ツール」を使用してディレクトリー・サーバーにログインする場合、複製サプライヤー資格情報を使用することはできません。

手順

1. Web ブラウザーを開きます。
2. 以下の URL を入力します。

オプション	説明
接続タイプ	URL
非セキュア	http://host_name:12100/IDSWebApp
セキュア	https://host_name:12101/IDSWebApp

3. 「**Directory Server ログイン**」ページで、以下のアクションを実行します。
 - a. 「**LDAP サーバー名**」リストから、ディレクトリー・サーバー・インスタンスを選択します。
 - b. 「**ユーザー ID**」フィールドに、DN 値を入力します。
 - c. 「**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。
4. 「**ログイン**」をクリックします。

コンソールのレイアウト

Web 管理ツールのレイアウトが分かっていると、必要なコントロールや操作のステータスを見つけることができます。

「IBM Security Directory Server Web 管理ツール」コンソールは、次の 5 つの領域から構成されます。

バナー・エリア

バナーはページの一番上にあり、アプリケーション名「IBM Security Directory Server Web 管理ツール」と IBM のロゴが表示されます。

ナビゲーション領域

ナビゲーション領域はページの左側にあります。さまざまなコンソールまたはサーバーのタスクを表す、展開可能なカテゴリーが含まれています。使用可能なタスクは、ユーザー特権やサーバーの機能 (あるいはその両方) によって異なります。

作業域 作業域には、ナビゲーション領域で選択されたタスクに関連するタスクが表示されます。例えば、ナビゲーション領域で「**サーバー管理**」 > 「**サーバー・セキュリティーの管理 (Managing server security)**」を展開すると、作業域には「**設定**」パネルが表示されます。このパネルのタブを使用すると、サーバー・セキュリティー設定に関連するタスクを実行できます。

サーバー状況域

サーバー状況領域は作業域の上部にあります。ここにはサーバー名、サーバー・ステータス、およびログインしているユーザーのユーザー ID が表示されます。さらに、2 つのアイコン・リンクがあり、1 つはサーバーの始動/停止/再始動のリンク、もう 1 つは一般ヘルプ情報のリンクです。タスクを選択すると、選択されたタスクの名前、エラー・ログ・ファイルへのリンク、およびタスク・ヘルプのリンクが表示されます。

注: コンソール管理者としてログインしている場合、この領域にはコンソール管理者が表示され、タスク・ヘルプの目次へのリンクが示されます。

タスク状況域

タスク状況領域は作業域の下部にあります。現在のタスクの状況を表示します。

コンソールのログオフ

コンソールからログオフするには、ナビゲーション領域の「ログアウト」をクリックします。

このタスクについて

「ログアウトの正常終了」パネルに次のようなメッセージが表示されます。

サーバーから正常にログオフしました。 This action has occurred because you hit the logout button. Please note that this browser window and any other browser windows opened while you were working on the server have now expired. No further interaction can occur with the server by clicking in these windows.

You can re-login by clicking here.

このメッセージ内の **here** をクリックすると、「IBM Security Directory Server Web 管理ログイン・ページ」に戻ります。

Web 管理ツールでのテーブルの使用

IBM Security Directory Server Web 管理ツールには、属性と項目のリストなどの情報がテーブルで表示されます。

テーブルにはいくつかのユーティリティーが備わっており、これらのテーブルの項目を検索したり、編成したり、テーブル項目に対してアクションを実行したりすることができます。

テーブルのアイコン

IBM Security Directory Server Web 管理ツール・テーブルには、テーブル内の情報を編成したり見つけたりするのに役立つアイコンがあります。行っているタスクとテーブルによって、一部のアイコンが表示されることも表示されないこともあります。表示される可能性のあるアイコンの包括的なリストを以下に示します。

-  「すべて選択」アイコンをクリックすると、テーブルの項目がすべて選択されます。
-  テーブル内で選択されている項目をすべてクリアするには、「選択をすべて解除」アイコンをクリックします。
-  「行フィルターの表示」アイコンをクリックすると、テーブルのすべての列について行フィルターが表示されます。フィルター操作の詳細については、27ページの『フィルター』を参照してください。

- 
 「行フィルターの非表示」アイコンをクリックすると、テーブルのすべての列について行フィルターが非表示になります。フィルター操作の詳細については、27 ページの『フィルター』を参照してください。
- 
 「すべてのフィルターのクリア」アイコンをクリックすると、テーブルに設定されたフィルターがすべてクリアされます。フィルター操作の詳細については、27 ページの『フィルター』を参照してください。
- 
 「ソートの編集」アイコンをクリックすると、テーブルの情報がソートされます。ソートの詳細については、26 ページの『ソート』を参照してください。
- 
 テーブルに対して設定されているすべてのソートをクリアするには、「すべてのソートのクリア」アイコンをクリックします。ソートの詳細については、26 ページの『ソート』を参照してください。
- 
 テーブル・データを非表示にするには、「テーブルの縮小表示」アイコンをクリックします。
- 
 「テーブルの展開」アイコンをクリックすると、テーブル・データが表示されます。
- 
 「列の構成」アイコンをクリックすると、テーブル内の列の配置が変わります。詳細については、28 ページの『再配列』を参照してください。

「アクションの選択」メニュー

「アクションの選択」メニューには、選択したテーブルに対して可能なすべてのアクションが包括的にリストされます。

例えば、アイコンを使用してソートとフィルターの表示と非表示を切り替える代わりに、「アクションの選択」メニューを使用できます。「アクションの選択」メニューを使用してテーブル内容进行操作できます。例えば、「属性の管理」パネルでは、「表示」、「追加」、「編集」、「コピー」、および「削除」などのアクションが、ツールバーのボタンのほかに「アクションの選択」メニューにも表示されます。また、テーブルがサポートする場合は、「アクションの選択」メニューを使用して「検出ツールバーを表示」の表示と非表示を切り替えることができます。テーブル項目の検索については、27 ページの『検索』を参照してください。

「アクションの選択」メニューを使用してアクションを実行するには、以下の手順を実行します。

- 「アクションの選択」メニューをクリックします。
- 実行したいアクションを選択します（「ソートの編集」など）。

3. 「実行」をクリックします。

ペー징ング

テーブルの別のページを表示させるには、テーブルの下部にあるナビゲーション・コントロールを使用します。

ナビゲーション・フィールドに特定のページ番号を入力して「実行」をクリックすると、そのページを表示させることができます。また、「次へ」矢印と「前へ」矢印を使用してページ間を移動することもできます。

デフォルトの復元 (Restore Defaults)

この機能呼び出すと、テーブルのフィルター機能とソート機能のデフォルト設定が復元されます。

デフォルトの動作では、行フィルターが非表示になり、現在設定されているソート基準またはフィルター基準がリセットされます。テーブルのツールバーには、この機能のアイコンは用意されていません。テーブル・ユーザー・アクション・リストを使用して、この機能にアクセスすることができます。デフォルトを復元するには、テーブルに対して以下のアクションを実行します。

- 「アクションの選択」ドロップダウン・メニューをクリックして「デフォルトの復元」を選択し、「実行」をクリックします。

ソート

テーブル内の項目のソート方法を変更するには、以下の手順を実行します。

このタスクについて

手順

1. 以下のステップのいずれかを実行します。
 - テーブルの「ソートの編集」アイコンをクリックします。
 - 「アクションの選択」ドロップダウン・メニューをクリックし、「ソートを編集」を選択し、「実行」をクリックします。ソート用ドロップダウン・メニューがテーブルの各列に表示されます。
2. 「第 1 ソート」ドロップダウン・メニューから、ソートする列を選択します。ソートの対象とする他のソート可能な任意の列についても同様に操作します。
3. ドロップダウン・メニューから「昇順」「降順」を選択することによって、昇順でソートするか降順でソートするかを選択します。昇順がデフォルトのソート順序です。また、列見出しを使用してソートすることもできます。各列には小さい矢印があります。上向きの矢印は列を昇順でソートすることを意味します。下向きの矢印は列を降順でソートすることを意味します。ソート順序を変更するには、列ヘッダーをクリックします。
4. ソートの準備ができたなら、「ソート」をクリックします。

タスクの結果

すべてのソートをクリアするには、「すべてのソートのクリア」アイコンをクリックします。

検索

テーブル内の特定の項目を検出するには、以下の手順を実行します。

このタスクについて

注: 行っているタスクとテーブルによって、「**検索ツールバーの表示 (Show find toolbar)**」オプションが表示されることも表示されないこともあります。

1. 「**アクションの選択**」ドロップダウン・メニューから「**検出ツールバーを表示**」を選択し、「**実行**」をクリックします。
2. 「**検索対象 (Search for)**」フィールドに検索基準を入力します。
3. 必要に応じて、「**条件 (Conditions)**」ドロップダウン・メニューから検索条件を選択します。このメニューのオプションは以下のとおりです。
 - **含む (Contains)**
 - **前方一致 (Starts with)**
 - **後方一致 (Ends with)**
 - **完全一致突き合わせ (Exact match)**
4. 「**列 (Column)**」ドロップダウン・メニューから、検索の基準とする列を選択します。
5. 「**方向 (Direction)**」ドロップダウン・メニューから、結果を降順で表示させるか昇順で表示させるかを選択します。結果を降順で表示させるには、「**下 (Down)**」を選択します。結果を昇順で表示させるには、「**上 (Up)**」を選択します。
6. 検索結果を「**検索対象**」フィールドの大/小文字基準にも一致させる場合は、「**大文字小文字の区別**」チェック・ボックスを選択します。
7. 必要な基準を入力したら、「**検索**」をクリックして属性を検索します。

フィルター

テーブル内の項目をフィルタリングするには、以下の手順を実行します。

このタスクについて

手順

1. 以下のステップのいずれかを実行します。
 - 「**フィルターの表示**」アイコンをクリックします。
 - 「**アクションの選択**」ドロップダウン・メニューをクリックして「**行フィルターの表示**」を選択し、「**実行**」をクリックします。
2. フィルターに掛ける列の上にある「**フィルター**」をクリックします。
3. 「**条件 (Conditions)**」ドロップダウンから以下のいずれかの条件を選択します。
 - **包含**
 - **前方一致 (Starts with)**
 - **後方一致 (Ends with)**
4. フィルターで適用するテキストをフィールドに入力します。例えば、「**開始**」を選択した場合は「**C**」と入力します。

5. 大文字テキストと小文字テキストを区別する場合は、「大文字小文字の区別」チェック・ボックスを選択します。
6. 属性にフィルターを掛ける準備ができたなら、「OK」をクリックします。
7. フィルターをかけるすべての列に対して、ステップ 2 からステップ 6 を繰り返します。

タスクの結果

すべてのフィルターをクリアするには、「すべてのフィルターのクリア」アイコンをクリックします。

行フィルターを非表示にするには、「フィルターの表示」アイコンを再度クリックします。

再配列

テーブル内の列の表示順序を表示する場合や、テーブルから列を削除する場合は、「列の構成」オプションを使用します。テーブル内の列を再配列するには、以下のステップを実行します。

このタスクについて

1. 以下のステップのいずれかを実行します。
 - テーブルの「列の構成」アイコンをクリックします。
 - 「アクションの選択」ドロップダウン・メニューをクリックし、「列の構成」を選択して「実行」をクリックします。
2. テーブル内のすべての列名のリストとチェック・ボックスを含むセクションが表示されます。このセクションで、以下のステップを実行します。
 - 表示されている列を表示または除去するには、列名の横にあるチェック・ボックスを選択またはクリアします。
 - テーブル内の特定の列の表示順序を変更するには、列名を選択し、必要に応じて上矢印ボタンまたは下矢印ボタンをクリックします。
3. 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして変更内容を保存します。
 - 変更を行わずにパネルに戻るには、「キャンセル」をクリックします。

Web 管理ツールのセットアップ

Web 管理ツールをセットアップする場合は、以下の情報を参照してください。

アプリケーション・サーバーを開始したら、ディレクトリー・サーバーを管理するコンソールをセットアップする必要があります。IBM Security Directory Server Web 管理ツールのログイン・ページからコンソール管理者としてログインし、以下のタスクを実行します。

コンソール管理

「IBM Security Directory Server Web 管理ツール」コンソールを管理するには、コンソール管理者としてログインする必要があります。

コンソールのセットアップが完了したら、「ログアウト」をクリックして終了します。詳細については、24 ページの『コンソールのログオフ』を参照してください。

コンソール管理者ログインの変更

ここで説明する手順に従うことにより、コンソール管理者 ID を変更できます。

このタスクについて

コンソール管理者 ID を変更するには、以下の手順を実行します。

手順

1. ナビゲーション領域で「コンソール管理」を展開します。
2. 「コンソール管理者ログインの変更」をクリックします。
3. 新しい管理者 ID を入力します。注: 指定できるコンソール管理者 ID は 1 つのみです。指定した新しい ID で管理者 ID が置き換えられます。Web 管理ツールをデプロイした時点でのデフォルトのコンソール管理者の値は **superadmin** です。
4. 現在の管理者パスワードを入力します。パスワード **secret** は、変更するまでは新しい管理者 ID のパスワードと同じです。

コンソール管理パスワードの変更

セキュリティ上の理由から、デフォルトのコンソール管理者パスワード **secret** は、別のパスワードに変更してください。

このタスクについて

注: パスワード・ポリシーはコンソール管理者のパスワードに対しては実行できないので、管理者は、組織的な方法を実施してパスワード・ポリシーで使用した構成がコンソール管理者のパスワードに対しても実行されるようにする必要があります。

コンソール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。

手順

1. ナビゲーション領域で「コンソール管理」を展開します。
2. 「コンソール管理者パスワードの変更」をクリックします。
3. 現在のパスワードを入力します。
4. 新しいパスワードを入力します。
5. タイプミスがないことを確認するために、新しいパスワードをもう一度入力します。
6. 「OK」をクリックします。

コンソールでのサーバーの追加、変更、および除去

この機能では、コンソールでサーバーの追加、変更、および除去を行うことができます。

コンソールでサーバーを追加、編集、または削除するには、以下の手順を使用します。

コンソールへのサーバーの追加:

以下に説明する手順に従うことで、コンソールにサーバーを追加できます。

このタスクについて

手順

1. ナビゲーション領域で「**コンソール管理**」を展開します。
2. 「**コンソール・サーバーの管理**」をクリックします。サーバー・ホスト名およびポート番号をリストした表が表示されます。
3. 「**追加**」をクリックします。
4. 指定されたホスト名または IP アドレスおよびサーバー・ポートで実行されている登録済みの IBM Security Directory Server インスタンスを識別する、固有の名前を指定します。サーバー名は、「**Directory Server ログイン**」パネルの「**LDAP サーバー名**」リストに表示されます。「サーバー名」フィールドに名前が指定されていない場合、「**Directory Server ログイン**」パネルの「**LDAP サーバー名**」リストにはサーバー・インスタンスとして `hostname:port` の組み合わせが表示されます。
5. サーバーのホスト名アドレスまたは IP アドレスを入力します。(例: `servername.austin.ibm.com`)
6. 「**サポートされる管理サーバー**」チェック・ボックスを選択して、管理ポートの制御を使用可能にします。
7. ポート番号を指定するか、またはデフォルトを受け入れます。**注:** 複数のサーバー・インスタンスが同一のマシン上で実行されている場合、ホスト名は同じままでも、ディレクトリー・サーバー・インスタンスに割り当てられている正しいポートを指定する必要があります。
8. サーバーが SSL に対応しているかどうかを指定します。『**コンソール・プロパティの管理**』のステップ 5 (31 ページ) を完了します。
9. 変更を適用する場合は「**OK**」をクリックします。変更を行わずにパネルを終了する場合は「**キャンセル**」をクリックします。

コンソールでのサーバーの変更:

以下に記載する手順により、コンソールでサーバーを変更することができます。

このタスクについて

サーバーのポート番号または SSL の対応状況を変更するには、以下の手順を実行します。

手順

1. ナビゲーション領域で「**コンソール管理**」を展開します。
2. 「**コンソール・サーバーの管理**」をクリックします。サーバー・ホスト名とポート番号のリストが表示されます。
3. 変更するサーバーの横のラジオ・ボタンを選択します。
4. 「**編集**」をクリックします。
5. ポート番号を変更できます。

6. サーバーが SSL に対応しているかどうかを変更できます。SSL を使用可能にしている場合は、『**コンソール・プロパティの管理**』のステップ 5 を完了します。
7. 変更を適用する場合は「**OK**」をクリックします。変更を行わずにパネルを終了する場合は「**キャンセル**」をクリックします。

コンソールからのサーバーの除去:

以下に示す指示により、コンソールからサーバーを除去することができます。

このタスクについて

手順

1. ナビゲーション領域で「**コンソール管理**」を展開します。
2. 「**コンソール・サーバーの管理**」をクリックします。サーバー・ホスト名とポート番号のリストが表示されます。
3. 除去するサーバーの横のラジオ・ボタンを選択します。
4. 「**削除**」をクリックします。
5. サーバーを削除するかどうか確認するメッセージが表示されます。サーバーを除去する場合は「**OK**」をクリックします。サーバーを除去せずにパネルを終了する場合は「**キャンセル**」をクリックします。

コンソール・プロパティの管理

以下に示す指示により、コンソール・プロパティを管理することができます。

このタスクについて

1. ナビゲーション領域で「**コンソール管理**」を展開します。
2. 「**コンソール・プロパティの管理**」をクリックします。
3. 「**コンポーネント管理**」をクリックし、コンソール内のすべてのサーバーで使用可能にするコンポーネントを指定します。デフォルトでは、すべてのコンポーネントが使用可能です。

注: ユーザーが適切なサーバー権限を持っていなかったり、必要な機能がサーバーに備わっていない場合、管理コンポーネントやそのタスクの一部は、たとえ使用可能であっても表示されません。

4. 「**セッション・プロパティ**」をクリックし、コンソール・セッションのタイムアウト制限を設定します。デフォルト設定は、60 分です。

注: セッションは、設定した時間が経過してから 3 分から 5 分間有効である場合があります。これは、タイマー間隔に作用するアプリケーション・サーバーのバックグラウンド・スレッドによってセッションの無効化が実行されるためです。このタイマー間隔によってセッションのタイムアウト期間が延長されます。

5. 「**SSL 鍵データベース**」をクリックし、必要に応じて、Secure Sockets Layer (SSL) 経由で他の LDAP サーバーと通信できるようにコンソールをセットアップします。鍵データベースのパスとファイル名、鍵パスワード、トラステッド・データベースのパスとファイル名、トラステッド・パスワードを、該当するフィールドに設定します。サポートされるファイル・タイプは `jks` です。鍵データベ

ースと SSL の詳細については、167 ページの『iKeyman ツール』および 154 ページの『Secure Sockets Layer』を参照してください。

webadmin 検索用プロパティの管理

以下に示す情報により、webadmin 検索用のプロパティを管理できます。

このタスクについて

ユーザーは、「webadmin 検索用プロパティの管理」パネルを使用して、Web 管理検索の検索設定を構成することができます。ただし、属性値制御の制限数がサポートされていない場合、「webadmin 検索用プロパティの管理」パネルは表示されません。

webadmin 検索の検索設定を構成するには、以下のようになります。

1. ナビゲーション領域で「**コンソール管理**」を展開します。
2. 「**webadmin 検索用プロパティの管理**」をクリックします。
3. 各項目に返される属性の最大数を指定します。「**属性の数 (Number of attributes)**」をクリックした場合は、数値を入力する必要があります。選択しない場合は「**無制限**」をクリックします。
4. 各属性に返される値の最大数を指定します。「**値の数**」をクリックする場合は、数値を必ず入力してください。選択しない場合は「**無制限**」をクリックします。
5. 「**OK**」をクリックして変更を保存し、「**概要**」パネルに戻ります。

Web 管理ツールでのシナリオ・ベースのヘルプ・ファイルの表示

Web 管理ツールのシナリオ・ベースのヘルプ・ファイルを表示するには、以下のコマンドを実行します。

このタスクについて

1. IBM Security Directory Server バージョン 6.3 をインストールして、ディレクトリー・サーバー・インスタンスを作成します。詳しくは、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。
2. 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ます。
3. Web 管理ツールの「コンソール管理ログイン」パネルにログオンして、ディレクトリー・サーバー・インスタンスを追加します。
4. Web 管理ツールの「Directory Server ログイン」パネルを使用して、ディレクトリー・サーバーにログオンします。
5. Web 管理ツールの作業域の右上隅にある「？」アイコンをクリックします。これにより、目次ヘルプ・ファイルが起動します。
6. 目次ヘルプ・ファイルの末尾にサンプル・シナリオがリストされています。

IBM Security Directory スキーマ

スキーマは、データをディレクトリーに保管する方法を管理する一連の規則です。スキーマは、許可される項目のタイプ、その項目の属性構造、およびその属性の構文を定義します。

注: オブジェクト・クラスの説明や構文など、サーバーに同梱されるスキーマ情報は英語で記述されています。これは、翻訳はされていません。

データは、ディレクトリー項目を使用してディレクトリーに保管されます。項目は、必須のオブジェクト・クラスとその属性で構成されます。属性は、必須またはオプションです。オブジェクト・クラスは、項目が記述する情報の種類を指定し、項目に含まれる属性のセットを定義します。各属性には、1 つ以上の関連する値があります。項目についての詳細は、525 ページの『ディレクトリー項目』を参照してください。

IBM Security Directory のスキーマは定義済みです。ただし、追加の要件がある場合にはスキーマを変更できます。

IBM Security Directory Server は、動的スキーマをサポートしています。スキーマはディレクトリー情報の一部として公開され、サブスキーマ項目 (DN="cn=schema") 内で使用できます。このスキーマを照会する場合は `ldap_search()` API を使用し、変更する場合は `ldap_modify()` API を使用します。API について詳しくは、IBM Security Directory Server の資料の『プログラミング・リファレンス』セクションを参照してください。

このスキーマは、LDAP バージョン 3 RFC (Request For Comments) (標準仕様) に含まれるスキーマよりも多くの構成情報を持っています。例えば、ある属性のために、保守する必要がある索引を指定することができます。こうした追加の構成情報は、必要に応じてサブスキーマ項目で保守されます。追加オブジェクト・クラスが、サブスキーマ項目 `IBMsubschema` 向けに定義されています。このサブスキーマ項目には、拡張されたスキーマ情報を保持する `MAY` 属性があります。

IBM Security Directory Server では、ネーミング・コンテキスト用に定義されたスキーマを特別なディレクトリー項目 `cn=schema` に格納する必要があります。この項目には、サーバー用に定義されたスキーマがすべて含まれています。スキーマ情報を検索するには、以下の項目を使用して、`ldap_search` を実行します。

```
DN: "cn=schema", search scope: base, filter: objectclass=subschema
or objectclass=*
```

スキーマでは、以下の属性タイプの値が指定されます。

- `objectClasses` (35 ページの『オブジェクト・クラス』を参照。)
- `attributeTypes` (46 ページの『属性の処理』を参照。)
- `IBMAttributeTypes` (47 ページの『IBMAttributeTypes 属性』を参照。)
- `matching rules` (48 ページの『同等性突き合わせ規則』を参照)。
- `ldap syntaxes` (62 ページの『属性構文』を参照)。

これらのスキーマ定義の構文は、LDAP バージョン 3 RFC に基づいています。

サンプル・スキーマ項目の定義例は、以下のとおりです。

```
objectclasses=( 1.3.6.1.4.1.1466.101.120.111
NAME 'extensibleObject'
SUP top AUXILIARY )

objectclasses=(2.5.20.1
NAME 'subschema'
AUXILIARY MAY
( dITStructureRules
$ nameForms
$ ditContentRules
$ objectClasses
```

```

$ attributeTypes
$ matchingRules
$ matchingRuleUse )
objectclasses=( 2.5.6.1
NAME 'alias'
SUP top STRUCTURAL
MUST aliasedObjectName )

attributeTypes {
( 2.5.18.10 NAME 'subschemaSubentry' EQUALITY distinguishedNameMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 NO-USER-MODIFICATION
SINGLE-VALUE USAGE directoryOperation )
( 2.5.21.5 NAME 'attributeTypes'
EQUALITY objectIdentifierFirstComponentMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.3 USAGE directoryOperation )
( 2.5.21.6 NAME 'objectClasses'
EQUALITY objectIdentifierFirstComponentMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.37 USAGE directoryOperation )
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE directoryOperation )
}

ldapSyntaxes {
( 1.3.6.1.4.1.1466.115.121.1.5 DESC 'Binary' )
( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'Boolean' )
( 1.3.6.1.4.1.1466.115.121.1.12 DESC 'DN' )
( 1.3.6.1.4.1.1466.115.121.1.15 DESC 'Directory String' )
( 1.3.6.1.4.1.1466.115.121.1.24 DESC 'Generalized Time' )
( 1.3.6.1.4.1.1466.115.121.1.26 DESC 'IA5 String' )
( 1.3.6.1.4.1.1466.115.121.1.27 DESC 'INTEGER' )
( 1.3.6.1.4.1.1466.115.121.1.50 DESC 'Telephone Number' )
( 1.3.6.1.4.1.1466.115.121.1.53 DESC 'UTC Time' )
}

matchingRules {
( 2.5.13.2 NAME 'caseIgnoreMatch'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
( 2.5.13.0 NAME 'objectIdentifierMatch'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
( 2.5.13.30 NAME 'objectIdentifierFirstComponentMatch'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
( 2.5.13.4 NAME 'caseIgnoreSubstringsMatch'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.58 )
}

```

上記の例で示すように、単一の実動において、ある属性タイプの属性値をすべて指定する必要はありません。

スキーマ情報は、`ldap_modify` API を使用して変更することができます。詳しくは、IBM Security Directory Server の資料の『プログラミング・リファレンス』セクションを参照してください。DN `cn=schema` を使用することにより、属性タイプまたはオブジェクト・クラスを追加、削除、または置換できます。スキーマ・エンティティを削除するには、oid を括弧付きで (oid) と指定します。全記述を指定することもできます。スキーマ項目を追加するか、あるいは LDAP バージョン 3 定義、または IBM 属性の拡張定義、またはその両方の定義でスキーマ項目を置換できます。

共通スキーマ・サポート

この機能により、共通サポート・スキーマを使用可能にすることができます。

IBM Security Directory Server は、以下の場所で定義されている標準ディレクトリー・スキーマをサポートします。

- Internet Engineering Task Force (IETF) LDAP バージョン 3 RFC (RFC 2252 や 2256 など)
- Directory Enabled Network (DEN)
- Desktop Management Task Force (DMTF) の Common Information Model (CIM)
- Network Application Consortium の Lightweight Internet Person Schema (LIPS)

このバージョンの LDAP には、デフォルト・スキーマ構成に LDAP バージョン 3 で定義されたスキーマが含まれています。また、DEN スキーマ定義も含まれていません。

IBM は、一連の拡張共通スキーマ定義も提供しています。これは、IBM の他の製品が LDAP ディレクトリーを利用する際に共有されます。例えば、以下のものがあります。

- ePerson、グループ、国、組織、組織単位および役割、地区、都道府県などの、ホワイト・ページ・アプリケーションのためのオブジェクト
- アカウント、サービス、アクセス・ポイント、権限、認証、セキュリティー・ポリシーなどの、他のサブシステムのためのオブジェクト

オブジェクト ID (OID)

オブジェクト ID (OID) は、オブジェクトを一意に識別する 10 進数のストリングです。このオブジェクトは通常、オブジェクト・クラスまたは属性です。

これらの数値は、IANA (Internet Assigned Number Authority) から入手できます。IANA Web サイトは、<http://www.iana.org/iana/> にあります。

OID がない場合は、オブジェクト・クラス名または属性名に `-oid` を付けたものを使用します。例えば、属性 `tempID` を作成した場合は、OID を `tempID-oid` と指定できます。

オブジェクト・クラス

オブジェクト・クラスは、オブジェクトを記述するために使用できる属性のセットを指定します。例えば、オブジェクト・クラス `tempEmployee` を作成した場合、そこには、`idNumber`、`dateOfHire`、または `assignmentLength` など、臨時の従業員に関連した属性を含めることができます。

ユーザーは、組織の必要に応じて、カスタム・オブジェクト・クラスを追加することができます。IBM Security Directory Server のスキーマは、以下のような基本的なタイプのオブジェクト・クラスを提供します。

- グループ (Groups)
- ロケーション
- 組織 (Organizations)
- ユーザー (People)

注: IBM Security Directory Server に固有のオブジェクト・クラスには、プレフィックス `ibm-` が付いています。

オブジェクト・クラスの定義

オブジェクト・クラスは、タイプ、継承、および属性の特性によって定義することができます。

オブジェクト・クラス・タイプ:

オブジェクト・クラス・タイプは、構造化、抽象、および補助の 3 つのうちいずれかです。

構造化 すべての項目は、少なくとも 1 つの構造化オブジェクト・クラスに属している必要があります。このオブジェクト・クラスは、項目の基本内容を定義します。このオブジェクト・クラスは、実際のオブジェクトを表します。すべての項目が構造化オブジェクト・クラスに属する必要があるため、これは最も一般的なタイプのオブジェクト・クラスです。

抽象 このタイプは、他の(構造化) オブジェクト・クラスのスーパークラス、またはテンプレートとして使用されます。このタイプは、構造化オブジェクト・クラスのセットに共通する属性のセットを定義します。これらのオブジェクト・クラスは、抽象クラスのサブクラスとして定義された場合、定義された属性を継承します。従属オブジェクト・クラスごとに属性を定義する必要はありません。

補助 このタイプは、特定の構造化オブジェクト・クラスに属する項目に関連付けることができる追加属性を示します。項目が属することができる構造化オブジェクト・クラスは 1 つのみですが、複数の補助オブジェクト・クラスに属する必要があります。

オブジェクト・クラスの継承:

IBM Security Directory Server は、オブジェクト・クラスおよび属性の定義のためのオブジェクト継承をサポートします。新しいオブジェクト・クラスは、親クラス(複数継承)、および追加または変更された属性によって定義できます。

各項目は、1 つの構造化オブジェクト・クラスに割り当てられます。すべてのオブジェクト・クラスが、抽象オブジェクト・クラス `top` から継承します。オブジェクト・クラスは、他のオブジェクト・クラスから継承することもできます。オブジェクト・クラスの構造は、特定の項目の必須属性と許可属性のリストを決定します。オブジェクト・クラス継承は、オブジェクト・クラス定義の順序によって異なります。オブジェクト・クラスは、先行するオブジェクト・クラスからのみ継承できます。例えば、LDIF ファイルでユーザー項目のオブジェクト・クラス構造を以下のよう定義できます。

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
```

この構造では、`organizationalPerson` オブジェクト・クラスと `top` オブジェクト・クラスから継承しますが、`person` オブジェクト・クラスは、`top` オブジェクト・クラスからのみ継承します。したがって、項目に `organizationalPerson` オブジェクト・クラスを割り当てる場合は、上位オブジェクト・クラスから必須属性と許可属性が自動的に継承されます。この場合は、`person` オブジェクト・クラスです。

属性 `ibm-slapdSchemaCheck` が構成ファイル内で V3 に設定されている場合、存在できる構造化オブジェクト・クラスは各項目 1 つのみです。複数の構造化オブジェクト・クラスを追加する場合、これらのクラスには親子関係が形成されている必要があります。例えば、項目タイプ `person` の X は、以下の構造化オブジェクト・クラスを使用して定義できます。

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
```

この場合、項目 X について、子構造化オブジェクト・クラス `organizationalPerson` の `MUST` 属性を定義する必要があります。

属性 `ibm-slapdSchemaCheck` が構成ファイル内で `V3_lenient` に設定されている場合は、1 つの項目に構造化オブジェクト・クラスが 1 つ以上存在できます。複数の構造化オブジェクト・クラスを追加する場合、これらのクラスで親子関係が形成されている必要はありません。例えば、項目 `Y` も、以下の構造化オブジェクト・クラスを使用して定義できます。

```
objectClass: person
objectClass: account
```

この場合、項目 `Y` について、構造化オブジェクト・クラス `person` および `account` の `MUST` 属性を定義する必要があります。

注: IBM Security Directory Server では、属性 `ibm-slapdSchemaCheck` はデフォルトで `V3_lenient` に設定されています。

スキーマの更新操作は、処理されコミットされる前に、スキーマ・クラス階層との整合性が検査されます。

属性:

すべてのオブジェクト・クラスに、多数の必須属性とオプションの属性が含まれています。必須属性とは、オブジェクト・クラスを使用することによって項目に存在していることが必要である属性です。オプションの属性とは、オブジェクト・クラスを使用することによって項目に存在している場合がある属性です。

IBM Security Directory Server のオブジェクト・クラスの表示

スキーマ内のオブジェクト・クラスを表示するには、**Web 管理** ツールまたはコマンド行を使用します。

Web 管理の使用:

Web 管理ツールを使用してスキーマ内のオブジェクト・クラスを表示するには、以下の手順を実行します。

このタスクについて

ナビゲーション領域で「スキーマ管理」を展開して、「オブジェクト・クラスの管理」をクリックします。

読み取り専用のパネルが表示されます。このパネルでは、スキーマのオブジェクト・クラスおよびそれらの特性を参照できます。オブジェクト・クラスは、アルファベット順に表示されます。テーブル・オプションを使用して、表示するオブジェクト・クラスを探し出します。これらのオプションの使用方法については、24 ページの『Web 管理ツールでのテーブルの使用』を参照してください。

対象とするオブジェクト・クラスが見つかったと、そのタイプ、必須属性、およびオプションの属性を表示させることができます。各特性の完全なリストを表示するには、必須属性とオプション属性のドロップダウン・メニューを展開してください。

注: Web 管理ツールを使用して管理サーバーにアクセスする場合は、以下のようになります。

- 「オブジェクト・クラスの管理」パネルのステータス・バーには、ツールが管理サーバーに接続されたことを示すメッセージが表示されます。管理サーバーでサ

ポートされていないパネルにアクセスすると、そのパネルの機能がサポート外であることを示すメッセージが表示されます。

- 「オブジェクト・クラスの管理」パネルは、`ibm-supportedcapabilities` 属性の `rootDSE` にある機能に基づいて使用可能になります。

オブジェクト・クラスに関する追加情報を表示するには、以下の手順を実行します。

1. オブジェクト・クラスを選択します。
2. 「表示」をクリックします。

「オブジェクト・クラスの表示」パネルが表示されます。

このパネルには、以下の 2 つのタブがあります。「フォーマット済み表示」タブには、オブジェクト・クラス名、説明、OID、オブジェクト・クラス・タイプ、上位オブジェクト・クラス、必須属性、必須継承属性、オプションの属性、およびオプションの継承属性が表示されます。これらの情報は、印刷可能なフォーマットで表示されます。「サーバー表示」タブには、サーバーの属性ファイルで使用されているフォーマットで情報が表示されます。

完了したら、「閉じる」をクリックして「オブジェクト・クラスの管理」パネルに戻ります。

コマンド・ラインの使用:

スキーマ内のオブジェクト・クラスを表示するには、以下のコマンドを実行します。

このタスクについて

```
idsldapsearch -b cn=schema -s base objectclass=* objectclasses
```

オブジェクト・クラスの追加

この機能では、オブジェクト・クラスを追加できます。

Web 管理の使用:

以下に示す手順を使用することで、オブジェクト・クラスを追加できます。

このタスクについて

ナビゲーション領域の「スキーマ管理」が展開されていない場合は、これを展開し、「オブジェクト・クラスの管理」をクリックします。新規のオブジェクト・クラスを作成するには、以下の手順を実行します。

1. 「追加」をクリックします。注: ナビゲーション領域の「スキーマ管理」を展開し、次に「オブジェクト・クラスの追加」をクリックすることによっても、このパネルにアクセスすることができます。
2. 「一般プロパティ」タブでは、以下を行います。
 - 「オブジェクト・クラス名」を入力します。これは必須フィールドで、オブジェクト・クラスの機能を表す名前です。例えば、臨時従業員を追跡する場合に使用するオブジェクト・クラスには、`tempEmployee` と入力します。

- オブジェクト・クラスの「記述」を入力します (臨時の従業員に使用するオブジェクト・クラスなど)。
 - オブジェクト・クラスの「OID」を入力します。これは必須フィールドです。35 ページの『オブジェクト ID (OID)』を参照してください。OID を持っていない場合は、オブジェクト・クラス名に **oid** を付けたものを使用できます。例えば、オブジェクト・クラス名が **tempEmployee** であれば、OID は **tempEmployeeoid** となります。
 - メニューから 1 つ以上の「上位オブジェクト・クラス」を選択します。これを選択することにより、他の属性の継承元のオブジェクト・クラスが決定されます。通常、「上位オブジェクト・クラス」は **top** ですが、他のオブジェクト・クラスにしてもかまいません。あるいは、他のオブジェクト・クラスと組み合わせて使用することもできます。例えば、**tempEmployee** の上位オブジェクト・クラスは、**top** および **ePerson** の場合があります。
 - 「オブジェクト・クラス・タイプ」を選択します。オブジェクト・クラス・タイプについて詳しくは、35 ページの『オブジェクト・クラス・タイプ』を参照してください。
 - オブジェクト・クラスの必須属性とオプションの属性を指定して、継承された属性を表示する場合は、「属性」タブをクリックします。新しいオブジェクト・クラスを追加する場合は「OK」をクリックします。変更を行わずに「オブジェクト・クラスの管理」に戻る場合は「キャンセル」をクリックします。
3. 「属性」タブで以下の手順を実行します。
- アルファベット順にリストされた「使用可能な属性」から属性を選択したら、「必須に追加」をクリックして属性を必須にするか、「オプションに追加」をクリックして、オブジェクト・クラスのオプションの属性にします。選択した属性の該当するリストに属性が表示されます。
 - 選択するすべての属性について、このプロセスを繰り返します。
 - 属性を選択して、必要に応じて「移動先 (Move to)」または「除去」ボタンをクリックすることで、属性のあるリストから別のリストに移動したり、選択したリストから属性を削除したりできます。
 - 必須属性と継承された属性 (オプション) のリストを表示することができます。継承された属性は、「一般」タブで選択された「上位オブジェクト・クラス」に基づいています。継承された属性を変更することはできません。ただし、「一般」タブの「上位オブジェクト・クラス」を変更した場合は、継承された属性の別のセットが表示されます。
4. 新しいオブジェクト・クラスを追加する場合は「OK」をクリックします。変更を行わずに「オブジェクト・クラスの管理」に戻る場合は「キャンセル」をクリックします。

注: 属性を追加せずに「一般」タブで「OK」をクリックした場合は、新しいオブジェクト・クラスを編集することによって属性を追加できます。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、オブジェクト・クラスを追加できます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( <myobjectClass-oid> NAME '<myObjectClass>' DESC '<An object class
I defined for my LDAP application>' SUP '<objectclassinheritance>'
<objectclasstype> MUST (<attribute1> $ <attribute2>)
MAY (<attribute3> $ <attribute4> )
```

オブジェクト・クラスの変更

オブジェクトを記述するための属性のセットを指定するオブジェクト・クラスを変更することができます。

スキーマは、自由に変更できるわけではありません。変更の制限の詳細については、69 ページの『許可されないスキーマの変更』を参照してください。

Web 管理の使用:

Web 管理ツールを使用することで、オブジェクト・クラスを表示することができます。

このタスクについて

ナビゲーション領域の「スキーマ管理」が展開されていない場合は、これを展開し、「オブジェクト・クラスの管理」をクリックします。オブジェクト・クラスを編集するには、以下の手順を実行します。

手順

1. 編集するオブジェクト・クラスの隣にあるラジオ・ボタンをクリックします。
2. 「編集」をクリックします。注: 「オブジェクト・クラス」列のオブジェクト・クラス名をクリックして「オブジェクト・クラスの編集」パネルを開き、オブジェクト・クラスの属性を編集することもできます。
3. 以下のタブのいずれかを選択します。

オプション	説明
<p>以下の操作を行うには、「一般」タブを使用します。</p>	<ul style="list-style-type: none"> • 「記述」を変更します。 • 「上位オブジェクト・クラス」を変更します。メニューから 1 つ以上の上位オブジェクト・クラスを選択します。これにより、他の属性の継承元のオブジェクト・クラスが判別されます。通常、「上位オブジェクト・クラス」は top ですが、他のオブジェクト・クラスにしてもかまいません。あるいは、他のオブジェクト・クラスと組み合わせて使用することもできます。例えば、tempEmployee の上位オブジェクト・クラスは、top および ePerson の場合があります。 • 「オブジェクト・クラス・タイプ」を変更します。オブジェクト・クラス・タイプを選択します。オブジェクト・クラス・タイプについて詳しくは、35 ページの『オブジェクト・クラス・タイプ』を参照してください。 • オブジェクト・クラスの必須属性とオプションの属性を変更して、継承された属性を表示するには、「属性」タブをクリックします。変更を適用する場合は「OK」をクリックします。変更を適用せずに「オブジェクト・クラスの管理」に戻る場合は「キャンセル」をクリックします。

オプション	説明
<p>以下の操作を行うには、「属性」タブを使用します。</p>	<ul style="list-style-type: none"> • アルファベット順にリストされた「使用可能な属性」から属性を選択したら、「必須に追加」をクリックして属性を必須にするか、「オプションに追加」をクリックして、オブジェクト・クラスのオプションの属性にします。選択した属性の該当するリストに属性が表示されます。 • 選択するすべての属性について、このプロセスを繰り返します。 • 属性を選択して、必要に応じて「移動先 (Move to)」または「除去」ボタンをクリックすることで、属性をあるリストから別のリストに移動したり、選択したリストから属性を削除したりできます。 • 必須属性と継承された属性 (オプション) のリストを表示することができます。継承された属性は、「一般」タブで選択された「上位オブジェクト・クラス」に基づいています。継承された属性を変更することはできません。ただし、「一般」タブの「上位オブジェクト・クラス」を変更した場合は、継承された属性の別のセットが表示されます。

4. 変更を適用する場合は「OK」をクリックします。変更を行わずに「オブジェクト・クラスの管理」に戻る場合は「キャンセル」をクリックします。

コマンド・ラインの使用:

以下に示すコマンドを発行することにより、スキーマに含まれているオブジェクト・クラスを表示できます。

このタスクについて

```
idsldapsearch -b cn=schema -s base objectclass=* objectclasses
```

コマンド行を使用してオブジェクト・クラスを変更するには、以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=schema
changetype: modify
replace: objectclasses
objectclasses: ( <myobjectClass-oid> NAME ' <myObjectClass>' DESC ' <An object class
I defined for my LDAP application>' SUP ' <newsuperiorclassobject>'
<newobjectclasstype> MUST (<attribute1> $ <attribute2>)
MAY (<attribute3> $ <attribute4> )
```

注: 「cn=schema」項目に対する変更 - 置き換え要求では、他の項目に対する変更 - 置き換え要求では発生しない特殊な動作が発生します。通常、変更 - 置き換え要求では、指定した属性の値はすべて変更操作で指定した新規の値セットに置き換えら

れます。しかし、スキーマに適用した場合は、参照値のみが置き換えられます。それ以外の場合、この例では「myObjectClass」の定義が置き換えられますが、同時に他のすべてのオブジェクト・クラスの定義も削除されます。同じ動作は、属性タイプの値を置き換える変更 - 置き換え操作でも発生します。

オブジェクト・クラスのコピー

この機能により、オブジェクト・クラスをコピーすることができます。

Web 管理の使用:

以下に示す説明に従うことにより、Web 管理ツールを使用してオブジェクト・クラスをコピーすることができます。

このタスクについて

ナビゲーション領域の「スキーマ管理」が展開されていない場合は、これを展開し、「オブジェクト・クラスの管理」をクリックします。オブジェクト・クラスをコピーするには、以下の手順を実行します。

手順

1. コピーするオブジェクト・クラスの隣にあるラジオ・ボタンをクリックします。
2. 「コピー」をクリックします。
3. 以下のタブのいずれかを選択します。

オプション	説明
<p>以下の操作を行うには、「一般」タブを使用します。</p>	<ul style="list-style-type: none"> • 新しい「オブジェクト・クラス名」を入力します。例えば、tempEmployee を tempEmployee2 としてコピーすることができます。 • 「記述」を変更します。 • 新しい OID を入力します。35 ページの『オブジェクト ID (OID)』を参照してください。コピーしたオブジェクト・クラス用の登録済み OID がない場合は、ローカルで使用する OID を作成できます。例えば、新規のオブジェクト・クラスの名前が tempEmployee2 の場合、tempEmployee2oid という OID を使用できます。 • 「上位オブジェクト・クラス」を変更します。メニューから 1 つ以上の上位オブジェクト・クラスを選択します。これにより、他の属性の継承元のオブジェクト・クラスが判別されます。通常、「上位オブジェクト・クラス」は top ですが、他のオブジェクト・クラスにしてもかまいません。あるいは、他のオブジェクト・クラスと組み合わせて使用することもできます。例えば、tempPerson2 の上位オブジェクト・クラスは、top および ePerson の場合があります。 • 「オブジェクト・クラス・タイプ」を変更します。オブジェクト・クラス・タイプを選択します。オブジェクト・クラス・タイプについて詳しくは、35 ページの『オブジェクト・クラス・タイプ』を参照してください。 • オブジェクト・クラスの必須属性とオプションの属性を変更して、継承された属性を表示するには、「属性」タブをクリックします。変更を適用する場合は「OK」をクリックします。変更を適用せずに「オブジェクト・クラスの管理」に戻る場合は「キャンセル」をクリックします。

オプション	説明
<p>以下の操作を行うには、「属性」タブを使用します。</p>	<ul style="list-style-type: none"> • アルファベット順にリストされた「使用可能な属性」から属性を選択したら、「必須に追加」をクリックして属性を必須にするか、「オプションに追加」をクリックして、オブジェクト・クラスのオプションの属性にします。選択した属性の該当するリストに属性が表示されます。 • 選択するすべての属性について、このプロセスを繰り返します。 • 属性を選択して、必要に応じて「移動先 (Move to)」または「除去」ボタンをクリックすることで、属性をあるリストから別のリストに移動したり、選択したリストから属性を削除したりできます。 • 必須属性と継承された属性 (オプション) のリストを表示することができます。継承された属性は、「一般」タブで選択された「上位オブジェクト・クラス」に基づいています。継承された属性を変更することはできません。ただし、「一般」タブの「上位オブジェクト・クラス」を変更した場合は、継承された属性の別のセットが表示されます。

4. 変更を適用する場合は「OK」をクリックします。変更を行わずに「オブジェクト・クラスの管理」に戻る場合は「キャンセル」をクリックします。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、オブジェクト・クラスをコピーすることができます。

このタスクについて

スキーマに含まれているオブジェクト・クラスを表示するには、以下のコマンドを発行します。

```
idsldapsearch -b cn=schema -s base objectclass=* objectclasses
```

コピーするオブジェクト・クラスを選択します。エディターを使用して該当する情報を変更し、<filename> に変更を保管します。以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=schema
changetype: modify
replace: objectclasses
objectclasses: ( <mynewobjectclass-oid> NAME 'mynewObjectClass'
DESC 'A new object class I copied for my LDAP application'
SUP '<superiorclassobject>'<objectclasstype>
MUST (<attribute1> $ <attribute2>)
MAY (<attribute3> $ <attribute4> $ <attribute3> )
```

オブジェクト・クラスの削除

オブジェクトを記述するための属性のセットを指定する、オブジェクト・クラスを削除することができます。

スキーマは、自由に変更できるわけではありません。変更の制限の詳細については、69 ページの『許可されないスキーマの変更』を参照してください。

Web 管理の使用:

Web 管理ツールを使用することにより、オブジェクト・クラスを削除できます。

このタスクについて

ナビゲーション領域の「スキーマ管理」が展開されていない場合は、これを展開し、「オブジェクト・クラスの管理」をクリックします。オブジェクト・クラスを削除するには、以下の手順を実行します。

手順

1. 削除するオブジェクト・クラスの隣にあるラジオ・ボタンをクリックします。
2. 「削除」をクリックします。
3. オブジェクト・クラスを除去するときは、確認のプロンプトが出されます。オブジェクト・クラスを削除する場合は「OK」をクリックします。変更を行わずに「オブジェクト・クラスの管理」に戻る場合は「キャンセル」をクリックします。

コマンド・ラインの使用:

以下に示すコマンドを使用して、属性のセットを指定するオブジェクト・クラスを削除できます。

このタスクについて

スキーマに含まれているオブジェクト・クラスを表示するには、以下のコマンドを発行します。

```
idsldapsearch -b cn=schema -s base objectclass=* objectclasses
```

削除するオブジェクト・クラスを選択し、以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: ( <myobjectclass-oid> NAME 'myObjectClass'
DESC 'An object class I defined for my LDAP application'
SUP 'objectclassinheritance' <objectclasstype >
MUST (<attribute1> $ <attribute2>) >
MAY (<attribute3> $ <attribute4> )
```

属性の処理

この機能により、属性を処理できます。

各ディレクトリー項目は、そのオブジェクト・クラスを通じて、関連する一連の属性を持っています。オブジェクト・クラスは項目に含まれる情報のタイプを記述し

ますが、実際のデータは属性に含まれています。属性は、名前、住所、電話番号など、特定のデータ要素を保持する 1 つ以上の名前と値のペアで表されます。IBM Security Directory Server では、名前と値のペア、記述属性 (例: `commonName (cn)`)、および特定の情報の断片 (例: `John Doe`) としてデータを表します。

例えば、`John Doe` の項目には、複数の属性の名前と値のペアが含まれることがあります。

```
dn: uid=jdoe, ou=people, ou=mycompany, o=sample
objectClass: top
objectClass: person
objectClass: organizationalPerson
cn: John Doe
sn: Doe
givenName: Jack
givenName: John
```

標準属性はスキーマ・ファイルですでに定義されていますが、組織の必要に応じて、属性を作成、編集、コピー、または削除することができます。

オブジェクト・クラスのカスタム属性を作成する場合は、属性を以下のサイズに制限する必要があります。

- バイナリー・データ: 2,000,000,000 バイト
- ストリング・データ: 32,700 バイト

Web 管理ツールで上記よりも大きいサイズの属性を作成しようとすると、サーバーはエラー「長さフィールド値が範囲外です」を生成します。

IBMAttributeTypes 属性

IBMAttributeTypes 属性を使用することで、LDAP バージョン 3 規格で扱われていない属性のスキーマ情報を定義できます。

IBMAttributeTypes の値は、以下の文法に従う必要があります。

```
IBMAttributeTypesDescription = "(" whsp
numericoid whsp
[ "DBNAME"qdescribers ]; at most 2 names (table, column)
[ "ACCESS-CLASS" whsp IBMAccessClass whsp ]
[ "LENGTH" wlen whsp ]; maximum length of attribute
[ "EQUALITY"whsp ]; create index for matching rule
[ "ORDERING"whsp ]; create index for matching rule
[ "APPROX"whsp ]; create index for matching rule
[ "SUBSTR"whsp ]; create index for matching rule
[ "REVERSE"whsp ]; reverse index for substring
[ "ENCRYPT"whsp scheme whsp ]; encryption scheme
[ "SECURE-CONNECTION-ONLY"whsp ]; secure connection required
[ "RETURN-VALUE whsp returnValue whsp ]; value to be returned
[ "NONMATCHABLE whsp ] ;; attribute can only be used in existence filters
whsp ")"

scheme =
  "SSHA" /
  "AES-128" /
  "AES-192" /
  "AES-256" /
  "SHA-224" /
  "SHA-256" /
  "SHA-384" /
  "SHA-512" /
  "SSHA-224" /
  "SSHA-256" /
  "SSHA-384" /
  "SSHA-512"

returnValue =
  "encrypted" /
  "type-only"

IBMAccessClass =
  "NORMAL"/ ; this is the default
```

"SENSITIVE"/
"CRITICAL"/
"RESTRICTED"/
"SYSTEM"/

numericoid

属性タイプの値を `IBMAttributeTypes` の値と相互に関連させるために使用します。

DBNAME

最大で 2 つの名前を指定できます。最初の名前は、この属性に使用される表名です。2 番目の名前は、この表内の完全に正規化された属性値に使用される列名です。名前を 1 つだけしか指定しないと、その名前は、表名としても列名としても使用されます。`DBNAME` を指定しない場合は、(属性タイプからの) 短縮属性名が使用されます。

ACCESS-CLASS

同様のアクセス権を必要としている属性は、クラス内にグループ化されます。属性は、ディレクトリー・スキーマ・ファイル内の属性クラスにマッピングされます。これらのクラスはそれぞれ独立しています。したがって、あるクラスにアクセスしても、それが別のクラスへのアクセスを意味するわけではありません。許可は、属性アクセス・クラス全体に対して設定されます。ある特定の属性クラスに設定された許可は、個々の属性アクセス権が指定されない限り、このアクセス・クラス内のすべての属性に適用されます。

IBM では、ユーザー属性へのアクセスの評価に使用する属性クラスとして `normal`、`sensitive`、`critical`、`system`、および `restricted` の 5 つを定義しています。例えば、属性 `commonName` は `normal` クラスに属し、属性 `userPassword` は `critical` クラスに属します。ユーザー定義属性は、特に指定がない限り、`normal` アクセス・クラスに属します。詳細については、552 ページの『アクセス権』を参照してください。

`ACCESS-CLASS` を省略すると、標準 (`normal`) にデフォルト設定されます。

LENGTH

この属性の最大長です。長さは、バイト数として表されます。(IBM Security Directory Server には、属性の長さを大きくする方法が用意されています。) 属性タイプ値では、`STRING`

(`attr-oid ... SYNTAX syntax-oid{len} ...`)

は、`oid` の付いた属性タイプ (`attr-oid`) は最大長を持つ、ということを示すために使用できます。

属性の長さを小さくする必要がある場合は、56 ページの『既存の属性を変更する手作業手順』を参照してください。

EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE

上記の属性のいずれかを使用すると、対応する突き合わせ規則に従って索引が生成されます。検索のパフォーマンスを向上させるため、検索フィルターで使用する属性には、`EQUALITY` 索引を指定する必要があります。

同等性突き合わせ規則

突き合わせ規則は、検索操作のときに文字列比較を行うためのガイドラインを提供します。

突き合わせ規則は、以下の 3 つのカテゴリーに分けられます。

- 同等性
- 順序付け
- サブストリング

表 1. 同等性突き合わせ規則とその OID および構文

同等性突き合わせ規則		
突き合わせ規則	OID	構文
bitStringMatch	2.5.13.16	ビット・ストリング
booleanMatch	2.5.13.13	Boolean
caseExactIA5Match	1.3.6.1.4.1.1466.109.114.1	Directory String 構文
caseExactMatch	2.5.13.5	Directory String 構文
caseIgnoreIA5Match	1.3.6.1.4.1.1466.109.114.2	IA5 String 構文
caseIgnoreIA5SubstringsMatch	1.3.6.1.4.1.1466.109.114.3	IA5 String 構文
caseIgnoreListMatch	2.5.13.11	ディレクトリー・ストリング
caseIgnoreMatch	2.5.13.2	Directory String 構文
distinguishedNameMatch	2.5.13.1	DN - distinguished name
generalizedTimeMatch	2.5.13.27	Generalized Time 構文
ibm-entryUuidMatch	1.3.18.0.2.22.2	Directory String 構文
integerFirstComponentMatch	2.5.13.29	Integer 構文 - 整数値
integerMatch	2.5.13.14	Integer 構文 - 整数値
numericStringMatch	2.5.13.8	数値ストリング
objectIdentifierFirstComponentMatch	2.5.13.30	OID を格納するためのストリング。OID は、数字 (0 から 9) と小数点 (.) を含むストリングです。.
objectIdentifierMatch	2.5.13.0	OID を格納するためのストリング。OID は、数字 (0 から 9) と小数点 (.) を含むストリングです。
octetStringMatch	2.5.13.17	Directory String 構文
presentationAddressMatch	2.5.13.22	表示アドレス
protocolInformationMatch	2.5.13.24	プロトコル情報
telephoneNumberMatch	2.5.13.20	Telephone Number 構文
uniqueMemberMatch	2.5.13.23	名前および任意指定の UID
uTCTimeMatch	2.5.13.25	UTC Time 構文

表 2. 順序付け突き合わせ規則とその OID および構文

順序付け突き合わせ規則		
突き合わせ規則	OID	構文
caseExactOrderingMatch	2.5.13.6	Directory String 構文
caseIgnoreOrderingMatch	2.5.13.3	Directory String 構文
distinguishedNameOrderingMatch	1.3.18.0.2.4.405	DN - 識別名

表 2. 順序付け突き合わせ規則とその OID および構文 (続き)

順序付け突き合わせ規則		
突き合わせ規則	OID	構文
generalizedTimeOrderingMatch	2.5.13.28	Generalized Time 構文
integerOrderingMatch	2.5.13.15	整数
numericStringOrderingMatch	2.5.13.9	数値ストリング
octetStringOrderingMatch	2.5.13.18	オクテット・ストリング

表 3. サブストリング突き合わせ規則とその OID および構文

サブストリング突き合わせ規則		
突き合わせ規則	OID	構文
caseExactSubstringsMatch	2.5.13.7	Directory String 構文
caseIgnoreListSubstringsMatch	2.5.13.12	サブストリング・アサーション
caseIgnoreSubstringsMatch	2.5.13.4	Directory String 構文
numericStringSubstringsMatch	2.5.13.10	サブストリング・アサーション
telephoneNumberSubstringsMatch	2.5.13.21	Telephone Number 構文

注: UTC 時刻は、ASN.1 規格によって定義されたタイム・ストリング・フォーマットです。ISO 8601 および X680 を参照してください。UTC 時刻形式の時間値を格納するには、この構文を使用します。突き合わせ規則 `uTCTimeMatch` は使用しないことをお勧めします。代わりに `generalizedTimeMach` を使用してください。83 ページの『一般化時刻および UTC 時刻』を参照してください。

索引付けの規則

情報の検索をより早くするため、属性に索引付け規則を付加する必要があります。

索引を付けずに属性のみを指定すると、IBM Security Directory Server によって以下の索引付け規則が適用されます。

- 同等性
- 順序付け
- ほぼ等しい
- サブストリング
- 反転

属性向け索引付け規則の仕様:

属性に索引付け規則を指定すると、属性値に特別な索引を作成して保守することを管理できます。

索引付け規則により、索引付けされた属性を含むフィルターを使用した検索で、応答時間が向上します。以下の 5 タイプの索引付け規則が、検索フィルターで適用される操作と関連しています。

同等性 以下の検索操作に適用されます。

- equalityMatch '='

例えば、

```
"cn = John Doe"
```

順序付け

以下の検索操作に適用されます。

- greaterOrEqual '>='
- lessOrEqual '<='

例:

```
"sn >= Doe"
```

ほぼ等しい

以下の検索操作に適用されます。

- approxMatch '~='

例:

```
"sn ~= doe"
```

サブストリング

サブストリング構文を使用した検索操作に適用されます。

- substring '*'

例えば、

```
"sn = McC*"
"cn = J*Doe"
```

反転 以下の検索操作に適用されます。

- '*' substring

例:

```
"sn = *baugh"
```

検索フィルターで使用する属性には、少なくとも「同等性」の索引付けを指定することをお勧めします。

属性の表示

スキーマ内の属性を表示するには、**Web 管理** ツールまたはコマンド行を使用します。

Web 管理の使用:

スキーマに格納されている属性を表示するには、以下の手順を実行します。

このタスクについて

ナビゲーション領域で「スキーマ管理」を展開して、「属性の管理」をクリックします。読み取り専用のパネルが表示されます。このパネルでは、スキーマの属性およびそれらの特性を参照できます。属性は、アルファベット順に表示されます。テーブル・オプションを使用して、表示する属性を探し出します。これらのオプションの使用方法については、24 ページの『Web 管理ツールでのテーブルの使用』を参照してください。

注: Web 管理ツールを使用して管理サーバーにアクセスする場合は、以下のようになります。

- 「属性の管理」パネルのステータス・バーには、ツールが管理サーバーに接続されたことを示すメッセージが表示されます。管理サーバーでサポートされていないパネルにアクセスすると、そのパネルの機能がサポート外であることを示すメッセージが表示されます。
- 「属性の管理」パネルは、ibm-supportedcapabilities 属性の rootDSE にある機能に基づいて使用可能になります。

対象とする属性が見つかり、その属性が複数值かどうかに関係なく、構文および含まれるオブジェクト・クラスを表示させることができます。属性のオブジェクト・クラスのリストを参照するには、オブジェクト・クラスのドロップダウン・メニューを展開します。

属性に関する追加情報を表示するには、以下の手順を実行します。

1. 属性を選択します。
2. 「表示」をクリックします。

「属性の表示」パネルが表示されます。

このパネルには、以下の 2 つのタブがあります。「フォーマット済み表示」タブには、属性名、説明、OID、上位属性、構文、属性の長さ、複数の値が使用可能なステータス、突き合わせ規則、IBM 拡張、および索引規則が表示されます。これらの情報は、印刷可能なフォーマットで表示されます。「サーバー表示」タブには、サーバーの属性ファイルで使用されているフォーマットで情報が表示されます。

操作が完了したら、「閉じる」をクリックして IBM Security Directory Server の「属性の管理」パネルに戻ります。

コマンド・ラインの使用:

スキーマに格納されている属性を表示するには、以下のコマンドを実行します。

このタスクについて

```
idsldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

属性の追加

この機能により、属性を追加できます。

新規属性を作成するには、以下の方法が有効です。

Web 管理ツールがよく使用されます。

Web 管理の使用:

以下に示す説明に従って、Web 管理ツールを使用して属性を追加できます。

このタスクについて

ナビゲーション領域の「スキーマ管理」が展開されていない場合は、これを展開し、「属性の管理」をクリックします。新規属性を作成するには、以下の手順を実行します。

1. 「追加」をクリックします。注: ナビゲーション領域の「スキーマ管理」を展開して「属性の追加」をクリックし、このパネルにアクセスすることもできます。
2. 「属性名」を入力します (**tempId** など)。これは必須フィールドです。先頭文字は英字にする必要があります。
3. 属性の「記述」を入力します (**臨時の従業員に割り当てた ID 番号** など)。
4. 属性の「OID」を入力します。これは必須フィールドです。35 ページの『オブジェクト ID (OID)』を参照してください。登録済みの OID がない場合は、oid を付加した属性名を使用できます。例えば、属性名が **tempID** であれば、OID は **tempIDoid** となります。このフィールドの値は変更可能です。
5. ドロップダウン・リストから「上位属性」を選択します。上位属性は、プロパティを継承する元の属性を判別します。
6. ドロップダウン・リストから「構文」を選択します。構文については、62 ページの『属性構文』を参照してください。
7. この属性の最大長を指定する「属性長」を入力します。長さは、バイト数として表されます。デフォルト値は 240 です。
8. 「複数値を使用可能」チェック・ボックスを選択すると、属性に複数の値を持たせることができます。複数値について詳しくは、用語集の項目を参照してください。
9. 同等性、順序付け、およびサブストリングの突き合わせ規則の、各ドロップダウン・メニューから突き合わせ規則を選択します。突き合わせ規則の完全なリストについては、48 ページの『同等性突き合わせ規則』を参照してください。
10. 「IBM 拡張」タブをクリックして属性に追加の拡張を指定するか、「OK」をクリックして新しい属性を追加します。変更を行わずに「属性の管理」に戻るには、「キャンセル」をクリックします。
11. 「IBM 拡張」タブで以下を行います。
 - **DB2 表名**を入力します。このテーブル名の切り捨てなしの最大長は 128 バイトです。このフィールドをブランクのままにしておくと、サーバーが DB2 表名を生成します。DB2 表名を入力した場合は、DB2 列名も入力する必要があります。6.0 より前のバージョンの IBM Security Directory Server を使用しているサーバーの場合、切り捨てなしの最大長は 16 バイトに制限されます。
 - 「**DB2 列名**」を変更します。このフィールドをブランクのままにしておくと、サーバーが DB2 列名を生成します。DB2 列名を入力した場合は、DB2 表名も入力する必要があります。この列名の切り捨てなしの最大長は 16 バイトです。
 - ドロップダウン・リストから「通常」、「重要」、または「重大」を選択し、「セキュリティー・クラス」を設定します。セキュリティー・クラスについては、『セキュリティー・クラス・アクセス権』のセキュリティー・クラスのセクションを参照してください。
 - 1 つ以上の索引付け規則を選択して、索引付け規則を設定します。索引付け規則について詳しくは、50 ページの『索引付けの規則』を参照してください。注: 検索フィルターに使用する属性すべてに対して、少なくとも「同等性」の索引付けを指定することをお勧めします。
 - 「暗号化スキームの選択」ボックスから暗号化スキームを選択します。

- 属性値の検索の戻りの型を「**検索で戻す値**」ボックスから選択します。
 - 「**値を表示または変更するためセキュア接続が必要**」チェック・ボックスを選択して、暗号化属性へのアクセス時のセキュア接続を指定します。
 - 属性を検索フィルターで使用可能にするかどうかを指定するには、「**検索フィルターで属性を使用可能**」チェック・ボックスを選択します。
12. 新しい属性を追加する場合は「**OK**」をクリックします。変更を行わずに「**属性の管理**」に戻る場合は「**キャンセル**」をクリックします。

注: 拡張を追加せずに「一般」タブで「OK」をクリックした場合は、新しい属性を編集することで拡張を追加できます。

コマンド・ラインの使用:

以下に示すコマンドを使用することで、属性を追加できます。

このタスクについて

以下の例では、Directory String 構文 (62 ページの『属性構文』を参照) および大文字と小文字を区別しない突き合わせ (48 ページの『同等性突き合わせ規則』を参照) を使用して `myAttribute` という属性の属性タイプ定義を追加します。この定義の IBM 固有部分では、属性データが「`myAttrTable`」という表の「`myAttrColumn`」という列に格納されることが指定されています。これらの名前を指定しなかった場合、デフォルトでは、表名と列名の両方が「`myAttribute`」になります。この属性は「通常」アクセス・クラスに割り当てられ、値の最大長は 200 バイトになります。

```
idsldapmodify -D <admin> -w <adminpw> -i myschema.ldif
```

`myschema.ldif` ファイルには、以下の情報が格納されています。

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' )
DESC 'An attribute I defined for my LDAP application'
EQUALITY 2.5.13.2 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
{200} USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oidDBNAME ( 'myAttrTable' 'myAttrColumn' )
ACCESS-CLASS normal LENGTH 200 )
```

注: この例では、「長さ」を指定できる場所が 2 箇所あります。この例では、長さとして 200 が指定されています。例:

- {200} USAGE userApplications)
- ACCESS-CLASS normal LENGTH 200)

上記のコードのように長さを指定します。これらの両方の場所で長さを指定する場合、両方の値は一致している必要があります。

詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の `idsldapmodify` および `idsldapadd` のコマンド情報を参照してください。

属性の変更

ディレクトリー項目に関連付けられている属性は、変更することができます。属性を変更するには、**Web 管理ツール**またはコマンド行を使用します。

スキーマは、自由に変更できるわけではありません。変更の制限の詳細については、69 ページの『許可されないスキーマの変更』を参照してください。

定義した属性を使用する項目を追加する前であれば、定義のどの部分でも変更することができます。属性を使用する項目を追加してからでも、以下の編集手順を使用することにより、索引付け規則を変更し、属性長のサイズを大きくすることができます。また、複数値を使用可能にするための変更もできます。

注: 既存の項目が単一値の場合に限り、複数値を使用不可にできます。既存の項目が複数値の場合、複数値オプションは使用不可にできません。

属性を編集するには、以下のいずれかの方法を使用します。**Web 管理ツール**を使用する方法が推奨されます。

Web 管理の使用:

ここで説明する手順に従うことにより、Web 管理ツールを使用して属性を変更できます。

このタスクについて

ナビゲーション領域の「スキーマ管理」が展開されていない場合は、これを展開し、「属性の管理」をクリックします。属性を編集するには、以下の手順を実行します。

手順

1. 編集する属性の隣にあるラジオ・ボタンをクリックします。
2. 「編集」をクリックします。**注:** 「名前」列の属性名をクリックして「属性の編集」パネルを開くことでも、属性を編集することができます。
3. 以下のタブのいずれかを選択します。

オプション	説明
以下の操作を行うには、「一般」タブを使用します。	<ul style="list-style-type: none">• 「記述」を変更します。• 「上位属性」を変更します。• 「構文」を変更します。• 「属性の長さ」を設定します。注: 属性長のサイズは、増加のみ可能です。属性長のサイズを小さくする場合は、属性を編集する前に追加の手順を実行する必要があります。56 ページの『既存の属性を変更する手作業手順』を参照してください。• 「複数値」の設定を変更します。• 「突き合わせ規則」を選択します。

オプション	説明
「IBM 拡張」タブを使用して、以下を実行します。	<ul style="list-style-type: none"> • 属性の拡張を編集します。 • 「セキュリティー・クラス」を変更します。注: system または restricted というセキュリティー区分が存在する属性のセキュリティー・クラスは変更できません。 • 「索引付け規則」を変更します。 • 変更を適用する場合は「OK」をクリックします。変更を行わずに「属性の管理」に戻る場合は「キャンセル」をクリックします。

4. 属性の編集を完了したら、「閉じる」をクリックして「概要」パネルに戻ります。

コマンド・ラインの使用:

以下に示すコマンドを使用することにより、属性を変更できます。

このタスクについて

以下の例では、属性に索引付けを追加し、高速に検索できるようにします。定義を変更するには、`idsldapmodify` コマンドと LDIF ファイルを使用します。

注: 属性長のサイズは増加のみ可能です。属性長のサイズを小さくする場合は、属性を編集する前に追加の手順を実行する必要があります。『既存の属性を変更する手作業手順』を参照してください。

```
idsldapmodify -D <adminDn> -w <adminpw> -i myschemachange.ldif
```

`myschemachange.ldif` ファイルには、以下の情報が格納されています。

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' ) DESC 'An attribute
I defined for my LDAP application' EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {200} USAGE userApplications )
-
replace: ibmattributetypes
ibmattributetypes: ( myAttribute-oidDBNAME ( 'myAttrTable' 'myAttrColumn' )
ACCESS-CLASS normal LENGTH 200 EQUALITY SUBSTR )
```

注: 変更対象が `ibmattributetypes` セクションのみであっても、置換操作では、定義の両方の部分 (`attributetypes` および `ibmattributetypes`) を指定する必要があります。唯一の変更は、同等性およびサブストリング突き合わせの索引を要求するために、定義の最後に「EQUALITY SUBSTR」を追加することです。

このユーティリティーについては、「*IBM Security Directory Server Version 6.3 Command Reference*」の `idsldapadd` コマンドの情報を参照してください。

既存の属性を変更する手作業手順:

ある属性の定義を変更する必要がありますが、その属性のテーブルがすでに取り込まれている場合は、ここで説明する手順を使用できます。

このタスクについて

手順

1. LDIF ファイルにディレクトリー・データをエクスポートするには、**idsdb2ldif** ユーティリティを使用します。
2. 次のようにして、データベースを構成解除します。idsucfgdb-I
`<instance_name> -r`
3. スキーマ・ファイルの属性定義を変更します。54 ページの『属性の変更』を参照してください。
4. データベースを構成します。
5. **idsldif2db** または **idsbulkload** ユーティリティを使用して、データをデータベースにインポートします。

属性のコピー

この機能により、属性をコピーすることができます。

属性をコピーするには、以下のいずれかの方法を使用します。Web 管理ツールがよく使用されます。

Web 管理の使用:

以下に示すコマンドをコマンド行で使用することにより、属性をコピーすることができます。

このタスクについて

ナビゲーション領域の「スキーマ管理」が展開されていない場合は、これを展開し、「属性の管理」をクリックします。属性をコピーするには、以下の手順を実行します。

1. コピーする属性の隣にあるラジオ・ボタンをクリックします。
2. 「コピー」をクリックします。
3. 「属性名」フィールドに新規属性の名前を入力します。例えば、**tempID** を **tempID2** としてコピーすることができます。
4. 属性の「記述」を変更します (臨時の従業員に割り当てた ID 番号など)。
5. 新しい **OID** を入力します。35 ページの『オブジェクト ID (OID)』を参照してください。コピーした属性用の登録済み **OID** がない場合は、ローカルで使用する **OID** を作成できます。例えば、新規の属性の名前が **tempID2** の場合、**tempID2oid** という **OID** を使用できます。
6. ドロップダウン・リストから「上位属性」を選択します。上位属性は、プロパティを継承する元の属性を判別します。
7. ドロップダウン・リストから「構文」を選択します。構文については、62 ページの『属性構文』を参照してください。
8. この属性の最大長を指定する「属性長」を入力します。長さは、バイト数として表されます。
9. 「複数値を使用可能」チェック・ボックスを選択すると、属性に複数の値を持たせることができます。複数値について詳しくは、用語集の項目を参照してください。

10. 同等性、順序付け、およびサブストリングの突き合わせ規則の、各ドロップダウン・メニューから突き合わせ規則を選択します。突き合わせ規則の完全なリストについては、48 ページの『同等性突き合わせ規則』を参照してください。
11. 属性の追加の拡張を変更するには「**IBM 拡張**」タブをクリックします。変更を適用するには「**OK**」をクリックします。変更を行わずに「**属性の管理**」に戻るには「**キャンセル**」をクリックします。
12. 「**IBM 拡張**」タブで以下を行います。
 - **DB2 表名**を入力します。このテーブル名の切り捨てなしの最大長は 128 バイトです。このフィールドをブランクのままにしておくと、サーバーが DB2 表名を生成します。DB2 表名を入力した場合は、DB2 列名も入力する必要があります。6.0 より前のバージョンの IBM Security Directory Server を使用しているサーバーの場合、切り捨てなしの最大長は 16 バイトに制限されます。
 - 「**DB2 列名**」を入力します。この列名の切り捨てなしの最大長は 16 バイトです。このフィールドをブランクのままにしておくと、サーバーが DB2 列名を生成します。DB2 列名を入力した場合は、DB2 表名も入力する必要があります。
 - ドロップダウン・リストから「**Normal (通常)**」、「**Sensitive (重要)**」、または「**Critical (重大)**」を選択して、「**セキュリティー・クラス**」を変更します。**注:** セキュリティー区分が system または restricted になっている属性のセキュリティー・クラスは変更できません。
 - 1 つ以上の索引付け規則を選択して、**索引付け規則**を変更します。索引付け規則について詳しくは、50 ページの『索引付けの規則』を参照してください。**注:** 検索フィルターに使用するすべての属性に対して、少なくとも「同等性」の索引付けを指定することが勧められます。
13. 変更を適用する場合は「**OK**」をクリックします。変更を行わずに「**属性の管理**」に戻る場合は「**キャンセル**」をクリックします。

注: 拡張を追加せずに「**一般**」タブで「**OK**」をクリックした場合は、新しい属性を編集することによって拡張を追加または編集できます。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、属性をコピーすることができます。

このタスクについて

スキーマに含まれている属性を表示させるには、以下のコマンドを発行します。

```
idsldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

コピーする属性を選択します。エディターを使用して該当する情報を変更し、`<filename>` に変更を保管します。その後、以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where `<filename>` contains:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( <mynewAttribute-oid> NAME ' <mynewAttribute>' DESC ' <A new
```

```
attribute I copied for my LDAP application> EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {200} USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oidDBNAME ( 'myAttrTable' 'myAttrColumn' )
ACCESS-CLASS normal LENGTH 200 )
```

属性の削除

ディレクトリー項目に関連付けられている属性を削除することができます。属性を削除するには、**Web 管理ツール**またはコマンド行を使用します。

スキーマは、自由に変更できるわけではありません。変更の制限の詳細については、69 ページの『許可されないスキーマの変更』を参照してください。

属性を削除するには、以下のいずれかの方法を使用します。**Web 管理ツール**を使用する方法が推奨されます。

Web 管理の使用:

ここで説明する手順に従うことにより、**Web 管理ツール**で、ディレクトリー項目に関連付けられている属性を削除できます。

このタスクについて

ナビゲーション領域の「スキーマ管理」が展開されていない場合は、これを展開し、「属性の管理」をクリックします。属性を削除するには、以下の手順を実行します。

手順

1. 削除する属性の隣にあるラジオ・ボタンをクリックします。
2. 「削除」をクリックします。
3. 属性を除去するときは、確認のプロンプトが出されます。属性を削除する場合は「OK」をクリックします。変更を行わずに「属性の管理」に戻る場合は「キャンセル」をクリックします。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、ディレクトリー項目に関連付けられている属性を削除できます。

このタスクについて

```
idsldapmodify -D <admindn> -w <adminpw> -i myschemadelete.ldif
```

myschemadelete.ldif ファイルには、以下の情報が格納されています。

```
dn: cn=schema
changetype: modify
delete: attributetypes
attributetypes: ( myAttribute-oid )
-
delete: ibmattributetypes
ibmattributetypes: ( myAttribute-oid )
```

詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の **idsldapadd** コマンド情報を参照してください。

暗号化属性

DirDataAdmin 役割および SchemaAdmin 役割が割り当てられたローカルの管理グループ・メンバーは、ディレクトリー・データベースで暗号化される属性を指定できます。暗号化の場合、パスワード情報用にサポートされている暗号化スキームのサブセットが使用されます。

属性は、片方向または両方向のいずれかの暗号化スキームを使用して暗号化できます。サポートされている暗号化スキームには、AES-256、AES-192、AES-128、SSHA、SHA-224、SHA-256、SHA-384、SHA-512、SSHA-224、SSHA-256、SSHA-384、および SSHA-512 などがあり、サポートされている属性構文にはディレクトリー・ストリング、IA5 ストリング、識別名 (DN)、および電話番号などがあります。

暗号化属性ポリシーでは、DirDataAdmin 役割および SchemaAdmin 役割が割り当てられているローカル管理グループ・メンバーが、暗号化属性へのアクセスがセキュア接続を使用するクライアントに限定されるよう指定できるようにします。さらに、このポリシーにより、グループ・メンバーは、特定の属性を一致しない属性として定義することができます。このような属性は、存在フィルターでのみ使用できます。また、このポリシーでは、グループ・メンバーに対し、検索時に返される値を暗号化するかどうか、または属性名のみを返すかどうかを指定できるようにします。

注: 暗号化属性の検索フィルター・アサーションは、完全一致突き合わせ、または存在のいずれにもできます。サブストリング突き合わせ、順序付け、および近似一致は使用できません。

暗号化する属性を指定すると、既存のサーバー・データは、次にサーバーを始動したときに初めて暗号化されます。この操作にかかる時間は、暗号化される項目の数によって決まります。暗号化属性ポリシーは、Web 管理ツールを使用して管理できます。

Web 管理の使用:

以下に示す指示により、Web 管理ツールを使用して属性を暗号化することができます。

このタスクについて

ナビゲーション領域の「スキーマ管理」が展開されていない場合は、これを展開し、「暗号化属性の管理」をクリックします。

「暗号化属性の管理」タブでは、暗号化属性を管理する方法が提供されています。ユーザーはこのタブを使用して、既存の暗号化可能属性を管理し、暗号化属性に追加することができます。

「暗号化属性の管理」タブは、サーバーで暗号化属性の `ibm-supportedcapability` OID がサポートされ、`rootDSE` 検索で `OID` が戻される場合にのみ使用可能です。

暗号化が可能な属性を管理するには、以下のようになります。

手順

1. 属性を暗号化するには、「暗号化に使用可能な属性」セクションの「属性の選択」リストから、対象とする暗号化可能属性を選択します。
2. 「暗号化スキームの選択」ボックスから暗号化スキームを選択します。
3. 属性値の検索の戻りの型を「検索で戻す値」ボックスから選択します。
4. 暗号化属性にアクセスするときのセキュア接続を使用可能にするには、「値を表示または変更するためセキュア接続が必要」チェック・ボックスを選択します。
5. 選択した暗号化可能属性を検索フィルターで使用可能にするかどうかを指定するには、「検索フィルターで属性を使用可能」チェック・ボックスを選択します。
6. 「暗号化に追加」ボタンをクリックして、「属性の選択」ボックスから選択した暗号化可能属性を「暗号化属性」テーブルに取り込みます。
7. 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして変更内容を適用し、このパネルを終了します。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

タスクの結果

暗号化属性を管理するには、以下のようになります。

1. 「暗号化属性」テーブルから属性を除去するには、除去する暗号化属性の「選択」列をクリックし、「除去」ボタンをクリックするか、「アクションの選択」ボックスから「除去」を選択して「実行」をクリックします。
2. 属性の暗号化設定を編集するには、編集する暗号化属性の「選択」列をクリックした後、「暗号化設定の編集」ボタンをクリックするか、「アクションの選択」ボックスから「暗号化設定の編集」を選択して「実行」をクリックします。
3. 「暗号化属性」テーブルから属性をすべて除去するには、「すべて除去」ボタンをクリックするか、「アクションの選択」ボックスから「すべて除去」を選択して「実行」をクリックします。
4. 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして変更内容を適用し、このパネルを終了します。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

暗号化設定の編集:

ここで説明する手順に従うことにより、暗号化設定を編集できます。

このタスクについて

この「暗号化設定の編集」パネルには、暗号化のタイプ、検索の戻りの型、属性にアクセスする接続のタイプ、および検索フィルターなど、暗号化属性の既存の値の指定および変更で使用される設定が含まれています。

暗号化属性を編集するには、以下のようになります。

1. 「暗号化スキームの選択」ボックスから暗号化スキームを選択します。
2. 属性値の検索の戻りの型を「検索で戻す値」ボックスから選択します。
3. 暗号化属性にアクセスするときのセキュア接続を使用可能にするには、「値を表示または変更するためセキュア接続が必要」チェック・ボックスを選択します。

4. 「検索フィルターで属性を使用可能」チェック・ボックスを選択して、選択した暗号化属性が検索フィルターで使用可能かどうかを指定します。
5. 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして、暗号化属性値に対して行った変更をディレクトリー・スキーマに保存します。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

複製環境での暗号化属性:

複製時には、セキュア接続を介して属性を複製する必要があります。また、複製プロセスでは、サプライヤーとコンシューマーとの間で非互換機能を使用するかどうかを判別します。

例えば、サプライヤーが属性を暗号化したが、コンシューマーが暗号化をサポートしていない、という場合、複製プロセスは開始されません。また、ネットワーク内に古いリリースで稼働しているサーバーがあると、複製されたスキーマ変更は失敗します。

各サーバーで暗号鍵が共有されること、また、管理者により、各属性がすべてのサーバーで暗号化されるようにすることが推奨されます。暗号鍵がサプライヤーとコンシューマーの間で異なると、変更はデコードされ、平文として複製されます。

コマンド行の使用

以下に示すコマンドを発行することにより、属性を暗号化する (例えば、AES 暗号化スキームを使用して uid 属性を暗号化する) ことができます。

このタスクについて

```
ldapmodify -D <adminDN> -w <adminPW>
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes:( 0.9.2342.19200300.100.1.1 NAME 'uid' DESC 'Typically a user
shortname or userid.'
EQUALITY 1.3.6.1.4.1.1466.109.114.2 ORDERING 2.5.13.3 SUBSTR 2.5.13.4
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
replace: IBMAttributetypes
IBMAttributetypes:( 0.9.2342.19200300.100.1.1 DBNAME( 'uid'uid' )
ACCESS-CLASS normal LENGTH 256 EQUALITY ORDERING SUBSTR APPROX
ENCRYPT AES256 SECURE-CONNECTION-REQUIREDRETURN-VALUEencrypted))
```

属性構文

属性構文は、データの要求する形式を示します。以下に示す表を参照することにより、属性構文について詳しく知ることができます。

表 4. 属性構文

構文	OID
Attribute Type Description 構文	1.3.6.1.4.1.1466.115.121.1.3
Binary - octet string	1.3.6.1.4.1.1466.115.121.1.5
ビット・ストリング	1.3.6.1.4.1.1466.115.121.1.6
Boolean - TRUE/FALSE	1.3.6.1.4.1.1466.115.121.1.7
証明書	1.3.6.1.4.1.1466.115.121.1.8
証明書リスト	1.3.6.1.4.1.1466.115.121.1.9
証明書ペア	1.3.6.1.4.1.1466.115.121.1.10

表 4. 属性構文 (続き)

構文	OID
国ストリング	1.3.6.1.4.1.1466.115.121.1.11
デリバリー・メソッド	1.3.6.1.4.1.1466.115.121.1.14
Directory String 構文	1.3.6.1.4.1.1466.115.121.1.15
DIT Content Rule Description 構文	1.3.6.1.4.1.1466.115.121.1.16
DITStructure Rule Description 構文	1.3.6.1.4.1.1466.115.121.1.17
DN - distinguished name	1.3.6.1.4.1.1466.115.121.1.12
拡張ガイド	1.3.6.1.4.1.1466.115.121.1.21
ファクシミリ電話番号	1.3.6.1.4.1.1466.115.121.1.22
FAX	1.3.6.1.4.1.1466.115.121.1.23
Generalized Time 構文	1.3.6.1.4.1.1466.115.121.1.24
ガイド	1.3.6.1.4.1.1466.115.121.1.25
IA5 String 構文	1.3.6.1.4.1.1466.115.121.1.26
IBM Attribute Type Description	1.3.18.0.2.8.1
Integer 構文 - 整数値	1.3.6.1.4.1.1466.115.121.1.27
JPEG	1.3.6.1.4.1.1466.115.121.1.28
LDAP Syntax Description 構文	1.3.6.1.4.1.1466.115.121.1.54
Matching Rule Description	1.3.6.1.4.1.1466.115.121.1.30
Matching Rule Use Description	1.3.6.1.4.1.1466.115.121.1.31
MHS OR アドレス	1.3.6.1.4.1.1466.115.121.1.33
名前および任意指定の UID	1.3.6.1.4.1.1466.115.121.1.34
Name Form Description	1.3.6.1.4.1.1466.115.121.1.35
数値ストリング	1.3.6.1.4.1.1466.115.121.1.36
Object Class Description 構文	1.3.6.1.4.1.1466.115.121.1.37
オクテット・ストリング	1.3.6.1.4.1.1466.115.121.1.40
その他のメールボックス	1.3.6.1.4.1.1466.115.121.1.39
郵便アドレス	1.3.6.1.4.1.1466.115.121.1.41
表示アドレス	1.3.6.1.4.1.1466.115.121.1.43
プロトコル情報	1.3.6.1.4.1.1466.115.121.1.42
印刷可能ストリング	1.3.6.1.4.1.1466.115.121.1.44
OID を格納するためのストリング。OID は、数字 (0 から 9) と小数点 (.) を含むストリングです。35 ページの『オブジェクト ID (OID)』を参照してください。	1.3.6.1.4.1.1466.115.121.1.38
サブストリング・アサーション	1.3.6.1.4.1.1466.115.121.1.58
サポート・アルゴリズム	1.3.6.1.4.1.1466.115.121.1.49
Telephone Number 構文	1.3.6.1.4.1.1466.115.121.1.50
テレックス番号	1.3.6.1.4.1.1466.115.121.1.52
テレテックス端末 ID	1.3.6.1.4.1.1466.115.121.1.51

表 4. 属性構文 (続き)

構文	OID
UTC Time 構文。UTC 時刻は、ASN.1 規格によって定義されたタイム・ストリング・フォーマットです。ISO 8601 および X680 を参照してください。UTC 時刻形式の時間値を格納するには、この構文を使用します。83 ページの『一般化時刻および UTC 時刻』を参照してください。	1.3.6.1.4.1.1466.115.121.1.53

固有属性

固有属性機能を使用すると、指定した属性がディレクトリー内で固有な値を必ず持つようになります。これらの属性は、`cn=uniqueattributes,cn=localhost` および `cn=uniqueattributes,cn=IBMpolicies` という 2 つの項目でのみ指定できます。

固有属性の値は、その属性を固有のものとして指定しているサーバーに保管されます。固有属性の検索結果は、そのサーバーのデータベースでのみ固有となります。参照からの結果を含む検索結果は、固有でない場合があります。

注: バイナリー属性、運用属性、構成属性、および `objectclass` 属性は、固有のものとして指定できません。

固有属性の作成:

この機能により、固有属性を作成することができます。

注: 属性ごとに、言語タグは固有属性と相互に排他的です。特定の属性を固有属性として指定した場合、その属性に言語タグを関連付けることはできません。

固有属性項目を追加または変更する際、リストされた固有属性タイプに対して固有の制約事項を作成するとエラーが生じる場合、ディレクトリーに項目は追加または作成されません。項目を作成または変更するには、問題を解決し、追加または変更のコマンドを再発行する必要があります。例えば、固有属性項目をディレクトリーに追加する際、リストされた固有属性タイプの表に対して固有の制約事項を作成できない場合は (重複した値がデータベースに存在することが原因で)、固有属性項目はディレクトリーに追加されません。DSA is unwilling to perform というエラーが発行されます。

注: `cn=localhost` および `cn=IBMpolicies` の両方の下に項目を作成した場合、これらの 2 つの項目の結果の共用体は、その固有属性リストを統合したものになります。例えば、属性 `cn` および `employeeNumber` を固有のものとして `cn=localhost` に指定し、属性 `cn` および `telephoneNumber` を固有のものとして `cn=IBMploicies` に指定した場合、サーバーは属性 `cn`、`employeeNumber`、および `telephoneNumber` を固有属性として扱います。

アプリケーションが、既存のディレクトリー項目を複製する属性の値を持つ項目をディレクトリーに追加しようとする時、LDAP サーバーから結果コード 20 のエラー (LDAP: error code 20 - Attribute or Value Exists) が送出されます。

サーバーは、始動後に固有属性のリストを検査し、DB2 制約が各属性に存在するかどうかを確認します。`idsbulkload` ユーティリティーで除去したり、ユーザーが手動で除去したことが原因で属性に対する制約事項が存在しない場合は、それが固

有属性リストから除去され、エラー・ログ (ibmslapd.log) にエラー・メッセージが記録されます。例えば、属性 cn を cn=uniqueattributes、cn=localhost 内で固有のものとして指定し、その属性に対する DB2 制約が存在しない場合は、以下のメッセージがログに記録されます。

```
Values for the attribute CN are not unique.  
The attribute CN was removed from the unique attribute  
entry: CN=UNIQUEATTRIBUTES,CN=LOCALHOST
```

Web 管理の使用:

以下に示す説明に従うことにより、Web 管理ツールで、固有属性を作成することができます。

このタスクについて

ナビゲーション領域で「サーバー管理」カテゴリを展開します。「固有属性の管理」をクリックします。

手順

1. 固有属性として追加する属性を「使用可能な属性」メニューから選択します。リストされる使用可能な属性は、固有のものとして指定可能な属性です。例えば、sn を選択します。**注:** 属性は、cn=localhost コンテナおよび cn=IBMpolicies コンテナの両方に置かれるまで、使用可能な属性のリストに残ります。
2. 「cn=localhost への追加」または「cn=IBMpolicies への追加」のいずれかをクリックします。これら 2 つのコンテナの差は、cn=IBMpolicies 項目は複製されるが、cn=localhost 項目は複製されないことです。属性は、該当するリスト・ボックスに表示されます。同じ属性を両方のコンテナにリストできます。**注:** cn=localhost と cn=IBMpolicies の両方の下に項目を作成した場合、これらの 2 つの項目の結果の共用体は、その固有属性リストを統合したものになります。例えば、属性 cn および employeeNumber を固有のものとして cn=localhost に指定し、属性 cn および telephoneNumber を固有のものとして cn=IBMpolicies に指定した場合、サーバーは、属性 cn、employeeNumber、および telephoneNumber を固有属性として扱います。
3. 属性キャッシュに追加する属性ごとに、この処理を繰り返します。**注:** IBM Security Directory Server 6.3 リリース以降、属性キャッシュは非推奨になりました。今後は、属性キャッシュの使用を避けてください。
4. 変更を保管する場合は「OK」をクリックします。変更を行わずにこのパネルを終了する場合は「キャンセル」をクリックします。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、固有属性を作成することができます。

このタスクについて

属性に固有な値を持たせる必要があることを指定するには、以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=uniqueattributes,cn=localhost
changetype: add
ibm-UniqueAttributeTypes:sn
objectclass: top
objectclass: ibm-UniqueAttributes
```

属性をさらに追加するには、以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=uniqueattributes,cn=localhost
cn: uniqueattributes
changetype: modify
add: ibm-UniqueAttributeTypes
ibm-UniqueAttributeTypes:AIXAdminUserId
-
add: ibm-UniqueAttributeTypes
ibm-UniqueAttributeTypes:adminGroupNames
```

固有属性のリストからの属性の除去:

固有属性のリストから属性を除去するには、**Web 管理**ツールもコマンド行も使用することができます。

注: cn=uniqueattributes,cn=localhost および

cn=uniqueattributes,cn=IBMpolicies の両方に固有属性が存在し、一方の項目だけからそれを除去した場合、サーバーは、引き続きその属性を固有属性として扱います。この属性は、両方の項目から除去された時に、非固有となります。

Web 管理の使用:

以下に示す指示により、Web 管理ツールを使用して固有属性を除去することができます。

このタスクについて

ナビゲーション領域で「サーバー管理」カテゴリを展開します。「固有属性の管理」をクリックします。

手順

1. 該当するリスト・ボックスで、リストから除去する属性をクリックして選択します。例えば、前のタスクの AIXAdminUserId などです。
2. 「除去」をクリックします。
3. リストから除去する属性ごとにこの処理を繰り返します。
4. 変更を保管する場合は「OK」をクリックします。変更を行わずにこのパネルを終了する場合は「キャンセル」をクリックします。

タスクの結果

注: 最後の固有属性を cn=localhost または cn=IBMpolicies リスト・ボックスから除去すると、そのリスト・ボックスのコンテナ項目 cn=uniqueattributes,cn=localhost または cn=uniqueattributes,cn=IBMpolicies が自動的に削除されます。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、固有属性のリストから属性を除去することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=uniqueattributes,cn=localhost  
changetype: modify  
cn: uniqueattributes  
ibm-UniqueAttributeTypes:AIXAdminUserId
```

例えば、cn=localhost に保管されている固有属性をすべて除去するには、以下のコマンドを発行します。

```
idsldapdelete -D <adminDN> -w <Adminpw> "cn=uniqueattributes,cn=localhost"
```

ディレクトリーからこの固有属性項目を削除すると、固有属性に適用される固有の制約事項が除去され、この属性に非固有値を再び指定できるようになります。

サブスキーマ項目

サブスキーマ項目については、以下の情報を参照してください。

サブスキーマ項目は、1 つのサーバーにつき 1 つあります。ディレクトリー内のすべての項目は、暗黙の subschemaSubentryattribute 属性タイプを持っています。subschemaSubentry 属性タイプの値は、項目に対応するサブスキーマ項目の DN です。同じサーバー内のすべての項目は、サブスキーマ項目を共有します。また、それらの項目の subschemaSubentryattribute 属性タイプには、同じ値が設定されます。サブスキーマ項目には、DN (cn=schema) がハードコーディングされています。

サブスキーマ項目は、top、subschema、および IBMsubschemata というオブジェクト・クラスに属しています。IBMsubschemata オブジェクト・クラスは、MUST 属性を持っておらず、MAY 属性タイプ (IBMattributeTypes) を 1 つ持っています。

IBMsubschemata オブジェクト・クラス

IBMsubschemata オブジェクト・クラスは、サブスキーマ項目内でのみ使用します。

```
( <objectClass-oid-TBD> NAME 'IBMsubschemata' AUXILIARY  
MAY IBMattributeTypes )
```

スキーマの照会

スキーマの照会で ldap_search() API を使用します。

ldap_search() API を使用して、サブスキーマ項目を照会することができます。例:

```
DN: "cn=schema"  
search scope : base  
filter: objectclass=subschema or objectclass=*
```

この例では、スキーマ全体が検索されます。選択した属性タイプの値すべてを検索するには、ldap_search で **attrsparameter** を使用します。特定の属性タイプの特定の値のみを検索することはできません。

ldap_search API について詳しくは、「*IBM Security Directory Server Version 6.3 Programming Reference*」を参照してください。

動的スキーマ

動的にスキーマを変更するには、cn=schema という DN を指定して、ldap_modify API を使用する必要があります。一度に追加、削除、または置換できるスキーマ・エンティティは 1 つのみです。例えば、属性タイプ 1 つ、オブジェクト・クラス 1 つなどです。

スキーマ・エンティティを削除するには、oid を以下のように括弧で囲みます。

```
( oid )
```

詳細な説明を指定することもできます。いずれの場合でも、削除するスキーマ・エンティティを見つけるために使用する突き合わせ規則は、objectIdentifierFirstComponentMatch です。

スキーマ・エンティティを追加または置換するには、LDAP バージョン 3 の定義を指定する必要があります。IBM の定義を指定することも可能です。すべての場合において、ユーザーは、影響させるスキーマ・エンティティの定義 (1 つまたは複数) のみを指定する必要があります。

例えば、属性タイプ cn (OID は 2.5.4.3) を削除するには、以下の行を指定して **ldap_modify()** を実行します。

```
LDAPModattr;  
LDAPMod *attrs[] = { &attr, NULL };  
char*vals [] = { "( 2.5.4.3)", NULL };  
attr.mod_op = LDAP_MOD_DELETE;  
attr.mod_type = "attributeTypes";  
attr.mod_values = vals;  
ldap_modify_s(ldap_session_handle, "cn=schema", attrs);
```

OID が 20.20.20 で NAME の長さが 20 文字の属性タイプ bar を追加するには、以下のように指定します。

```
char*vals1[] = { "( 20.20.20 NAME 'bar' SUP NAME )", NULL };  
char*vals2[] = { "( 20.20.20 LENGTH 20 )", NULL };  
LDAPModattr1;  
LDAPModattr2;  
LDAPMod *attrs[] = { &attr1, &attr2, NULL };  
attr1.mod_op = LDAP_MOD_ADD;  
attr1.mod_type = "attributeTypes";  
attr1.mod_values = vals1;  
attr2.mod_op = LDAP_MOD_ADD;  
attr2.mod_type = "IBMAttributeTypes";  
attr2.mod_values = vals2;  
ldap_modify_s(ldap_session_handle, "cn=schema", attrs);
```

注: ACCESS-CLASS タイプは、system または restricted に変更することも、system または restricted から変更することもできません。

Web 管理ツールおよび **idsldapmodify** コマンドの使用例については、46 ページの『属性の処理』を参照してください。

ldap_modify API について詳しくは、IBM Security Directory Server の資料の『プログラミング・リファレンス』セクションを参照してください。

アクセス・コントロール

スキーマを動的に変更するのに必要な権限が付与されている必要があります。

動的スキーマ変更を実行できるのは、複製サプライヤー、サーバー管理者、または管理者グループのメンバーのみです。

レプリカ生成

スキーマの複製は `cn=ibmpolicies` で設定し、`cn=schema` における変更点が、指定した複製合意に複製されるようにする必要があります。

前のリリースでは、スキーマの変更は、ディレクトリー・サーバーで設定されているすべての合意に伝搬されました。ただし、IBM Security Directory Server 6.0 以降のバージョンでは、スキーマの変更は `cn=ibmpolicies` 以下での合意にのみ伝搬されます。スキーマの変更は、ディレクトリー情報ツリー (DIT) 内のその他の合意には伝搬されません。

動的スキーマの変更を実行すると、他の `ldap_modify` 操作と同様に、その内容が複製されます。327 ページの『スキーマ更新およびパスワード・ポリシー更新の複製』を参照してください。

詳細については、310 ページの『レプリカ生成』を参照してください。

許可されないスキーマの変更

サーバーの操作に影響を与えるようなスキーマの変更は許可されていません。ディレクトリー・サーバーによって必要とされるスキーマ定義は変更しないでください。

スキーマは、自由に変更できるわけではありません。以下の変更に関する制約事項を考慮する必要があります。

- スキーマを変更しても、スキーマの一貫性が失われないようにすること。
- 別の属性タイプのスーパータイプである属性タイプは削除しないこと。オブジェクト・クラスの「MAY」または「MUST」属性タイプとなっている属性タイプは削除しないこと。
- 別のオブジェクト・クラスのスーパークラスであるオブジェクト・クラスは削除しないこと。
- 存在しないエンティティー (構文またはオブジェクト・クラスなど) を参照するオブジェクト・クラスまたは属性タイプは追加しないこと。
- 属性タイプまたはオブジェクト・クラスを変更する場合、これらが存在しないエンティティー (構文またはオブジェクト・クラスなど) を参照するようには変更しないこと。

以下のスキーマ定義は、ディレクトリー・サーバーによって要求されます。

オブジェクト・クラス

スキーマのオブジェクト・クラス定義には、サーバーの操作に影響を与えるような変更は行わないでください。

以下のオブジェクト・クラス定義は変更しないでください。

- `accessGroup`
- `accessRole`
- `alias`
- `referral`
- `replicaObject`

- top
- ibm-slappedPwdPolicyAdmin
- ibm-pwdPolicyExt
- pwdPolicy

属性

この機能では、属性を記述します。

以下の属性定義は変更しないでください。

運用属性:

運用属性はサーバーによって保持されています。これらの属性は、サーバーが項目について管理する情報を反映するか、またはサーバーの動作に影響を及ぼします。

これらの属性には、以下のような特殊な特性があります。

- これらの属性は、検索要求時に (名前で) 要求しないと、検索操作で返されません。
- これらの属性は削除できません。
- これらの属性はオブジェクト・クラスの一部ではありません。ディレクトリー・サーバーは、どの項目にこれらの属性が格納されるかを制御します。

次の運用属性のリストは、IBM Security Directory Server によってサポートされている属性です。

- aclEntry
- aclPropagate
- aclSource
- aliasedObjectName、aliasedentryName
- createTimestamp
- creatorsName
- entryOwner
- hasSubordinates
- ibm-allGroups
- ibm-allMembers
- ibm-capabilitysubentry
- ibm-effectiveAcl
- ibm-entryChecksum
- ibm-entryChecksumOp
- ibm-entryUuid
- ibm-filterAclEntry
- ibm-filterAclInherit
- ibm-pwdAccountLocked
- ibm-replicationChangeLDIF
- ibm-replicationFailedChangeCount

- ibm-replicationFailedChanges
- ibm-replicationIsQuiesced
- ibm-replicationLastActivationTime
- ibm-replicationLastChangeId
- ibm-replicationLastFinishTime
- ibm-replicationLastGlobalChangeId
- ibm-replicationLastResult
- ibm-replicationLastResultAdditional
- ibm-replicationNextTime
- ibm-replicationPendingChangeCount
- ibm-replicationPendingChanges
- ibm-replicationperformance
- ibm-replicationState
- ibm-replicationThisServerIsMaster
- ibm-searchSizeLimit
- ibm-searchTimeLimit
- ibm-slapdCryptoSalt
- modifiersName
- modifyTimestamp
- numSubordinates
- ownerPropagate
- ownerSource
- pwdAccountLockedTime
- pwdChangedTime
- pwdExpirationWarned
- pwdFailureTime
- pwdGraceUseTime
- pwdHistory
- pwdReset
- subschemaSubentry
- subtreeSpecification

これらの属性の詳細については、675 ページの『付録 I. IBM Security Directory Server の必須属性定義』を参照してください。

特殊属性の説明である"+"は、検索要求の属性リストで、すべての運用属性を戻すために使用できます。検索要求に"+"がある場合、サーバーはクライアントが許可されるすべての運用属性を戻します。詳しくは、「*IBM Security Directory Server Version 6.3.1 Command Reference*」の **idsldapsearch** コマンド情報を参照してください。

以下の表には、サポート対象の特殊属性、および関連する運用属性がリストされています。

表 5. サポートされる特殊属性および関連する運用属性のリスト

属性	「+」属性によって返される属性	++ によって追加される属性
+	この列にリストされたすべての属性が返されます。	++ では、この列にリストされたすべての属性が返されます。
+ibmaci	aclentry aclsource aclpropagate entryowner ownersource ownerpropagate ibm-filterAclEntry ibm-filterAclInherit ibm-effectiveAcl	
+ibmentry	creatorsname createtimestamp modifiersname modifytimestamp subschemasubentry ibm-entryuuid ibm-capabilitiesubentry ibm-enabledcapabilities (1) ibm-supportedcapabilities (1) ibm-replicationThisServerIsMaster ibm-replicationIsQuiesced	++ibmentry では +ibmentry からの属性が含まれ、以下が追加されます。 ibm-allgroups ibm-allmembers ibm-entryChecksum ibm-entryChecksumOp numsubordinates hassubordinates
+ibmpwdpolicy	pwdAccountLockedTime pwdChangedTime pwdExpirationWarned pwdFailureTime pwdGraceUseTime pwdHistory pwdReset ibm-pwdAccountLocked ibm-pwdGroupPolicyDN ibm-pwdIndividualPolicyDN	
+ibmrepl	ibm-replicationChangeLDIF ibm-replicationLastActivationTime ibm-replicationLastChangeId ibm-replicationLastFinishTime ibm-replicationLastResult ibm-replicationLastResultAdditional ibm-replicationNextTime ibm-replicationPendingChangeCount ibm-replicationState ibm-replicationFailedChangeCount ibm-replicationperformance	++ibmrepl では +ibmrepl からの属性が含まれ、以下が追加されます。 ibm-replicationPendingChanges ibm-replicationFailedChanges

制限付き属性:

この情報により、IBM Security Directory Server の制限付き属性について理解できません。

IBM Security Directory Server は、以下の制限付き属性をサポートしています。

- aclEntry
- aclPropagate
- entryOwner
- ibm-filterAclEntry

- `ibm-filterAclInherit`
- `ownerPropagate`

ルート DSE の属性:

ルート DSE には、ディレクトリー・サーバーに関する情報が属性の形式で含まれています。

以下の属性はルート DSE に関連しているため、変更しないでください。

- `altServer`
- `changelog`
- `firstchangenumber`
- `IBMDirectoryVersion`
- `ibm-effectiveReplicationModel`
- `ibm-enabledCapabilities`
- `ibm-ldapservicename`
- `ibm-saslDigestrealmname`
- `ibm-serverId`
- `ibm-supportedCapabilities`
- `ibm-supportedReplicationModels`
- `lastchangenumber`
- `namingContexts`
- `supportedControl`
- `vendorName`
- `vendorVersion`

これらの属性について詳しくは、675 ページの『付録 I. IBM Security Directory Server の必須属性定義』を参照してください。

スキーマ定義属性:

スキーマ定義には、ディレクトリー・サーバーに関する情報が属性の形式で含まれています。

以下の属性はスキーマ定義に関連しているため、変更しないでください。

- `attributeTypes`
- `ditContentRules`
- `ditStructureRules`
- `IBMAttributeTypes`
- `ldapSyntaxes`
- `matchingRules`
- `matchingRuleUse`
- `nameForms`
- `objectClasses`
- `supportedExtension`

- supportedLDAPVersion
- supportedSASLMechanisms

これらの属性について詳しくは、675 ページの『付録 I. IBM Security Directory Server の必須属性定義』を参照してください。

構成属性:

以下の属性は、サーバーの構成に影響を与えます。

値を変更することはできますが、サーバーを正常に動作させるため、これらの属性の定義は変更しないでください。

- ibm-audit
- ibm-auditAdd
- ibm-auditAttributesOnGroupEvalOp
- ibm-auditBind
- ibm-auditCompare
- ibm-auditDelete
- ibm-auditExtOp
- ibm-auditExtOpEvent
- ibm-auditFailedOpOnly
- ibm-auditGroupsOnGroupControl
- ibm-auditLog
- ibm-auditModify
- ibm-auditModifyDN
- ibm-auditSearch
- ibm-auditUnbind
- ibm-auditVersion
- ibm-pwdPolicy
- ibm-replicaConsumerConnections
- ibm-replicaConsumerId
- ibm-replicaCredentialsDN
- ibm-replicaGroup
- ibm-replicaKeyfile
- ibm-replicaKeylabel
- ibm-replicaKeypwd
- ibm-replicaMethod
- ibm-replicaReferralURL
- ibm-replicaScheduleDN
- ibm-replicaServerId
- ibm-replicaURL
- ibm-replicationBatchStart
- ibm-replicationExcludedCapability

- ibm-replicationImmediateStart
- ibm-replicationOnHold
- ibm-replicationServerIsMaster
- ibm-replicationTimesUTC
- ibm-scheduleFriday
- ibm-scheduleMonday
- ibm-scheduleSaturday
- ibm-scheduleSunday
- ibm-scheduleThursday
- ibm-scheduleTuesday
- ibm-scheduleWednesday
- ibm-slapdAclCache
- ibm-slapdAclCacheSize
- ibm-slapdAdminDN
- ibm-slapdAdminGroupEnabled
- ibm-slapdAdminPW
- ibm-slapdAllowAnon
- ibm-slapdAllReapingThreshold
- ibm-slapdAnonReapingThreshold
- ibm-slapdAuthIntegration
- ibm-slapdBindWithUniqueAttrsEnabled
- ibm-slapdBoundReapingThreshold
- ibm-slapdBulkloadErrors
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxAge
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConfigPwdPolicyOn
- ibm-slapdCryptoSync
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdDerefAliases
- ibm-slapdDigestAdminUser

- ibm-slapdDigestAttr
- ibm-slapdDigestRealm
- ibm-slapdDistributedDynamicGroups
- ibm-slapdDN
- ibm-slapdEnableEventNotification
- ibm-slapdErrorLog
- ibm-slapdESizeThreshold
- ibm-slapdEThreadActivate
- ibm-slapdEThreadEnable
- ibm-slapdETimeThreshold
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdInvalidLine
- ibm-slapdIpAddress
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLanguageTagsEnabled
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdLog
- ibm-slapdLogArchivePath
- ibm-slapdLogMaxArchives
- ibm-slapdLogOptions
- ibm-slapdLogSizeThreshold
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions

- ibm-slapdMigrationInfo
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdProxyBackendServerDn
- ibm-slapdProxyBindMethod
- ibm-slapdProxyConnectionPoolSize
- ibm-slapdProxyDigestRealm
- ibm-slapdProxyDigestUserName
- ibm-slapdProxyDn
- ibm-slapdProxyNumPartitions
- ibm-slapdProxyPartitionBase
- ibm-slapdProxyPartitionIndex
- ibm-slapdProxyPw
- ibm-slapdProxyTargetURL
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplConflictMaxEntrySize
- ibm-slapdReplContextCacheSize
- ibm-slapdReplDbConns
- ibm-slapdReplMaxErrors
- ibm-slapdReplicateSecurityAttributes
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurityProtocol
- ibm-slapdSecurity
- ibm-slapdServerBackend
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslCipherSpecs

- ibm-slapdSSLExtSigalg
- ibm-slapdSslFIPsModeEnabled
- ibm-slapdSslFIPsProcessingMode
- ibm-slapdSSLKeyDatabase
- ibm-slapdSSLKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSslKeyRingFilePW
- ibm-slapdSslPKCS11Lib
- ibm-slapdSslPKCS11Keystorage
- ibm-slapdSslPKCS11Enabled
- ibm-slapdSslPKCS11AcceleratorMode
- ibm-slapdSslPKCS11TokenLabel
- ibm-slapdSuiteBMode
- ibm-replicaPKCS11Enabled
- ibm-slapdStartupTraceEnabled
- ibm-slapdSuffix
- ibm-slapdsupportedCapabilities
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTraceEnabled
- ibm-slapdTraceMessageLevel
- ibm-slapdTraceMessageLog
- ibm-slapdTransactionEnable
- ibm-slapdUniqueAttrForBindWithValue
- ibm-slapdUseProcessIdPW
- ibm-slapdVersion
- ibm-slapdWriteTimeout
- ibm-UniqueAttributeTypes
- ids-instanceDesc
- ids-instanceLocation
- ids-instanceVersion
- passwordMaxRepeatedChars
- passwordMinAlpaChars
- passwordMinDiffChars
- passwordMinOtherChars
- pwdAllowUserChange
- pwdAttribute
- pwdCheckSyntax
- pwdExpireWarning

- pwdFailureCountInterval
- pwdGraceLoginLimit
- pwdInHistory
- pwdLockout
- pwdLockoutDuration
- pwdMaxAge
- pwdMaxFailure
- pwdMinAge
- pwdMinLength
- pwdMustChange
- pwdSafeModify
- replicaBindDN
- replicaBindMethod
- replicaCredentials、replicaBindCredentials
- replicaHost
- replicaPort
- replicaUpdateTimeInterval
- replicaUseSSL

これらの属性の詳細については、675 ページの『付録 I. IBM Security Directory Server の必須属性定義』を参照してください。

ユーザー・アプリケーション属性:

定義を変更してはならないユーザー・アプリケーション属性を以下に示します。

- businessCategory
- cn、commonName
- changeNumber
- changes
- changeTime
- changeType
- deleteOldRdn
- description
- dn、distinguishedName
- globalGroupName
- ibm-changeInitiatorsName
- ibm-kn, 'ibm-kerberosName
- ibm-replCredName
- ibm-replDailySchedName
- ibm-replWeeklySchedName
- krbAliasedObjectName
- krbHintAliases

- krbPrincSubtree
- krbPrincipalName
- krbRealmName
- krbRealmName-V2
- member
- name
- newRdn
- newSuperior
- o、organizationName、organization
- objectClass
- ou、organizationalUnit、organizationalUnitName
- owner
- ref
- secretKey
- seeAlso
- targetDN

これらの属性の詳細については、675 ページの『付録 I. IBM Security Directory Server の必須属性定義』を参照してください。

構文

スキーマの構文は、変更しないでください。

突き合わせ規則

突き合わせ規則は、検索操作のときにストリング比較を行うためのガイドラインを提供します。突き合わせ規則には、サーバーの操作に影響を与えるような変更は行わないでください。

スキーマの検査

サーバーの初期設定では、スキーマ・ファイルが読み取られ、その一貫性と正確性が検査されます。

検査に失敗した場合は、サーバーは初期化に失敗し、エラー・メッセージを出力します。動的なスキーマの変更時、変更されたスキーマにも、一貫性と正確性の検査が行われます。この検査に合格しないと、エラーが戻されて、変更が失敗します。いくつかの検査は文法の一部です。例えば、1 つの属性タイプには最大 1 つのスーパータイプを含めることができ、1 つのオブジェクト・クラスには任意の数のスーパークラスを含めることができます。

属性タイプについては、以下の項目が検査されます。

- 2 つの異なる属性タイプが、同じ名前または OID を持っていないこと。
- 属性タイプの継承の階層で循環がないこと。
- 定義が後で示されたり、別のファイルに存在するとしても、属性タイプのスーパータイプも定義されていること。

- 属性タイプが、別の属性タイプのサブタイプである場合、これらの両方とも、同じ USAGE を持っていること。
- すべての属性タイプに、直接定義されたか、または継承される構文があること。
- NO-USER-MODIFICATION としてマーク付けされているのは、運用属性のみであること。

オブジェクト・クラスについては、以下の項目が検査されます。

- 2 つの異なるオブジェクト・クラスが、同じ名前または OID を持っていないこと。
- オブジェクト・クラスの継承の階層に循環がないこと。
- オブジェクト・クラスのスーパークラスも定義されていること (ただし、この定義は、後で表示されたり、単独のファイル内に存在したりする場合があります)。
- オブジェクト・クラスの MUST および MAY 属性タイプも定義されていること (ただし、この定義は、後で表示されたり、単独のファイル内に存在することがあります)。
- 構造化オブジェクト・クラスはすべて、トップの直接または間接のサブクラスであること。
- 抽象オブジェクト・クラスがスーパークラスを持っている場合は、そのスーパークラスも抽象であること。

スキーマの照合による項目の検査

この機能により、スキーマと照合して項目を検査することができます。

LDAP 操作を介して項目を追加または変更する場合、その項目は、スキーマと突き合わせて検査されます。デフォルトでは、このセクションに記述されている検査がすべて実施されます。ただし、ibmslapd.conf 構成ディレクティブに `ibm-slapdSchemaCheck` 値を指定すれば、実施を取りやめたい検査項目を個々に選択できます。スキーマ構成属性については、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。

スキーマに準拠させるため、以下の条件について項目が検査されます。

オブジェクト・クラスについては、以下の項目が検査されます。

- 属性タイプ "objectClass" について、少なくとも 1 つの値を持っていること。
- 任意の数の補助オブジェクト・クラス (ゼロを含む) を持つことができます。これは、検査ではなく説明です。これを使用不可にするオプションはありません。
- 任意の数の抽象オブジェクト・クラスを持つことができます (ただし、クラス継承の結果としてのみ)。つまり、項目が所有するすべての抽象オブジェクト・クラスについて、項目は、その抽象オブジェクト・クラスから直接または間接に継承する構造化オブジェクト・クラスまたは補助オブジェクト・クラスも所有します。
- 少なくとも 1 つの構造化オブジェクト・クラスを持っていること。
- 正確に 1 つの即時または基本構造化オブジェクト・クラスを持っていること。つまり、項目が指定されたすべての構造化オブジェクト・クラスでは、各オブジェクト・クラスがそのうちの 1 つの構造化オブジェクト・

クラスだけでスーパークラスである必要があります。最も派生の進んだオブジェクト・クラスは、項目の「即時」または「基本構造」オブジェクト・クラスと呼ばれます。単に、項目の「構造」オブジェクト・クラスとも呼ばれます。

- その即時構造化オブジェクト・クラスを (ldap_modify で) 変更することはできません。
- 項目が指定された各オブジェクト・クラスについて、その直接および間接のスーパークラスのすべてのセットが計算されます。これらのスーパークラスに項目が指定されていない場合は、自動的に追加されます。

項目の属性タイプの妥当性は、以下のようにして判別されます。

- 項目の MUST 属性タイプのセットは、継承された暗黙のオブジェクト・クラスを含めて、そのオブジェクト・クラスのすべての MUST 属性タイプのセットの共用体として計算されます。項目の MUST 属性タイプのセットが、項目に含まれている属性タイプのセットのサブセットでない場合、その項目は拒否されます。
- 項目の MAY 属性タイプのセットは、継承された暗黙のオブジェクト・クラスを含めて、そのオブジェクト・クラスのすべての MAY 属性タイプのセットの共用体として計算されます。項目に含まれている属性タイプのセットが、項目の MUST および MAY 属性タイプのセットの共用体のサブセットでない場合、その項目は拒否されます。
- 項目に対して定義された属性タイプが NO-USER-MODIFICATION としてマーク付けされている場合、その項目は拒否されます。

項目の属性タイプ値の妥当性は、以下のようにして判別されます。

- 項目に含まれているすべての属性タイプについて、属性タイプが単一値であり、項目が複数の値を持つ場合、その項目は拒否されます。
- 項目に含まれているすべての属性タイプのすべての属性値について、その構文が、その属性の構文用の構文検査ルーチンに従っていない場合、その項目は拒否されます。
- 項目に含まれているすべての属性タイプのすべての属性値について、その長さが、その属性タイプに割り当てられている最大長よりも長い場合、その項目は拒否されます。

DN の妥当性は、以下のようにして判別されます。

- 構文が識別名の BNF に準拠しているかどうかを検査します。準拠していない場合、項目は拒否されます。
- その項目に対して有効な属性タイプのみで RDN が構成されているかどうかを検査します。
- RDN で使用される属性タイプの値が項目内に示されているかどうかを検査します。

iPlanet との互換性

IBM Security Directory Server で使用されるパーサーでは、スキーマ属性タイプ (objectClassesand) の属性値を、iPlanet の文法を使用して指定できます。

例えば、descrs および numeric-oids は、(qdescrs と同様に) 単一引用符で囲んで指定することができます。ただし、スキーマ情報は、ldap_search を使用して、い

つでも参照できます。ファイル内の属性値において単一の動的変更が (ldap_modify を使用して) 実行されると、そのファイルは、すべての属性値が IBM Security Directory Server バージョン 6.0 以降の仕様に従っているファイルによって置き換えられます。ファイルおよび ldap_modify 要求で使用されるパーサーは同じであるため、属性値に対して iPlanet 文法を使用する ldap_modify も正常に処理されます。

iPlanet サーバーのサブスキーマ項目に対して照会を実行すると、結果として得られる項目では、指定の OID に対して複数の値がある場合があります。例えば、ある属性タイプに 2 つの名前 (cn と commonName など) がある場合、その属性タイプの説明は 2 回 (名前ごとに 1回) 指定されます。IBM Security Directory Server では、単一の属性タイプまたはオブジェクト・クラスの説明が、同じ内容で複数回現れるスキーマを構文解析することができます (NAME と DESCR は除く)。ただし、IBM Security Directory Server がスキーマを発行するときには、そのような属性タイプの単一の説明を、すべての名前 (短縮名が最初に示される) をリストして提供します。例えば、iPlanet では、以下のように共通名属性が記述されます。

```
( 2.5.4.3 NAME 'cn'  
DESC 'Standard Attribute'  
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )  
  
( 2.5.4.3 NAME 'commonName'  
DESC 'Standard Attribute, alias for cn'  
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

IBM Security Directory Server では、以下のように記述されます。

```
( 2.5.4.3 NAME ( 'cn' 'commonName' ) SUP name )
```

IBM Security Directory Server では、サブタイプがサポートされます。cn を名前のサブタイプにしない場合 (これは標準から逸脱します) は、以下の属性を宣言します。

```
( 2.5.4.3 NAME ( 'cn' 'commonName' )  
DESC 'Standard Attribute'  
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

最初の名前 (cn) は優先名、または短縮名として解釈されます。cn の後にある他の名前はすべて代替名として解釈されます。ストリング 2.5.4.3、cn、および commonName (大/小文字を区別しない) は、スキーマ内でも、ディレクトリーに追加された項目でも、区別なく使用することができます。

一般化時刻および UTC 時刻

日付および時刻関連の情報を指定するには、さまざまな表記法を使用することができます。

例えば、1999 年 2 月 4 日は、以下のように表現できます。

```
2/4/99  
4/2/99  
99/2/4  
4.2.1999  
04-FEB-1999
```

この他にも多数の表記が存在します。

IBM Security Directory Server は、LDAP サーバーに以下の 2 つの構文のサポートを要求することで、タイム・スタンプ表記を標準化しています。

- 標準時の構文は、以下の形式で表現されます。

```
YYYYMMDDHHMMSS[.fraction][(+|-)HHMM]Z
```

年には 4 桁、月、日、時、分、秒にはそれぞれ 2 桁を使用します。秒にはオプションとして、小数部も指定できます。他に情報を付加しなければ、日付および時刻は、現地時間帯であると見なされます。時刻が協定世界時で表されていることを示すには、時刻に大文字の Z を付加するか、現地時差を付加します。例:

```
"19991106210627.3"
```

現地時間で、1999 年 11 月 6 日の午後 9 時 6 分 27.3 秒であることを示します。

```
"19991106210627.3Z"
```

協定世界時です。

```
"19991106210627.3-0500"
```

最初の例と同様に現地時間ですが、協定世界時に対して 5 時間の時差があることを示しています。

オプションの小数点以下の秒数を指定する場合は、ピリオドまたはコンマが必要です。現地時間の時差の場合、'+' または '-' を HHMM 値の前に付けなければなりません。

- 協定世界時の構文は、以下の形式で表現されます。

```
YYMMDDHHMM[SS][(+|-)HHMM]Z
```

年、月、日、時、分、およびオプションである秒の各フィールドに 2 桁ずつ使用します。GeneralizedTime の場合と同様、オプションの時差を指定できます。例えば、現地時間が 1999 年 1 月 2 日の午前であり、協定世界時が 1999 年 1 月 2 日の正午である場合、UTCTime の値は、以下のいずれかで表現されます。

```
"9901021200Z"  
または  
"9901020700-0500"
```

現地時間が 2001 年 1 月 2 日の午前であり、協定世界時が 2001 年 1 月 2 日の正午である場合、UTCTime の値は、以下のいずれかで表現されます。

```
"0101021200Z"  
または  
"0101020700-0500"
```

UTCTime 時刻で年の値に使用できるのは、2 桁のみです。

サポートされる突き合わせ規則は、generalizedTimeMatchfor (同等性の場合) および generalizedTimeOrderingMatchfor (不等性の場合) です。サブストリング検索は使用できません。例えば、以下のフィルターは有効です。

```
generalized-timestamp-attribute=199910061030  
utc-timestamp-attribute>=991006  
generalized-timestamp-attribute=*
```

以下のフィルターは無効です。

```
generalized-timestamp-attribute=1999*  
utc-timestamp-attribute>=*1010
```

基本的なサーバー管理タスク

この機能により、基本的なサーバー管理タスクを実行することができます。

注: 特に断りのない限り、以下のタスクを実行できるのは、ディレクトリー管理者、グローバル管理グループ・メンバー、またはローカル管理グループ・メンバー(メンバーの役割に基づく)です。

- 『1 次管理者の識別名およびパスワードの変更』
- 86 ページの『サーバーの開始と停止』
- 88 ページの『サーバー状況の検査』
- 111 ページの『サーバー接続の管理』
- 113 ページの『接続プロパティの管理』
- 64 ページの『固有属性』

1 次管理者の識別名およびパスワードの変更

この機能により、1 次管理者の識別名およびパスワードを変更することができます。

このタスクは、ディレクトリー管理者のみが実行できます。

通常、管理者の名前とパスワードは、サーバーのインストールおよび構成時に設定されます。ただし、Web 管理ツールやコマンド行でも、管理者の名前とパスワードを変更できます。管理者のパスワード・セキュリティー制限の詳細については、247 ページの『管理パスワードおよびロックアウト・ポリシーの設定』を参照してください。

識別名についての詳細は、10 ページの『識別名 (DN)』を参照してください。

Web 管理の使用

ここで説明する手順に従うことにより、Web 管理ツールを使用して 1 次管理者の識別名およびパスワードを変更することができます。

このタスクについて

Web 管理ツールのナビゲーション領域で「ユーザー・プロパティ」をクリックします。2 つの選択肢が表示されます。

管理者ログインの変更

フィールドに新しい管理者 DN を指定して、現在のパスワードを入力します。「OK」をクリックします。変更を行わずに「概要」パネルに戻る場合は「キャンセル」をクリックします。

注: この選択項目は、ディレクトリー管理者としてログインしている場合のみ使用可能です。ユーザーまたは管理グループ・メンバーとしてログインしている場合は使用できません。

パスワードの変更

現在ログインしている DN のパスワードを変更するには、「現在のパスワード」フィールドに現在のパスワードを入力します。さらに新しいパスワードを「新規パスワード」フィールドに入力し、同じパスワードを「新規パスワードの確認」フィールドに再度入力し、「OK」をクリックします。変更を行わずに「概要」パネルに戻るには、「キャンセル」をクリックします。

コマンド・ラインの使用

コマンド行から **idsdnpw** コマンドまたは **idsxcfg** ユーティリティを使用することで、1 次管理者の識別名およびパスワードを変更することができます。

このタスクについて

idsdnpw コマンドは、以下のように使用します。

```
idsdnpw -u <adminDn> -p <adminPW>
```

idsxcfg ユーティリティを使用するには、コマンド行で「**idsxcfg**」と入力します。「IBM Security Directory Server 構成ツール」パネルが表示されたら、「**管理者 DN の管理**」を選択して管理者の DN を変更するか、「**管理者パスワードの管理**」を選択して管理者のパスワードを変更します。表示される指示に従ってください。**idsxcfg** ユーティリティの使用については、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。

サーバーの開始と停止

サーバーを開始または停止する場合は、以下の情報を参照してください。

サーバーを開始または停止するには、以下のいずれかの方法を使用します。

Web 管理の使用

Web 管理ツールを使用してサーバーを開始または停止する場合は、以下の情報を参照してください。

このタスクについて

注: 所定のディレクトリー・インスタンスの管理サーバー (**idsdiradm**) が実行されている必要があります。

サーバーの現在の状況 (始動しているか、停止しているか、構成モードで始動しているか) は、サーバー状況域の左上隅にアイコンで示されます。現在の状況は、作業域の最初の文にも示されます。例を以下に示します。

```
The Directory Server is currently running
```

手順

1. Web 管理ナビゲーション領域の「**サーバー管理**」をクリックし、展開されたリストの「**サーバーの始動/停止/再始動**」をクリックします (この操作をまだ実行していない場合)。**注:** Web 管理ツールを使用して管理サーバーにアクセスする場合は、以下ようになります。
 - 「サーバーの始動/停止/再始動」パネルのステータス・バーには、ツールが管理サーバーに接続されたことを示すメッセージが表示されます。管理サーバーでサポートされていないパネルにアクセスすると、そのパネルの機能がサポート外であることを示すメッセージが表示されます。
 - 「サーバーの始動/停止/再始動」パネルは、`ibm-supportedcapabilities` 属性の `rootDSE` に示されている機能に基づいて使用可能になります。
2. メッセージ領域には、サーバーの現在の状態 (停止、実行中、構成専用モードで実行中) が表示されます。サーバーの状態 (実行中または停止) に応じて、サーバーの状態を変更できるボタンが使用可能になります。

表 6. サーバーの状況に基づく使用可能なアクション

サーバーの状況	使用可能なボタン
停止中	始動、閉じる
実行中	停止、再始動、閉じる
構成専用モードで実行中 (Running in configuration only mode)	停止、再始動、閉じる

- サーバーが稼働している場合、「停止」をクリックするとサーバーが停止し、「再始動」をクリックするとサーバーが停止してから開始されます。
 - サーバーが停止している場合、「始動」をクリックするとサーバーが開始されます。
 - 「閉じる」をクリックすると、「概要」パネルに戻ります。
3. サーバーが正常に始動または停止すると、メッセージが表示されます。

タスクの結果

サーバー構成保守を実行する必要がある場合は、「構成専用モードで始動/再始動」チェック・ボックスを選択します。このモードでは、システム管理者のみがサーバーにバインドできます。他の接続は、DB2 バックエンドを使用可能にして（「構成専用モードで始動/再始動」チェック・ボックスを選択解除して）サーバーを再始動するまで、すべて拒否されます。詳細については、17 ページの『構成専用モード』を参照してください。

注: 構成保守はサーバーの実行中に行えます。

コマンド行または Windows の「サービス」アイコンの使用

以下に示すコマンドを使用して、サーバーを開始することができます。

このタスクについて

注: `ibmdirctl` の管理サーバー (`idsdiradm`) が実行されている必要があります。

```
ibmdirctl -h mymachine -D myDN -w mypassword -p <adminportnumber> start
```

または

```
idsslapd -I <instancename>
```

サーバーを停止するには、以下のコマンドを使用します。

```
ibmdirctl -h mymachine -D myDN -w mypassword -p <adminportnumber> stop
```

または

```
idsslapd -I <instancename> -k
```

上記のコマンドで、サーバーをそれぞれ始動または停止できます。詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の `ibmdirctl` および `idsdiradm` のコマンド情報を参照してください。

Windows システムの場合は、前のコマンドを使用するか、以下の手順を実行します。

1. デスクトップから、「マイ コンピュータ」アイコンをダブルクリックします。

2. 「コントロール パネル」アイコンをダブルクリックします。
3. 「管理ツール」アイコンをダブルクリックします。
4. 「サービス」アイコンをダブルクリックします。
5. サーバーを開始するには、「コントロール パネル」->「管理ツール」->「サービス」を選択し、「IBM Security Directory Server Instance V6.3 - <インスタンス名>」を選択して「開始」をクリックします。
6. サーバーを停止するには、「コントロール パネル」->「管理ツール」->「サービス」を選択し、「IBM Security Directory Server Instance V6.3 - <インスタンス名>」を選択して「停止」をクリックします。

注: Windows マシンでタイム・ゾーンを変更する場合、サーバーおよび管理サーバーに時間の変更を認識させるために、サーバーおよび管理サーバーを再始動する必要があります。これで管理サーバーのログのタイム・スタンプは、サーバーのログのタイム・スタンプに一致します。

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・インスタンスを開始または停止するには、以下のようにします。

- インスタンス管理ツールで、開始または停止するディレクトリー・サーバー・インスタンスを選択し、「始動/ 停止」をクリックします。

サーバー状況の検査

以下の情報を使用して、サーバーの状況を検査します。

cn=monitor でオブジェクト・クラスを検索することによって、サーバーの状況を検査できます。以下のいずれかの方法でこのアクションを実行してください。

Web 管理の使用

Web 管理ツールを使用してサーバーの状況を確認するには、以下の手順を実行します。

このタスクについて

ナビゲーション領域で「サーバー管理」カテゴリーを展開します。「サーバー・ステータスの表示」をクリックします。このパネルには、9 つのタブがあります。このパネルの下部で、「再表示」ボタンをクリックすると、現在のタブに表示されているステータスが更新されます。「閉じる」をクリックすると、IBM Security Directory Server の「概要」パネルに戻ります。

注: Web 管理ツールを使用して管理サーバーにアクセスする場合は、以下のようになります。

- 「サーバー・ステータスの表示」パネルのタイトルが、「管理サーバー・ステータスの表示」に変わります。
- 「管理サーバー・ステータスの表示」パネルのステータス・バーには、ツールが管理サーバーに接続されたことを示すメッセージが表示されます。管理サーバーでサポートされていないパネルにアクセスすると、そのパネルの機能がサポート外であることを示すメッセージが表示されます。
- 「管理サーバー・ステータスの表示」パネルは、ibm-supportedcapabilities 属性の rootDSE にある機能に基づいて使用可能になります。

ディレクトリー・サーバーが実行中であれば、以下の情報が表示されます。

「一般」タブ:

サーバーに関する一般的な情報を表示するには、「一般」タブを使用します。

「一般」タブには、以下の情報が表示されます。

ホスト名

LDAP サーバーのホスト名。

サーバーの状況

サーバーは、「実行中」、「構成専用モードで実行中」、または「停止」のいずれかです。サーバー状況領域の左隅に表示される 3 つのアイコンにより、サーバーの状況をいつでも確認することができます。

開始時刻

サーバーを始動した時刻。開始時刻は、以下の形式で表示されます。

year-month-day hour:minutes:seconds GMT

現在時刻

サーバーの現在の時刻。現在の時刻は、以下の形式で表示されます。

year-month-day hour:minutes:seconds GMT

合計スレッド

サーバーで使用されているワーカー・スレッドの数。

書き込み時ブロックされたスレッドの合計

クライアントにデータを返送しているスレッドの数。

読み取り時ブロックされたスレッドの合計

クライアントからデータを読み取っているスレッドの数。

接続数 現在アクティブな接続の数。

合計接続

サーバー始動後の接続の合計数。

送信された項目数

サーバーの始動後にサーバーによって送信された項目の数。

別名の参照解除のバイパス

別名処理をバイパスできるかどうかを示すサーバー・ランタイム値。ディレクトリーに別名オブジェクトが存在しない場合は `true` が表示され、ディレクトリーに 1 つ以上の別名オブジェクトが存在する場合は `false` が表示されます。

SSL 接続の総数

サーバー始動後の SSL 接続の合計数。この情報は、接続先サーバーが接続タイプ・カウント・モニター機能をサポートする場合にのみ表示されます。

TLS 接続の総数

サーバー始動後の TLS 接続の合計数。この情報は、接続先サーバーが接続タイプ・カウント・モニター機能をサポートする場合にのみ表示されます。

システム情報:

オペレーティング・システムと使用可能なディスク・スペースに関する情報を表示するには、「システム情報」をクリックします。

次の情報が表示されます。

オペレーティング・システム名

LDAP サーバーで稼働するオペレーティング・システムの名前を指定します。

DB2 データベースが保管されるディレクトリーが使用するディスク・スペース (K バイト)

DB2 データベースを格納するディレクトリーが使用するディスク・スペースの量をキロバイト単位で指定します。

DB2 データベースで使用可能なディスク・スペース (K バイト)

DB2 データベースに使用できるディスク・スペースの量をキロバイト単位で指定します。

操作カウント:

サーバーの操作に関する情報を表示するには、「操作カウント 1」をクリックします。

次の情報が表示されます。

要求された操作数

サーバーが始動した後に開始された要求の数。

完了した操作数

サーバーの始動後に完了した要求の数。

要求された検索操作の数

サーバーの始動後に開始された検索の数。

完了した検索操作の数

サーバーの始動後に完了した検索の数。

要求されたバインド操作の数

サーバー始動後のバインド要求の数。

完了したバインド操作の数

サーバーの始動後に完了したバインド要求の数。

要求されたアンバインド操作の数

サーバー始動後のアンバインド要求の数。

完了したアンバインド操作の数

サーバーの始動後に完了したアンバインド要求の数。

要求された追加操作の数

サーバー始動後の追加要求の数。

完了した追加操作の数

サーバーの始動後に完了した追加要求の数。

要求された削除操作の数

サーバー始動後の削除要求の数。

完了した削除操作の数

サーバーの始動後に完了した削除要求の数。

要求された RDN 変更操作の数

サーバー始動後の RDN 変更要求の数。

完了した RDN 変更操作の数

サーバーの始動後に完了した RDN 変更要求の数。

注: Web 管理ツールを使用して管理サーバーにアクセスする場合は、一部のフィールドが表示されません。

以下の情報を表示するには、「**操作カウント 2**」をクリックします。

要求された変更操作の数

サーバー始動後の変更要求の数。

完了した変更操作の数

サーバーの始動後に完了した変更要求の数。

要求された比較操作の数

サーバー始動後の比較要求の数。

完了した比較操作の数

サーバーの始動後に完了した比較要求の数。

要求された中止操作の数

サーバー始動後の中止要求の数。

完了した中止操作の数

サーバーの始動後に完了した中止要求の数。

要求された拡張操作の数

サーバー始動後の拡張要求の数。

完了した拡張操作の数

サーバーの始動後に完了した拡張要求の数。

要求された不明操作の数

サーバー始動後の不明要求の数。

完了した不明操作の数

サーバーの始動後に完了した不明要求の数。

デッドロックのために失敗したトランザクション内にはない操作の数

デッドロックが原因で失敗した、トランザクション内にはない操作の数。

デッドロック検出機能で待機する操作の数

デッドロック検出機能で待機する操作の数。

デッドロック検出機能で待機する操作の最大数

デッドロック検出機能で一度に待機する操作の最大数。

トランザクション内にはない再試行された操作の数

トランザクション内にはない操作のうち、デッドロックを回避するために再試行された操作の数。

注: Web 管理ツールを使用して管理サーバーにアクセスする場合は、一部のフィールドが表示されません。

トランザクション・カウント:

サーバーのトランザクションに関する情報を表示するには、「トランザクション・カウント」をクリックします。

次の情報が表示されます。

要求されたトランザクションの数

サーバーの始動後に開始されたトランザクション要求の数。

完了したトランザクションの数

コミット要求またはロールバック要求が完了したトランザクションの数。

要求されたトランザクションのコミットの数

サーバーの始動後に要求されたトランザクションのコミットの数。

コミットされたトランザクションの数

サーバーの始動後に正常にコミットされたトランザクションの数。

要求された終了トランザクションのロールバックの数

サーバーの始動後に受信した終了トランザクションのロールバック要求の数。

ロールバックされたトランザクションの数

要求によって、または操作の障害が原因でロールバックされたトランザクションの数。

要求されたトランザクション準備操作の数

サーバーの始動後に要求されたトランザクション準備操作の数。

完了したトランザクション準備操作の数

サーバーの始動後に完了したトランザクション準備操作の数。

準備を要求されたが、まだコミットまたはロールバックされていないトランザクションの数

準備を要求されたが、まだコミットまたはロールバックされていないトランザクションの数。

注: 「再表示」をクリックすると、このパネルの情報を更新できます。「閉じる」をクリックすると、「概要」パネルに戻ります。

作業キュー:

作業キューに関する情報を表示するには、「作業キュー」をクリックします。

次の情報が表示されます。

使用可能なワーカー・スレッドの数

作業に振り向けることができるワーカー・スレッドの数。

作業キューの深さ

作業キューの現在のサイズ。

作業キューの最大サイズ

作業キューの最大サイズ。

自動接続クリーナーで閉じられた接続の数

自動接続クリーナーによって閉じられたアイドル状態接続の数。

自動接続クリーナーが実行された回数

自動接続クリーナーが実行された回数。

注: Web 管理ツールを使用して管理サーバーにアクセスした場合は、一部のフィールドが表示されません。

ワーカー・ステータスの表示:

現在アクティブになっているワーカー・スレッドに関する情報を表示するには、「ワーカー・ステータスの表示」をクリックします。

この情報は、サーバーが予想どおりに稼働していない場合やパフォーマンスが低い場合に役に立ちます。この検索を実行すると、完了するまでサーバーのアクティビティはすべて中断されます。その旨を示す警告が表示され、この操作が完了するまでの時間は、接続数とアクティブ・ワーカー・スレッドの数によって異なるというメッセージが表示されます。情報を表示するには、「はい」をクリックします。

以下のワーカー・スレッド情報がテーブルに表示されます。

スレッド ID

ワーカー・スレッドの ID (2640 など)。

操作 受信した作業要求のタイプ (検索など)。

バインド DN

サーバーのバインドに使用する DN。

クライアント IP

クライアントの IP アドレス。

ワーカー・スレッドの詳細を表示するには、詳細を表示したいワーカー・スレッドを「ワーカー・ステータスの表示」テーブルから選択して「表示」をクリックします。選択したワーカー・スレッドに関する以下の情報フィールドが表示されます。

スレッド ID

ワーカー・スレッドの ID (2640 など)。

操作 受信した作業要求のタイプ (検索など)。

LDAP バージョン

LDAP バージョンのレベル (V1、V2 または V3)

バインド DN

サーバーのバインドに使用する DN。

クライアント IP

クライアントの IP アドレス。

クライアント・ポート

クライアントが使用するポート。

接続 ID

接続を識別する数値。

受信場所

作業要求を受け取った日時。

要求パラメーター

操作の追加情報。例えば、要求が検索の場合は、以下の情報も表示されません。

```
base=cn=workers,cn=monitor
scope=baseObject
derefaliases=neverDerefAliases
typesonly=false
filter=(objectclass=*)
attributes=all
```

「ワーカー・ステータスの表示」パネルに戻るには、「閉じる」をクリックします。

トレースおよびログ:

サーバーのトレースとログの情報を表示するには、「**トレースおよびログ**」をクリックします。

以下の情報が表示されます。

使用可能なトレース

サーバーに対する現在のトレース値。トレース・データを収集する場合は TRUE、収集しない場合は FALSE を指定します。トレース機能の使用可能化と始動について詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の **ldaptrace** コマンド情報を参照してください。

トレース・メッセージ・レベル

サーバーに対する現在の `ldap_debug` 値。値は 16 進数形式です。例を以下に示します。

```
0x0=0
0xffff=65535
```

詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」のセクション『*Debugging levels*』を参照してください。

トレース・メッセージ・ログ

トレース出力が入るファイルの名前。

注: 値が `stderr` の場合は、出力は LDAP サーバーを始動したコマンド・ウィンドウに表示されます。コマンド行からサーバーを始動しなかった場合、データは表示されません。

サーバー・ログに追加されたメッセージの数

サーバーの始動後に記録されたエラー・メッセージの数。

DB2 ログに追加されたメッセージの数

サーバーの始動後に記録された DB2 エラー・メッセージの数。

監査ログに追加されたメッセージの数

サーバーの始動後に監査ログによって記録されたメッセージの数。

監査ログに追加されたエラー・メッセージの数

監査ログによって記録された失敗操作メッセージの数。

永続検索:

永続検索接続に関する情報を表示するには、「**永続検索**」をクリックします。

次の情報が表示されます。

送信された変更の数

サーバーの始動後に送信された変更の数を示します。

アクティブな接続の数

アクティブな永続検索接続の数を示します。

除去された接続の数

ネットワークまたはクライアントに障害が発生したために除去された接続の数を示します。

保留中の変更の数

永続検索によってこれから処理される、キュー内の新規更新の数を示します。

コマンド・ラインの使用

コマンド行を使用してサーバーの状況を確認するには、以下に示すベースで **idsldapsearch** コマンドを使用します。

このタスクについて

- cn=monitor
- cn=workers,cn=monitor
- cn=connections,cn=monitor
- cn=changelog,cn=monitor
- cn=system,cn=monitor

cn=monitor コマンドの使用:

サーバーのプロパティを表示するには、**cn=monitor** コマンドを使用します。

```
idsldapsearch -h <servername> -p <portnumber> -b cn=monitor -s base objectclass=*
```

次の情報が表示されます。

cn=monitor

version=IBM Security Directory (SSL), Version 6.3

directoryversion

フィックスパックのレベルを示す特定のバージョン番号。

totalconnections

サーバー始動後の接続の合計数。

total_ssl_connections

サーバー始動後の SSL 接続の合計数。

total_tls_connections

サーバー始動後の TLS 接続の合計数。

currentconnections

アクティブな接続の数。

maxconnections

許可されているアクティブな接続の最大数。

writewaiters

クライアントにデータを返送しているスレッドの数。

readwaiters

クライアントからデータを読み取っているスレッドの数。

opsinitiated

サーバー始動後の要求の数。

livethreads

サーバーで使用されているワーカー・スレッドの数。

opscompleted

サーバーの始動後に完了した要求の数。

entriessent

サーバーの始動後にサーバーによって送信された項目の数。

searchesrequested

サーバーの始動後に要求された検索の数。

searchescompleted

サーバーの始動後に完了した検索の数。

bindsrequested

サーバーの始動後に要求されたバインド操作の数。

bindscompleted

サーバーの始動後に完了したバインド操作の数。

unbindsrequested

サーバーの始動後に要求されたアンバインド操作の数。

unbindscompleted

サーバーの始動後に完了したアンバインド操作の数。

addsrequested

サーバーの始動後に要求された追加操作の数。

addscompleted

サーバーの始動後に完了した追加操作の数。

addsfromsuppliers

複製サプライヤーから受信した更新操作の数。

deletesrequested

サーバーの始動後に要求された削除操作の数。

deletescompleted

サーバーの始動後に完了した削除操作の数。

deletesfromsuppliers

複製サプライヤーから受信した削除操作の数。

modrdnsrequested

サーバーの始動後に要求された RDN の変更操作の数。

modrdnscompleted

サーバーの始動後に完了した RDN の変更操作の数。

modrdnsfromsuppliers

複製サプライヤーから受信した RDN の変更操作の数。

modifiesrequested

サーバーの始動後に要求された変更操作の数。

modifiescompleted

サーバーの始動後に完了した変更操作の数。

modifiesfromsuppliers

複製サプライヤーから受信した変更操作の数。

comparesrequested

サーバーの始動後に要求された比較操作の数。

comparescompleted

サーバーの始動後に完了した比較操作の数。

abandonsrequested

サーバーの始動後に要求された中止操作の数。

abandonscompleted

サーバーの始動後に完了した中止操作の数。

extopsrequested

サーバーの始動後に要求された拡張操作の数。

extopscompleted

サーバーの始動後に完了した拡張操作の数。

unknownopsrequested

サーバーの始動後に要求された不明な操作の数。

unknownopscompleted

サーバーの始動後に完了した不明な操作の数。

transactionsrequested

開始済みのトランザクション要求の数。

transactionscompleted

完了したトランザクション操作の数。

transactionpreparesrequested

要求されたトランザクション準備操作の数。

transactionpreparescompleted

完了したトランザクション準備操作の数。

transactioncommitsrequested

要求されたトランザクションのコミット操作の数。

transactionscommitted

コミットされたトランザクション操作の数。

transactionrollbacksrequested

ロールバック用に要求されたトランザクション操作の数。

transactionsrolledback

ロールバックされたトランザクション操作の数。

transactionspreparedwaitingoncommit

コミット/ロールバックを待機している準備されたトランザクション操作の数。

slapderrorlog_messages

サーバーの始動後またはリセットの実行後に記録されたサーバー・エラー・メッセージの数。

slapdclierrors_messages

サーバーの始動後またはリセットの実行後に記録された DB2 エラー・メッセージの数。

auditlog_messages

サーバーの始動後またはリセットの実行後に記録された監査メッセージの数。

auditlog_failedop_messages

サーバーの始動後またはリセットの実行後に記録された操作失敗メッセージの数。

filter_cache_size

キャッシュで許可されているフィルターの最大数。

filter_cache_current

現在キャッシュ内にあるフィルターの数。

filter_cache_hit

キャッシュ内で見つかったフィルターの数。

filter_cache_miss

フィルター・キャッシュを使用しようとしたが、一致する操作がキャッシュ内に見つからなかった検索操作の数。

filter_cache_bypass_limit

この制限より多くの項目を戻す検索フィルターはキャッシュされません。

entry_cache_size

キャッシュ内で許可されるエントリーの最大数。

entry_cache_current

現在キャッシュ内にある項目の数。

entry_cache_hit

キャッシュ内で見つかったエントリーの数。

entry_cache_miss

キャッシュ内で見つからなかったエントリーの数。

group_members_cache_size

メンバーをキャッシュする必要があるグループの最大数。

group_members_cache_current

メンバーが現在キャッシュされているグループの数。

group_members_cache_hit

グループ・メンバーのキャッシュからメンバーが要求および検索されたグループの数。

group_members_cache_miss

DB2 から取得されたメンバーを必要とするグループ・メンバーのキャッシュ内で見つかった、要求されたメンバーが属するグループの数。

group_members_cache_bypass

グループ・メンバーのキャッシュに格納されるグループ内で許可されるメンバーの最大数。

acl_cache

ACL キャッシュがアクティブ (TRUE) か非アクティブ (FALSE) かを示すブール値。

acl_cache_size

ACL キャッシュ内の項目の最大数。

operations_waiting

デッドロック検出機能で待機する操作の数。

maximum_operations_waiting

デッドロック検出機能で同時に待機する操作の最大数。

operations_retried

デッドロックが原因で再試行した操作の数。

operations_deadlocked

デッドロック内の操作の数。

cached_attribute_total_size

属性キャッシュが使用しているメモリーの容量 (キロバイト)。

cached_attribute_configured_size

属性キャッシュが使用できるメモリーの容量 (キロバイト)。

cached_attribute_auto_adjust

属性キャッシュの自動調整がオンまたはオフのいずれに構成されているかを示します。

cached_attribute_auto_adjust_time

属性キャッシュの自動調整が開始される、構成済みの時間を示します。

cached_attribute_auto_adjust_time_interval

その日に属性キャッシュの自動調整が繰り返される時間間隔を示します。

cached_attribute_hit

changelog 属性キャッシュによって処理できるフィルター内で属性が使用された回数。この値は次の形式で報告されます。

```
cached_attribute_hit=attrname:####
```

cached_attribute_size

changelog 属性キャッシュ内でこの属性が使用しているメモリーの容量。この値は次の形式でキロバイト単位で報告されます。

```
cached_attribute_size=attrname:#####
```

cached_attribute_candidate_hit

フィルターで使用されるすべての属性がキャッシュされている場合に、changelog 属性キャッシュによって処理されるフィルター内で使用されたキャッシュされていない属性のうち、最も頻繁に使用された最大 10 個のリスト。この値は次の形式で報告されます。

```
cached_attribute_candidate_hit=attrname:####
```

このリストは、キャッシュする属性を決定する際に役に立ちます。通常は、メモリーの制約があるため、属性キャッシュに書き込む属性の数は制限することになります。

currenttime

サーバーの現在の時刻。現在の時刻は、以下の形式で表示されます。

```
year-month-day hour:minutes:seconds GMT
```

starttime

サーバーを始動した時刻。開始時刻は、以下の形式で表示されます。

```
year-month-day hour:minutes:seconds GMT
```

trace_enabled

サーバーに対する現在のトレース値。トレース・データを収集する場合は TRUE、収集しない場合は FALSE を指定します。トレース機能の使用可能化と始動について詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の **ldaptrace** コマンド情報を参照してください。

trace_message_level

サーバーに対する現在の ldap_debug 値。値は 16 進数形式です。例を以下に示します。

```
0x0=0  
0xffff=65535
```

詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」のセクション『*Debugging levels*』を参照してください。

trace_message_log

サーバーに対する現在の LDAP_DEBUG_FILE 環境変数設定。

auditinfo

現在の監査構成を含みます。この属性は、管理者によってモニター検索が開始された場合にのみ表示されます。

en_currentregs

イベント通知のクライアント登録の現在の数。

en_notificationssent

サーバーが始動した後にクライアントに送信されたイベント通知の合計数。

currentpersistentsearches

アクティブな永続検索接続の数を示します。

persistentsearchpendingchanges

永続検索によってこれから処理される、キュー内の新規更新の数を示します。

persistentsearchprocessedchanges

永続検索プロセスによって処理された変更の数を示します。

lostpersistentsearchconns

切断した永続検索接続の数を示します。

bypass_deref_aliases

別名処理をバイパスできるかどうかを示すサーバー・ランタイム値。ディレク

トリーに別名オブジェクトが存在しない場合は true が表示され、ディレクトリーに 1 つ以上の別名オブジェクトが存在する場合は false が表示されます。

available_workers

作業に振り向けることができるワーカー・スレッドの数。

current_workqueue_size

作業キューの現在の深さ。

largest_workqueue_size

作業キューの最大サイズ。

idle_connections_closed

自動接続クリーナーによって閉じられたアイドル状態接続の数。

auto_connection_cleaner_run

自動接続クリーナーが実行された回数。

注: IBM Security Directory Server 6.3 リリース以降、属性キャッシュは非推奨になりました。今後は、属性キャッシュを使用しないでください。

cn=workers,cn=monitor コマンドの使用:

ワーカー・スレッドに関する情報を取得するには、**cn=workers,cn=monitor** コマンドを使用します。

ワーカー・スレッド情報を取得するには、監査を使用可能にし、次のコマンドを発行します。

```
idsldapsearch -D <adminDN> -w <adminpw> -b cn=workers,cn=monitor  
-s base objectclass=*
```

このコマンドにより、各アクティブ・ワーカーごとに次のタイプの情報が得られます。

cn=workers,cn=monitor

cn=workers

objectclass=container

cn=thread2640,cn=workers,cn=monitor

thread ワーカー・スレッドの数 (例: 2640)。

ldapversion

LDAP バージョンのレベル (V3 または V2)。

binddn

サーバーのバインドに使用する DN。

clientip

クライアントの IP アドレス。

clientport

クライアントが使用するポート。

connectionid

接続を識別する数値。

received

作業要求を受け取った日時。

workrequest

受け取った作業要求のタイプと要求に関する追加情報。例えば、要求が検索の場合は、以下の情報も表示されます。

```
base=cn=workers,cn=monitor
scope=baseObject
derefaliases=neverDerefAliases
typesonly=false
filter=(objectclass=*)
attributes=all
```

cn=connections,cn=monitor コマンドの使用:

サーバー接続に関する情報を取得するには、**cn=connections,cn=monitor** コマンドを使用します。

```
idsldapsearch -D <adminDN> -w <adminpw> -h <servername> -p <portname> -b
cn=connections,cn=monitor -s base objectclass=*
```

この検索を実行すると、以下のような結果が返されます。

```
cn=connections,cn=monitor
connection=3546 : 9.48.181.83 : 2005-02-28 21:53:54 GMT: 1 : 5 : CN=ROOT ::
connection=3550 : 9.48.181.83 : 2005-02-28 21:53:54 GMT: 1 : 3 : CN=ROOT ::
connection=3551 : 9.48.181.83 : 2005-02-28 21:53:55 GMT: 1 : 4 : CN=ROOT ::
connection=3553 : 9.48.181.83 : 2005-02-28 21:53:55 GMT: 1 : 3 : CN=ROOT ::
connection=3554 : 9.48.181.83 : 2005-02-28 21:53:55 GMT: 1 : 5 : CN=ROOT ::
connection=3555 : 9.48.181.83 : 2005-02-28 21:53:55 GMT: 1 : 2 : CN=ROOT ::
connection=3556 : 9.48.181.83 : 2005-02-28 21:53:55 GMT: 1 : 2 : CN=ROOT ::
connection=3557 : 9.48.181.83 : 2005-02-28 21:53:55 GMT: 1 : 1 : CN=ROOT ::
connection=3558 : 9.48.181.83 : 2005-02-28 21:53:55 GMT: 1 : 1 : CN=ROOT ::
connection=3559 : 9.48.181.83 : 2005-02-28 21:53:55 GMT: 0 : 1 : CN=ROOT ::
```

connection=xxxx

接続番号。

9.48.181.83

サーバー IP アドレス。

2005-02-28 21:53:54 GMT

サーバーの現在の時刻。現在の時刻は、以下の形式で表示されます。

```
year-month-day hour:minutes:seconds GMT
```

1 : 5 最初の数値が opsinprogress、次の数値が opscompleted を表します。

- opsinprogress – 進行中の要求の数。
- opscompleted – サーバーの始動後に完了した要求の数。

CN=ROOT

これは、接続がバインドされるとき DN です。

cn=changelog,cn=monitor コマンドの使用:

変更ログに関する情報を取得するには、**cn=changelog,cn=monitor** コマンドを使用します。

```
idsldapsearch -D <adminDN> -w <adminpw> -h <servername> -p <portname> -b
cn=changelog,cn=monitor -s base objectclass=*
```

この検索を実行すると、以下のような結果が返されます。

```
CN=CHANGELOG,CN=MONITOR
cached_attribute_total_size=0
cached_attribute_configured_size=0
```

cached_attribute_total_size

changelog 属性キャッシュによって使用されているメモリーの容量 (キロバイト)。この数値には、個々の属性キャッシュには課せられないキャッシュの管理に使用される追加メモリー容量が含まれます。したがって、この合計サイズは、すべての属性キャッシュで使用されるメモリーの合計よりも大きくなります。

cached_attribute_configured_size

changelog 属性キャッシュが使用できるメモリーの最大容量 (キロバイト)。

cached_attribute_hit

changelog 属性キャッシュが処理できるフィルターで属性が使用された回数。この値は次の形式で報告されます。

```
cached_attribute_hit=attrname:####
```

cached_attribute_size

changelog 属性キャッシュ内でこの属性が使用しているメモリーの容量。この値は次の形式でキロバイト単位で報告されます。

```
cached_attribute_size=attrname:#####
```

cached_attribute_candidate_hit

フィルターが使用するすべての属性がキャッシュされている場合に、changelog 属性キャッシュが処理できるフィルターで使用されたキャッシュされていない属性のうち、もっとも頻繁に使用されたものが最大 10 個のリスト形式で表されます。この値は次の形式で報告されます。

```
cached_attribute_candidate_hit=attrname:####
```

このリストは、キャッシュする属性を決定する際役に立ちます。通常は、メモリーの制約があるため、属性キャッシュに書き込む属性の数は制限することになります。

注: IBM Security Directory Server 6.3 リリース以降、属性キャッシュは非推奨になりました。今後は、属性キャッシュを使用しないでください。

cn=system,cn=monitor コマンドの使用:

ディレクトリー・サーバーが稼働しているマシンからシステム情報を収集するには、**cn=system,cn=monitor** コマンドを使用します。

```
idsldapsearch -D <adminDN> -w <adminpw> -b cn=system,cn=monitor  
-s base objectclass=*
```

返される情報は、ディレクトリー・サーバーが稼働しているオペレーティング・システムによって異なります。Windows オペレーティング・システムが稼働しているマシンでは、以下の情報が返されます。

memoryUsed

使用された仮想メモリーの量 (KB)。

memoryFree

アイドル・メモリーの量 (KB)。

operatingSystem

オペレーティング・システム名。インスタンスの場合は、Windows または Windows-X640。

diskSpaceUsedByDB

DB2 データベースが保管されるディレクトリーが使用するディスク・スペース (KB)。

diskSpaceAvailableToDB

DB2 データベースで使用可能なディスク・スペース (KB)。

Windows 以外のオペレーティング・システムが稼働しているマシンでは、以下の情報が返されます。

operatingSystem

オペレーティング・システム名。インスタンスの場合は、Linux-x32、Linux-x64、Linux-PPC、Linux-Z、Solaris、Solaris-x86、または AIX。

diskSpaceUsedByDB

DB2 データベースが保管されるディレクトリーが使用するディスク・スペース (KB)。

diskSpaceAvailableToDB

DB2 データベースで使用可能なディスク・スペース (KB)。

キャッシュ・ステータスの表示

キャッシュ・ステータスを表示するには、以下の手順を実行します。

このタスクについて

ナビゲーション領域で「サーバー管理」カテゴリーを展開します。「キャッシュ・ステータスの表示」をクリックします。このパネルには、以下の 6 つのタブがあります。このパネルの下部で、「再表示」ボタンをクリックすると、現在のタブに表示されているステータスが更新されます。「閉じる」をクリックすると、IBM Security Directory Server の「概要」パネルに戻ります。

項目キャッシュのタブ

項目キャッシュ内のエレメントに関する情報を表示するには、「項目キャッシュ」タブを使用します。

「項目キャッシュ」には、以下の情報が表示されます。

項目キャッシュのエレメント数

「項目キャッシュのエレメント数」フィールドの値は、現在項目キャッシュにあるエレメントの数を示します。 **cn=monitor** 項目の属性 **entry_cache_current** は、このフィールドに関連付けられています。

項目キャッシュの最大エレメント数

「項目キャッシュの最大エレメント数」フィールドの値は、項目キャッシュに対して指定されたエレメントの最大数を示します。 **cn=monitor** 項目の属性 **entry_cache_size** は、このフィールドに関連付けられています。

項目キャッシュのヒット

「項目キャッシュのヒット」フィールドの値は、検索またはその他の LDAP

操作中にエレメントが項目キャッシュで検出された回数を示します。

cn=monitor 項目の属性 **entry_cache_hit** は、このフィールドに関連付けられています。

項目キャッシュの欠落

「項目キャッシュの欠落」フィールドの値は、検索またはその他の LDAP 操作中にエレメントが項目キャッシュで使用不可になった回数を示します。

cn=monitor 項目の属性 **entry_cache_miss** は、このフィールドに関連付けられています。

「フィルター・キャッシュ」タブ

検索フィルター・キャッシュに関する情報を表示するには、「フィルター・キャッシュ」タブを使用します。

「フィルター・キャッシュ」タブには、以下の情報が表示されます。

フィルター・キャッシュのエレメント数

「フィルター・キャッシュのエレメント数」フィールドの値は、現在フィルター・キャッシュにあるエレメントの数を示します。**cn=monitor** 項目の属性 **filter_cache_current** は、このフィールドに関連付けられています。

フィルター・キャッシュの最大エレメント数

「フィルター・キャッシュの最大エレメント数」フィールドの値は、フィルター・キャッシュに対して指定されたエレメントの最大数を示します。

cn=monitor 項目の属性 **filter_cache_size** は、このフィールドに関連付けられています。

フィルター・キャッシュのヒット

「フィルター・キャッシュのヒット」フィールドの値は、検索操作やその他の LDAP 操作の実行中に、フィルター・キャッシュでエレメントが検出された回数を示します。**cn=monitor** 項目の属性 **cn=monitor** は、このフィールドに関連付けられています。

フィルター・キャッシュの欠落

「フィルター・キャッシュの欠落」フィールドの値は、検索操作やその他の LDAP 操作の実行中に、フィルター・キャッシュでエレメントが使用不可になった回数を示します。**cn=monitor** 項目の **filter_cache_miss** 属性は、このフィールドに関連付けられます。

フィルター・キャッシュに追加される簡易検索の最大エレメント数

「フィルター・キャッシュに追加される簡易検索の最大エレメント数」フィールドの値は、フィルター・キャッシュに追加される検索操作のエレメントの最大数を示します。**cn=monitor** 項目の **filter_cache_bypass_limit** 属性は、このフィールドに関連付けられます。

ACL キャッシュ・タブ

アクセス制御リスト・キャッシュに関する情報を表示するには、「ACL キャッシュ」タブを使用します。

「ACL キャッシュ」タブには、以下の情報が表示されます。

キャッシュ ACL 情報

「キャッシュ ACL 情報」フィールドの値は、ACL キャッシュが使用可能かどうかを示します。 **cn=monitor** 項目の **acl_cache** 属性は、このフィールドに関連付けられます。

ACL キャッシュの最大エレメント数

「ACL キャッシュの最大エレメント数」フィールドの値は、ACL キャッシュに対して指定されたエレメントの最大数を示します。 **cn=monitor** 項目の属性 **acl_cache_size** は、このフィールドに関連付けられています。

グループ・メンバーのキャッシュ・タブ

メンバーに関するキャッシュ情報と、そのメンバーの項目が設定された **uniquemember** 属性値を表示するには、「グループ・メンバーのキャッシュ」タブを使用します。

「グループ・メンバーのキャッシュ」には、以下の情報が表示されます。

キャッシュ内で許可されるグループの最大数

「キャッシュ内で許可されるグループの最大数」フィールドの値は、キャッシュされるグループの最大数を示します。 **group_members_cache_size** 属性は、このフィールドに関連付けられます。

キャッシュできるグループ内のメンバーの最大数

「キャッシュできるグループ内のメンバーの最大数」フィールドの値は、グループ・メンバーのキャッシュ内のグループでキャッシュできるメンバーの最大数を示します。 **group_members_cache_bypass_limit** 属性は、このフィールドに関連付けられます。

キャッシュ内のグループ数

「キャッシュのグループ数」フィールドの値は、グループ・メンバーのキャッシュ内でメンバーが現在キャッシュされているグループの数を示します。 **group_members_cache_current** 属性は、このフィールドに関連付けられます。

グループ・キャッシュのヒット

「グループ・キャッシュのヒット」フィールドの値は、グループ・メンバーのキャッシュから正常に取得されたグループ・メンバーの要求の数を示します。 **group_members_cache_hit** 属性は、このフィールドに関連付けられます。

グループ・キャッシュの欠落

「グループ・キャッシュの欠落」フィールドの値は、グループ・メンバーのキャッシュ内で使用不可で、DB2 から正常に取得されたグループ・メンバーの要求の数を示します。 **group_members_cache_miss** 属性は、このフィールドに関連付けられます。

ディレクトリー・キャッシュ属性

ディレクトリー・キャッシュ属性に関する情報を表示するには、「ディレクトリー・キャッシュ属性」タブを使用します。

以下の情報を表示するには、「ディレクトリー・キャッシュ属性」をクリックします。ステータス項目が表形式で表示されます。

注: ディレクトリー・キャッシュ属性が存在しない場合、「ディレクトリー・キャッシュ属性」テーブルは表示されません。代わりに、ディレクトリー・キャッシュ属性が存在しないことを示すメッセージが表示されます。

表7. ディレクトリー・キャッシュ属性の表

属性 [△]	キャッシュ・ヒットの数 [△]	キャッシュ・サイズ [△]

属性 属性の名前を示します。

キャッシュ・ヒットの回数

属性フィルターがキャッシュされてから使用された回数を示します。

キャッシュ・サイズ

この属性キャッシュによって使用されるメモリー容量を示します。

このタブには、以下の 2 つの編集不可フィールドもあります。

キャッシュ対象属性の合計サイズ (キロバイト)

キャッシュによって使用されているメモリー容量を示します。

注: この数値には、キャッシュの管理に使用される追加のメモリー容量も含まれます。その合計容量は、個々の属性キャッシュで使用されるメモリーの合計よりも大きくなります。

キャッシュ属性の構成済みサイズ (キロバイト)

属性キャッシュが使用できるメモリーの最大容量を示します。

注: IBM Security Directory Server 6.3 リリース以降、属性キャッシュは非推奨になりました。今後は、属性キャッシュを使用しないでください。

ディレクトリー・キャッシュ候補

ディレクトリー・キャッシュ候補に関する情報を表示するには、「ディレクトリー・キャッシュ候補」タブを使用します。

「ディレクトリー・キャッシュ候補」には、ディレクトリー・キャッシュ候補に関する情報が表形式で表示されます。

注: ディレクトリー・キャッシュ候補が存在しない場合、「ディレクトリー・キャッシュ候補」テーブルは表示されません。代わりに、ディレクトリー・キャッシュ候補が存在しないことを示すメッセージが表示されます。

表8. ディレクトリー・キャッシュ候補の表

属性 [△]	ヒットの回数 [△]

属性 属性の名前を示します。

ヒットの回数

属性フィルターの使用回数を示します。

サーバー機能 (ルート DSE) 情報の表示

この情報に従い、サーバー機能 (ルート DSE) の情報を表示します。

ルート DSE エントリーには LDAP サーバー・インスタンスについての情報が含まれており、ルート DSE 検索で照会できます。サーバー・インスタンスは、ルート DSE 検索の実行時に、以下の側面を表示します。

- ルート DSE 属性とそれらの値
- サポートされ、使用可能になっている機能の OID
- サポートされる拡張機能と制御の OID

ルート DSE を表示するには、以下のいずれか 1 つの方法を使用します。

Web 管理の使用

ここで説明する手順に従い、Web 管理ツールを使用してルート DSE 検索を開始することができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「サーバー機能の表示 (ルート DSE)」をクリックします。次に、「一般」をクリックします。

「一般」タブには、以下の情報が表示されます。

サーバー・インスタンス名

このフィールドには、サーバーで稼働しているディレクトリー・サーバー・インスタンスの名前が表示されます。このフィールドには、ルート DSE エントリーの `ibm-slapdServerInstanceName` 属性の値が取り込まれます。

サーバー ID

このフィールドには、サーバーの最初の始動時にサーバーに割り当てられる固有の ID が表示されます。この ID は、サーバーの役割を判別するために複製トポロジーで使用されます。このフィールドには、ルート DSE エントリーの `ibm-serverId` 属性の値が取り込まれます。

ポート番号

このフィールドには、サーバーが `listen` している非セキュア・ポートが表示されます。このフィールドは、サーバーでセキュア・ポートが使用可能に設定されていない場合にのみ存在します。このフィールドには、ルート DSE エントリーの `port` 属性の値が取り込まれます。

ディレクトリー・バージョン

このフィールドには、サーバーにインストールされている IBM Security Directory Server のバージョンが表示されます。このフィールドには、ルート DSE エントリーの `ibmdirectoryversion` 属性の値が取り込まれます。

サーバー・バックエンド

このフィールドには、このサーバーがデータベースをロードするのか、プロキシー・バックエンドをロードするのかが指定されます。このフィールドには、ルート DSE エントリーの `ibm-slapdServerBackend` 属性の値が取り込まれます。

サポートされる監査バージョン

このフィールドには、サポートされる監査のバージョンが表示されます。このフィールドには、ルート DSE エントリーの `ibm-supportedAuditVersion` 属性の値が取り込まれます。

LDAP サービス名

このフィールドには、サーバーのホスト名が表示されます。Kerberos レalm が定義されている場合、値は `hostname@realmname` の形式で表示されます。このフィールドには、ルート DSE エントリーの `ibm-ldapservicename` 属性の値が取り込まれます。

セキュリティー

このフィールドには、サーバーが `listen` しているセキュア SSL ポートが表示されます。このフィールドには、ルート DSE エントリーの `security` 属性の値が取り込まれます。

サイズ制限

このフィールドには、非管理ユーザーが開始する検索で戻される項目数の限度が表示されます。このフィールドには、ルート DSE エントリーの `ibm-slapedSizeLimit` 属性の値が取り込まれます。

時間制限 (秒)

このフィールドには、非管理ユーザーが開始する検索要求の処理にかかる最大時間 (秒) が表示されます。このフィールドには、ルート DSE エントリーの `ibm-slapedTimeLimit` 属性の値が取り込まれます。

別名の参照解除

このフィールドには、サーバーに参照解除の処理がどのように構成されているかが表示されます。このフィールドには、ルート DSE エントリーの `ibm-slapedDerefAliases` 属性の値が取り込まれます。

ベンダー名

このフィールドには、サーバーで稼働している LDAP のバージョンのサブライヤーが表示されます。このフィールドには、ルート DSE エントリーの `vendorname` 属性の値が取り込まれます。例えば IBM Security Directory Server では、この属性は International Business Machines (IBM) に設定されます。

ベンダー・バージョン

このフィールドには、ディレクトリー・サーバーのバージョンが表示されます。このフィールドには、ルート DSE エントリーの `vendorversion` 属性の値が取り込まれます。例えば IBM Security Directory Server (TDS) 6.3 の場合、ベンダー・バージョンは 6.3 に設定されます。

サブスキーマのサブ項目

このフィールドには、属性がスキーマを指定できるようにするためのサブスキーマ項目の名前が表示されます。このフィールドには、ルート DSE エントリーの `subschemasubentry` 属性の値が取り込まれます。値は `cn=schema` に設定されます。

SASL ダイジェスト・レム名

このフィールドには、サーバーに関連付けられている SASL ダイジェスト・レム名が表示されます。このフィールドには、ルート DSE エントリーの `ibm-sasldigestrealmname` 属性の値が取り込まれます。

サポートされる LDAP バージョン

このリストには、現行サーバーによってインプリメントされた LDAP バージョンが表示されます。このリストには、ルート DSE エントリーの supportedldapversion 属性の値が取り込まれます。この属性の値は、サーバーによってインプリメントされる LDAP プロトコルのバージョンです。

命名コンテキスト

このリストには、サーバーで使用可能なネーミング・コンテキストが表示されます。このリストには、ルート DSE エントリーの namingcontexts 属性の値が取り込まれます。この属性の値は、このサーバーがマスターまたはシャドウを生成する命名コンテキストに対応します。サーバーが情報をマスター化またはシャドウ化しない場合 (例えば、サーバーが公開 X.500 ディレクトリーに対する LDAP ゲートウェイである場合など)、この属性は存在しません。

サーバーにディレクトリー全体が含まれる場合、属性は単一の値を持ちますが、その値はルートのヌル DN を示す空ストリングです。これにより、クライアントがサーバーに接続するときに、検索に適した基本オブジェクトを選択できます。

ネーミング・コンテキストの構成

このフィールドには、サーバーの構成項目が格納されるサフィックスが表示されます。このフィールドには、ルート DSE エントリーの ibm-configurationnamingcontext 属性の値が取り込まれます。

「再表示」をクリックすると、このパネルの情報を更新できます。「概要」パネルに戻るには「閉じる」をクリックします。サポートされている機能に関する情報を表示するには、「サポートされる機能」をクリックします。「サポートされる機能」タブには、以下の情報が表示されます。

サポートされる機能

このリストには、現在サーバーでサポートされているサーバー機能が表示されます。このリストには、ルート DSE エントリーの ibm-supportedcapabilities 属性の値が取り込まれます。

「再表示」をクリックすると、このパネルの情報を更新できます。「概要」パネルに戻るには「閉じる」をクリックします。使用可能な機能に関する情報を表示するには、「使用可能な機能」をクリックします。「使用可能な機能」タブには、以下の情報が表示されます。

使用可能な機能

このリストには、現在サーバーで使用可能になっているサーバー機能が表示されます。このリストには、ルート DSE エントリーの ibm-enabledcapabilities 属性の値が取り込まれます。

「再表示」をクリックすると、このパネルの情報を更新できます。「閉じる」をクリックして「概要」パネルに戻ります。サポートされる拡張機能に関する情報を表示するには、「サポートされる拡張機能」をクリックします。「サポートされる拡張機能」タブには、以下の情報が表示されます。

サポートされる拡張機能

このリストには、サーバーでサポートされる拡張操作のオブジェクト ID

(OID) が表示されます。このリストには、ルート DSE エントリーの supportedExtension 属性の値が取り込まれます。

「再表示」をクリックすると、このパネルの情報を更新できます。「概要」パネルに戻るには「閉じる」をクリックします。サポートされている制御に関する情報を表示するには、「サポートされる制御」をクリックします。「サポートされる制御」タブには、以下の情報が表示されます。

サポートされる制御

このリストには、サーバーでサポートされる制御のオブジェクト ID (OID) が表示されます。このリストには、ルート DSE エントリーの supportedControl 属性の値が取り込まれます。

「再表示」をクリックすると、このパネルの情報を更新できます。「概要」パネルに戻るには「閉じる」をクリックします。サポートされている SASL メカニズムに関する情報を表示するには、「サポートされる SASL メカニズム」をクリックします。「サポートされる SASL メカニズム」タブには、以下の情報が表示されます。

サポートされる SASL メカニズム

このリストには、サーバーでサポートされる SASL メカニズムの名前がすべて表示されます。このリストには、ルート DSE エントリーの supportedSaslMechanisms 属性の値が取り込まれます。この属性には、サーバーに登録されている SASL 機構が含まれています。

「再表示」をクリックすると、このパネルの情報を更新できます。「概要」パネルに戻るには「閉じる」をクリックします。

コマンド行の使用

サーバー・インスタンスに対してルート DSE 検索を実行すると、ルート DSE 属性およびそれらの値、サポートされる使用可能な機能の OID、サポートされる拡張機能および制御の OID が表示されます。示されているコマンドを発行して、ルート DSE 検索を開始することができます。

このタスクについて

```
idsldapsearch -s base -b "" objectclass=*
```

ルート DSE 属性について詳しくは、623 ページの『ルート DSE 内の属性』を参照してください。

サーバーで現在使用可能に設定されているサーバー機能をリストするには、次のコマンドを発行します。

```
idsldapsearch -s base -b "" objectclass=* ibm-supportedcapabilities
```

サーバーで現在使用可能に設定されているサーバー機能をリストするには、次のコマンドを発行します。

```
idsldapsearch -s base -b "" objectclass=* ibm-enabledcapabilities
```

サーバー接続の管理

以下の情報を使用して、サーバー接続を管理します。

サーバーの接続状況を確認するには、以下のいずれかの方法を使用します。

Web 管理の使用

以下の説明に従い、Web 管理ツールを使用してサーバー接続を管理することができます。

このタスクについて

ナビゲーション領域で「サーバー管理」カテゴリを展開します。「サーバー接続の管理」をクリックします。以下の情報を含む表が各接続ごとに表示されます。各見出しの隣の矢印を使用して、降順ソートまたは昇順ソートを指定できます。また、「アクションの選択」ドロップダウン・リストから「ソートの編集」を選択して「実行」をクリックするか、あるいは「ソートの編集」アイコンをクリックすると、最大 3 つのソート基準を指定できます。

DN サーバーへのクライアント接続の DN を指定します。

IP アドレス

サーバーに接続するクライアントの IP アドレスを指定します。

開始時刻

接続された日時を指定します。

状況 接続がアクティブかアイドルかを指定します。進行中の操作がある場合は、接続はアクティブと見なされます。

保留中の操作

接続を確立してから保留されている操作の数を示します。

完了した操作

接続ごとに完了した操作の数を指定します。

タイプ 接続が SSL と TLS のどちらで保護されているのかを指定します。これ以外で保護されている場合、フィールドはブランクになります。

注:

- この表は、最大 20 個の接続を同時に表示します。

この表を DN または IP アドレスのどちらで表示するのかを指定するには、パネル上部にあるドロップダウン・メニューを展開し、該当する項目を選択します。デフォルトの設定は、DN による表示です。同様に、表の表示順を昇順または降順のいずれかに指定できます。

「再表示」をクリックするか、あるいは「アクションの選択」ドロップダウン・リストから「再表示」を選択して「実行」をクリックすると、現在の接続情報を更新できます。

管理者として、または DirDataAdmin 役割または ServerConfigGroupMember 役割があるローカル管理グループのメンバーとしてログオンしている場合は、サーバー接続を切断するもう 1 つの選択肢がパネル上に表示されます。このサーバー接続切断機能により、サービス妨害攻撃を停止したり、サーバーへのアクセスを制御したりすることができます。接続を切断するには、ドロップダウン・メニューを展開して、DN または IP アドレス、あるいはその両方を選択し、「切断」をクリックします。選択内容に応じて以下のアクションが実行されます。

表 9. 切断の規則

選択した DN	選択した IP アドレス	処置
<DNvalue>	なし	指定の DN とバインドしているすべての接続が切断されます。
なし	<IPvalue>	指定の IP アドレスを介しているすべての接続が切断されます。
<DNvalue>	<IPvalue>	指定の DN としてバインドし、指定の IP アドレスを介しているすべての接続が切断されます。
なし	なし	これは有効な条件ではありません。必ず DN、IP アドレスのいずれか、またはこれら両方を指定して、切断機能を使用してください。

ドロップダウン・メニューのデフォルト値は、どちらも「なし」です。

この要求を実行しているサーバー接続以外のサーバー接続をすべて切断するには、「すべて切断」をクリックします。確認の警告が表示されます。「OK」をクリックして切断アクションを進めるか、または「キャンセル」をクリックしてアクションを終了し、「サーバー接続の管理」パネルに戻ります。

コマンド・ラインの使用

以下のコマンドを実行して、サーバー接続を表示することができます。

このタスクについて

```
idsldapsearch -D <adminDN> -w <adminPW> -h <servername> -p <portnumber>
-b cn=connections,cn=monitor -s base objectclass=*
```

このコマンドは情報を以下の形式で戻します。

```
cn=connections,cn=monitor
connection=1632 : 9.41.21.31 : 2002-10-05 19:18:21 GMT: 1 : 1 : CN=ADMIN : :
connection=1487 : 127.0.0.1 : 2002-10-05 19:17:01 GMT: 1 : 1 : CN=ADMIN : :
```

注: 該当する場合は、各接続に SSL または TLS インディケータが追加されません。

サーバーの接続を終了するには、以下のいずれかのコマンドを発行します。

```
# To disconnect a specific DN:
idsldapexop -D <adminDN> -w <adminPW> -op unbind -dn cn=john

# To disconnect a specific IP address:
idsldapexop -D <adminDN> -w <adminPW> -op unbind -ip 9.182.173.43

#To disconnect a specific DN over a specific IP address:
idsldapexop -D <adminDN> -w <adminPW> -op unbind -dn cn=john -ip 9.182.173.43

#To disconnect all connections:
idsldapexop -D <adminDN> -w <adminPW> -op unbind -all
```

接続の終了について詳しくは、「IBM Security Directory Server Version 6.3 Command Reference」の **ldapexop** コマンド情報を参照してください。

接続プロパティの管理

この機能により、接続プロパティを管理することができます。

接続プロパティの管理機能では、次のようなクライアントの接続を終了することにより、サーバーのロックを防止できます。

- データを低速で送信する、データを部分的に送信する、またはデータを送信しない。
- データ結果を読み取らないか、または低速で結果を読み取る。
- アンバインドしない。
- 匿名でバインドする。

また、この機能を使用すると、長時間実行されるタスクによりバックエンドが使用中になっている場合でも管理者はいつでもサーバーにアクセスすることができます。

Web 管理の使用

ここで説明する手順に従うことにより、Web 管理ツールを使用して接続プロパティを管理できます。

このタスクについて

以下の選択肢が表示されるのは、この機能をサポートしているサーバーに、管理者または管理グループのメンバーとしてログインしている場合のみです。

ナビゲーション領域で「**サーバー管理**」カテゴリを展開します。「**接続プロパティの管理**」をクリックします。

注: 実際の最大しきい値数は、プロセスごとに許可されているファイル数によって制限されます。UNIX または Linux システムでは、**ulimit -a** コマンドを使用して制限を決定できます。Windows システムでは、この値は固定されています。

1. 「**一般**」タブを選択します。
2. 「**匿名接続の許可**」チェック・ボックスがすでに選択されているので、匿名バインドは許可されています。これはデフォルトの設定です。このチェック・ボックスをクリックすると、「**匿名接続の許可**」機能が選択解除されます。このアクションにより、サーバーは匿名接続をすべてアンバインドします。**注:** 匿名バインドを禁止すると、アプリケーションによっては処理が失敗する場合があります。
3. 匿名接続のクリーンアップを開始するしきい値を設定します。「**匿名接続のクリーンアップしきい値**」フィールドに 0 から 65535 までの数値を指定できます。デフォルトの設定は 0 です。匿名接続の数がこの数値を超えると、「**アイドル・タイムアウト**」フィールドで設定したアイドル・タイムアウトの制限値に基づいて、接続がクリーンアップされます。
4. 認証済み接続のクリーンアップを開始するしきい値を設定します。「**認証済み接続のクリーンアップしきい値**」フィールドに 0 から 65535 までの数値を指定できます。デフォルトの設定は 1100 です。認証済み接続の数がこの数値を超えると、「**アイドル・タイムアウト**」フィールドで設定したアイドル・タイムアウトの制限値に応じて、接続がクリーンアップされます。
5. すべての接続のクリーンアップを開始するしきい値を設定します。「**全接続のクリーンアップしきい値**」フィールドに 0 から 65535 までの数値を指定できます。デフォルトの設定は 1200 です。接続数の合計数がこの数値を超えると、「**アイドル・タイムアウト**」フィールドで設定したアイドル・タイムアウトの制限値に応じて、接続がクリーンアップされます。

6. クリーンアップ処理によって接続を閉じるまでのアイドル状態の秒数を設定します。「アイドル・タイムアウト制限」フィールドには、0 から 65535 までの数値を指定できます。デフォルトの設定は 300 です。クリーンアップ処理が開始されると、この処理に従って、制限値を超える接続がすべて閉じられます。
7. 書き込み試行の後、次の書き込み試行を許可するまでの秒数を設定します。「結果タイムアウト制限」フィールドには、0 から 65535 までの数値を指定できます。デフォルト設定は 10 です。クリーンアップ処理が開始されると、この制限を超えた接続が閉じられます。注: Windows システムの場合、30 秒を超えると、接続は自動的にドロップされます。したがって、「結果タイムアウト制限」の設定値は 30 秒が経過するとオペレーティング・システムによってオーバーライドされます。
8. 完了したら、終了せずに変更を保存する場合は「適用」をクリックし、変更を適用して終了する場合は「OK」をクリックし、変更を行わずにこのパネルを終了するには「キャンセル」をクリックします。

コマンド・ラインの使用

以下に示すコマンドをコマンド行で使用することにより、接続プロパティを管理することができます。

このタスクについて

コマンド行を使用して同じ操作を実行するには、以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Connection Management,cn=Front End,cn=Configuration
changetype: modify
replace: ibm-slapdAllowAnon
ibm-slapdAllowAnon:TRUE
-
replace: ibm-slapdAnonReapingThreshold
ibm-slapdAnonReapingThreshold: 0
-
replace: ibm-slapdBoundReapingThreshold
ibm-slapdBoundReapingThreshold: 1100
-
replace: ibm-slapdAllReapingThreshold
ibm-slapdAllReapingThreshold: 1200
-
replace: ibm-slapdIdleTimeOut
ibm-slapdIdleTimeOut: 300
-
replace: ibm-slapdWriteTimeout
ibm-slapdWriteTimeout: 10
```

設定を動的に更新するには、以下の **idsldapexop** コマンドを発行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readconfig -scope entire
```

idsldapexop コマンドでは、これらの属性のうち動的に変更可能なもののみが更新されます。他の変更内容を有効にするには、サーバーを停止して再始動する必要があります。動的に更新可能な属性のリストについては、713 ページの『付録 L. 動的に変更される属性』を参照してください。

サーバー・プロパティの設定

サーバーのプロパティを設定する場合は、以下の情報を参照してください。

サーバーには、以下のプロパティを設定できます。

- 117 ページの『サーバー・ポートの変更および言語タグの使用可能化』
- 122 ページの『検索設定』
- 135 ページの『トランザクション・サポート』
- 132 ページの『イベント通知』
- 137 ページの『サフィックスの追加または除去』
- 301 ページの『参照』
- 145 ページの『属性キャッシュへの属性の追加と属性キャッシュからの属性の除去』
- 120 ページの『最小 ulimit』

Web 管理ツールが推奨方式ですが、LDAP コーティリティーを使用してサーバー構成ファイルを更新することもできます。LDAP 変更要求は、以下によって生成されます。

- IBM Security Directory Server に付属している C クライアントを使用する C アプリケーション。
- JNDI を使用する Java アプリケーション。
- 標準の V3 LDAP を生成するその他のインターフェース

提供される例では、**idsldapmodify** コマンドを使用します。

idsldapmodify コマンドは、対話モードで実行することも、入力をファイルに指定して実行することもできます。本書に記載されているほとんどの例では、

idsldapmodify コマンドで使用されるファイルの内容を記載しています。これらのファイルで使用するコマンドの一般的な形式は、以下のとおりです。

```
idsldapmodify -D adminDN -w password -i filename
```

サーバー構成の設定を動的に更新するには、以下の **idsldapexop** コマンドを入力する必要があります。次のコマンドは、動的な構成設定をすべて更新します。

```
idsldapexop -D adminDN -w adminPW -op readconfig -scope entire
```

次のコマンドは、単一の設定を更新します。

```
idsldapexop -D adminDN -w adminPW -op readconfig -scope single entry DN  
属性
```

idsldapexop コマンドでは、これらの属性のうち動的に変更可能なもののみが更新されます。他の変更内容を有効にするには、サーバーを停止してから再始動する必要があります。動的に更新可能な属性のリストについては、713 ページの『付録 L. 動的に変更される属性』を参照してください。詳細については、「*IBM Security Directory Server Version 6.3 Command Reference*」に記載されている **idsldapmodify** コマンドと **idsldapexop** コマンドの説明を参照してください。

注: サーバー構成設定の更新を許可されているのは、管理者および管理グループのメンバーのみです。

サーバー・ポートの変更および言語タグの使用可能化

この機能により、サーバーのポートを変更することができます。

注: サーバーのポート設定を変更する場合は、コンソールにあるサーバーのポート設定も変更する必要があります。30 ページの『コンソールでのサーバーの変更』を参照してください。

Web 管理の使用

ここで説明する手順に従うことにより、Web 管理ツールを使用してサーバー・ポートを変更できます。

このタスクについて

Web 管理ナビゲーション領域の「**サーバー管理**」カテゴリをクリックしてから、「**サーバー・プロパティの管理**」タブをクリックして「サーバー・プロパティの管理」パネルを表示します。このパネルは、「**一般**」タブが事前に選択された状態で表示されます。「**一般**」パネルには 2 つの読み取り専用情報フィールドがあり、サーバーのホスト名およびマシンにインストールされている IBM Security Directory Server のバージョン・レベルが表示されます。

このパネルには、それぞれ現在のポート番号を表示する「**非セキュア・ポート**」(デフォルト値は 389)、「**セキュア・ポート**」(デフォルト値は 636)、および言語タグ・サポートの有無を指定するチェック・ボックスという、3 つの変更可能な必須フィールドもあります。

注: 予約済みポートは 0 から 1023 です。登録済みポートは 1024 から 49151 です。動的ポートまたは専用ポートは 65535 から 49152 です。ポート設定を変更したり、言語タグを使用可能にしたりするには、以下の手順を実行します。

1. 「**非セキュア・ポート**」をクリックして、1 から 65535 までの数値を入力します。この例では、399 を入力します。サーバーのポート設定を変更する場合は、コンソールにあるサーバーのポート設定も変更する必要があります。30 ページの『コンソールでのサーバーの変更』を参照してください。
2. 「**セキュア・ポート**」をクリックして、1 から 65535 までの数値を入力します。この例では、699 を入力します。サーバーのポート設定を変更する場合は、コンソールにあるサーバーのポート設定も変更する必要があります。30 ページの『コンソールでのサーバーの変更』を参照してください。
3. 「**言語タグ・サポートの使用可能化**」チェック・ボックスをクリックして、言語タグのサポートを使用可能にします。デフォルトの設定は使用不可です。詳細については、530 ページの『言語タグ』を参照してください。**注:** 言語タグ機能を使用可能にしてから、言語タグを項目の属性に関連付けると、サーバーは言語タグ付きの項目を返します。後で言語タグ機能を使用不可にした場合でも、言語タグ付きの項目が戻されます。サーバーの動作をアプリケーションは予期できない場合があります。潜在的な問題を回避するために、言語タグ機能を使用可能にした後で使用不可にすることはしないでください。
4. 完了したら、終了せずに変更を保存する場合は「**適用**」をクリックし、変更を適用して終了する場合は「**OK**」をクリックし、変更を行わずにこのパネルを終了するには「**キャンセル**」をクリックします。

ポート番号を変更した場合、変更内容を有効にするにはサーバーを停止する必要があります。86 ページの『サーバーの開始と停止』を参照してください。

注: 言語タグは動的に使用可能にしたり使用不可にしたりできます。この際、サーバーを再始動する必要はありません。
サーバーを停止したら、管理サーバーをローカル・マシン上で停止および始動して、ポートを再同期化する必要があります。13 ページの『ディレクトリー管理サーバー』を参照してください。サーバーを再始動します。

コマンド・ラインの使用

以下に示すコマンドをコマンド行で使用することにより、サーバー・ポートを変更することができます。

このタスクについて

言語タグ機能が使用可能であるかどうかを確認するには、属性 **ibm-enabledCapabilities** を指定してルート DSE 検索を発行します。

```
idsldapsearch -b "" -s base objectclass=* ibm-enabledCapabilities
```

OID **1.3.6.1.4.1.4203.1.5.4** が返された場合は、機能が使用可能になっています。

言語タグ・サポートが使用可能でない場合は、言語タグを属性に関連付ける LDAP 操作が拒否され、以下のエラー・メッセージが表示されます。

```
LDAP_NO_SUCH_ATTRIBUTE
```

コマンド行からデフォルト・ポート以外のポートを割り当て、言語タグを使用可能にするには、以下のコマンドを実行します。

```
idsldapmodify -D <adminDN> -w <password> -i <filename>
```

where <filename> contains:

```
dn: cn=configuration
changetype: modify
replace: ibm-slapdPort
ibm-slapdPort: 399
-
replace: ibm-slapdSecurePort
ibm-slapdSecurePort: 699

dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
replace: ibm-slapdLanguageTagsEnabled
ibm-slapdLanguageTagsEnabled: TRUE
```

変更した内容を有効にするには、サーバーを停止する必要があります。86 ページの『サーバーの開始と停止』を参照してください。

注: 言語タグは動的に使用可能にしたり使用不可にしたりできます。この際、サーバーを再始動する必要はありません。
サーバーを停止したら、管理サーバーをローカル・マシン上で停止および始動して、ポートを再同期化する必要があります。13 ページの『ディレクトリー管理サーバー』を参照してください。

パフォーマンスの設定

サーバーのパフォーマンスを設定する場合は、以下の情報を参照してください。

注: 最新のチューニング情報については、IBM Security Directory Server の資料の『パフォーマンス・チューニングとキャパシティー計画』セクションを参照してください。

検索制限と接続設定を変更すると、パフォーマンスの向上が可能です。

Web 管理の使用

Web 管理ツールを使用してサーバーのパフォーマンスを管理するには、以下の手順を実行します。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「サーバー・プロパティの管理」をクリックします。次に、「パフォーマンス」タブをクリックします。

「パフォーマンス」タブでは、データベース接続の設定を構成するときに、ディレクトリーのパフォーマンスを向上させることができます。LDAP サーバーは、特定の数の DB2(R) サーバーへの接続を維持します。この数は、「データベース接続の最大数」フィールドに設定できます。DB2 接続の数を増やすことにより、LDAP の並行性レベルを増加させ、スループット・パフォーマンスを改善することができます。データベース接続の設定を変更してパフォーマンスを改善するには、以下のステップを実行します。

1. 「データベース接続の最大数」フィールドにデータベース接続の最大数を指定します。これは、サーバーが使用する DB2 接続の数を設定します。このフィールドは、接続先サーバーがプロキシ・サーバーとして構成されている場合には使用できません。
2. 「複製用データベース接続の最大数」フィールドに複製用データベース接続の最大数を指定します。これにより、サーバーが複製のために使用する DB2 接続の数が設定されます。このフィールドは、接続先サーバーがプロキシ・サーバーとして構成されている場合には使用できません。
3. トランザクション内にはない操作がデッドロックにならないようにするためにバックエンドが行う再試行の最大回数を指定します。「再試行」を選択する場合は、トランザクション内にはない操作に対して許可する再試行回数を入力する必要があります。選択しない場合は「無制限」を選択します。指定できる値は数値だけです。
4. 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして変更内容を適用し、パネルを終了します。
 - 「適用」をクリックして変更内容を適用し、このパネルを表示させたままにします。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

変更した内容を有効にするには、サーバーを再始動する必要があります。

コマンド・ラインの使用

指定されたコマンドをコマンド行で発行して、同じ操作を実行することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Directory,cn=RDBM Backends,cn=IBM Directory,cn=Schemas,cn=Configuration
changetype: modify
replace: ibm-slapdDbConnections
ibm-slapdDbConnections:15
-
replace: ibm-slapdRep1DbConns
ibm-slapdRep1DbConns:4
```

最小 ulimit

ディレクトリー・サーバーは、サーバーの円滑な実行に重要となる最小 ulimit オプション値を適用しようとしています。

ディレクトリー・サーバーは始動時に、現行プロセスの ulimit オプション値が、構成ファイルに指定された規定の ulimit オプション値以上であるかを検証します。この検証が不合格である場合は、サーバーは現行プロセスの ulimit オプション値を規定の値に設定するようにします。サーバーがこの設定に失敗した場合は、構成専用モードで開始されます。

以下に、標準的な ulimit オプションをすべてリストします。これらの値は、ディレクトリー・サーバーの円滑な実行に重要です。

注: ulimit オプションは、プロキシー・サーバーおよびバックエンド・サーバーに対してのみ適用されます。管理サーバー・プロセスに対しては、最小 ulimit オプション値は指定されていません。

重要なメモリー・パラメーター

仮想メモリー・サイズ

このオプションには、スタック、ヒープ、およびメモリー・マップのファイルなど、すべてのタイプのメモリーが含まれています。この制限を超過してメモリーを割り振ろうとすると、メモリー不足エラーで失敗します。このオプションの値は、キロバイト (KB) で指定します。

最大常駐セット・サイズ (RSS)

このオプションは、任意の 1 プロセスのために物理メモリーにスワップインできるメモリー量を制限します。このオプションの値は、キロバイト (KB) で指定します。

注: AIX ではこの ulimit オプションが定義されていますが、Solaris では定義されていません。

データ・セグメント

このオプションは、プロセスがヒープに割り振ることのできるメモリー量を制限します。このオプションの値は、キロバイト (KB) で指定します。

スタック・サイズ

このオプションは、プロセスがスタックに割り振ることのできるメモリー量を制限します。このオプションの値は、キロバイト (KB) で指定します。

重要なファイル・パラメーター

ファイル・サイズ

このオプションは、プロセスで作成可能なファイルの最大サイズを制限します。これは、512 バイトのブロック単位で指定します。

Nofile このオプションは、単一プロセスに属するファイル記述子の数を制限します。ファイル記述子には、ファイルだけでなく、インターネット通信のソケットも含まれます。

注: Solaris の場合、オープン・ファイル数の制限は、サーバーの始動時に、オープン・ファイル数のハード制限値に設定されます。ulimit 機能を使用してオープン・ファイル数の制限を変更することはできません。

以下の表には、オペレーティング・システムのデフォルト値、および重要なオプションに対する 既定の最小 ulimit 値がリストされています。

表 10. システムに固有の ulimit 値

Ulimit オプション	AIX		Solaris	
	オペレーティング・システムのデフォルト	規定の最小	オペレーティング・システムのデフォルト	規定の最小
データ・セグメント・サイズ	256 MB	256 MB	無制限	256 MB
仮想メモリー	無制限	1 GB	無制限	1 GB
Nofile	2000	500	256	256
最大常駐セット・サイズ (rss)	64 MB	256 MB	N/A	N/A
ファイル・サイズ	1024 MB	1024 MB	無制限	1024 MB
スタック・サイズ	64 MB	64 MB	8 MB	8 MB

表 11. システムに固有の ulimit 値

Ulimit オプション	Linux	
	オペレーティング・システムのデフォルト	規定の最小
データ・セグメント・サイズ	無制限	256 MB
仮想メモリー	無制限	1 GB
Nofile	1024	500
最大常駐セット・サイズ (rss)	N/A	N/A
ファイル・サイズ	無制限	1024 MB
スタック・サイズ	10 MB	10 MB

注: オペレーティング・システムのデフォルトの ulimit オプション値は、カーネル・バージョンが異なったり、同じカーネル・バージョンでもシェルが異なったりすると、変わる場合があります。

管理者は、Web 管理ツールまたはコマンド・ラインを使用して最小 ulimit オプション値を変更できます。

Web 管理の使用

Web 管理ツールを使用して、最小 ulimit オプション値を設定できます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「サーバー・プロパティの管理」をクリックします。次に、「Ulimit 設定」タブをクリックします。

手順

1. 仮想メモリー・サイズを指定するには、「サイズ」を選択してテキスト・ボックスにキロバイトで値を指定します。また、仮想メモリー・サイズを無制限と指定するには、「無制限」を選択します。
2. 常駐セット・サイズを指定するには、「サイズ」を選択してテキスト・ボックスにキロバイトで値を指定します。また、常駐セット・サイズを無制限と指定するには、「無制限」を選択します。
3. データ・セグメント・サイズを指定するには、「サイズ」を選択してテキスト・ボックスにキロバイトで値を指定します。また、データ・セグメント・サイズを無制限と指定するには、「無制限」を選択します。
4. スタック・サイズを指定するには、「サイズ」を選択してテキスト・ボックスにキロバイトで値を指定します。また、スタック・サイズを無制限と指定するには、「無制限」を選択します。
5. ファイル・サイズ (512 バイトのブロック単位) を指定するには、「ファイル・サイズ」を選択してテキスト・ボックスに値を指定します。また、ファイル・サイズを無制限と指定するには、「無制限」を選択します。
6. 単一プロセスに属するファイル記述子の数を「オープン・ファイル記述子の数」テキスト・ボックスに入力します。
7. 「OK」または「適用」をクリックして、設定を有効にします。

コマンド・ラインの使用

ulimit オプション値は、ldapmodify コマンド行ユーティリティーを使用して変更できます。例えば、仮想メモリーの ulimit 値を変更するには、以下に示されているコマンドを発行します。

このタスクについて

```
ldapmodify-D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=ulimits, cn= configuration
changetype: modify
replace: ibm-slapdUlimitVirtualMemory
ibm-slapdUlimitVirtualMemory: <New prescribed ulimit for virtual memory>
```

同様に、ldapmodify コマンドを使用すると、データ・セグメント・サイズ、nofile、最大常駐セット・サイズ (rss)、ファイル・サイズ、およびスタック・サイズなど、その他の ulimit オプション値も変更できます。

検索設定

検索パラメーターを設定して、ページ化された検索やソートされた検索などのユーザー検索機能を制御できます。

ページ付け結果を使用して、検索要求から戻されるデータの量を管理できます。すべての結果を一度に受け取る代わりに、項目のサブセット (ページ) を要求できま

す。以降の検索要求では、操作が取り消されるか、または最後の結果が戻されるまで、次の結果ページが表示されます。ソートされた検索により、クライアントは、基準リスト (各基準はソート・キーを表します) でソートされた検索結果を受け取ることができます。これを選択すると、ソートの実行責任がクライアント・アプリケーションからサーバーに移動するため、より効率的にソートを実行できます。

オブジェクト・クラスが `alias` または `aliasObject` のディレクトリー項目には、ディレクトリー内の別の項目を参照するために使用される `aliasedObjectName` 属性が格納されています。検索要求でのみ、別名を参照解除するかどうかを指定できます。参照解除とは、元の項目まで別名を逆方向にトレースすることを指します。別名の参照解除オプションが「常時」または「検索」に設定されている検索での IBM Security Directory Server の応答時間は、参照解除オプションが「なし」に設定されている検索の場合より長くなる可能性があります。この応答時間は、ディレクトリー内に別名項目が存在する場合に問題となります。

サーバー・サイドの参照解除オプションには、「なし」、「検出」、「検索」、または「常時」を設定できます。このオプションの値は、検索要求で指定された遅延オプションの値と論理 AND 演算によって結合されます。結果の値は、検索操作の参照解除オプションとして使用されます。

検索設定を構成するには、以下の操作を実行します。

Web 管理の使用

Web 管理ツールを使用することにより、管理設定を検索することができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「サーバー・プロパティの管理」をクリックします。次に、「検索設定」タブをクリックします。

1. 「検索サイズ上限」で、「項目」または「無制限」ラジオ・ボタンをクリックします。「項目」を選択した場合は、1 回の検索で戻される項目の最大数をフィールドに必ず指定してください。デフォルトの設定は 500 です。この値より多くの項目が検索基準を満たす場合、超過分は戻されません。この制限は管理者または管理グループ・メンバーには適用されません。
2. 「検索時間制限」で、「秒」または「無制限」ラジオ・ボタンをクリックします。「秒」を選択する場合は、サーバーが要求の処理に消費する最大時間をこのフィールドに指定する必要があります。デフォルトの設定は 900 です。この制限は管理者または管理グループ・メンバーには適用されません。
3. 「別名の参照解除」で、「別名の参照解除」のドロップダウン・メニューを展開し、以下のいずれかのオプションを選択します。デフォルトの設定は「常時」です。

なし 別名の参照解除は一切実行されません

検出 検索の開始点を検出するときは別名を参照解除しますが、開始項目の下位項目を検索するときは参照解除しません。

検索 検索の開始点より下の項目を検索するときは別名を参照解除しますが、開始項目を検出しているときは参照解除しません。

常時 検索の開始点を検出するときにも、開始項目より下位の項目を検索するときにも、必ず別名を参照解除します。「常時」がデフォルトの設定です。

注: このオプションは、使用しているサーバーが別名の参照解除をサポートしている場合にのみ使用可能です。

4. 「**ページ検索設定**」で、以下の手順を実行します。
 - a. 検索結果のページング機能を管理者に制限するには、「**管理者にのみページ検索の実行を許可する**」チェック・ボックスを選択します。
 - b. 「**ページ検索のアイドル・タイムアウト (秒)**」フィールドで、ページ検索のアイドル・タイムアウトを秒単位で指定します。
 - c. 「**同時ページ検索の最大数**」フィールドで、サーバーによって許可される同時に処理可能な未処理のページ検索結果操作の最大数を指定します。デフォルト設定は **3** です。**注:** 値を **0** に設定すると、ページ検索が使用不可になります。
5. 「**ソート検索設定**」で、以下の手順を実行します。
 - a. 検索結果のソート機能を管理者に制限するには、「**管理者にのみソート検索の実行を許可する**」チェック・ボックスを選択します。
 - b. 「**ソート検索で使用できる最大属性数**」フィールドで、ソート検索で使用可能な属性の最大数を指定します。デフォルト設定は **3** です。**注:** 値を **0** に設定すると、ソート検索が使用不可になります。
6. 「**仮想リスト・ビュー検索**」で、以下の手順を実行します。
 - a. 仮想リスト・ビュー検索を有効または無効にするには、「**仮想リスト・ビュー検索を有効にする**」チェック・ボックスを選択またはクリアします。このコントロールは、cn=VirtualListView, cn=Configuration 項目の ibm-slapdVLVEnabled 属性に関連付けられます。**注:** 仮想リスト・ビューのサポートは、動的に使用可能または使用不可にすることができます。
 - b. 「**仮想リスト・ビュー検索のオフセット前の最大項目数**」フィールドに、各仮想リスト・ビュー検索で送信可能なオフセット前の最大項目数を指定します。このフィールドは、「cn=VirtualListView, cn=Configuration」項目の「ibm-slapdMaxVLVBeforeCount」属性に関連付けられています。

注: 仮想リスト・ビューについて詳しくは、130 ページの『仮想リスト・ビュー』を参照してください。
7. 「**永続検索**」で、以下の手順を実行します。
 - a. 「**永続検索を使用可能にする**」チェック・ボックスを選択して、永続検索を使用可能にします。
 - b. 「**同時永続検索の最大数 (最大 2000)**」フィールドに数値を入力して、許可する同時永続検索の最大数を指定します。

注: 永続検索について詳しくは、131 ページの『永続検索』を参照してください。
8. 完了したら、終了せずに変更を保存する場合は「**適用**」をクリックし、変更を適用して終了する場合は「**OK**」をクリックし、変更を行わずにこのパネルを終了するには「**キャンセル**」をクリックします。

検索の詳細については、『ページングとソートを使用したディレクトリーの検索』を参照してください。

コマンド・ラインの使用

以下に示すコマンドをコマンド行で使用することにより、同じ操作を実行できます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Configuration
changetype: modify
replace: ibm-slapdTimeLimit
ibm-slapdTimeLimit:900
-
replace : ibm-slapdDerefAliases
ibm-slapdDerefAliases: {never|find|search|always}
-
replace: ibm-slapdSizeLimit
ibm-slapdSizeLimit:500

dn: cn=Directory,cn=RDBM Backends,cn=IBM Directory,cn=Schemas,cn=Configuration
changetype: modify
replace: ibm-slapdPagedResAllowNonAdmin
ibm-slapdPagedResAllowNonAdmin: false
-
replace: ibm-slapdPagedResLmt
ibm-slapdPagedResLmt: 3
-
replace: ibm-slapdSortKeyLimit
ibm-slapdSortKeyLimit: 3
-
replace: ibm-slapdSortSrchAllowNonAdmin
ibm-slapdSortSrchAllowNonAdmin: false

dn: cn=Front End, cn=Configuration
changetype: modify
replace: ibm-slapdIdleTimeOut
ibm-slapdIdleTimeOut:300

dn: cn=VirtualListView, cn=Configuration
changetype: modify
replace: ibm-slapdVLVEnabled
ibm-slapdVLVEnabled: <value to be set as either true or false>
-
replace ibm-slapdMaxVLVBeforeCount
ibm-slapdMaxVLVBeforeCount: <value to be set in numerals>

dn: cn=Persistent Search, cn=Configuration
changetype: modify
replace: ibm-slapdEnablePersistentSearch
ibm-slapdEnablePersistentSearch: TRUE
-
replace: ibm-slapdMaxPersistentSearches
ibm-slapdMaxPersistentSearches: <value to be set in numerals>
```

設定を動的に更新するには、以下の **idsldapexop** コマンドを発行します。

```
idsldapexop -D <adminDN> -w<adminPW> -op readconfig -scope entire
```

コマンド行を使用した検索の実行方法について詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の **ldapsearch** コマンドの情報を参照してください。

ページングとソートを使用したディレクトリーの検索

検索機能は、属性の索引付けが使用可能な場合に、その属性の先頭 240 バイトのみに対してフィルターで一致するものを検索します。検索要求でソートを指定すると、サーバーは最初の 240 バイトだけを使用して、検索で検出された項目をソートします。

ユーザー・アプリケーションまたはクライアント・アプリケーションは、該当のテーブルに対する索引付けが有効になっているかどうかに応じて、先頭の 240 バイトよりも後の値内で検索フィルターに一致する項目が存在しても、その項目がクライアントに返されない場合があることを考慮に入れる必要があります。

注: この制限は、IBM Security Directory Server に固有の制限です。他のオペレーティング・システム上の IBM LDAP サーバー、z/OS®、i5/OS™ では、制約事項が異なる場合があります。制約事項については、各オペレーティング・システムの資料を参照してください。

管理者は、**Web 管理ツール** (「スキーマ管理」 > 「属性の管理」 > **属性名** > 「編集」 > 「**IBM 拡張**」) で属性の定義を調べるか、cn=schema の検索で返された属性の定義を調べることで、属性の索引付けが有効になっているかどうかを確認することができます。**Web 管理ツール**で属性定義を表示すると、**IBM 拡張タブ**に以下の規則が表示されます。

索引付け規則

同等性
順序付け
ほぼ等しい
サブストリング
反転

属性に対して該当する索引付け規則がチェックされます。**idsldapsearch** ユーティリティを使用する場合、**ibmattributetypes** 値には、キーワード APPROX、EQUALITY、ORDERING、SUBSTR、または REVERSE が入ります。例えば cn 属性には、以下の索引が定義されています。

```
attributetypes=( 2.5.4.3 NAME ( 'cn' 'commonName' ) DESC 'This is the X.500  
commonName attribute, which contains a name of an object.  
If the object corresponds to a person, it is typically the  
persons full name.' SUP 2.5.4.41 EQUALITY 2.5.13.2  
ORDERING 2.5.13.3 SUBSTR 2.5.13.4 )  
ibmattributetypes=( 2.5.4.3 DBNAME ( 'cn' 'cn' ) ACCESS-CLASS NORMAL LENGTH  
256 EQUALITY ORDERING SUBSTR APPROX )
```

50 ページの『索引付けの規則』を参照してください。

ソート済み検索制御

ソート済み検索制御を処理する場合は、以下の情報を参照してください。

ソート済み検索結果は、制限されたソート機能を持つ LDAP クライアントまたはソート機能を持っていない LDAP クライアントにソート機能を提供します。ソート済み検索結果によって、LDAP クライアントは、基準のリストに基づいてソートされた検索結果を受け取ることができます。ここで、各基準はソート・キーを表します。ソート基準には、属性タイプ、比較の規則、および降順があります。サーバーは、この基準を使用して検索結果をソートします。ユーザーは、このソート結果を返すこととなります。これにより、ソートの実行責任がクライアント・アプリケーションからサーバーに移動するため、サーバー上でより効率的にソートを実行できるようになります。例えば、クライアント・アプリケーションでケイマン諸島の支社にいる従業員のリストを名字、通称、および電話番号でソートすることもできます。この場合、ソートできるように検索リストが 2 回作成されるのではなく (最初にサーバー上で作成され、結果がすべて返されてからクライアント上でもう一度作成されるのではなく)、検索リストは 1 回だけ作成されます。その後、この検索リストがソートされます。ユーザーは、このソート結果をクライアント・アプリケーションに返すこととなります。

サーバーは、各属性に基づいて検索項目をソートします。デフォルトでは、1 回の検索操作について最大 3 つのソート・キー (属性名) を指定することができます。この管理制限の値を変更するには、`ibmslapd.conf` ファイルの以下の行を変更します。

```
ibm-slapdSortKeyLimit: 3
```

このアクションを実行する方法については、122 ページの『検索設定』を参照してください。この行が存在しない場合は、この行を追加して新しい最大値に設定してください。この行が存在しない場合、サーバーはデフォルト値を使用します。

デフォルトでは、サーバーは、匿名のバインドも含め、管理者以外のバインドからの要求を受け入れます。検索結果をソートしてから返すと、単純に結果を返す場合よりも多くのサーバー・リソースが使用されます。そのため、管理者権限がバインドされたユーザーからの要求だけを受け入れるようにサーバーを構成することをお勧めします。管理者のバインドだけを使用して実行依頼された検索結果のソート要求を受け入れるには、`ibmslapd.conf` ファイルの行 `ibm-slapdSortSrchAllowNonAdmin: true` を `ibm-slapdSortSrchAllowNonAdmin: false` に変更します。122 ページの『検索設定』を参照してください。この行が存在しない場合、この行を追加して値を `False` に設定すると、管理者のバインドだけをソート検索操作の対象にすることができます。

LDAP サーバーは、検索要求の終了時にすべての参照をクライアントに戻します。ソート検索要求の重要度を設定するかどうかは、クライアント・サービスを使用するアプリケーションで決定する必要があります。参照サーバーがこうした制御をサポートしていない場合は、クライアント・サービスを使用するアプリケーションで、アプリケーションに基づいた適切な処理を行う必要があります。さらに、LDAP サーバーは、参照サーバーがソート済み検索制御をサポートしていることを保証しません。一部がソートされていない複数のリストがクライアント・アプリケーションに返される場合があります。エンド・ユーザーに対してこの情報を表示する最適な方法は、クライアント・アプリケーションで決定する必要があります。考えられる解決策を以下に示します。

- すべての参照結果を結合してからユーザーに表示する。
- 複数のリストとそれに対応する参照サーバーのホスト名を表示する。
- 追加のステップを実行せずに、サーバーから返されたすべての結果をそのままユーザーに表示する。

正確にソートされたリストを 1 つだけ取得するには、クライアント・アプリケーションで参照をオフにする必要があります。オフにしないと、ソート済み検索制御を指定して参照を追跡した場合に、予期しない結果が発生する可能性があります。

サーバーのソート済み検索結果を使用する場合は、以下の点に注意する必要があります。

- サーバーは、基礎となる DB2 データベースを使用して検索結果をソートします。そのため、データベースのデータ・コード・ページによってソート後の検索結果が異なる場合があります (特に、データベースのコード・ページが UTF-8 の場合)。
- サーバーは、ソート・キー属性に対して指定された順序付け規則を無視します。現在、サーバーは順序付け規則をサポートしていません。

- マルチサーバーのソート (参照) はサポートされていません。サーバーは、参照サーバーでソート済み検索結果がサポートされるようにすることはできません。

サーバー・サイドでのソート済み検索制御については、RFC 2891 を参照してください。検索結果をソートするための制御 OID は 1.2.840.113556.1.4.473 であり、サポートされている機能としてルート DSE 情報に含まれています。

単純ページ付け結果

単純ページ付け結果を処理する場合は、以下の情報を参照してください。

単純ページ付け結果で提供されるページング機能によって、LDAP クライアントは、リスト全体ではなく、検索結果のサブセット (ページ) のみを受け取ることができます。各項目の次のページは、後続のページ付け結果検索要求ごとにクライアント・アプリケーションに返されます。この要求は、操作が取り消されるか最後の結果が返されるまで、クライアントによって送信されます。サーバーは、ページ・サイズがサーバーの `sizeLimit` 値以上の場合は要求を単一の操作で満たすことができるため、単純ページ付け結果要求を無視します。

検索結果のページングでは、単純ページ付け結果要求が存続する限りサーバー・リソースが保持されるため、単純ページ付け結果検索要求の使用によるサーバー・リソースの乱用や誤用を防ぐための新しい管理制限事項がいくつか導入されています。

`ibm-slapdPagedResAllowNonAdmin`

デフォルトでは、サーバーは、匿名のバインドも含め、管理者以外のバインドからの要求を受け入れます。管理者権限がバインドされたユーザーの単純ページ付け結果検索要求だけをサーバーで受け入れるには、`ibmslapd.conf` ファイルの以下の行を変更する必要があります。

```
ibm-slapdPagedResAllowNonAdmin: true to ibm-slapdPagedResAllowNonAdmin: false
```

122 ページの『検索設定』を参照してください。この行が存在しない場合に管理者のバインドのみを許可するには、この行を追加して値を `false` に設定します。

`ibm-slapdPagedResLmt`

デフォルトでは、サーバーで許可される未処理の単純ページ付け結果操作は常に最大 3 件です。以後のページ付け結果要求の応答を高速化するために、サーバーは、検索要求が行われている間、ユーザーが単純ページ付け結果要求を取り消すか最後の結果がクライアント・アプリケーションに戻されるまでデータベース接続をオープンしたままにします。この管理制限は、未処理の単純ページ付け結果検索要求によってすべてのデータベース接続が使用されていることが原因で、サーバーによって処理されている他の操作が拒否されたサービスにならないように設計されています。一貫性のある結果を得るには、`ibm-slapdPagedResLmt` に設定する値を、サーバーの最大データベース接続数より小さくします。この管理制限の値を変更するには、`ibmslapd.conf` ファイルの以下の行を変更します。

```
ibm-slapdPagedResLmt: 3
```

122 ページの『検索設定』を参照してください。この行が存在しない場合は、この行を追加して新しい最大値に設定してください (この行が存在しない場合、サーバーはデフォルト値を使用します)。

ibm-slapdIdleTimeOut

アイドル・タイムアウト管理制限は、単純ページ付け結果要求のためにオープンしたままにしている DB2 データベース接続のタイムアウトを管理するために設けられています。単純ページ付け結果要求に対するデフォルトのアイドル・タイムは 500 秒です。例えば、クライアント・アプリケーションがページとページの間で 510 秒間停止することになっている場合、サーバーは要求をタイムアウトにしてデータベース接続を解放します。解放されたデータベース接続は、他のサーバー操作で使用することができます。サーバーは、実行依頼された次の単純ページ付け結果要求について、該当するエラーをクライアント・アプリケーションに返します。この時点で、クライアント・アプリケーションは単純ページ付け結果要求を再開する必要があります。単純ページ付け結果要求それぞれに対するアイドル・タイマーは、クライアント・アプリケーションにページが戻されるごとにリセットされます。サーバーは、タイムアウトになった単純ページ付け結果要求を 5 秒ごとにチェックします。そのため、ibm-slapdIdleTimeOut の値を 5 秒未満に設定しても、単純ページ付け結果要求がタイムアウトになるまで 5 秒間待機する必要があります。この管理制限の値を変更するには、ibmslapd.conf ファイルの以下の行を変更します。

```
ibm-slapdIdleTimeOut: 300
```

122 ページの『検索設定』を参照してください。この行が存在しない場合は、この行を追加して新しい最大値に設定してください (この行が存在しない場合、サーバーはデフォルト値を使用します)。

LDAP サーバーは、検索要求が終了するとすべての参照をクライアントに戻します。これは制御なしで検索する場合と同じです。つまり、返された結果がサーバー上に 10 ページある場合は、各ページの最後ではなく 10 ページ目ですべての参照が返されます。参照を追跡する場合、クライアント・アプリケーションは Cookie をヌルに設定して、初期ページ付け結果要求を各参照サーバーに送信する必要があります。ページ付け結果のサポートの重要度を設定するかどうかは、クライアント・サービスを使用するアプリケーションで決定する必要があります。参照サーバーがこうした制御をサポートしていない場合は、クライアント・サービスを使用するアプリケーションで、アプリケーションに基づいた適切な処理を行う必要があります。さらに、LDAP サーバーは、参照サーバーがページ付け結果制御をサポートしていることを保証しません。一部がページングされていない複数のリストがクライアント・アプリケーションに返される場合があります。エンド・ユーザーに対してこの情報を表示する最適な方法は、クライアント・アプリケーションで決定する必要があります。考えられる解決策を以下に示します。

- すべての参照結果を結合してからユーザーに表示する。
- 複数のリストとそれに対応する参照サーバーのホスト名を表示する。
- 追加のステップを実行せずに、サーバーから返されたすべての結果をそのままユーザーに表示する。

正確にページングされたリストを 1 つだけ取得するには、クライアント・アプリケーションで参照をオフにする必要があります。オフにしないと、ページ付け結果検索制御を指定して参照を追跡した場合に、予期しない結果が発生する可能性があります。

サーバー・サイドでの単純ページ付け結果制御に関する詳細については、RFC 2686 を参照してください。単純ページ付け結果の制御 OID は 1.2.840.113556.1.4.319 です。これは、サポート対象の制御としてルート DSE 情報に含まれています。

バックエンド・サーバーでページングがサポートされている場合は、プロキシ・サーバーでもページ制御がサポートされ、プロキシ・サーバーのルート DSE に制御が登録されます。ただし、バックエンド・サーバーの `ibm-slapdPagedResAllowNonAdmin` と `ibm-slapdPagedResLmt` の値は、プロキシ・サーバーでは検証されません。管理者は、これらの値の同期を保つ必要があります。これら 2 つの属性の値が異なっていることが原因でバックエンド・サーバーから返されたエラーは、すべてエラーとみなされてクライアントに返されます。

仮想リスト・ビュー

仮想リスト・ビュー (VLV) は、多数の項目を持つ順序付けリストを表示する必要がある場合に使用できる GUI 技術です。VLV では、少数の項目が表示されるウィンドウを使用して、ソートされた大規模なデータ・セットのスクロール可能ビューが表示されます。

注: IBM Security Directory Server の VLV サポートは、以下のインターネット・ドラフトに従っています。

- Virtual List View extension for LDAP search operations (draft-ietf-ldapext-ldapv3-ylv-09.txt).
- Virtual List View extension for LDAP C API (draft-smith-ldap-c-api-ext-ylv-00.txt)

VLV 検索要求には、必要なターゲット項目を識別するための基準、ターゲット項目の前の項目数 (before count)、ターゲット項目の後の項目数 (after count) が含まれています。ターゲット項目は、以下の 2 つの方式のいずれかで VLV 要求制御に指定されます。

- オフセット・ベース: この方式では、ターゲット項目のリスト内のオフセットを指示することにより VLV 要求制御にターゲット項目を指定します。このリストとは、順序付けされた検索結果セットです。サーバーは、コンテンツ・カウント (クライアントによるリスト・カウントの推定値) とクライアントが指定したオフセットを検査し、コンテンツ・カウントに関するサーバー独自の理論に基づいて、リスト内の対応するオフセットを計算します。
 - オフセットの値が 1 であり、コンテンツ・カウントの値が 1 以外の場合は、そのターゲットがリスト内の最初の項目であることを示しています。
 - オフセットの値とコンテンツ・カウントの値が等しい場合は、そのターゲットがリスト内の最後の項目であることを示しています。
 - コンテンツ・カウントの値がゼロである場合は、サーバーが独自のコンテンツ・カウントの推定値を使用する必要があることを示しています。
- アサーション・ベース: この方式では、クライアントが属性のアサーション値を指定します。このアサーション値は、検索操作に付加されたソート制御の主ソート・キーとして指定された属性の値と比較されます。ターゲット項目は、指定された値より大か等しい値で、リストの最初の項目と特定されます。

注: アサーション・ベースの方式では、指定された条件を満たす項目が存在しないことがあります。その場合、ターゲット項目は存在しません。

電話帳内の名前を表示する必要がある場合を例に説明します。

Ari, Bob, Chris, David, John, Mike, Nancy, Peter, Rosy, Ted という 10 個の名前がアルファベット順に並んでいる電話帳があるとします。

ここで、以下のパラメーターで cn 属性のソートを指定するオフセット・ベースの VLV 検索要求を考えてみます。

```
offset=4
before count=1
after count=1
content count=0 (This means that the server must use its own content count estimate)
```

この場合、検索結果は以下のようになります。

Chris, David, John

次に、以下のパラメーターが指定されたアサーション・ベースの VLV 検索要求を考えてみます。

```
before count = 1
after count = 1
assertion = Jake
```

この場合、検索結果は以下のようになります。

David, John, Mike

注: Jake は存在しないため、ソート順の次の項目 (この場合は John) が索引項目になります。

VLV を有効にする方法については、『**検索設定**』のステップ 6 (6 (124 ページ)) を参照してください。

永続検索

永続検索を使用すると、LDAP サーバーに発生した変更に関する通知を LDAP クライアントが受信できるようになります。この永続検索のメカニズムは、すべてのユーザーで使用可能です。

ただし、戻される各項目に対して ACL チェックが実施されます。ユーザーは、アクセス権限がある項目または項目の一部のみを取得できます。また、トランザクションの一部であるディレクトリー・データの更新も永続検索によってレポートされます。永続検索メカニズムはすべてのユーザーに利用可能であるため、サーバーが処理する並行永続検索数を限定する必要があります。構成ファイル内で `ibm-slapdMaxPersistentSearches` オプションを設定する必要があります。

注: 永続検索は、サブツリー `cn=Deleted Objects` オブジェクトに対してはサポートされていません。

永続検索メカニズムでは項目を返し続けることが可能ですが、非管理ユーザーに適用される検索サイズおよび時間制限は、永続検索にも適用されます。サイズおよび時間制限は、返される項目が初期の突き合わせセットの一部であるか、更新された突き合わせセットの一部であるかに関係なく適用されます。例えば、サイズ制限が 500 で、450 の項目が初期の結果セットの一部として送信されている場合に、更新通知が 50 件になったら、永続検索は `LDAP_SIZELIMIT_EXCEEDED` エラーを返しま

す。同様に、時間制限が 10 秒である場合は、項目が初期の突き合わせセットと更新通知のいずれから返されたかに関係なく、10 秒後に LDAP_TIMELIMIT_EXCEEDED エラーが戻されます。

永続検索メカニズムがページングまたはソートと併用される場合、ページングまたはソートは初期の結果セットに対してのみ適用可能です。また、変更ログが使用可能に設定されている場合は、永続検索プラグインの前に変更ログ・プラグインを実行する必要があります。

注: IBM Security Directory Server は、ルート DSE 検索の場合に属性 `ibm-supportedcontrol` に対して OID 2.16.840.1.113730.3.4.3 を返します。

永続検索メカニズムのサポートのため、構成ファイルには以下の項目が追加されます。

```
dn: cn=Persistent Search, cn=Configuration
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdPersistentSearch
cn: Persistent Search
ibm-slapdEnablePersistentSearch:TRUE
ibm-slapdMaxPersistentSearches:100
```

`ibm-slapdEnablePersistentSearch` はブール型の属性であり、永続検索を使用可能にするかどうかを決定します。この属性には、TRUE または FALSE のいずれかの値を割り当てます。この属性のデフォルト値は TRUE です。属性

`ibm-slapdMaxPersistentSearches` は、同時に許可される永続検索の最大数を決定します。この属性のデフォルト値は 100 であり、許可される最大値は 2000 です。永続検索を使用可能にする方法については、『**検索設定**』のステップ 7 (124 ページ) を参照してください。

イベント通知

イベント通知機能により、サーバーは登録済みクライアントに、ディレクトリー・ツリーの項目の変更、追加、または削除を通知できます。この通知は、非送信請求メッセージの形式で実行されます。

イベントが発生すると、サーバーはクライアントに、メッセージを LDAP v3 非送信請求通知として送信します。messageID は 0 であり、メッセージの形式は拡張操作応答です。responseName フィールドは登録 OID に設定されます。応答フィールドには、固有の登録 ID とイベントの発生時刻を示すタイム・スタンプが設定されます。時刻フィールドは UTC 時刻形式です。

トランザクションが発生すると、そのトランザクション・ステップに対応するイベント通知は、トランザクション全体が完了するまで送信されません。

注: イベントが登録されると、イベントが登録された項目の ACL がチェックされます。アクセス項目の下の項目に対するアクセス権が付与されていないユーザーが、これらの項目の変更通知を受け取ることがあります。これらのユーザーには、正確な変更内容が通知されるわけではなく、変更が行われたということのみが通知されます。元の項目の ACL が変更されてユーザー・アクセスが許可されなくなった場合、ユーザーがアクセスできなくとも、登録されたイベントは残ります ACL の詳細については、546 ページの『**アクセス制御リスト**』を参照してください。

イベント通知について詳しくは、「*IBM Security Directory Server Version 6.3.1 Programming Reference*」を参照してください。

イベント通知の有効化

以下のいずれかの手順を使用することにより、イベント通知を使用可能にすることができます。

このタスクについて

Web 管理の使用:

Web 管理ツールを使用することにより、イベント通知を使用可能にすることができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「**サーバー管理**」をクリックしてから、展開されたリスト上で「**サーバー・プロパティの管理**」をクリックします。次に、「**イベント通知**」タブをクリックします。

1. 「**イベント通知を使用可能にする**」チェック・ボックスを選択してイベント通知を使用可能にします。「**イベント通知を使用可能にする**」が使用不可の場合は、サーバーは、このパネルの他のオプションをすべて無視します。
2. 「**接続ごとの最大登録数**」を設定します。「**登録**」または「**無制限**」ラジオ・ボタンをクリックします。「**登録**」を選択する場合は、このフィールドで接続ごとの最大登録数を必ず指定してください。最大登録数は 2,147,483,647 です。登録数のデフォルトの設定は 100 です。
3. 「**最大合計登録数**」を設定します。この選択項目は、サーバーで一度に可能な登録の数を設定します。「**登録**」または「**無制限**」ラジオ・ボタンをクリックします。「**登録**」を選択する場合は、このフィールドで接続ごとの最大登録数を必ず指定してください。最大登録数は 2,147,483,647 です。デフォルトの登録数は「**無制限**」です。
4. 完了したら、終了せずに変更を保存する場合は「**適用**」をクリックし、変更を適用して終了する場合は「**OK**」をクリックし、変更を行わずにこのパネルを終了するには「**キャンセル**」をクリックします。
5. イベント通知を使用可能にした場合は、変更した内容を有効にするために、サーバーを再始動する必要があります。設定のみを変更した場合は、サーバーを再始動する必要はありません。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、同じ操作を実行できます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Event Notification,cn=Configuration
changetype: modify
replace: ibm-slapdEnableEventNotification
ibm-slapdEnableEventNotification:TRUE
-
```

```
replace: ibm-slapdMaxEventsPerConnection
ibm-slapdMaxEventsPerConnection:100
-
replace: ibm-slapdMaxEventsTotal
ibm-slapdMaxEventsTotal:0
```

イベント通知を使用可能にした場合は、変更した内容を有効にするために、サーバーを再始動する必要があります。設定のみを変更した場合は、サーバーを再始動する必要はありません。

設定を動的に更新するには、以下の **idsldapexop** コマンドを発行します。

```
idsldapexop -D <adminDN> -w<adminPW> -op readconfig -scope entire
```

idsldapexop コマンドでは、これらの属性のうち動的に変更可能なもののみが更新されます。他の変更内容を有効にするには、サーバーを停止して再始動する必要があります。動的に更新可能な属性のリストについては、713 ページの『付録 L. 動的に変更される属性』を参照してください。

イベント通知の無効化

以下のいずれかの手順を使用することにより、イベント通知を使用不可にすることができます。

Web 管理の使用:

Web 管理ツールを使用することにより、イベント通知を使用不可にすることができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「**サーバー管理**」をクリックしてから、展開されたリスト上で「**サーバー・プロパティの管理**」をクリックします。次に、「**イベント通知**」タブをクリックします。

手順

1. 「**イベント通知を使用可能にする**」チェック・ボックスを選択解除して、トランザクション処理を使用可能にします。
2. 完了したら、終了せずに変更を保存する場合は「**適用**」をクリックし、変更を適用して終了する場合は「**OK**」をクリックし、変更を行わずにこのパネルを終了するには「**キャンセル**」をクリックします。
3. 変更した内容を有効にするには、サーバーを再始動する必要があります。

コマンド・ラインの使用:

コマンドを発行することにより、コマンド行を使用して同じ操作を実行することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Event Notification,cn=Configuration
changetype: modify
replace: ibm-slapdEnableEventNotification
ibm-slapdEnableEventNotification:FALSE
```

変更した内容を有効にするには、サーバーを再始動する必要があります。

トランザクション・サポート

トランザクション処理により、アプリケーションは、一連の項目の更新を 1 つの操作にグループ化できます。

通常、各個別 LDAP オペレーションは、データベース内の独立したトランザクションとして扱われます。操作のグループ化は、1 つの操作に失敗するとトランザクション全体が失敗するために 1 つの操作が別の操作に依存する場合に有用です。トランザクションの設定により、サーバー上で可能なトランザクション・アクティビティの制約が決定します。

トランザクション・サポートについて詳しくは、IBM Security Directory Server の資料の『プログラミング・リファレンス』セクションを参照してください。

トランザクション・サポートの有効化

以下のいずれかの手順を使用することにより、トランザクション・サポートを使用可能にすることができます。

このタスクについて

Web 管理の使用:

ここで説明する手順に従ってトランザクション・サポートを使用可能にするには、Web 管理ツールを使用します。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「サーバー・プロパティの管理」をクリックします。次に、「トランザクション」タブをクリックします。

1. 「トランザクション処理を使用可能にする」チェック・ボックスを選択して、トランザクション処理を使用可能にします。「トランザクション処理を使用可能にする」が使用不可の場合、サーバーは、このパネルの他のオプション（「トランザクションごとの最大操作数」や「保留時間制限」など）をすべて無視します。
2. 「トランザクションの最大数」を設定します。「トランザクション」または「無制限」ラジオ・ボタンをクリックします。「トランザクション」を選択した場合は、トランザクションの最大数をフィールドに指定する必要があります。トランザクションの最大数は 2,147,483,647 です。トランザクション数のデフォルトの設定は 20 です。
3. 「トランザクションごとの最大操作数」を設定します。「操作」または「無制限」ラジオ・ボタンをクリックします。「操作」を選択する場合は、このフィールドでトランザクションごとの最大操作数を必ず指定してください。トランザクション当たりの最大操作数は 500 です。数値が小さいほど、パフォーマンスは良くなります。デフォルトは 5 です。
4. 「準備からコミットまでの間のタイムアウト」で、「秒」または「無制限」のいずれかを選択します。「秒」を選択する場合、フィールドには、トランザクションの準備操作からコミット操作までの許可される最大秒数を指定する必要があります。

5. 「**保留時間制限**」を設定します。この選択項目では、保留中のトランザクションの最大タイムアウト値を秒単位で設定します。「秒」または「**無制限**」ラジオ・ボタンをクリックします。「秒」を選択する場合は、このフィールドでトランザクションごとの最長時間を秒単位で指定する必要があります。最大秒数は 2,147,483,647 です。これより長い時間経過しても完了しないトランザクションは取り消されます (ロールバックされます)。デフォルトは 300 秒です。
6. 完了したら、終了せずに変更を保存する場合は「**適用**」をクリックし、変更を適用して終了する場合は「**OK**」をクリックし、変更を行わずにこのパネルを終了するには「**キャンセル**」をクリックします。
7. トランザクション・サポートを使用可能にした場合、変更した内容を有効にするには、サーバーを再始動する必要があります。設定のみを変更した場合は、サーバーを再始動する必要はありません。

コマンド・ラインの使用:

以下のコマンドを発行することにより、コマンド行を使用して同じ操作を実行することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Transaction,cn=Configuration
changetype: modify
replace: ibm-slapdTransactionEnable
ibm-slapdTransactionEnable: TRUE
-
replace: ibm-slapdMaxNumOfTransactions
ibm-slapdMaxNumOfTransactions: 20
-
replace: ibm-slapdMaxOpPerTransaction
ibm-slapdMaxOpPerTransaction: 5
-
replace: ibm-slapdMaxTimeLimitOfTransactions
ibm-slapdMaxTimeLimitOfTransactions: 300
```

設定を動的に更新するには、以下の **idsldapexop** コマンドを発行します。

```
idsldapexop -D <adminDN> -w<adminPW> -op readconfig -scope entire
```

idsldapexop コマンドでは、これらの属性のうち動的に変更可能なもののみが更新されます。他の変更内容を有効にするには、サーバーを停止して再始動する必要があります。動的に更新可能な属性のリストについては、713 ページの『付録 L. 動的に変更される属性』を参照してください。

トランザクション・サポートの無効化

次のいずれかの手順を使用することにより、トランザクション処理を使用不可にすることができます。

このタスクについて

Web 管理の使用:

Web 管理ツールを使用することで、トランザクション・サポートを使用不可にすることができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「サーバー・プロパティの管理」をクリックします。次に、「トランザクション」タブをクリックします。

手順

1. 「トランザクション処理を使用可能にする」チェック・ボックスを選択解除して、トランザクション処理を無効にします。
2. 完了したら、終了せずに変更を保存する場合は「適用」をクリックし、変更を適用して終了する場合は「OK」をクリックし、変更を行わずにこのパネルを終了するには「キャンセル」をクリックします。
3. 変更した内容を有効にするには、サーバーを再始動する必要があります。

コマンド・ラインの使用:

以下のコマンドを発行することにより、コマンド行を使用して同じ操作を実行することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Transaction,cn=Configuration
changetype: modify
replace: ibm-slappedTransactionEnable
ibm-slappedTransactionEnable: False
```

変更した内容を有効にするには、サーバーを再始動する必要があります。

サフィックスの追加または除去

この機能では、サフィックスを追加したり除去したりできます。

サフィックスは、ローカルで保持されているディレクトリー階層の先頭の項目を識別する DN です。LDAP では相対命名方式が使用されているため、この DN は、その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・サーバーは、複数のサフィックスを持つことが可能です。各サフィックスは、ローカルで保持されているディレクトリー階層を識別します (o=sample など)。

注: サフィックスに一致する特定の項目は、当該ディレクトリーに追加する必要があります。

ディレクトリーに追加される項目は、DN の値 (例えば、ou=Marketing,o=sample) に一致するサフィックスを持っている必要があります。照会に含まれているサフィックスが、ローカル・データベースに対して構成されているいずれのサフィックスとも同じでない場合、この照会は、デフォルト参照で識別されている LDAP サーバーで参照されます。LDAP デフォルト参照を指定しない場合、戻される結果には、オブジェクトが存在しない旨が示されます。

サフィックスの作成または追加

以下に示す方法のいずれかを使用することで、サフィックスを作成したり追加したりできます。

このタスクについて

Web 管理の使用:

ここで説明する手順に従うことで、Web 管理ツールを使用してサフィックスを定義できます。

このタスクについて

注: cn=localhost、cn=Deleted Objects、cn=schema および cn=ibmpolicies などの定義済みのサフィックスは、追加または除去することはできません。したがって、これらのサフィックスはパネルには表示されません。

まだ行っていない場合は、Web 管理ナビゲーション領域の「**サーバー管理**」をクリックしてから、展開されたリスト上で「**サーバー・プロパティの管理**」をクリックします。次に、「**サフィックス**」タブをクリックします。

1. サフィックス DN を入力します (**c=Italy** など)。サフィックスの文字の最大数は 1000 です。
2. 「**追加**」をクリックします。
3. 追加するサフィックスの数だけこのプロセスを繰り返します。
4. 完了したら、終了せずに変更を保存する場合は「**適用**」をクリックし、変更を適用して終了する場合は「**OK**」をクリックし、変更を行わずにこのパネルを終了するには「**キャンセル**」をクリックします。

コマンド・ラインの使用:

以下のコマンドを発行することで、コマンド行を使用してサフィックスを追加できます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
DN: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
changetype: modify
add: ibm-slapdSuffix
ibm-slapdSuffix: <suffixname>
ibm-slapdSuffix: <suffix2>
ibm-slapdSuffix: <suffix3>
```

設定を動的に更新するには、以下の **idsldapexop** コマンドを発行します。

```
idsldapexop -D <adminDN> -w<adminPW> -op readconfig -scope single "cn=Directory,
cn=RDBM Backends,cn=IBM Directory,cn=Schemas,cn=Configuration" ibm-slapdSuffix
```

idscfgsuf コマンドを使用して、サフィックスを 1 つずつ追加することもできます。

```
idscfgsuf -I <instancename> -s <suffixname>
```

注:

- 詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の **idscfgsuf** コマンド情報を参照してください。
- 構成ユーティリティー **idsxcfg** を使用して、サフィックスの追加および除去を行うこともできます。詳細については、IBM Security Directory Server の資料の『インストールと構成』のセクションを参照してください。
- idscfgsuf または idsxcfg を使用してサフィックスを追加するには、サーバー・インスタンスを停止する必要があります。

サフィックスの除去

以下に示すいずれかの方法を使用して、サフィックスを除去することができます。

このタスクについて

Web 管理の使用:

以下に示す指示により、Web 管理ツールを使用してサフィックスを除去することができます。

このタスクについて

注: cn=localhost、cn=Deleted Objects、cn=schema および cn=ibmpolicies などの定義済みのサフィックスは、追加または除去することはできません。したがって、これらのサフィックスはパネルには表示されません。

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「サーバー・プロパティの管理」をクリックします。次に、「サフィックス」タブをクリックします。

手順

1. 「現在のサフィックス DN」リスト・ボックスから、除去するサフィックスを選択します。
2. 「除去」をクリックします。
3. 完了したら、終了せずに変更を保存する場合は「適用」をクリックし、変更を適用して終了する場合は「OK」をクリックし、変更を行わずにこのパネルを終了するには「キャンセル」をクリックします。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、同じ操作を実行できます。

このタスクについて

注: cn=localhost、cn=pwdpolicy、cn=schema および cn=ibmpolicies などのシステムで定義されたサフィックスの除去は、サポートされていません。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
DN: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
changetype: modify
delete: ibm-slapdSuffix
ibm-slapdSuffix: <suffixname>
ibm-slapdSuffix: <suffix2>
ibm-slapdSuffix: <suffix3>
```

変更した内容を有効にするには、サーバーを再始動する必要があります。

idsucfgsuf コマンドを使用して、サフィックスを 1 つずつ削除することもできます。

```
idsucfgsuf -I <instancename> -s <suffixname>
```

注:

- 詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の **idsucfgsuf** コマンド情報を参照してください。
- 構成ユーティリティー **idsxcfg** を使用して、サフィックスの追加および除去を行うこともできます。詳しくは、*IBM Security Directory Server* の資料の『インストールと構成』セクションを参照してください。
- **idsucfgsuf** または **idsxcfg** を使用してサフィックスを削除するには、サーバー・インスタンスを停止する必要があります。

トゥームストーンによる削除された項目の記録

IBM Security Directory Server には、トゥームストーン機能が組み込まれています。この機能により、削除される項目のすべての属性などの情報を、バックエンド・データベースからその項目が削除される前に、トゥームストーン・サブツリーに記録することができます。

ibm-slapdTombstoneEnabled=TRUE を設定してトゥームストーン機能を有効にする場合、削除項目の命名属性は以下の値を含む適切な長さになるようにしてください。

- 元の項目名
- トゥームストーン UUID を示す追加の文字

項目名を含む属性がトゥームストーンのタグに対応できるだけの十分な大きさでない場合、削除操作は戻り値 **LDAP_OBJECT_CLASS_VIOLATION** を返して失敗する可能性があります。

トゥームストーン機能を使用すると、削除対象項目をトゥームストーン・サブツリーに移動することができます (**cn=Deleted Objects**)。その後、その項目の属性テーブルが更新され、**isDeleted** などの属性が追加されて、削除済み項目としてマークが付けられます。

注:

- この機能は、ディレクトリー・サーバーのプライマリー RDBM バックエンドでのみサポートされます。
- トゥームストーンは、構成、スキーマ、または変更ログのバックエンドではサポートされていません。
- トゥームストーン機能は、デフォルトで使用不可に設定されています。

トゥームストーン機能は、**ibmslapd.conf** ファイルの項目 **cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configurationentry** の

ibm-slapdTombstoneEnabled 属性によって定義されます。また、構成ファイルの項目 cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration の ibm-slapdTombstoneLifetime 属性によって、トゥームストーンの有効期間が定義されます。トゥームストーンの有効期間により、削除項目の有効期間が決まります。デフォルト値は 7 日間です。

トゥームストーンを使用可能または使用不可に設定するには、以下のいずれかの方法を使用します。

Web 管理の使用

Web 管理ツールを使用してトゥームストーン機能を有効にするには、以下の手順を実行します。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「サーバー・プロパティの管理」をクリックします。「削除設定」タブをクリックします。

このパネルでは、トゥームストーン構成パラメーターを制御できます。このパネルは、1 次管理者またはサーバー構成グループのメンバーに対してのみ表示されます。

1. トゥームストーンを有効にするには、「削除された項目の記録」チェック・ボックスをクリックします。このコントロールは、ibm-slapdTombstoneEnabled 属性に関連付けられています。
2. 「削除された項目の有効期間」セクションで、トゥームストーンの有効期間の値を入力します。必要な値をフィールドから選択することにより、有効期間を日数または時間数で指定することができます。デフォルト値は 7 日です。このコントロールは、ibm-slapdTombstoneLifetime 属性に関連付けられています。

コマンド・ラインの使用

トゥームストーン機能を有効にするには、以下のコマンドを実行します。

このタスクについて

```
idsldapmodify -D <bindDN> -w <password> -f <file>
```

where <file> contains:

```
dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
ibm-slapdTombstoneEnabled: TRUE
```

構成ファイルを再読み取りするには、以下のコマンドを使用します。

```
idsldapexop -D <bindDN> -w <password> -op readconfig -scope entire
```

トゥームストーンの有効期間を設定するには、以下のコマンドを使用します。

```
idsldapmodify -D <bindDN> -w <password>
```

```
dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
ibm-slapdTombstoneLifetime: <value to be set in hours>
```

構成ファイルを再読み取りするには、以下のコマンドを使用します。

```
idsldapexop -D <bindDN> -w <password> -op readconfig -scope entire
```

ldapdelete ユーティリティーでパラメーター -L を使用すると、cn=Deleted オブジェクトの下の項目を削除できます。これには、最初に次のコマンドを発行して、cn=Deleted オブジェクトの下のすべてのトゥームストーンを表示します。

```
idsldapsearch -b "cn=Deleted Objects"-r -D <bindDN> -w <password> objectclass=* dn
```

次に、ldif ファイルに出力を保存し、ldapdelete コマンドへの入力としてその ldif ファイルを使用して次のコマンドを発行します。

```
idsldapdelete -c -L -f <file> -D <bindDN> -w <password>
```

キャッシュ・プロパティの管理

Web 管理 ツールを使用することで、項目キャッシュ、フィルター・キャッシュ、ACL キャッシュ、グループ・メンバー・キャッシュ、および属性キャッシュを構成できます。

Web 管理ナビゲーション領域の「**サーバー管理**」をクリックしてから、展開されたリスト上で「**キャッシュ・プロパティの管理**」をクリックします。このパネルには、キャッシュ・プロパティを管理する 5 つのタブがあります。

注: IBM Security Directory Server 6.3.1 リリース以降、属性キャッシュは非推奨になりました。今後は、属性キャッシュの使用を避けてください。

項目キャッシュ

以下に示す指示により、項目キャッシュを構成することができます。

このタスクについて

「項目キャッシュ」タブをクリックし、以下に示されたステップに従います。

Web 管理の使用:

以下に示す指示により、Web 管理ツールを使用して項目キャッシュを構成することができます。

このタスクについて

1. 「項目キャッシュの最大エレメント数」フィールドに、項目キャッシュに格納するエレメントの最大数を表す値を入力します。
2. 完了したら、以下のステップのいずれかを行います。
 - 「**OK**」をクリックして変更内容を保存し、このパネルを終了します。
 - 「**適用**」をクリックして変更内容を適用し、このパネルを表示させたままにします。
 - 「**キャンセル**」をクリックし、変更を行わずにこのパネルを終了します。

コマンド行の使用:

以下に示すコマンドを発行することにより、項目キャッシュを構成することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

```
where <filename> contains:
```

```
dn: cn=Front End, cn=Configuration
changetype: modify
replace: ibm-slapdEntryCacheSize
ibm-slapdEntryCacheSize: <value to be set in numerals>
```

フィルター・キャッシュ

以下に示す指示により、フィルター・キャッシュを構成することができます。

このタスクについて

フィルター・キャッシュを構成するには、「フィルター・キャッシュ」タブをクリックして、以下に示されたステップに従います。

Web 管理の使用:

以下に示す指示により、Web 管理ツールを使用してフィルター・キャッシュを構成することができます。

手順

1. 「検索フィルター・キャッシュの最大エレメント数」フィールドに、検索フィルター・キャッシュに格納するエレメントの最大数を表す値を入力します。
2. 単一の検索操作で検索フィルター・キャッシュに追加する最大エレメント数を指定します。「エレメント」を選択する場合は、フィールドに数値を入力してください。選択しない場合は「無制限」を選択します。
3. 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして変更内容を保存し、このパネルを終了します。
 - 「適用」をクリックして変更内容を適用し、このパネルを表示させたままにします。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

コマンド行の使用:

以下に示すコマンドを発行することにより、フィルター・キャッシュを構成することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
where <filename> contains:
dn: cn=Front End, cn=Configuration
changetype: modify
replace: ibm-slapdFilterCacheSize
ibm-slapdFilterCacheSize: <value to be set in numerals>
-
replace: ibm-slapdFilterCacheBypassLimit
ibm-slapdFilterCacheBypassLimit: <value to be set in numerals>
```

ACL キャッシュ

ACL キャッシュを構成するには、「ACL キャッシュ」タブをクリックして、以下の手順に従います。

このタスクについて

Web 管理の使用:

ここで説明する手順に従うことにより、Web 管理ツールを使用できます。

手順

1. 「キャッシュ ACL 情報」チェック・ボックスを選択し、ACL 情報のキャッシュを使用可能にします。
2. 「ACL キャッシュの最大エレメント数」フィールドに、ACL キャッシュに入れるエレメントの最大数を表す値を入力します。
3. 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして変更内容を保存し、このパネルを終了します。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

コマンド行の使用:

以下に示すコマンドをコマンド行で使用することにより、同じ操作を実行できます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
where <filename> contains:
dn: cn=Front End, cn=Configuration
changetype: modify
replace: ibm-slapdACLCache
ibm-slapdACLCache: TRUE
-
replace: ibm-slapdACLCacheSize
ibm-slapdACLCacheSize: <value to be set in numerals>
```

グループ・メンバー・キャッシュ

グループ・メンバー・キャッシュは、項目キャッシュの拡張です。このキャッシュには、メンバー値と固有のメンバー属性値が、それらの項目とともに格納されます。提供されるいずれかのタスクを使用して、グループ・メンバー・キャッシュを構成することができます。

このタスクについて

Web 管理の使用:

以下に示す指示により、Web 管理ツールを使用してグループ・メンバー・キャッシュを構成することができます。

このタスクについて

グループ・メンバーのキャッシュを構成するには、「グループ・メンバー・キャッシュ」タブをクリックして、以下に示されたステップに従います。

手順

1. 「キャッシュ内のグループの最大数」フィールドに、グループ・メンバーのキャッシュに入れるメンバーを持つグループの最大数を表す値を入力します。

2. 「キャッシュできるグループ内のメンバーの最大数」フィールドに、グループ・メンバーのキャッシュに入れるグループ内のメンバーの最大数を表す値を入力します。
3. 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして変更内容を保存し、このパネルを終了します。
 - 「適用」をクリックして変更内容を適用し、このパネルを表示させたままにします。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

コマンド行の使用:

以下に示すコマンドを発行することにより、グループ・メンバー・キャッシュを構成することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
where <filename> contains:

dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
changetype: modify
replace: ibm-slapdGroupMembersCacheSize
ibm-slapdGroupMembersCacheSize:25
-
replace: ibm-slapdGroupMembersCacheBypassLimit
ibm-slapdGroupMembersCacheBypassLimit: 50
```

属性キャッシュへの属性の追加と属性キャッシュからの属性の除去

属性キャッシュを使用することにより、データベース内ではなくメモリー内でフィルターを解決できます。キャッシュの使用には、LDAP の追加、削除、変更、または `modrdn` 操作を実行する度に、フィルター・キャッシュのようにフラッシュしない、という利点もあります。

注: IBM Security Directory Server 6.3.1 リリース以降、属性キャッシュは非推奨になりました。今後は、属性キャッシュの使用を避けてください。

メモリーに格納する属性を決定する場合は、以下の点を考慮する必要があります。

- サーバーで使用可能なメモリーのサイズ
- ディレクトリーのサイズ
- アプリケーションが通常使用する検索フィルターの種類

注: 属性キャッシュ・マネージャーは、完全一致突き合わせフィルターおよび存在フィルターの両方を解決できます。また、結合または分離である複合フィルターも解決できます。さらに、複合フィルター内のサブフィルターは、完全一致突き合わせ、存在、結合、または分離である必要があります。

すべての属性を属性キャッシュに追加できるわけではありません。属性をキャッシュに追加できるかどうかを調べるには、以下のように `ldapexop` コマンドを使用します。

追加できる属性の場合

```
ldapexop -D <adminDN> -w <adminPW> -op getattributes -attrType attribute_cache
-matches true
```

追加できない属性の場合:

```
ldapexop -D <adminDN> -w <adminPW> -op getattributes -attrType attribute_cache
-matches false
```

属性キャッシュは、手動または自動のいずれでも構成できます。属性キャッシュを手動で構成する場合、最初に管理者はキャッシュする属性を把握する必要があります。属性キャッシュを最も効果的なものにするため、管理者は `cn=monitor` 検索を実行する必要があります。この検索により、キャッシュされる属性、キャッシュ内の各属性で使用されるメモリー量、属性キャッシュで使用されるメモリー総量、属性キャッシュ用に構成されたメモリー量、および検索フィルターで最も頻繁に使用される属性のリストに関する情報が提供されます。管理者はこの情報を使用して、属性キャッシュに使用可能なメモリーの量、および必要に応じてキャッシュする属性を決定できます。

また、自動属性キャッシュを使用可能に設定した場合は、管理者によって、定義されたメモリーの制限内で、キャッシュが有効である属性の組み合わせがディレクトリー・サーバーによってトラッキングされます。サーバーは、管理者によって構成された時間間隔に従って、特定の時間に属性キャッシュを更新します。

通常は、メモリーの制約があるため、属性キャッシュに書き込む属性の数は制限することになります。キャッシュに格納する属性を決定しやすくするため、ディレクトリー・キャッシュ候補リストおよび変更ログ・キャッシュ候補リストを表示して、使用のアプリケーションによる使用頻度が高い属性検索フィルターの上位 10 種類を見つめます。88 ページの『サーバー状況の検査』を参照してください。詳細については、IBM Security Directory Server の資料の『パフォーマンス・チューニングとキャパシティー計画』セクションに記載されている『キャッシュに入れる属性の判別』も参照してください。

属性キャッシュに対する属性の設定および追加:

以下のいずれかの方法を使用することで、属性キャッシュに対して属性を設定および追加することができます。

このタスクについて

Web 管理の使用:

以下に示す情報を使用することで、Web 管理ツールを使用して属性を追加できます。

このタスクについて

- ディレクトリー・キャッシュに対して使用可能なメモリーのサイズをキロバイト単位で変更できます。デフォルトは、16384 キロバイト (16 MB) です。
- 変更ログ・キャッシュに対して使用可能なメモリーのサイズをキロバイト単位で変更できます。デフォルトは、16384 キロバイト (16 MB) です。

注: 変更ログを構成していない場合、この選択は使用できません。

手順

1. 「属性キャッシュ」タブをクリックし、以下に示す手順を実行します。
2. ディレクトリーの自動属性キャッシュを使用可能にするため、以下の手順を実行します。

- a. 「ディレクトリーの自動属性キャッシュを使用可能にする」チェック・ボックスを選択します。これにより、このグループ内のほかの要素が使用可能になります。
 - b. ディレクトリーの自動属性キャッシュの開始時刻を「開始時刻」テキスト・ボックスに入力します。
 - c. 「間隔」リストで、ディレクトリーの自動属性キャッシュの実行間隔を選択します。
3. 変更ログの自動属性キャッシュを使用可能にするため、以下の手順を実行します。
 - a. 「変更ログの自動属性キャッシュを使用可能にする」チェック・ボックスを選択します。これにより、このグループ内のほかの要素が使用可能になります。
 - b. 変更ログの自動属性キャッシュの開始時刻を「開始時刻」テキスト・ボックスに入力します。
 - c. 「間隔」リストで、変更ログの自動属性キャッシュの実行間隔を選択します。

注: 変更ログ内を頻繁に検索する必要があり、かつその検索のパフォーマンスが重要になる場合以外は、変更ログの自動属性キャッシュを使用可能に設定しないでください。

4. 属性を追加するため、以下の手順を実行します。
 - a. 「使用可能な属性」ドロップダウン・メニューから、キャッシュする属性を選択します。このメニューに表示されるのは、キャッシュ属性として指定可能な属性のみです。例えば、sn を選択します。**注:** 属性は、Directory コンテナと Changelog コンテナの両方に置かれるまで、使用可能な属性のリストに残ります。
 - b. 「データベースに追加」または「変更ログに追加」ボタンのいずれかをクリックします。属性は、該当するリスト・ボックスに表示されます。両方のコンテナに同じ属性を登録できます。
 - c. キャッシュに入れる個々の属性について、このプロセスを繰り返します。**注:** 属性を「データベースの下のキャッシュ属性」と「変更ログの下のキャッシュ属性」の両方のリスト・ボックスに追加すると、その属性はドロップダウン・リストから削除されます。changelog を使用不可にした場合、「変更ログに追加」ボタンは使用不可になり、「変更ログの下のキャッシュ属性」リスト・ボックスに項目を追加できなくなります。「データベースの下のキャッシュ属性」リスト・ボックスに属性を追加した場合、使用可能な属性のリストからその属性は削除されます。
 - d. 完了したら、終了せずに変更を保存する場合は「適用」をクリックし、変更を適用して終了する場合は「OK」をクリックし、変更を行わずにこのパネルを終了するには「キャンセル」をクリックします。

コマンド・ラインの使用:

以下に示すコマンドを発行することで、同じ属性を持つ複数のディレクトリー属性キャッシュを作成できます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
changetype: modify
add: ibm-slapdCachedAttribute
ibm-slapdCachedAttribute:sn
-
add: ibm-slapdCachedAttribute
ibm-slapdCachedAttribute:cn
-
replace: ibm-slapdcachedattributesize
ibm-slapdcachedattributesize: 16384
```

属性キャッシュからの属性の除去:

提供されているタスクのいずれかを使用して、属性キャッシュから属性を除去することができます。

このタスクについて

Web 管理の使用:

以下に示す指示により、Web 管理ツールを使用してタスクを実行することができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「キャッシュ・プロパティの管理」をクリックします。次に、「属性キャッシュ」タブをクリックします。

手順

1. 該当するリスト・ボックスで、属性キャッシュから除去する属性をクリックして選択します。例えば、前のタスクの AIXAdminGroupId などです。
2. 「除去」をクリックします。
3. リストから除去する属性ごとにこの処理を繰り返します。
4. 完了したら、終了せずに変更を保存する場合は「適用」をクリックし、変更を適用して終了する場合は「OK」をクリックし、変更を行わずにこのパネルを終了するには「キャンセル」をクリックします。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、同じ操作を実行できます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
DN: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
changetype: modify
delete: ibm-slapdCachedAttribute
ibm-slapdCachedAttribute:sn
```

DB2 のパスワード・モニター

DB2 のパスワード・モニター機能を使用することで、サーバー構成ファイル内の DB2 パスワード値を定期的にモニターするよう、サーバーを構成できます。この構成により、このパスワード値を使用することで、データベースとの接続が確立できるようになります。DB2 のパスワード・モニター機能は、構成ファイルからパスワードを取得し、それを使用してデータベースとの接続を試行します。

ディレクトリー・サーバー・インスタンスは、構成ファイルにあるデータベース所有者のパスワード情報を利用して、DB2 データベースとの接続を確立します。システム上のユーザーのパスワードが構成ファイル内の値と同期していないと、データベースへの接続に失敗します。

DB2 のパスワード・モニター機能では、システム上の DB2 ユーザーのパスワードのモニターが可能であり、そのパスワードがディレクトリー・サーバー・インスタンスで使用されているパスワードと整合していないことが検出された場合にアラートを出します。不整合が検出されると、ディレクトリー・サーバー・インスタンスのログ・ファイルにメッセージが書き込まれます。監査が有効になっている場合は、監査ログ・ファイルにもメッセージが書き込まれます。また、ディレクトリー・サーバー・インスタンスの実行中に、Web 管理ツールを使用して DB2 のパスワードを更新することもできます。

DB2 パスワードを更新する、または DB2 のパスワード・モニターを使用可能に設定するには、以下のいずれかの方法を使用します。

- Web 管理
- コマンド・ライン

Web 管理の使用

ここで説明する手順に従うことにより、Web 管理ツールを使用して、DB2 パスワードの更新と DB2 パスワード・モニターの使用可能化の両方を行うことができます。

このタスクについて

DB2 パスワードを更新する方法:

Web 管理ツールを使用して DB2 パスワードを更新できます。

このタスクについて

Web 管理ナビゲーション領域の「サーバー管理」をクリックし、展開されたリスト上で「DB2 インスタンス所有者」をクリックします (この操作をまだ実行していない場合)。このパネルには、DB2 インスタンス名および DB2 インスタンス所有者名が表示されます。このパネルで、以下の手順を実行して DB2 管理者のパスワードを変更します。

1. 「新規パスワード」フィールドに新規パスワードを入力します。
2. 「パスワードの確認」フィールドにパスワードを再入力します。
3. 変更内容を保存するには「パスワードの変更」をクリックします。変更を行わずに「概要」パネルに戻るには「キャンセル」をクリックします。

注: このパネルは、1 次管理者またはサーバー構成グループのメンバーに対してのみ表示されます。Web 管理ツールを使用して DB2 パスワードを更新する場合は、SSL の使用が推奨されます。

パスワード・モニターを使用可能に設定する方法:

ここで説明する手順を使用することで、パスワード・モニターを使用可能にすることができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「サーバー・プロパティの管理」をクリックします。「データベース」タブをクリックします。

このパネルを使用すると、DB2 のパスワード・モニターを使用可能に設定し、パスワード・モニターのレベルを設定できます。このパネルは、1 次管理者またはサーバー構成グループのメンバーに対してのみ表示されます。パスワード・モニター・レベルを設定するには、以下のステップを行います。

1. DB2 のパスワード・モニターを使用可能にするには、「**DB2 インスタンスのパスワード・モニターを有効にする**」チェック・ボックスをクリックします。
2. 「パスワード・モニター間隔 (最大 65535 分/45 日)」フィールドで、パスワードのモニター間隔を指定します。このフィールドのデフォルト値は 1 日です。
3. 「OK」ボタンをクリックします。

コマンド行の使用

以下のコマンドを発行して DB2 パスワードを更新することができます。

このタスクについて

```
ldapmodify -h <ldaphost> -p <ldap port> -D <bindDN> -w <password> -f <filename>
```

where filename contains:

```
dn:cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
changetype: modify
replace: ibm-slapdDbUserPw
ibm-slapdDbUserPw: <password value to be set>
```

readConfig 拡張操作を発行して、モニター機能で使用されているパスワードを更新します。これを行うには、以下のコマンドを実行します。

```
ldapexop -op readconfig -scope entire
```

DB2 のパスワード・モニターを使用可能にするには、以下のコマンドを使用します。

```
ldapmodify -h <ldaphost> -p <ldap port> -D <bindDN> -w <password> -f <filename>
```

where filename contains:

```
dn:cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
changetype: modify
replace: ibm-slapdDbPwMonIntervalMins
ibm-slapdDbPwMonIntervalMins: <value to be set in minutes>
```

注: ディレクトリー・サーバー・インスタンスは、デフォルトの 24 時間/1440 分、または構成ファイル内の属性 `ibm-slapdDbPwMonIntervalMins` によって指定された間隔で、定期的にモニターするように変更されます。 `ibm-slapdDbPwMonIntervalMins` 属性がゼロに設定されている場合、そのサーバーでモニターは実行されません。

ディレクトリー通信のセキュリティー

この情報に従って、ディレクトリー通信を保護します。

ディレクトリー内のデータを保護された状態に維持するために必要な以下の手順を使用できます。

セキュリティー設定の構成

この機能により、セキュリティー設定を構成することができます。

IBM Security Directory Server では、Secure Sockets Layer (SSL) セキュリティーまたは Transaction Layer Security (TLS) (あるいはその両方) を使用してデータを暗号化することにより、LDAP のアクセスを保護することができます。SSL または TLS により IBM Security Directory Server との LDAP 通信をセキュアにすると、サーバー認証およびクライアント認証の両方がサポートされます。詳細については、154 ページの『Secure Sockets Layer』および 154 ページの『Transaction Layer Security』を参照してください。

注: SSL または TLS を使用するには、システムに GSKit をインストールしておく必要があります。最初に GSKit を使用して鍵データベース・ファイルと証明書を作成しておかないと、SSL または TLS は使用できません。GSKit コマンド行ユーティリティーを使用して、Certificate Management Services (CMS) 鍵データベースを作成する方法については、163 ページの『gskcapicmd ツール』を参照してください。CMS または PKCS11 以外の鍵データベースを管理するには、167 ページの『iKeyman ツール』を参照してください。

Web 管理の使用

説明に従うことにより、Web 管理ツールで、セキュリティー設定を構成することができます。

このタスクについて

以下の手順を実行します。

手順

1. Web 管理コンソールに移動します。
2. 「サーバー管理」をクリックします。
3. 「セキュリティー・プロパティーの管理」をクリックします。
4. 「設定」をクリックします。
5. セキュリティー接続のタイプを使用可能にするには、以下のラジオ・ボタンのいずれかを選択します。

オプション	説明
なし	サーバーがクライアントから非セキュア通信のみを受信できるようにします。デフォルトのポートは、389 です。

オプション	説明
SSL	サーバーがクライアントからセキュア通信 (デフォルトのポートは 636) および非セキュア通信 (デフォルトのポートは 389) の両方を受信できるようにします。デフォルト・ポートは 636 です。
SSL のみ	サーバーがクライアントからセキュア通信のみを受信できるようにします。これは、サーバーを構成する際の最もセキュアな方法です。デフォルト・ポートは 636 です。
TLS	サーバーがデフォルトのポートである 389 を介して、クライアントからセキュア通信および非セキュア通信を受信できるようにします。セキュア通信の場合、クライアントは TLS 拡張操作を開始する必要があります。詳細については、154 ページの『Transaction Layer Security』を参照してください。
SSL および TLS	<p>サーバーがデフォルトのポートである 389 を介して、クライアントからセキュア通信および非セキュア通信を受信できるようにします。デフォルト・ポートでセキュア通信を行う場合、クライアントは TLS 拡張操作を開始する必要があります。サーバーは、SSL ポート 636 経由でもセキュア通信を受信します。詳細については、154 ページの『Transaction Layer Security』を参照してください。</p> <p>注:</p> <ul style="list-style-type: none"> • 「TLS オプション」と「SSL および TLS オプション」が使用できるのは、サーバーが TLS をサポートしている場合のみです。 • 「TLS」と「SSL」を同時に使用することはできません。セキュア・ポート経由で TLS 開始要求を送信すると、操作エラーが発生します。

6. 認証方法を選択します。 **注:** クライアントにサーバー証明書を配布する必要があります。サーバーおよびクライアント認証の場合は、各クライアント証明書をサーバーの鍵データベースに追加する必要があります。

オプション	説明
サーバー認証	<p>サーバー認証を行う場合、IBM Security Directory Server は、最初の SSL ハンドシェイク中に、クライアントに対して IBM Security Directory Server の X.509 証明書を提供します。クライアントがサーバーの証明書の妥当性検査を行うと、暗号化されたセキュアな通信チャネルが IBM Security Directory Server とクライアント・アプリケーションとの間に確立されます。</p> <p>サーバー認証を機能させるには、IBM Security Directory Server の鍵データベース・ファイル内に、秘密鍵および関連するサーバー証明書が必要です。</p>
サーバーおよびクライアントの認証	<p>このタイプの認証では、LDAP クライアントと LDAP サーバーとの間で、双方向の認証が提供されます。クライアント認証の場合、LDAP クライアントは、X.509 標準に基づいたデジタル証明書を持っている必要があります。このデジタル証明書は、IBM Security Directory Server に対して、LDAP クライアントを認証するために使用します。161 ページの『クライアント認証』を参照してください。</p>

7. 完了したら、終了せずに変更を保存する場合は「適用」をクリックし、変更を適用して終了する場合は「OK」をクリックし、変更を行わずにこのパネルを終了するには「キャンセル」をクリックします。
8. 変更内容を有効にするには、IBM Security Directory Server と管理サーバーの両方を停止して再始動する必要があります。
 - a. サーバーを停止します。このタスクの実行についての詳細が必要な場合は、86 ページの『サーバーの開始と停止』を参照してください。
 - b. 以下のいずれかの方法を使用して、管理サーバーを停止します。
 - リモート側で次のコマンドを発行します。 `ibmdirctl -D <adminDN> -w <adminPW> admstop`
 - ローカル側で次のコマンドを発行します。 `idsdiradm <instancename> -k`
このタスクの実行についての詳細が必要な場合は、14 ページの『ディレクトリー管理サーバーのインスタンスの停止』を参照してください。
 - c. 管理サーバーを始動します。これは、ローカル側で行う必要があります。
 - 次のコマンドを発行します。 `idsdiradm <instancename>`
このタスクの実行についての詳細が必要な場合は、14 ページの『ディレクトリー管理サーバーのインスタンスの始動』を参照してください。
 - d. サーバーを開始します。このタスクの実行についての詳細が必要な場合は、86 ページの『サーバーの開始と停止』を参照してください。

コマンド・ラインの使用

コマンド行でコマンドを使用することにより、セキュリティ設定を構成することができます。

このタスクについて

コマンド行を使用して SSL 通信を構成するには、以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSslAuth
ibm-slapdSslAuth: {serverAuth | serverClientAuth}
-
replace: ibm-slapdSecurity
ibm-slapdSecurity: {none | SSL | SS10nly | TLS | SSLTLS}
```

ユーザーは、鍵データベース・ファイルが使用されるインスタンス所有者のファイルに対する必要なアクセス権を提供する必要があります。また、変更した内容を有効にするには、サーバーおよび管理サーバーを再始動する必要があります。

Transaction Layer Security

Transaction Layer Security については、以下の情報を参照してください。

Transport Layer Security (TLS) は、クライアントとサーバー間の通信におけるプライバシーおよびデータ保全性を確保するプロトコルです。

TLS は次の 2 つの層で構成されています。

TLS Record Protocol

Data Encryption Standard (DES) や RC4 などのデータ暗号化方式を適用するか、または暗号化を適用せずに接続のセキュリティを提供します。この対称暗号化の鍵は、接続ごとに固有の鍵が生成されます。この鍵は、TLS Handshake Protocol によってネゴシエーションが行われる秘密鍵をベースとしています。 TLS Record Protocol は、暗号化なしでも使用できます。

TLS Handshake Protocol

このプロトコルでは、サーバーとクライアントが互いに認証し合い、データを交換する前に暗号化アルゴリズムと暗号鍵のネゴシエーションを実行できます。

TLS は、クライアントのユーティリティで -Y オプションを使用して起動されます。

注: TLS と SSL を同時に使用することはできません。SSL ポート経由で TLS の開始要求 (-Y オプション) を指定すると、操作エラーが発生します。

Secure Sockets Layer

SSL (Secure Sockets Layer) を処理する場合は、以下の情報を参照してください。

IBM Security Directory Server で SSL (Secure Sockets Layer) セキュリティを使用し、データを暗号化することにより、LDAP アクセスを保護することができます。

SSL を使用して IBM Security Directory Server との LDAP 通信を保護する場合、サーバー認証とクライアント認証の両方がサポートされます。

サーバー認証では、IBM Security Directory Server が X.509 規格に基づくデジタル証明書を持っている必要があります。このデジタル証明書を使用して、ディレクトリー管理ツールの `idsldapsearch` などのクライアント・アプリケーションや、アプリケーション開発パッケージを使用して作成されたアプリケーションに対して、SSL 経由の LDAP アクセス用に IBM Security Directory Server が認証されます。

サーバー認証の場合、IBM Security Directory Server は、最初の SSL ハンドシェイクの実行時に、IBM Security Directory Server の X.509 証明書をクライアントに提供します。クライアントがサーバーの証明書の妥当性検査を行うと、暗号化されたセキュアな通信チャネルが IBM Security Directory Server とクライアント・アプリケーションとの間に確立されます。

サーバー認証を機能させるには、IBM Security Directory Server の鍵データベース・ファイル内に、秘密鍵とそれに関連するサーバー証明書が含まれている必要があります。

クライアント認証では、LDAP クライアントと LDAP サーバーとの間で、双方向の認証が提供されます。

クライアント認証の場合、LDAP クライアントは、X.509 標準に基づいたデジタル証明書を持っている必要があります。このデジタル証明書は、IBM Security Directory Server に対して、LDAP クライアントを認証するために使用します。161 ページの『クライアント認証』を参照してください。

インターネット上でビジネスを行う場合は、VeriSign などのよく知られた認証局 (CA) を使用して、信頼性の高いサーバー証明書を取得することをお勧めします。

SSL によるサーバーのセキュリティー保護:

サーバー認証のために IBM Security Directory Server の SSL サポートを使用可能にする場合に必要となる、ハイレベルなステップの概要は以下のとおりです。

このタスクについて

これらのステップでは、IBM Security Directory Server がすでにインストールされ、構成されていることを前提にしています。

手順

1. IBM GSKit パッケージをインストールします (まだインストールしていない場合)。GSKit パッケージのインストールについては、IBM Security Directory Server の資料の『インストールと構成』のセクションを参照してください。

注:

- `GSKIT_LOCAL_INSTALL_MODE` 環境変数が `true` に設定されている場合、ユーザーは `LD_LIBRARY_PATH` に設定したパスに基づいて、自分で選択した GSKit バージョンを使用できます。この環境変数が設定されている場合は、`LD_LIBRARY_PATH`、`LIB`、または `LIBPATH` で設定されているパスを使用するライブラリーがロードされます。この環境変数が設定されていない場合は、

システムにインストールされている GSKit ライブラリー (例えば、UNIX ベースのシステムの場合は、`/usr/lib` または `/usr/lib64` など) がロードされます。この環境変数は、クライアント・サーバーでのみサポートされます。すべてのサーバー・サイドのラッパー・スクリプトは、この変数を明示的に割り当て解除します。

- `GSKIT_CLIENT_VERSION` 環境変数は、GSKit ライブラリーのメジャー・バージョンに設定されています。この環境変数を使用すると、ユーザーは、Security Directory Server で使用する GSKit ライブラリーのメジャー・バージョン番号に設定できます。メジャー・バージョン番号が変わると、GSKit ライブラリーの名前も変わります。例えば、GSKit 7 に付属の `ssl` ライブラリーの名前は `gsk7ssl` で、GSKit 8 に付属の `ssl` ライブラリーの名前は `gsk8ssl` です。この環境変数は、クライアント・サイドでのみサポートされます。すべてのサーバー・サイドのラッパー・スクリプトは、この変数を明示的に割り当て解除します。

2. **ikeyman** ユーティリティを使用して、IBM Security Directory Server 秘密鍵およびサーバー証明書を生成します。サーバーの証明書は、VeriSign などの商用 CA (commercial CA) から署名を受けることも、**ikeyman** ツールで自己署名することもできます。CA の公開証明書 (または自己署名証明書) は、クライアント・アプリケーションの鍵データベース・ファイルにも配布する必要があります。

注: Security Directory Server バージョン 6.3 には、GSKit バージョン 8 が提供されています。GSKit バージョン 8 では、`gskikm` ユーティリティは使用できません。

3. サーバーの鍵データベース・ファイルおよび関連付けられたパスワード `stash` ファイルをサーバーに保管します。通常、これらのファイルは、鍵データベースのデフォルト・パスである `instance_directory/etc` ディレクトリーに保管します。
4. Web ベースの LDAP 管理インターフェースにアクセスして、LDAP サーバーを構成します。手順については、151 ページの『Web 管理の使用』を参照してください。
5. マスター IBM Security Directory Server と 1 つ以上のレプリカ・サーバーとの間でもセキュア通信を確立する場合は、さらに以下のステップを実行する必要があります。
 - a. レプリカ・ディレクトリー・サーバーを構成します。マスターについては、上記のステップを実行しますが、各レプリカについては、このステップを実行しません。SSL を使用するようにレプリカを構成した場合、SSL 使用時のレプリカとマスターは、同等の役割を持ちます。レプリカと通信するときにマスターは、(SSL を使用する) LDAP クライアントになります。
 - b. マスター・ディレクトリー・サーバーを構成します。
 - 1) マスター・ディレクトリー・サーバーの鍵データベース・ファイルに、レプリカの署名されたサーバー証明書をトラステッド・ルートとして追加します。この場合、マスター・ディレクトリーは、実際の LDAP クライアントになります。自己署名証明書を使用する場合は、IBM Security Directory Server の各レプリカから自己署名証明書をすべて抽出し、それらをマスターの鍵データベースに追加して、トラステッド・ルートとしてマーク付けする必要があります。基本的にマスターは、レプリカ・サーバーの SSL クライアントとして構成します。

- 2) レプリカ・サーバーを認識するように、マスターの IBM Security Directory Server を構成します。IBM Security Directory Server のレプリカが SSL 通信で利用するポートを使用するには、replicaPort 属性を設定する必要があります。
- c. マスター・サーバーと各レプリカ・サーバーをともに再始動します。

注:

- a. 使用できる鍵データベースは、LDAP サーバー当たり 1 つのみです。
- b. ユーザーは、ファイルが使用されるインスタンス所有者の鍵データベース・ファイルに対する必要なアクセス権を提供する必要があります。
- c. 複製環境の SSL セットアップでは、SSL モードでの LDAP クライアントとの通信に、サプライヤーのフロントエンドで使用される kdb ファイル (cn=SSL, cn=Configuration の下) ではなく、サプライヤーとコンシューマーで別々の kdb ファイルを使用できます。
- d. プロキシ・サーバーの場合、バックエンド・サーバーとの SSL 通信にプロキシ・サーバーが構成されていると、サーバー構成ファイルで指定された同じ kdb ファイル (cn=SSL, cn=Configuration の下) が使用されます。

サーバー認証の設定:

ここで説明する方法により、サーバー認証を設定できます。

このタスクについて

サーバー認証用に、cn=SSL, cn=Configuration 項目の ibmslapd.conf ファイルを変更できます。Web 管理ツールを使用するには、151 ページの『Web 管理の使用』を参照してください。

コマンド行を使用するには、以下を行います。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSSLAuth
ibm-slapdSSLAuth: serverAuth
```

変更した内容を有効にするには、サーバーおよび管理サーバーを再始動する必要があります。

外部認証局 (CA) からのサーバー証明書:

ここで説明する手順を実行して、外部認証局 (CA) のサーバー証明書を保護することができます。

このタスクについて

IBM Security Directory Server とそのクライアントとの間でセキュア接続を確立するには、サーバーが X.509 証明書と秘密鍵を持っている必要があります。

以下のステップは、秘密鍵を生成し、必要なサーバー証明書を外部の CA から取得して IBM Security Directory Server で使用できるようにするためのステップです。

手順

1. 管理者またはルートとしてログオンします。**注:** サーバーの構成プロセスで作成した管理者 DN が `cn=root` の場合、省略せずに完全な管理者 DN を入力します。`root` のみを入力しないよう注意してください。
2. 鍵データベース・ファイルを作成するディレクトリーに移動します。このディレクトリーは、秘密鍵および証明書を保管するディレクトリーでもあります。
3. **ikeyman** を実行し、新規の鍵データベース・ファイルを作成します。鍵データベース・ファイルの名前には、有効であれば、任意の値を指定できます。どのようなファイル名を付けても、SSL を使用するよう LDAP サーバーを構成するときに、そのファイル名を指定する必要があります。絶対パス名を指定する必要がありますことに注意してください。秘密鍵と公開鍵のペアおよび認証要求を生成するときは、**ikeyman** ユーティリティーを使用します。追加情報については、167 ページの『iKeyman ツール』を参照してください。**注:** デフォルトでは、GSKit で作成された新しい KDB をサーバーで読み取ることはできません。所有者を `idsldap.chown idsldap:idsldap <mykeyring>.*` に変更する必要があります。Kerberos サービス名の変更については、IBM Security Directory Server の資料の『トラブルシューティングとサポート』セクションを参照してください。
4. VeriSign を外部 CA として使用している場合は、以下のようにして VeriSign から証明書を取得します。
 - a. VeriSign Web サイトの <http://www.verisign.com/server/index.html> にアクセスします。
 - b. 「**IBM Internet Connection Server**」をクリックします。
 - c. このサイトの情報を確認したら、「**開始**」をクリックします。
 - d. 必要な情報を提供し、必要なステップに従って、ユーザーのサーバー証明書を要求します。VeriSign は、外部で生成された高保証サーバー証明書を取得するためにサポートされる、主要な認証局です。
5. 他の CA を使用する場合は、その CA の指示に従って、認証要求ファイルの内容を提出します。

タスクの結果

作成された証明書を CA から受け取るには、以下の手順を実行します。

1. ユーザーのサーバー ID を使用してログオンします。
2. 鍵データベース・ファイルを作成したディレクトリーに移動します。
3. CA からの署名付き証明書をこのディレクトリーのファイルに格納します。このファイルは、次のステップで使用されます。
4. 同じディレクトリーから **ikeyman** を実行し、証明書を鍵データベース・ファイル内に取り込みます。
5. LDAP サーバーの Web 管理インターフェースにアクセスし、鍵データベース・ファイルのファイル仕様も含めて各種の SSL パラメーターを構成します。151 ページの『Web 管理の使用』を参照してください。
6. 鍵データベース・ファイルに複数の証明書がある場合は、IBM Security Directory Server で使用する証明書をデフォルトに設定する必要があります。
7. IBM Security Directory Server を始動します。

注: パスワードをパスワード stash ファイル内に保存するように **ikeyman** に指示した場合は、ibmslapd.conf ファイル内のパスワードを変更または設定する必要はありません。

自己署名サーバー証明書の使用:

ここで説明する手順に従い、自己署名証明書を使用して鍵データベース・ファイルを作成することができます。

このタスクについて

イントラネット環境で IBM Security Directory Server を使用している場合は、**ikeyman** を使用して、ユーザー自身のサーバー証明書を作成します。**ikeyman** を使用すると、VeriSign の高保証サーバー証明書を購入しなくても、SSL を使用する IBM Security Directory Server をテストすることもできます。このタイプの証明書は、自己署名証明書と呼ばれます。

1. 各サーバー上では、以下を実行します。
 - a. 鍵データベース・ファイルを作成するディレクトリーに移動します。このディレクトリーは、秘密鍵および証明書を保管するディレクトリーでもあります。
 - b. 新規の鍵データベース・ファイル、および CA 証明書として使用される自己署名証明書要求を作成します。
 - 使用可能な最大鍵サイズを使用します。
 - 低保証の証明書ではなく、セキュア・サーバー証明書を使用します。
 - c. 認証要求ファイルを取得します。この証明書は **ikeyman** ツールにより、自動的に鍵データベース・ファイルに取り込まれます。
2. クライアント用に作成されたアプリケーションを使用している場合は、各クライアント・マシン上で以下のステップを実行します。
 - a. CA 証明書要求ファイルをクライアント・マシン上のアクセス可能な場所に配置します。
 - b. CA 証明書要求ファイルをクライアントの鍵データベースに取り込みます。
 - c. 取り込んだ証明書要求ファイルをトラステッド・ルートとしてマーク付けします。

詳細については、167 ページの『iKeyman ツール』を参照してください。

注:

1. サーバー証明書をサーバーの鍵データベース・ファイルに取り込むときは、事前に CA 証明書をサーバーの鍵データベース・ファイルに取り込み、それをトラステッド・ルートとしてマーク付けしておく必要があります。
2. **ikeyman** を使用して IBM Security Directory Server の鍵データベース・ファイルを管理するときは、必ずその鍵データベース・ファイルが入っているディレクトリーに移動するようにしてください。
3. IBM Security Directory Server は、それぞれ独自の秘密鍵と証明書を持っている必要があります。複数の IBM Security Directory Server が、同じ秘密鍵と証明書を使用していると、セキュリティー上のリスクが高くなります。サーバーのい

れかの鍵データベース・ファイルが危険にさらされた場合でも、各サーバーごとに異なる証明書と秘密鍵を使用していれば、機密漏れを最小限にとどめることができます。

IBM Security Directory Server にアクセスするための LDAP クライアントの設定 :

LDAP クライアントの中には、1 つ以上の自己署名サーバー証明書を持ち、それがクライアントによって「トラステッド」とマーク付けされているものがあります。以下で説明するステップを使用して、そうした LDAP クライアントの鍵データベース・ファイルを作成することができます。

このタスクについて

このプロセスを使用すると、トラステッド・ルートとして使用するクライアントの鍵データベース・ファイルに、他のソース、VeriSign などからの CA 証明書をインポートすることもできます。トラステッド・ルートとは、信用できるエンティティ (VeriSign や自己署名サーバー証明書の作成者など) が署名した X.509 証明書のことです。トラステッド・ルートは、クライアントの鍵データベース・ファイルにインポートされ、トラステッドとしてマーク付けされます。

1. サーバーの証明書ファイル (cert.arm) をクライアント・ワークステーションにコピーします。
2. **ikeman** を実行し、新規クライアント鍵データベース・ファイルを作成するか既存のクライアント鍵データベース・ファイルにアクセスします。新しいクライアント鍵データベースについては、管理を容易にするために、クライアントと関連したファイル名を選択してください。例えば、LDAP クライアントが Fred のマシン上で実行されている場合は、ファイル名を FRED.KDB のように選択します。
3. サーバーの証明書を既存のクライアント鍵データベースに追加するには、以下を実行します。
 - a. 「**鍵データベース・ファイル**」をクリックし、「**開く**」をクリックします。
 - b. 既存の鍵データベース・ファイルのパスおよび名前を入力し、「**OK**」をクリックします。
 - c. パスワードを入力します。
 - d. 「**署名者証明書を確認 (Ensure signer certificates)**」が選択されています。「**追加**」をクリックします。
 - e. サーバーの証明書ファイルの名前および場所を入力します。
 - f. サーバー証明書項目のラベル (Corporate Directory Server など) を、クライアントの鍵データベース・ファイルに入力し、「**OK**」をクリックします。
4. 新しいクライアント鍵データベースを作成するには、以下を実行します。
 - a. 「**鍵データベース・ファイル**」をクリックし、「**新規 (New)**」をクリックします。
 - b. 新しいクライアント鍵データベースの名前と場所を入力し、「**OK**」をクリックします。
 - c. パスワードを入力します。

- d. 新しいクライアント鍵データベースが作成されたら、上記の (サーバーの証明書を既存の鍵データベース・ファイルに追加する) ステップを繰り返します。

5. **ikeyman** を終了します。

詳細については、167 ページの『iKeyman ツール』を参照してください。

LDAP クライアントとサーバーとの間にセキュア SSL 接続が確立されると、LDAP クライアントは、サーバーの自己署名証明書を使用して、接続先のサーバーが正しいことを確認します。

LDAP クライアントがセキュアに接続する必要がある IBM Security Directory Server ごとに、上記のステップを繰り返します。

鍵データベース・ファイルへの鍵リング・ファイルのマイグレーション:

以下に示す指示により、MKKF ユーティリティーで作成された古い鍵リング・ファイルをマイグレーションすることができます。

このタスクについて

1. **ikeyman** を始動します。
2. 「**鍵データベース・ファイル**」をクリックし、「**開く**」をクリックします。
3. 鍵リング・ファイルのパスおよびファイル名を入力し、「**OK**」をクリックします。
4. 鍵リング・ファイルのパスワードを入力します。パスワードを指定せずに鍵リング・ファイルを作成した場合は、古い MKKF を使用して、このファイルに必ずパスワードを割り当てる必要があります。
5. 古い鍵リング・ファイルを開いたら、「**鍵データベース・ファイル**」をクリックし、「**名前を付けて保存**」を選択します。
6. 鍵データベースのタイプが **CMS 鍵データベース・ファイル**に設定されていることを確認します。鍵データベース・ファイルの名前と場所を入力し、「**OK**」をクリックします。

クライアント認証:

この機能により、クライアント認証を取得することができます。

クライアント認証では、LDAP クライアントと LDAP サーバーとの間で、双方向の認証が提供されます。

クライアント認証の場合、LDAP クライアントは、X.509 標準に基づいたデジタル証明書を持っている必要があります。このデジタル証明書は、IBM Security Directory Server に対して、LDAP クライアントを認証するために使用します。

Simple Authentication and Security Layer (SASL) を使用すると、接続プロトコルに認証サポートを追加することができます。プロトコルには、サーバーに対してユーザーを識別および認証するためのコマンドが含まれています。SASL は、必要に応じて、後続のプロトコル対話用のセキュリティー・レイヤーをネゴシエーションできます。

サーバーは、認証コマンドまたはクライアント応答を受け取ると、ユーザー確認のための質問を発行するか、あるいは、障害の発生もしくは処理の完了を知らせます。クライアントは、ユーザー確認のための質問を受け取ると、プロトコルのプロファイルに応じて、応答を発行したり、交換を終了したりします。

認証プロトコルの交換時に、SASL メカニズムは認証を実行し、クライアントからサーバーに許可 ID (userid と呼ばれる) を送信して、メカニズム固有のセキュリティ・レイヤーの使用をネゴシエーションします。

LDAP サーバーは、クライアントから LDAP バインド要求を受け取ると、以下の順序でその要求を処理します。

1. サーバーは LDAP バインド要求を構文解析して、以下の情報を検索します。
 - クライアントが認証を試みる際の DN。
 - 使用する認証方式。
 - 資格情報 (要求に含まれるパスワードなど)。
 - 認証方式が SASL の場合、サーバーは、使用する SASL メカニズムの名前も LDAP バインド要求から検索します。
2. サーバーは、要求から検索した DN を正規化します。
3. サーバーは、LDAP バインド要求に含まれる LDAP コントロールを検索します。
4. 認証方式が SASL の場合、サーバーは、(要求で指定された) SASL メカニズムがサポートされているかどうかを判別します。その SASL メカニズムがサポートされていない場合、サーバーは、クライアントにエラー戻りコードを送り、バインド処理を終了します。
5. SASL メカニズムがサポートされており (=EXTERNAL)、SSL 認証タイプがサーバーおよびクライアントの認証の場合、サーバーは、既知の CA から発行されたクライアント証明書が有効であるかどうかを検査するとともに、クライアントの証明書チェーン上の証明書に無効なものや取り消されたものがないかも検査します。ldap_sasl_bind で指定されたクライアント DN およびパスワードが NULL の場合は、クライアントの x.509v3 証明書に入っている DN が、後続の LDAP 操作に対する認証された ID として使用されます。それ以外の場合、クライアントは、無名で認証されるか (DN およびパスワードが NULL の場合)、またはそのクライアントが提供したバインド情報に基づいて認証されます。
6. 認証方式が単純認証の場合、サーバーは、DN が空ストリングであるかどうか、または資格情報がないかどうかを検査します。
7. DN が空ストリングの場合、または、DN も資格情報も指定されていない場合、サーバーは、クライアントが無名でバインドしているものと見なし、そのクライアントに有効な結果を戻します。接続用の DN および認証方式は、それぞれ NULL および LDAP_AUTH_NONE のまま変わりません。
8. クライアントがまだバインドされておらず、バインド操作中に証明書が存在しない場合は、接続は拒否されます。

クライアント認証の設定:

以下に示すコマンドをコマンド行で使用することにより、クライアント認証の設定を実行できます。

このタスクについて

クライアント認証用に、`cn=SSL, cn=Configuration` 項目の `ibmslapd.conf` ファイルを変更できます。Web 管理ツールを使用するには、151 ページの『Web 管理の使用』を参照してください。

コマンド行を使用するには、以下を行います。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=SSL,cn=Configuration
cn: SSL
changetype: modify
replace: ibm-slapdSSLAUTH
ibm-slapdSSLAUTH: serverClientAuth
```

変更した内容を有効にするには、サーバーおよび管理サーバーを再始動する必要があります。

gskcapiCmd ツール

GSKCapiCmd は、CMS 鍵データベース内で鍵、証明書、および証明要求を管理するために使用できるツールです。**GSKCapiCmd** は、CMS 鍵データベースおよび PKCS11 鍵データベースをサポートします。

CMS と PKCS11 以外の鍵データベースを管理する場合は、Java ツールである **ikeyman** を使用する必要があります。**GSKCapiCmd** は、CMS 鍵データベースのすべての側面を管理するために使用できます。**GSKCapiCmd** を使用する場合、Java がシステムにインストールされている必要はありません。**GSKit** ツール **GSKCapiCmd** については、「**GSKCapiCmd User's Guide**」を参照してください。

LDAP サーバーと C ベースの LDAP クライアントとの間のサーバー認証またはサーバー・クライアント認証をサポートするための CMS 鍵データベースを作成するには、**GSKCapiCmd** ツールを使用します。この例では、LDAP サーバーと C ベースの LDAP クライアントとの間のサーバー認証およびサーバー・クライアント認証は、自己署名証明書を使用して実行されます。

注: 32 ビットのプラットフォームでは **gsk8capiCmd** ユーティリティを、64 ビットのプラットフォームでは **gskcapiCmd** ユーティリティを使用します。

CMS 鍵データベースを使用したサーバー認証の構成

LDAP サーバーと C ベースの LDAP クライアントとの間のサーバー認証をセットアップするには、以下のタスクを実行します。

LDAP サーバー・システム上

serverkey.kdb

1. 鍵データベース・ファイルを作成して格納するディレクトリーを IBM Security Directory Server システム上に作成し、その作業ディレクトリーに移動します。
2. IBM Security Directory Server が使用する CMS 鍵データベースを作成します。

```
gskcapiCmd -keydb -create -db serverkey.kdb -pw serverpwd -stash
```

ここで、*serverkey.kdb* は作成する鍵データベースで、*serverpwd* はパスワードです。

3. デフォルトの自己署名証明書を作成して、*serverkey.kdb* 鍵データベースに追加します。

```
gsk8capicmd -cert -create -db serverkey.kdb -pw serverpwd ¥  
-label serverlabel -dn "cn=LDAP_Server,o=sample" -default_cert yes
```

ここで、*-dn* 値は、証明書を一意的に識別するために使用されま
す。

4. 鍵データベースから証明書をバイナリー *der* 形式でファイルに抽出します。この例では、証明書はバイナリー *der* 形式でファイルに抽出されます。

注: 証明書は、base64 エンコードの ASCII データ形式 (*.arm*) で抽出することもできます。

```
gsk8capicmd -cert -extract -db serverkey.kdb -pw serverpwd ¥  
-label serverlabel -target server.der -format binary
```

5. 構成ファイル内で、証明書を使用するように IBM Security Directory Server インスタンスを構成します。

```
idsldapmodify -h server.in.ibm.com -p 389 -D cn=root -w root ¥  
-i /home/dsrdbm01/serverauth.ldif
```

serverauth.ldif ファイルには、以下の形式のコードが記述されています。

```
dn: cn=SSL, cn=Configuration  
changetype: modify  
replace: ibm-slapdSslAuth  
ibm-slapdSslAuth: serverAuth  
  
dn: cn=SSL, cn=Configuration  
changetype: modify  
replace: ibm-slapdSecurity  
ibm-slapdSecurity: SSL  
  
dn: cn=SSL, cn=Configuration  
changetype: modify  
replace: ibm-slapdSslKeyDatabase  
ibm-slapdSslKeyDatabase: /home/dsrdbm01/keys/serverkey.kdb  
  
dn: cn=SSL, cn=Configuration  
changetype: modify  
replace: ibm-slapdSslCertificate  
ibm-slapdSslCertificate: serverlabel  
  
dn: cn=SSL, cn=Configuration  
changetype: modify  
replace: ibm-slapdSslKeyDatabasepw  
ibm-slapdSslKeyDatabasepw: serverpwd
```

6. 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します。

```
ibmslapd -I dsrdbm01 -k  
ibmdiradm -I dsrdbm01 -k
```

7. 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始動します。

```
ibmslapd -I dsrdbm01 -n -t  
ibmdiradm -I dsrdbm01 -t
```

C ベースの LDAP クライアント・システム上

1. LDAP クライアント・システム上で、鍵データベース・ファイルを格納するディレクトリーを作成して、その作業ディレクトリーに移動します。
2. C ベースの LDAP クライアントが使用する CMS 鍵データベース・ファイルを作成します。

```
gsk8capicmd -keydb -create -db clientkey.kdb -pw clientpwd
```

- 抽出されたサーバー証明書 (server.der) をサーバー・システムからクライアント・システムにインポートします。
- 抽出されたサーバー証明書をクライアントの鍵データベース・ファイルに追加します。

```
gsk8capicmd -cert -add -db clientkey.kdb -pw clientpwd ¥
-label serverlabel -file server.der -format binary
```

- 追加された証明書を検証するには、以下のコマンドを実行します。

```
gsk8capicmd -cert -list -db clientkey.kdb -pw clientpwd
```

LDAP クライアントと LDAP サーバー間の SSL 通信を検証するには、以下の形式の **idsldapsearch** コマンドを実行します。

```
idsldapsearch -Z -h server.in.ibm.com -p 636 -K /usr/client/clientkey.kdb ¥
-P clientpwd -s base -b "o=sample" objectclass=*
o=sample
objectclass=top
objectclass=organization
o=sample
```

CMS 鍵データベースを使用したサーバー・クライアント認証の構成

LDAP サーバーと C ベースの LDAP クライアントとの間でサーバー・クライアント認証をセットアップするには、以下のタスクを実行します。

C ベースの LDAP クライアント・システム上

- 鍵データベース・ファイルを格納するディレクトリを作成して、その作業ディレクトリに移動します。
- C ベースの LDAP クライアントが使用する CMS 鍵データベース・ファイルを作成します。

```
gsk8capicmd -keydb -create -db clientkey.kdb -pw clientpwd
```

ここで、*clientkey.kdb* は作成する鍵データベースで、*clientpwd* はパスワードです。

- デフォルトの自己署名証明書を作成して、*clientkey.kdb* 鍵データベースに追加します。

```
gsk8capicmd -cert -create -db clientkey.kdb -pw clientpwd -label ¥
clientlabel -dn "cn=LDAP_Client,o=sample" -default_cert yes
```

ここで、*-dn* 値は、証明書を一意的に識別するために使用されません。

- クライアントの鍵データベースから証明書をバイナリー *der* 形式でファイルに抽出します。この例では、証明書はバイナリー *der* 形式でファイルに抽出されます。

注: 証明書は、base64 エンコードの ASCII データ形式 (.arm) で抽出することもできます。

```
gsk8capicmd -cert -extract -db clientkey.kdb -pw clientpwd -label ¥
clientlabel -target client.der -format binary
```

- 抽出されたサーバー証明書 (server.der) をサーバー・システムからクライアント・システムにインポートします。
- 抽出されたサーバー証明書をクライアントの鍵データベース・ファイルに追加します。

```
gsk8capicmd -cert -add -db clientkey.kdb -pw clientpwd ¥
-label serverlabel -file server.der -format binary
```

LDAP サーバー・システム上

1. IBM Security Directory Server システム上に、鍵データベース・ファイルを作成および格納するディレクトリーを作成して、その作業ディレクトリーに移動します。
2. IBM Security Directory Server が使用する CMS 鍵データベースを作成します。

```
gsk8capicmd -keydb -create -db serverkey.kdb -pw serverpwd -stash
```

ここで、*serverkey.kdb* は作成する鍵データベースで、*serverpwd* はパスワードです。

3. デフォルトの自己署名証明書を作成して、*serverkey.kdb* 鍵データベースに追加します。

```
gsk8capicmd -cert -create -db serverkey.kdb -pw serverpwd -label ¥
serverlabel -dn "cn=LDAP_Server,o=sample" -default_cert yes
```

ここで、*-dn* 値は、証明書を一意的に識別するために使用されません。

4. サーバーの鍵データベースから証明書をバイナリー *der* 形式でファイルに抽出します。この例では、証明書はバイナリー *der* 形式でファイルに抽出されます。

注：証明書は、base64 エンコードの ASCII データ形式 (*.arm*) で抽出することもできます。

```
gsk8capicmd -cert -extract -db serverkey.kdb -pw serverpwd ¥
-label serverlabel -target server.der -format binary
```

5. 抽出されたクライアント証明書 (*client.der*) をクライアント・システムからサーバー・システムにインポートします。
6. 抽出されたクライアント証明書をサーバーの鍵データベース・ファイルに追加します。

```
gsk8capicmd -cert -add -db serverkey.kdb -pw serverpwd ¥
-label clientlabel -file client.der -format binary
```

7. 構成ファイル内で、証明書を使用するように IBM Security Directory Server インスタンスを構成します。

```
idsldapmodify -h server.in.ibm.com -p 389 -D cn=root -w root ¥
-i /home/dsrdbm01/clientserverauth.ldif
```

clientserverauth.ldif ファイルには、以下の形式のコードが記述されています。

```
dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslAuth
ibm-slapdSslAuth: serverClientAuth

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSecurity
ibm-slapdSecurity: SSL

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabase
ibm-slapdSslKeyDatabase: /home/dsrdbm01/cskeys/serverkey.kdb

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslCertificate
ibm-slapdSslCertificate: serverlabel

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabasepw
ibm-slapdSslKeyDatabasepw: serverpwd
```

8. 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します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
```

9. 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始動します。

```
ibmslapd -I dsrdm01 -n -t
ibmdiradm -I dsrdm01 -t
```

クライアントとサーバー間の SSL 通信を検証するには、

```
idsldapsearch
```

コマンドを以下の形式でクライアント・システム上で実行します。

```
idsldapsearch -Z -h server.in.ibm.com -p 636 -K /usr/client/clientkey.kdb ¥
-P clientpwd -s base -b "o=sample" objectclass=*
o=sample
objectclass=top
objectclass=organization
o=sample
```

iKeyman ツール

鍵管理プログラムの **iKeyman** は、IBM Java に付属しています。このプログラムは、鍵ファイルを管理するための使いやすい GUI で、Java アプレットとしてインプリメントされています。

IBM Security Directory Server バージョン 6.3.1 をインストールすると、IBM JAVA バージョン 6 が使用可能になります。**iKeyman** ユーティリティーは、Windows の場合は `<SDS_Install_Directory>%java%¥jre¥bin` ディレクトリー、Linux の場合は `/opt/ibm/ldap/V6.3.1/java/jre/bin` ディレクトリー、AIX システムと Solaris システムの場合は `/opt/IBM/ldap/V6.3.1/java/jre/bin` ディレクトリーに格納されています。

注: JAVA_HOME を設定するようにプロンプトが出された場合、IBM Security Directory Server の java サブディレクトリーに設定できます。IBM Security Directory Server を使用する場合は、LIBPATH 環境変数を以下のように設定する必要があります。

Linux プラットフォームの場合

```
$export LIBPATH=$JAVA_HOME/bin:$JAVA_HOME/jre/bin:$LIBPATH
```

Windows プラットフォームの場合

```
c:¥> set LIB=%JAVA_HOME%¥bin; %JAVA_HOME%¥jre¥bin; %LIB%
```

AIX システムでは、LIBPATH 環境変数を使用して、ライブラリー・パスを指定します。Solaris システムでは、LD_LIBRARY_PATH 環境変数を使用します。

iKeyman ユーティリティーでは、公開鍵と秘密鍵のペアの作成、認証要求の作成、認証要求の鍵データベース・ファイルへの取り込み、および鍵データベース・ファイル内の鍵の管理を行うことができます。

注: Secure Sockets Layer 通信を設定する場合、使用するアプリケーションに適合した正しい鍵データベース・ファイル・タイプを使用してください。例えば、**Web 管理** コンソールなどの Java ベース・アプリケーションでは JKS ファイル・タイプが必要になり、IBM Security Directory Server などの C アプリケーションでは CMS 鍵データベース・ファイル・タイプが必要になります。

iKeyman を使用して、以下のタスクを実行することができます。

- 鍵ペアの作成と認証局からの証明書の要求
- 証明書の鍵データベース・ファイルへの保管

- 鍵と証明書の管理
 - 鍵データベース・パスワードの変更
 - 鍵に関する情報の表示
 - 鍵の削除
 - 鍵を鍵データベースのデフォルト鍵にする
 - 自己署名用の鍵ペアと認証要求の作成
 - 鍵のエクスポート
 - 鍵の鍵データベースへのインポート
 - 鍵をトラステッド・ルートとして指定する
 - トラステッド・ルート鍵の指定を解除する
 - 既存の鍵の証明書を要求する
- 鍵リング・ファイルの鍵データベース・フォーマットへのマイグレーション

鍵ペアの作成と認証局からの証明書の要求:

鍵ペアを作成して、認証局からの証明書を要求することができます。

このタスクについて

クライアントおよびサーバー認証を必要とする LDAP サーバーにクライアント・アプリケーションを接続するには、公開鍵と秘密鍵のペア、および証明書を作成する必要があります。

サーバー認証のみを必要とする LDAP サーバーにクライアント・アプリケーションが接続している場合は、公開鍵と秘密鍵のペア、および証明書を作成する必要はありません。この場合は、トラステッド・ルートとしてマーク付けされたクライアント鍵データベース・ファイルに証明書を保管するのみで構いません。サーバーの証明書を発行した認証局 (CA) がクライアント鍵データベースにまだ定義されていない場合は、CA からの CA 証明書を要求し、それを鍵データベースに保管し、トラステッドとしてマーク付けする必要があります。175 ページの『鍵をトラステッド・ルートとして指定する』を参照してください。

クライアントは、自分の秘密鍵を使用して、サーバーに送信するメッセージに署名します。サーバーは、自分に送信されるメッセージを暗号化するための公開鍵をクライアントに送信します。サーバーは、その公開鍵で暗号化されたメッセージを自分の秘密鍵で暗号化解除します。

クライアントが自分の公開鍵をサーバーに送信するには、クライアントの証明書が必要です。証明書には、クライアントの公開鍵、クライアント証明書に関連付けられた識別名、証明書のシリアル番号、および証明書の有効期限が含まれます。証明書は、クライアントの ID を検査する CA から発行されます。

CA によって署名される証明書を作成するための基本手順は以下のとおりです。

1. **ikeyman** を使用して認証要求を作成します。
2. 作成した認証要求を CA に実行依頼します。認証要求を CA に実行依頼するには、電子メールを使用するか、CA の Web ページのオンライン実行依頼を利用します。

3. CA からの応答をサーバーのファイルシステム上のアクセス可能な場所に保管します。
4. 証明書を鍵データベース・ファイルに保管します。

注: トラストド CA のデフォルト・リストにない CA から署名付きのクライアント証明書を取得する場合は、その CA の証明書を取得し、それを鍵データベースに保管して、トラストドとしてマーク付けする必要があります。これは、署名付きクライアント証明書を鍵データベース・ファイルに保管する前に行う必要があります。

公開鍵と秘密鍵のペアを作成して証明書を要求するには、以下の手順を実行します。

1. 以下のコマンドを入力して、**ikeyman** Java ユーティリティーを開始します。

```
ikeyman
```

2. 「**鍵データベース・ファイル**」を選択します。
3. 「**新規**」を選択します (鍵データベースがすでに存在する場合は、「**開く**」を選択します)。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「**OK**」をクリックします。

注: 鍵データベースは、1 つ以上の鍵ペアと証明書を保管するためにクライアントやサーバーが使用するファイルです。

5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「**OK**」をクリックします。
6. 「**作成**」を選択します。
7. 「**新規証明書要求 (New Certificate Request)**」を選択します。
8. ユーザー割り当てラベルを鍵ペアに指定します。鍵データベース・ファイル内の鍵ペアと証明書は、このラベルで識別されます。
9. 低保証クライアント証明書を要求する場合は、共通名を入力します。共通名は、固有なユーザーのフルネームでなければなりません。
10. 高保証セキュア・サーバー証明書を要求する場合は、以下を行う必要があります。
 - サーバーの X.500 共通名を入力します。通常は、www.ibm.com のような TCP/IP 完全修飾ホスト名として入力します。VeriSign サーバー証明書を入手するには、完全修飾ホスト名を指定する必要があります。
 - 組織名を入力します。これは、組織の名前です。VeriSign セキュア・サーバー証明書を入手する場合、VeriSign のアカウントがすでにあるときは、そのアカウントと同じ名前をこのフィールドに入力する必要があります。
 - 組織の単位名を入力します。このフィールドは、必要に応じて入力します。
 - サーバーが設置されている地域を入力します。このフィールドは、必要に応じて入力します。
 - サーバーが設置されている都道府県の省略形 (3 文字) を入力します。
 - サーバーの設置場所の郵便番号を入力します。
 - サーバーの設置場所の国別コード (2 文字) を入力します。
11. 「**OK**」をクリックします。

12. 認証要求ファイルの名前と場所を確認するメッセージが表示されます。「OK」をクリックします。
13. 認証要求を CA に送信します。

VeriSign の低保証証明書またはセキュア・サーバー証明書を要求する場合は、電子メールで VeriSign に認証要求を送る必要があります。

低保証認証要求の場合は、簡単な書式で VeriSign に電子メールを送ることができます。セキュア・サーバー認証要求の場合は、所定の書式に従って電子メールを送る必要があります。セキュア・サーバー認証要求の書式については、<http://www.verisign.com/server/index.html> を参照してください。

14. CA から証明書を受け取ったら、それを鍵ペアが保管されている鍵データベースに保管します。証明書を鍵データベースに保管するには **ikeyman** を使用します。『証明書の鍵データベースへの保管』を参照してください。

注: 鍵データベース・パスワードは定期的に変更するようにしてください。パスワードに有効期限を設定した場合は、パスワード変更の時期を常に把握しておく必要があります。パスワード変更前にパスワードが失効すると、パスワードを変更するまで鍵データベースを使用できません。

証明書の鍵データベースへの保管:

以下に示す指示により、証明書を鍵データベース内に保管することができます。

このタスクについて

CA から応答を受け取ったら、証明書を鍵データベースに保管する必要があります。

証明書を鍵データベースに保管するには、以下の手順を実行します。

1. **ikeyman** と入力して、Java ユーティリティを開始します。
2. 「**鍵データベース・ファイル**」を選択します。
3. 「**開く**」を選択します。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「**OK**」をクリックします。
5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「**OK**」をクリックします。
6. 「**作成**」を選択します。
7. 中央のウィンドウにある「**個人用証明書**」を選択します。
8. 「**受取**」をクリックします。
9. CA から受け取った署名付き証明書を入れる証明書ファイルの名前と場所を入力します。「**OK**」をクリックします。

鍵データベース・パスワードの変更:

ここで説明する手順に従うことにより、鍵データベース・パスワードを変更することができます。

このタスクについて

1. ikeyman と入力して、Java ユーティリティを開始します。
2. 「鍵データベース・ファイル」を選択します。
3. 「開く」を選択します。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「OK」をクリックします。
5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「OK」をクリックします。
6. 「鍵データベース・ファイル」を選択します。
7. 「パスワードの変更」を選択します。
8. <New password> を入力します。
9. <New password> を確認します。
10. 必要があれば、パスワードの有効期限を選択して設定します。
11. パスワードを暗号化してディスクに保管する場合は、「ファイルに対してパスワードを隠しておきますか？」を選択します。
12. 「OK」をクリックします。
13. stash パスワード・ファイルの名前と場所が示されたメッセージが表示されます。「OK」をクリックしてください。

注：パスワードは秘密鍵を保護するので重要です。秘密鍵は、文書に署名したり、公開鍵で暗号化されたメッセージを暗号解除したりするために使用できる唯一の鍵です。

鍵に関する情報の表示:

鍵に関する情報 (名前、サイズ、トラステッド・ルートかどうかなど) を表示するには、以下のステップを実行します。

このタスクについて

1. ikeyman と入力して、Java ユーティリティを開始します。
2. 「鍵データベース・ファイル」を選択します。
3. 「開く」を選択します。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「OK」をクリックします。
5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「OK」をクリックします。
6. 個人用証明書として指定した鍵に関する情報を表示させるには、以下を行います。
 - 「鍵データベースの内容 (Key database content)」セクションの下にあるリストから「個人証明書 (Personal Certificates)」を選択します。
 - 証明書を選択します。
 - 「表示/編集」をクリックし、選択した鍵の情報を表示します。
 - 「OK」をクリックし、個人証明書のリストに戻ります。

7. 署名者の証明書として指定された鍵の情報を表示するには、以下の手順を実行します。
 - 「**鍵データベースの内容 (Key database content)**」セクションの下にあるリストから「**署名者証明書 (Signer Certificates)**」を選択します。
 - 証明書を選択します。
 - 「**表示/編集**」をクリックし、選択した鍵の情報を表示します。
 - 「**OK**」をクリックし、署名者の証明書のリストに戻ります。

鍵の削除:

ここで説明する手順に従って、鍵を削除します。

このタスクについて

鍵を削除するには、以下の手順を実行します。

手順

1. `ikeyman` と入力して、Java ユーティリティを開始します。
2. 「**鍵データベース・ファイル**」を選択します。
3. 「**開く**」を選択します。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「**OK**」をクリックします。
5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「**OK**」をクリックします。
6. 「**鍵データベースの内容 (Key database content)**」セクションの下にあるリストから削除する鍵のタイプ (個人証明書、署名者証明書、または個人証明書要求) を選択します。
7. 証明書を選択します。
8. 「**削除**」をクリックします。
9. 削除の確認には「**はい**」をクリックします。

鍵を鍵リング内のデフォルト鍵にする:

ここで説明する手順に従うことにより、鍵を鍵リング内のデフォルト鍵にすることができます。

このタスクについて

デフォルト鍵は、サーバーがセキュアな通信のために使用する秘密鍵でなければなりません。

鍵を鍵リング内のデフォルト鍵にするには、以下の手順を実行します。

1. `ikeyman` と入力して、Java ユーティリティを開始します。
2. 「**鍵データベース・ファイル**」を選択します。
3. 「**開く**」を選択します。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「**OK**」をクリックします。

5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「OK」をクリックします。
6. 「鍵データベースの内容 (Key database content)」セクションの下にあるリストから「個人証明書 (Personal Certificates)」を選択します。
7. 必要な証明書を選択します。
8. 「表示/編集」を選択します。
9. 「証明書をデフォルトとして設定」ボックスを選択します。「OK」をクリックします。

自己署名用の鍵ペアと認証要求の作成:

以下に示す説明に従うことにより、自己署名用の鍵ペアと認証要求を作成することができます。

このタスクについて

定義上、セキュア・サーバーには、公開鍵と秘密鍵のペア、および証明書が必要です。

サーバーは、自分の秘密鍵を使用して、クライアントに送信するメッセージに署名します。サーバーは、自分に送信されるメッセージを暗号化するための公開鍵をクライアントに送信します。サーバーは、その公開鍵で暗号化されたメッセージを自分の秘密鍵で暗号化解除します。

サーバーが自分の公開鍵をクライアントに送信するには、サーバーの証明書が必要です。証明書には、サーバーの公開鍵、サーバー証明書に関連付けられた識別名、証明書のシリアル番号、および証明書の有効期限が含まれます。証明書は、サーバーの ID を検査する CA から発行されます。

ユーザーは、以下の証明書のいずれかを要求できます。

- VeriSign から発行される低保証証明書。これは、機密保護機能のある環境のベータ・テストなど、非商用目的に最適です。
- インターネット上で商用ビジネスを行うためのサーバー証明書。VeriSign やその他の CA から入手できます。
- 自己署名サーバー証明書 (プライベートな Web ネットワークにおいて、自分自身の CA として機能する場合)。

VeriSign などの CA を利用してサーバー証明書に署名する方法については、168 ページの『鍵ペアの作成と認証局からの証明書の要求』を参照してください。

一般に、自己署名証明書を作成するには、以下の手順を実行します。

1. ikeyman と入力して、Java ユーティリティを開始します。
2. 「鍵データベース・ファイル」を選択します。
3. 「新規」を選択します (鍵データベースがすでに存在する場合は、「開く」を選択します)。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「OK」をクリックします。**注:** 鍵データベースは、1 つ以上の鍵ペアと証明書を保管するためにクライアントやサーバーが使用するファイルです。

5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「OK」をクリックします。
6. 「新規自己署名 (New self-signed)」をクリックします。
7. 以下の入力を指定します。
 - 鍵ペアのユーザー割り当てラベル。鍵データベース・ファイル内の鍵ペアと証明書は、このラベルで識別されます。
 - 必要な証明書のバージョン。
 - 必要な鍵のサイズ。
 - 必要な署名アルゴリズム。
 - サーバーの X.509 共通名。通常は、www.ibm.com のような TCP/IP 完全修飾ホスト名として入力します。
 - 組織名。これは、組織の名前です。
 - 組織の単位名。このフィールドは、必要に応じて入力します。
 - サーバーが設置されている地域。このフィールドは、必要に応じて入力します。
 - サーバーが設置されている都道府県の省略形 (3 文字)。
 - サーバーが設置されている場所に該当する郵便番号。
 - サーバーの設置場所の国別コード (2 文字)。
 - 証明書の有効期間。
8. 「OK」をクリックします。

鍵のエクスポート:

鍵ペアまたは証明書を別のコンピューターに転送する必要がある場合は、鍵データベースからファイルに鍵ペアをエクスポートします。

このタスクについて

転送先のコンピューターでは、鍵ペアを鍵リングにインポートします。

鍵データベースから鍵をエクスポートするには、以下の手順を実行します。

1. ikeyman と入力して、Java ユーティリティを開始します。
2. 「鍵データベース・ファイル」を選択します。
3. 「開く」を選択します。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「OK」をクリックします。
5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「OK」をクリックします。
6. 「鍵データベースの内容 (Key database content)」セクションの下にあるリストから「個人証明書 (Personal Certificates)」を選択します。
7. 必要な証明書を選択します。
8. 「エクスポート/インポート」をクリックします。
9. 「アクション・タイプ (Action type)」として「鍵をエクスポート (Export Key)」を選択します。

10. 鍵付きファイル・タイプを選択します。

注: IBM Security Directory Server では、CMS 鍵データベース・ファイル・タイプが必要です。

11. ファイル名を指定します。
12. 場所を指定します。
13. 「OK」をクリックします。
14. ファイルの必須パスワードを入力します。「OK」をクリックします。

鍵のインポート:

ここで説明する手順に従うことにより、鍵を鍵リング内にインポートできます。

このタスクについて

手順

1. ikeyman と入力して、Java ユーティリティを開始します。
2. 「鍵データベース・ファイル」を選択します。
3. 「開く」を選択します。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「OK」をクリックします。
5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「OK」をクリックします。
6. 「鍵データベースの内容 (Key database content)」セクションの下にあるリストから「個人証明書 (Personal Certificates)」を選択します。
7. 必要な証明書を選択します。
8. 「エクスポート/インポート」をクリックします。
9. 「アクション・タイプ (Action type)」として「鍵をインポート」を選択します。
10. 必要な鍵タイプ・ファイルを選択します。注: Secure Sockets Layer 通信を設定する場合は、アプリケーションに対し正しい鍵データベース・ファイル・タイプを使用するようにしてください。例えば、Web 管理コンソールなどの Java ベースのアプリケーションには JKS ファイル・タイプ、IBM Security Directory Server などの C アプリケーションには CMS 鍵データベース・ファイル・タイプが必要です。
11. ファイルの名前と場所を入力します。
12. 「OK」をクリックします。
13. ソース・ファイルの必須パスワードを入力します。「OK」をクリックします。

鍵をトラステッド・ルートとして指定する:

トラステッド・ルート鍵は、公開鍵と関連付けられた CA の識別名を合わせたものです。トラステッド・ルートは、以下にリストされている新しい鍵データベースごとに定義されます。

このタスクについて

- Entrust.net Certification Authority (2048)
- Entrust.net Client Certification Authority
- Entrust.net Global Client Certification Authority
- Entrust.net Global Secure Server Certification Authority
- Entrust.net Secure Server Certification Authority
- RSA Secure Server Certification Authority
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3

注: 上記の各トラステッド・ルートは、デフォルトで最初からトラステッド・ルートになるように設定されます。

鍵をトラステッド・ルートとして指定するには、以下の手順を実行します。

1. ikeyman と入力して、Java ユーティリティを開始します。
2. 「鍵データベース・ファイル」を選択します。
3. 「開く」を選択します。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「OK」をクリックします。
5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「OK」をクリックします。
6. 「鍵データベースの内容 (Key database content)」セクションの下にあるリストから「署名者証明書 (Signer Certificates)」を選択します。
7. 「取り込み」をクリックします。
8. 「CA 証明書の追加」ダイアログ・ボックスから、必要な証明書を選択します。
9. 「表示/編集」を選択します。

10. 「証明書をトラステッド・ルートとして設定」チェック・ボックスを選択し、「OK」をクリックします。
11. 「鍵データベース・ファイル」を選択し、「閉じる」を選択します。

トラステッド・ルート鍵の指定解除:

トラステッド・ルート鍵は、公開鍵と関連付けられた CA の識別名を合わせたものです。トラステッド・ルートは、それぞれの新しい鍵データベース内で、提供されているリストでの共有として定義されます。

このタスクについて

- Entrust.net Certification Authority (2048)
- Entrust.net Client Certification Authority
- Entrust.net Global Client Certification Authority
- Entrust.net Global Secure Server Certification Authority
- Entrust.net Secure Server Certification Authority
- RSA Secure Server Certification Authority
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3

注: 上記の各トラステッド・ルートは、デフォルトで最初からトラステッド・ルートになるように設定されます。

鍵のトラステッド・ルート状況を解除するには、以下の手順を実行します。

1. ikeyman と入力して、Java ユーティリティを開始します。
2. 「鍵データベース・ファイル」を選択します。
3. 「開く」を選択します。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「OK」をクリックします。

5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「OK」をクリックします。
6. 「鍵データベースの内容 (Key database content)」セクションの下にあるリストから「署名者証明書 (Signer Certificates)」を選択します。
7. 必要な証明書を選択します。
8. 「表示/編集」を選択します。
9. 「証明書をトラステッド・ルートとして設定」チェック・ボックスをクリアします。「OK」をクリックします。
10. 「鍵データベース・ファイル」を選択し、「閉じる」を選択します。

既存の鍵の認証要求:

ここで説明する手順に従って、既存の鍵の認証要求を作成できます。

このタスクについて

1. ikeyman と入力して、Java ユーティリティを開始します。
2. 「鍵データベース・ファイル」を選択します。
3. 「開く」を選択します。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「OK」をクリックします。
5. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「OK」をクリックします。
6. 「鍵データベースの内容 (Key database content)」セクションの下にあるリストから「個人証明書 (Personal Certificates)」を選択します。
7. 必要な証明書を選択します。
8. 「エクスポート/インポート」をクリックします。
9. 「アクション・タイプ (Action type)」として「鍵をエクスポート (Export Key)」を選択します。
10. 必要な鍵付きファイル・タイプを選択します。
11. 証明書のファイル名と場所を入力します。
12. 「OK」をクリックします。
13. 「鍵データベース・ファイル」を選択し、「閉じる」を選択します。

認証要求を CA に送信します。

VeriSign の低保証証明書またはセキュア・サーバー証明書を要求する場合は、電子メールで VeriSign に認証要求を送る必要があります。

低保証認証要求の場合は、簡単な書式で VeriSign に電子メールを送ることができます。セキュア・サーバー認証要求の場合は、所定の書式に従って電子メールを送る必要があります。セキュア・サーバー認証要求の書式については、<http://www.verisign.com/server/index.html> を参照してください。

鍵リング・ファイルの鍵データベース・フォーマットへのマイグレーション:

以下に示されている手順により、鍵リング・ファイルを鍵データベース・フォーマットにマイグレーションすることができます。

このタスクについて

mkkf で作成した既存の鍵リング・ファイルを **ikeyman** で使用するフォーマットにマイグレーションするには、**ikeyman** プログラムを使用します。

鍵リング・ファイルをマイグレーションするには、以下の手順を実行します。

1. **ikeyman** と入力して、Java ユーティリティを開始します。
2. 「**鍵データベース・ファイル**」を選択します。
3. 「**開く**」を選択します。
4. 鍵データベース・タイプ、鍵データベース・ファイルの名前と場所を指定します。「**OK**」をクリックします。
5. 指示に従って、鍵リング・ファイルのパスワードを入力します。「**OK**」をクリックします。
6. 「**鍵データベース・ファイル**」を選択します。
7. 「**名前を付けて保存**」を選択します。
8. 鍵データベースのタイプとして「**CMS**」を選択します。
9. ファイル名を指定します。
10. 場所を指定します。
11. 「**OK**」をクリックします。

鍵データベースの設定

鍵データベースを設定する場合は、以下の情報を参照してください。

鍵データベースを設定するには、以下のいずれかの手順を使用します。

Web 管理の使用

Web 管理ツールを使用して鍵データベースを設定するには、以下の手順を実行します。

このタスクについて

Web 管理ナビゲーション領域の「**サーバー管理**」をクリックし、展開されたリスト上で「**セキュリティー・プロパティの管理**」をクリックします (この操作をまだ実行していない場合)。次に、「**鍵データベース**」タブをクリックします。

1. 「**鍵データベースのパスおよびファイル名**」を指定します。これは、鍵データベース・ファイルの完全修飾ファイル仕様です。パスワード stash ファイルが定義されている場合、そのファイルの拡張子は **.sth** で、同じファイル仕様を持つものと見なされます。
2. 「**鍵パスワード**」を指定します。パスワード stash ファイルが使用されていない場合は、鍵データベース・ファイルのパスワードをここで指定する必要があります。「**パスワードの確認**」フィールドにパスワードを再度入力します。
3. 「**鍵ラベル**」を指定します。この管理者定義鍵ラベルは、鍵データベースのどの部分を使用するかを示します。
4. 終了したら、「**OK**」をクリックして変更を適用します。

注: このファイルをサーバーで使用するには、ユーザー ID **ldap** でこのファイルを読み取れるように設定する必要があります。ファイルのアクセス権については、IBM Security Directory Server の資料の『トラブルシューティングとサポート』セクションを参照してください。

コマンド・ラインの使用

以下のコマンドを実行して、SSL と TLS の鍵データベースを設定することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSSLKeyDatabase
ibm-slapdSSLKeyDatabase: <databasename>
-
replace: ibm-slapdSSLKeyDatabasePW
ibm-slapdSSLKeyDatabasePW: <password>
-
replace: ibm-slapdSslKeyRingFilePW
ibm-slapdSslKeyRingFilePW: <password>
```

変更した内容を有効にするには、サーバーおよび管理サーバーを再始動する必要があります。

PKCS#11

PKCS#11 は、LDAP ユーザーが暗号ハードウェアを使用できるようにするためのインターフェースです。**PKCS#11** を使用すると、LDAP ユーザーは暗号ハードウェアを使用して、鍵データベース・ファイルを安全に格納できると同時に、暗号操作を迅速化することができます。

PKCS#11 インターフェースを使用して、以下のタイプの暗号デバイスを構成することができます。

アクセラレーター

このデバイスは、カード・スロットや LAN 接続などの永続的接続によって、ホストに接続されます。アクセラレーターの主な目的は、サーバーの 1 秒当たりの暗号操作数を増加させることです。秘密鍵ストレージは SSL KDB (鍵データベース) ファイルに保持されていて、必要に応じてアクセラレーターに読み込まれます。このタイプのデバイスの使用を検討する必要があるのは、暗号操作数の増加のみが目標である場合です。サーバーの秘密鍵に対するハードウェア保護の強化は関係ありません。

アクセラレーター付き鍵ストレージ

このデバイスは主に、暗号のパフォーマンスが検討課題であると同時にサーバーの秘密鍵のセキュリティの強固さも重要であるサーバー・アプリケーション向けです。秘密鍵と証明書はデバイスに格納されます。暗号操作に秘密鍵が必要な場合、ハードウェア・デバイスがアダプター上でローカルに秘密鍵を使用します。アプリケーションが暗号化されていない形式で鍵にアクセスすることは絶対にできません。この種のデバイスでは、通常、外部アクセスから鍵を保護するための改ざん防止処理が採用されています。

PKCS#11 インターフェースを使用するようにサーバーを構成する方法

ディレクトリー・サーバーは、項目「dn: cn=SSL, cn=Configuration」の元で、PKCS#11 インターフェースを使用するように構成できます。

このタスクについて

Web 管理の使用:

以下に示す指示により、Web 管理ツールを使用してセキュリティー・プロパティを管理することができます。

このタスクについて

Web 管理ツールのナビゲーション領域で「サーバー管理」カテゴリを展開し、「セキュリティー・プロパティの管理」タブをクリックします。次に、「PKCS#11 設定」タブをクリックします。「PKCS#11 設定」パネルが表示されます。このパネルは、ibm-supportedCapabilities のルート DSE 検索で PKCS#11 インターフェース・サポート OID 1.3.18.0.2.32.67 が戻される場合にのみ表示されます。

注: このパネルで指定した設定を有効にするには、「セキュリティー・プロパティの管理」カテゴリの「設定」パネルで、「PKCS#11 インターフェース・サポートを有効にする」チェック・ボックスを選択する必要があります。

PKCS#11 インターフェースがサポートされるハードウェアを設定するには、以下の手順を実行します。

1. 鍵ストレージの場所を暗号ハードウェアとして指定するには、「暗号ハードウェアの鍵ストレージを使用可能にする」チェック・ボックスを選択します。
2. 「対称暗号」、「ダイジェスト」、または「ランダム・データ生成プログラム」チェック・ボックスを選択することにより、暗号ハードウェアの必要なアクセラレーション機能を選択します。

注: 「アクセラレーター・モード・オプション」セクションの下のチェック・ボックスは 1 つ以上選択できます。

3. 「暗号ハードウェアのライブラリー・パスおよびファイル名」テキスト・ボックスで、PKCS#11 インターフェースを使用してアクセスする暗号ハードウェア・ドライバのライブラリー・パスを指定します。
4. 「トークン・パスワード」テキスト・ボックスで、暗号ハードウェアのスロットにアクセスする際に使用するパスワードを指定します。
5. 「確認パスワード」テキスト・ボックスで、パスワードを再入力します。
6. 「トークン・ラベル」テキスト・ボックスで、アクセスする暗号ハードウェアのスロットのトークン・ラベルを指定します。
7. 完了したら、以下のステップのいずれかを行います。
 - a. 「OK」をクリックして変更を適用し、このパネルを終了します。
 - b. 「適用」をクリックして変更内容を適用し、このパネルを表示させたままにします。
 - c. 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

注: 変更した内容を有効にするには、サーバーを再始動する必要があります。

コマンド・ラインの使用:

以下に示すコマンドを発行することにより、パススルー認証を構成することができます。

このタスクについて

コマンド行を使用して、PKCS#11 インターフェースを使用するようにサーバーを構成するには、以下のコマンドを発行します。

```
ldapmodify -D <adminDN> -w <adminPW> -i <filename>

where <filename> contains:

dn: cn=ssl,cn=configuration
changetype: modify
replace: ibm-slapdSecurity
ibm-slapdSecurity: SSLOnly
-
replace: ibm-slapdSslAuth
ibm-slapdSslAuth: serverauth
-
replace: ibm-slapdSslCertificate
ibm-slapdSslCertificate: tlabel1
-
replace: ibm-slapdSslPKCS11Enabled
ibm-slapdSslPKCS11Enabled: True
-
replace: ibm-slapdSslPKCS11Lib
ibm-slapdSslPKCS11Lib: /opt/nfast/toolkits/pkcs11/libcknfast.so
-
replace: ibm-slapdSslPKCS11Keystorage
ibm-slapdSslPKCS11Keystorage: true
-
replace: ibm-slapdSslPKCS11TokenLabel
ibm-slapdSslPKCS11TokenLabel: OpCard
-
replace: ibm-slapdSslPKCS11TokenPW
ibm-slapdSslPKCS11TokenPW: PASSWORD
```

SSL 通信と TLS 通信の暗号化レベルの設定

SSL 通信と TLS 通信の暗号化レベルを設定することができます。

デフォルトでは、SSL バージョンと TLS バージョンの IBM Security Directory Server は、SSL ハンドシェイクまたは TLS ハンドシェイクで暗号をクライアントとネゴシエーションする際に以下の暗号を使用します。

注: 構成専用モードでは、パスワード・ポリシー機能は利用できませんが、パスワード暗号化のレベルは変更できます。

Web 管理の使用

Web 管理ツールを使用して暗号化の SSL レベルを設定するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「サーバー管理」カテゴリを展開します。

手順

1. 「セキュリティー・プロパティーの管理」をクリックします。
2. 「暗号化」をクリックします。

3. サーバーにアクセスするクライアントに基づいて、使用する暗号化の方法を選択します。AES-128 がデフォルトの暗号化レベルです。複数の暗号化方法を選択した場合、デフォルトでは最高レベルの暗号化が使用されますが、選択された下位の暗号化レベルを使用するクライアントにも、サーバーへのアクセス権があります。IBM Security Directory Server では、AES (Advanced Encryption Standard) レベルの暗号化がサポートされています。AES の詳細については、<http://csrc.nist.gov/encryption/aes/> の NIST Web ページを参照してください。

表 12. サポートされる暗号化のレベル

暗号化レベル	属性
168 ビット鍵と SHA-1 MAC を用いる Triple-DES 暗号化	ibm-slapdSslCipherSpec: TripleDES-168
56 ビット鍵と SHA-1 MAC を用いる DES 暗号化	ibm-slapdSslCipherSpec: DES-56
128 ビット鍵と SHA-1 MAC を用いる RC4 暗号化	ibm-slapdSslCipherSpec: RC4-128-SHA
128 ビット鍵と MD5 MAC を用いる RC4 暗号化	ibm-slapdSslCipherSpec: RC4-128-MD5
40 ビット鍵と MD5 MAC を用いる RC2 暗号化	ibm-slapdSslCipherSpec: RC2-40-MD5
40 ビット鍵と MD5 MAC を用いる RC4 暗号化	ibm-slapdSslCipherSpec: RC4-40-MD5
AES 128 ビット暗号化	ibm-slapdSslCipherSpec: AES-128
AES 256 ビット暗号化	ibm-slapdSslCipherSpec: AES

注: SSL と TLS は AES 192 暗号化をサポートしません。選択した暗号は、`ibm-slapdsslCipherSpec` キーワードと上記の表に記載された属性を使用して構成ファイルに格納されます。例えば、Triple-DES のみを使用する場合は、「**168 ビット鍵と SHA-1 MAC を用いる Triple-DES 暗号化**」を選択します。属性 `ibm-slapdSslCipherSpec: TripleDES-168` が `ibmslapd.conf` ファイルに追加されます。この場合、サーバーに対して SSL 接続を確立できるのは、Triple-DES もサポートするクライアントだけです。複数の暗号を選択できます。

4. 連邦情報処理標準 (FIPS) モード対応機能がサーバーでサポートされている場合は、ヘッダー「インプリメンテーション (Implementation)」の下に、「**FIPS 認証インプリメンテーションを使用する (Use FIPS certified implementation)**」チェック・ボックスが選択済みの状態で表示されます。これにより、サーバーは、ICC FIPS 認証ライブラリーからの暗号化アルゴリズムを使用できるようになります。このチェック・ボックスの選択を解除した場合は、非 FIPS 認証ライブラリーからの暗号化アルゴリズムが使用されます。注: サーバーを構成すれば FIPS 処理モードをオンにできます。また、FIPS 用のライブラリーもオンにする必要があります。
5. 完了したら、終了せずに変更を保存する場合は「適用」をクリックし、変更を適用して終了する場合は「OK」をクリックし、変更を行わずにこのパネルを終了するには「キャンセル」をクリックします。

コマンド・ラインの使用

コマンド行を使用して暗号化の SSL レベルを設定するには (この例では、168 ビット鍵と SHA-1 MAC によるトリプル DES 暗号化)、以下のコマンドを実行します。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSslCipherSpec
ibm-slapdSslCipherSpec: TripleDES-168
```

他の暗号化値については、183 ページの表 12 を参照してください。

暗号化のレベルを複数追加するには、<filename> に次の以下の情報を記述しておく必要があります。

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSslCipherSpec
ibm-slapdSslCipherSpec: RC2-40-MD5
ibm-slapdSslCipherSpec: AES
ibm-slapdSslCipherSpec: AES-128
ibm-slapdSslCipherSpec: RC4-128-MD5
ibm-slapdSslCipherSpec: RC4-128-SHA
ibm-slapdSslCipherSpec: TripleDES-168
ibm-slapdSslCipherSpec: DES-56
ibm-slapdSslCipherSpec: RC4-40-MD5
```

コマンド行を使用して FIPS モードをオフにするには、以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSslFIPSMoDeEnabled
ibm-slapdSslFIPSMoDeEnabled: false
```

変更した内容を有効にするには、サーバーおよび管理サーバーを再始動する必要があります。

NIST SP 800-131A のサポート

NIST SP 800-131A ガイドラインに移行するためには、LDAP 環境が準拠するべきセキュリティ要件を特定する必要があります。

米国連邦情報・技術局 (NIST) Special Publication (SP) 800-131A ガイドラインは、暗号鍵管理の指針を示したものです。このガイドラインには、以下の事項が記載されています。

- 鍵管理の手順。
- 暗号アルゴリズムの使用方法。
- 使用するアルゴリズムとその最小強度。
- セキュア通信のための鍵の長さ。

NIST SP 800-131A について詳しくは、<http://csrc.nist.gov/publications/PubsSPs.html> Web サイトにある「*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*」(英文)を参照してください。

Suite B モードは、SP 800-131A 規格の限定的なサブセットです。Suite B は、NSA の国家安全のためのアプリケーション向けの暗号アルゴリズム・ポリシーを Transport Layer Security (TLS) プロトコルとともに使用するよう定義します。Suite B については、<http://tools.ietf.org/html/rfc6460> Web サイトにある「*Suite B Profile for Transport Layer Security (TLS) RFC 6460*」(英文)を参照してください。

政府機関および金融機関は、製品が指定のセキュリティー要件に準拠していることを保証するために NIST SP 800-131A ガイドラインを使用します。

NIST SP 800-131A への移行のサポート

NIST SP 800-131A への移行に必要なプロトコル、暗号アルゴリズム、および鍵の長さを特定する必要があります。

NIST SP 800-131A ガイドラインへの移行のために、IBM Security Directory Server バージョン 6.3.1 では以下のものがサポートされます。

- Transport Layer Security (TLS) 1.2 プロトコル。
- TLS 1.2 以外のプロトコルの無効化。
- 以下の鍵の強度を持つ公開鍵。
 - 最小サイズが 2048 ビットの RSA 鍵。
 - 最小サイズが 160 ビットまたは曲線 p160 である楕円曲線 (EC) 鍵。
- 2048 ビット以上の RSA 鍵、あるいは 160 ビットまたは曲線 p160 以上の EC 鍵を持つ証明書。
- 最低でも SHA2 署名アルゴリズムを使用したデジタル署名。
- TLS 1.2 署名およびハッシュ・アルゴリズムの制限の設定。
- Suite B モード。

IBM Security Directory Server バージョン 6.3.1 をインストールすると、NIST SP 800-131A への移行のサポートはデフォルトで無効に設定されます。

TLS 1.2 署名およびハッシュ・アルゴリズムや Suite B モードなどの機能を設定するには、セキュア・ポートを介したセキュア接続を行うようにディレクトリー・サーバーを構成します。非セキュア・ポートを介したセキュア接続を行うようにディレクトリー・サーバーを構成した場合、これらの機能はサポートされません。セキュア・ポートを介した接続を受け入れるようにサーバーを構成すると、サーバーは、TLS 開始拡張操作ではなく、Transport Layer Security (TLS) プロトコルを使用します。TLS プロトコルおよび TLS 開始拡張操作について詳しくは、187 ページの『IBM Security Directory Server での TLS プロトコルと TLS 開始拡張操作との相違点』を参照してください。

ディレクトリー・サーバー環境でのセキュア通信の構成設定:

ディレクトリー・サーバーをセキュア通信用に構成するために必要な構成設定を特定する必要があります。

ディレクトリー・サーバーをセキュア通信用に構成するには、構成ファイルの `cn=SSL,cn=Configuration` 項目に必要な属性を設定しなければなりません。

ディレクトリー・サーバーが連邦情報処理標準 (FIPS) モード使用可能化をサポートしている場合は、FIPS 処理モードで始動するようにサーバーを構成できます。FIPS 処理モードを設定した場合、サーバーでは以下のものが使用されます。

- ICC FIPS 認証ライブラリーからの認証暗号化アルゴリズムが暗号化に使用されま
す。
- FIPS によってサポートされる最もセキュアな暗号が採用されます。
- サーバーとクライアントの間の通信の保護には TLS プロトコルのみが使用されま
す。
- 特定のバージョンの TLS プロトコルに対して最もセキュアな暗号が使用されま
す。

表 13. FIPS 処理モードの属性

属性	値
<code>ibm-slapdSecurity</code>	SSL SSLOnly SSLTLS TLS
<code>ibm-slapdSslFIPSMoDeEnabled</code>	true (デフォルトでは true)
<code>ibm-slapdSslFIPsProcessingMoDe</code>	true
<code>ibm-slapdSslAuth</code>	serverClientAuth serverAuth
<code>ibm-slapdSslCertificate</code>	certificate_label
<code>ibm-slapdSslKeyDatabase</code>	keydatabasefile_with_path
<code>ibm-slapdSslKeyDatabasepw</code>	keydatabasefile_password

ibm-slapdSecurity

サーバーが受け入れる接続のタイプを指定します。

次の値のいずれかを選択してください。

- **SSL** は、セキュア通信用のセキュア・ポート上の接続を受け入れるためのサー
バーを指定します。このサーバーは、非セキュア・ポート上の非セキュア
通信も受け入れます。
- **SSLOnly** は、セキュア通信用のセキュア・ポート上の接続のみを受け入れる
ためのサーバーを指定します。
- **SSLTLS** は、セキュア通信用のセキュア・ポートおよび非セキュア・ポート上
の接続を受け入れるためのサーバーを指定します。このサーバーは、非セキ
ュア・ポート上の非セキュア通信も受け入れます。
- **TLS** は、セキュア通信および非セキュア通信用の非セキュア・ポート上の接
続を受け入れるためのサーバーを指定します。

ibm-slapdSslFIPSMoDeEnabled

サーバーが GSKit ライブラリーの ICC バージョンを使用するかどうかを指定
します。

次の値のいずれかを選択してください。

- **true** は、サーバーが GSKit ライブラリーの ICC バージョンを使用するこ
とを指定します。
- **false** は、サーバーが BSAFE バージョンを使用することを指定します。

ibm-slapdSslFIPsProcessingMode

サーバーは FIPS モードで動作しているかを指定します。

次の値のいずれかを選択してください。

- **true** は、サーバーが FIPS 処理モードで稼働することを指定します。
- **false** は、サーバーが FIPS 処理モードを非アクティブにすることを指定します。

ibm-slapdSslAuth

セキュア接続用の認証タイプを指定します。

次の値のいずれかを選択してください。

- **serverClientAuth** は、サーバーおよびクライアントの認証をサポートします。
- **serverAuth** は、クライアントでのサーバー認証をサポートします。

ibm-slapdSslCertificate

鍵データベース・ファイル内でサーバーの個人証明書を識別するためのラベルを指定します。

ibm-slapdSslKeyDatabase

LDAP サーバーの鍵データベース・ファイルへのファイル・パスを指定します。

ibm-slapdSslKeyDatabasepw

LDAP サーバーの鍵データベース・ファイルのパスワードを指定します。

セキュア・サーバーを構成するためには、サーバーを FIPS 処理モードで始動したい場合を除き、`ibm-slapdSslFIPsProcessingMode` 属性を `true` に設定しないでください。

IBM Security Directory Server での TLS プロトコルと TLS 開始拡張操作との相違点

ディレクトリー・サーバー環境では、`cn=SSL,cn=Configuration` 項目の `ibm-slapdSecurity` 属性を `SSL`、`SSLOnly`、`SSLTLS`、または `TLS` のいずれかの値に設定することにより、接続を保護できます。

セキュア・ポートを介した TLS プロトコルでの接続を保護するには、`ibm-slapdSecurity` 属性を `SSL` または `SSLOnly` に設定する必要があります。TLS プロトコルでのセキュア接続要求をサーバーに送信するには、`-Z` パラメーターを指定してクライアント・ユーティリティーを実行し、セキュア・ポートを介して接続します。

注: `-Z` パラメーターを指定してクライアント・ユーティリティーを実行し、非セキュア・ポートを介して TLS プロトコルでの要求を送信した場合、要求は失敗します。

非セキュア・ポートを介した TLS開始拡張操作での接続を保護するには、`ibm-slapdSecurity` 属性を `TLS` に設定する必要があります。TLS 開始拡張操作要求をサーバーに送信するには、`-Y` パラメーターを指定してクライアント・ユーティリティーを実行します。`-Y` パラメーターが指定されると、クライアント・ユーテ

イリティーは TLS 開始拡張操作を使用します。サーバーとの接続を保護するために、内部 で TLS プロトコルが使用されます。

注: **-Y** パラメーターを指定してクライアント・ユーティリティーを実行し、セキュア・ポートを介して TLS 開始拡張操作での要求を送信した場合、要求は失敗します。

`ibm-slapdSecurity` 属性を `SSLTLS` に設定した場合、サーバーは TLS プロトコルでも TLS 開始拡張操作でも受け入れることができます。 **-Z** パラメーターを指定してクライアント・ユーティリティーを実行し、セキュア・ポートで接続する場合、サーバーおよびクライアントは TLS プロトコルを使用します。 **-Y** パラメーターを指定してクライアント・ユーティリティーを実行し、非セキュア・ポートで接続する場合、サーバーおよびクライアントは TLS 開始拡張操作を使用します。

SSL および TLS プロトコルを使用したディレクトリー・サーバー・インスタンス :

SSL および TLS プロトコルを使用してディレクトリー・サーバーを構成できます。LDAP 環境でセキュリティ要件を満たすために必要なセキュア通信プロトコルを特定し、設定する必要があります。

ディレクトリー・サーバーをセキュア通信に構成すると、サーバーは SSLv3/TLS 1.0 プロトコル・スイートまたは TLS 開始拡張操作を使用して接続を保護します。

IBM Security Directory Server バージョン 6.3.1 以降では、ディレクトリー・サーバーを、以下のプロトコルを使用してセキュア通信を行うよう構成できます。

- SSLv3
- TLS 1.0
- TLS 1.1
- TLS 1.2

注: TLS 1.1 および TLS 1.2 プロトコルはデフォルトでは無効になっています。

SSLv3、TLS 1.0、TLS 1.1、または TLS 1.2 プロトコル

SSLv3、TLS 1.0、TLS 1.1、TLS 1.2 プロトコル、またはこれらのプロトコルの組み合わせを使用するには、`ibm-slapdSecurityProtocol` 属性に適切な値を設定します。プロトコルを設定する前に、必要なプロトコルの OID がサーバーに含まれているかどうかを確認する必要があります。必要な OID が存在するかどうかを確認するには、検索フィルターとして `ibm-supportedCapabilities` 属性を使用してルート DSE 検索を実行します。

表 14. プロトコルおよび OID 値

プロトコル	<code>ibm-supportedCapabilities</code> 属性に割り当てられた OID 値
TLS 1.0	1.3.18.0.2.32.102
TLS 1.2	1.3.18.0.2.32.103
TLS 1.2	1.3.18.0.2.32.104

複数のセキュア通信プロトコルを設定するには、**idslapdmodify** コマンドを実行して、複数の **ibm-slapdSecurityProtocol** 属性項目およびそのプロトコル値を追加します。**ibm-slapdSecurityProtocol** 属性は、構成ファイル内の **cn=SSL, cn=Configuration DN** 項目の下に追加する必要があります。**ibm-slapdSecurityProtocol** に無効な値を割り当てた場合は、サーバーの始動時にエラーが生成されます。

プロトコルを使用するには、構成ファイル内に適切な暗号を追加します。ディレクトリー・サーバー構成ファイルには、SSLv3、TLS 1.0、および TLS 1.1 プロトコルの暗号がデフォルトで存在します。TLS 1.2 プロトコルの場合、構成ファイルには TLS 1.2 でサポートされる暗号は含まれていません。**ibm-slapdSslCipherSpec** 属性を複数回追加することにより、プロトコルに対して複数の暗号を追加できます。構成ファイルの **cn=SSL, cn=Configuration** 項目の下に適切な暗号を追加してください。プロトコルの暗号が構成ファイルに設定されていない場合は、サーバーの始動時にエラーが生成されます。サポートされるプロトコルおよび暗号については、197 ページの『バージョン 6.3、フィックスパック 17 以降におけるプロトコルおよび暗号』を参照してください。

ibm-slapdSslCipherSpec に無効な暗号を割り当てた場合は、サーバーの始動時にエラーが生成されます。例えば、**ibm-slapdSslCipherSpec** 属性を追加し、値 **HELLO** を指定すると、サーバーは以下のエラーを生成して終了します。

```
GLPSSL009E An incorrect value of HELLO was given for the SSL cipher specification.
```

TLS 1.1 プロトコルの場合、ディレクトリー・サーバーでは構成ファイルにある 8 つの暗号のうち、6 つの暗号がサポートされます。RC4-40-MD5 暗号および RC2-40-MD5 暗号は、TLS 1.1 プロトコルを使用するサーバーではサポートされません。RC4-40-MD5 暗号および RC2-40-MD5 暗号のみを設定し、TLS 1.1 プロトコルを使用してサーバーを構成した場合、サーバーはエラーを生成して終了します。

TLS 1.2 プロトコルのみを使用するようにディレクトリー・サーバーを構成すると、その他のすべてのプロトコル (SSLv3、TLS 1.0、TLS 1.1 など) は無効になります。TLS 1.2 プロトコルのみを使用してサーバーを構成すると、構成ファイル内にある、SSLv3、TLS 1.0、または TLS 1.1 でサポートされる暗号はディレクトリー・サーバーでは無視されます。

プロトコルを使用してサーバーを正常に設定した場合、ルート DSE 検索を実行すると、**ibm-enabledCapabilities** 属性内のプロトコルに関連付けられた **OID** が表示されます。

表 15. **ibm-slapdSecurityProtocol** 属性、**ibm-slapdSecurity** 属性、セキュア通信モード、パラメーター、およびポートの関係

ibm-slapdSecurityProtocol の値	ibm-slapdSecurity の値	セキュア通信のモード	-Z オプションによるセキュア・ポート	-Y オプションによる非セキュア・ポート
SSLV3	SSL SSLonly	SSLv3 プロトコル	はい	いいえ
	SSLTLS	SSLv3 プロトコル	はい	いいえ
	TLS	TLS 始動の拡張操作	いいえ	いいえ
	SSLTLS	TLS 始動の拡張操作	いいえ	いいえ

表 15. *ibm-slapdSecurityProtocol* 属性、*ibm-slapdSecurity* 属性、セキュア通信モード、パラメーター、およびポートの関係 (続き)

<i>ibm-slapdSecurityProtocol</i> の値	<i>ibm-slapdSecurity</i> の値	セキュア通信のモード	-Z オプションによるセキュア・ポート	-Y オプションによる非セキュア・ポート
TLS10	SSL SSLOnly	TLS 1.0 プロトコル	はい	いいえ
	SSLTLS	TLS 1.0 プロトコル	はい	いいえ
	TLS	TLS 始動の拡張操作	いいえ	はい
	SSLTLS	TLS 始動の拡張操作	いいえ	はい
TLS11	SSL SSLOnly	TLS 1.1 プロトコル	はい	いいえ
	SSLTLS	TLS 1.1 プロトコル	はい	いいえ
	TLS	TLS 始動の拡張操作	いいえ	はい
	SSLTLS	TLS 始動の拡張操作	いいえ	はい
TLS12	SSL SSLOnly	TLS 1.2 プロトコル	はい	いいえ
	SSLTLS	TLS 1.2 プロトコル	はい	いいえ
	TLS	TLS 始動の拡張操作	いいえ	はい
	SSLTLS	TLS 始動の拡張操作	いいえ	はい

旧バージョンの *GSKit* で作成された鍵データベース・ファイルを使用するディレクトリー・サーバーは、TLS 1.2 プロトコルで動作する場合があります。サポートされる TLS 1.2 の暗号のうち、以下の条件を満たしている暗号が、既存の証明書で機能します。

- 証明書と暗号の公開鍵に互換性がある。
- 証明書と暗号の署名およびハッシュ・アルゴリズムに互換性がある。

証明書の変更が必要となるシナリオは、以下のとおりです。

- 既存の証明書の公開鍵と比べて、異なる公開鍵で暗号を使用する場合。
- NIST SP 800-131A ガイドラインを満たす署名およびハッシュ・アルゴリズムを使用する場合。

既存の証明書が SP 800-131A 要件を満たさない場合は、要件を満たす証明書を取得します。

詳しくは、「*GSKCapiCmd Users Guide*」の鍵データベース、証明書、および認証要求についての章を参照してください。「*GSKCapiCmd Users Guide*」は、IBM Security Access Manager for Web 資料の Web サイトからダウンロードできます。

注: NIST SP 800-131A ガイドラインを満たす証明書が含まれる鍵データベース・ファイルを使用してサーバーを構成すると、サーバーは TLS 1.2 プロトコルによる接続を保護するために、より多くの処理を行います。したがって、サーバーが TLS 1.2 プロトコルによる接続を保護するために要する処理時間も長くなる可能性があります。

ディレクトリー・サーバーの始動メッセージ、ログ・メッセージ、および *rootDSE* の結果

ディレクトリー・サーバーに対してプロトコルを設定しない場合、サーバーはデフォルト・プロトコルをセキュア通信に使用します。以下のメッセージは、サーバーがセキュア通信に構成された場合に設定されるデフォルト・プロトコルを示します。

```
GLPSSL039I Secure communication using the SSLV3 protocol is enabled.
GLPSSL039I Secure communication using the TLS10 protocol is enabled.
```

このメッセージは、サーバーの始動時に表示されます。メッセージは、ディレクトリー・サーバー・インスタンスの `ibmslapd.log` ファイルにも記録されます。

AIX、Linux、および Solaris システムの場合

`ibmslapd.log` ファイルのデフォルトの場所は、`instance_home/idsslapd-instance_name/logs` ディレクトリーです。

Windows システムの場合

`ibmslapd.log` ファイルのデフォルトの場所は、`drive%idsslapd-instance_name%logs` ディレクトリーです。

ディレクトリー・サーバーで `ibm-slapdSecurityProtocol` に `SSLV3,TLS10,TLS11,TLS12` 値を設定した場合は、以下のメッセージが表示されます。

```
GLPSSL039I Secure communication using the SSLV3 protocol is enabled.
GLPSSL039I Secure communication using the TLS10 protocol is enabled.
GLPSSL039I Secure communication using the TLS11 protocol is enabled.
GLPSSL039I Secure communication using the TLS12 protocol is enabled.
```

プロトコルおよび暗号に関する詳細メッセージを確認するには、サーバーのトレース・メッセージを調べる必要があります。

`rootDSE` の結果で `ibm-slapdSecurityProtocol` 属性を照会することにより、サーバーに設定されているセキュア通信プロトコルを確認できます。

例

例 1: ディレクトリー・サーバーがセキュア通信に構成されているかどうかを確認するには、以下のコマンドを実行します。

```
idsldapsearch -h server.com -p port -s base -b "" objectclass=* security
security=none
```

`security` 属性が `none` の場合、サーバーはセキュア通信に構成されていません。

例 2: FIPS 処理モードでディレクトリー・サーバーを構成するには、`ldapmodify` コマンドを実行します。以下に例を示します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSs1FIPsProcessingMode
ibm-slapdSs1FIPsProcessingMode: true
```

セキュア・サーバーを構成するときは、サーバーを FIPS 処理モードで始動したい場合を除き、`ibm-slapdSs1FIPsProcessingMode` 属性を `true` に設定しないでください。

注: 変更内容を適用するには、Directory Server と管理サーバーを再起動する必要があります。

例 3: サーバーが FIPS 処理モードであるかどうかを確認するには、サーバーに対して `idsldapsearch` コマンドを実行して、ルート DSE の結果を取得します。以下に例を示します。

```
idsldapsearch -h server.com -p port -s base -b "" objectclass=*%
ibm-ssl1fipsprocessingmode
ibm-ssl1fipsprocessingmode=ON
```

ibm-slapdSecurity 属性が SSL、SSLOnly、または SSLTLS に設定された場合は、ibm-sslfpipsprocessingmode 属性がリストされます。

ibm-slapdSecurity 属性が TLS に設定された場合、ibm-sslfpipsprocessingmode 属性は検索結果にリストされません。

- 例 4:** サーバーがセキュア通信でサポートしているプロトコルを確認するには、**ldapsearch** コマンドを実行して、ルート DSE の結果を取得します。この検索結果で、ibm-slapdSecurityProtocol 属性値を調べてください。

```
idsldapsearch -p port -s base -b "" objectclass=* ibm-slapdSecurityProtocol
ibm-slapdSecurityProtocol=SSLV3,TLS10
```

管理サーバーがサポートするセキュア通信プロトコルを確認するには、**ldapsearch** コマンドを実行して、ルート DSE の結果を取得します。この検索結果で、admindaemon-securityprotocol 属性値を調べてください。

```
idsldapsearch -p admin_port -s base -b "" objectclass=* admindaemon-securityprotocol
admindaemon-securityprotocol=SSLV3,TLS10
```

セキュア通信プロトコルを使用するディレクトリー・サーバーに ibm-slapdSecurityProtocol 属性が設定されていない場合は、デフォルト・プロトコル値 SSLV3,TLS10 が設定されます。

- 例 5:** サーバーがサポートする暗号をサーバー・トレースから確認することもできます。サーバー・トレース・ファイルで、キーワード *cipher* を調べてください。サーバー・トレースを取得するには、以下のコマンドを実行します。

```
#ldtrc on
#ibmslapd -h 65536 -I dsrdbm01 2>&1 | tee server_trace.txt
```

- 例 6:** ハンドシェイクで使用される暗号を確認するには、使用するオペレーティング・システムに応じて以下のアクションを実行します。

AIX、Linux、Solaris、および HP-UX

1. ksh または bash シェルを開きます。
2. 以下のコマンドを実行します。

```
export LDAP_DEBUG=65535
export LDAP_DEBUG_FILE=/tmp/ldapclient_trace.out

idsldapsearch -h server -p port -Z -K key.kdb ¥
-P kPWD -s base -b "" objectclass=* security
```

Microsoft Windows

1. コマンド・プロンプトにアクセスします。
2. 以下のコマンドを実行します。

```
set LDAP_DEBUG=65535
set LDAP_DEBUG_FILE=c:\¥ldapclient_trace.out

idsldapsearch -h server -p port -Z -K key.kdb -P kPWD
-s base -b "" objectclass=* security
```

セキュリティー・プロトコルおよび暗号によるディレクトリー・サーバーの構成:

LDAP 環境のセキュリティー要件を満たすために必要なプロトコルを使用してディレクトリー・サーバーを構成します。

始める前に

セキュア通信用の鍵データベース・ファイルおよび証明書を作成します。

詳しくは、「*GSKCapiCmd Users Guide*」の鍵データベース、証明書、および認証要求についての章を参照してください。「*GSKCapiCmd Users Guide*」は、IBM Security Access Manager for Web 資料の Web サイトからダウンロードできます。

ディレクトリー・サーバー・インスタンス所有者の鍵データベース・ファイル、証明書、およびファイル・パスに対して必要な許可 (rwx) を設定します。

このタスクについて

SSL および TLS プロトコル、または TLS 開始拡張操作を使用したセキュア接続を受け入れるようにディレクトリー・サーバーを構成できます。

複数のプロトコルを使用してディレクトリー・サーバーを構成するには、`ibm-slapdSecurityProtocol` 属性および必要な値を複数回追加します。

手順

1. インスタンス所有者としてログインします。
2. セキュア通信用にディレクトリー・サーバーを構成するには、`idsldapmodify` コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i config_file.ldif
```

`config_file.ldif` ファイルには、以下の項目が格納されています。

```
dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslAuth
ibm-slapdSslAuth: serverClientAuth

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSecurity
ibm-slapdSecurity: SSLTLS

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabase
ibm-slapdSslKeyDatabase: /home/dsrdbm01/keys/serverkey.kdb

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslCertificate
ibm-slapdSslCertificate: serverlabel

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabasepw
ibm-slapdSslKeyDatabasepw: keyfilePWD
```

3. 必要なプロトコルを使用してディレクトリー・サーバーを構成します。
 - TLS 1.2 プロトコルを設定するには、`idsldapmodify` コマンドを以下の形式で実行します。

```
idsldapmodify -h host_name -p port -D adminDN -w adminPWD
dn: cn=SSL, cn=Configuration
changetype: modify
add: ibm-slapdSecurityProtocol
ibm-slapdSecurityProtocol: TLS12
```

- SSLv3、TLS 1.0、TLS 1.1、および TLS 1.2 プロトコルを設定するには、`idsldapmodify` コマンドを以下の形式で実行します。

```
idsldapmodify -h host_name -p port -D adminDN -w adminPWD
dn: cn=SSL, cn=Configuration
changetype: modify
add: ibm-slapdSecurityProtocol
ibm-slapdSecurityProtocol: SSLV3
-
add: ibm-slapdSecurityProtocol
ibm-slapdSecurityProtocol: TLS10
-
add: ibm-slapdSecurityProtocol
```

```
ibm-slapdSecurityProtocol: TLS11
-
add: ibm-slapdSecurityProtocol
ibm-slapdSecurityProtocol: TLS12
```

4. TLS 1.2 プロトコルに対してサポートされる暗号を追加するため、**idsldapmodify** コマンドを以下の形式で実行します。

```
idsldapmodify -p port -D adminDN -w adminPWD -i TLS12cipher_file.ldif
```

TLS12cipher_file.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=SSL,cn=Configuration
changetype: modify
add: ibm-slapdSslCipherSpec
ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_CBC_SHA256
-
add: ibm-slapdSslCipherSpec
ibm-slapdSslCipherSpec: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
-
add: ibm-slapdSslCipherSpec
ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
-
add: ibm-slapdSslCipherSpec
ibm-slapdSslCipherSpec: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

5. ディレクトリー・サーバーおよび管理サーバーを再始動します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
ibmslapd -I dsrdbm01 -n
ibmdiradm -I dsrdbm01
```

例

- 例 1:** ディレクトリー・サーバーがサポートするセキュア通信プロトコルを確認するには、**ldapsearch** コマンドを実行して、ルート DSE の結果を取得します。この検索結果で、**ibm-slapdSecurityProtocol** 属性値を調べてください。

```
idsldapsearch -p port -s base -b "" objectclass=* ibm-slapdSecurityProtocol
ibm-slapdSecurityProtocol=SSLV3,TLS10,TLS11,TLS12
```

管理サーバーがサポートするセキュア通信プロトコルを確認するには、**ldapsearch** コマンドを実行して、ルート DSE の結果を取得します。この検索結果で、**admindaemon-securityprotocol** 属性値を調べてください。

```
idsldapsearch -p admin_port -s base -b "" objectclass=* admindaemon-securityprotocol
admindaemon-securityprotocol=SSLV3,TLS10,TLS11,TLS12
```

サーバーに複数のセキュア通信プロトコルが設定されている場合、**ibm-slapdSecurityProtocol** 属性および **admindaemon-securityprotocol** 属性には、コンマで区切られたプロトコルが示されます。

- 例 2:** **ibm-slapdSecurityProtocol** が **SSLV3,TLS10,TLS11** に設定されている場合に、サーバーがセキュア通信でサポートしている暗号を確認するには、**ldapsearch** コマンドを実行して、ルート DSE の結果を取得します。この検索結果で、**ibm-sslcpiphers** 属性値を調べてください。

```
idsldapsearch -p port -s base -b "" objectclass=* ibm-sslcpiphers
ibm-sslcpiphers=352F04050A090306
```

ibm-slapdSecurityProtocol が **SSLV3,TLS10,TLS11** に設定されている場合に、管理サーバーがセキュア通信でサポートしている暗号を確認するには、**ldapsearch** コマンドを実行して、ルート DSE の結果を取得します。この検索結果で、**admindaemon-sslcpiphers** 属性値を調べてください。

```
idsldapsearch -p adm_port -D adminDN -w adminPWD -s base -b "" ¥
objectclass=* admindaemon-sslcpiphers
```

```
admindaemon-sslcpiphers=352F04050A090306
```

この出力で、`ibm-sslcpiphers` 属性および `admindaemon-sslcpiphers` 属性には、SSLv3、TLS 1.0、および TLS 1.1 プロトコルについて構成ファイル内にあるすべての暗号の 16 進値が含まれます。SSLv3、TLS 1.0、および TLS 1.1 の暗号は、暗号の 16 進値を連結することによって示されます。

`ibm-slapdSecurity` 属性が SSL、SSLOnly、または SSLTLS に設定された場合は、`ibm-sslcpiphers` 属性および `admindaemon-sslcpiphers` 属性が示されます。`ibm-slapdSecurity` 属性が TLS に設定された場合、検索結果には `ibm-sslcpiphers` 属性および `admindaemon-sslcpiphers` 属性は示されません。

例 3: `ibm-slapdSecurityProtocol` が TLS12 に設定されている場合に、サーバーがセキュア通信でサポートしている暗号を確認するには、`ldapsearch` コマンドを実行して、ルート DSE の結果を取得します。この検索結果で、`ibm-tlsciphers` 属性の値を調べてください。

```
idsldapsearch -p port -s base -b "" objectclass=* ibm-tlsciphers
```

```
ibm-tlsciphers=TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

`ibm-slapdSecurityProtocol` が TLS12 に設定されている場合に、管理サーバーがセキュア通信でサポートしている暗号を確認するには、`ldapsearch` コマンドを実行して、ルート DSE の結果を取得します。この検索結果で、`admindaemon-tlsciphers` 属性の値を調べてください。

```
idsldapsearch -p adm_port -D adminDN -w adminPWD -s base -b "" ¥
objectclass=* admindaemon-tlsciphers
```

```
admindaemon-tlsciphers=TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

この出力の `ibm-tlsciphers` 属性および `admindaemon-tlsciphers` 属性には、TLS 1.2 プロトコルの暗号が示されます。TLS 1.2 暗号は、コンマ区切りの文字列として示されます。

注: 構成ファイル内で `ibm-slapdSecurity` 属性値が SSL、SSLOnly、または SSLTLS に設定された場合は、`ibm-tlsciphers` 属性および `admindaemon-tlsciphers` 属性が示されます。`ibm-slapdSecurity` 属性が TLS に設定された場合、検索結果にはこの属性および暗号値は示されません。

Web 管理ツールを使用したプロトコルおよび暗号によるディレクトリー・サーバーの構成:

Web 管理ツールを使用すると、LDAP 環境のセキュリティー要件を満たすために必要なセキュリティー・プロトコルを使用してディレクトリー・サーバーを構成できます。

始める前に

セキュア通信の鍵データベース・ファイルおよび証明書を作成します。

詳しくは、「*GSKCapiCmd Users Guide*」の鍵データベース、証明書、および認証要求についての章を参照してください。「*GSKCapiCmd Users Guide*」は、IBM Security Access Manager for Web 資料の Web サイトからダウンロードできます。

ディレクトリー・サーバー・インスタンス所有者の鍵データベース・ファイル、証明書、およびファイル・パスに対して必要な許可 (rwx) を設定します。

手順

1. Web 管理ツールにディレクトリー・サーバー管理者としてログインします。
2. ナビゲーション領域で、「**サーバー管理**」 > 「**セキュリティ・プロパティの管理**」を展開し、「**設定**」をクリックします。
3. 「**設定**」パネルで、接続タイプ、認証方式、およびセキュア通信プロトコルを指定します。
 - a. セキュア・ポートおよび非セキュア・ポートでの接続を受け入れるため、「**SSL および TLS**」をクリックします。
 - b. セキュア通信プロトコルを設定するには、必要なプロトコルを選択します。
 - c. サーバーおよびクライアントの認証方式を有効にするには、「**サーバーおよびクライアントの認証**」をクリックします。
 - d. 「**適用**」をクリックします。
4. 「**セキュリティ・プロパティの管理**」で、「**暗号化**」をクリックします。
 - a. セキュア通信プロトコルに必要な暗号を選択します。
 - b. 「**適用**」をクリックします。
5. 「**セキュリティ・プロパティの管理**」で、「**鍵データベース**」をクリックします。
6. 「**鍵データベース**」パネルで、鍵データベース・ファイルおよびパスワードを指定します。
 - a. 「**鍵データベースのパスおよびファイル名**」フィールドに、鍵データベース・ファイルの名前を絶対パス名で入力します。
 - b. 「**鍵パスワード**」フィールドに、鍵データベース・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、鍵データベース・パスワードを入力します。
 - d. 「**鍵ラベル**」フィールドに、証明書を一意的に識別するラベルを入力します。
 - e. 「**適用**」をクリックします。
7. 「**OK**」をクリックします。
8. ナビゲーション領域で、「**サーバー管理**」 > 「**サーバーの始動/停止/再始動**」を展開し、「**再始動**」をクリックします。
9. ディレクトリー・サーバー・インスタンスが存在するコンピューターにアクセスします。
10. インスタンス所有者としてログインします。
11. 管理サーバーを再始動します。

```
ibmdiradm -I dsrdbm01 -k  
ibmdiradm -I dsrdbm01
```

バージョン 6.3、フィックスパック 17 以降におけるプロトコルおよび暗号:

IBM Security Directory Server バージョン 6.3 フィックスパック 17 以降で、セキュア通信のサポート対象プロトコルおよび暗号を使用します。

サーバー/クライアント環境でのセキュア通信では、以下のプロトコルがサポートされています。

- SSLv3
- TLS 1.0
- TLS 1.1
- TLS 1.2

サーバー/クライアント環境でのセキュア通信では、以下の暗号がサポートされています。

表 16. SSLv3、TLS 1.0、および TLS 1.1 プロトコルでのサポートされる暗号および TLS 1.0 および TLS 1.1 プロトコルでの FIPS 承認済み暗号

ibmslapd.conf ファイル内の暗号	16 進値	SSLv3 および TLS 1.0 プロトコルのサポート対象	TLS 1.1 プロトコルのサポート対象	TLS 1.0 および TLS 1.1 プロトコル用の FIPS 承認済み暗号
RC4-40-MD5	03	はい	いいえ	いいえ
RC4-128-MD5	04	はい	はい	いいえ
RC4-128-SHA	05	はい	はい	いいえ
RC2-40-MD5	06	はい	いいえ	いいえ
DES-56	09	はい	はい	いいえ
TripleDES-168	0A	はい	はい	はい
AES-128	2F	はい	はい	はい
AES	35	はい	はい	はい

表 17. サーバーによりサポートされる TLS 1.2 暗号、FIPS 承認済み TLS 1.2 暗号、およびクライアント・ユーティリティによりサポートされるデフォルトの TLS 1.2 暗号

サーバーによりサポートされる TLS 1.2 暗号	FIPS 承認済み TLS 1.2 暗号	クライアント・ユーティリティによりサポートされるデフォルトの TLS 1.2 暗号
TLS_RSA_WITH_RC4_128_SHA	いいえ	いいえ
TLS_RSA_WITH_3DES_EDE_CBC_SHA	はい	はい
TLS_RSA_WITH_AES_128_CBC_SHA	はい	はい
TLS_RSA_WITH_AES_256_CBC_SHA	はい	はい
TLS_RSA_WITH_AES_128_GCM_SHA256	はい	はい
TLS_RSA_WITH_AES_256_GCM_SHA384	はい	はい
TLS_RSA_WITH_AES_128_CBC_SHA256	はい	はい
TLS_RSA_WITH_AES_256_CBC_SHA256	はい	はい
TLS_ECDHE_RSA_WITH_RC4_128_SHA	いいえ	いいえ
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	はい	いいえ
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	はい	いいえ
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	はい	いいえ
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	はい	はい
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	はい	はい
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	はい	はい
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	はい	はい
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	いいえ	いいえ
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	はい	いいえ
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	はい	はい
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	はい	はい
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	はい	はい
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	はい	はい

表 17. サーバーによりサポートされる TLS 1.2 暗号、FIPS 承認済み TLS 1.2 暗号、およびクライアント・ユーティリティによりサポートされるデフォルトの TLS 1.2 暗号 (続き)

サーバーによりサポートされる TLS 1.2 暗号	FIPS 承認済み TLS 1.2 暗号	クライアント・ユーティリティによりサポートされるデフォルトの TLS 1.2 暗号
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	はい	はい
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	はい	はい
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	はい	はい

バージョン 6.3.0.15 または旧バージョンにおけるプロトコルおよび暗号:

IBM Security Directory Server バージョン 6.3.0.15 または旧バージョンのディレクトリー・サーバーおよびクライアント環境で、セキュア通信用のサポート対象プロトコルおよび暗号を使用します。

IBM Security Directory Server バージョン 6.3.0.15 または旧バージョンにおけるサーバーとクライアントとの間のセキュア通信では、以下のプロトコルがサポートされます。

- SSLv3/TLS 1.0 プロトコル・スイート

IBM Security Directory Server バージョン 6.3.0.15 または旧バージョンにおけるサーバーとクライアントとの間のセキュア通信では、以下の暗号がサポートされません。

表 18. SSLv3/TLS 1.0 プロトコル・スイートでサポートされる暗号および TLS 1.0 プロトコルの FIPS 承認済み暗号

ibmslapd.conf ファイル内の暗号	16 進値	SSLv3/TLS 1.0 プロトコル・スイートのサポート対象	TLS 1.0 プロトコル用の FIPS 承認済み暗号
RC4-40-MD5	03	はい	いいえ
RC4-128-MD5	04	はい	いいえ
RC4-128-SHA	05	はい	いいえ
RC2-40-MD5	06	はい	いいえ
DES-56	09	はい	いいえ
TripleDES-168	0A	はい	はい
AES-128	2F	はい	はい
AES	35	はい	はい

TLS 1.2 署名およびハッシュ・アルゴリズム:

TLS 1.2 署名およびハッシュ・アルゴリズムを使用して、通信を、署名およびハッシュ・アルゴリズム基準を満たす TLS 1.2 プロトコルおよび証明書に制限することができます。

TLS 1.2 署名およびハッシュ・アルゴリズムの制限を設定すると、サーバーはチェーン内のクライアント証明書が、指定された設定に準拠しているかどうかを検証します。クライアント証明書が設定された制約を満たさない場合、通信は失敗します。

TLS 1.2 署名付きでありハッシュ・アルゴリズムの制限が設定された IBM Security Directory Server を使用するには、以下の作業を行う必要があります。

- IBM Global Security Kit バージョン 8.0.14.24 以降をインストールします。

- セキュア・ポートでの接続を受け入れるようにサーバーを構成します。
ibm-slapdSecurity 属性を SSL、SSLOnly、または SSLTLS に設定します。
- TLS 1.2 プロトコルを使用したセキュア・ポートでの通信用にサーバーを構成します。
- 必要な TLS 1.2 暗号を構成します。
- 構成ファイルの cn=SSL, cn=Configuration 項目の下に、ibm-slapdSSExtSigalg 属性および適切な値を追加します。複数の TLS 1.2 署名およびハッシュ・アルゴリズム値を設定するには、構成ファイルに複数の ibm-slapdSSExtSigalg 属性項目を追加する必要があります。属性値が有効な TLS 1.2 署名およびハッシュ・アルゴリズムでない場合、サーバーはエラーを生成し、構成専用モードで始動します。

以下の TLS 1.2 署名およびハッシュ・アルゴリズムがサポートされます。

```
GSK_TLS_SIGALG_RSA_WITH_SHA224
GSK_TLS_SIGALG_RSA_WITH_SHA256
GSK_TLS_SIGALG_RSA_WITH_SHA384
GSK_TLS_SIGALG_RSA_WITH_SHA512
GSK_TLS_SIGALG_ECDSA_WITH_SHA224
GSK_TLS_SIGALG_ECDSA_WITH_SHA256
GSK_TLS_SIGALG_ECDSA_WITH_SHA384
GSK_TLS_SIGALG_ECDSA_WITH_SHA512
```

TLS 1.2 署名およびハッシュ・アルゴリズムを使用してディレクトリー・サーバーを構成した後、ディレクトリー・サーバーおよび管理サーバーに対してルート DSE 検索を実行し、設定を確認します。

表 19. ディレクトリー・サーバーおよび管理サーバーに設定されている TLS 1.2 署名およびハッシュ・アルゴリズムについてのルート DSE 検索の結果

サーバー	ルート DSE の結果の値
ディレクトリー・サーバー	ibm-slapdSSExtSigalg=GSK_TLS_SIGALG_RSA_WITH_SHA224, GSK_TLS_SIGALG_RSA_WITH_SHA256,GSK_TLS_SIGALG_RSA_WITH_SHA384, GSK_TLS_SIGALG_RSA_WITH_SHA512,GSK_TLS_SIGALG_ECDSA_WITH_SHA224, GSK_TLS_SIGALG_ECDSA_WITH_SHA256,GSK_TLS_SIGALG_ECDSA_WITH_SHA384, GSK_TLS_SIGALG_ECDSA_WITH_SHA512
管理サーバー	admindaemon-sslsextsigalg=GSK_TLS_SIGALG_RSA_WITH_SHA224, GSK_TLS_SIGALG_RSA_WITH_SHA256,GSK_TLS_SIGALG_RSA_WITH_SHA384, GSK_TLS_SIGALG_RSA_WITH_SHA512,GSK_TLS_SIGALG_ECDSA_WITH_SHA224, GSK_TLS_SIGALG_ECDSA_WITH_SHA256,GSK_TLS_SIGALG_ECDSA_WITH_SHA384, GSK_TLS_SIGALG_ECDSA_WITH_SHA512

注:

- TLS 1.2 署名およびハッシュ・アルゴリズムの制限を使用してサーバーを構成した場合、サーバーはセキュア・ポートでのみ listen します。
- サーバーが TLS 1.2 プロトコルで通信するように構成されていない場合、構成ファイル内の ibm-slapdSSExtSigalg 属性は無視されます。サーバーは、既存の設定を使用します。

TLS 1.2 署名およびハッシュ・アルゴリズムの制限の構成:

サーバーで TLS 1.2 署名およびハッシュ・アルゴリズムの制限を構成して、通信を、指定された基準を満たす TLS 1.2 プロトコルおよび証明書に制限します。

始める前に

セキュア通信用の鍵データベース・ファイルおよび証明書を作成します。

詳しくは、「*GSKCapiCmd Users Guide*」の鍵データベース、証明書、および認証要求についての章を参照してください。「*GSKCapiCmd Users Guide*」は、IBM Security Access Manager for Web 資料の Web サイトからダウンロードできます。

ディレクトリー・サーバー・インスタンス所有者の鍵データベース・ファイル、証明書、およびファイル・パスに対して必要な許可 (rwx) を設定します。

手順

1. インスタンス所有者としてログインします。
2. サーバーをセキュア通信用に構成し、TLS 1.2 暗号を設定するには、**idsldapmodify** コマンドを実行します。

```
idsldapmodify -h host_name -p port -D adminDN -w adminPWD -i sign_config.ldif
```

sign_config.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslAuth
ibm-slapdSslAuth: serverClientAuth

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSecurity
ibm-slapdSecurity: SSL

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabase
ibm-slapdSslKeyDatabase: /home/dsrdbm01/keys/serverkey.kdb

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslCertificate
ibm-slapdSslCertificate: serverlabel

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabasepw
ibm-slapdSslKeyDatabasepw: keyfilePWD

dn: cn=SSL, cn=Configuration
changetype: modify
add: ibm-slapdSslCipherSpec
ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_CBC_SHA256

dn: cn=SSL, cn=Configuration
changetype: modify
add: ibm-slapdSslCipherSpec
ibm-slapdSslCipherSpec: TLS_RSA_WITH_AES_256_GCM_SHA384
```

3. サーバーに TLS 1.2 プロトコルを設定するには、**idsldapmodify** コマンドを実行します。

```
idsldapmodify -h host_name -p port -D adminDN -w adminPWD
dn: cn=SSL, cn=Configuration
changetype: modify
add: ibm-slapdSecurityProtocol
ibm-slapdSecurityProtocol: TLS12
```

4. TLS 1.2 署名およびハッシュ・アルゴリズムの制限を設定するには、**idsldapmodify** コマンドを実行します。

```
idsldapmodify -h host_name -p port -D adminDN -w adminPWD
dn: cn=SSL, cn=Configuration
changetype: modify
add: ibm-slapdSslExtSigalg
ibm-slapdSslExtSigalg: GSK_TLS_SIGALG_RSA_WITH_SHA256
-
add: ibm-slapdSslExtSigalg
ibm-slapdSslExtSigalg: GSK_TLS_SIGALG_RSA_WITH_SHA384
```

5. ディレクトリー・サーバーおよび管理サーバーを再始動します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
ibmslapd -I dsrdbm01 -n
ibmdiradm -I dsrdbm01
```

例

例 1 TLS 1.2 署名およびハッシュ・アルゴリズムが設定されているかどうかを確認するには、**idsldapsearch** コマンドを実行して、ルート DSE の結果を取得します。

ディレクトリー・サーバーに対してルート DSE 検索を実行する:

```
idsldapsearch -p port -s base -b "" objectclass=* ibm-slappdSSExtSigalg  
ibm-slappdSSExtSigalg=GSK_TLS_SIGALG_RSA_WITH_SHA256,  
GSK_TLS_SIGALG_RSA_WITH_SHA384
```

管理サーバーに対してルート DSE 検索を実行する:

```
idsldapsearch -p admin_port -s base -b "" objectclass=*  
admindaemon-sslsextsigalg  
admindaemon-sslsextsigalg=GSK_TLS_SIGALG_RSA_WITH_SHA256,  
GSK_TLS_SIGALG_RSA_WITH_SHA384
```

Web 管理ツールを使用した TLS 1.2 署名およびハッシュ・アルゴリズムの制限の構成:

Web 管理ツールを使用して、TLS 1.2 署名およびハッシュ・アルゴリズムの制限が設定されたディレクトリー・サーバーを構成することができます。

始める前に

TLS 1.2 署名およびハッシュ・アルゴリズムの制限に必要な鍵データベース・ファイルおよび証明書を作成します。

詳しくは、「*GSKCapiCmd Users Guide*」の鍵データベース、証明書、および認証要求についての章を参照してください。「*GSKCapiCmd Users Guide*」は、IBM Security Access Manager for Web 資料の Web サイトからダウンロードできます。

ディレクトリー・サーバー・インスタンス所有者の鍵データベース・ファイル、証明書、およびファイル・パスに対して必要な許可 (rwx) を設定します。

手順

1. Web 管理ツールにディレクトリー・サーバー管理者としてログインします。
2. ナビゲーション領域で、「サーバー管理」 > 「セキュリティ・プロパティの管理」を展開し、「設定」をクリックします。
3. 「設定」パネルで、接続タイプ、認証方式、およびセキュア・プロトコルを指定します。
 - a. セキュア・ポートおよび非セキュア・ポートでの接続を受け入れるには、「SSL」をクリックします。
 - b. サーバーおよびクライアントの認証方式を有効にするには、「サーバーおよびクライアントの認証」をクリックします。
 - c. セキュア通信プロトコルを設定するには、「TLS 1.2」を選択します。
 - d. 「適用」をクリックします。
4. 「セキュリティ・プロパティの管理」で、「暗号化」をクリックします。
 - a. TLS 1.2 プロトコルに必要な暗号を選択します。
 - b. 「適用」をクリックします。
5. 「セキュリティ・プロパティの管理」で、「鍵データベース」をクリックします。

6. 「鍵データベース」パネルで、鍵データベース・ファイル、パスワード、および鍵ラベルを指定します。
 - a. 「鍵データベースのパスおよびファイル名」フィールドに、鍵データベース・ファイルの名前を絶対パス名で入力します。
 - b. 「鍵パスワード」フィールドに、鍵データベース・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、鍵データベース・パスワードを入力します。
 - d. 「鍵ラベル」フィールドに、証明書を一意的に識別するラベルを入力します。
 - e. 「適用」をクリックします。
7. 「セキュリティー・プロパティーの管理」で、「署名アルゴリズム」をクリックします。
 - a. ディレクトリー・サーバーに設定する TLS 1.2 署名およびハッシュ・アルゴリズムを選択します。
 - b. 「適用」をクリックします。
8. 「OK」をクリックします。
9. ナビゲーション領域で、「サーバー管理」 > 「サーバーの始動/停止/再始動」を展開し、「再始動」をクリックします。
10. ディレクトリー・サーバー・インスタンスが稼働しているコンピューターにアクセスします。
11. インスタンス所有者としてログインします。
12. 管理サーバーを再始動します。

```
ibmdiradm -I dsrdbm01 -k
ibmdiradm -I dsrdbm01
```

Suite B モード:

ディレクトリー・サーバーで Suite B モードを構成して、LDAP 環境のセキュリティー要件を拡張することができます。

Suite B モードは、NIST SP 800-131A 規格の限定的なサブセットです。Suite B では、Transport Layer Security (TLS) 1.2 プロトコル・バージョンと共に使用する暗号アルゴリズム・ポリシーが定義されます。

サーバーで Suite B を構成するには、サーバーに Suite B モードの OID が含まれていなければなりません。サーバーが Suite B モードをサポートしている場合は、ルート DSE 検索を実行すると、ibm-supportedCapabilities 属性には OID 値 1.3.18.0.2.32.101 が返されます。

Suite B モードでディレクトリー・サーバーを構成するには、以下の条件を満たしている必要があります。

- IBM Global Security Kit バージョン 8.0.14.24 以降をインストールします。
- セキュア・ポートでの接続を受け入れるように Directory Server を構成してください。ibm-slapdSecurity 属性を SSL、SSLOnly、または SSLTLS に設定します。
- ibm-slapdSslFIPSMoDeEnabled 属性を true に設定します。

Suite B モードでサーバーを構成すると、セキュア通信は以下のプロトコル、暗号、証明書、署名およびハッシュ・アルゴリズムに制限されます。

プロトコル

TLS 1.2 プロトコルが Suite B モードでサポートされる唯一のプロトコルです。

公開鍵 証明書の公開鍵は、最小サイズ EC 256 ビットでなければなりません。

署名アルゴリズム

証明書の署名アルゴリズムは、最小サイズ ECDSA 256 ビット (曲線 P256) および SHA256 でなければなりません。

ハッシュ・アルゴリズム

ハッシュ・アルゴリズムの最小サイズは SHA256 でなければなりません。

暗号仕様

Suite B モードでは以下の暗号がサポートされます。

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

重要: より強い署名およびハッシュ・アルゴリズムを持つ暗号を使用するには、サーバー鍵ファイルの証明書に、同程度またはより強い署名およびハッシュ・アルゴリズムが含まれていなければなりません。

Suite B でサポートされる暗号セキュリティのレベルは、128 ビットと 192 ビットの 2 つです。このレベルは、すべての暗号アルゴリズムが提供するべき最低限の強度を定義します。

Suite B 128 ビット処理モードでは、以下の暗号がサポートされます。

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Suite B 192 ビット処理モードでは、サポートされる暗号スイートは TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 です。

注意:

サポートされないプロトコル、暗号、および署名/ハッシュ・アルゴリズムを使用するクライアント・ユーティリティと Suite B モードのサーバーの間の通信は失敗する可能性があります。

注:

- 複製、分散ディレクトリー、またはパススルー・トポロジー内のサーバーは、同じ Suite B 暗号セキュリティ・レベルで構成する必要があります。
- Suite B の基準を満たす証明書が含まれている鍵データベース・ファイルを使用してサーバーを構成すると、サーバーは TLS 1.2 プロトコルによる接続を保護するために、より多くの処理を行います。したがって、サーバーが Suite B モードでの接続を保護するために要する処理時間も長くなる可能性があります。

Suite B モードの構成設定

Suite B モードを使用してディレクトリー・サーバーを構成するには、`ibm-slapdSuiteBMode` 属性に適切な暗号セキュリティ・レベルを設定します。変更内容を適用するには、Directory Server と管理サーバーを再始動する必要があります。

以下のような場合、ディレクトリー・サーバーはエラーを生成し、構成モードで始動します。

- `ibm-slapdSuiteBMode` 属性値が 128 または 192 以外である場合。
- 構成ファイル内に複数の `ibm-slapdSuiteBMode` 属性項目がある場合。

`ibm-slapdSecurity` 属性が TLS に設定された場合は、`ibm-slapdSuiteBMode` 属性が有効な値に設定されていても、サーバーは Suite B モードで構成されません。

サーバーを Suite B モードで構成した後、ディレクトリー・サーバーおよび管理サーバーに対してルート DSE 検索を実行すると、Suite B 値が表示されます。

表 20. ディレクトリー・サーバーおよび管理サーバーに設定されている Suite B 暗号セキュリティ・レベルについてのルート DSE 検索の結果

サーバー	Suite B 暗号セキュリティ・レベル	ルート DSE の結果の値
ディレクトリー・サーバー	128	<code>ibm-slapdSuiteBMode=128</code>
	192	<code>ibm-slapdSuiteBMode=192</code>
管理サーバー	128	<code>admindaemon-suitebmode=128</code>
	192	<code>admindaemon-suitebmode=192</code>

また、ルート DSE 検索結果に Suite B の OID があるかを調べることで、サーバーに Suite B モードが設定されているかどうかを確認できます。サーバーで Suite B モードが有効になっている場合、ルート DSE 検索を実行すると、`ibm-enabledCapabilities` 属性には OID 値 `1.3.18.0.2.32.101` が返されます。

注:

- サーバーを Suite B モードで構成すると、サーバーは通信に TLS 1.2 プロトコルを使用します。ディレクトリー・サーバーで Suite B モードを構成するために `ibm-slapdSecurityProtocol` を TLS12 に設定する必要はありません。
- サーバーを Suite B モードで設定する場合は、
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 暗号および
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 暗号が指定された
`ibm-slapdSslCipherSpec` 属性項目を構成ファイル内に追加しないでください。サーバーは、サポートされる Suite B 暗号のうち、設定された GSKit 環境で有効なものを使用します。
- 以下の条件が満たされている場合、TLS 1.2 プロトコルに基づくクライアントは Suite B 準拠のサーバーと正常に通信できます。
 - さまざまな曲線および暗号をサポートする証明書がクライアントで使用されており、Suite B のすべての制限を満たす一致が確認された場合。

特定の組み合わせが有効であっても、クライアント環境を Suite B モードで構成する必要があります。Suite B モードでサーバーおよびクライアント環境を設定すると、基盤となる標準が変更された場合でも、両方の環境が Suite B に準拠することが保証されます。

ログ・メッセージ

ディレクトリー・サーバーが Suite B モードで構成されているかどうかを確認するには、サーバー始動メッセージまたは `ibmslapd.log` ファイルを調べます。

メッセージには、Suite B モードが有効か無効かが記述されています。Suite B モードが有効になっている場合、ディレクトリー・サーバーでは、サーバーに設定されている暗号セキュリティー・レベルも示されます。

AIX、Linux、および Solaris システムの場合

`ibmslapd.log` ファイルのデフォルトの場所は、`instance_home/idsslapd-instance_name/logs` ディレクトリーです。

Windows システムの場合

`ibmslapd.log` ファイルのデフォルトの場所は、`drive%idsslapd-instance_name%logs` ディレクトリーです。

Suite B に関する詳細メッセージを確認するには、サーバーのトレース・メッセージを調べる必要があります。

Suite B モードの構成:

ディレクトリー・サーバーを Suite B モードで構成し、TLS 1.2 プロトコルおよびサポートされる Suite B 暗号を使用して通信を保護します。

始める前に

必要な Suite B 暗号セキュリティー・レベル用の鍵データベース・ファイルおよび証明書を作成します。

詳しくは、「*GSKCapiCmd Users Guide*」の鍵データベース、証明書、および認証要求についての章を参照してください。「*GSKCapiCmd Users Guide*」は、IBM Security Access Manager for Web 資料の Web サイトからダウンロードできます。

ディレクトリー・サーバー・インスタンス所有者の鍵データベース・ファイル、証明書、およびファイル・パスに対して必要な許可 (`rwX`) を設定します。

このタスクについて

Suite B モードのディレクトリー・サーバーを 128 ビットまたは 192 ビットの暗号セキュリティー・レベルに構成できます。

手順

1. インスタンス所有者としてログインします。
2. セキュア通信用にディレクトリー・サーバーを構成するには、`idsldapmodify` コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i suiteB_file.ldif
```

suiteB_file.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslAuth
ibm-slapdSslAuth: serverClientAuth

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSecurity
ibm-slapdSecurity: SSL

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabase
ibm-slapdSslKeyDatabase: /home/dsrdm01/keys/serverkey.kdb

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslCertificate
ibm-slapdSslCertificate: serverlabel

dn: cn=SSL, cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabasepw
ibm-slapdSslKeyDatabasepw: keyfilePWD
```

3. **idsldapmodify** コマンドを実行して、**ibm-slapdSuiteBMode** 属性に適切な暗号セキュリティ・レベルを設定します。

Suite B モードを 128 ビット・プロファイルに設定する場合:

```
idsldapmodify -h host_name -p port -D adminDN -w adminPWD
dn: cn=SSL, cn=Configuration
changetype: modify
add: ibm-slapdSuiteBMode
ibm-slapdSuiteBMode: 128
```

Suite B モードを 192 ビット・プロファイルに設定する場合:

```
idsldapmodify -h host_name -p port -D adminDN -w adminPWD
dn: cn=SSL, cn=Configuration
changetype: modify
add: ibm-slapdSuiteBMode
ibm-slapdSuiteBMode: 192
```

4. ディレクトリー・サーバーおよび管理サーバーを再始動して、変更を適用します。

```
ibmslapd -I dsrdm01 -k
ibmdiradm -I dsrdm01 -k
ibmslapd -I dsrdm01 -n
ibmdiradm -I dsrdm01
```

例

- 例 1 ディレクトリー・サーバーが 128 ビット暗号セキュリティの Suite B モードで構成されている場合は、ルート DSE 検索を実行すると、以下の結果が返されます。

ディレクトリー・サーバーに対してルート DSE 検索を実行する:

```
idsldapsearch -p port -s base -b "" objectclass=* ibm-slapdSuiteBMode
ibm-slapdSuiteBMode=128
```

管理サーバーに対してルート DSE 検索を実行する:

```
idsldapsearch -p admin_port -s base -b "" objectclass=*
admindemon-suitebmode
admindemon-suitebmode=128
```

- 例 2 ディレクトリー・サーバーが 192 ビット暗号セキュリティの Suite B モードで構成されている場合は、ルート DSE 検索を実行すると、以下の結果が返されます。

ディレクトリー・サーバーに対してルート DSE 検索を実行する:

```
idsldapsearch -p port -s base -b "" objectclass=* ibm-slapdSuiteBMode
ibm-slapdSuiteBMode=192
```

管理サーバーに対してルート DSE 検索を実行する:

```
idsldapsearch -p admin_port -s base -b "" objectclass =*  
admindaemon-suitebmode  
admindaemon-suitebmode=192
```

例 3 サーバー・トレース・メッセージを取得するには、以下のコマンドを実行します。

```
ldtrc on  
ibmslapd -h 65535 -I dsrdbm01 2>&1 | tee server_trace.txt
```

Web 管理ツールを使用した Suite B モードの構成:

Web 管理ツールを使用して、ディレクトリー・サーバーを Suite B モードで構成することができます。

始める前に

必要な Suite B 暗号セキュリティ・レベル用の鍵データベース・ファイルおよび証明書を作成します。

詳しくは、「*GSKCapiCmd Users Guide*」の鍵データベース、証明書、および認証要求についての章を参照してください。「*GSKCapiCmd Users Guide*」は、IBM Security Access Manager for Web 資料の Web サイトからダウンロードできます。

ディレクトリー・サーバー・インスタンス所有者の鍵データベース・ファイル、証明書、およびファイル・パスに対して必要な許可 (rwx) を設定します。

このタスクについて

Suite B モードのディレクトリー・サーバーを 128 ビットまたは 192 ビットの暗号セキュリティ・レベルに構成できます。

手順

1. Web 管理ツールにディレクトリー・サーバー管理者としてログインします。
2. ナビゲーション領域で、「サーバー管理」 > 「セキュリティ・プロパティの管理」を展開し、「設定」をクリックします。
3. 「設定」パネルで、接続タイプ、認証方式、および Suite B モードを指定します。
 - a. セキュア・ポートおよび非セキュア・ポートでの接続を受け入れるには、「SSL」をクリックします。
 - b. サーバーおよびクライアントの認証方式を有効にするには、「サーバーおよびクライアントの認証」をクリックします。
 - c. Suite B モードを設定するには、必要な暗号セキュリティ・レベルを選択します。
 - d. 「適用」をクリックします。
4. 「セキュリティ・プロパティの管理」で、「鍵データベース」をクリックします。
5. 「鍵データベース」パネルで、鍵データベース・ファイル、パスワード、および鍵ラベルを指定します。
 - a. 「鍵データベースのパスおよびファイル名」フィールドに、鍵データベース・ファイルの名前を絶対パス名で入力します。

- b. 「鍵パスワード」フィールドに、鍵データベース・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、鍵データベース・パスワードを入力します。
 - d. 「鍵ラベル」フィールドに、証明書を一意的に識別するラベルを入力します。
 - e. 「適用」をクリックします。
6. 「OK」をクリックします。
 7. ナビゲーション領域で、「サーバー管理」 > 「サーバーの始動/停止/再始動」を展開し、「再始動」をクリックします。
 8. ディレクトリー・サーバー・インスタンスが稼働しているコンピューターにアクセスします。
 9. インスタンス所有者としてログインします。
 10. 管理サーバーを再始動します。

```
ibmdiradm -I dsrdbm01 -k
ibmdiradm -I dsrdbm01
```

NIST SP 800-131A 機能およびディレクトリー・サーバー・トポロジーのサポート

トポロジー内で NIST SP 800-131A への移行をサポートするように構成されたディレクトリー・サーバーの動作を特定する必要があります。

トポロジー内の IBM Security Directory Server バージョン 6.3.1 サーバーをセキュア通信に使用すると、以下の動作が見られます。

複製トポロジー:

複製トポロジーでは、サプライヤー・サーバーとコンシューマー・サーバーは、コンシューマー・サーバーに設定されている最もセキュアなプロトコルを使用します。セキュア通信の場合、プロトコルによってサポートされるコンシューマー・サーバーの構成ファイル内で最も優先度の高い暗号が使用されます。

TLS 1.2 署名およびハッシュ・アルゴリズムの制限を構成した場合、サプライヤー・サーバー上の証明書は、コンシューマー・サーバー上に構成されている署名およびハッシュ・アルゴリズムで署名されなければなりません。

複製トポロジーでは、サプライヤー・サーバーとコンシューマー・サーバーは、同じ Suite B 暗号セキュリティ・レベルで構成する必要があります。

分散ディレクトリー:

分散ディレクトリー・トポロジーでは、プロキシ・サーバーとバックエンド・サーバーは、バックエンド・サーバーに設定されている最もセキュアなプロトコルを使用します。セキュア通信の場合、プロトコルによってサポートされるバックエンド・サーバーの構成ファイル内で最も優先度の高い暗号が使用されます。

TLS 1.2 署名およびハッシュ・アルゴリズムの制限を構成した場合、プロキシ・サーバー上の証明書は、バックエンド・サーバー上に構成されている署名およびハッシュ・アルゴリズムで署名されなければなりません。

分散ディレクトリーのセットアップでは、プロキシ・サーバーとバックエンド・サーバーは、同じ Suite B 暗号セキュリティ・レベルで構成する必要があります。

パススルー認証:

パススルー認証のセットアップでは、認証サーバーとパススルー・サーバーは、パススルー・サーバーに設定されている最もセキュアなプロトコルを使用します。セキュア通信の場合、プロトコルによってサポートされるパススルー・サーバーの構成ファイル内で最も優先度の高い暗号が使用されます。

TLS 1.2 署名およびハッシュ・アルゴリズムの制限を構成した場合、認証サーバー上の証明書は、パススルー・サーバー上に構成されている署名およびハッシュ・アルゴリズムで署名されなければなりません。

パススルー認証では、認証サーバーとパススルー・サーバーは、同じ Suite B 暗号セキュリティ・レベルで構成する必要があります。

ディレクトリー・サーバーのさまざまなバージョンの相互運用性

LDAP 環境での相互運用が可能となる、IBM Security Directory Server の該当するバージョンおよび設定を特定する必要があります。

IBM Security Directory Server バージョン 6.3.1 は、さまざまなバージョンのサーバーと相互運用できますが、これは NIST SP 800-131A のサポートが有効か無効かによるものです。

NIST SP 800-131A 移行のサポートが無効になっている場合の相互運用性

NIST SP 800-131A のサポートを有効にせずに IBM Security Directory Server バージョン 6.3.1 サーバーまたはクライアントを使用すると、以下の動作が見られません。

ディレクトリー・サーバー環境

セキュア通信用に構成されている IBM Security Directory Server バージョン 6.3.1 サーバーは、IBM Security Directory Server バージョン 6.3.0.15 または旧バージョンのサーバーと相互運用できます。

セキュア通信用に構成されている IBM Security Directory Server バージョン 6.3.1 サーバーは、以下のトポロジーにおいて、旧バージョンのセキュア・サーバーと共に使用することができます。

- レプリカ生成
- 分散ディレクトリー
- パススルー認証

IBM Security Directory Server バージョン 6.3.1 サーバーは、構成を変更することなしに、さまざまなバージョンのクライアント・ユーティリティと相互運用できます。

クライアント環境

IBM Security Directory Server バージョン 6.3.1 クライアント・ユーティリティは、構成を変更することなしに、さまざまなバージョンのサーバーと共に使用できます。

NIST SP 800-131A 移行のサポートが有効になっている場合

IBM Security Directory Server バージョン 6.3.1 サーバーまたはクライアント環境が、NIST SP 800-131A への移行をサポートするよう構成されている場合、以下の応答が見られます。

ディレクトリー・サーバー環境

トポロジー内のディレクトリー・サーバーをセキュア通信用に構成した場合は、以下の応答が見られます。

複製トポロジー:

サプライヤー・サーバーが IBM Security Directory Server バージョン 6.3.0.15 以前であり、コンシューマー・サーバーが IBM Security Directory Server バージョン 6.3 フィックスパック 17 以降であって次のいずれかの設定を使用して構成されている場合、複製が失敗します。

- TLS 1.2 プロトコル。
- TLS 1.2 署名およびハッシュ・アルゴリズムの制限。
- Suite B モード。

サプライヤー・サーバーおよびコンシューマー・サーバーが IBM Security Directory Server バージョン 6.3 フィックスパック 17 以降である場合、サプライヤー・サーバーは、コンシューマー・サーバーに設定されているプロトコルおよび暗号を使用してセキュア接続を確立しようとします。EC 公開鍵が含まれている鍵データベース・ファイルを使用してコンシューマー・サーバーが構成されている場合、セキュア接続を確立するには、EC 公開鍵を持つ鍵データベース・ファイルがサプライヤー・サーバーに含まれていなければなりません。そうしないと、サプライヤー・サーバーはコンシューマー・サーバーとのセキュア接続の確立に失敗する可能性があります。

複製トポロジーで TLS 1.2 署名およびハッシュ・アルゴリズムの制限が構成されている場合、サプライヤー・サーバーとコンシューマー・サーバーの両方に、互換性のある鍵、証明書、署名およびハッシュ・アルゴリズムの制限が含まれていなければなりません。そうしないと、サプライヤー・サーバーはコンシューマー・サーバーとのセキュア接続の確立に失敗する可能性があります。

複製トポロジーで Suite B モードが構成されている場合、複製トポロジー内のすべてのサーバーは、同じ Suite B 暗号セキュリティ・レベルで構成する必要があります。そうしないと、複製が失敗することがあります。

分散ディレクトリー:

プロキシ・サーバーが IBM Security Directory Server バージョン 6.3.0.15 以前であり、バックエンド・サーバーが IBM Security Directory Server バージョン 6.3 フィックスパック 17 以降であって次のいずれかの設定を使用して構成されている場合、分散ディレクトリーのセットアップが失敗します。

- TLS 1.2 プロトコル。
- TLS 1.2 署名およびハッシュ・アルゴリズムの制限。

- Suite B モード。

プロキシ・サーバーおよびバックエンド・サーバーが IBM Security Directory Server バージョン 6.3 フィックスパック 17 以降である場合、プロキシ・サーバーは、バックエンド・サーバーに設定されているプロトコルおよび暗号を使用してセキュア接続を確立しようとしています。EC 公開鍵が含まれている鍵データベース・ファイルを使用してバックエンド・サーバーが構成されている場合、セキュア接続を確立するには、EC 公開鍵を持つ鍵データベース・ファイルがプロキシ・サーバーに含まれていなければなりません。そうしないと、プロキシ・サーバーはバックエンド・サーバーとのセキュア接続の確立に失敗する可能性があります。

分散ディレクトリーのセットアップで TLS 1.2 署名およびハッシュ・アルゴリズムの制限が構成されている場合、すべてのサーバーには、互換性のある鍵、証明書、署名およびハッシュ・アルゴリズムの制限が含まれていなければなりません。そうしないと、プロキシ・サーバーはバックエンド・サーバーとのセキュア接続の確立に失敗する可能性があります。

分散ディレクトリーのセットアップで Suite B モードが構成されている場合、すべてのサーバーは、同じ Suite B 暗号セキュリティ・レベルで構成する必要があります。そうしないと、サーバーはセキュア接続の確立に失敗する可能性があります。

パススルー認証:

認証サーバーが IBM Security Directory Server バージョン 6.3.0.15 以前であり、パススルー・サーバーが IBM Security Directory Server バージョン 6.3 フィックスパック 17 以降であって次のいずれかの設定を使用して構成されている場合は、パススルー認証が失敗します。

- TLS 1.2 プロトコル。
- TLS 1.2 署名およびハッシュ・アルゴリズムの制限。
- Suite B モード。

認証サーバーおよびパススルー・サーバーが IBM Security Directory Server バージョン 6.3 フィックスパック 17 以降である場合、認証サーバーは、パススルー・サーバーに設定されているプロトコルおよび暗号を使用してセキュア接続を確立しようとしています。EC 公開鍵が含まれている鍵データベース・ファイルを使用してパススルー・サーバーが構成されている場合、セキュア接続を確立するには、EC 公開鍵を持つ鍵データベース・ファイルが認証サーバーに含まれていなければなりません。そうしないと、認証サーバーはパススルー・サーバーとのセキュア接続の確立に失敗する可能性があります。

パススルー認証に対して TLS 1.2 署名およびハッシュ・アルゴリズムの制限が構成されている場合、すべてのサーバーには、互換性のある鍵、証明書、署名およびハッシュ・アルゴリズムの制限が含まれていなければなりません。そうしないと、認証サーバーはパススルー・サーバーとのセキュア接続の確立に失敗する可能性があります。

パススルー認証に対して Suite B モードが構成されている場合、すべてのサーバーは、同じ Suite B 暗号セキュリティ・レベルで構成する必要があります。そうしないと、サーバーはセキュア接続の確立に失敗する可能性があります。

IBM Security Directory Server バージョン 6.3 フィックスパック 17 以降のサーバーと旧バージョンのクライアント:

6.3.0.17 以降のディレクトリー・サーバーと、バージョン 6.3.0.15 以前のクライアント・ユーティリティーの間のセキュア通信は、サーバーが以下を使用して構成されている場合は失敗する可能性があります。

- TLS 1.1 または TLS 1.2 プロトコル。
- TLS 1.2 署名およびハッシュ・アルゴリズムの制限。
- Suite B モード。

クライアント環境

クライアント・ユーティリティーと IBM Security Directory Server バージョン 6.3.0.15 以前のサーバーとの間のセキュア通信は、クライアント環境が以下を使用して構成されている場合、失敗する可能性があります。

- TLS 1.1 または TLS 1.2 プロトコル。
- TLS 1.2 署名およびハッシュ・アルゴリズムの制限。
- Suite B モード。

NIST SP 800-131A への移行をサポートするクライアント・ユーティリティー

NIST SP 800-131A への移行に必要なプロトコル、暗号アルゴリズム、および鍵の長さをサポートするクライアント・ユーティリティーを特定する必要があります。

NIST SP 800-131A ガイドラインに移行する場合、以下を使用することで IBM Security Directory Server クライアント環境を構成することができます。

- TLS 1.2 プロトコル。
- TLS 1.2 署名およびハッシュ・アルゴリズム。
- Suite B モード

この構成は、以下のクライアント・ユーティリティーでサポートされます。

idsdirectl

IBM Security Directory Server の始動、停止、再始動、またはステータスの照会を行うためのコマンド。

idsldapadd, idsldapmodify

LDAP 項目を追加または変更するためのコマンド。

idsldapchangepwd

LDAP 項目のパスワードを変更するためのコマンド。

idsldapdelete

ディレクトリー・サーバーから 1 つ以上の項目を削除するためのコマンド。

idsldapexop

拡張操作を実行するためのコマンド。

idsldapmodrdn

相対識別名 (RDN) の変更、または項目の親の変更を行うためのコマンド。

idsldapsearch

ディレクトリー・サーバーを検索して、フィルターに一致する項目を見つけるためのコマンド。

SSL および TLS プロトコルを使用したクライアント・ユーティリティー:

IBM Security Directory Server クライアント環境で、サポートされる SSL および TLS プロトコル・バージョンを、ディレクトリー・サーバーとのセキュア通信に使用できます。

LDAP クライアント環境でセキュリティー要件を満たすためにセキュア・プロトコルまたは複数のプロトコルを設定できます。クライアント・ユーティリティーで以下のプロトコルを使用して、ディレクトリー・サーバーとの接続を保護することができます。

- SSLv3
- TLS 1.0
- TLS 1.1
- TLS 1.2

サーバーにも構成されているプロトコルを使用してクライアントがサーバーからの接続を要求すると、セキュア接続が確立します。サーバーおよびクライアントはセキュア接続を確立しようとする際に、指定されたプロトコルで使用できる最もセキュアな暗号を採用するようにネゴシエーションします。要求内で使用されたプロトコルがサーバーに設定されていない場合、サーバーおよびクライアントはセキュア接続の確立に失敗します。

LDAP クライアント環境でプロトコルを指定していない場合は、デフォルトで SSLv3/TLS 1.0 プロトコル・スイートがセキュア接続に使用されます。

旧バージョンの IBM Security Directory Server は、バージョン 6.3 フィックスパック 17 以降のクライアント・ユーティリティーと TLS 1.2 プロトコルで接続しようとする、失敗する可能性があります。

旧バージョンの GSKit で作成された鍵データベース・ファイルを使用するクライアント環境は、TLS 1.2 プロトコルで動作する場合があります。以下の条件を満たしている TLS 1.2 暗号が、既存の証明書で機能します。

- 証明書と暗号の公開鍵に互換性がある。
- 証明書と暗号の署名およびハッシュ・アルゴリズムに互換性がある。

以下のシナリオでは、証明書の変更が必要となる可能性があります。

- 既存の証明書の公開鍵と比べて、異なる公開鍵で暗号を使用する場合。
- NIST SP 800-131A ガイドラインを満たす署名およびハッシュ・アルゴリズムを使用する場合。

既存の証明書が NIST SP 800-131A 要件を満たさない場合は、要件を満たす証明書を取得します。

詳しくは、「*GSKCapiCmd Users Guide*」の鍵データベース、証明書、および認証要求についての章を参照してください。「*GSKCapiCmd Users Guide*」は、IBM Security Access Manager for Web 資料の Web サイトからダウンロードできます。

クライアント環境でのセキュア通信プロトコル

LDAP クライアント環境でセキュア通信用のプロトコルを構成するには、`LDAP_OPT_SECURITY_PROTOCOL` 変数に適切なプロトコル値を設定します。複数のプロトコル値はコンマ (,) で区切ります。スペースを使用しないでください。スペースを使用すると、クライアント環境は必要なプロトコルで構成されない可能性があります。

次の表に、`LDAP_OPT_SECURITY_PROTOCOL` でサポートされるプロトコルおよび値を示します。複数のプロトコルが設定されている場合、サーバーとクライアントは、両者に共通している最もセキュアなプロトコルおよび暗号を採用するようにネゴシエーションします。

表 21. 各プロトコルの `LDAP_OPT_SECURITY_PROTOCOL` の値

プロトコル	値
SSLv3	SSLV3
TLS 1.0	TLS10
TLS 1.1	TLS11
TLS 1.2	TLS12

重要:

- プロトコルの暗号を指定すると、指定された暗号のリストは、そのプロトコルに関する LDAP クライアントの暗号リストをオーバーライドします。LDAP クライアントの暗号は、そのプロトコルに関するディレクトリー・サーバーの暗号のサブセットでなければなりません。
- クライアント環境にプロトコルおよび暗号を設定するときは、以下のアクションを実行する必要があります。
 - すべてのプロトコル・レベルについて、使用可能な暗号を指定します。
 - 上位のプロトコルは、下位のプロトコルよりも暗号の適用範囲が広くなるようにしてください。

例えば、`LDAP_OPT_SECURITY_PROTOCOL` 変数には TLS10,TLS12 値が設定されています。16 進値が 35 (1 バイト表記) である暗号の RFC 5246 標準表記は `TLS_RSA_WITH_AES_256_CBC_SHA` です。`LDAP_OPT_SSL_CIPHER` に 35 を設定する場合は、`LDAP_OPT_SSL_CIPHER_EX` にも TLS12 の `TLS_RSA_WITH_AES_256_CBC_SHA` 暗号を設定する必要があります。

- 複数のプロトコルが設定される場合、上位のプロトコルには、より優先度の高い暗号が含まれていなければなりません。優先度は、ディレクトリー・サーバー構成ファイルでの暗号の順序に基づきます。

クライアント環境でのプロトコルの構成:

クライアント環境で SSL または TLS プロトコル・バージョンを構成して、ディレクトリ・サーバーと確実に通信することができます。

始める前に

- IBM Security Directory Server クライアント・パッケージをインストールします。
- IBM Global Security Kit バージョン 8.0.14.24 以降をインストールします。

手順

1. オペレーティング・システムのコマンド行にアクセスします。
2. `LDAP_OPT_SECURITY_PROTOCOL` 変数に、適切なプロトコル値を設定します。

注: Windows システム上で `bash` シェルを実行すると、UNIX の規則に従うことができます。

- LDAP クライアント環境で SSLv3、TLS 1.0、TLS 1.1、および TLS 1.2 プロトコルを設定するには、以下のようにします。

プラットフォーム	以下のコマンドを実行します。
AIX、Linux、Solaris、および HP-UX	<code>\$export LDAP_OPT_SECURITY_PROTOCOL=SSLV3,TLS10,TLS11,TLS12</code>
Windows	<code>c:¥> set LDAP_OPT_SECURITY_PROTOCOL=SSLV3,TLS10,TLS11,TLS12</code>

- LDAP クライアント環境で TLS 1.2 プロトコルを設定するには、以下のようにします。

プラットフォーム	以下のコマンドを実行します。
AIX、Linux、Solaris、および HP-UX	<code>\$export LDAP_OPT_SECURITY_PROTOCOL=TLS12</code>
Windows	<code>c:¥> set LDAP_OPT_SECURITY_PROTOCOL=TLS12</code>

3. プロトコルを構成した後に、同じコンソールからクライアント・ユーティリティーを実行します。以下に例を示します。

```
export LDAP_OPT_SECURITY_PROTOCOL=TLS12

idsldapsearch -h server.com -p secure_port -Z -K clientkey.kdb ¥
-P clientPWD -s base -b "" objectclass =* security

security=ssltls
```

次のタスク

クライアント環境でプロトコルを構成した後は、プロトコルに対して適切な暗号を構成します。『クライアント・ユーティリティーおよび暗号』を参照してください。

クライアント・ユーティリティーおよび暗号:

クライアント環境でプロトコルの暗号を設定していない場合、サーバーおよびクライアントはプロトコルのデフォルトの暗号を使用します。

サポートされる暗号およびプロトコルについて詳しくは、197 ページの『バージョン 6.3、フィックスパック 17 以降におけるプロトコルおよび暗号』を参照してください。

クライアント環境での SSLv3、TLS 1.0、または TLS 1.1 プロトコルに対する暗号の設定

`LDAP_OPT_SSL_CIPHER` 変数に暗号の 16 進値を指定して、クライアント・ユーティリティーがサーバー上の 1 つ以上の暗号についてネゴシエーションできるようにします。暗号を区切り文字で区切らないでください。

プロトコルおよび暗号を指定しない場合、クライアント・ユーティリティーでは SSLv3/TLS 1.0 プロトコル・スイート、および暗号のデフォルト・リストからの暗号 `352F04050A090306` が使用されます。

暗号を設定するときは、`LDAP_OPT_SECURITY_PROTOCOL` 変数にも SSLV3、TLS10、または TLS11 プロトコル値を設定する必要があります。

クライアント環境での TLS 1.2 プロトコルの暗号の設定

`LDAP_OPT_SSL_CIPHER_EX` 変数に暗号値を指定して、LDAP クライアント環境に TLS 1.2 プロトコルの暗号を設定します。複数の暗号はコンマ (,) で区切ります。スペースを使用しないでください。

TLS 1.2 暗号を設定するときは、`LDAP_OPT_SECURITY_PROTOCOL` 変数にも TLS12 プロトコル値を設定する必要があります。

クライアント環境での暗号の構成:

ディレクトリー・サーバーとのセキュア通信を行うために、クライアント環境でプロトコルに対してサポートされる暗号を構成できます。

始める前に

- IBM Security Directory Server クライアント・パッケージをインストールします。
- IBM Global Security Kit バージョン 8.0.14.24 以降をインストールします。

このタスクについて

`LDAP_OPT_SSL_CIPHER` 変数を設定して、SSLv3、TLS 1.0、または TLS 1.1 プロトコルの暗号を構成します。この変数には、暗号の 16 進値を設定します。

`LDAP_OPT_SSL_CIPHER_EX` 変数を設定して、TLS 1.2 プロトコルの暗号を構成します。複数の TLS 1.2 暗号はコンマ (,) で区切ります。スペースを使用しないでください。

手順

1. オペレーティング・システムのコマンド行にアクセスします。
2. クライアント環境で必要なプロトコルの暗号を設定します。

注: Windows システム上で `bash` シェルを実行すると、UNIX の規則に従うことができます。

- LDAP クライアント環境で SSLv3、TLS 1.0、または TLS 1.1 プロトコルの暗号を設定するには、以下のようにします。

AIX、Linux、Solaris、および HP-UX プラットフォームの場合

```
$export LDAP_OPT_SSL_CIPHER=352F04050A09
```

Windows プラットフォームの場合

```
c:\> set LDAP_OPT_SSL_CIPHER=352F04050A09
```

- LDAP クライアント環境で TLS 1.2 プロトコルの暗号を設定するには、以下のようにします。

AIX、Linux、Solaris、および HP-UX プラットフォームの場合

```
$export LDAP_OPT_SSL_CIPHER_EX=TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

Windows プラットフォームの場合

```
c:\> set LDAP_OPT_SSL_CIPHER_EX=TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

3. 暗号を構成した後に、同じコンソールからクライアント・ユーティリティーを実行します。以下に例を示します。

```
export LDAP_OPT_SECURITY_PROTOCOL=SSLV3,TLS10,TLS11,TLS12
```

```
export LDAP_OPT_SSL_CIPHER=352F04050A09
```

```
export LDAP_OPT_SSL_CIPHER_EX=TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

```
idsldapsearch -h server.com -p secure_port -Z -K clientkey.kdb ¥  
-P clientPWD -s base -b "" objectclass =* security
```

```
security=ssltls
```

クライアント・ユーティリティーおよび TLS 1.2 署名およびハッシュ・アルゴリズム:

クライアント・ユーティリティーとサーバーの間の通信で、サポートされる TLS 1.2 署名およびハッシュ・アルゴリズムを TLS 1.2 プロトコルと共に使用するよう制限することができます。TLS 1.2 プロトコルを使用したセキュア通信にクライアント環境を設定する必要があります。

TLS 1.2 署名およびハッシュ・アルゴリズムを設定すると、クライアントはチェーン内のサーバー証明書が準拠しているかどうかを検証します。サーバー証明書が制限を満たさない場合、通信は失敗します。TLS 1.2 署名およびハッシュ・アルゴリズムを構成した後、セキュア通信クライアント・ユーティリティーからディレクター・サーバーのセキュア・ポートにバインドする必要があります。

以下の TLS 1.2 署名およびハッシュ・アルゴリズムがサポートされます。

```
GSK_TLS_SIGALG_RSA_WITH_SHA224  
GSK_TLS_SIGALG_RSA_WITH_SHA256  
GSK_TLS_SIGALG_RSA_WITH_SHA384  
GSK_TLS_SIGALG_RSA_WITH_SHA512  
GSK_TLS_SIGALG_ECDSA_WITH_SHA224  
GSK_TLS_SIGALG_ECDSA_WITH_SHA256  
GSK_TLS_SIGALG_ECDSA_WITH_SHA384  
GSK_TLS_SIGALG_ECDSA_WITH_SHA512
```

LDAP クライアント環境での TLS 1.2 署名およびハッシュ・アルゴリズムの設定

LDAP クライアント環境で TLS 1.2 署名およびハッシュ・アルゴリズムを設定するには、`LDAP_OPT_SSL_EXTN_SIGALG` 変数に適切な値を設定する必要があります。

複数の TLS 1.2 署名およびハッシュ・アルゴリズムを使用するには、以下に従ってください。

- 複数の値はコンマ (,) で区切ります。
- スペースを使用しないでください。スペースを使用すると、クライアント環境が正しく構成されない可能性があります。

変数に無効な値を設定すると、サーバーとの通信が失敗する可能性があります。

注: クライアント環境で `LDAP_OPT_SECURITY_PROTOCOL` 変数に `TLS12` 値を設定する必要があります。

クライアント環境での TLS 1.2 署名およびハッシュ・アルゴリズムの制限の構成:

クライアント環境で TLS 1.2 署名およびハッシュ・アルゴリズムの制限を構成して、TLS 1.2 プロトコルでの通信を保護することができます。

始める前に

- IBM Security Directory Server クライアント・パッケージをインストールします。
- IBM Global Security Kit バージョン 8.0.14.24 以降をインストールします。

手順

1. オペレーティング・システムのコマンド行にアクセスします。
2. `LDAP_OPT_SSL_EXTN_SIGALG` 変数に TLS 1.2 署名およびハッシュ・アルゴリズム値を設定します。

注: Windows システム上で `bash` シェルを実行すると、UNIX の規則に従うことができます。

AIX、Linux、Solaris、および HP-UX プラットフォームの場合

```
$export LDAP_OPT_SSL_EXTN_SIGALG=GSK_TLS_SIGALG_RSA_WITH_SHA256,GSK_TLS_SIGALG_RSA_WITH_SHA384
```

Windows プラットフォームの場合

```
c:¥> set LDAP_OPT_SSL_EXTN_SIGALG=GSK_TLS_SIGALG_RSA_WITH_SHA256,GSK_TLS_SIGALG_RSA_WITH_SHA384
```

3. TLS 1.2 署名およびハッシュ・アルゴリズムの制限を構成した後、同じコンソールからクライアント・ユーティリティを実行します。以下に例を示します。

```
export LDAP_OPT_SECURITY_PROTOCOL=TLS12

export LDAP_OPT_SSL_CIPHER_EX=TLS_RSA_WITH_AES_256_CBC_SHA256
export LDAP_OPT_SSL_EXTN_SIGALG=GSK_TLS_SIGALG_RSA_WITH_SHA256
idsldapsearch -h server.com -p secure_port -Z -K clientkey.kdb ¥
-P clientPWD -s base -b "" objectclass =* security

security=ssl
```

クライアント・ユーティリティおよび Suite B モード:

クライアント環境で Suite B モードを設定して、ディレクトリー・サーバーとのセキュア通信に TLS 1.2 プロトコルおよび Suite B 暗号を使用することができます。

Suite B モードで LDAP クライアント環境を設定する場合は、セキュア通信用クライアント・ユーティリティでディレクトリー・サーバーのセキュア・ポートにバインドする必要があります。

LDAP クライアント環境での Suite B モードの設定

LDAP クライアント環境で Suite B モードを構成するには、`LDAP_OPT_SUITEB_MODE` 変数に有効な Suite B 暗号セキュリティ・レベルを設定してください。Suite B 128 ビット処理モードの場合は、この変数に 128 を割り当てます。Suite B 192 ビット処理モードの場合は、この変数に 192 を割り当てます。

注:

- クライアント環境を Suite B モードで構成すると、クライアント・ユーティリティーは通信に TLS 1.2 プロトコルを使用します。クライアント環境で Suite B モードを構成する目的で `LDAP_OPT_SECURITY_PROTOCOL` を TLS12 に設定しないでください。
- クライアント環境を Suite B モードで設定するときは、`LDAP_OPT_SSL_CIPHER_EX` 変数に `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256` 暗号および `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384` 暗号を設定しないでください。クライアント・ユーティリティーは、サポートされる Suite B 暗号のうち、設定された GSKit 環境で有効なものを使用します。

注意:

Suite B モードのクライアント・ユーティリティーと、サポートされないプロトコル、暗号、署名およびハッシュ・アルゴリズムを使用するサーバーとの間の通信は、失敗する可能性があります。

クライアント環境での Suite B モードの構成:

クライアント環境で Suite B モードを構成して、Suite B モードのディレクトリー・サーバーとの通信を保護します。

始める前に

- IBM Security Directory Server クライアント・パッケージをインストールします。
- IBM Global Security Kit バージョン 8.0.14.24 以降をインストールします。

このタスクについて

クライアント環境で Suite B モードを 128 ビットまたは 192 ビットの暗号セキュリティ・レベルに構成できます。

手順

1. オペレーティング・システムのコマンド行にアクセスします。
2. `LDAP_OPT_SUITEB_MODE` 変数に有効な Suite B 暗号セキュリティ・レベルを設定します。

注: Windows システム上で `bash` シェルを実行すると、UNIX の規則に従うことができます。

- Suite B モードを 128 ビットの暗号セキュリティ・レベルに設定する場合:

プラットフォーム	以下のコマンドを実行します。
AIX、Linux、Solaris、および HP-UX	<code>\$export LDAP_OPT_SUITEB_MODE=128</code>

プラットフォーム	以下のコマンドを実行します。
Windows	c:¥> set LDAP_OPT_SUITEB_MODE=128

- Suite B モードを 192 ビットの暗号セキュリティー・レベルに設定する場合:

プラットフォーム	以下のコマンドを実行します。
AIX、Linux、Solaris、および HP-UX	\$export LDAP_OPT_SUITEB_MODE=192
Windows	c:¥> set LDAP_OPT_SUITEB_MODE=192

3. Suite B モードを構成した後に、同じコンソールからクライアント・ユーティリティーを実行します。以下に例を示します。

```
export LDAP_OPT_SUITEB_MODE=128

idsldapsearch -h server.com -p secure_port -Z -K clientkey.kdb ¥
-P clientPWD -s base -b "" objectclass =* ibm-slappSuiteBMode

ibm-slappSuiteBMode=128
```

Web 管理ツールを使用した NIST SP 800-131A への移行のサポート

NIST SP 800-131A への移行に必要なサポート・ブラウザ、Web 管理ツール、アプリケーション・サーバー、および IBM Java Development Kit バージョンを使用しなければなりません。

Web 管理ツールを使用して、NIST SP 800-131A への移行をサポートするディレクトリー・サーバーに接続するには、以下の依存関係を満たす必要があります。

- Web 管理ツールを、WebSphere Application Server 組み込みバージョン 7.0.0.25 以降にデプロイする。
- IBM Java Development Kit バージョン 1.6 SR14 以降を使用する。
- TLS 1.0、TLS 1.1、および TLS 1.2 のセキュア通信プロトコルをサポートするブラウザを使用する。例えば、Microsoft Windows Internet Explorer バージョン 8.0 以降では、TLS 1.0、TLS 1.1、および TLS 1.2 プロトコルがサポートされます。

NIST SP 800-131A への移行をサポートする目的で、Web 管理ツールはデプロイ先の Web アプリケーション・サーバーに依存しています。WebSphere Application Server 組み込みバージョンは、IBM Java Development Kit セキュリティー機能を使用して、必要なセキュリティー・レベルをサポートします。

注: 組織で必要とされるディレクトリー・サーバーおよび WebSphere Application Server 組み込みバージョンのセキュリティー・レベルを設定することをお勧めします。

Web 管理ツールを使用して NIST SP 800-131A への移行をサポートするためには、以下の構成が必要です。

1. IBM Security Directory Server バージョン 6.3.1 をインストールします。詳しくは、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。
2. Web 管理ツールおよび WebSphere Application Server 組み込みバージョンをインストールします。詳しくは、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。

3. 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ます。詳しくは、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。
4. ディレクトリー・サーバー用の CMS 鍵データベース・ファイルおよび Web 管理ツール用の JKS 鍵データベース・ファイルを作成します。詳細については、223 ページの『自己署名証明書を使用した鍵データベース・ファイルの作成』を参照してください。
5. セキュア通信に必要なプロトコルおよび暗号を使用してディレクトリー・サーバー・インスタンスを構成します。詳細については、188 ページの『SSL および TLS プロトコルを使用したディレクトリー・サーバー・インスタンス』を参照してください。
6. ご使用のブラウザで、TLS 1.0、TLS 1.1、および TLS 1.2 セキュア通信プロトコルを有効にします。詳しくは、Microsoft TechNet Web サイト (<http://technet.microsoft.com/en-US/>) で、introducing TLS v1.2 キーワードを検索します。
7. JKS 鍵データベースを使用して、Web 管理ツールを構成します。
8. WebSphere Application Server 組み込みバージョンを、組織で必要とされるセキュリティ・レベルに構成します。

Web 管理ツールで連邦情報処理標準 (FIPS) モードおよびセキュリティ標準のレベルを設定し、使用するには、WebSphere Application Server 組み込みバージョン 7.0.0.25 以降の **wsadmin** ツールを使用します。以下の FIPS モード、セキュリティ標準のレベル、およびプロトコルがサポートされます。

表 22. FIPS モード、セキュリティ標準のレベル、およびプロトコルの間の関係

FIPS モード	セキュリティ標準のレベル	Web 管理ツールでサポートされるプロトコル
false	なし	<ul style="list-style-type: none"> • SSL_TLS • SSL v3 • TLS 1.0 • TLS 1.1 • TLS 1.2
true	FIPS140-2 モード	TLS 1.0
true	SP800-131 transition モード	<ul style="list-style-type: none"> • TLS 1.0 • TLS 1.1 • TLS 1.2
true	SP800-131 strict モード	TLS 1.2
true	Suite B 128	TLS 1.2
true	Suite B 192	TLS 1.2

JKS 鍵データベースの使用による Web 管理ツールの構成:

JKS 鍵データベース・ファイルを使用して Web 管理ツールを構成し、ディレクトリー・サーバー・インスタンスとのセキュア通信に Web 管理ツールを使用するようにします。

始める前に

JKS 鍵データベースを使用して Web 管理ツールを構成するには、以下のステップを実行する必要があります。

- JKS 鍵データベースを作成します。詳細については、223 ページの『自己署名証明書を使用した鍵データベース・ファイルの作成』を参照してください。
- Web 管理ツールおよび WebSphere Application Server 組み込みバージョンをインストールします。IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。
- 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ます。IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。

手順

1. ご使用のコンピューター上のブラウザにアクセスします。
2. Web 管理ツールの URL を入力します。Web 管理ツールの URL は、以下の形式です。http://ip_address:12100/IDSWebApp
3. 「**コンソール管理ログイン**」ページで、以下の値を指定します。
 - a. 「**ユーザー ID**」フィールドに、コンソール管理者のユーザー ID を入力します。デフォルト値は superadmin です。ユーザー ID の値をログイン後に変更する必要があります。
 - b. 「**パスワード**」フィールドに、コンソール管理者のユーザー ID のパスワードを入力します。デフォルト値は secret です。ログイン後に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。
4. 「**コンソール管理**」 > 「**コンソール・プロパティの管理**」をクリックします。
5. 「**コンソール・プロパティの管理**」ウィザードで、「**SSL 鍵データベース**」をクリックします。
6. 「**SSL 鍵データベース**」パネルで、以下の手順を実行します。
 - a. 「**鍵データベースのパスおよびファイル名**」フィールドに、JKS 鍵データベース・ファイル名をパス付きで入力します。
 - b. 「**鍵パスワード**」フィールドに、JKS 鍵データベース・ファイル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、JKS 鍵データベース・ファイルのパスワードを入力します。
 - d. 「**鍵データベース・ファイル・タイプ**」リストから、jks を選択します。
 - e. 信頼データベースの詳細情報が鍵データベースの詳細情報と同じである場合は、「**鍵データベースと同じ**」をクリックします。
 - f. オプション: 「**信頼データベース・パスおよびファイル名**」フィールドに、JKS 信頼データベース・ファイル名をパス付きで入力します。
 - g. オプション: 「**信頼パスワード**」フィールドに、JKS 鍵データベース・ファイルのパスワードを入力します。

- h. オプション: 「**確認パスワード**」フィールドに、JKS 鍵データベース・ファイルのパスワードを入力します。
 - i. オプション: 「**信頼データベース・ファイル・タイプ**」リストから、jks を選択します。
 - j. 変更を適用するには、「**OK**」をクリックします。
7. 「**コンソール・プロパティの管理**」ウィザードで、「**セキュリティ・プロトコルの管理**」をクリックします。
 8. ディレクトリー・サーバーとのセキュア通信にセキュリティ・プロトコルを使用するには、組織のセキュリティ要件に従ってプロトコルをクリックします。プロトコル値は、デPLOYされた Web 管理ツール・プロファイルの `idswebapp.properties` ファイル内の `SSLContextAlgorithm` 項目に設定されます。
 9. 変更を適用するには、「**OK**」をクリックします。
 10. 「**ログアウト**」をクリックします。

次のタスク

以下の構成を行う必要があります。

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、組織のセキュリティ要件に従ったセキュリティ・レベルに構成します。
2. Web 管理ツールのコンソールで、ディレクトリー・サーバーをそのセキュア・ポートおよび管理セキュア・ポートと共に追加します。IBM Security Directory Server の資料の『管理』セクションを参照してください。

自己署名証明書を使用した鍵データベース・ファイルの作成:

鍵データベースの自己署名証明書を作成し、それを CA 証明書に置き換える前に、公開鍵および署名アルゴリズムに対する公開/秘密鍵をテストします。

始める前に

鍵データベース・ファイルを作成するには、以下の要件を満たす必要があります。

- AIX、Linux、および Solaris の場合は root ユーザーとして、また Microsoft Windows の場合は管理メンバーとして、コンピューターにログインします。
- ディレクトリー・サーバー用の CMS 鍵データベースを作成するには、サーバーが存在するコンピューターに IBM Global Security Kit バージョン 8.0.14.24 以降が含まれている必要があります。
- JKS 鍵データベースを作成するには、Web 管理ツールが存在するコンピューターに IBM Java Development Kit バージョン 1.6 SR14 以降が含まれていなければなりません。

詳しくは、「*GSKCapiCmd Users Guide*」の鍵データベース、証明書、および認証要求についての章を参照してください。「*GSKCapiCmd Users Guide*」は、IBM Security Access Manager for Web 資料の Web サイトからダウンロードできます。

ikeyman または **ikeycmd** ユーティリティの使用については、IBM SDK Java Technology 資料の Web サイトを参照してください。

このタスクについて

ご使用のコンピューターに **GSKit 32 ビット**が含まれている場合は、**gsk8capicmd** コマンドを使用します。ご使用のコンピューターに **GSKit 64 ビット**が含まれている場合は、**gsk8capicmd_64** コマンドを使用します。このタスクが完了すると、鍵データベース・ファイルに以下のデータが格納されます。

- JKS 鍵データベース・ファイルから抽出された署名者証明書を持つ CMS 鍵データベース・ファイル。
- CMS 鍵データベース・ファイルから抽出された署名者証明書を持つ JKS 鍵データベース・ファイル。

手順

1. 自己署名証明書付き CMS 鍵データベースを作成するため、以下のステップを実行します。
 - a. 必要な特権を使用してコンピューターにログインします。
 - b. CMS 鍵データベースを作成するため、**gsk8capicmd_64** コマンドを以下の形式で実行します。

```
gsk8capicmd_64 -keydb -create -db serverkey.kdb -pw serverpwd
-type cms -expire 1000 -stash -fips
```
 - c. 鍵サイズが 2048 で、署名アルゴリズムが SHA512WithRSA の自己署名証明書を作成するには、**gsk8capicmd_64** コマンドを以下の形式で実行します。

```
gsk8capicmd_64 -cert -create -db serverkey.kdb -pw serverpwd -label serverlabel
-dn "cn=LDAP_Server,o=sample" -size 2048 -default_cert yes -sigalg SHA512WithRSA
```
 - d. 鍵データベースから証明書データを抽出するため、**gsk8capicmd_64** コマンドを以下の形式で実行します。

```
gsk8capicmd_64 -cert -extract -db serverkey.kdb -pw serverpwd -label serverlabel
-target server.der -format binary
```
 - e. CMS 鍵データベースから抽出した証明書が含まれているファイルを、Web 管理ツールが存在するコンピューターに転送します。
2. 自己署名証明書付きの JKS 鍵データベースを作成するため、以下のステップを実行します。
 - a. 必要な特権を使用してコンピューターにログインします。
 - b. **JAVA_HOME** 変数および **PATH** 変数に、IBM Security Directory Server で提供される IBM Java ロケーションを設定します。

AIX および Solaris

```
export JAVA_HOME=/opt/IBM/1dap/V6.3.1/java
export PATH=/opt/IBM/1dap/V6.3.1/java/jre/bin:$PATH
```

Linux

```
export JAVA_HOME=/opt/ibm/1dap/V6.3.1/java
export PATH=/opt/ibm/1dap/V6.3.1/java/jre/bin:$PATH
```

Windows

```
set JAVA_HOME=C:\Program Files\IBM\1dap\V6.3.1\java
set PATH=C:\Program Files\IBM\1dap\V6.3.1\java\jre\bin;%PATH%
```

- c. JKS 鍵データベースを作成するため、**ikeycmd** コマンドを以下の形式で実行します。

```
ikeycmd -keydb -create -db webadminkey.jks -pw webadminpwd
-type jks -expire 1000 -stash
```
- d. 鍵サイズが 2048 で、署名アルゴリズムが SHA512WithRSA の自己署名証明書を作成するには、**ikeycmd** コマンドを以下の形式で実行します。

```
ikeycmd -cert -create -db webadminkey.jks -pw webadminpwd -label webadminlabel  
-dn "cn=LDAP_WebAdmin,o=sample" -size 2048 -sig_alg SHA512WithRSA
```

- e. 鍵データベースから証明書データを抽出するには、**ikeycmd** コマンドを以下の形式で実行します。

```
ikeycmd -cert -extract -db webadminkey.jks -pw webadminpwd -label webadminlabel  
-target webadmin.der -format binary
```

- f. JKS 鍵データベースから抽出した証明書が含まれているファイルを、ディレクトリー・サーバー・インスタンスが存在するコンピューターに転送します。

3. ディレクトリー・サーバー・インスタンスが存在するコンピューターで、JKS 鍵データベースから抽出した証明書を CMS 鍵データベースに追加します。

```
gsk8capicmd_64 -cert -add -db serverkey.kdb -pw serverpwd -label webadminlabel  
-file webadmin.der -format binary
```

4. Web 管理ツールが存在するコンピューターで、CMS 鍵データベースから抽出した証明書を JKS 鍵データベースに追加します。

```
ikeycmd -cert -add -db webadminkey.jks -pw webadminpwd -file server.der  
-label serverlabel -format binary
```

次のタスク

構成を続行するには、以下の手順を実行します。

- ディレクトリー・サーバー・インスタンスで CMS 鍵データベースおよび詳細情報を追加します。詳しくは、『192 ページの『セキュリティ・プロトコルおよび暗号によるディレクトリー・サーバーの構成』』を参照してください。
- Web 管理ツールのコンソールで、JKS 鍵データベースおよび詳細情報を追加します。

アプリケーション・サーバーでの FIPS モードおよびセキュリティ・レベルの構成:

アプリケーション・サーバーで **wsadmin** ツールの AdminTask オブジェクトを使用して、セキュア通信の FIPS モードおよびセキュリティ・レベルを構成します。

始める前に

Web 管理ツールを使用してディレクトリー・サーバーに確実に接続するには、以下の条件が満たされていないとなりません。

- JKS 鍵データベースを使用して Web 管理ツールを構成します。221 ページの『JKS 鍵データベースの使用による Web 管理ツールの構成』を参照してください。
- セキュア通信に必要なプロトコルおよび暗号を使用してディレクトリー・サーバー・インスタンスを構成します。詳細については、188 ページの『SSL および TLS プロトコルを使用したディレクトリー・サーバー・インスタンス』を参照してください。
- AIX、Linux、および Solaris の場合は root ユーザーとして、また Microsoft Windows の場合は管理メンバーとして、コンピューターにログインします。

手順

1. 現行ディレクトリーを、デプロイされた Web 管理ツール・プロファイルの bin ディレクトリーに変更します。各オペレーティング・システムにおけるデフォルトの Web 管理ツール・プロファイル・ロケーションを、次の表に示します。

オペレーティング・システム	デフォルトのプロファイル・ロケーション
AIX および Solaris	/opt/IBM/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/
Linux	/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/
Windows	C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile\

2. WebSphere 管理 (wsadmin) スクリプト・プログラムを開始するには、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	以下のコマンドを実行します。
AIX、Linux、および Solaris	./wsadmin.sh
Windows	wsadmin.bat

3. 現在の WebSphere 構成の FIPS 設定を取得するには、以下のコマンドを実行します。

```
AdminTask getFipsInfo
```

4. 組織の要件に従って FIPS モードおよびセキュリティー・レベルを構成するには、次のいずれかのコマンドを実行します。

セキュリティー・レベル	以下のコマンドを実行します。
FIPS140-2 モード	AdminTask enableFips { -enableFips true -fipsLevel FIPS140-2 }
SP800-131 transition モード	AdminTask enableFips { -enableFips true -fipsLevel transition }
SP800-131 strict モード	AdminTask enableFips { -enableFips true -fipsLevel SP800-131 }
Suite B 128	AdminTask enableFips { -enableFips true -suiteBLevel 128 }
Suite B 192	AdminTask enableFips { -enableFips true -suiteBLevel 192 }

FIPS コマンドについて詳しくは、IBM WebSphere Application Server 資料の Web サイトで、キーワード enableFips を検索してください。

5. オプション: セキュリティー・レベルを設定するコマンドを実行して、ID が WASX7015E のエラー・メッセージが生成された場合は、以下のコマンドを実行します。

SP800-131 strict モード

```
AdminTask listCertStatusForSecurityStandard { -fipsLevel SP800-131 }
AdminTask convertCertForSecurityStandard { -fipsLevel SP800-131 }
AdminTask enableFips { -enableFips true -fipsLevel SP800-131 }
```

Suite B 128

```
AdminTask listCertStatusForSecurityStandard { -suiteBLevel 128 }
AdminTask convertCertForSecurityStandard { -suiteBLevel 128 }
AdminTask enableFips { -enableFips true -suiteBLevel 128 }
```

Suite B 192

```
AdminTask listCertStatusForSecurityStandard { -suiteBLevel 192 }
AdminTask convertCertForSecurityStandard { -suiteBLevel 192 }
AdminTask enableFips { -enableFips true -suiteBLevel 192 }
```

詳しくは、IBM WebSphere Application Server 資料の Web サイトで、キーワード `listCertStatusForSecurityStandard` または `convertCertForSecurityStandard` を検索してください。

- 構成変更を保存するには、以下のコマンドを実行します。

```
AdminTask save
```

- 現在の WebSphere 構成の FIPS 設定を取得するには、以下のコマンドを実行します。

```
AdminTask getFipsInfo
```

- `wsadmin` を終了するには、以下のコマンドを実行します。

```
quit
```

- Web 管理ツールに関連付けられているアプリケーション・サーバーに構成変更を適用するには、以下のコマンドを実行します。

```
stopServer.sh server1
startServer.sh server1
```

- ご使用のコンピューターで、TLS 1.0、TLS 1.1、および TLS 1.2 プロトコルをサポートするブラウザにアクセスします。
- Web 管理ツールのセキュア URL を入力します。Web 管理ツールのセキュア URL は、以下の形式です。 `https://ip_address:12101/IDSWebApp`
- 「**Directory Server ログイン**」ページで、以下の値を指定します。
 - 「**LDAP サーバー名**」フィールドで、ディレクトリー・サーバー・インスタンスを選択します。
 - 「**ユーザー ID**」フィールドに、LDAP ユーザー ID を入力します。
 - 「**パスワード**」フィールドに、LDAP ユーザー ID のパスワードを入力します。
 - 「**ログイン**」をクリックします。

鍵データベースからの証明書のインポート

旧バージョンの `GSKCapiCmd` コマンドを使用して作成された鍵データベースの証明書を、新しいバージョンの `GSKCapiCmd` コマンドを使用して別の鍵データベースにインポートします。

始める前に

ソース・コンピューターから証明書をエクスポートし、その証明書をターゲット・コンピューターにインポートするには、以下の条件を満たしていなければなりません。

- ソース・コンピューターには、IBM Global Security Kit (GSKit) の旧バージョンが含まれている必要があります。

- ターゲット・コンピューターには、新しいバージョンの IBM Global Security Kit が含まれている必要があります。IBM Security Directory Server バージョン 6.3.1 には、IBM Global Security Kit バージョン 8.0.14.26 以降が必要です。

このタスクについて

証明書を含む有効な鍵データベース・ファイルが、旧バージョンの **GSKCapiCmd** コマンドを使用して作成された場合は、その証明書をターゲット・コンピューターにエクスポートします。

新しいバージョンの **GSKCapiCmd** コマンドを使用して作成された鍵データベース・ファイルで、この証明書を再使用します。これは、新しいバージョンの IBM Global Security Kit に関する互換性の問題を解決するためです。

手順

1. 旧バージョンの **GSKit** が含まれているコンピューターに、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。例えば、**GSKit** バージョン 7 です。
2. CMS 鍵データベースを作成するには、以下のコマンドを実行します。

注: ご使用のコンピューターに 32 ビット **GSKit** が含まれている場合は、**gsk7capiCmd** コマンドを使用します。ご使用のコンピューターに 64 ビット **GSKit** が含まれている場合は、**gsk7capiCmd_64** コマンドを使用します。

```
gsk7capiCmd -keydb -create -db source.kdb -pw myPwd123 -type cms
-expire 1000 -stash -fips
```

3. 鍵サイズが 2048 で、ハッシュ・アルゴリズムが sha384 の自己署名証明書を作成するには、以下のコマンドを実行します。

```
gsk7capiCmd -cert -create -db source.kdb -pw myPwd123 -label testlabel
-dn "cn=LDAP_Server.com,ou=myDept,o=sample" -size 2048 -fips
-sigalg sha384 -expire 1000
```

4. 特定のラベルを持つ証明書を CMS 鍵データベースから、/transfer/ ディレクトリーにある別の CMS 鍵データベースにエクスポートするには、以下のコマンドを実行します。

```
gsk7capiCmd -cert -export -db source.kdb -pw myPwd123 -label testlabel -type cms
-target /transfer/test.kdb -target_pw myPwd123 -target_type cms
```

5. /transfer/test.kdb ファイル内の証明書を検証するには、以下のコマンドを実行します。

```
gsk7capiCmd -cert -list -db /transfer/test.kdb -pw myPwd123
```

6. /transfer/ ディレクトリー内にある鍵データベースおよびその関連ファイルをターゲット・コンピューターに転送します。
7. 証明書を CMS 鍵データベースから別の CMS 鍵データベースにインポートするには、新しいバージョンの **GSKit** から、以下のコマンドを実行します。

注: ご使用のコンピューターに 32 ビット **GSKit** が含まれている場合は、**gsk8capiCmd** コマンドを使用します。ご使用のコンピューターに 64 ビット **GSKit** が含まれている場合は、**gsk8capiCmd_64** コマンドを使用します。

```
gsk8capiCmd_64 -cert -import -db /transfer/test.kdb -pw myPwd123 -label testlabel
-type cms -target /target/target.kdb -target_pw myPwd123 -target_type cms
-new_label testlabel
```

コマンドが操作を正常に完了すると、証明書はソースとターゲットの両方の鍵データベースで使用できます。

8. /target/target.kdb ファイル内の証明書を検証するには、以下のコマンドを実行します。

```
gsk8capicmd_64 -cert -list -db /target/target.kdb -pw myPwd123
```

次のタスク

インポートされた証明書が含まれている鍵データベースをディレクトリー・サーバー・インスタンスで使用するには、そのインスタンスに鍵データベース・ファイルおよび関連する詳細情報を追加します。

JKS 鍵データベースからの証明書のエクスポート

以前のバージョンの JKS (Java 鍵ストア形式) 鍵データベースから、新しいバージョンの別の JKS 鍵データベースに証明書をエクスポートします。

始める前に

ソース・コンピューターからターゲット・コンピューターに証明書をエクスポートするには、以下の条件を満たしている必要があります。

- ソース・コンピューターに以前のバージョンの Web 管理ツールが備えられている必要があります。このツールは、WebSphere Application Server 組み込みバージョンにデプロイされており、JKS 鍵データベースで設定されます。
- ターゲット・コンピューターに新しいバージョンの Web 管理ツールが備えられている必要があります。このツールは、WebSphere Application Server 組み込みバージョンにデプロイされています。
- ターゲット・コンピューターに新しいバージョンの IBM Java Development Kit が備えられている必要があります。IBM Security Directory Server バージョン 6.3.1 には、IBM Java Development Kit バージョン 1.6 SR 14 以降が必要です。

このタスクについて

以前のバージョンの **ikeyman** または **ikeycmd** コマンドにより作成された証明書を持つ有効な JKS 鍵データベース・ファイルがある場合、証明書をターゲット・コンピューターにエクスポートします。エクスポートする理由は以下のとおりです。

- 新しいバージョンの JKS コマンドにより作成された JKS 鍵データベース・ファイルで証明書を再利用するため。
- 新しいバージョンの IBM Java Development Kit との互換性の問題を解決するため。

手順

1. WebSphere Application Server 組み込みバージョンにデプロイされている、以前のバージョンの Web 管理ツールが備えられているコンピューターにログインします。
2. JKS 鍵データベースおよび関連するファイルをターゲット・コンピューターに転送します。
3. `JAVA_HOME` 変数および `PATH` 変数に、IBM Security Directory Server で提供される IBM Java ロケーションを設定します。

オペレーティング・システム	実行するコマンド:
AIX および Solaris	export JAVA_HOME=/opt/IBM/ldap/V6.3.1/java export PATH=/opt/IBM/ldap/V6.3.1/java/jre/bin:\$PATH
Linux	export JAVA_HOME=/opt/ibm/ldap/V6.3.1/java export PATH=/opt/ibm/ldap/V6.3.1/java/jre/bin:\$PATH
Windows	set JAVA_HOME=C:\Program Files\IBM\ldap\V6.3.1\java set PATH=C:\Program Files\IBM\ldap\V6.3.1\java\jre\bin;%PATH%

4. /source/source.jks ファイルにある証明書を確認するには、以下のコマンドを実行します。

```
ikeycmd -cert -list -db /transfer/test.jks -pw myPwd123
```

5. ラベルを持つ証明書をソース JKS 鍵データベースからターゲット JKS 鍵データベースにエクスポートするには、以前のバージョンの **ikeycmd** から以下のコマンドを実行します。

```
ikeycmd -cert -export -db /source/source.jks -pw myPwd123 -label testlabel -type jks  
-target /transfer/test.jks -target_pw myPwd123 -target_type jks
```

6. /target/test.jks ファイルにある証明書を確認するには、以下のコマンドを実行します。

```
ikeycmd -cert -list -db /target/test.jks -pw myPwd123
```

次のタスク

証明書を持つターゲット JKS 鍵データベースを Web 管理ツールで使用するには、Web 管理ツール・コンソールで JKS 鍵データベース・ファイルを追加します。

証明書取り消し検査

この機能により、証明書取り消しを検査することができます。

SSL 設定でサーバーとクライアント認証の使用を選択した場合は、失効した証明書または有効期限切れの証明書を検査するようにサーバーを構成する場合があります。

クライアントがサーバーに認証要求を送信すると、サーバーは証明書を読み取って、失効した証明書を含むリストとともに LDAP サーバーに照会を送信します。リストにクライアント証明書が見つからない場合、クライアントとサーバー間の通信は SSL を介して許可されます。証明書が見つかった場合、通信は許可されません。

SSL 証明書の取り消し検査を構成するには、以下のいずれかの方法を使用します。

Web 管理の使用

ここで説明する手順に従うことにより、Web 管理ツールを使用して SSL 証明書取り消し検査を使用可能にすることができます。

このタスクについて

「サーバー管理」の下で、Web 管理ツールのナビゲーション領域にある「セキュリティー・プロパティの管理」カテゴリーを展開し、「証明書取り消し」タブを選択します。

手順

1. 「サーバーのホスト名:ポート」ドロップダウン・リストから証明書取り消しリストを含む LDAP サーバーおよびポートを選択するか、サーバーのホスト名およびポート番号を `hostname:port` の形式でフィールドに入力します。
2. 「バインド DN」フィールドに、サーバーに接続するために使用するバインド DN を指定します。バインド DN を指定しない場合は、匿名バインドが使用されます。
3. 「バインド・パスワード」フィールドにバインド・パスワードを指定します。「パスワードの確認」フィールドにパスワードを再度入力します。
4. 完了したら、終了せずに変更を保存する場合は「適用」をクリックし、変更を適用して終了する場合は「OK」をクリックし、変更を行わずにこのパネルを終了するには「キャンセル」をクリックします。

タスクの結果

注: 有効期限は証明書自体に含まれているため、有効期限切れの証明書は、リストには含まれません。

コマンド・ラインの使用

コマンド行を使用して、SSL 証明書取り消し検査を構成することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=CRL,cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdCrlHost
ibm-slapdCrlHost: <newhostname>
-
replace: ibm-slapdCrlPassword
ibm-slapdCrlPassword: <password>
-
replace: ibm-slapdCrlPort
ibm-slapdCrlPort: <portnumber>
-
replace: ibm-slapdCrlUser
ibm-slapdCrlUser: <username>
```

変更した内容を有効にするには、サーバーおよび管理サーバーを再始動する必要があります。

ディレクトリー・アクセス権限のセキュリティ

この情報に従って、ディレクトリー・アクセス権限を保護します。

ディレクトリー・データへのアクセスは、ディレクトリー管理者が完全に制御できます。LDAP ディレクトリーでは、ディレクトリーを使用しようとするユーザーを識別するバインド操作をクライアントが実行する必要があります。IBM Security Directory Server では、数種類のバインド・メカニズムがサポートされています。

- 簡易
- DIGEST-MD5

- Kerberos (GSSAPI と呼ばれる)
- EXTERNAL

ディレクトリー・サーバーは、パススルー認証をサポートしています。これにより管理者は、他のディレクトリー・サーバー (OpenLDAP、Active Directory など) を使用するようにディレクトリー・サーバーを構成して、バインドの認証を実行することができます。266 ページの『パススルー認証』を参照してください。

簡易バインドでは、DN とパスワードが必要です。DN が提供されない場合、バインドは匿名バインドと呼ばれます。管理者は、匿名バインドを許可しないようにディレクトリーを構成できます。113 ページの『接続プロパティの管理』を参照してください。一般に、DN はディレクトリー内の項目に対応しています。ディレクトリー・サーバーに対するバインドで使用されるパスワードは、DN が指定されている項目に関連付けられている `userpassword` 属性の値です。ディレクトリー・サーバーは、パスワードに使用できる値の種類、およびパスワードを変更する必要がある頻度を決定するパスワード・ポリシーを適用するように構成できます。235 ページの『パスワード・ポリシー設定』を参照してください。ディレクトリーに格納されるパスワード・データは暗号化されます。『パスワード暗号化』を参照してください。ディレクトリー管理者は、管理グループを構成して一部の管理責任を委任できます。このグループのメンバーには、ディレクトリー内での特定の権限を割り当てることができます。これらのグループの DN およびパスワードは、サーバー構成の一部として保管されます。パスワードは暗号化されます。また、管理パスワード・ポリシーを構成できます。247 ページの『管理パスワードおよびロックアウト・ポリシーの設定』を参照してください。

構成では、DIGEST-MD5 および Kerberos (GSSAPI) の情報を使用してください。EXTERNAL メカニズム (PKI または証明書ベースの認証とも呼ばれる) は、ディレクトリー・サーバーによって実行される認証に依存しています。サーバーがサーバー/クライアント認証用に構成されている場合は、SSL または TLS が使用されます。クライアント接続は、サーバーが信頼する認証局 (CA) により発行された証明書をクライアントが提供した後でのみ確立されます。クライアント証明書には DN が 1 つ含まれており、この DN を使用して、このクライアント接続のユーザーが識別されます。EXTERNAL バインドをサポートするようにディレクトリー・サーバーを構成する方法については、151 ページの『セキュリティ設定の構成』を参照してください。

パスワード暗号化

IBM Security Directory Server を使用することにより、ユーザー・パスワードに対する無許可アクセスを防止できます。片方向暗号化形式を使用すると、ユーザー・パスワードを暗号化してディレクトリーに保管することができます。暗号化により、すべてのユーザーおよびシステム管理者がクリア・パスワードにアクセスできなくなります。

管理者は、片方向暗号化形式または両方向暗号化形式のいずれかで `userPassword` 属性値を暗号化するよう、サーバーを構成することができます。

片方向暗号化形式は以下のとおりです。

- crypt
- MD5

- SHA-1
- Salted SHA-1
- SHA-2
- Salted SHA-2

サーバーを構成した後は、新規パスワード (新規ユーザーの場合) または変更したパスワード (既存ユーザーの場合) は暗号化されてからディレクトリー・データベースに格納されます。暗号化されたパスワードには暗号化アルゴリズム名を示すタグが付くため、異なる形式で暗号化したパスワードをディレクトリーに共存させることができます。暗号化構成を変更しても、既存の暗号化されたパスワードは変更されず、引き続き有効となります。

クリア・パスワードを取得する必要があるアプリケーション (中間層認証エージェントなど) の場合、ディレクトリー管理者は、ユーザー・パスワードを両方向暗号化するかあるいは暗号化を実行しないようにサーバーを構成する必要があります。この場合、ディレクトリーに格納されるクリア・パスワードは、ディレクトリーの ACL メカニズムによって保護されます。

両方向暗号化形式は以下のとおりです。

- AES

AES は両方向暗号化オプションです。このオプションでは、`userPassword` 属性の値をディレクトリー内で暗号化し、元のクリアな形式で項目の一部として取得することができます。またこのオプションでは、128、192、および 256 ビット長のキーを使用するように構成できます。中間層認証サーバーなどの一部のアプリケーションではパスワードを平文形式で検索する必要がありますが、2 次的な永続記憶装置にクリア・パスワードを格納することが、会社のセキュリティー・ポリシーで禁止されている場合があります。このオプションによって、両方の要件を満たすことができます。

バインド要求で与えたパスワードが `userPassword` 属性の複数の値のいずれかと一致すれば、単純バインドは成功です。

Web 管理を使用してサーバーを構成すると、以下の暗号化オプションのいずれかを選択することができます。

なし 暗号化を行いません。パスワードは平文形式で格納されます。

crypt パスワードを UNIX `crypt` 暗号化アルゴリズムによって暗号化してからディレクトリーに格納します。

MD5 パスワードを MD5 メッセージ・ダイジェスト・アルゴリズムによって暗号化してからディレクトリーに格納します。

SHA-1 パスワードを SHA-1 暗号化アルゴリズムによって暗号化してからディレクトリーに格納します。

Salted SHA-1

パスワードを Salted SHA-1 暗号化アルゴリズムによって暗号化してからディレクトリーに格納します。

SHA-2 パスワードを SHA-2 ファミリーの暗号化アルゴリズムによって暗号化して

からディレクトリーに格納します。SHA-2 ファミリーの暗号化アルゴリズムでサポートされる暗号化スキームは、以下のとおりです。

- SHA-224
- SHA-256
- SHA-384
- SHA-512

Salted SHA-2

パスワードを Salted SHA-2 ファミリーの暗号化アルゴリズムによって暗号化してからディレクトリーに格納します。Salted SHA-2 ファミリーの暗号化アルゴリズムでサポートされる暗号化スキームは、以下のとおりです。

- SSHA-224
- SSHA-256
- SSHA-384
- SSHA-512

AES128

パスワードは、AES128 アルゴリズムで暗号化してからディレクトリーに格納され、項目の一部として、元のクリアな形式で取得されます。

AES192

パスワードは、AES192 アルゴリズムで暗号化してからディレクトリーに格納され、項目の一部として、元のクリアな形式で取得されます。

AES256

パスワードは、AES256 アルゴリズムで暗号化してからディレクトリーに格納され、項目の一部として、元のクリアな形式で取得されます。

注: 前のリリースで使用可能だった `imask` 形式は、現在のリリースでは暗号化オプションとして使用できません。ただし、既存の `imask` 暗号化値は現在のリリースでも処理できます。

デフォルト・オプションは **AES256** です。変更内容は、サーバー構成ファイルのパスワード暗号化ディレクティブに登録されます。

```
ibm-SlapdPwEncryption: AES256
```

サーバー構成ファイルは以下の場所にあります。

```
<instance_directory>%etc%ibmslapd.conf
```

`userPassword` の他に、`secretKey` 属性の値も必ずディレクトリー内で「AES256」暗号化されます。`userPassword` とは異なり、`secretKey` の値にはこの暗号化が強制的に実行されます。他のオプションはありません。`secretKey` 属性は、IBM 定義のスキーマです。アプリケーションは、常に暗号化されている必要がある機密データをディレクトリー内に保管する場合や、ディレクトリー・アクセス制御を使用してデータを平文フォーマットで取り出す場合に、この属性を使用することができます。

構成ファイルについて詳しくは、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。

パスワード暗号化をタイプを指定するには、以下のいずれかの方法を使用します。

注:

1. UNIX の crypt 方式を使用する場合は、先頭から 8 文字のみが有効となります。
2. 片方向暗号化されたパスワードは、パスワードの比較に使用することはできません。ログイン・パスワードは、ユーザー・ログイン時に暗号化され、格納されているパスワードと比較され、一致するかどうか検証されます。

Web 管理の使用

以下に示す指示により、パスワード暗号化を設定することができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「セキュリティー・プロパティーの管理」をクリックします。「パスワード暗号化」タブをクリックします。

パスワード暗号化を設定するには、以下を行います。

1. 「パスワード暗号化メカニズムの設定」フィールドから、パスワード暗号化タイプを選択します。
2. 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして変更を適用し、このパネルを終了します。
 - 「適用」をクリックして変更内容を適用し、このパネルを表示させたままにします。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

コマンド・ラインの使用

以下に示すコマンドをコマンド行で使用することにより、暗号化のタイプを変更することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=configuration
changetype: modify
replace: ibm-slapdPWEncryption
ibm-slapdPWEncryption: <password encryption mechanism>
```

Here, the ibm-slapdPWEncryption attribute can be assigned any of the following values: none, aes128, aes192, aes256, crypt, sha, ssha, md5 sha224, sha256, sha384, sha512, ssha224, ssha256, ssha384, or ssha512.

更新した設定を動的に有効にするには、以下の `idsldapexop` コマンドを発行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readconfig -scope single
"cn=configuration" ibm-slapdPWEncryption
```

パスワード・ポリシー設定

パスワード・ポリシーを設定する場合は、以下の情報を参照してください。

パスワード・ポリシーは、IBM Security Directory Server でのパスワードの使用法および管理方法を制御する一連の規則です。これらの規則を設定すると、ユーザーが定期的にパスワードを変更すること、およびパスワードが組織のパスワード構文要件を満たすことが保証されます。これらの規則では、古いパスワードの再利用を制限したり、バインド試行失敗が指定の回数を超えた場合にユーザーをロックアウトすることもできます。

管理者がパスワード・ポリシーをオンにする要求を送信すると、サーバーで `ibm-pwdPolicyStartTime` 属性が生成されます。この属性は、クライアント要求によって削除や変更することができないオプションの属性です。 `ibm-pwdPolicyStartTime` 属性を変更できるのは、管理制御権を持つ管理者のみです。この属性の値は、管理者がパスワード・ポリシーをオンにしたときとオフにしたときに変更されます。 `ibm-pwdPolicyStartTime` 属性をオンにしてからオフにすると、この属性の値がリセットされます。 `modifyTimestamp` 項目に基づいて評価されるユーザー項目の最終変更時刻、および `ibm-pwdPolicyStartTime` は、変更されている可能性があります。その結果、パスワード・ポリシーをオンまたはオフにしたときに、有効期限が切れている一部の古いパスワードが期限切れにならない場合があります。

注: パスワード・ポリシー項目を個別のパスワード・ポリシーまたはグループ・パスワード・ポリシーとしてユーザー項目またはグループ項目に関連付けるには、最初にそのパスワード・ポリシー項目を作成しておく必要があります。参照先のパスワード・ポリシー項目が存在しない場合、「実行を望んでいません (unwilling to perform)」というメッセージが返されます。ユーザーまたはグループ項目によってパスワード・ポリシー項目が参照されている場合、そのパスワード・ポリシー項目の名前を変更したり削除したりすることはできません。変更や削除を行うには、その項目とユーザー項目またはグループ項目との関連を削除する必要があります。

パスワードについては、245 ページの『パスワードのガイドライン』を参照してください。

IBM Security Directory Server には、3 つのタイプのパスワード・ポリシー (個別、グループ、およびグローバルのパスワード・ポリシー) があります。

グローバル・パスワード・ポリシー

グローバル・パスワード・ポリシーを処理する場合は、以下の情報を参照してください。

グローバル・パスワード・ポリシー項目 (`cn=pwdpolicy,cn=ibmpolicies`) がサーバーによって作成されると、属性 `ibm-pwdPolicy` がデフォルト値である `FALSE` に設定されます。この場合、サーバーはすべてのパスワード・ポリシー項目を無視します。サーバーによりパスワード規則が適用されるのは、`ibm-pwdPolicy` 属性が `TRUE` に設定されている場合のみです。グローバル・パスワード・ポリシーが適用され、`cn=pwdpolicy,cn=ibmpolicies` の `ibm-pwdGroupAndIndividualEnabled` 属性が `TRUE` に設定されている場合、パスワード・ポリシーを評価する際に、グループ・パスワード・ポリシーと個別パスワード・ポリシーも考慮されます。

注: 管理制御権を持っているグローバル管理グループ・メンバー、1 次管理者、ローカル管理グループ・メンバーは、グループ・パスワード・ポリシーと個別パスワード・ポリシーの有効と無効を切り替えることができます。

グループ・パスワード・ポリシー

グループ・パスワード・ポリシーを処理する場合は、以下の情報を参照してください。

グループ・パスワード・ポリシーを使用すると、グループのメンバーを特別なパスワード規則のセットによって制御できます。グループ・パスワード・ポリシーの場合、`accessGroup`、`accessRole`、`groupOfNames` などの任意のユーザー・グループ・オブジェクトで、パスワード・ポリシー項目を指す `ibm-pwdGroupPolicyDN` 属性を使用することができます。

1 つのユーザー項目が複数のグループに属している場合があるため、ユーザーのグループ・ポリシーを決定する前に、複数のグループ・パスワード・ポリシー項目が評価されます。複合グループ・ポリシーを評価するために、グループ・パスワード・ポリシー項目が結合されます。これにより、他の属性よりも優先される最も制限の厳しい属性値を持つ属性の集合が形成されます。

個別のパスワード・ポリシー

個別のパスワード・ポリシーを処理する場合は、以下の情報を参照してください。

個別パスワード・ポリシーを使用すると、すべてのユーザー項目に専用のパスワード・ポリシーを設定できます。個別パスワード・ポリシーでは、パスワード・ポリシー項目を指す `ibm-pwdIndividualPolicyDN` 属性を使用して、ユーザーが専用のパスワード・ポリシー項目を持つように拡張できます。パスワード・ポリシー項目の属性を変更することによって、管理者は、ユーザー項目を変更せずに一連のユーザーのパスワード・ポリシーを効率よく管理できます。

注: 管理者は、パスワード・ポリシー拡張ユーザー項目の `ibm-pwdIndividualPolicyDN` 属性に `cn=noPwdPolicy` という値を割り当てることにより、特定のユーザーをすべてのパスワード・ポリシー制御から除外することができます。

パスワード・ポリシーの評価

ユーザーの有効なパスワード・ポリシーを評価するには、ユーザーに関連付けられたすべてのパスワード・ポリシーが個別パスワード・ポリシーとともに考慮されます。

グループ・パスワード・ポリシーが考慮され、最後にグローバル・パスワード・ポリシーが考慮されます。ある属性が個別パスワード・ポリシー項目に定義されていない場合、その属性は複合グループ・パスワード・ポリシー項目の中で検索されます。複合グループ・ポリシー項目の中でも検出されなかった場合は、グローバル・パスワード・ポリシー項目の中にある該当の属性が使用されます。グローバル・パスワード・ポリシー項目にもその属性が定義されていない場合は、デフォルト値が使用されます。

注: 指定されたユーザーの有効なパスワード・ポリシーを表示するには、有効パスワード・ポリシー拡張操作 (`effectpwdpolicy`) を使用します。有効なパスワード・ポリシーを計算するために使用されるパスワード・ポリシー項目に関する情報も、この拡張操作を使用して表示できます。この拡張操作について詳しくは、「*IBM Security Directory Server Version 6.3.1 Command Reference*」を参照してください。

ユーザーのグループ・パスワード・ポリシーの評価:

ユーザー項目は複数のグループに属している場合があるため、ユーザーの複合グループ・ポリシーを決定するために複数のグループ・パスワード・ポリシー項目が評価される場合があります。ユーザーの複合グループ・パスワード・ポリシーは、ルールのリストを参照して決定することができます。

1. パスワード・ポリシー項目の `ibm-pwdPolicy` が `False` に設定されている場合、その項目内に定義された属性は、複合グループ・パスワード・ポリシーの決定に使用されません。属性が設定されていない場合、属性にはデフォルト値 `False` が使用されます。
2. ユーザーが属しているすべてのグループで、`ibm-pwdGroupPolicyDN` の値が `cn=noPwdPolicy` である場合、そのユーザーについて評価される複合グループ・パスワードはありません。この場合、そのユーザーに個別パスワード・ポリシーが定義されていない限り、いずれのポリシーも (グローバル・ポリシーさえも) 適用されません。
3. デフォルト以外の値を使用して定義された属性は、デフォルト値で定義された場合より制約が強くなります。また、デフォルト値は、まったく定義されていない場合より制約が強くなります。
4. パスワード・ポリシー属性 `passwordMinAlphaChars`、`pwdMinLength`、および `passwordMinOtherChars` は、相互に依存する属性です。例えば、`passwordMinAlphaChars` の値は、`pwdMinLength` の値から `passwordMinOtherChars` の値を引いた結果より小さいか等しい値に設定する必要があります。属性値間にこの相互依存性があるため、あるポリシーから 1 つの属性を選択すると、その他の 2 つの属性も同じポリシーから選択されます。

選択の順序は、`pwdMinLength`、`passwordMinOtherChars`、`passwordAlphaChars` です。つまり、選択はまず、`pwdMinLength` の最大値を選出することで行われます。2 つのグループ・ポリシーの `pwdMinLength` 属性の値が同じ場合には、`passwordMinOtherChars` の値が最大のものが選択されます。1 つの属性が選択されると、その他の 2 つの属性は自動的に選択されます。

5. `passwordMaxConsecutiveRepeatedChars` 属性は、パスワード内で特定の文字を連続して繰り返し使用できる最大回数を制限するために使用します。`passwordMaxRepeatedChars` および `passwordMaxConsecutiveRepeatedChars` は両方とも、互いに独立して使用可能または使用不能に設定できます。ただし、これらの属性を両方とも使用可能にする場合には、以下の規則が適用されます。
 - `passwordMaxRepeatedChars` 属性の値は、`passwordMaxConsecutiveRepeatedChars` 属性の値より大きいか等しくなければなりません。
 - 複数のパスワード・ポリシーを使用可能にすると、`passwordMaxConsecutiveRepeatedChars` は、`passwordMaxRepeatedChars` の選出元と同じポリシーから選出されます。すべてのポリシーで `passwordMaxRepeatedChars` を使用不可にした場合は、`passwordMaxConsecutiveRepeatedChars` の最も制限の強い値が選出されます。
 - `passwordMaxConsecutiveRepeatedChars` 属性を 0 に設定すると、連続する繰り返し文字の数は検査されません。`passwordMaxConsecutiveRepeatedChars` を 1 に設定すると、特定の文字の直後に同じ文字をもう 1 つ続けることはできま

せん。例えば、passwordMaxConsecutiveRepeatedChars 属性を 1 に設定すると、「aba」はパスワードとして有効な値ですが、「aab」は無効値になります。

同様に、passwordMaxConsecutiveRepeatedChars 属性を 2 に設定した場合、パスワード内で同じ文字を連続して使用できる最大回数は 2 回です。

6. 最も制限の強い属性値を優先的に使用してすべてのグループ・パスワード・ポリシー項目の属性が結合され、属性結合が形成されます。最強制限の属性値の決定方法を以下の表に示します。

表 23. 最強制限の属性値の決定

パスワード・ポリシー属性	説明	制限が強い方の値	有効な値	デフォルト値
pwdAttribute	pwdAttribute 属性は、パスワード・ポリシーが適用されている属性の名前を指定します。この属性は、userPassword 属性にのみ設定できます。	N/A	userPassword	userPassword
pwdMinAge	pwdMinAge 属性は、パスワードの最終変更後、パスワードが次に変更されるまでに経過する必要がある秒数を指定します。	より大きい値	0 以上 (GE)	0 - 存続期間制限なし
pwdMaxAge	pwdMaxAge 属性は、パスワードの有効期限が切れるまでの秒数を指定します (0 はパスワードの有効期限が切れないことを意味します)。	より小さい値	GE 0	0 - パスワードの有効期限切れなし
pwdInHistory	pwdInHistory 属性は、pwdHistory 属性に格納されるパスワードの数を指定します。	より大きい値	0 から 10	0 - パスワード履歴なし
pwdCheckSyntax	pwdCheckSyntax 属性は、パスワードの構文を検査するかどうかを指示します。pwdCheckSyntax 属性の値は、以下のオプションを示します。 <ul style="list-style-type: none"> • '0': 構文検査を行わない • '1': サーバーで構文検査を行うが、(パスワードがハッシュ化されていたり、他の理由により) サーバーが構文を検査できない場合は受け入れる • '2': サーバーで構文検査を行うが、サーバーが構文を検査できない場合は、エラーを返してパスワードを拒否する 	より大きい値	0, 1, 2 1 - サーバーで構文検査できない場合、パスワードを受け入れる、2 - サーバーで構文検査できない場合、パスワードを拒否する	0
pwdMinLength	pwdMinLength 属性は、パスワード・ストリングに設定する必要がある最小の長さを指定します。サーバーは、pwdCheckSyntax 属性の値に基づいて最小の長さを検査します。	より大きい値	GE 0	0 - 最小の長さなし
pwdExpireWarning	pwdExpireWarning 属性は、パスワードの有効期限が切れる前、有効期限の警告メッセージが認証ユーザーに返される期間を最大秒数で指定します。	より大きい値	GE 0	0 - 警告を送信しない
pwdGraceLoginLimit	pwdGraceLoginLimit 属性は、ユーザーを認証するために有効期限切れのパスワードを使用できる回数を指定します。	より小さい値	GE 0	0 - 猶予ログインなし
pwdLockout	pwdLockout 属性は、指定した連続バインド試行失敗回数に達した後で、認証用にパスワードを使用できるかどうかを指定します。	True	True/False	False
pwdLockoutDuration	pwdLockoutDuration 属性は、指定した 'pwdMaxFailure' バインド試行失敗の回数に達したために、パスワードを認証のために使用できない秒数を指定します。	より大きい値	GE 0	0 - リセットまでロックアウト
pwdMaxFailure	pwdMaxFailure 属性は、これ以降の認証でパスワードを考慮しなくなるまでの連続バインド試行失敗の最大回数を指定します。pwdMaxFailure 属性に 0 の値を設定する場合、pwdLockout の値は無視されます。	より小さい値	GE 0	0 - 失敗カウントなし、ロックアウトなし

表 23. 最強制限の属性値の決定 (続き)

パスワード・ポリシー属性	説明	制限が強い方の値	有効な値	デフォルト値
pwdFailureCountInterval	pwdFailureCountInterval 属性は、有効または無効なバインド試行の後にパスワードの失敗項目が失敗カウンターから除去されるまでの秒数を指定します。有効なバインドの場合、パスワードの失敗はユーザー項目から除去されます。無効なバインドの場合、pwdFailureCountInterval の期限が切れる前のパスワードの失敗項目が除去され、最新のパスワードの失敗項目がユーザー項目に記録されます。	より大きい値	GE 0	0 – カウントなし、認証成功によりリセット
pwdMustChange	pwdMustChange 属性は、管理者によるパスワードの再設定後に、ユーザーが初めてディレクトリーにバインドするときに、ユーザーがパスワードを変更する必要があるかどうかを指定します。	True	True/False	True/False (cn=noPwdPolicy の場合)
pwdAllowUserChange	pwdAllowUserChange 属性は、ユーザーが自分のパスワードを変更できるかどうかを指定します。	True	True/False	True
pwdSafeModify	pwdSafeModify 属性は、パスワードの変更時に既存のパスワードを送信する必要があるかどうかを指定します。	True	True/False	False
ibm-pwdPolicy	ibm-pwdPolicy 属性は、パスワード・ポリシーをオンにするかオフにするかを指定します。	True	True/False	False
passwordMinAlphaChars	passwordMinAlphaChars 属性は、パスワード・ストリングに含める必要がある英字の最小数を指定します。サーバーが英字の数を検査できない場合、サーバーは pwdCheckSyntax 属性の値に基づいて処理を続行します。	より大きい値	GE 0	0 – 最小英字数の適用なし
passwordMinOtherChars	passwordMinOtherChars 属性は、パスワード・ストリングに含める必要がある数字および特殊文字の最小数を指定します。サーバーがその他の文字数を検査できない場合、サーバーは pwdCheckSyntax 属性の値に基づいて処理を続行します。	より大きい値	GE 0	0 – その他の文字の最小数なし
passwordMaxRepeatedChars	passwordMaxRepeatedChars 属性は、パスワード内で特定の 1 文字を使用できる最大回数を指定します。サーバーが実際のパスワード文字を検査できない場合、サーバーは pwdCheckSyntax 属性の値に基づいて処理を続行します。	より小さい値	GE 0	0 – 最大繰り返し文字なし
passwordMaxConsecutiveRepeatedChars	passwordMaxConsecutiveRepeatedChars 属性は、パスワード内で特定の文字を連続して繰り返し使用できる最大回数を制限するために使用します。	より小さい値	GE 0	0 – 連続する反復文字の最大数なし
passwordMinDiffChars	passwordMinDiffChars 属性は、古いパスワードおよび pwdHistory に格納されているパスワードの文字と異なっている必要がある新規パスワードの文字の最小数を指定します。パスワードが片方向で暗号化されていて、サーバーが実際のパスワード文字を検査できない場合、サーバーは pwdCheckSyntax 属性の値に基づいて処理を続行します。	より大きい値	GE 0	0 – パスワード間の異なっている文字の最小数なし

上で定義した規則に基づき、ユーザーの複合グループ・ポリシーが決定されます。複合グループ・ポリシーの決定方法をさらによく理解するために、以下の表に示すいくつかの例を検討してください。

表 24. 複合グループ・ポリシーの決定

グループ X のパスワード・ポリシー	グループ Y のパスワード・ポリシー	グループ Z のパスワード・ポリシー	複合グループのパスワード・ポリシー
<p>pwdMaxAge = 86400</p> <p>pwdSafeMode = True</p> <p>pwdMaxFailure = 5</p> <p>ibm-pwdPolicy = True</p> <p>ibm-pwdPolicyStarttime = 20060406200000</p>	<p>pwdMaxAge = 43200</p> <p>pwdSafeMode = False</p> <p>ibm-pwdPolicy = True</p> <p>ibm-pwdPolicyStarttime = 20060306200000</p>	<p>pwdCheckSyntax = 1</p> <p>ibm-pwdPolicy = True</p> <p>ibm-pwdPolicyStarttime = 20060506200000</p>	<p>pwdMaxAge = 43200</p> <p>pwdSafeMod = True</p> <p>pwdCheckSyntax = 1</p> <p>pwdMaxFailure = 5</p> <p>ibm-pwdPolicy = True</p> <p>ibm-pwdPolicyStarttime = 20060306200000</p>
<p>pwdMaxAge = 86400</p> <p>ibm-pwdPolicy = True</p>	<p>pwdMaxAge = 43200</p> <p>pwdSafeMode = True</p>	<p>pwdMaxAge = 0</p> <p>ibm-pwdPolicy = True</p>	<p>pwdMaxAge = 86400</p> <p>pwdSafeMode = False</p> <p>ibm-pwdPolicy = True</p> <p>注: グループ Y のパスワード・ポリシーは複合グループ・ポリシーの計算には使用されません。このポリシーの ibm-pwdPolicy が定義されていないため、デフォルトで FALSE に設定されるからです。</p>
<p>pwdMinLength = 10</p> <p>passwordMinOtherChars = 4</p> <p>passwordMinAlphaChars= 6</p> <p>ibm-pwdPolicy = True</p>	<p>pwdMinLength = 12</p> <p>ibm-pwdPolicy = True</p>		<p>pwdMinLength = 12</p> <p>ibm-pwdPolicy = True</p>
<p>pwdMinLength = 10</p> <p>passwordMinOtherChars = 4</p> <p>passwordMinAlphaChars = 6</p> <p>ibm-pwdPolicy = True</p>		<p>pwdMinLength = 10</p> <p>passwordMinOtherChars = 5</p> <p>passwordMinAlphaChars = 3</p> <p>ibm-pwdPolicy = True</p>	<p>pwdMinLength =10</p> <p>passwordMinOtherChars = 5</p> <p>passwordMinAlphaChars = 3</p> <p>ibm-pwdPolicy = True</p>
<p>passwordMaxConsecutiveRepeatedChars=0</p> <p>passwordMaxRepeatedChars=5</p> <p>ibm-pwdPolicy = True</p>	<p>passwordMaxConsecutiveRepeatedChars=2</p> <p>ibm-pwdPolicy = True</p>	<p>passwordMaxRepeatedChars=3</p> <p>ibm-pwdPolicy = True</p>	<p>passwordMaxRepeatedChars=3</p> <p>passwordMaxConsecutiveRepeatedChars=0</p> <p>ibm-pwdPolicy = True</p>
<p>passwordMaxConsecutiveRepeatedChars=4</p> <p>passwordMaxRepeatedChars=0</p> <p>ibm-pwdPolicy = True</p>	<p>passwordMaxConsecutiveRepeatedChars=1</p> <p>passwordMaxRepeatedChars=0</p> <p>ibm-pwdPolicy = True</p>		<p>passwordMaxConsecutiveRepeatedChars=1</p> <p>passwordMaxRepeatedChars=0</p> <p>ibm-pwdPolicy = True</p>
<p>passwordMaxConsecutiveRepeatedChars=4</p> <p>passwordMaxRepeatedChars=2</p> <p>ibm-pwdPolicy = True</p>	<p>passwordMaxConsecutiveRepeatedChars=2</p> <p>passwordMaxRepeatedChars=3</p> <p>ibm-pwdPolicy = True</p>		<p>passwordMaxConsecutiveRepeatedChars=4</p> <p>passwordMaxRepeatedChars=2</p> <p>ibm-pwdPolicy = True</p>

有効なパスワード・ポリシーの評価:

ユーザーの有効なパスワード・ポリシーが評価されるのは、グローバル・パスワード・ポリシー項目の `ibm-pwdPolicy` 属性が TRUE に設定されている場合のみです。グローバル・ポリシーが使用不可になっている場合でも、個別ポリシーやグループ・ポリシーなど、他のパスワード・ポリシーを使用可能にできます。ただし、これらのポリシー規則はユーザーに影響を与えません。

ibm-pwdPolicy が TRUE に設定されている場合、ibm-pwdPolicyStartTime 属性は現在のシステム時刻に設定されます。この設定は、グローバル・パスワード・ポリシー項目が FALSE に設定されている場合にも実行されます。ただし、グローバル・ポリシーが使用可能になっていない限り、ibm-pwdPolicyStartTime 値は有効なポリシーの評価には使用されません。グローバル・ポリシーが使用可能に設定されると、この属性の値が個別ポリシーから、次にグループ・ポリシーから、そして最後にグローバル・ポリシーから選択されます。ibm-pwdPolicyStartTime は、すべてのアクティブ・パスワード・ポリシーにあるため、個別ポリシーの開始時刻があれば、それが他のポリシーの開始時刻をオーバーライドして、ユーザーの有効なパスワード・ポリシーの開始時刻になります。

以下の表に、ユーザーの有効なパスワード・ポリシーの判別方法を示す一連の例を示します。

表 25. 有効なパスワード・ポリシーの判別

個別のパスワード・ポリシー	グループ・パスワード・ポリシー	グローバル・パスワード・ポリシー	有効なパスワード・ポリシー
pwdMaxAge = 86400	pwdMaxAge =43200	ibm-pwdPolicy = True	pwdMaxAge = 86400
ibm-pwdPolicy = True	ibm-pwdPolicy = True	pwdMinAge = 43200	ibm-pwdPolicy = True
pwdMinAge = 21600	pwdInHistory = 5	pwdInHistory = 3	pwdMinAge = 21600
pwdLockout = True	ibm-pwdPolicyStarttime = 20060306200000	pwdCheckSyntax = 0	pwdInHistory = 5
ibm-pwdPolicyStarttime = 20060406200000		pwdMinLength = 0	pwdCheckSyntax = 0
		pwdExpireWarning = 0	pwdMinLength = 0
		pwdGraceLoginLimit = 0	pwdExpireWarning = 0
		pwdLockoutDuration = 0	pwdGraceLoginLimit = 0
		pwdMaxFailure =0	pwdLockoutDuration = 0
		pwdFailureCount Interval=0	pwdMaxFailure =0
		passwordMinAlpha Chars=0	pwdFailureCountInterval=0
		passwordMinOther Chars=0	passwordMinAlphaChars=0
		passwordMax RepeatedChars=0	passwordMinOtherChars=0
		passwordMinDiff Chars=0	passwordMaxRepeatedChars=0
		pwdLockout=False	passwordMinDiffChars=0
		pwdAllowUser Change=True	pwdLockout=True
		pwdMustChange=True	pwdAllowUserChange=True
		pwdSafeModify =False	pwdMustChange=True
		ibm-pwdPolicyStarttime = 20060506200000	pwdSafeModify=False
			ibm-pwdPolicyStarttime = 20060406200000

表 25. 有効なパスワード・ポリシーの判別 (続き)

個別のパスワード・ポリシー	グループ・パスワード・ポリシー	グローバル・パスワード・ポリシー	有効なパスワード・ポリシー
<p>pwdMaxAge = 86400</p> <p>ibm-pwdPolicy = True</p> <p>pwdMinAge = 21600</p> <p>pwdMinLength = 8</p> <p>pwdLockout = True</p> <p>ibm-pwdPolicyStarttime = 20060406200000</p>	<p>pwdMaxAge =43200</p> <p>ibm-pwdPolicy = True</p> <p>pwdInHistory = 5</p> <p>ibm-pwdPolicyStarttime = 20060306200000</p>	<p>ibm-pwdPolicy = True</p> <p>pwdMinAge = 0</p> <p>pwdInHistory = 3</p> <p>pwdCheckSyntax = 0</p> <p>pwdMinLength = 10</p> <p>pwdExpireWarning = 0</p> <p>pwdGraceLoginLimit = 0</p> <p>pwdLockoutDuration = 0</p> <p>pwdMaxFailure =0</p> <p>pwdFailureCount Interval=0</p> <p>passwordMinAlpha Chars=4</p> <p>passwordMinOther Chars=4</p> <p>passwordMax RepeatedChars=0</p> <p>passwordMinDiff Chars=0</p> <p>pwdLockout=False</p> <p>pwdAllowUser Change=True</p> <p>pwdMustChange =True</p> <p>pwdSafeModify =False</p> <p>ibm-pwdPolicyStarttime = 20060506200000</p>	<p>pwdMaxAge = 86400</p> <p>ibm-pwdPolicy = True</p> <p>pwdMinAge = 21600</p> <p>pwdInHistory = 5</p> <p>pwdCheckSyntax = 0</p> <p>pwdMinLength = 8</p> <p>pwdExpireWarning = 0</p> <p>pwdGraceLoginLimit = 0</p> <p>pwdLockoutDuration = 0</p> <p>pwdMaxFailure =0</p> <p>pwdFailureCountInterval=0</p> <p>passwordMinAlphaChars=0</p> <p>passwordMinOtherChars=0</p> <p>passwordMaxRepeatedChars=0</p> <p>passwordMinDiffChars=0</p> <p>pwdLockout=True</p> <p>pwdAllowUserChange=True</p> <p>pwdMustChange=True</p> <p>pwdSafeModify=False</p> <p>ibm-pwdPolicyStarttime = 20060406200000</p>
<p>passwordMaxConsecutive RepeatedChars=1</p> <p>passwordMaxRepeated Chars=0</p> <p>ibm-pwdPolicy = True</p>	<p>passwordMaxConsecutive RepeatedChars=1</p> <p>passwordMaxRepeated Chars=10</p> <p>ibm-pwdPolicy = True</p>	<p>passwordMaxRepeated Chars=4</p> <p>ibm-pwdPolicy = True</p>	<p>passwordMaxConsecutive RepeatedChars=1</p> <p>passwordMaxRepeatedChars=0</p> <p>ibm-pwdPolicy = True</p>

パスワード・ポリシー属性

パスワード・ポリシー機能は、複数の運用属性に対し、指定されたディレクトリー項目のパスワード・ポリシー状態情報を提供します。

属性を使用すると、特定状態 (パスワードの有効期限切れ) の項目を照会でき、管理者は特定のポリシー状態をオーバーライドできます (ロック状態のアカウントのアンロック)。669 ページの『パスワード・ポリシー運用属性』を参照してください。

デフォルト設定の要約

すべてのユーザー・パスワードに対してデフォルトのパスワード・ポリシーが設定されます。

ユーザー・パスワードのデフォルトのパスワード・ポリシー設定を以下の表に示します。

表 26. ユーザー・パスワード・ポリシー設定

Web 管理ツール・パラメーター	デフォルト設定
使用可能になっているパスワード・ポリシー: <code>ibm-pwdPolicy</code>	false
パスワード暗号化: <code>ibm-slappwEncryption</code>	AES256
ユーザーは、パスワードの変更時に旧パスワードを指定する必要がある: <code>pwdSafeModify</code>	false
リセット後、ユーザーは必ずパスワードを変更する: <code>pwdMustChange</code>	true
パスワード有効期限: <code>pwdMaxAge</code>	0
期限切れ後の猶予ログイン回数: <code>pwdGraceLoginLimit</code>	0
バインド試行が指定した回数連続して失敗したらアカウントをロックアウトする: <code>pwdLockout</code>	false
アカウントがロックアウトされるまでのバインド試行の連続失敗回数: <code>pwdMaxFailure</code>	0
パスワード変更の最小時間間隔: <code>pwdMinAge</code>	0
アカウント・ロックアウトの有効期限が切れるまでの時間。アカウント・ロックアウトを永続させることも可能: <code>pwdLockoutDuration</code>	0
不正なログインの有効期限が切れるまでの時間。正しいパスワードを使用した場合のみ不正なログインをクリアすることも可能: <code>pwdFailureCountInterval</code>	0
再利用前に必要なパスワードの最小変更回数: <code>pwdInHistory</code>	0
パスワード構文を検査する: <code>pwdCheckSyntax</code>	0
最小の長さ: <code>pwdMinLength</code>	0
英字の最小数: <code>passwordMinAlphaChars</code>	0
数字および特殊文字の最小数: <code>passwordMinOtherChars</code>	0
繰り返し文字の最大数: <code>passwordMaxRepeatedChars</code>	0
連続反復文字の最大数: <code>passwordMaxConsecutiveRepeatedChars</code>	0
新パスワードの最小文字数 (旧パスワードの最小文字数と異なる値であること): <code>passwordMinDiffChars</code>	0

ディレクトリー管理者、管理グループのメンバー、およびマスター・サーバー DN 以外のすべてのユーザーは、構成したユーザー・パスワード・ポリシーを遵守しなければなりません。管理者、管理グループのメンバー、およびマスター・サーバー DN のパスワードには、有効期限はありません。ディレクトリー管理者、管理グループのメンバー、およびマスター・サーバー DN には、ユーザーのパスワードとユーザー・パスワード・ポリシーを変更できるアクセス・コントロール権限があります。グローバル管理グループのメンバーは、ユーザー・パスワード・ポリシーに従いますが、ユーザー・パスワード・ポリシーの設定を変更できる権限も持ちます。

管理者、管理グループのメンバー、およびマスター・サーバー DN のパスワード・ポリシーは、構成ファイルで設定します。

表 27. 管理パスワード・ポリシーの設定

管理パスワードの要件	デフォルト設定
使用可能になっているパスワード・ポリシー: <code>ibm-slappwConfigPwdPolicyOn</code>	false
バインド試行が指定した回数連続して失敗したらアカウントをロックアウトする: <code>pwdLockout</code>	true

表 27. 管理パスワード・ポリシーの設定 (続き)

管理パスワードの要件	デフォルト設定
パスワード・ロックアウト前に許容する無効なログインの回数: <code>pwdMaxFailure</code>	10
アカウント・ロックアウトの有効期限が切れるまでの時間。アカウント・ロックアウトを永続させることも可能: <code>pwdLockoutDuration</code>	300
不正なログインの有効期限が切れるまでの時間。正しいパスワードを使用した場合のみ不正なログインをクリアすることも可能: <code>pwdFailureCountInterval</code>	0
最小の長さ: <code>pwdMinLength</code>	8
英字の最小数: <code>passwordMinAlphaChars</code>	2
数字および特殊文字の最小数: <code>passwordMinOtherChars</code>	2
繰り返し文字の最大数: <code>passwordMaxRepeatedChars</code>	2
新パスワードの最小文字数 (旧パスワードの最小文字数と異なる値であること): <code>passwordMinDiffChars</code>	2

デフォルトでは、管理パスワード・ポリシーは `false` に設定されています。管理パスワード・ポリシーを有効にすると、その他の属性とそれらのデフォルト設定も有効になります。

パスワードのガイドライン

パスワードのガイドラインには、IBM Security Directory Server のユーザー項目用にサポートされている IBM Security Directory Server パスワード属性の値の詳細が含まれています。これらのガイドラインには、LDAP 環境を管理するために使用されるアカウントの詳細も含まれています。

ガイドラインには、IBM Security Directory Server のコマンド行ツールおよび C-API インターフェースを実行する際の混乱を少なくするために回避すべき文字が含まれています。

IBM Security Directory Server には、次の 2 種類のユーザー・アカウントがあります。

- アドミニストレーション・アカウント (LDAP 管理者 (`cn=root`)、管理者グループのメンバー、マスター・サーバー DN)。これらは `<instance_directory>/etc/ibmslapd.conf` ファイルに保管されます。
- Directory Server の C および Java (JNDI) API と組み合わせて使用するパスワード属性を持つユーザー項目 (`iNetOrgPerson`)。これらの項目は、Security Access Manager や WebSphere などのアプリケーションが使用するインターフェースです。Directory Server はパスワード項目の値を幅広くサポートしていますが、アプリケーションの資料を調べて、適用されるガイドラインや制約事項を確認する必要があります。

注: グローバル管理グループ・メンバー項目はディレクトリーに保管され、ユーザー項目と見なされます。

IBM Security Directory Server を使用する、サポート対象のパスワード値の詳細は、後出のセクションで説明します。

注: LDAP DB2 ユーザーは構成ファイルに保管されますが、パスワード・ポリシーには従いません。

ユーザー項目のパスワード (InetOrgPerson):

userPassword 属性フィールドでサポート対象の文字を使用して、C および Java API 経由で Directory Server に格納することができます。

Policy Director や WebSphere など、Directory Server を使用しているアプリケーションには、パスワード値に対して追加の制約が課される場合があります。詳細については、これらの製品の資料を参照してください。

- すべての英字の大文字と小文字および数字。
- それ以外のすべての ASCII 1 バイト文字もサポートされます。
- IBM Security Directory Server の資料の『インストールと構成』セクションで指定された言語については、2 バイト文字がサポートされます。
- パスワードでは、大文字小文字の区別を行います。(例えば、password = TeSt の場合、パスワード TEST または test を使用すると拒否されます。大文字と小文字を正確に記述した TeSt のみが受け入れられます。)

LDAP ibmslapd.conf ユーザー:

instance_directory/etc/ibmslapd.conf ファイル内のユーザーのパスワードには、サポート対象の文字のみ使用できます。

- 大文字と小文字を含むすべての英字と数字がサポートされます。
- それ以外のすべての ASCII 1 バイト文字もサポートされます。
- パスワードでは、大文字小文字の区別を行います。例えば、password = TeSt の場合、パスワード TEST または test を使用すると拒否されます。大文字と小文字を正確に記述した TeSt のみが受け入れられます。

注:

1. ibmslapd.conf ファイル内の定義済みユーザーは、以下の特権を持つことができます。
 - LDAP 管理者 (cn=root) - 1 次管理者
 - ローカル管理者グループのメンバー
 - 複製用のマスター ID (cn=MASTER)
 - LDAP DB 項目および変更ログ・データベース (LDAPDB2) の LDAP DB2 ユーザー

注: 管理パスワード・ポリシーは、DB2 ユーザー以外の上記すべてのユーザーに適用されます。

2. 管理者パスワードでの 2 バイト文字はサポートされていません。

パスワード属性を変更する Web 管理ツール:

サポート対象の文字を使用して、管理者パスワードを変更することができます。

Web 管理ツールを使用すると、パスワード属性フィールドの追加または変更において、以下の文字がサポートされます。

- 大文字と小文字を含むすべての英字と数字がサポートされます。
- それ以外のすべての ASCII 1 バイト文字もサポートされます。

- パスワードでは、大文字小文字の区別を行います。例えば、password = TeSt の場合、パスワード TEST または test を使用すると拒否されます。大文字と小文字を正確に記述した TeSt のみが受け入れられます。

注:

- 管理者パスワードについては、2 バイト文字はサポートされていません。
- ユーザー・パスワードについては、2 バイト文字がサポートされています。

特殊文字:

いくつかの文字については、動作中のシェルによって解釈される可能性があるため、パスワードに使用しないでください。

以下の特殊文字を使用しないでください。

```
~
:
\
"
|
```

例えば、リリース 6.0 以降のバージョンの Web 管理ツールを使用して、ユーザー・パスワード属性に値 "%¥"test¥' を割り当てる場合、コマンド行で以下のパスワードを指定する必要があります。

```
-w"%¥¥"test¥'
```

以下に検索例を示します。

```
idsldapsearch -b" " -sbase-Dcn=newEntry,o=sample-w¥"¥¥¥"test¥' objectclass=*
```

注: このパスワードは、エスケープ文字のない元のパスワードを使用する、Web 管理ツールの Java アプリケーションで有効です。上記の例で、Web 管理ツールのバインド・パスワードは、Web 管理ツールでパスワードを割り当てるときに入力されたものと同じです。

```
"¥"test¥'
```

管理パスワードおよびロックアウト・ポリシーの設定

以下に示すコマンドを発行することで、管理パスワード・ポリシーをオンにすることができます。

このタスクについて

注: 管理パスワード・ポリシーは、コマンド行でのみ設定できます。Web 管理ツールは、管理パスワード・ポリシーには対応していません。

```
idsldapmodify -D <adminDN> -w <adminPW> -p <port> -i <filename>
```

where <filename> contains:

```
dn: cn=pwdPolicy Admin,cn=Configuration
changetype: modify
replace: ibm-slapdConfigPwdPolicyOn
ibm-slapdConfigPwdPolicyOn: true
```

管理パスワード・ポリシーを使用可能にし、デフォルト設定を変更するには、以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -p <port> -i <filename>
```

where <filename> contains:

```

dn: cn=pwdPolicy Admin,cn=Configuration
changetype: modify
replace: ibm-slappdConfigPwdPolicyOn
ibm-slappdConfigPwdPolicyOn: TRUE
-
replace: pwdlockout
pwdlockout: TRUE
#select TRUE to enable, FALSE to disable
-
replace:pwdmaxfailure
pwdmaxfailure: 10
-
replace:pwdlockoutduration
pwdlockoutduration: 300
# Value of pwdlockoutduration is in seconds.
-
replace:pwdfailurecountinterval
pwdfailurecountinterval: 0
-
replace:pwdminlength
pwdminlength: 8
-
replace:passwordminalphachars
passwordminalphachars: 2
-
replace:passwordminotherchars
passwordminotherchars: 2
-
replace:passwordmaxrepeatedchars
passwordmaxrepeatedchars: 2
-
replace:passwordmindiffchars
passwordmindiffchars: 2

```

管理アカウントのアンロック

管理アカウントのアンロックについては、以下の情報を参照してください。

このタスクについて

管理者が、ローカル管理グループ・メンバーまたはマスター・サーバー DN のパスワードを変更することでアカウントをアンロックしても、そのアカウントは、構成読み取り拡張操作が実行されて新規パスワードが有効になるまでロックされたままです。ローカル管理グループ・メンバーのパスワードの変更は、動的構成の更新要求が行われるまで有効になりません。管理者は、構成ファイルを変更したら、即時に動的更新要求を発行する必要があります。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```

dn: cn=admin1,cn=adminingroup,cn=configuration
changetype: modify
replace:ibm-slappdadminpw
ibm-slappdadminpw: newpassword123

```

設定を動的に更新するには、以下の `idsldapexop` コマンドを発行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readconfig -scope entire
```

注: 管理者のアカウントがロックされた場合、そのアカウントをアンロックするには、ローカル・コンソールにログオンする以外方法はありません。

グローバル・パスワード・ポリシー設定

グローバル・パスワード・ポリシーを設定する場合は、以下の情報を参照してください。

グローバル・パスワード・ポリシーは、RDBMS バックエンドに格納されている項目に適用されます。グローバル・パスワード・ポリシーを設定するには、以下のいずれかの手順を使用します。

Web 管理の使用:

Web 管理ツールを使用して、グローバル・パスワード・ポリシーを設定することができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「パスワード・ポリシーの管理」をクリックします。このパネルで、以下の操作を実行することができます。

- DIT に新規パスワード・ポリシーを追加する。
- 既存のパスワード・ポリシーを編集する。
- ポリシーの新規名およびロケーションを指定して、既存のパスワード・ポリシーのコピーを作成する。
- 既存のパスワード・ポリシーを削除する。

注: グローバル・パスワード・ポリシーは削除できません。

- 選択したパスワード・ポリシーの詳細を表示する。

パスワード・ポリシーを追加するには:

パスワード・ポリシーを追加する場合は、以下の情報を参照してください。

このタスクについて

新規パスワード・ポリシーを DIT に追加するには、「追加」ボタンをクリックするか「アクションの選択」リストから「追加」を選択し、次にパスワード・ポリシー・テーブルの「実行」をクリックします。これで、ポリシー定義ウィザードが起動します。このウィザードで、固有のパスワード・ポリシー名および必須の属性とその値を指定することによって、新規パスワード・ポリシーを定義できます。

属性選択:

属性選択とポリシー定義ウィザードの詳細については、以下の情報を参照してください。

このタスクについて

「ポリシー定義」ウィザードは、「属性選択」パネル、「パスワード・ポリシー設定 1」パネル、「パスワード・ポリシー設定 2」パネル、「パスワード・ポリシー設定 3」パネルから構成されています。「ポリシー定義」ウィザードのこれらのパネルを使用して、新しいパスワード・ポリシーの追加、既存のパスワード・ポリシーの編集、既存のパスワード・ポリシーのコピーの作成を行うことができます。

新規パスワード・ポリシーを追加したり既存のパスワード・ポリシーをコピーしたりする場合、ユーザーは「属性選択」パネルでパスワード・ポリシーに固有の名前を指定する必要があります。また、「属性選択」テーブルから属性を選択することにより、必須属性の値を指定することもできます。既存のパスワード・ポリシーを編集するときは、パスワード・ポリシー名を変更することはできませんが、選択したパスワード・ポリシーの属性値を変更することはできます。

注: 「属性選択」パネルの「属性選択」テーブルで選択する属性によっては、新規パスワード・ポリシーの追加時または既存のパスワード・ポリシーの編集やコピー時に、「ポリシー定義」ウィザードのすべてのパネルを開く必要がない場合があります。

このパネルで、以下の操作を実行することができます。

- 「ポリシー名」フィールドに固有のパスワード・ポリシー名を入力する。追加およびコピー操作では、固有のパスワード・ポリシー名を指定する必要があります。編集操作では、「ポリシー名」フィールドは読み取り専用です。
- パスワード・ポリシーに組み込む属性をテーブルから選び、グローバル・パスワード・ポリシー内にあるそれらの属性の値をオーバーライドする。

パスワード・ポリシー設定 1:

「パスワード・ポリシー設定 1」パネルのコントロールは、「属性選択」パネルでの属性の選択に基づいて表示されます。このパネルで、以下のタスクを実行することができます。

このタスクについて

1. パスワード・ポリシーを使用可能にするには、「**使用可能 (ibm-pwdPolicy)**」チェック・ボックスを選択します。パスワード・ポリシーを使用不可にするには、「**使用可能 (ibm-pwdPolicy)**」チェック・ボックスをクリアします。属性 `ibm-pwdPolicy` は、このコントロールに関連付けられています。
2. ユーザーが自分のパスワードを変更できるようにするには、「**ユーザーはパスワードを変更できる (pwdAllowUserChange)**」チェック・ボックスを選択します。
3. 管理者がパスワードをリセットした後にユーザーが必ず自分のパスワードを変更するようにするには、「**リセット後、ユーザーは必ずパスワードを変更する (pwdMustChange)**」チェック・ボックスを選択します。
4. ユーザーが新規パスワードの設定時に現在のパスワードを必ず指定するようにするには、「**ユーザーは、変更中に現在のパスワードを指定する必要がある (pwdSafeModify)**」チェック・ボックスを選択します。
5. パスワード・ポリシーの開始日時を設定するには、「パスワード・ポリシーの開始時刻 (`ibm-pwdPolicyStartTime`)」の下にあるフィールドに日時を入力します。日付を設定する場合、「カレンダー」アイコンをクリックするとカレンダーを使用できます。

注: パスワード・ポリシーの開始日時を設定できるのは、管理者およびローカル管理者グループのメンバーのみです。

6. このグループでは、パスワードの期限切れまでの日数を設定できます。「**日数**」を選択する場合、フィールドに日数を入力する必要があります。選択しない場合、パスワードが期限切れにならないようにするには、「**パスワードを期限切れにしない**」を選択します。
7. このグループでは、パスワードの最小経過期間を設定できます。「**日数**」を選択する場合は、パスワードの最終変更後にパスワードが変更可能になる日数をフィールドに入力する必要があります。選択しない場合は「**パスワードはいつでも変更できる**」を選択します。

- このグループでは、パスワード期限切れの警告状況をパスワード期限切れの何日前に表示するかを設定できます。「有効期限切れまでの日数」を選択する場合は、ユーザーにパスワードの有効期限を警告するために、パスワード期限切れまでの日数をフィールドに入力する必要があります。選択しない場合は「警告しない」を選択します。
- 「ログイン」フィールドに、パスワードの有効期限切れ後に許可される猶予ログイン試行回数を入力します。

完了したら、以下のステップのいずれかを行います。

- 「戻る」をクリックして、「属性選択」パネルにナビゲートします。
- 「次へ」をクリックして、パスワード・ポリシーの構成を続行します。
- 「キャンセル」をクリックしてすべての変更を廃棄し、「パスワード・ポリシーの管理」パネルにナビゲートします。
- 「完了」をクリックしてすべての変更内容を保存し、「パスワード・ポリシーの管理」パネルにナビゲートします。

パスワード・ポリシー設定 2:

「パスワード・ポリシー設定 2」パネルおよび「パスワード・ポリシー設定 2」パネルのコントロールは、「属性選択」パネルでの属性の選択に基づいて表示されます。このパネルで、以下のタスクを実行することができます。

このタスクについて

手順

- パスワードをロックアウトするまでにユーザーに許可されるバインド試行失敗の最大回数を設定する。「回数」を選択する場合は、パスワードのロックアウトまでに許可されるバインド試行失敗の最大回数を入力する必要があります。パスワードをロックアウトするまでに許可されるバインド試行失敗の最大回数を無制限に設定するには、「無制限」を選択します。
- パスワード認証をロックされたままにする期間を設定する。期間を指定するには、フィールドに期間の値を選択して入力し、フィールドから単位を選択します。選択しない場合は「無制限」を選択します。
- バインド試行失敗をフラッシュするまでの期間を設定する。期間を指定するには、フィールドに期間の値を選択して入力し、フィールドから単位を選択します。選択しない場合は「無制限」を選択します。

パスワード・ポリシー設定 3:

「パスワード・ポリシー設定 3」パネルおよび「パスワード・ポリシー設定 3」パネルのコントロールは、「属性選択」パネルでの属性の選択に基づいて表示されます。このパネルで、以下のタスクを実行することができます。

このタスクについて

- 「再利用前に必要なパスワードの最小変更回数 (pwdInHistory)」フィールドには、古いパスワードを再利用する前に保管するパスワードの最小数を入力します。

2. 「パスワード構文を検査する (pwdCheckSyntax)」リストからパスワード構文の検査項目を選択して、パスワードの構文を検査するかどうかを指定できます。
「パスワード構文の検査 (pwdCheckSyntax)」リストで選択可能な項目は、「構文を検査しない」、「構文を検査する (両方向暗号化のみ)」、および「構文を検査する」です。
3. 「最小の長さ (pwdMinLength)」フィールドには、使用するパスワードの最小の長さを入力します。
4. 「英字の最小数 (passwordMinAlphaChars)」フィールドには、パスワードに含める必要がある英字の最小数を入力します。
5. 「数字および特殊文字の最小数 (passwordMinOtherChars)」フィールドには、パスワードに含める必要がある数字および特殊文字の最小数を入力します。
6. 「パスワードで 1 つの文字を使用できる最大回数 (passwordMaxRepeatedChars)」フィールドには、1 つのパスワード内で許可される反復文字の最大数を入力します。
7. 「連続反復文字の最大数 (passwordMaxConsecutiveRepeatedChars)」フィールドに、パスワードに使用できる連続反復文字の最大数の値を入力します。
8. 「前のパスワードと異なる文字の最小数 (passwordMinDiffChars)」フィールドには、前のパスワードと異なる新規パスワードの文字の最小数を入力します。

パスワード・ポリシーを編集するには:

パスワード・ポリシーを編集する場合は、以下の情報を参照してください。

このタスクについて

既存のパスワード・ポリシーを編集するには、対象の行を選択し、「編集」ボタンをクリックするか「アクションの選択」リストから「編集」を選択し、次にパスワード・ポリシー・テーブルの「実行」をクリックします。これでポリシー定義ウィザードが起動し、選択したパスワード・ポリシーが表示されます。ユーザーは、必要な属性とその値を変更することで、選択したパスワード・ポリシーを編集できます。

既存のパスワード・ポリシーのコピーを作成するには:

既存のパスワード・ポリシーのコピーを作成する場合は、以下の情報を参照してください。

このタスクについて

既存のパスワード・ポリシーのコピーを作成するには、対象の行を選択し、「コピー」ボタンをクリックするか「アクションの選択」リストから「コピー」を選択し、次にパスワード・ポリシー・テーブルの「実行」をクリックします。これでポリシー定義ウィザードが起動し、選択したパスワード・ポリシーが表示されます。コピーするには、新規のパスワード・ポリシー名とポリシーの場所を指定する必要があります。このとき、属性値の変更もできます。

パスワード・ポリシーを削除するには:

既存のパスワード・ポリシーを削除するには、対象の行を選択し、「削除」ボタンをクリックするか「アクションの選択」リストから「削除」を選択し、次にパスワード・ポリシー・テーブルの「実行」をクリックします。

このタスクについて

注: グローバル・パスワード・ポリシーは削除できません。

コマンド・ラインの使用:

指定されたコマンドを実行して、パスワード・ポリシーを有効にすることができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -p <port> -k
dn: cn=pwdpolicy,cn=ibmpolicies
ibm-pwdpolicy:true
ibm-pwdGroupAndIndividualEnabled:true
```

グループ・パスワード・ポリシーおよび個別パスワード・ポリシーを定義するには、以下のコマンドを発行します。

```
idsldapadd -D <adminDN> -w <adminPW>
dn: cn=grp1_pwd_policy,cn=ibmpolicies
objectclass: container
objectclass: pwdPolicy
objectclass: ibm-pwdPolicyExt
objectclass: top
cn: grp_pwd_policy
pwdAttribute: userPassword
pwdGraceLoginLimit: 1
pwdLockoutDuration: 30
pwdMaxFailure: 2
pwdFailureCountInterval: 5
pwdMaxAge: 999
pwdExpireWarning: 0
pwdMinLength: 8
pwdLockout: true
pwdAllowUserChange: true
pwdMustChange: false
ibm-pwdpolicy:true

idsldapadd -D <adminDN> -w <adminPW>
dn: cn=individual1_pwd_policy,cn=ibmpolicies
objectclass: container
objectclass: pwdPolicy
objectclass: ibm-pwdPolicyExt
objectclass: top
cn: grp_pwd_policy
pwdAttribute: userPassword
pwdGraceLoginLimit: 3
pwdLockoutDuration: 50
pwdMaxFailure: 3
pwdFailureCountInterval: 7
pwdMaxAge: 500
pwdExpireWarning: 0
pwdMinLength: 5
pwdLockout: true
pwdAllowUserChange: true
pwdMustChange: false
ibm-pwdpolicy:true
```

グループ・パスワード・ポリシーおよび個別パスワード・ポリシーをグループまたはユーザーに関連付けるには、以下のコマンドを発行します。例えば、グループ・パスワード・ポリシーをグループに関連付けるには、次のように入力します。

```
idsldapmodify -D <adminDN> -w <adminPW> -k
dn: cn=group1,o=sample
changetype: modify
add: ibm-pwdGroupPolicyDN
ibm-pwdGroupPolicyDN: cn=grp1_pwd_policy,cn=ibmpolicies
```

個別パスワード・ポリシーをユーザーに関連付けるには、次のように入力します。

```
idsldapmodify -D <adminDN> -w <adminPW> -k
dn:cn=user1 ,o=sample
changetype:modify
add:ibm-pwdIndividualPolicyDN
ibm-pwdIndividualPolicyDN:cn= Individual1 _pwd_policy,cn=ibmpolicies
```

pwdsafemodify の設定時のパスワードの変更

ここで説明する手順を使用することで、パスワードを変更できます。

このタスクについて

Security Directory Server LDAP クライアントを使用している場合は、「ldapchangepwd」ユーティリティを使用してユーザーのパスワードを変更できます。ただし、非 Security Directory Server LDAP クライアントを使用している場合、ユーザー・パスワードを変更するには以下のようにします。

例えば、ユーザー「cn=user,o=sample」のパスワード「passw001rd」を「passw007rd」に更新する必要があるとします。これを行うには、以下のコマンドを実行します。

```
ldapmodify -p <port> -D <bindDN> -w <bindPassword> -i <input file>

dn: cn=user,o=sample
changetype: modify
delete: userpassword
userpassword: <old password value>
-
add: userpassword
userpassword: <new password value>
```

Kerberos のセットアップ

認証に使用する Kerberos サーバーをセットアップする必要があります。

IBM Security Directory Server は、AIX サーバーおよび AIX 64 ビット・クライアントに対して、IBM ネットワーク認証サービスなどの Kerberos バージョン 1.4 サーバーをサポートします。

注: Kerberos 認証を使用するには、IBM Network Authentication Service クライアントをインストールしておく必要があります。

ネットワーク認証サービスの下で、クライアント (ユーザーまたはサービス) はチケットの要求を鍵配布センター (KDC) に送信します。KDC はクライアントの発券許可証 (TGT) を作成し、クライアントのパスワードを鍵として使用して暗号化して、暗号化された TGT をクライアントに戻します。クライアントは、パスワードを使用して TGT を暗号化解除しようとしています。暗号化解除に成功すると、クライアントは、クライアントの ID の証明を示すために、暗号化解除された TGT を保存します。

TGT は、指定した時刻に有効期限切れになるものですが、クライアントに対し、特定のサービスに対する許可を付与する追加チケットの取得を許可します。これらの追加チケットの要求と付与は、ユーザーの介入を必要としません。

ネットワーク認証サービスは、ネットワーク上の 2 つのポイント間の認証済み (任意で暗号化されます) 通信をネゴシエーションします。これにより、アプリケーションは、クライアントがファイアウォールのどちらの側に存在するかに関係なく、

セキュリティーのレイヤーを提供できます。このため、ネットワーク認証サービスは、ネットワークのセキュリティーで重要な役割を果たします。

LDAP サーバー・サービス名を、プリンシパル名 ldap/
<hostname>.<mylocation>.<mycompany>.com を使用して鍵配布センター (KDC) に作成する必要があります。

注: 環境変数 **LDAP_KRB_SERVICE_NAME** は、LDAP Kerberos サービス名が大文字か小文字かを決定するために使用されます。この変数を LDAP に設定すると、大文字の LDAP Kerberos サービス名が使用されます。変数を設定しない場合は、小文字の ldap が使用されます。この環境変数は LDAP クライアントおよびサーバーの両方で使用されます。デフォルトではこの変数は設定されません。Kerberos サービス名の変更について詳しくは、IBM Security Directory Server の資料の『トラブルシューティングとサポート』セクションを参照してください。

ネットワーク認証サービスは、以下のコンポーネントを提供します。

鍵配布センター

KDC は、レルムの全プリンシパルの秘密鍵へのアクセス権を持つ、トラステッド・サーバーです。KDC は、認証サーバー (AS) と発券サーバー (TGS) という 2 つの部分で構成されています。AS は、TGT を発行することで初期クライアント認証を処理します。TGS は、クライアントがサービスの認証に使用するサービス・チケットを発行します。

管理サーバー

管理サーバーは、ネットワーク認証サービス・データベースへの管理アクセス権を提供します。このデータベースには、プリンシパル、鍵、ポリシー、およびレルムに関するその他の管理情報が含まれます。管理サーバーは、プリンシパルとポリシーを追加、変更、削除、および表示することができます。

パスワード変更サービス

パスワード変更サービスを使用すると、ユーザーはパスワードを変更できます。パスワード変更サービスは、管理サーバーによって提供されます。

クライアント・プログラム

クライアント・プログラムは、資格情報 (チケット) の操作、keytab ファイルの操作、パスワードの変更、およびその他の基本ネットワーク認証サービス操作を実行するために提供されます。

アプリケーション・プログラミング・インターフェース (API)

セキュアな分散アプリケーションの開発を許可するために、ライブラリーとヘッダー・ファイルが提供されています。提供される API については、「Application Development Reference」を参照してください。

Web 管理の使用

Web 管理ツールを使用することで、Kerberos 項目を作成することができます。

このタスクについて

「サーバー管理」で、Web 管理ツールのナビゲーション領域にある「セキュリティー・プロパティーの管理」カテゴリーを展開します。サーバーで Kerberos がサポートされる場合 (つまり、kerberos でサポートされる機能 OID 1.3.18.0.2.32.30 をサー

バーが持っている場合) は、「**Kerberos**」タブを選択します。サーバーで Kerberos がサポートされない場合、このタブは表示されません。

手順

1. 「**Kerberos 認証を使用可能にする**」チェック・ボックスを選択し、Kerberos 認証を使用可能にします。**注:** Kerberos 認証を使用するには、Kerberos クライアントをインストールしておく必要があります。
2. ディレクトリー管理者が既存の ACL データのセットを Kerberos 認証方式で使用できるようにするには、「**Kerberos ID を LDAP DN にマップする**」チェック・ボックスを選択します。詳細については、257 ページの『Kerberos の ID マッピング』を参照してください。
3. `hostName.domainName` の形式で Kerberos レルムを入力します (例: `TEST.AUSTIN.IBM.COM`)。この形式では大/小文字は区別されません。
4. Kerberos keytab ファイルのパスおよびファイル名を入力します。このファイルには、LDAP サーバーの `kerberos` アカウントに関連付けられた、このサーバーの LDAP サーバーの秘密鍵が含まれます。このファイルと SSL 鍵データベース・ファイルは保護される必要があります。
5. ディレクトリー管理者としてログインしている場合は、形式 `ibm-kn=value@realm` または `ibm-KerberosName=value@realm` (例: `ibm-kn=root@TEST.AUSTIN.IBM.COM`) を使用して、代替管理者 ID を入力します。このフィールドを管理グループのメンバーが編集することはできません。**注:** この ID は、Kerberos レルムで有効な ID にする必要があります。この ID の値には、大文字小文字の区別はありません。
6. 完了したら、終了せずに変更を保存する場合は「**適用**」をクリックし、変更を適用して終了する場合は「**OK**」をクリックし、変更を行わずにこのパネルを終了するには「**キャンセル**」をクリックします。

コマンド・ラインの使用

以下に示すコマンドを発行することにより、Kerberos 項目を作成できます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Kerberos, cn=Configuration
cn: Kerberos
ibm-slapdKrbAdminDN: ibm-kn=admin@MYREALM.AUSTIN.IBM.COM
ibm-slapdKrbEnable: true
ibm-slapdKrbIdentityMap: true
ibm-slapdKrbKeyTab: /keytabs/mykeytab.keytab
ibm-slapdKrbRealm: MYREALM.AUSTIN.IBM.COM
objectclass: ibm-slapdKerberos
objectclass: ibm-slapdconfigEntry
objectclass: top
```

keytab ファイルを変更するなど、Kerberos 項目を変更するには、以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Kerberos, cn=Configuration
changetype: modify
replace: ibm-slapdKrbKeyTab
ibm-slapdKrbKeyTab: /keytabs/mynewkeytab.keytab
```

Kerberos の使用

コマンド行を使用して Kerberos 認証を行うには、事前に Kerberos を初期設定しておく必要があります。

以下のコマンドを実行して、Kerberos を初期設定します。

```
kinit <kerberos_principlename>@<realm_name>
```

Kerberos を認証に使用するには、`idsldapadd` コマンドおよび `idsldapsearch` コマンド上で、**GSSAPI** パラメーターとともに、`-m` オプションを指定する必要があります。例:

```
idsldapsearch-V 3 -m GSSAPI -b <"cn=us"> objectclass=*
```

Kerberos の ID マッピング

ID マッピングを使用すると、ディレクトリー管理者は、既存の ACL データのセットを Kerberos 認証方式で使用できます。

IBM Security Directory Server の ACL は、ディレクトリー・サーバーに接続されたクライアントに割り当てられている識別名 (DN) に基づいています。アクセス権は、その DN に与えられている許可と、その DN をメンバーとして含むグループへの許可に基づいて決定されます。GSSAPI のバインド方式を使用する場合 (つまり、サーバーへの認証に Kerberos を使用する場合)、DN は、

IBM-KN=your_principal@YOUR_REALM_NAME のような形式で表現されます。このタイプの DN は、アクセス ID またはアクセス・グループのメンバーとして使用できません。Kerberos ID マッピング機能を使用すると、すでにディレクトリー内に存在する項目に、この DN のアクセス権を与えることもできます。

例えば、Reginald Bender のディレクトリーに以下の項目がある場合を考えます。

```
dn: cn=Reginald Bender, ou=internal users, o=ibm.com, c=US
objectclass: top
objectclass: person
objectclass: organizationalperson
cn: Reginald Bender
sn: Bender
aclentry: access-id:CN=THIS:critical:rwc
aclentry: group:CN=ANYBODY:normal:rsc
userpassword: cL1eNt
```

この項目のアクセス権を使用すると、DN `cn=Reginald Bender, ou=internal users, o=ibm.com, c=US` でバインドしているすべてのユーザーが、パスワードなどの重要情報を参照できます (それ以外のユーザーは参照できません)。

Reginald Bender が Kerberos を使用してサーバーにバインドした場合、DN は、`IBM-KN=rbender@SW.REALM_1` のようになります。ID マッピングがサーバー上で使用可能になっていない場合、ユーザーは項目のパスワードを参照できません。

ID マッピングが使用可能になっている場合、この項目が以下の行を含むよう変更されていれば、ユーザーはパスワードを参照できます。

```
dn: cn=Reginald Bender, ou=internal users, o=ibm.com, c=US...
objectclass: ibm-securityidentities
altsecurityidentities: Kerberos:rbender@SW.REALM_1
```

Reginald Bender がディレクトリー・サーバーにバインドすると、サーバーはまずディレクトリー全体を検索し、ディレクトリーが KDC (鍵配布センター) アカун ト・レジストリーであるかどうかを判別します。ディレクトリーが KDC でない場合、サーバーは、Kerberos のユーザー・プリンシパルとレルムに一致する値を持つ

altsecurityidentities 属性が含まれる項目がないかどうか、ディレクトリーを検索します。この例では、rbender がユーザー・プリンシパルで SW.REALM_1 がレルムです。これは、Kerberos ID マッピングのデフォルト値です。この値が指定された属性を持つ項目が複数あると、バインドは失敗します。マッピングは 1 対 1 でなければなりません。マッピングが成功すると、Reginald Bender は、cn=Reginald Bender, ou=internal users, o=ibm.com, c=US (およびこの値をメンバーとして含むすべてのアクセス・グループ) に対するすべてのアクセス権を所有します。

IBM Security Directory Server を使用して Kerberos アカウント情報 (krbRealmName-V2 =*realm_name* および krbPrincipalName = *princ_name@realm_name*) を保管すると、KDC のバックキング・ストアとして機能させることができます。

Kerberos ID マッピングが使用可能になっているサーバーは最初に、以下の例のようなオブジェクト・クラス krbRealm-V2 および krbRealmName-V2=*realm_name* を持つ項目がないかどうか、ディレクトリーを検索します。

```
dn: krbRealmName-V2=SW.REALM_1, o=ibm.com, c=US
objectclass: krbRealm-V2
krbRealmName-V2: SW.REALM_1
```

項目が見つからない場合、サーバーは、前述したデフォルトの Kerberos ID マッピングを使用します。項目が複数見つかった場合、バインドは失敗します。

ただし、ディレクトリーに以下のような単一記入項目が含まれている場合です。

```
dn: krbRealmName-V2=SW.REALM_1, ou=Group, o=ibm.com, c=US
objectclass: krbRealm-V2
krbRealmName-V2: SW.REALM_1
krbPrincSubtree: ou=internal users, o=ibm.com, c=US
krbPrincSubtree: ou=external users, o=ibm.com, c=US
```

サーバーは、krbPrincSubtree の値としてリストされている各サブツリーを検索し、属性 krbPrincipalName を持つ項目がないかどうかを調べます。

今回のリリースの場合、Reginald Bender に対して ID マッピングを機能させるには、cn=Reginald Bender, ou=internal users, o=ibm.com, c=US 項目に以下の 2 つの属性を追加する必要があります。

```
objectclass: extensibleObject
krbPrincipalName: rbender@SW.REALM_1
```

ディレクトリーが KDC アカウント・レジストリーでない場合、最後の項目は以下のようになります。

```
dn: cn=Reginald Bender, ou=internal users, o=ibm.com, c=US...
objectclass: ibm-securityidentities
altsecurityidentities: Kerberos:rbender@SW.REALM_1...
```

ディレクトリーが KDC アカウント・レジストリーの場合、最後の項目は以下のようになります。

```
dn: cn=Reginald Bender, ou=internal users, o=ibm.com, c=US ...
objectclass: extensibleObject
krbPrincipalName: rbender@SW.REALM_1
```

いずれの場合も、クライアントは cn=Reginald Bender, ou=internal users, o=ibm.com, c=US にマップされます。

項目が見つからず DN がマップされない場合、マッピングは失敗しますが、バインドは成功します。ただし、複数の DN がマップされると、バインドは失敗します。

ID マッピングを使用すると、既存の ACL と Kerberos 認証を一緒に使用できます。マップされた ID を持つ Kerberos を使用するクライアントには、2 つの異なった ID があります。この 2 つの ID はどちらも、アクセス権の付与の際に評価されます。

ID マッピングには、コストがかかります。バインド時の内部検索はパフォーマンスに影響し、ID マッピングでは、マップする項目に該当する属性を追加するための追加設定が必要となります。

今回のリリースでデフォルト ID マッピングを使用する場合、管理者 (Kerberos または LDAP) は、KDC 内のデータと LDAP サーバー内のデータを同期させる必要があります。データを同期しないと、ACL の評価が適切に行われなため、誤った結果が戻されます。

注: KrbPrincipal などのオブジェクト・クラスと KrbPrincSubtree、KrbAliasedObjectName、および KrbHintAliases などの属性は、IBM Directory を Kerberos KDC として定義するために使用されます。詳細については、Kerberos の資料を参照してください。

DIGEST-MD5 構成

DIGEST-MD5 は、SASL 認証機構です。クライアントで Digest-MD5 を使用すると、パスワードが平文形式では送信されません。また、リプレイ・アタックがプロトコルによって防止されます。

DIGEST-MD5 機構を構成するには、以下のいずれかの方法を使用します。

Web 管理の使用

Web 管理ツールを使用することにより、DIGEST-MD5 メカニズムを構成することができます。

このタスクについて

「サーバー管理」の下で、Web 管理ツールのナビゲーション領域にある「**セキュリティー・プロパティーの管理**」カテゴリーを展開してから「**DIGEST-MD5**」タブを選択します。「Digest-MD5」タブは、次の 2 つの条件のいずれかが満たされる場合にのみ表示されます。

- ルート DSE 検索で、Digest-MD5 の `ibm-supportedCapabilities` OID `1.3.18.0.2.32.69` が戻される。
- ルート DSE 検索で、`supportedSaslMechanisms` 属性の値として DIGEST-MD5 が戻される。

「Digest-MD5」タブがロードされると、タブ内のコントロールの値は、構成ファイルの項目「`cn=Digest, cn=Configuration`」の Digest-MD5 パラメーターの値に更新されます。

手順

1. 「**Digest-MD5 を使用可能にする**」チェック・ボックスを選択して、Digest-MD5 メカニズムを使用可能にします。注: 「**Digest-MD5 を使用可能にする**」チェッ

ク・ボックスを選択すると、このタブにある Digest-MD5 パラメーター関連の他のコントロールが使用可能になり、これらのコントロールへの変更が許可されます。

2. 「サーバー・レルム」では、事前選択された「デフォルト」設定 (サーバーの完全修飾ホスト名) を選択できます。あるいは「レルム」をクリックして、サーバーを構成する対象のレルムの名前を入力します。注: 構成項目に `ibm-slapdDigestRealm` 属性を設定すると、サーバーはこの値をレルムのデフォルト値の代わりに使用します。この場合は「レルム」ボタンが事前に選択されており、レルムの値がフィールド内に表示されています。このレルムの名前は、使用するユーザー名およびパスワードを調べるために、クライアントによって使用されます。
複製を使用する場合は、すべてのサーバーを同じレルムで構成します。
3. 「ユーザー名の属性」では、事前選択された「デフォルト」設定 (uid) を使用することも、「属性」をクリックして、DIGEST-MD5 SASL バインド中にユーザー項目を一意に識別するためにサーバーが使用する属性の名前を入力することもできます。注: 構成項目に `ibm-slapdDigestAttr` 属性が設定されていると、サーバーはユーザー名属性のデフォルトの代わりにその値を使用します。この場合は「属性」ボタンが事前に選択されており、属性値がフィールド内に表示されています。
4. ディレクトリー管理者としてログインしている場合は、「管理者ユーザー名」の下に管理者のユーザー名を入力します。このフィールドを管理グループのメンバーが編集することはできません。DIGEST-MD5 SASL バインドで指定したユーザー名がこのストリングと一致した場合、このユーザーは管理者となります。注: 管理者ユーザー名には、大/小文字の区別があります。
5. 完了したら、終了せずに変更を保存する場合は「適用」をクリックし、変更を適用して終了する場合は「OK」をクリックし、変更を行わずにこのパネルを終了するには「キャンセル」をクリックします。

コマンド・ラインの使用

以下に示すコマンドをコマンド行で使用することにより、DIGEST-MD5 メカニズムを構成できます。

このタスクについて

`cn=Digest,cn=configuration` 項目を作成するには、以下のコマンドを入力します。

```
idsldapadd -D <adminDN> -w <adminpw> -i <filename>
```

where <filename> contains:

```
dn: cn=Digest,cn=configuration
cn: Digest
ibm-slapdDigestRealm: <realm name>
ibm-slapdDigestAttr: <uuid>
ibm-slapdDigestAdminUser: <Adminuser>
ibm-slapdDigestEnabled: true
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdDigest
```

DIGEST-MD5 の設定を変更するには、以下のコマンドを使用します。

```
idsldapmodify -D <adminDN> -w <adminpw> -i <filename>
```

where <filename> contains:

```

dn: cn=Digest,cn=configuration
changetype: modify
replace: ibm-slapdDigestRealm
ibm-slapdDigestRealm: <newrealmname>
-
replace: ibm-slapdDigestAttr
ibm-slapdDigestAttr: <newattribute>
-
replace: ibm-slapdDigestAdminUser
ibm-slapdDigestAdminUser: <newAdminuser>

```

Digest MD5 メカニズムを使用してユーザーをサーバーにバインドする方法を以下の例に示します。

```

idsldapsearch -h <ldaphost> -p ldapport -U <username> -w <password> -m DIGEST-MD5
-G <realm> -b o=sample cn=gw*

```

注: Digest MD5 バインドを実行するには、`-h <hostname>` オプションを指定する必要があります。バインドがローカル・マシンから実行される場合でも、`<hostname>` パラメーターは、該当の Security Directory Server マシンの IP アドレスまたは FQDN (完全修飾ドメイン・ネーム) でなければなりません。localhost またはループバック IP アドレスを `-h` の値として指定すると、エラーが発生することがあります。

固有の属性値によるバインド

識別名 (DN) とパスワードの代わりに、固有値を持つ属性とパスワードを使用して、ディレクトリー・サーバーにバインドできます。DN 値は長い場合がありますが、固有の属性値の方が記憶するのが簡単です。

制約事項: 固有の属性値によるバインド操作は、プロキシ・サーバーではサポートされていません。

バインド操作において固有値を持つ属性とパスワードを使用するには、次の操作が必要です。

- ディレクトリー・サーバー・インスタンスで固有値を持つ属性を識別します。
- `cn=Configuration` 項目の下で `ibm-slapdUniqueAttrForBindWithValue` 属性を構成し、その値を固有値を持つ属性で設定します。例えば、`mail` や `uid` などの固有値を持つ属性を使用します。 `ibm-slapdUniqueAttrForBindWithValue` 属性では複数値の属性を割り当てることができますが、複数値の属性の値は固有にする必要があります。

重要: 以下の属性タイプは `ibm-slapdUniqueAttrForBindWithValue` 属性に割り当てないでください。

- 属性値で = 文字を使用している属性。
- 暗号化属性。

バインド操作の属性を変更するには、`ibm-slapdUniqueAttrForBindWithValue` 属性値を変更して、ディレクトリー・サーバーおよび管理サーバーを再始動します。

以下の例では、`ibm-slapdUniqueAttrForBindWithValue` 属性を持つ `cn=Configuration` 項目を示します。

```

dn: cn=Configuration
cn: Configuration
ibm-slapdAdminDN: cn=root
ibm-slapdAdminGroupEnabled: true
ibm-slapdAdminPW: {AES256}0iBLFmJJXwLM5eocBxeJZw=
...
...

```

```
ibm-slapdTimeLimit: 900
ibm-slapdTraceMessageLevel: 0xFFFF
ibm-slapdTraceMessageLog: /home/dsrdbm01/idsslapd-dsrdbm01/logs/traceibmslapd.log
ibm-slapdUniqueAttrForBindWithValue: mail
ibm-slapdVersion: 6.3.1
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdTop
```

エラー・コード

バインド操作で属性を使用すると、ディレクトリー・サーバーは、以下の理由により LDAP_INVALID_CREDENTIALS エラーを生成します。

- バインド操作で使用される属性がいずれの項目にも関連付けられていません。
- パスワードが正しくありません。
- 属性に固有値が含まれていないか、または複数の項目が属性値に関連付けられています。

ibmslapd.log ファイルには、エラー・メッセージも記録されます。

他の条件に対してディレクトリー・サーバーがエラーを生成した場合は、LDAP_INVALID_CREDENTIALS エラー・コードを返します。サーバー・トレースを活性化した場合は、traceibmslapd.log ファイルにもエラー・メッセージが記録されます。

固有の属性値によるバインドでの監査ログの項目

セキュリティ上の目的により、監査ログを有効にして、ディレクトリー・サーバーで失敗した操作および成功した操作をすべて記録することができます。サーバーは、サーバーに対して固有の属性値によるバインドとなった操作について、監査ログ・ファイルに以下の属性を記録します。

- bindDN: unique_attr_value
- name: DN_entry_value

bindDN 項目は unique_attr_value を記録しますが、これはサーバーでのバインドに使用されていました。name 項目は DN 項目を記録しますが、これは固有の属性値に関連付けられています。以下の例では、これらの値を持つ監査記録を示します。

```
AuditV3--2013-05-20-21:43:38.903+5:30--V3 Bind--bindDN: al.garcia@sample.com
--client: 127.0.0.1:17042--connectionID: 2--received: 2013-05-20-21:43:38.881+5:30
--Success
controlType: 1.3.6.1.4.1.42.2.27.8.5.1
criticality: false
name: cn=Al Garcia, ou=Home Entertainment, ou=Austin, o=sample
authenticationChoice: simple
AuditV3--2013-05-20-21:43:38.961+5:30--V3 Search--bindDN: al.garcia@sample.com
--client: 127.0.0.1:17042--connectionID: 2--received: 2013-05-20-21:43:38.896+5:30
--Success
controlType: 1.3.6.1.4.1.42.2.27.8.5.1
criticality: false
base: o=sample
scope: wholeSubtree
derefAliases: neverDerefAliases
typesOnly: false
filter: (objectclass=*)
numberOfEntriesReturned: 2
AuditV3--2013-05-20-21:43:38.962+5:30--V3 Unbind--bindDN: al.garcia@sample.com
--client: 127.0.0.1:17042--connectionID: 2--received: 2013-05-20-21:43:38.962+5:30
--Success
```

パススルー認証での固有の属性値によるバインド

バインド操作用に構成された属性を使用して、認証サーバーで認証を行うことができます。バインド操作で DN 値とパスワードを使用する代わりに、固有の属性値とパスワードを使用します。

認証サーバーでユーザー項目が使用できない場合、サーバーはエラーを生成します。固有の属性値とパスワードによるパススルー認証の場合は、認証サーバーでこの項目が使用可能である必要があります。

バインド操作の固有値による属性の構成

バインド操作において、DN 値の代替として使用する固有値によって属性を構成します。認証の目的では、固有の属性値の方が記憶するのが簡単です。

手順

1. インスタンス所有者としてログインします。
2. バインド用の属性として固有値により属性を構成するには、以下のように **idsldapmodify** コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setBindAttr.ldif
```

setBindAttr.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Configuration
changetype: modify
add: ibm-slapdUniqueAttrForBindWithValue
ibm-slapdUniqueAttrForBindWithValue: mail
```

3. ディレクトリー・サーバーおよび管理サーバーを再始動します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
ibmslapd -I dsrdbm01 -n
ibmdiradm -I dsrdbm01
```

例

固有の属性値によりディレクトリー・サーバーにバインドするには、**idsldapsearch** コマンドを以下の形式で実行します。

```
idsldapsearch -h server.com -p port -D al.garcia@sample.com -w userPWD ¥
-s sub -b "cn=A1 Garcia, ou=Home Entertainment, ou=Austin, o=sample" objectclass=*
```

```
cn=A1 Garcia,ou=Home Entertainment,ou=Austin,o=sample
objectclass=top
objectclass=person
objectclass=organizationalPerson
objectclass=inetOrgPerson
cn=A1 Garcia
sn=Garcia
telephonenumber=1-812-855-7579
mail=al.garcia@sample.com
internationaliSDNNumber=755-7095
title=LEAD TA / MAINTENANCE
sealso=cn=Cynthia Flowers, ou=Home Entertainment, ou=Austin, o=sample
postalcode=1377
```

属性 - 値の固有の組み合わせによるバインド

識別名 (DN) とパスワードの代わりに、固有の属性 - 値ペアとパスワードを使用して、ディレクトリー・サーバーにバインドできます。

この機能は、前述の 261 ページの『固有の属性値によるバインド』というセクションで説明されている機能に似ています。

制約事項: 固有の属性と値ペアを使用するバインド操作は、プロキシ・サーバーではサポートされていません。

バインド操作において属性 - 値ペアとパスワードを使用するには、次の操作が必要です。

- ディレクトリー・サーバー・インスタンスで固有の、属性と値ペアを識別します。
- `cn=Configuration` 項目の下に `ibm-slapdBindWithUniqueAttrsEnabled` 属性を構成し、その値を「TRUE」に設定します。
- サーバーおよび管理サーバーを再始動します。

注: 以下の状況では、バインド操作に属性 - 値ペアを使用しないでください。

- 属性値に = 文字を含む属性。
- 暗号化属性。
- ローカル管理グループのメンバー用に構成された管理 DN と同じ、属性と値ペア。例えば、管理 DN `cn=lagm1` を持つローカル管理グループ・メンバーが存在していて、`cn` の値が "lagm1" のユーザーがディレクトリー・サーバーに存在する場合、`cn=lagm1` とディレクトリー・サーバー内のそのユーザーのパスワードの組み合わせを使用したバインド操作は失敗します。これは、サーバーがローカル管理グループ・メンバーの資格情報を使用して、ユーザー資格情報の検証を試みるためです。

以下の例では、`ibm-slapdBindWithUniqueAttrsEnabled` 属性を持つ `cn=Configuration` 項目を示しています。

```
dn: cn=Configuration
cn: Configuration
ibm-slapdAdminDN: cn=root
ibm-slapdAdminGroupEnabled: true
ibm-slapdAdminPW: {AES256}0iBLFmJJXwLM5eocBxeJZw==
...
...
ibm-slapdTimeLimit: 900
ibm-slapdTraceMessageLevel: 0xFFFF
ibm-slapdTraceMessageLog: /home/dsrdbm01/idsslslapd-dsrdbm01/logs/traceibmslapd.log
ibm-slapdBindWithUniqueAttrsEnabled: true
ibm-slapdVersion: 6.3.1
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdTop
```

エラー・コード

バインド操作に属性 - 値ペアを使用すると、ディレクトリー・サーバーでは、以下の理由により `LDAP_INVALID_CREDENTIALS` エラーが発生します。

- バインド操作に使用される属性 - 値ペアがいずれの項目にも関連付けられていません。
- パスワードが正しくありません。
- 属性 - 値ペアが固有でないか、または属性 - 値ペアに複数の項目が関連付けられています。

ibmslapd.log ファイルには、エラー・メッセージも記録されます。

他の条件に対してディレクトリー・サーバーがエラーを生成した場合は、LDAP_INVALID_CREDENTIALS エラー・コードを返します。サーバー・トレースを活性化した場合は、traceibmslapd.log ファイルにもエラー・メッセージが記録されます。

固有の属性値によるバインドでの監査ログの項目

セキュリティー上の目的により、監査ログを有効にして、ディレクトリー・サーバーで失敗した操作および成功した操作をすべて記録することができます。サーバーは、固有の属性 - 値ペアによるサーバーでのバインドとなった操作について、監査ログ・ファイルに以下の属性を記録します。

- bindDN: unique_attr=attr_value
- name: DN_entry_value

bindDN 項目は unique_attr=attr_value を記録しますが、これはサーバーでのバインドに使用されていました。name これは固有の属性と値のペアに関連付けられている DN 項目を記録します。以下の例では、これらの値を持つ監査記録を示します。

```
AuditV3--2013-05-20-21:43:38.903+5:30--V3 Bind--bindDN: mail=al.garcia@sample.com
--client: 127.0.0.1:17042--connectionID: 2--received: 2013-05-20-21:43:38.881+5:30
--Success
controlType: 1.3.6.1.4.1.42.2.27.8.5.1
criticality: false
name: cn=Al Garcia, ou=Home Entertainment, ou=Austin, o=sample
authenticationChoice: simple
AuditV3--2013-05-20-21:43:38.961+5:30--V3 Search--bindDN: al.garcia@sample.com
--client: 127.0.0.1:17042--connectionID: 2--received: 2013-05-20-21:43:38.896+5:30
--Success
controlType: 1.3.6.1.4.1.42.2.27.8.5.1
criticality: false
base: o=sample
scope: wholeSubtree
derefAliases: neverDerefAliases
typesOnly: false
filter: (objectclass=*)
numberOfEntriesReturned: 2
AuditV3--2013-05-20-21:43:38.962+5:30--V3 Unbind--bindDN: mail=al.garcia@sample.com
--client: 127.0.0.1:17042--connectionID: 2--received: 2013-05-20-21:43:38.962+5:30
--Success
```

パススルー認証のための属性 - 値の固有の組み合わせによるバインド

固有の属性 - 値ペアを使用して、認証サーバーで認証を行うことができます。バインド操作で DN 値とパスワードを使用する代わりに、固有の属性 - 値ペアとパスワードを使用します。

認証サーバーでユーザー項目が使用できない場合、サーバーはエラーを生成します。固有の属性値とパスワードによるパススルー認証の場合は、認証サーバーでこの項目が使用可能である必要があります。

「固有の属性値によるバインド」と「属性 - 値の固有の組み合わせによるバインド」の違い

2 つの機能の違いと、それぞれの機能が推奨される状況について説明します。

説明として、以下のユーザー項目を使用します。

```
dn: uid=agarcia,o=sample
uid: agarcia
cn: Al
sn: Garcia
userpassword: secret
mail: al.garcia@sample.com
employeeNumber: 123456
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
```

ユーザーの属性 `uid`、`mail`、`employeeNumber` の値は、そのユーザー項目のあるディレクトリーで固有であるとしてします。LDAP 管理者が、`ibm-slapdUniqueAttrForBindWithValue` の値を "mail" に構成すると、電子メール ID をバインド DN として使用することでユーザーはサーバーにバインドできます。例えば、電子メール ID は `al.garcia@sample.com` のような値になります。

また、LDAP 管理者は `ibm-slapdBindWithUniqueAttrsEnabled` を "true" にして有効設定すると、ユーザーは以下のいずれかの方法でサーバーにバインドできます。

- `mail=al.garcia@sample.com`
- `employeeNumber=123456`
- `uid=agarcia`

LDAP 管理者は、どの機能を有効にするかを決める必要があります。これは、Security Directory Server と通信するアプリケーションに対してユーザーが認証する方法によって異なります。ユーザーがアプリケーションで `mail` や `employeeNumber` などの任意の固有の属性を使用できるようにする場合、管理者は 263 ページの『属性 - 値の固有の組み合わせによるバインド』の機能を有効にする必要があります。ユーザーがアプリケーションで `uid` などのある特定の固有の属性を指定できるようにする場合、管理者は 261 ページの『固有の属性値によるバインド』の機能を使用する必要があります。

パススルー認証

パススルー・メカニズムを使用すると、ユーザー項目またはパスワードが別のサーバー上にある場合でも、認証サーバーでユーザーが認証されます。

ユーザー項目または資格情報がサーバー上にない場合でも、認証サーバーでバインドまたは比較操作を実行できます。認証サーバーがバインド操作に対するパススルー認証をサポートしている場合は、ルート DSE 検索により、1.3.18.0.2.32.78 OID 値を持つ `ibm-supportedCapabilities` 属性が返されます。サーバーが比較操作に対するパススルーをサポートしている場合は、ルート DSE 検索により、1.3.18.0.2.32.100 OID 値を持つ `ibm-supportedCapabilities` 属性が返されます。

パススルー認証が設定されると、認証サーバーは、クライアントの代わりに外部ディレクトリー・サーバー、パススルー・サーバーからの資格情報の確認を試みま

す。ディレクトリー・サーバーの場合、ユーザー項目またはユーザー資格情報がディレクトリー情報ツリー (DIT) がないことがあります。プロキシ・サーバーの場合、ユーザー項目またはユーザー資格情報がプロキシ・バックエンド・サーバーがないことがあります。

ディレクトリー・サーバーがパススルーをサポートするのは、以下の基準がすべて満たされている場合のみです。

- パススルー・インターフェース構成を持つディレクトリー・サーバー上で、`ibm-slapdPtaEnabled` 属性が `TRUE` に設定されている。`ibm-slapdPtaEnabled` 属性値が `TRUE` に設定されている場合、サーバーではバインド操作および比較操作に対するパススルーがサポートされます。`ibm-slapdPtaEnabled` 属性は動的属性です。属性に変更を適用するには、`readconfig` 拡張操作を実行する必要があります。
- ディレクトリー・サーバー上の適切なサブツリーに対して、パススルー認証が構成されて設定されている。
- 認証 DN 項目が、パススルー認証に対して構成されているサブツリーに存在している。認証サーバー上では、認証 DN 項目は存在しないか、または `userpassword` 属性を持っていません。
- 認証用の資格情報が `userpassword` 属性に格納されているパスワードである。

パススルー認証の例

パススルー認証を構成して使用するには、現在のディレクトリー・サーバー環境で必要なパススルー・インターフェースを識別する必要があります。

認証サーバーとして IBM Security Directory Server を使用する必要があります。ユーザー項目または資格情報を保持しているパススルー・サーバーは、LDAP V3 準拠のディレクトリー・サーバーにすることが可能です。

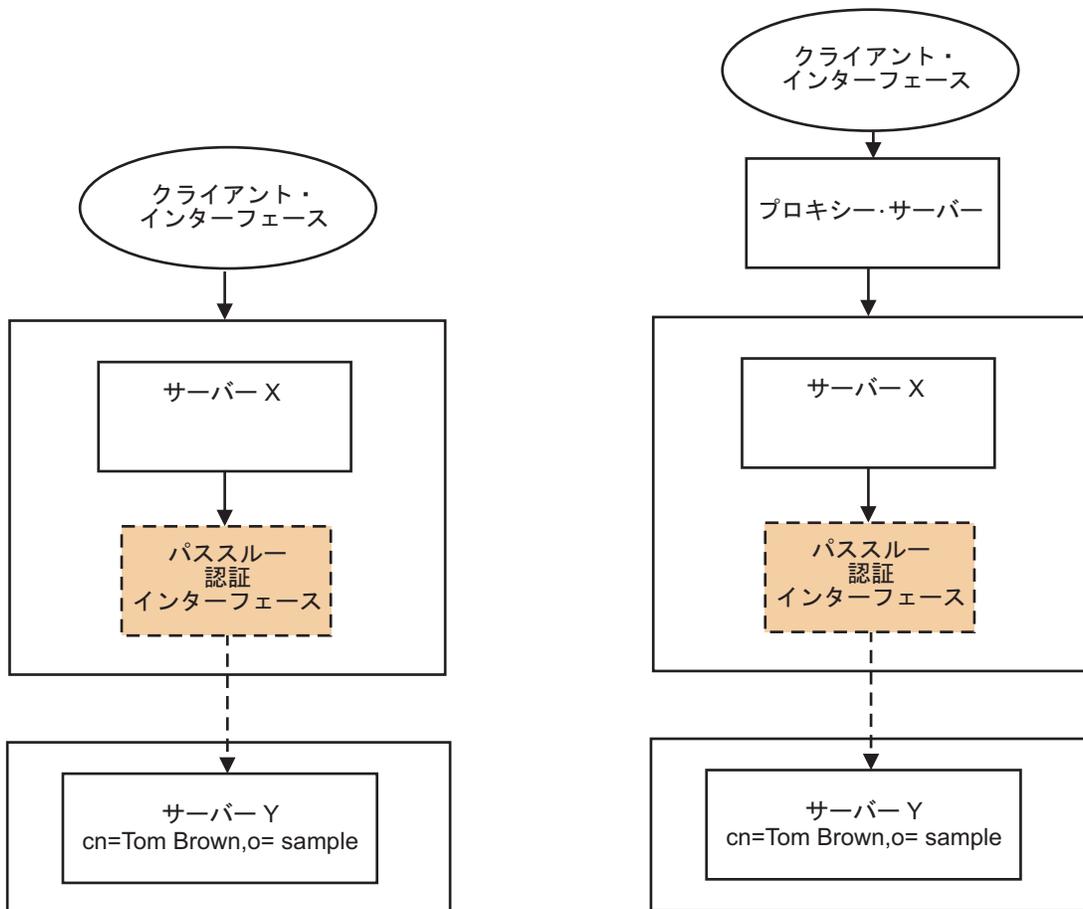


図 1. パススルー認証アーキテクチャー

パススルー・インターフェースに対して構成の変更を加えた場合は、ディレクトリー・サーバーを再始動する必要があります。構成ファイル内のパススルー・インターフェース項目は動的ではありません。

認証サーバーが以下の操作をサポートしている場合はパススルー認証を使用できます。

- パススルー・インターフェースを持つバックエンド・サーバーが含まれているプロキシ・サーバーに対する要求のバインドまたは比較。
- パススルー・インターフェースで構成されたディレクトリー・サーバーに対する要求のバインドまたは比較。

ディレクトリー・サーバーによる単純なバインドまたは比較操作、あるいは SSL を使用または使用しない LDAP クライアントによる比較操作のみを実行できます。ダイジェスト、Kerberos、またはカスタマイズされたバインド操作はサポートされていません。

例えば、環境にサーバー X とサーバー Y の 2 つのサーバーがあり、ユーザー項目 cn=Tom Brown,o=sample がサーバー Y に格納されているとします。

この場合、ユーザー Tom Brown がディレクトリー・サーバー X に対して認証を試みると、ユーザーを認証するために以下のチェックが行われます。

1. サーバー X は、ユーザーのバインド資格情報がサーバー上にあるかどうかをチェックします。
2. 項目または資格情報が使用できない場合、サーバー X は、サブツリーに対してパススルー認証インターフェースが設定されているかどうかをチェックします。
3. ユーザー項目がパススルー認証の候補である場合は、バインド資格情報がパススルー・サーバー Y に送信され、認証が行われます。
4. パススルー・サーバー Y がこのユーザー資格情報を確認した場合は認証が成功し、確認できない場合は認証が失敗します。

分散ディレクトリーのシナリオの場合は、プロキシ・サーバーが資格情報をバックエンド・サーバーに送付し、パススルー認証のチェックが行われます。

前のシナリオでは、ユーザー項目の DN がサーバー X とサーバー Y で同一である場合、単純なパススルー認証インターフェースが想定されています。属性マッピングが指定されていない場合は、認証サーバーの項目の DN がパススルー・サーバーの項目の DN をミラーリングしている必要があります。ただし、認証サーバーとパススルー・サーバー上で、ユーザー項目が常に同一である必要はありません。両方のサーバーで、ディレクトリー階層のレイアウトが異なる場合があります。サーバー X のユーザー項目 `cn=Tom Brown,o=sample` は、サーバー Y の他の DN にマップできます。このような状況の場合は、サーバー X とサーバー Y の項目で固有値を持つ属性を識別する必要があります (例えば、`uid`)。IBM Security Directory Server の固有値を持つ属性を使用して、パススルー・サーバーの属性にマップすることができます。このマップ情報を使用してパススルー・サーバーを照会し、必要な DN を取得することができます。

パススルー認証に無効な項目を使用した場合は、`LDAP_INVALID_CREDENTIALS` エラーにより、認証が拒否されることがあります。

パススルーに対応するために、以下の項目は構成しないでください。

- パススルー認証用の以下のサブツリーまたはこれらのサブツリーの下の子項目。
`cn=configuration`, `cn=schema`, `cn=ibmpolicies`, `cn=changelog`, および `cn=localhost`.
- ネストしたパススルー項目はサポートされていません。`ou=myco`, `o=sample1` 項目に対してあるパススルー・インターフェースが存在し、`ou=mydept`, `ou=myco`, `o=sample1` 項目に対して別のパススルー・インターフェースが存在する場合、サーバーは通常モードでの始動に失敗することがあります。
- 複数のパススルー項目のそれぞれが、同じパススルー・サブツリーにサービスを提供している別個のパススルー・サーバーを持つような状況はサポートされていません。

パススルー認証のオブジェクト・クラスおよび属性

現在のディレクトリー・サーバー環境でパススルー認証インターフェースを構成するには、適切なオブジェクト・クラスと関連属性を使用する必要があります。

パススルー認証を設定するための構成属性

パススルー認証の項目は、ディレクトリー・サーバー・インスタンスの構成ファイル `ibmslapd.conf` 内にあります。パススルー認証を設定または設定解除するには、

cn=configuration DN 項目の下の `ibm-slapdPtaEnabled` 属性を変更する必要があります。パススルー対応を有効にするには、`ibm-slapdPtaEnabled` 属性を `TRUE` に設定します。パススルー対応を無効にするには、`ibm-slapdPtaEnabled` 属性を `FALSE` に設定します。パススルー認証インターフェースを作成するには、パススルー認証構成に固有のすべてのサブツリーを `cn=Passthrough Authentication`, `cn=configuration` コンテナ項目の下で 1 つのレベルにする必要があります。以下の項目は、パススルー認証コンテナの例です。

```
dn: cn=Passthrough Authentication, cn=Configuration
cn: Passthrough Authentication
objectclass: top
objectclass: container
```

構造化オブジェクト・クラス

`cn=Passthrough Authentication`, `cn=configuration` コンテナ項目の 1 レベル下に、パススルー認証項目を追加する必要があります。パススルー認証項目には、`ibm-slapdPta` オブジェクト・クラスが含まれている必要があります。このオブジェクト・クラスには、パススルー認証設定に固有のサブツリーが含まれている必要があります。

補助オブジェクト・クラス

パススルー認証の項目を構成するには、補助オブジェクト・クラスを追加することが必要になる場合があります。補助オブジェクト・クラス `ibm-slapdPtaExt` および `ibm-PtaReferral` は、パススルー認証に関連付けられています。

`ibm-slapdPtaExt`

パススルー認証項目用の属性マッピング設定が含まれています。属性マッピングを指定するには、`ibm-slapdPta` オブジェクト・クラスを持つパススルー認証項目にこのオブジェクト・クラスを追加する必要があります。

`ibm-PtaReferral`

ディレクトリー情報ツリー (DIT) 内の項目のパススルー認証用のリンク属性が含まれています。

`ibm-slapdPta` オブジェクト・クラスの属性

`ibm-slapdPta` オブジェクト・クラスを持つパススルー認証項目を構成するには、その属性を設定する必要があります。

表 28. `ibm-slapdPta` オブジェクト・クラスの `MUST` および `MAY` 属性

属性名	属性タイプ (MUST/MAY)	説明	例
<code>ibm-slapdPtaURL</code>	MUST	パススルー・サーバーの URL 情報。この URL には、完全修飾ホスト名または IP アドレス、およびポート情報が含まれている必要があります。SSL 接続の場合は <code>ldaps://</code> を使用します。	<code>ldap://server:port</code> または <code>ldaps://server:port</code> (SSL の場合)

表 28. *ibm-slapdPta* オブジェクト・クラスの *MUST* および *MAY* 属性 (続き)

属性名	属性タイプ (MUST/MAY)	説明	例
<i>ibm-slapdPtaSubtree</i>	MUST	パススルー認証および認証要求の確認用に構成されたディレクトリー・サーバー・インスタンス内のサブツリー。	<code>o=sample</code>
<i>ibm-slapdPtaResultTimeout</i>	MAY	<code>ldap_result()</code> 呼び出し時にパススルー認証インターフェースが待機するミリ秒。値は、ミリ秒で指定します。デフォルト値は 1000 ミリ秒です。	1000
<i>ibm-slapdPtaMigratePwd</i>	MAY	認証が成功した場合、ローカル・ディレクトリー項目にユーザー・パスワードを格納します。属性が項目内にはない場合は、デフォルト値 <code>false</code> が割り当てられます。	<code>false</code>
<i>ibm-slapdPtaConnectionPoolSize</i>	MAY	各パススルー・サーバーに対して接続の数を設定します。最小プール・サイズは 2、デフォルトは 4 です。	4

***ibm-slapdPtaExt* オブジェクト・クラスの属性**

ibm-slapdPtaExt オブジェクト・クラスを持つパススルー認証項目で属性マッピングを指定するには、その属性を設定する必要があります。

表 29. *ibm-slapdPtaExt* オブジェクト・クラスの *MUST* および *MAY* 属性

属性名	属性タイプ (MUST/MAY)	説明	例
<i>ibm-slapdPtaSearchBase</i>	MUST	項目を検索するパススルー・サーバーの検索ベース。	<code>o=sample1</code>
<i>ibm-slapdPtaAttrMapping</i>	MUST	パススルー・サーバーの属性に対する IBM Security Directory Server の属性のマッピング。属性マッピングの例は、 <code>cn \$ uid</code> です。これは、IBM Security Directory Server の <code>cn</code> 属性がパススルー・サーバーの <code>uid</code> 属性にマップされることを示します。	<code>attr1 \$ attr2</code>
<i>ibm-slapdPtaBindDN</i>	MUST	パススルー・サーバーのバインド DN 値。	<code>cn=admin1</code>
<i>ibm-slapdPtaBindPW</i>	MUST	パススルー・サーバーのバインド・パスワード。	<code>password123</code>

ibm-PtaReferral オブジェクト・クラスの属性

ibm-PtaReferral オブジェクト・クラスを持つ項目のパススルー認証に対してリンク属性を指定するには、その属性を設定する必要があります。

表 30. *ibm-PtaReferral* オブジェクト・クラスの *MUST* および *MAY* 属性

属性名	属性タイプ (MUST/MAY)	説明	例
ibm-PtaLinkAttribute	MUST	<p>この属性には、パススルー・サーバーのマッピング属性の名前が値として含まれています。例えば、empNo のようになります。</p> <p>特別なケースが 2 つあります。</p> <ul style="list-style-type: none">• <code>_DN_</code> 値は、<code>ibm-PtaLinkValue</code> 属性に項目の DN が含まれていることを示します。これをパススルー・サーバーにマップする必要があります。• <code>_DISABLE_</code> 値は、その項目でパススルー認証を実行することが禁止されていることを示します。この場合、<code>LDAP_INVALID_CREDENTIALS</code> 戻りコードがクライアントに送信されます。 <p><code>_DN_</code> および <code>_DISABLE_</code> では大文字と小文字を区別しません。</p>	empNo
ibm-PtaLinkValue	MUST	パススルー・サーバーを検索するために、リンク属性とともに使用する値。	E0345

SSL を介したパススルー認証

SSL を介したパススルー認証を構成するには、特定の要件が満たされているようにする必要があります。

以下の条件を満たすようにします。

- 外部パススルー認証サーバーと IBM Security Directory Server の両方がセキュア・モードで実行されている必要があります。IBM Security Directory Server 内のパススルー認証構成では、追加の鍵ストア (kdb) ファイルは必要ありません。これは、メインのサーバー・コンポーネントによって使用されるのと同じ鍵ストア・ファイルに依存します。IBM Security Directory Server は、SSL を介したパススルー認証のための SSL 通信用に構成する必要があります。
- 外部パススルー認証サーバーは、IBM Security Directory Server によって使用されるのと同じ鍵ストア・ファイルおよび鍵ストア・パスワードを使用して、LDAP クライアントと通信する必要があります。
- パススルー認証用の `ibm-slapdPtaURL` パラメーターは、次の形式の `ldaps://` URL である必要があります。

```
ibm-slapdPtaURL: ldaps://host_name:secure_port
```

パススルー認証プロセス中、IBM Security Directory Server は、外部パススルー認証サーバーのクライアントとして動作します。このクライアント/サーバー通信が正常に動作するためには、互換性のある鍵ペアが必要です。IBM Security Directory Server で使用する鍵ペアおよび鍵ストア・ファイルを作成する方法については、151 ページの『ディレクトリー通信のセキュリティ』のセクションを参照してください。

パススルー認証シナリオ

パススルー認証シナリオを使用して、現在のディレクトリー・サーバー環境に適した構成を識別します。

以下の基本的なシナリオに対して、パススルー認証を構成できます。

- 属性マッピングが設定されており、項目が認証サーバー内にある。
- 属性マッピングおよびパスワード移行が設定されており、項目が認証サーバー内にある。
- 属性マッピングは設定されておらず、項目は認証サーバー内にない。
- `ibm-ptaReferral` 補助オブジェクト・クラスを使用して、属性マッピングが設定されている。
- パススルー認証が Active Directory グローバル・カタログに対して設定されている。

分散ディレクトリーのサブツリーに対して単一のパススルー・サーバーを使用する場合は、すべてのバックエンド・サーバーにおいてパススルー・インターフェースを構成する必要があります。同じサブツリーに対して複数のパススルー・サーバーを使用する場合は、適切なバックエンド・サーバーにおいて必要なパススルー・インターフェースを構成する必要があります。

シナリオ 1: 認証サーバーの項目に対する属性マッピング:

認証サーバーにおいて資格情報が含まれていないユーザー項目に対して、属性マッピングを構成することができます。

このシナリオでは、認証サーバーにおいてすべての項目に固有値を持つ属性を識別する必要があります。また、すべての項目について認証サーバー内の属性に一意的にマップできる属性をパススルー・サーバー内で見つけることも必要です。属性の名前が両方のサーバーで一致している必要はありません。

認証サーバーからパススルー・サーバーにマップするために識別された属性には、固有値が含まれている必要があります。この属性を使用して、パススルー・サーバー内の項目に対して、パススルー認証が必要になる認証サーバー内のすべての項目をマップすることも必要です。例えば、認証サーバー内の `uid=Tom456` をパススルー・サーバー内の `userPrincipalName=Tom456` にマップすることができます。属性マッピングを設定したら、パススルー・サーバーでの `userPrincipalName=Tom456` フィルターによる検索で、一致する項目を 1 つだけ取得する必要があります。複数の項目が返された場合、パススルー認証は失敗し、エラー・メッセージが生成されます。

このシナリオでは、認証サーバーで以下の状態が発生する場合があります。

- 固有値を持つ属性が認証サーバー内に存在し、それに一致する、固有値を持つ属性がパススルー・サーバー内に存在している。
- 固有値を持つ属性が認証サーバー内に存在しない。

ケース 1: 固有値を持つ属性が認証サーバー内に存在している:

認証サーバー内の項目には uid 属性が含まれており、この属性の値はすべての項目に対して固有の値です。認証サーバー内のすべての項目をパススルー・サーバー内の項目に直接マップできます。

例えば、認証サーバー内の uid 属性をパススルー・サーバー内の userPrincipalName 属性にマップできます。以下の例は、認証サーバーの項目を示しています。

```
dn: cn=Tom Brown,o=sample cn: Tom sn: Brown uid: Tom456
objectclass: organizationalPerson objectclass: person objectclass: top
objectclass: inetOrgPerson
```

以下の例は、属性マッピングに対して認証サーバーのパススルー・インターフェースで構成できるマップを示しています。

```
ibm-slapdPtaAttrMapping : uid $ userPrincipalName
```

ケース 2: 固有値を持つ属性が認証サーバー内に存在していない:

認証サーバーにおいて固有値を持つ属性が識別できない場合は、すべての項目に固有値を持つ属性を追加します。

固有値を持つ属性を追加するには、補助オブジェクト・クラスを作成して、それに属性を追加します。また、項目に関連付けられている既存のオブジェクト・クラスの属性を使用することもできます。この場合、認証サーバー内の固有値を持つこの属性をパススルー・サーバー内の属性にマップできます。以下の例は、固有値を持つ属性の追加後の認証サーバーの項目を示しています。

```
dn: cn=Tom Brown,o=sample
cn: Tom
sn: Brown
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: inetOrgPerson
objectclass: my-aux-class
uniqueAttrValue: my_value
```

以下の例は、属性マッピングに対して認証サーバーのパススルー・インターフェースで構成できるマップを示しています。

```
ibm-slapdPtaAttrMapping : uniqueAttrValue $ userPrincipalName
```

パススルー認証の固有属性を使用した属性マッピングの構成:

認証サーバー内の資格情報を持たないサブツリーの項目をサーバーで認証するには、属性マッピングを設定します。

手順

1. インスタンス所有者としてログインします。

2. ディレクトリー・サーバー・インスタンス上でパススルー認証を設定するには、以下のように **idsldapmodify** コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setPtaFile.ldif
```

setPtaFile.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Configuration
changetype: modify
replace: ibm-slapdPtaEnabled
ibm-slapdPtaEnabled: true
```

3. **ibm-slapdPtaEnabled** 属性に加えられた変更を適用するには、以下のように **idsldapexop** コマンドを実行します。

```
idsldapexop -h server.com -p port -D adminDN -w adminPWD -op readconfig ¥
-scope single cn=Configuration ibm-slapdPtaEnabled
```

4. 属性マッピングに対してパススルー・インターフェースを構成するには、以下のように **idsldapmodify** コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setAttrMap.ldif
```

setAttrMap.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Passthrough Server1, cn=Passthrough Authentication, cn=Configuration
changetype: add
cn: Passthrough Server1
ibm-slapdPtaURL: ldap://hostnameOfPassThroughServer:port
ibm-slapdPtaSubtree: o=sample
ibm-slapdPtaAttrMapping: uid $ userPrincipalName
ibm-slapdPtaSearchBase: cn=users,dc=pta,dc=com
ibm-slapdPtaBindDN: bind_DN
ibm-slapdPtabindPW: bind_PWD
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdPta
objectclass: ibm-slapdPtaExt
```

5. ディレクトリー・サーバーおよび管理サーバーを再始動します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
ibmslapd -I dsrdbm01 -n
ibmdiradm -I dsrdbm01
```

例

- 例 1:** 認証サーバー内の項目を検索するには、**idsldapsearch** コマンドを以下の形式で実行します。

```
idsldapsearch -h server.com -p port -D cn=Tom Brown,o=sample -w userPWD ¥
-s sub -b "cn=Tom Brown,o=sample" objectclass=*
cn=Tom Brown,o=sample
cn=Tom
sn=Brown
uid=Tom456
objectclass=inetOrgPerson
objectclass=organizationalPerson
objectclass=person
objectclass=top
```

- 例 2:** ユーザー・パスワード値を比較するには、**idsldapcompare** コマンドを以下の形式で実行します。

```
idsldapcompare -h server.com -p port -D adminDN -w adminPWD ¥
cn=Tom Brown,o=sample userpassword=userPWD
比較 true
```

パススルー認証用の固有属性の作成および属性マッピングの構成:

認証サーバー内の資格情報を持たない項目に対して、固有値を持つ属性を作成し、属性マッピングを構成します。

手順

1. インスタンス所有者としてログインします。
2. 属性マッピングの属性を作成します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i uniqAttr.ldif
```

uniqAttr.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( uniqueAttrValue-OID NAME 'uniqueAttrValue' DESC
'To use for attribute mapping in the authentication server' EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE USAGE directoryOperation )
-
add: ibmattributetypes
ibmattributetypes: ( uniqueAttrValue-OID DBNAME ( 'uniqueAttrValue' )
ACCESS-CLASS NORMAL LENGTH 240 )
```

3. 属性に関連付けられている補助オブジェクト・クラスを作成します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i uniqObj.ldif
```

uniqObj.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( my-aux-class-OID NAME 'my-aux-class' DESC
'An object class to hold attribute with unique value for attribute mapping'
SUP top AUXILIARY MUST (uniqueAttrValue) )
```

4. オブジェクト・クラスおよび属性を、認証サーバー内でパススルー認証を必要とする項目に追加します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i addObjAttr.ldif
```

addObjAttr.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Tom Brown,o=sample
changetype: modify
add: objectclass
objectclass: my-aux-class
-
add: uniqueAttrValue
uniqueAttrValue: Tom456

dn: cn=Bob John,o=sample
changetype: modify
add: objectclass
objectclass: my-aux-class
-
add: uniqueAttrValue
uniqueAttrValue: Bob890
```

5. ディレクトリー・サーバー・インスタンス上でパススルー認証を設定するには、以下のように **idsldapmodify** コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setPtaFile.ldif
```

setPtaFile.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Configuration
changetype: modify
replace: ibm-slapdPtaEnabled
ibm-slapdPtaEnabled: true
```

6. **ibm-slapdPtaEnabled** 属性値に加えられた変更を適用するには、以下のように **idsldapexop** コマンドを実行します。

```
idsldapexop -h server.com -p port -D adminDN -w adminPWD -op readconfig ¥
-scope single cn=Configuration ibm-slapdPtaEnabled
```

7. 属性マッピングに対してパススルー・インターフェースを構成するには、以下のように **idsldapmodify** コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setAttrMap.ldif
```

setAttrMap.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Passthrough Server1, cn=Passthrough Authentication, cn=Configuration
changetype: add
cn: Passthrough Server1
ibm-slapdPtaURL: ldap://hostnameOfPassThroughServer:port
ibm-slapdPtaSubtree: o=sample
ibm-slapdPtaAttrMapping: uniqueAttrValue $ userPrincipalName
ibm-slapdPtaSearchBase: cn=users,dc=pta,dc=com
```

```
ibm-slapdPtaBindDN: bind_DN
ibm-slapdPtabindPW: bind_PWD
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdPta
objectclass: ibm-slapdPtaExt
```

8. ディレクトリー・サーバーおよび管理サーバーを再始動します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
ibmslapd -I dsrdbm01 -n
ibmdiradm -I dsrdbm01
```

例

例 1: 認証サーバー内の項目を検索するには、`idsldapsearch` コマンドを以下の形式で実行します。

```
idsldapsearch -h server.com -p port -D cn=Bob John,o=sample -w userPWD ¥
-s sub -b "cn=Bob John,o=sample" objectclass=*
cn=Bob John,o=sample
cn=Bob
sn=John
uniqueAttrValue=Bob890
objectclass=my-aux-class
objectclass=person
objectclass=top
```

例 2: ユーザー・パスワード値を比較するには、`idsldapcompare` コマンドを以下の形式で実行します。

```
idsldapcompare -h server.com -p port -D adminDN -w adminPWD ¥
cn=Bob John,o=sample userpassword=userPWD
比較 true
```

シナリオ 2: 認証サーバー内の項目に対する属性マッピングおよびパスワード移行:

パススルー・サーバーで項目が正常に認証された場合、認証サーバー内にその項目に対するパスワードを格納できます。次に認証を行う場合、パススルー・サーバーで認証を行う必要はありません。

このシナリオでは、項目は認証サーバー内に存在しています。認証サーバー内の項目の固有属性を、パススルー・サーバー内の項目の属性にマップできます。

最初の認証に成功すると、ユーザーが指定したパスワードが、認証サーバー内のユーザー項目の `userpassword` 属性に格納されます。認証サーバーは、サーバーで設定されている暗号化スキームでパスワードを暗号化して格納します。認証サーバーでパスワード・ポリシーが設定されている場合、パスワードは設定されているパスワード・ポリシーに従う必要があります。ユーザーからの以降の認証要求は認証サーバーで認証され、パススルー・サーバーには送付されません。

パススルー・サーバーと認証サーバーの間でパスワードの整合性を確保する必要があります。これらのパスワードに不整合が生じると、セキュリティに関する潜在的な脅威となる場合があります。また、認証サーバーとパススルー・サーバーの間でパスワードの健全性も確保する必要があります。

認証サーバーで監査機能を有効にしている場合、サーバーはユーザー項目に対してパスワードが変更された際に監査ログに記録します。以下の例では、パスワード移行が設定されている場合のユーザー項目に関する監査記録を示します。

```
AuditV3--2013-06-05-19:17:39.949+5:30--V3 Bind--bindDN:
cn=A1 Garcia, ou=Home Entertainment, ou=Austin, o=sample
--client: 127.0.0.1:9111--connectionID: 1--received: 2013-06-05-19:17:39.836+5:30
--Success
controlType: 1.3.6.1.4.1.42.2.27.8.5.1
criticality: false
passthroughBindDN: cn=A1 Garcia, ou=Home Entertainment, ou=Austin, o=sample
passthroughServer: ldap://127.0.0.1:1389
passthroughBindRC: 0
```

```

AuditV3--2013-06-05-19:17:39.949+5:30--V3 Bind--bindDN: CN=ROOT--client: 127.0.0.1:9623
--connectionID: 2--received: 2013-06-05-19:17:39.948+5:30--Success
controlType: 1.3.18.0.2.10.15
criticality: true
controlType: 1.3.6.1.4.1.42.2.27.8.5.1
criticality: false
name: CN=ROOT
authenticationChoice: simple
Admin Acct Status: Not Locked
AuditV3--2013-06-05-19:17:40.029+5:30--V3 Modify--bindDN: CN=ROOT--client: 127.0.0.1:9623
--connectionID: 2--received: 2013-06-05-19:17:39.949+5:30--Success
controlType: 1.3.18.0.2.10.15
criticality: true
controlType: 1.3.6.1.1.12
criticality: true
object: cn=Al Garcia, ou=Home Entertainment, ou=Austin, o=sample
add: userpassword
AuditV3--2013-06-05-19:17:40.030+5:30--V3 Unbind--bindDN: CN=ROOT--client: 127.0.0.1:9623
--connectionID: 2--received: 2013-06-05-19:17:40.029+5:30--Success
AuditV3--2013-06-05-19:17:52.101+5:30--V3 Unbind--bindDN:
cn=Al Garcia, ou=Home Entertainment, ou=Austin, o=sample--client: 127.0.0.1:9111
--connectionID: 1--received: 2013-06-05-19:17:52.100+5:30--Success

```

この監査記録の例では、ユーザー項目でパスワードが更新された際に、以下の操作が記録されます。

1. ユーザーによる最初のパススルー認証が正常に行われると、サーバーは管理者の資格情報で認証サーバーにバインドされます。
2. サーバーは、正常に行われた認証においてユーザーが指定したパスワードで、ユーザー項目内に `userpassword` 属性を追加します。
3. `userpassword` 属性の追加後、サーバーはアンバインドされます。

パススルー認証用の属性マッピングおよびパスワード移行の構成:

認証サーバー内のサブツリーの項目に対して、属性マッピングおよびパスワード移行を構成します。認証が正常に行われた項目に対しては、以降の認証に使用するために認証サーバー内に該当する項目のパスワードを格納することができます。

手順

1. インスタンス所有者としてログインします。
2. ディレクトリー・サーバー・インスタンス上でパススルー認証を設定するには、以下のように `idsldapmodify` コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setPtaFile.ldif
```

`setPtaFile.ldif` ファイルには、以下の項目が格納されています。

```
dn: cn=Configuration
changetype: modify
replace: ibm-slapdPtaEnabled
ibm-slapdPtaEnabled: true
```

3. `ibm-slapdPtaEnabled` 属性値に加えられた変更を適用するには、以下のように `idsldapexop` コマンドを実行します。

```
idsldapexop -h server.com -p port -D adminDN -w adminPWD -op readconfig ¥
-scope single cn=Configuration ibm-slapdPtaEnabled
```

4. 属性マッピングおよびパスワード移行に対してパススルー・インターフェースを構成するには、以下のように `idsldapmodify` コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setPtaPwdMigFile.ldif
```

`setPtaPwdMigFile.ldif` ファイルには、以下の項目が格納されています。

```
dn: cn=Passthrough Server1, cn=Passthrough Authentication, cn=Configuration
changetype: add
cn: Passthrough Server1
ibm-slapdPtaURL: ldap://hostnameOfPassThroughServer:port
ibm-slapdPtaSubtree: o=sample
ibm-slapdPtaAttrMapping: uid $ userPrincipalName
ibm-slapdPtaSearchBase: cn=users,dc=pta,dc=com
```

```
ibm-slapdPtaBindDN: bind_DN
ibm-slapdPtabindPW: bind_PWD
ibm-slapdPtaMigratePwd: TRUE
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdPta
objectclass: ibm-slapdPtaExt
```

5. ディレクトリー・サーバーおよび管理サーバーを再始動します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
ibmslapd -I dsrdbm01 -n
ibmdiradm -I dsrdbm01
```

例

例 1: 認証サーバー内の項目を検索するには、**idsldapsearch** コマンドを以下の形式で実行します。

```
idsldapsearch -h server.com -p port -D cn=Tom Brown,o=sample -w userPWD ¥
-s sub -b "cn=Tom Brown,o=sample" objectclass=*
cn=Tom Brown,o=sample
cn=Tom
sn=Brown
uid=Tom456
userpassword=userPWD
objectclass=inetOrgPerson
objectclass=organizationalPerson
objectclass=person
objectclass=top
```

例 2: ユーザー・パスワード値を比較するには、**idsldapcompare** コマンドを以下の形式で実行します。

```
idsldapcompare -h server.com -p port -D adminDN -w adminPWD ¥
cn=Tom Brown,o=sample userpassword=userPWD
比較 true
```

シナリオ 3: 認証サーバー内に存在しない項目の構成:

項目が認証サーバー内に存在しない場合でも、サブツリーの項目に対してパススルー認証を構成することができます。

認証サーバーでバインド操作または比較操作を実行すると、サーバーはユーザー項目が存在するかどうかをチェックします。項目が存在しない場合、サーバーは項目がパススルーの候補であるかどうかをチェックします。パススルー・インターフェースが設定されている場合、認証サーバーは DN および資格情報をパススルー・サーバーに送付します。認証が成功すると、サーバーは LDAP_SUCCESS を返します。認証が失敗した場合、サーバーは LDAP_INVALID_CREDENTIALS を返します。認証サーバーに項目が存在しない場合、パスワード移行は設定されていても無視されません。

認証サーバー内に存在しない項目に対するパススルー認証の構成:

項目が認証サーバー内に存在しない場合でも、パススルー認証のためにサブツリーの項目を構成します。

手順

1. インスタンス所有者としてログインします。
2. ディレクトリー・サーバー・インスタンス上でパススルー認証を設定するには、以下のように **idsldapmodify** コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setPtaFile.ldif
```

setPtaFile.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Configuration
changetype: modify
replace: ibm-slapdPtaEnabled
ibm-slapdPtaEnabled: true
```

3. **ibm-slapdPtaEnabled** 属性値に加えられた変更を適用するには、以下のように **idsldapexop** コマンドを実行します。

```
idsldapexop -h server.com -p port -D adminDN -w adminPWD -op readconfig ¥
-scope single cn=Configuration ibm-slapdPtaEnabled
```

4. サブツリーの項目に対してパススルー・インターフェースを構成するには、以下のように **idsldapmodify** コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD ¥
-i setPtaNonExistEntriesFile.ldif
```

setPtaNonExistEntriesFile.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Passthrough Server1, cn=Passthrough Authentication, cn=Configuration
changetype: add
cn: Passthrough Server1
ibm-slapdPtaURL: ldap://hostnameOfPassThroughServer:port
ibm-slapdPtaSubtree: o=sample
ibm-slapdPtaConnectionPoolSize: 6
ibm-slapdPtaResultTimeout: 100
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdPta
```

5. ディレクトリー・サーバーおよび管理サーバーを再始動します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
ibmslapd -I dsrdbm01 -n
ibmdiradm -I dsrdbm01
```

例

- 例 1: 認証サーバー内の項目を検索するには、**idsldapsearch** コマンドを以下の形式で実行します。

```
idsldapsearch -h server.com -p port -D cn=Tom Brown,o=sample -w userPWD ¥
-s base -b "" objectclass=* namingcontexts

namingcontexts=CN=SCHEMA
namingcontexts=CN=LOCALHOST
namingcontexts=CN=IBMPOLICIES
namingcontexts=O=SAMPLE
```

- 例 2: ユーザー・パスワード値を比較するには、**idsldapcompare** コマンドを以下の形式で実行します。

```
idsldapcompare -h server.com -p port -D adminDN -w adminPWD ¥
cn=Tom Brown,o=sample userpassword=userPWD
比較 true
```

シナリオ 4: **ibm-ptaReferral** オブジェクト・クラスを使用した属性マッピング:

ibm-ptaReferral オブジェクト・クラスで属性マッピングを設定し、パススルー・サーバー内の項目に直接にはマップされていないユーザーを認証することができます。

このシナリオでは、認証サーバー内の複数の項目をパススルー・サーバー内の 1 つの項目にマップすることが必要になる場合があります。例えば、ユーザーが認証サーバー内に複数の LDAP 項目を持っている場合は、多対 1 のマッピングが必要になります。

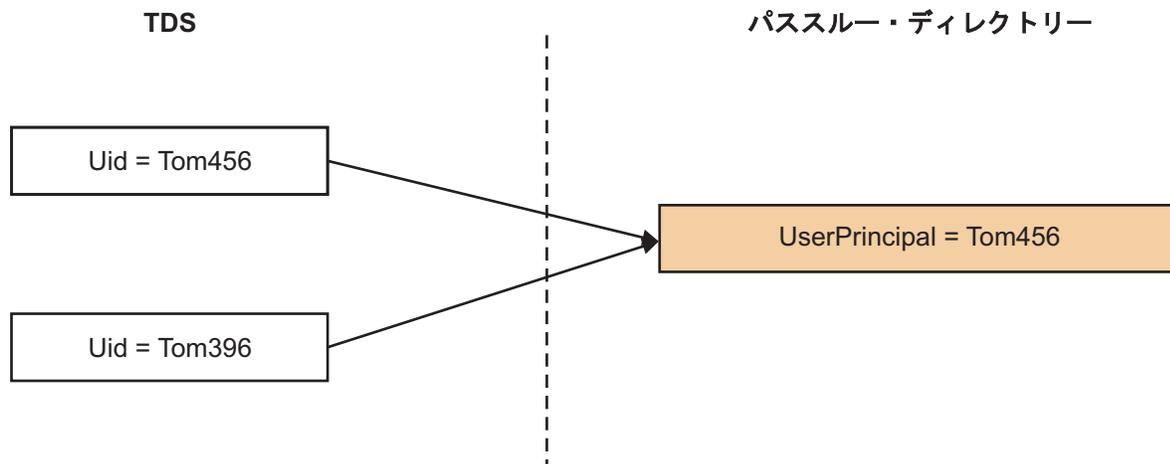


図2. 属性マッピング

この例では、認証サーバー内の uid=Tom456 項目をパススルー・サーバー内の userPrincipalName=Tom456 項目にマップできます。ただし、uid=Tom396 項目を userPrincipalName=Tom456 項目にマップすることはできません。これは、項目は同じユーザーに属しているにもかかわらず、その値が異なっているためです。この場合、パススルー・サーバー上に対応するマップ項目が存在しないため、uid=Tom396 に対する認証要求が失敗することがあります。この問題を解決するには、認証サーバー内のマップ対象の項目に `ibm-ptaReferral` 補助オブジェクト・クラスを追加する必要があります。また、`ibm-ptaReferral` オブジェクト・クラスの `MUST` 属性 `ibm-PtaLinkAttribute` および `ibm-PtaLinkValue` に適切な値を割り当てる必要があります。

ユーザーが認証サーバー上で認証を試みると、パススルー・インターフェースは `ibm-ptaReferral` オブジェクト・クラスが存在するかどうかをチェックします。項目内に `ibm-ptaReferral` オブジェクト・クラスが存在する場合、インターフェースは `ibm-PtaLinkAttribute` および `ibm-PtaLinkValue` 属性値を使用して、パススルー・サーバーで確認を行います。

パススルー認証に対して項目を構成するために `ibm-ptaReferral` 補助オブジェクト・クラスを追加した場合、項目に対して構成された属性マッピングは無視されます。

このシナリオでは、認証サーバーで以下の状態が発生する場合があります。

- 属性値を使用して、認証サーバー内の項目をパススルー・サーバー内の項目にマップすることができる。
- 属性値を使用しても、認証サーバー内の項目をパススルー・サーバー内の項目にマップすることはできない。

ケース 1: 認証サーバー内の項目がパススルー・サーバー内の項目にマップできる:

パススルー・サーバー内にマッピング項目が含まれていない項目の場合は、この項目に `ibm-ptaReferral` 補助オブジェクト・クラスを追加する必要があります。

例えば、uid=Tom396 項目をパススルー・サーバー内の userPrincipalName=Tom456 項目にマップするには、項目に以下の値が含まれている必要があります。

```
dn: cn=Tom Brown1,o=sample
cn: Tom
sn: Brown1
uid: Tom396
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: inetOrgPerson
objectclass: ibm-ptaReferral
ibm-ptaLinkAttribute: userPrincipalName
ibm-ptaLinkValue: Tom456
```

ケース 2: 認証サーバー内の項目がパススルー・サーバー内の項目にマップできない:

認証サーバー内にマップ対象の固有属性が存在しない場合は、DN 値をマップとして設定できます。

認証サーバー内の DN を知っておく必要があります。これは、パススルー・サーバー内の項目にマップできます。DN をマップ値として使用するには、`ibm-PtaLinkAttribute` 属性を `_DN_` に設定する必要があります。`ibm-PtaLinkValue` 属性値を、パススルー・サーバー内のマップ対象項目の DN に設定する必要があります。ユーザーが認証を試みると、パススルー・インターフェースは指定した DN 値と指定した資格情報を取得して、ユーザーを確認します。

以下の例は、`ibm-PtaLinkAttribute` が `_DN_` に設定された項目を示しています。

```
dn: cn=Tom Brown1,o=sample
uid:Tom396
cn: Tom
sn: Brown1
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: ibm-ptaReferral
ibm-ptaLinkAttribute: _DN_
ibm-ptaLinkValue: cn=Tom456,cn=users,dc=pta,dc=com
```

DN 値を設定された項目に対してパススルー対応を指定しない場合は、`ibm-PtaLinkAttribute` を `_DISABLE_` に設定する必要があります。

ibm-ptaReferral オブジェクト・クラスを使用した、項目に対するパススルー認証の構成:

パススルー・サーバー内の項目に直接にはマップされていない、認証サーバー内の項目に対してパススルー認証を構成します。このような項目に対しては、パススルー認証用に `ibm-ptaReferral` オブジェクト・クラスを追加して、オブジェクト・クラスの属性を設定します。

手順

1. インスタンス所有者としてログインします。
2. `ibm-ptaReferral` オブジェクト・クラスとその属性を、パススルー・サーバー内の項目にマップする対象となる項目に追加します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setAuxObjAttr.ldif
```

`setAuxObjAttr.ldif` ファイルには、以下の項目が格納されています。

```
dn: cn=Tom Brown1,o=sample
changetype: modify
add: objectclass
objectclass: ibm-ptaReferral
-
add: ibm-ptalinkAttribute
ibm-ptalinkAttribute: userPrincipalName
-
add: ibm-ptalinkValue
ibm-ptalinkValue: Tom456
```

3. ディレクトリー・サーバー・インスタンス上でパススルー認証を設定するには、以下のように **idsldapmodify** コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setPtaFile.ldif
```

setPtaFile.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Configuration
changetype: modify
replace: ibm-slappTaEnabled
ibm-slappTaEnabled: true
```

4. **ibm-slappTaEnabled** 属性に加えられた変更を適用するには、以下のように **idsldapexop** コマンドを実行します。

```
idsldapexop -h server.com -p port -D adminDN -w adminPWD -op readconfig ¥
-scope single cn=Configuration ibm-slappTaEnabled
```

5. 属性マッピングに対してパススルー・インターフェースを構成するには、以下のように **idsldapmodify** コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setAttrMap.ldif
```

setAttrMap.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Passthrough Server1, cn=Passthrough Authentication, cn=Configuration
changetype: add
cn: Passthrough Server1
ibm-slappTaURL: ldap://hostnameOfPassThroughServer:port
ibm-slappTaSubtree: o=sample
ibm-slappTaAttrMapping: uid $ userPrincipalName
ibm-slappTaSearchBase: cn=users,dc=pta,dc=com
ibm-slappTaBindDN: bind_DN
ibm-slappTaBindPW: bind_PWD
objectclass: top
objectclass: ibm-slappConfigEntry
objectclass: ibm-slappTa
objectclass: ibm-slappTaExt
```

6. ディレクトリー・サーバーおよび管理サーバーを再始動します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
ibmslapd -I dsrdbm01 -n
ibmdiradm -I dsrdbm01
```

例

- 例 1:** 認証サーバー内の項目を検索するには、**idsldapsearch** コマンドを以下の形式で実行します。

```
idsldapsearch -h server.com -p port -D cn=Tom Brown1,o=sample -w userPWD1 ¥
-s sub -b "cn=Tom Brown1,o=sample" objectclass=*
cn=Tom Brown1,o=sample
cn=Tom
sn=Brown1
ibm-ptalinkAttribute=userPrincipalName
ibm-ptalinkValue=Tom456
objectclass=ibm-ptaReferral
objectclass=inetOrgPerson
objectclass=organizationalPerson
objectclass=person
objectclass=top
```

- 例 2:** ユーザー・パスワード値を比較するには、**idsldapcompare** コマンドを以下の形式で実行します。

```
idsldapcompare -h server.com -p port -D adminDN -w adminPWD ¥
cn=Tom Brown1,o=sample userpassword=userPWD1
比較 true
```

ibm-ptaReferral オブジェクト・クラスを使用して DN 値を設定することによるパススルー認証の構成:

パススルー DN 値をマップ値として設定することにより、認証サーバー内の項目に対してパススルー認証を構成します。認証サーバー内の項目に固有値を持つ属性が含まれていない場合は、DN 値をマップ値として使用できます。

手順

1. インスタンス所有者としてログインします。
2. `ibm-ptaReferral` オブジェクト・クラスとその属性を、パススルー・サーバー内の項目にマップする対象となる項目に追加します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setAuxObjAttr.ldif
```

`setAuxObjAttr.ldif` ファイルには、以下の項目が格納されています。

```
dn: cn=Tom Brown1,o=sample
changetype: modify
add: objectclass
objectclass: ibm-ptaReferral-
-
add: ibm-ptalinkAttribute
ibm-ptalinkAttribute: _DN_
-
add: ibm-ptalinkValue
ibm-ptalinkValue: userPrincipalName=Tom456,cn=users,dc=pta,dc=com
```

3. ディレクトリー・サーバー・インスタンス上でパススルー認証を設定するには、以下のように `idsldapmodify` コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setPtaFile.ldif
```

`setPtaFile.ldif` ファイルには、以下の項目が格納されています。

```
dn: cn=Configuration
changetype: modify
replace: ibm-slapdPtaEnabled
ibm-slapdPtaEnabled: true
```

4. `ibm-slapdPtaEnabled` 属性に加えられた変更を適用するには、以下のように `idsldapexop` コマンドを実行します。

```
idsldapexop -h server.com -p port -D adminDN -w adminPWD -op readconfig ¥
-scope single cn=Configuration ibm-slapdPtaEnabled
```

5. 属性マッピングに対してパススルー・インターフェースを構成するには、以下のように `idsldapmodify` コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setAttrMap.ldif
```

`setAttrMap.ldif` ファイルには、以下の項目が格納されています。

```
dn: cn=Passthrough Server1, cn=Passthrough Authentication, cn=Configuration
changetype: add
cn: Passthrough Server1
ibm-slapdPtaURL: ldap://hostnameOfPassThroughServer:port
ibm-slapdPtaSubtree: o=sample
ibm-slapdPtaAttrMapping: uid $ userPrincipalName
ibm-slapdPtaSearchBase: cn=users,dc=pta,dc=com
ibm-slapdPtaBindDN: bind_DN
ibm-slapdPtaBindPW: bind_PWD
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdPta
objectclass: ibm-slapdPtaExt
```

6. ディレクトリー・サーバーおよび管理サーバーを再始動します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
ibmslapd -I dsrdbm01 -n
ibmdiradm -I dsrdbm01
```

例

例 1: 認証サーバー内の項目を検索するには、`idsldapsearch` コマンドを以下の形式で実行します。

```
idsldapsearch -h server.com -p port -D cn=Tom Brown1,o=sample -w userPWD1 ¥
-s sub -b "cn=Tom Brown1,o=sample" objectclass=*
cn=Tom Brown1,o=sample
cn=Tom
sn=Brown1
ibm-ptaLinkAttribute=_DN_
ibm-ptaLinkValue=userPrincipalName=Tom456,cn=users,dc=pta,dc=com
objectclass=ibm-ptaReferral
objectclass=inetOrgPerson
objectclass=organizationalPerson
objectclass=person
objectclass=top
```

例 2: ユーザー・パスワード値を比較するには、`idsldapcompare` コマンドを以下の形式で実行します。

```
idsldapcompare -h server.com -p port -D adminDN -w adminPWD ¥
cn=Tom Brown1,o=sample userpassword=userPWD1
比較 true
```

シナリオ 5: Active Directory グローバル・カタログに対するパススルー認証の構成:

パススルー認証用の DN および資格情報を、特定のパススルー・サーバーの代わりに Microsoft Active Directory フォレストに送付できます。

外部サーバーに対して認証を行うには、パススルー認証用に属性マッピングを構成することが必要になる場合があります。属性マッピングでは、ユーザーが認証を行うパススルー・インターフェースで以下の情報を指定する必要があります。

- 属性マッピング (`ibm-slapdPtaAttrMapping`) (認証サーバーとパススルー・サーバーで DN が同一ではない場合)
- パススルー認証サブツリー (`ibm-slapdPtaSubtree`)
- 検索ベース (`ibm-slapdPtaSearchBase`)
- パススルー・サーバー URL (`ibm-slapdPtaURL`)
- バインド DN (`ibm-slapdPtaBindDN`)
- バインド・パスワード (`ibm-slapdPtabindPW`)

特定の外部サーバーの代わりに Active Directory フォレストに対して認証を行うには、NULL 検索ベース (『』) を指定する必要があります。Active Directory フォレストに対して認証を行う場合は、`ibm-slapdPtaSearchBase` 属性に値を設定しないでください。この属性は空にしておく必要があります。認証サーバーは、Active Directory に対する検索をグローバル・カタログ検索にするために『』という検索ベースを使用します。この検索は、グローバル・カタログ・ポート 3268 を介して送付されます。

Active Directory グローバル・カタログについて詳しくは、Microsoft TechNote Web サイトで、キーワード *Global Catalog and LDAP searches* を検索してください。

Active Directory グローバル・カタログに対してパススルー認証を構成する:

Microsoft Active Directory グローバル・カタログに接続するようにパススルー認証インターフェースを設定することにより、認証サーバーに対して認証を行うサブツリーの項目を構成します。

手順

1. インスタンス所有者としてログインします。
2. ディレクトリー・サーバー・インスタンス上でパススルー認証を設定するには、以下のように **idsldapmodify** コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD -i setPtaFile.ldif
```

setPtaFile.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Configuration
changetype: modify
replace: ibm-slapdPtaEnabled
ibm-slapdPtaEnabled: true
```

3. **ibm-slapdPtaEnabled** 属性値に加えられた変更を適用するには、以下のように **idsldapexop** コマンドを実行します。

```
idsldapexop -h server.com -p port -D adminDN -w adminPWD -op readconfig ¥
-scope single cn=Configuration ibm-slapdPtaEnabled
```

4. サブツリーの項目に対してパススルー・インターフェースを構成するには、以下のように **idsldapmodify** コマンドを実行します。

```
idsldapmodify -h server.com -p port -D adminDN -w adminPWD ¥
-i setPtaGlobalCatlogFile.ldif
```

setPtaGlobalCatlogFile.ldif ファイルには、以下の項目が格納されています。

```
dn: cn=Passthrough Server1, cn=Passthrough Authentication, cn=Configuration
changetype: add
cn: Passthrough Server1
ibm-slapdPtaAttrMapping: uid $ userPrincipalName
ibm-slapdPtaBindDN: bind_DN
ibm-slapdPtabindPW: bind_PWD
ibm-slapdPtaSubtree: o=sample
ibm-slapdPtaSearchBase:
ibm-slapdPtaURL: ldap://hostname:3268
ibm-slapdPtaConnectionPoolSize: 6
ibm-slapdPtaResultTimeout: 100
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdPta
objectclass: ibm-slapdPtaExt
```

5. ディレクトリー・サーバーおよび管理サーバーを再始動します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
ibmslapd -I dsrdbm01 -n
ibmdiradm -I dsrdbm01
```

パススルー認証の拡張シナリオ:

ここではパススルー認証の拡張シナリオについて説明します。

シナリオ 6: 複数のパススルー認証サーバーの構成:

IBM Security Directory Server 内の指定されたユーザー・コンテナを、複数のパススルー・サーバーとマップすることができます。

このシナリオが機能するようにするには、IBM Security Directory Server バージョン 6.3.1.5 をインストールする必要があります。

パススルー認証の他のすべてのシナリオでは、IBM Security Directory Server 内の指定されたユーザー・コンテナは、いずれか 1 つのパススルー認証サーバーにマップされます。これは 1:1 マッピングです。複数のユーザー・コンテナをいずれか 1 つのパススルー認証サーバーにマップすることもできるため、N:1 マッピングの構成も可能です。

ただし、このシナリオでは、どのユーザー・コンテナを指定しても、複数のパススルー認証サーバーにマップすることができます。ここでは、1:N マッピングの構成が可能です。例えば、パススルー・サーバーが 2 つあるとします。これらいずれのサーバーについても、ユーザーは IBM Security Directory Server の `ou=users,o=sample` の下に保管されます。この場合、2 つのパススルー認証サーバーの構成は、以下に示すようなものになります。

```
dn: cn=ad1, cn=Passthrough Authentication, cn=Configuration
cn: ad1
ibm-slapdPtaAttrMapping: uid $ samAccountName
ibm-slapdPtaBindDN: cn=Administrator,ou=users,dc=ad1,dc=com
ibm-slapdPtabindPW: {AES256}SDHQJXZcNduBRxzW3nUsw==
ibm-slapdPtaConnectionPoolSize: 4
ibm-slapdPtaMigratePwd: false
ibm-slapdPtaSearchBase: ou=users,dc=ad1,dc=com
ibm-slapdPtaSubtree: ou=users,o=sample
ibm-slapdPtaURL: ldap://127.0.0.1:7389
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdPta
objectclass: ibm-slapdPtaExt
```

```
dn: cn=ad2, cn=Passthrough Authentication, cn=Configuration
cn: ad2
ibm-slapdPtaAttrMapping: uid $ samAccountName
ibm-slapdPtaBindDN: cn=Administrator,ou=users,dc=ad2,dc=com
ibm-slapdPtabindPW: {AES256}SDHQJXZcNduBRxzW3nUsw==
ibm-slapdPtaConnectionPoolSize: 4
ibm-slapdPtaMigratePwd: false
ibm-slapdPtaSearchBase: ou=users,dc=ad2,dc=com
ibm-slapdPtaSubtree: ou=users,o=sample
ibm-slapdPtaURL: ldap://127.0.0.1:4389
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdPta
objectclass: ibm-slapdPtaExt
```

このシナリオが機能するようにするには、以下の要件を満たす必要があります。

- `ibm-slapdPtaSubtree` の値が、両方のパススルー認証サーバーで同じである必要があります。
- ユーザー・コンテナ内のすべてのユーザーには、ユーザーの資格情報を保管するパススルー認証サーバーの ID が含まれている必要があります。
- サーバー ID は、補助オブジェクト・クラス `ptaServerInfo` および属性 `ptaServerId` を使用して保管する必要があります。
- 属性の値は、パススルー・サーバー構成の `CN` 属性の値と同じである必要があります。

例えば、ユーザー `uid=tbrown,ou=users,o=sample` はパススルー認証サーバー内に資格情報 `cn=ad1, cn=Passthrough Authentication, cn=Configuration` を持ち、ユーザー `uid=jdoe,ou=users,o=sample` はパススルー認証サーバー内に資格情報 `cn=ad2, cn=Passthrough Authentication, cn=Configuration` を持つと仮定します。ユーザー項目は、以下に示すように設定します。

```
dn: uid=tbrown,ou=users,o=sample
cn: Tom Brown
sn: Brown
uid: tbrown
ptaServerId: ad1
objectclass: inetOrgPerson
```

```
objectclass: ptaServerInfo
dn: uid=jdoe,ou=users,o=sample
cn: John Doe
sn: Doe
uid: jdoe
ptaServerId: ad2
objectclass: inetOrgPerson
objectclass: ptaServerInfo
```

このシナリオでは、ユーザーが IBM Security Directory Server にバインドすると、以下の処理が実行されます。

1. サーバーは、ユーザー項目に保管されている **ptaServerId** 値からパススルー認証サーバーを識別します。
2. 識別されたパススルー認証サーバー上で検索を行って、ユーザー DN を取得します。
3. 次に、パススルー認証サーバーで認証を行います。

したがって、このシナリオが正しく機能するようにするには、パススルー認証サーバー構成の CN 属性の値が、すべてのサーバーで固有である必要があります。構成内に CN 属性が複数存在する場合、ユーザー項目への格納には、最初の値のみを使用する必要があります。

オブジェクト・クラス ptaServerInfo および属性 ptaServerId のスキーマ定義をここで指定する必要があります。これらを IBM Security Directory Server にカスタム・オブジェクト・クラスおよびカスタム属性として追加する必要があります。

```
objectclasses=( ptaServerInfo-oid NAME 'ptaServerInfo'
DESC 'This auxiliary class has attributes used in the person entries
to store PTA server information.' SUP 'top' AUXILIARY MAY ( ptaServerId ) )
```

```
attributetypes=( ptaServerId-oid NAME 'ptaServerId'
DESC 'ID that uniquely identifies a PTA server where the actual user is
located, and where PTA needs to be performed' EQUALITY 2.5.13.2 SUBSTR
2.5.13.4
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE USAGE userApplications )
```

Web 管理ツールを使用したパススルー認証の構成

以下に示す指示により、Web 管理ツールを使用してパススルー認証を構成することができます。

このタスクについて

まだ行っていない場合は、Web 管理ツールのナビゲーション領域で「**サーバー管理**」カテゴリーの下にある「**セキュリティー・プロパティの管理**」を展開して、「**パススルー認証**」タブをクリックします。

このパネルで、以下を行うことができます。

- 「**パススルー認証を使用可能にする**」チェック・ボックスを選択またはクリアして、パススルー認証を使用可能または使用不可にする。
- サブツリーのパススルー項目をパススルー認証用に構成する。「**追加**」をクリックするとパススルー認証用サブツリーの構成ウィザードが表示されます。それを使用して、サブツリーのパススルー項目をパススルー認証用に構成できます。

- サブツリーの既存のパススルー項目をパススルー認証用に編集する。「編集」をクリックするとパススルー認証用サブツリーの構成ウィザードが表示されます。それを使用して、サブツリーの既存のパススルー項目をパススルー認証用に編集できます。
- パススルー認証用に構成されたサブツリーの既存のパススルー項目を削除する。これを行うには、「パススルー認証用に構成されたサブツリー」テーブルからサブツリーを選択して、「削除」ボタンをクリックします。
- パススルー認証用に構成されたサブツリーのパススルー項目の詳細を表示する。これを行うには、「パススルー認証用に構成されたサブツリー」テーブルからサブツリーを選択し、「アクションの選択」リストから「表示」を選択して「実行」をクリックします。
- 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして変更を保存し、「概要」パネルにナビゲートします。
 - 「適用」をクリックして変更内容を保存し、このパネルに残ります。
 - 「キャンセル」をクリックして変更内容を廃棄し、「概要」パネルにナビゲートします。

サブツリーのパススルー項目をパススルー認証用に構成するには、以下のステップを実行します。

手順

1. 「パススルー認証」パネルで、「追加」をクリックします。
2. 「サブツリー設定」パネルでは、以下のアクションを実行できます。
 - フィールドにサブツリー DN を入力し、「追加」ボタンをクリックしてサブツリー DN の保管用リストに追加する。
 - 「参照」ボタンをクリックし、「項目の参照」パネルから必要な行を選択して複数のサブツリー DN を入力する。
 - サブツリー DN を選択し、「除去」ボタンをクリックしてサブツリー DN 保管用のリストからサブツリー DN を除去する。
 - 「ホスト名」フィールドにパススルー・サーバーのホスト名を指定する。これは必須フィールドです。
 - 「ポート」フィールドにパススルー・サーバーのポート番号を指定する。これは必須フィールドです。
 - 「SSL 暗号化を使用可能にする」チェック・ボックスを選択して、パススルー・サーバーで SSL 暗号化を使用可能にする。
 - 「この directory server にユーザー・パスワードを移行」フィールドから値を選択して、パススルー・サーバーにより処理されたすべての成功したバインド要求についてユーザー・パスワードをローカル・ディレクトリーに保存するかどうかを指定する。このコントロールのデフォルト値は「False」です。
 - 「パススルー認証のためのパススルー・サーバーへの接続の数」フィールドに、パススルー・サーバー項目ごとに必要な接続の数を指定する。
 - 「パススルー認証のタイムアウト」フィールドにタイムアウト値を指定する。パススルー認証インターフェースは、ソケットからの結果をタイムアウト期間まで待ち、その後クライアント要求を戻します。

注:

- 「cn=< pass-through server >, cn=Passthrough Authentication, cn=Configuration」項目の属性「ibm-slapdPtaResultTimeout」は、このコントロールに関連付けられています。
 - タイムアウト値は、ミリ秒で指定します。このフィールドの上限は 60000 ミリ秒 (60 秒または 1 分) です。
 - 「次へ」をクリックします。
3. 属性マッピングを構成するため、以下のステップを実行します。
- a. 「属性マッピングを使用可能にする」チェック・ボックスを選択して、属性マッピングを使用可能にします。「属性マッピングを使用可能にする」チェック・ボックスを選択すると、「属性マッピング」パネルにある他のコントロールも使用可能になります。
 - b. 「パススルー・サーバーのバインド DN」フィールドには、パススルー・サーバーにバインドするためのバインド DN を入力します。
 - c. 「パススルー・サーバーのバインド・パスワード」フィールドに、パススルー・サーバーにバインドするためのバインド・パスワードを入力します。
 - d. 「検索ベース DN」フィールドに、項目検索対象のパススルー・サーバーの検索ベース DN を入力するか、「参照」ボタンをクリックして、パススルー・サーバーから既存の DN を選択できる「項目の参照」パネルを表示します。
 - e. 「この directory server の属性」リストから、パススルー・サーバーの属性にマップする必要がある属性を選択します。
 - f. 「パススルー directory server の属性」リストから、Security Directory Server 属性にマップする必要がある属性を選択します。
 - g. 完了したら、以下のステップのいずれかを行います。
 - 「戻る」をクリックして、「サブツリー設定」パネルにナビゲートします。
 - 「完了」をクリックして変更内容を保存し、「パススルー認証」にナビゲートします。
 - 「キャンセル」をクリックして変更を廃棄し、「パススルー認証」にナビゲートします。

パススルー認証のトラブルシューティング

ディレクトリー・サーバー環境での問題を識別して修正するには、パススルー認証トラブルシューティング情報を使用します。

- パススルー・サーバー内の、マッピングに影響を与える項目を変更する場合は、整合性を確保するために、認証サーバー内のマッピングを更新する必要があります。DN を更新して、パススルー・サーバーでの変更や名前変更を確実に認証サーバーに適用します。
- プロキシ・サーバーに対してパススルー認証を実行できるのは、パススルー・サブツリーがプロキシ・サーバー上の区画ベースの一部である場合のみです。

- プロキシ・サーバーに対する操作において予期しない結果が生じた場合は、プロキシ・バックエンド・サーバー上の `ibmslapd.log` ファイルでエラー・メッセージを確認してください。 `ibmslapd.log` ファイルで、以下のエラー・メッセージを検索します。

```
12/20/11 15:08:56 GLPSRV165E タイムアウトのために、パススルー認証が失敗しました。
12/20/11 15:08:56 ホスト 'ldapServer'、ポート '389'、URL ldap://ldapServer:389'
でパススルー認証検索が失敗しました。(12/20/11 15:08:56 Pass-through authentication
search failed on host 'ldapServer', port '389', url ldap://ldapServer:389')
12/20/11 15:08:56 GLPSRV163E 項目 'cn=user_21,o=sample' の 'ldap://ldapServer:389'
でパススルー・バインドが失敗しました。
```

操作がタイムアウトすると、予期しない結果が生じる場合があります。このような状況では、パススルー認証項目内の `cn=Passthrough Authentication`、`cn=Configuration` の下の `ibm-slapdPtaResultTimeout` 属性の値を増加させてください。タイムアウト値は、ミリ秒で指定します。この属性でサポートされている最大値は 60000 ミリ秒 (60 秒) です。

- 分散ディレクトリーでパススルー認証を構成する場合は、プロキシ・バックエンド・サーバー上の `ibmslapd.log` ファイルを確認して問題を解決します。
- パススルー認証を監査するには、認証サーバーで `ibm-auditPTABindInfo` 属性を `true` に設定します。 `ibm-auditPTABindInfo` 属性は、構成ファイルの `cn=Audit`、`cn=Log Management`、`cn=Configuration DN` 項目の下にあります。デフォルトでは、 `ibm-auditPTABindInfo` は `true` に設定されています。バインド操作または比較操作でパススルーの詳細を含めるための前提条件は、 `ibm-audit` 属性が `true` に設定されていることです。バインド操作および比較操作を監査する必要があります。次の例は、パススルー認証の監査ログ項目を示しています。

```
AuditV3--2011-06-21-11:17:39.813+00:00--V3 Bind--bindDN:
cn=XXX,ou=users,o=sample -client: 127.0.0.1:51900--connectionID: 10--received:
2011-06-21-11:17:39.811+00:00 --Success controlType: 1.3.6.1.4.1.42.2.27.8.5.1
criticality: false passthroughBindDN: uid=XXX,c=in,dc=com passthroughServer:
ldap://server:port passthroughBindRC: 0 AuditV3--2011-06-21-11:17:39.815+00:00--V3
Compare--bindDN: cn= XXX,ou=users,o=sample --client: 127.0.0.1:51900--
connectionID: 10--received: 2011-06-21-11:17:39.813+00:00 --Success controlType:
1.3.6.1.4.1.42.2.27.8.5.1 criticality: false passthroughBindDN: uid=XXX,c=in,dc=com
passthroughServer: ldap://server:port passthroughBindRC: 0。ここで、
```

`passthroughBindDN:` は、パススルー・サーバーでバインドを確認するのに使用された DN です

`passthroughServer:` は、パススルー・サーバーの LDAP URL です

`passthroughBindRC:` は、バインド操作でパススルー・サーバーから返された戻りコードです

管理グループ作成

ディレクトリー・サーバーの管理タスクを管理するには、固有の ID とパスワードを持つ管理グループ・メンバーを作成する必要があります。

管理グループ・メンバーを作成する場合は、以下の点について考慮する必要があります。

- 1 次管理者 ID は固有でなければなりません。
- 管理グループ・メンバー DN は、ディレクトリー・サーバー内で固有でなければなりません。

- ディレクトリー・サーバー管理者および管理グループ・メンバーの Kerberos または Digest-MD5 ID は固有でなければなりません。
- ディレクトリー・サーバーの複製サプライヤー DN 値は固有でなければなりません。つまり、ディレクトリー・サーバーの複製サプライヤー DN は、管理グループ・メンバー DN または 1 次管理者 DN のいずれとも一致してはいけません。

1 次管理者は、以下の項目にアーカイブ・ログ属性が設定されていることを確認する必要があります。

- cn=Audit, cn=Log Management, cn=Configuration
- cn=Admin Audit, cn=Log Management, cn=Configuration

項目にアーカイブ属性を設定することにより、ローカル管理者メンバーがデフォルトのアーカイブ・ログ設定を変更してしまう危険を回避できます。デフォルト設定を変更すると、監査ログのアーカイブに影響を与えます。

デフォルトのログ設定を更新するには、以下の属性を更新します。

- ibm-slapdLogMaxArchives
- ibm-slapdLogSizeThreshold
- ibm-slapdLogArchivePath

管理役割

この機能により、管理役割を構成することができます。

管理グループ・メンバーを構成する際に、1 次管理者はメンバーに管理役割を明示的に割り当てる必要があります。管理メンバーに割り当て可能な役割は以下のとおりです。

- 監査管理者 (AuditAdmin) - 監査管理役割が割り当てられている管理グループのメンバーは、以下のログと設定に制限なしでアクセスすることができます。
 - 監査ログ
 - 管理監査ログ
 - 他のすべてのサーバー・ログ
 - 監査ログ設定 (cn=Audit, cn=Log Management, cn=Configuration)
 - 管理監査ログ設定 (cn=Admin Audit, cn=Log Management, cn=Configuration)
 - デフォルト・ログ管理設定 (cn=Default, cn=Log Management, cn=Configuration)
- ディレクトリー・データ管理者 (DirDataAdmin) – この役割が割り当てられている管理グループ・メンバーは、RDBM バックエンド内のすべての項目に制限なしでアクセスすることができます。ただし、RDBM 項目のパスワード属性の設定に関しては、メンバーは、通常のパスワード・ポリシー規則に従う必要があります。
- 管理者なし (NoAdmin) - 1 次管理者が構成ファイル・ユーザーに対し「管理者なし」の役割を割り当てると、そのユーザーには何の管理特権もなくなります。1 次管理者は、この役割を定義することで、管理グループ・メンバーのすべての管理特権を取り消すことができます。
- パスワード管理者 (PasswordAdmin) – パスワード管理者役割が割り当てられている管理グループのメンバーには、他のユーザーのアカウントをアンロックしたり、RDBM バックエンド内のユーザーのパスワードを変更したりする権限があります。ただし、グローバル管理グループ・メンバー・アカウントのパスワードを

変更する権限はありません。また、このようなメンバーは、サーバーに設定されているパスワード・ポリシーの制約による拘束を受けません。RDBM バックエンド内の項目のユーザー・パスワード・フィールドの追加および削除もできますが、構成ファイルに定義されたユーザーに変更を加えることはできません。この役割を割り当てられたユーザーが行ったパスワード変更は、ACL による制御の対象にはなりません。ただし、ユーザーが自分自身のパスワードを変更する場合は、通常ユーザー・パスワード・ポリシー規則が適用されます。

- 複製管理者 (ReplicationAdmin) - 「複製管理者」の役割を割り当てられた管理グループのメンバーは、複製トポロジー・オブジェクトを更新する権限を持ちます。この役割のメンバーが行った変更は、ACL または他のどの構成ファイル設定による制御の対象にもなりません。
- スキーマ管理者 (SchemaAdmin) - 「スキーマ管理者」の役割を割り当てられた管理グループのメンバーは、スキーマ・バックエンドのみに対する無制限のアクセス権限を持ちます。
- サーバー構成グループ・メンバー (ServerConfigGroupMember) - 「サーバー構成グループ・メンバー」の役割を割り当てられた管理者グループのメンバーは、構成バックエンドに対する制限付きの更新アクセス権限を持ちます。つまり、サーバー構成グループ・メンバーは、cn=Configuration 下の項目に対して制限付きの更新アクセス権限を持つということです。この役割のユーザーは、特定のタスク (特に、他のローカル管理者および 1 次管理者に関連するタスクまたはセキュリティー関連のタスク) を実行することはできません。例えば、1 次管理者および管理グループの資格情報を変更したり、管理グループのメンバーを追加したり削除したりすることはできません。また、この役割のユーザーは、cn=AdminGroup, cn=Configuration 下の管理グループ・メンバー項目の DN、パスワード、Kerberos ID、または Digest-MD5 ID を変更することもできません。自分自身の DN、Kerberos ID、または Digest-MD5 ID を変更する権限もありません。このユーザーには、管理グループ・メンバーに割り当てられている管理役割の追加、削除、または変更権限はありません。ただし、自分自身のパスワードは変更できます。さらに、この役割のユーザーは、他の管理グループ・メンバーまたは 1 次管理者のパスワードを表示することはできず、監査ログ設定および管理監査ログ設定 (cn=Audit, cn=Log Management, cn=Configuration 項目および cn=Admin Audit, cn=Log Management, cn=Configuration 項目全体) を追加、削除、または変更する権限も、監査ログおよび管理監査ログを消去する権限もありません。ただし、デフォルトのログ設定 (cn=Default, cn=Log Management, cn=Configuration 項目) の変更およびその他のすべてのサーバー・ログの消去は許可されています。また、この役割のユーザーは cn=Kerberos, cn=Configuration 項目または cn=Digest, cn=Configuration 項目を追加または削除することはできません。ただし、これらの項目下のすべての属性の検索はできます。このユーザーはこれらの項目の下位にあるすべての属性を変更できます。ただし、Kerberos および Digest-MD5 のルート・アドミニストレーター・バインド属性は除きます。このユーザーは、cn=Configuration エントリー下の ibm-slapdAdminDN、ibm-slapdAdminGroupEnabled、ibm-slapdAdminPW の各属性を検索または変更することはできません。このユーザーは動的構成変更を発行できます。
- サーバー始動/停止管理者 (ServerStartStopAdmin) - 「サーバー始動/停止管理者」の役割を割り当てられた管理グループのメンバーは、サーバーおよび管理者デーモンを開始または停止する権限を与えられます。

注: 分散ディレクトリー環境で、データベース・バックエンドの管理権限を委任する方法については、436 ページの『グローバル管理グループ』を参照してください。

以下の表は、管理グループ・メンバーが発行できる各種の拡張操作の相互参照表です。

表 31. 各種の拡張操作を出す権限を持つ管理役割

拡張操作	監査管理	ディレクトリー・データ管理者	複製管理者	スキーマ管理者	サーバー構成グループのメンバー	サーバー始動/停止管理者	パスワード管理者	管理者なし
TLS 開始 - この操作は、Transport Layer Security の始動を要求するために使用します。OID = 1.3.6.1.4.1.1466.20037	はい	はい	はい	はい	はい	はい	はい	はい
イベント登録 - この操作は、SecureWay V3.2 Event サポートへのイベントの登録を要求するために使用します。OID = 1.3.18.0.2.12.1	はい	はい	はい	はい	はい	はい	はい	はい
イベントの登録抹消 - この操作は、イベント登録要求を使用して登録したイベントの登録抹消を要求するために使用します。OID = 1.3.18.0.2.12.3	はい	はい	はい	はい	はい	はい	はい	はい
トランザクション開始 - この操作は、SecureWay V3.2 のトランザクション・コンテキストの開始を要求するために使用します。OID = 1.3.18.0.2.12.5	はい	はい	はい	はい	はい	はい	はい	はい
トランザクション終了 - この操作は、SecureWay V3.2 のトランザクション・コンテキストの終了 (コミット/ロールバック) を要求するために使用します。OID = 1.3.18.0.2.12.6	はい	はい	はい	はい	はい	はい	はい	はい
トレースを動的に使用可能/使用不可に設定します。OID = 1.3.18.0.2.32.14	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
カスケード制御複製 - この操作では、要求されたアクションを発行先のサーバー上で実行し、この呼び出しを複製トポロジーでこの操作の下位に置かれているすべてのコンシューマーに継続的に転送します。OID = 1.3.18.0.2.12.15	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
制御複製 - この操作は、サブライヤーによる即時の複製、複製の中断、複製の再開のいずれかを適用するときに使用します。この操作は、複製の合意に対する更新をクライアントが許可されている場合にのみ許可されます。OID = 1.3.18.0.2.12.16	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
制御複製キュー - この操作では、指定の合意の項目に「複製済み」とマークが付けられません。この操作は、複製の合意に対する更新をクライアントが許可されている場合にのみ許可されます。OID = 1.3.18.0.2.12.17	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
サーバーの静止または静止解除 - この操作では、サブツリーをクライアント更新を受け入れない状態にします (またはこの状態を終了します)。ただし、サーバー管理制御を持つディレクトリー管理者として認証されたクライアントからの更新は除きます。OID = 1.3.18.0.2.12.19	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

表 31. 各種の拡張操作を出す権限を持つ管理役割 (続き)

拡張操作	監査管理	ディレクトリ ー・データ管 理者	複製管理者	スキーマ管理者	サーバー構成グループ のメンバー	サーバー始動/ 停止管理者	パスワード管 理者	管理者なし
ログ消去要求 - この操作は、ログ・ファイルのクリアを要求するために使用します。OID = 1.3.18.0.2.12.20	はい	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ
行取得要求 - この操作は、ログ・ファイルからの行の取得を要求するために使用します。OID = 1.3.18.0.2.12.22	はい	はい	はい	はい	はい	はい	はい	いいえ
行数要求 - この操作は、ログ・ファイルの行数を要求するために使用します。OID = 1.3.18.0.2.12.24	はい	はい	はい	はい	はい	はい	はい	いいえ
サーバー始動/停止要求 - この操作は、LDAP サーバーの始動、停止、または再始動を要求するために使用します。OID = 1.3.18.0.2.12.26	いいえ	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ
構成更新要求 - この操作は、IBM Security Directory Server のサーバー構成の更新を要求するために使用します。OID = 1.3.18.0.2.12.28	はい	いいえ	はい	いいえ	はい	いいえ	いいえ	いいえ
DN 正規化要求 - この操作は、1 つの DN または一連の DN の正規化を要求するために使用します。OID = 1.3.18.0.2.12.30	はい	はい	はい	はい	はい	はい	はい	はい
接続強制終了要求 - この操作は、サーバーの接続の停止を要求するために使用します。この要求は、すべての接続を強制終了するものでも、バインド済み DN、IP、特定の IP からバインドされた DN のいずれかによる接続を強制終了するものでもかまいません。OID = 1.3.18.0.2.12.35	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
ユーザー・タイプ要求 - この操作は、バインドされているユーザーのユーザー・タイプの取得を要求するために使用します。OID = 1.3.18.0.2.12.37	はい	はい	はい	はい	はい	はい	はい	はい
サーバー・トレースの制御 - この操作は、IBM Security Directory Server でのトレースの活動化または非活動化を要求するために使用します。OID = 1.3.18.0.2.12.40	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
グループ評価 - この操作は、分散ディレクトリ環境で、特定の DN をメンバーとして持つすべてのグループを判別するために使用します。OID = 1.3.18.0.2.12.50	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
トポロジー複製 - この操作は、特定の複製コンテキストのトポロジー (そのコンテキストの複製の合意など) を定義するオブジェクトを複製するために使用します。コンテキストの複製グループ項目に対する更新権を持つユーザーなら、誰でもこの拡張操作を発行することができます。OID = 1.3.18.0.2.12.54	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

表 31. 各種の拡張操作を出す権限を持つ管理役割 (続き)

拡張操作	監査管理	ディレクトリー・データ管理者	複製管理者	スキーマ管理者	サーバー構成グループのメンバー	サーバー始動/停止管理者	パスワード管理者	管理者なし
イベント更新 - この操作は、イベント通知構成の再初期化を要求するために使用します (この操作を開始できるのはサーバーのみであり、ユーザーは開始できません)。OID = 1.3.18.0.2.12.31	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
ログ・アクセス更新 - この操作は、ログ・アクセス・プラグイン構成の再初期化を要求するために使用します (この操作を開始できるのはサーバーのみであり、ユーザーは開始できません)。OID = 1.3.18.0.2.12.32	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
固有属性 - この操作は、属性の重複する値を要求するために使用します。OID = 1.3.18.0.2.12.44	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
アカウント状況 - この操作は、アカウントがパスワード・ポリシーでロックされているかどうかを判別するために使用します。OID = 1.3.18.0.2.12.58	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
項目探索 - この操作は、特定の DN セットの詳細を見つけるために使用します。OID = 1.3.18.0.2.12.71	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
プロキシ役割の再開 - この操作は、バックエンド・サーバーの役割の再開を要求するために使用します。OID = 1.3.18.0.2.12.65	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
属性タイプの取得 - この操作は、属性タイプを要求するために使用します。OID = 1.3.18.0.2.12.46	いいえ	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ
ServerBackupRestore - この操作は、管理サーバーでディレクトリー・サーバーのデータおよび構成のバックアップを実行するか、既存のバックアップからディレクトリー・サーバーのデータおよび構成を復元することを要求するために使用します。OID = 1.3.18.0.2.12.81	いいえ	はい	いいえ	はい	はい	はい	いいえ	いいえ

以下の表は、異なる管理グループ・メンバーがアクセスを許可される各種オブジェクトの相互参照表です。

表 32. 各種オブジェクトへのアクセス用に管理役割に割り当てる許可

	監査設定/監査ログ		RDBM バックエンド		複製オブジェクト		スキーマ・バックエンド		構成バックエンド		プロキシ・バックエンド	サーバー始動/停止
	読み取り	書き込み	読み取り	書き込み	読み取り	書き込み	読み取り	書き込み	読み取り	書き込み		
監査管理者	はい	はい	いいえ**	いいえ	いいえ**	いいえ	はい	いいえ	はい	いいえ	注 1	いいえ
ディレクトリー・データ管理者	いいえ	いいえ	はい	はい	はい	はい	はい	いいえ	はい	いいえ	注 1	いいえ
複製管理者	いいえ	いいえ	いいえ**	いいえ**	はい	はい	はい	いいえ	はい	いいえ	注 1	いいえ
スキーマ管理者	いいえ	いいえ	いいえ**	いいえ	いいえ**	いいえ	はい	はい	はい	いいえ	注 1	いいえ
サーバー構成グループのメンバー	はい	いいえ	いいえ**	いいえ	いいえ**	いいえ	はい	いいえ	はい	はい*	注 1	いいえ
サーバー始動/停止管理者	いいえ	いいえ	いいえ**	いいえ	いいえ**	いいえ	はい	いいえ	はい	いいえ	注 1	はい
パスワード管理者	いいえ	いいえ	いいえ**	はい**	いいえ**	いいえ	はい	いいえ	はい	いいえ	注 1	いいえ
管理者なし	いいえ	いいえ	いいえ**	いいえ	いいえ**	いいえ	はい	いいえ	はい	いいえ	注 1	いいえ

- * - サーバー構成グループ・メンバーは、構成バックエンドに対する制限付きの更新アクセス権限を持ちます。
- ** - これらのオブジェクトに対するアクセス権限では、管理役割が提供する特別な権限はなく、ユーザーは通常の ACL 評価を通じてアクセスできます。
- 注 1 - プロキシでは、管理役割を持つ管理グループ・メンバーを匿名として取り扱い、それに対応するアクセス規則を適用します。

管理グループの使用可能化および使用不可化:

この操作を実行するには、IBM Security Directory Server 管理者である必要があります。

このタスクについて

注: このタスクおよびこの後の「管理グループの管理」タスクでは、管理グループのメンバーに対しては操作ボタンが使用不可になっています。管理グループのメンバーが表示できるのは、「管理グループの管理」パネルの「管理グループ・メンバー」テーブルのみです。

Web 管理の使用:

ここで説明する手順に従うことにより、Web 管理ツールのコマンドを使用して同じ操作を実行することができます。

このタスクについて

ナビゲーション領域で「サーバー管理」カテゴリを展開します。「管理グループの管理」をクリックします。

1. 管理グループを使用可能または使用不可にするには、「管理グループの使用可能化」の隣にあるチェック・ボックスをクリックします。このチェック・ボックスにチェック・マークを付けると、管理グループが使用可能になります。
2. 「OK」をクリックします。

注: 管理グループを使用不可にした場合でも、ログインしているメンバーは、再バインドを要求されるまで管理操作を継続できます。すでにバインドされている管理グループ・メンバーによる追加の操作を停止するには、アンバインド操作を実行します。詳細については、111 ページの『サーバー接続の管理』を参照してください。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、同じ操作を実行できます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Configuration
changetype: modify
replace: ibm-slapiAdminGroupEnabled
#specify TRUE to enable or FALSE to disable the administrative group
#TRUE has been preselected for you.
```

```
ibm-slapedAdminGroupEnabled: TRUE
objectclass: top
objectclass: ibm-slapedConfigEntry
objectclass: ibm-slapedTop
```

設定を動的に更新するには、以下の **idsldapexop** コマンドを発行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readconfig -scope single
cn=Configuration ibm-slapedAdminGroupEnabled
```

管理グループに対するメンバーの追加:

この操作を実行するには、IBM Security Directory Server 管理者である必要があります。

このタスクについて

Web 管理の使用:

以下に示す手順を使用することで、Web 管理ツールを使用して管理グループにメンバーを追加できます。

このタスクについて

管理グループにメンバーを追加するには、ナビゲーション領域で「サーバー管理」カテゴリを展開し、「管理グループの管理」をクリックします。次に、「管理グループの管理」で「追加」をクリックします。

「管理グループ・メンバーの追加」パネルで、以下の手順を実行します。

1. メンバーの管理者 DN を入力します (これは有効な DN 構文にする必要があります)。
2. メンバーのパスワードを入力します。管理者のパスワード・セキュリティー制限の詳細については、247 ページの『管理パスワードおよびロックアウト・ポリシーの設定』を参照してください。
3. 確認のため、メンバーのパスワードを再度入力します。
4. 必要に応じて、メンバーの「Digest-MD5 ユーザー名」を入力します。
5. オプションで、メンバーの「Kerberos ID」を入力します。Kerberos ID は `ibm-kn` または `ibm-KerberosName` のいずれかのフォーマットにする必要があります。値では大/小文字は区別されません。例えば、`ibm-kn=root@TEST.AUSTIN.IBM.COM` は `ibm-kn=ROOT@TEST.AUSTIN.IBM.COM` と同等です。**注:** このフィールドは、AIX プラットフォームおよび Windows プラットフォームの場合にのみ使用できます。kerberos でサポートされる機能 OID (1.3.18.0.2.32.30) がサーバー上で検出された場合、このフィールドは表示専用となります。
6. 「管理役割」セクションの下で、「管理グループ・メンバーの役割を定義する」チェック・ボックスを選択します。
7. 「使用可能な管理役割」ボックスから使用可能な管理役割を選択し、「追加」をクリックします。
8. 「OK」をクリックします。

注: Digest-MD5 ユーザー名には、大文字小文字の区別があります。管理グループに追加するメンバーごとにこの手順を繰り返します。

「管理グループ・メンバー」リスト・ボックスには、管理者 DN、Digest-MD5 ユーザー名 (指定した場合)、および Kerberos ID (指定した場合) が表示されます。

注: Kerberos サポートが使用できるプラットフォームは、AIX および Windows のみです。kerberos でサポートされる機能 OID (1.3.18.0.2.32.30) がサーバー上で検出された場合、Kerberos ID 列は、「管理グループ・メンバー」リスト・ボックスにのみ表示されます。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、管理グループにメンバーを追加できます。

このタスクについて

```
idsldapadd -D <adminDN> -w<adminPW> -i<filename>
```

where <filename> contains:

```
dn: cn=AdminGroup, cn=Configuration
cn: AdminGroup
objectclass: top
objectclass: container

dn: cn=admin1, cn=AdminGroup, cn=Configuration
cn: admin1
ibm-slapdAdminDN: <memberDN>
ibm-slapdAdminPW: <password>
ibm-slapdAdminRole: <role value>
ibm-slapdAdminRole: <role value2>
#ibm-slapdKrbAdminDN and ibm-slapdDigestAdminUser are optional attributes.
ibm-slapdKrbAdminDN: <KerberosID>
ibm-slapdDigestAdminUser: <DigestID>
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdAdminGroupMember
```

注:

- すでに管理グループにメンバーを作成済みの場合は、最初の項目を省略します。
- `ibm-slapdAdminRole` 属性の複数インスタンスが異なる役割値を使用して指定されていて、それらの役割値の 1 つが `NoAdmin` である場合は、他のすべての役割値は無視され、`NoAdmin` の役割を持つ管理グループ・メンバーが追加されます。

設定を動的に更新するには、以下の `idsldapexop` コマンドを発行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readconfig -scope subtree
cn=AdminGroup,cn=Configuration
```

管理グループ・メンバーの変更:

この操作を実行するには、IBM Security Directory Server 管理者である必要があります。

このタスクについて

Web 管理の使用:

以下に示すステップにより、管理グループ・メンバーの情報を変更することができます。

このタスクについて

管理グループ・メンバーの情報を変更するには、ナビゲーション領域で「サーバー管理」カテゴリーを展開し、「管理グループの管理」をクリックします。「管理グループの管理」パネルで、以下の手順を実行します。

1. 情報の変更対象メンバーを選択します。
2. 「編集」をクリックします。
3. メンバーの管理者 DN を変更します (これは有効な DN 構文にする必要があります)。
4. メンバーのパスワードを変更します。
5. 確認のため、メンバーのパスワードを再度入力します。
6. メンバーの **Kerberos ID** を入力または変更します。Kerberos ID は `ibm-kn` または `ibm-KerberosName` のいずれかのフォーマットにする必要があります。この値に大文字小文字の区別はありません。例えば、`ibm-kn=root@TEST.AUSTIN.IBM.COM` と `ibm-kn=ROOT@TEST.AUSTIN.IBM.COM` は同じ意味を持ちます。

注: このフィールドが使用できるプラットフォームは、AIX および Windows のみです。kerberos でサポートされる機能 OID (1.3.18.0.2.32.30) がサーバー上で検出された場合、このフィールドは表示専用となります。

7. メンバーの「**Digest-MD5 ユーザー名**」を入力します。Digest-MD5 ユーザー名には、大文字小文字の区別があります。
8. 「OK」をクリックします。

管理グループで変更するメンバーごとにこの手順を繰り返します。

注: 管理グループのメンバーである場合、パスワードは「ユーザー・プロパティ」->「パスワードの変更」パネルを使用して変更できます。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、管理グループ・メンバーを変更することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=admin1, cn=AdminGroup, cn=Configuration
cn: admin1
changetype: modify
replace: ibm-slapdAdminDN
ibm-slapdAdminDN: cn=<memberDN>
-
replace: ibm-slapdAdminPW
ibm-slapdAdminPW: <password>
-
replace: ibm-slapdKrbAdminDN
ibm-slapdKrbAdminDN: <KerberosID>
-
replace: ibm-slapdDigestAdminUser
ibm-slapdDigestAdminUser: <DigestID>
-
replace: ibm-slapdAdminRole
ibm-slapdAdminRole: <role value>
```

設定を動的に更新するには、以下の **idsldapexop** コマンドを発行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readconfig -scope subtree
cn=AdminGroup,cn=Configuration
```

管理グループからのメンバーの除去:

この操作を実行するには、IBM Security Directory Server 管理者である必要があります。

このタスクについて

サーバー管理の使用:

以下に示す指示により、「管理グループの管理」パネルで管理グループのメンバーを除去することができます。

このタスクについて

1. 除去するメンバーを選択します。
2. 「削除」をクリックします。
3. 除去の確認を求められます。
4. メンバーを削除する場合は「OK」をクリックします。変更を行わずに「管理グループの管理」パネルに戻る場合は「キャンセル」をクリックします。

管理グループから除去するメンバーごとにこの手順を繰り返します。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行で使用することにより、同じ操作を実行できます。

このタスクについて

```
idsldapdelete -D <adminDN> -w<adminPW> -i<filename>
```

where <filename> contains:

```
#list additional DNs here, one per line:
cn=admin1, cn=AdminGroup, cn=Configuration
```

複数のメンバーを除去するには、DN を列挙します。各 DN は別々の行に記述する必要があります。

注: 管理グループ・メンバーのバインド DN ではなく、管理グループ・メンバーを保持している項目の DN を指定してください。

設定を動的に更新するには、以下の **idsldapexop** コマンドを発行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readconfig -scope subtree
cn=AdminGroup,cn=Configuration
```

参照

参照を使用すると、サーバーはクライアントに対して、追加のディレクトリー・サーバーを参照するよう指示することができます。参照は、代替 LDAP サーバーの URL を指定します。この代替サーバーは、現在の LDAP サーバーのいずれのサブツリーでも検索されないオブジェクトに対する要求を処理します。

注:

- プロキシ環境では、プロキシ・サーバーは参照を返しません。参照オブジェクトは、クライアントが参照を追跡しないよう、通常のディレクトリー項目として返されます。
- プロキシ環境では、参照は推奨されません。

デフォルト参照を使用すると、以下のサーバーを指し示すことができます。

- (階層内における) このサーバーの直接の親
- 階層内の最上位サーバーなどの、「より多くの情報を持つ」サーバー
- ネーム・スペースの非結合部分を実行する可能性がある、「より多くの情報を持つ」サーバー

参照を使用して、以下のタスクを実行できます。

- 複数のサーバーにネーム・スペース情報を配布する。
- 相互に関連する一連のサーバー内のどこにデータがあるのかについて情報を提供する。
- 該当するサーバーにクライアント要求を送送する。

注: IBM Security Directory Server 6.0 以降がサポートするすべてのサーバーおよびクライアントは、IPv6 形式および IPv4 形式をサポートします。この 2 つの形式については、649 ページの『付録 E. IPv6 サポート』を参照してください。

参照を使用する利点として、以下のタスクを実行できる場合があります。

- 処理のオーバーヘッドを分散し、基本的なロード・バランシングを行う
- 組織の境界に沿ってデータの管理を分散する
- 組織独自の境界を超えて、広範な相互接続の可能性を提供する。

注: Linux、Solaris、および HP-UX プラットフォームでは、参照を追跡しているときにクライアントがハングした場合、システム環境で環境変数 LDAP_LOCK_REC が設定されているようにします。特定の値を指定する必要はありません。

```
set LDAP_LOCK_REC=anyvalue
```

他の LDAP ディレクトリーへの参照の設定

参照オブジェクト・クラスおよび referral 属性を使用することで、他の LDAP ディレクトリーへの参照を持つ項目を LDAP ディレクトリー内に作成することができます。

参照を使用することで、サーバーを複数関連付けることも可能です。その例を示します。

参照オブジェクト・クラスおよび ref 属性

参照オブジェクト・クラスおよび ref 属性は、分散されたネーム・レゾリューションを容易に行ったり、複数のサーバーに渡って検索を行ったりするために使用されます。

ref 属性は、参照するサーバー内で指定する項目に出現します。ref 属性の値は、参照されるサーバー内で保持されている項目を指します。

項目の作成:

参照の 1 つのセットアップは、管理するサブツリーに基づいて、サーバーを 1 つの階層に構成するために使用されます。次に、上位の (階層のルートに近い) 情報を保持するサーバーからのフォワード参照を提供し、その親サーバーを指すようデフォルト参照を設定します。

以下の構成の例では、ref 属性の使用方法が示されています。

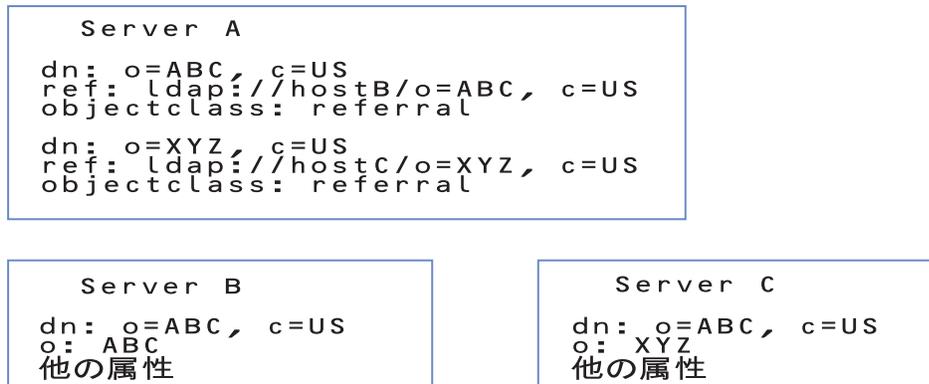


図 3. referral 属性の使用例

この例で、Server A は o=ABC, c=US および o=XYZ, c=US という 2 つの項目への参照を保持しています。o=ABC, c=US 項目に関して、Server A は Server B への参照を保持しています。o=XYZ, c=US 項目に関して、Server A は Server C への参照を保持しています。

サーバーと参照との関連付け:

参照経由でサーバーを関連付けるには、参照オブジェクトを使用して、従属参照用の他のサーバーを指し示します。また、別の場所 (通常は親サーバー) を指すデフォルト参照を定義する必要があります。

注: 参照オブジェクトは、コマンド行から **-M** オプションを指定することで表示できます。コマンド行ユーティリティについて詳しくは、「*IBM Security Directory Server Version 6.3.1 Command Reference*」を参照してください。

他のサーバーへの指示:

従属参照 (すなわち、このサーバーの下のネーム・スペースにあり、このサーバーが直接サービスを提供しない部分) 用として、他のサーバーを指し示す参照オブジェクトを使用します。

参照オブジェクトは他のオブジェクトと同様に、バックエンド (DB2) に入ります。参照オブジェクトは、以下の属性で構成されています。

dn: 識別名を指定します。これは、参照されるサーバーによってサービス提供されるネーム・スペースの一部です。

objectclass:

オブジェクト・クラス referral の値を指定します。

ref: サーバーの LDAP Web アドレスを指定します。この Web アドレスは、`ldap:// identifier, thehostname:port`、および DN で構成されています。ID には、ホスト名ストリング、または TCP/IP アドレスのどちらでも指定することができます。`hostname:port` と区切るため、DN の前にはスラッシュ (/) が必要です。また、この DN は、参照オブジェクトの DN と同じである必要があります。参照属性値に指定する DN と参照オブジェクトの DN は、一致する必要があります。通常は、参照サーバーが保持しているネーミング・コンテキストでのネーミング・コンテキストの項目か、その下でのネーミング・コンテキストの項目です。

```
dn:o=sample
objectclass:referral
ref:ldap://9.130.25.51:389/o=sample
```

分散ネーム・スペース・バインディング

IBM Security Directory Server アプリケーションがバインド DN と資格情報を変更するよう設計されているのでない場合、検索時には、元のサーバーにバインドまたはログインするのに使用されたものと同じ DN が使用されて参照先のサーバーにバインドします。

両方のサーバーにバインドして、参照を追跡できるようにするには、同じ DN に対して正しいアクセスをセットアップする必要があります。詳細については、22 ページの『「Web 管理ツール」によるディレクトリー・サーバーへのログオン』を参照してください。

参照を使用したネーム・スペース分散の例

参照を使用してネーム・スペースを分散するには、ネーム・スペース階層の計画を策定し、複数のサーバーをセットアップし、参照オブジェクトをセットアップする必要があります。

参照を使用してネーム・スペースを分散するステップを以下に示します。

1. ネーム・スペース階層を計画します。

```
country - US
company - IBM, Lotus
organizationalUnit - IBM Austin, IBM Endicott, IBM HQ
```

2. 複数のサーバーをセットアップします。それぞれのサーバーには、ネーム・スペースの一部を含めます。

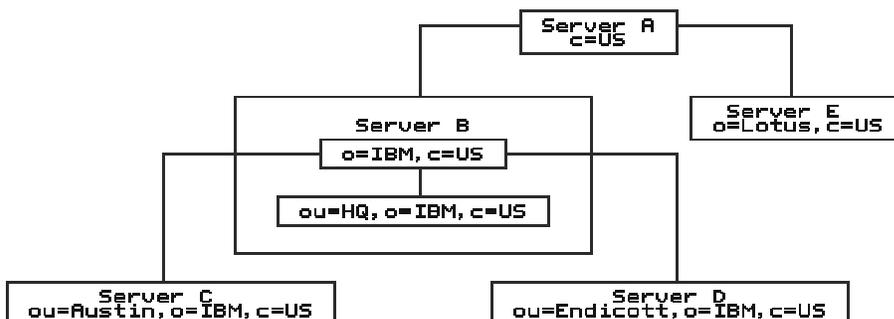


図4. サーバーのセットアップ

サーバーの説明を以下に示します。

Server A

米国内の他のサーバーを見つけるために使用されるサーバー。他の知識を持たないクライアントでも、最初にここにアクセスして、米国内の別のユーザーの情報を見つけることができます。

Server B

米国内の IBM に関するすべてのデータのハブ。すべての HQ 情報を直接保持しています。また、他の IBM データの場所についても、そのすべての情報 (参照) を保持しています。

Server C

IBM オースティンに関するすべての情報を保持しています。

Server D

IBM エンディコットに関するすべての情報を保持しています。

Server E

Lotus® に関するすべての情報を保持しています。

3. 他のサーバーの子孫を指すように参照オブジェクトをセットアップします。

```
dn: o=IBM, c=US
objectClass: referral
ref: ldap://ibm.com:389/o=IBM, c=US
dn: o=Lotus, c=US
objectClass: referral
ref: ldap://lotus.com:389/o=Lotus, c=US
```

← Server B へのポインター

← Server E へのポインター

図5. Server A データベース (LDIF 入力)

サーバーは、デフォルト参照を定義することもできます。デフォルト参照は、ネーム・スペース内のそれらのサーバーの下にはない情報を得ることを目的として、「より多くの情報を持つ」サーバーを指すために使用されます。

注: デフォルト参照 LDAP Web アドレスには、DN 部分は含まれません。

以下は、同じ 5 つのサーバーの配置です。上位参照用に使用されるデフォルト参照だけではなく、データベース内の参照オブジェクトも示しています。



図 6. 参照の例の要約

デフォルト参照の作成

デフォルト参照を作成および除去する場合、Web 管理ツールを使用することをお勧めします。

このタスクについて

Web 管理の使用

以下に示す指示により、Web 管理ツールを使用してデフォルト参照を作成したり除去したりすることができます。

このタスクについて

1. まだ行っていない場合は、Web 管理ツールを使用してマスター・サーバーへログオンします。
2. 「オブジェクト・クラスの選択」パネルの「構造化オブジェクト・クラス」リストから参照オブジェクト・クラスを選択して、参照項目を追加します。詳細については、526 ページの『項目の追加』を参照してください。
3. 「必須属性」タブで、「参照の管理」をクリックします。
4. 「参照の管理」パネルで「追加」をクリックして、「参照の追加」パネルを表示します。

注: 管理参照の場合、属性およびフィルターに関連するフィールドは表示されません。管理参照を作成するには、「サーバー管理」カテゴリの「サーバー・プロパティの管理」パネルで参照を追加します。

5. 「サーバー・ホスト名:ポート」ドロップダウン・リストから LDAP サーバーおよびポートを選択するか、サーバーのホスト名とポート番号を `hostname:port` の形式でフィールドに入力します。
 6. 参照先がセキュア (SSL) サーバーの場合には、「SSL の使用」を選択します。
 7. ターゲット・サーバーのディレクトリー情報ツリーに基本 DN を入力します。例えば、`ou=austin,o=sample` です。
 8. 参照 URL に組み込む属性を選択し、「追加」をクリックします。参照 URL から属性を除去するには、「選択された属性」フィールドで属性を強調表示し、「除去」をクリックします。
 9. 参照検索スコープを選択します。
 - 選択したオブジェクトの中だけで検索する場合は、「オブジェクト」を選択します。
 - 選択したオブジェクトの直接の子の範囲内のみで検索する場合は、「単一レベル」を選択します。
 - 選択した項目のすべての子孫を検索する場合は、「サブツリー」を選択します。
 - スコープを指定しない場合は、「なし」を選択します。
 10. 検索フィルターを指定します。詳細については、542 ページの『検索フィルター』を参照してください。
 11. 「OK」をクリックします。
 12. 追加する参照ごとに、上記のステップを繰り返します。
 13. 完了したら、「必須属性」タブで「次へ」をクリックします。
 14. 「オプションの属性」タブで、他の属性の値を必要に応じて入力します。
 15. 「完了」をクリックすると、項目が作成されます。
- 変更した内容を有効にするには、サーバーを再始動する必要があります。

コマンド・ラインの使用

以下に記載されている情報およびコマンドを使用して、別のサーバー上のディレクトリーを参照するデフォルト参照を定義します。

このタスクについて

注: デフォルト参照 LDAP URL には、DN 部分は含まれません。ldap:// ID と hostname:port のみが含まれています。

以下に例を示します。

注: この例は、ポート 389 を使用するローカル LDAP サーバーの例です。

```
idsldapadd -D <adminDN> -w <adminpw> -i <filename>
```

where <filename> contains:

```
# referral
dn: cn=Referral, cn=Configuration
cn: Referral
ibm-slapdReferral: ldap://<additional hostname:port>/<baseDN>?<attributes>?
<scope>?<filter>
ibm-slapdReferral: ldap://<additional hostname:port>/<baseDN>?<attributes>?
<scope>?<filter>
ibm-slapdReferral: ldap://<additional hostname:port>/<baseDN>?<attributes>?
<scope>?<filter>
objectclass: ibm-slapdReferral
objectclass: top
objectclass: ibm-slapdConfigEntry
```

例えば、2 つのサーバー server1 および server2 (セキュア・サーバー) に対する参照を、listen ポートが **389**、ベースが **ou=austin,o=sample**、属性が **cn**、**sn**、**description**、スコープが **base**、フィルターが **objectclass=*** で設定する場合、LDIF ファイルは以下ようになります。

```
# referral
dn: cn=Referral, cn=Configuration
cn: Referral
ibm-slapdreferral: ldap://server1.mycity.mycompany.com:389/
ou=austin,o=sample?cn,sn,description?base?objectclass=*
ibm-slapdreferral: ldaps://server2.mycity.mycompany.com:389/
ou=austin,o=sample?cn,sn,description?base?objectclass=*
objectclass: ibm-slapdReferral
objectclass: ibm-slapdConfigEntry
objectclass: top
```

サポートされる URL 形式の詳細については、649 ページの『付録 E. IPv6 サポート』を参照してください。

参照の変更

以下に示すいずれかの方法を使用することで、参照を編集できます。

このタスクについて

Web 管理の使用

以下に示す指示を使用することで、Web 管理ツールを使用して参照を変更することができます。

このタスクについて

1. まだ行っていない場合は、Web 管理ツールを使用してマスター・サーバーへログオンします。
2. 「項目の追加」パネルの「**必須属性**」タブで、「**参照の管理**」をクリックします。
3. 「**現在の参照**」セクションで、編集する参照を選択します。
4. 「**編集**」をクリックします。
5. この参照値が指し示すサーバーのホスト名およびポートを変更できます。

6. 参照先がセキュア (SSL) サーバーかどうかに関係なく、「**SSL の使用**」を変更できます。
7. ターゲット・サーバーのディレクトリー情報ツリーに基本 DN を変更できます。例えば、ou=austin,o=sample です。
8. 参照 URL に属性を追加することで、または参照 URL から属性を削除することで、参照 URL に組み込む必要のある属性を変更できます。
9. 参照検索スコープを変更できます。
10. 検索フィルターを変更できます。詳細については、542 ページの『検索フィルター』を参照してください。
11. 「**OK**」をクリックします。
12. 変更する各参照に対して、上記のステップを繰り返します。

変更した内容を有効にするには、サーバーを再始動する必要があります。

コマンド・ラインの使用

以下に示すコマンドを発行することで、server1 への参照を変更し、baseDN を ou=raleigh,o=sample にすることができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -M -i <filename>
```

where <filename> contains:

```
dn: cn=referral, cn= configuration
changetype: modify
replace: ibm-slapdReferral
ibm-slapdreferral: ldap://server1.mycity.mycompany.com:389/
ou=raleigh,o=sample?cn,sn,description?base?objectclass=*
```

注: 参照項目にアクセスするときに、通常項目のように項目を処理するには **-M** オプションを指定する必要があります。指定しない場合、サーバーは参照を返します。

参照の除去

以下に示すいずれかの方法を使用して、参照を除去することができます。

このタスクについて

Web 管理の使用

以下に示す指示により、Web 管理ツールを使用して参照を除去することができます。

このタスクについて

1. まだ行っていない場合は、Web 管理ツールを使用してマスター・サーバーへログオンします。
2. Web 管理ツールのナビゲーション領域で「**サーバー管理**」カテゴリーを展開し、「**サーバー・プロパティの管理**」を選択します。
3. 「**参照**」をクリックします。

注: 別のパネルで作業していて、参照を含む属性を持つ項目を追加または変更する場合、「**参照の管理**」をクリックしてこのパネルにアクセスできます。

4. 「現在の参照」セクションから、除去する参照を選択します。
5. 「除去」をクリックします。
6. 確認パネルが表示されます。参照を除去する場合は、「OK」をクリックします。変更を行わずに前のパネルに戻る場合は「キャンセル」をクリックします。
7. 除去する参照の数だけこのプロセスを繰り返すか、「すべて除去」をクリックして現在の参照をすべて除去します。
8. 完了したら、終了せずに変更を保存する場合は「適用」をクリックし、変更を適用して終了する場合は「OK」をクリックし、変更を行わずにこのパネルを終了するには「キャンセル」をクリックします。

変更した内容を有効にするには、サーバーを再始動する必要があります。

コマンド・ラインの使用

以下に示すコマンドを発行することにより、austin.ibm.com:389 などの単一のデフォルト参照を削除することができます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=referral, cn= configuration
changetype: modify
delete: ibm-slapdReferral
ibm-slapdReferral: ldap://referral.austin.ibm.com:389
```

すべてのデフォルト参照を削除するには、以下の手順を実行します。

```
idsldapdelete -D <adminDN> -w <adminPW> "cn=referral,cn=configuration"
```

レプリカ生成

複製は、ディレクトリー・サーバーのパフォーマンス、可用性、および信頼性を向上させるために使用する技法です。複製処理では、複数のディレクトリー・サーバーのデータが同期された状態に保たれます。ここで提供する情報により、複製の利点について詳しく知ることができます。

複製には、主に 3 つの利点があります。

- 情報の冗長: 複製は、サプライヤーのサーバーの内容をバックアップします。
- 高速な検索: 検索要求を 1 つのサーバーではなく、複数のサーバーで分担して処理できます。これにより、要求完了の応答時間が短縮されます。
- セキュリティーとコンテンツ・フィルタリング - レプリカはサプライヤー・サーバーのデータのサブセットを格納できます。

次のセクションでは、Web 管理ツール、コマンド行ユーティリティー、および LDIF ファイルを使用した複製のセットアップ例について説明します。シナリオは少しずつ複雑になります。

- 1 つのマスターおよび 1 つのレプリカ
- 1 つのマスター、1 つの転送、および 1 つのレプリカ
- 2 つのピア/マスター、2 つの転送、および 4 つのレプリカ
- ゲートウェイ複製

単一スレッドの複製合意からマルチスレッドの複製合意への切り替えが必要な場合の例について説明します。この例では、サーバー ID `wingspread-2389` のサーバー上の複製合意を、LDAP URL `ldap://wingspread:1389` のコンシューマーに切り替える場合を考えます。

```
dn: cn=wingspread-1389,ibm-replicaServerId=wingspread-2389,
ibm-replicaGroup=default,0=SAMPLE
cn: wingspread-1389
ibm-replicaconsumerid: wingspread-1389
ibm-replicacredentialsdn: cn=simple, cn=replication, cn=localhost
ibm-replicaurl: ldap://wingspread:1389
objectclass: ibm-replicationAgreement
objectclass: top
```

デフォルトでは、`ibm-replicamethod` は 1 (単一スレッド複製) です。複製方式を変更して使用する接続の数を指定するには、以下の `ldapmodify` コマンドを発行します。

```
ldapmodify -D <binddn> -w <password> -p <ldapport> -v -i <file>
```

where *file* contains:

```
dn: cn=wingspread-1389,ibm-replicaServerId=wingspread-2389,
ibm-replicaGroup=default,0=SAMPLE
ibm-replicamethod: 2
ibm-replicaconsumerconnections: 5
```

複製合意のデータを検証するには、以下のコマンドを発行します。

```
ldapsearch -L -p <ldapport>
-b cn=wingspread-1389,ibm-replicaServerId=wingspread-2389,ibm-replicaGroup=default,
0=SAMPLE objectclass=*
```

以下の出力が生成されます。

```
dn: cn=wingspread-1389,ibm-replicaServerId=wingspread-2389,
ibm-replicaGroup=default,0=SAMPLE
cn: wingspread-1389
ibm-replicaconsumerid: wingspread-1389
ibm-replicacredentialsdn: cn=simple, cn=replication, cn=localhost
ibm-replicaurl: ldap://wingspread:1389
objectclass: ibm-replicationAgreement
objectclass: top
ibm-replicaconsumerconnections: 5
ibm-replicamethod: 2
ibm-replicationonhold: FALSE
```

ここで、複製方式 (`ibm-replicamethod`) の値 2 は、マルチスレッドの複製を使用することを指定します。属性「`ibm-replicaconsumerconnections`」は、更新をコンシューマーに送信するために複製で使用される接続の数を示します。この値は、1 から 32 までの範囲で指定できます。この例では、サプライヤーは、複製に使用するために、コンシューマーへの接続を 5 つ確立します。

注: 複製合意を更新した後で、変更した内容を有効にするためにサーバーを再始動する必要があります。

今度は、複製状況をモニターする例について説明します。以下のコマンドを発行します。

```
ldapsearch -D <binddn> -w <password> -p <ldapport>
-b cn=wingspread-1389,ibm-replicaServerId=wingspread-2389,ibm-replicaGroup=default,
0=SAMPLE objectclass=* +ibmrepl
```

以下の出力が生成されます。

```
cn=wingspread-1389,ibm-replicaServerId=wingspread-2389,ibm-replicaGroup=default,0=SAMPLE
ibm-replicationChangeLDIF=N/A
ibm-replicationLastActivationTime=20080707152436Z
ibm-replicationLastChangeId=4855
ibm-replicationLastFinishTime=20080707152436Z
ibm-replicationLastResult=N/A
ibm-replicationLastResultAdditional=N/A
ibm-replicationNextTime=N/A
ibm-replicationPendingChangeCount=0
ibm-replicationState=ready
```

```

ibm-replicationFailedChangeCount=0
ibm-replicationperformance=[c=0,l=10,op=0,q=0,d=0,ws=0,s=0,ds=0,wd=0,wr=0,r=0,e=0,ss=1,rs=1]
ibm-replicationperformance=[c=1,l=10,op=0,q=0,d=0,ws=0,s=0,ds=0,wd=0,wr=0,r=0,e=0,ss=1,rs=1]
ibm-replicationperformance=[c=2,l=10,op=0,q=0,d=0,ws=0,s=0,ds=0,wd=0,wr=0,r=0,e=0,ss=1,rs=1]
ibm-replicationperformance=[c=3,l=10,op=0,q=0,d=0,ws=0,s=0,ds=0,wd=0,wr=0,r=0,e=0,ss=1,rs=1]
ibm-replicationperformance=[c=4,l=10,op=0,q=0,d=0,ws=0,s=0,ds=0,wd=0,wr=0,r=0,e=0,ss=1,rs=1]

```

この例では、コンシューマーへの 5 つの接続があります。属性名は等号の左方に表示されます。複製状況情報属性の中には、単一スレッドの複製のみで使用されるもの（ここでは値「N/A」が示されているもの）と、マルチスレッドの複製のみで使用されるものがあります。「+ibmrepl」を使用すると、すべての複製状況情報属性を簡単に要求することができます。変更の保留およびログに記録された複製エラーも含め、すべての属性を表示するには、「++ibmrepl」を使用してください。

「ibm-replicationperformance」属性は、マルチスレッドの複製を使用する複製合意のみに適用できます。単一スレッドの複製の場合、この属性の値は「N/A」になります。ibm-replicationperformance データの意味は以下の方法で解釈できます。

- c=0** これは接続番号です。この例では、5 つの接続があります。最初の接続が最もトラフィックが大きいことを示しています。ワークロードにより、ほかの接続の使用頻度が決まります。
- l=10** これは、各キューのサイズ制限です。各接続には 2 つのキューがあり、両方のキューは同じ長さです。1 つは、その接続を使用して送信する更新を入れるキュー（送信キューと呼ばれる）で、もう 1 つは、送信はしたがコンシューマーからの応答を受信していない更新を入れるキュー（受信キューと呼ばれる）です。更新が送信されると、その更新は送信キューから受信キューに移動します。受信キューがそのサイズ制限に達すると、コンシューマーから何らかの応答を受信するまでは、もう更新は送信されません。送信キューがそのサイズ制限に達すると、その接続にはもう更新を割り当てることはできません。すべての接続の送信キューがサイズ制限に達すると、サプライヤーは、コンシューマーがバックログを処理するまで待つ必要があります。
- op=0** 接続の送信キューに割り当てられた最後の操作の複製 ID。複製 ID は、コンシューマーに複製されるすべての更新に割り当てられます。
- q=0** 送信キューの現在のサイズ。
- d=0** 依存更新の数（項目の追加とそれに続く同一項目の変更は依存関係にあるとみなされ、依存更新を正しい順序で適用できるようにするには、同一の接続に割り当てる必要がある）。
- ws=0** 送信キューがサイズ制限に達した回数。
- ds=0** 送信された依存更新の数。
- wd=0** 送信キューが、追加の更新を送る前に依存更新を待機した回数。
- wr=0** 受信キューがサイズ制限に達した回数。
- r=0** コンシューマーからの応答を待機している複製更新の数。
- e=0** コンシューマーから報告された複製エラーの数。
- ss=1** 送信側スレッドのセッション・カウント（コンシューマーへの接続が確立されるたびに増加。）
- rs=1** 受信側スレッドのセッション・カウント。

複製に関連する用語

この用語集では、このセクションで使用する技術用語を定義します。

カスケード複製 (Cascading replication)

複数のサーバー層がある複製トポロジー。ピア/マスター・サーバーは、読み取り専用 (転送) サーバーのセットに複製された後、他のサーバーに複製されます。このようなトポロジーにより、マスター・サーバーからの複製作業の負荷が軽減されます。

コンシューマー・サーバー (Consumer server)

他の (サプライヤー) サーバーからの複製を介して変更を受信するサーバー。

資格情報 (Credentials)

サプライヤーがコンシューマーへのバインドに使用するメソッドおよび必須情報を識別します。単純なバインドの場合、資格情報には DN とパスワードが含まれます。資格情報は、レプリカ合意で指定された DN の項目に格納されます。

転送サーバー (Forwarding server)

送信されたすべての変更を複製する読み取り専用サーバー。この用語が指すサーバーは、ピア/マスター・サーバーとは対照的に読み取り専用であり、ピアを持つことができません。

ゲートウェイ・サーバー (Gateway server)

ローカル複製サイトから複製ネットワークに存在する他のゲートウェイ・サーバーにすべての複製トラフィックを転送するサーバー。複製ネットワーク内にある他のゲートウェイ・サーバーからの複製トラフィックも受信します。このトラフィックは、ゲートウェイ・サーバーによってローカル複製サイト上にあるすべてのサーバーに転送されます。

ゲートウェイ・サーバーはマスター (書き込み可能) にする必要があります。

マスター・サーバー (Master server)

任意のサブツリーで書き込み可能 (更新可能) なサーバー。

ネストされたサブツリー (Nested subtree)

ディレクトリーの複製されたサブツリー内のサブツリー。

ピア・サーバー (Peer server)

任意のサブツリーに複数のマスターがある場合に、マスター・サーバーに対して使用される用語。ピア・サーバーは、別のピア・サーバーから送信された変更を複製しません。元々そのサーバーで最初に行われた変更のみを複製します。

レプリカ・グループ (Replica group)

複製コンテキストにおいて作成される最初の項目には `objectclass ibm-replicaGroup` が含まれており、複製に参加するサーバーの集合を表します。これは、複製トポロジー情報を保護するように ACL を設定する場所として便利です。現在、管理ツールは、各複製コンテキストの下の `ibm-replicagroup=default` という名前の 1 つのレプリカ・グループをサポートしています。

レプリカ・サブエントリー (Replica subentry)

レプリカ・グループ項目の下には、サプライヤーとして複製に参加するサーバーごとに 1 つずつ、objectclass ibm-replicaSubentry を含む項目を 1 つ以上作成することができます。レプリカ・サブエントリーは、複製におけるサーバーの役割 (マスターまたは読み取り専用) を示します。読み取り専用のサーバーは複製合意を持ち、カスケード複製をサポートできます。

複製されたサブツリー (Replicated subtree)

あるサーバーから別のサーバーに複製されるディレクトリー情報ツリー (DIT) の一部。この設計の下では、サブツリーを一部のサーバーには複製することができ、その他のサーバーには複製できません。1 つのサブツリーをサーバーで書き込み可能にすると同時に、他のサブツリーを読み取り専用にするのが可能です。

複製ネットワーク (Replicating network)

接続されている複製サイトを含むネットワーク。

複製合意 (Replication agreement)

2 つのサーバー間の「接続」または「複製パス」を定義する、ディレクトリーに格納されている情報。一方のサーバーはサプライヤー (変更を送信する側)、もう一方のサーバーはコンシューマー (変更を受信する側) と呼ばれます。合意には、サプライヤーからコンシューマーへの接続を確立し、複製を計画するために必要な情報がすべて含まれています。

複製コンテキスト (Replication context)

複製サブツリーのルートを示します。ibm-replicationContext 補助オブジェクト・クラスを項目に追加し、その項目に複製領域のルートとしてのマークを付けることができます。複製に関連する構成情報は、複製コンテキストのベースの下に作成される一連の項目で保持されます。

複製サイト (Replication site)

ゲートウェイ・サーバー 1 つと、一緒に複製するように構成されるすべてのマスター・サーバー、ピア・サーバー、またはレプリカ・サーバー。

スケジュール (Schedule)

複製は、累積されてバッチで送信されるサプライヤーでの変更を使用して、特定の時刻に実行されるようにスケジュールできます。レプリカ合意には、スケジュールを提供する項目の DN があります。

サプライヤー・サーバー (Supplier server)

変更を他の (コンシューマー) サーバーに送信するサーバー。

複製トポロジ (Replication topology)

LDAP サーバー間で複製される情報とその複製方法を制御する、ディレクトリー内のオブジェクト・セット。以下のオブジェクトが含まれます。

- 複製コンテキスト
- 複製グループ
- 複製サブエントリー
- 複製合意
- 複製資格情報
- 複製スケジュール項目

複製ネットワーク内のすべての LDAP サーバーでは、複製トポロジータン同じになっている必要があります。

複製トポロジータン

ここで提供する情報および例により、複製トポロジータンについて詳しく知ることができます。

ディレクトリタンの特定の項目は、`ibm-replicationContext` オブジェクト・クラスを追加することによって、複製されたサブツリタンのルートとして識別されます。各サブツリタンは独立して複製されます。サブツリタンは、リーフ項目または他の複製されたサブツリタン (コンテキスト) に到達するまでディレクトリ情報ツリタン (DIT) を下にたどります。項目は、複製構成情報を格納するため、複製されたサブツリタンのルートの下に追加されます。これらの項目は、1 つ以上のレプリカ・グループ項目で、その下にレプリカ・サブエントリが作成されます。各レプリカ・サブエントリに関連付けられるのは、各サーバーによって提供される (複製先の) サーバーを識別し、資格情報とスケジュール情報を定義する複製合意です。

複製では、あるディレクトリタンに加えた変更が、1 つ以上の別のディレクトリタンに伝搬されます。つまり、あるディレクトリタンを変更すると、その内容が複数の別のディレクトリタンに反映されます。IBM Security Directory Server では、拡張マスター・レプリカ複製モデルがサポートされます。複製トポロジータンは、以下のものを含むように拡張されます。

- 特定のサーバーへのディレクトリ情報ツリタンのサブツリタンの複製
- カスケード複製と呼ばれるマルチレイヤータン・トポロジータン
- サブツリタンのによるサーバー役割 (サプライヤータンまたはコンシューマータン) の割り当て
- 複数のマスター・サーバー (ピアツピタン複製と呼びます)
- ネットワークを介して複製するゲートウェイ・サーバー

サブツリタンのによる複製の利点は、レプリカはディレクトリタン全体を複製する必要がないという点です。ディレクトリタンの一部、またはサブツリタンのレプリカを作成できます。

拡張モデルにより、マスターおよびレプリカタンの概念は変化します。これらの用語は、サーバーではなく、複製された特定のサブツリタンのに関してサーバーが持つ役割に適用されるようになりました。サーバーは、複数のサブツリタンのマスター、およびその他サーバータンのレプリカとして機能します。マスターという用語は、複製されたサブツリタンのクライアント更新を受け入れるサーバーに使用されます。レプリカという用語は、複製されたサブツリタンのサプライヤータンとして指定された他のサーバーからの更新のみを受け入れるサーバーに使用されます。

機能により定義されるディレクトリタンの役割には、マスター/ピア、ゲートウェイ、転送 (カスケード)、およびレプリカ (読み取り専用) の 4 タンタイプがあります。

表 33. サーバーの役割

<p>マスター/ピア </p>	<p>マスター/ピア・サーバーには、マスター・ディレクトリー情報が入っています。更新情報は、ここからレプリカに伝搬されます。すべての変更はマスター・サーバー上で行われ、そのマスターには、これらの変更をレプリカに伝搬する責任があります。</p> <p>ディレクトリー情報のマスターとして機能する複数のサーバーがあります。各マスターは、他のマスター・サーバーおよびレプリカ・サーバーを更新する責任があります。これはピア複製と呼ばれます。ピア複製により、パフォーマンスと信頼性が向上されます。パフォーマンスは、広範囲に分散したネットワークで更新を処理するローカル・サーバーの提供により向上します。信頼性は、1 次マスターが失敗した場合ただちに引き継ぐバックアップ・マスター・サーバーの提供により向上します。</p> <p>注:</p> <ol style="list-style-type: none"> 1. マスター・サーバーはすべてのクライアント更新を複製しますが、他のマスターから受け取った更新は複製しません。 2. ピア・サーバー間の更新は、直ちに実行することもできますし、スケジュールに従って実行することもできます。詳細については、417 ページの『複製スケジュールの作成』を参照してください。
<p>転送 (カスケード) </p>	<p>転送またはカスケード・サーバーは、そのサーバーに送信されるすべての変更を複製するレプリカ・サーバーです。これは、接続されているクライアントによって行われる変更のみを複製するマスター/ピア・サーバーとは対照的です。カスケード・サーバーは、多くのレプリカが広く分散されたネットワークで、マスター・サーバーの複製ワークロードを緩和できます。</p>
<p>ゲートウェイ </p>	<p>ゲートウェイ複製では、ゲートウェイ・サーバーを使用して、複製情報を複製ネットワークを介して効果的に収集および配布します。ゲートウェイ複製の主な利点はネットワーク・トラフィックの軽減です。</p>
<p>レプリカ (読み取り専用) </p>	<p>ディレクトリー情報のコピーを持つ追加のサーバー。レプリカは、マスター (またはマスターのレプリカであるサブツリー) のコピーです。レプリカは、複製されたサブツリーのバックアップとなります。</p>

レプリカ・サーバーで更新を要求できますが、実際には、参照をクライアントに戻すことによって更新がマスター・サーバーに転送されます。更新が正常に完了した場合は、マスター・サーバーは更新をレプリカに送信します。マスターが更新情報の複製を完了するまでは、要求元のレプリカ・サーバーにその変更は反映されません。複製に失敗した場合は、マスターを再始動しても引き続き失敗します。変更は、マスターで行われた順序で複製されます。324 ページの『複製エラーの処理』を参照してください。

レプリカを使用しなくなった場合は、サプライヤーからレプリカ合意を削除する必要があります。定義を残しておくこと、サーバーがすべての更新をキューに入れ、ディレクトリー・スペースを無駄に使用します。またサプライヤーは、欠落しているコンシューマーへの接続を試行し続け、データの送信を再試行します。

複製の概要

このセクションでは、複製トポロジーの各タイプに関するハイレベルな説明を行います。

シンプル複製

複製で基本となるのは、マスター・サーバーとレプリカ・サーバーの関係です。マスター・サーバーは、ディレクトリーまたはディレクトリーのサブツリーを含むことができます。ここで提供する情報および例により、それについて詳しく知ることができます。

マスターは書き込み可能です。したがって、所定のサブツリーに対する更新をクライアントから受け取ることができます。レプリカ・サーバーは、マスター・サーバーのディレクトリーのコピー、またはマスター・サーバーのディレクトリーの一部のコピーを含むことができます。レプリカは読み取り専用です。したがって、クライアントが直接更新を行うことはできません。その代わりに、レプリカは、マスター・サーバーに対するクライアント要求を参照します。マスター・サーバーは要求された更新を実行し、それらをレプリカ・サーバーに複製します。

1 つのマスター・サーバーは、複数のレプリカを所有できます。各レプリカは、マスターのディレクトリー全体のコピーを含むことも、ディレクトリーのサブツリーを含むこともできます。次の例では、マスター・サーバーのディレクトリー全体のコピーをレプリカ 2 が含んでおり、レプリカ 1 とレプリカ 3 はそれぞれマスター・サーバーのディレクトリーのサブツリーのコピーを含んでいます。

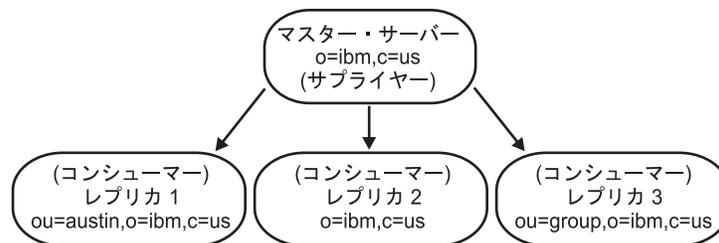


図7. マスター - レプリカ間の複製

2 つのサーバー間の関係は役割という点でも説明できます。つまり、サプライヤーとコンシューマーという役割です。上記の例では、マスター・サーバーが各レプリカに対するサプライヤーです。また各レプリカが、マスター・サーバーのコンシューマーです。

カスケード複製

カスケード複製は、複数のサーバー層があるトポロジーです。ここで提供する情報および例により、それについて詳しく知ることができます。

マスター・サーバーは読み取り専用 (転送) サーバーのセットに複製され、さらにそのセットは他のサーバーに複製されます。そのようなトポロジーでは、マスター・サーバーの複製作業の負荷が軽減されます。以下のこのタイプのトポロジーの例では、マスター・サーバーが 2 つの転送サーバーのサプライヤーになっています。転送サーバーには 2 つの役割があります。転送サーバーは、マスター・サーバーのコンシューマーであると同時に、それらに関連付けられているレプリカ・サーバーのサプライヤーでもあります。レプリカ・サーバーは、それぞれの転送サーバーのコンシューマーです。例:

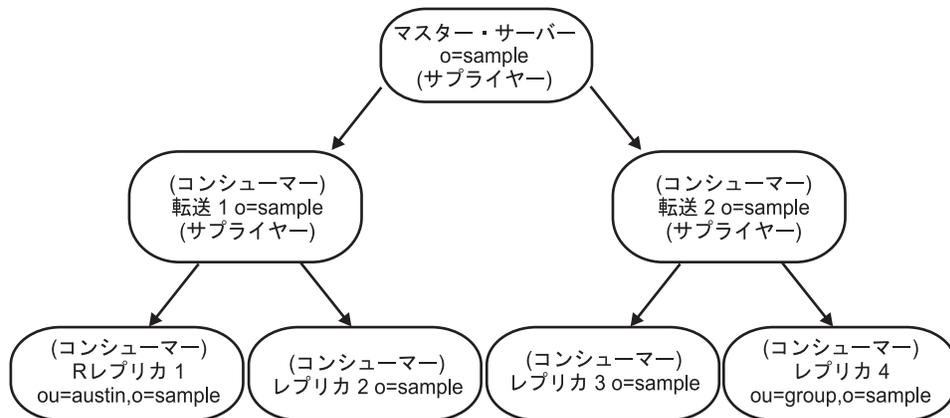


図8. カスケード複製

ピアツーピア複製

ディレクトリー情報のマスターとして機能する複数のサーバーがあります。各マスターは、他のマスター・サーバーおよびレプリカ・サーバーを更新する責任があります。これはピア複製と呼ばれます。ここで提供する情報および例により、それについて詳しく知ることができます。

ピア複製により、パフォーマンス、可用性、および信頼性が向上します。パフォーマンスは、広範囲に分散したネットワークで更新を処理するローカル・サーバーの提供により向上します。可用性および信頼性が向上するのは、プライマリー・マスターに障害が発生した場合でも、バックアップ・マスター・サーバーが即時にそれを引き継いでくれるからです。ピア・マスター・サーバーは、すべてのクライアント更新をレプリカおよび他のピア・マスターに複製しますが、他のマスター・サーバーから受け取った更新は複製しません。

注: ピアツーピア複製で、追加操作および変更操作を行った場合に発生する競合は、タイム・スタンプを基にして解決されます。320 ページの『複製の競合解決』を参照してください。

注: ピア・マスターごとに 1 つのレプリカ・サーバーがあるピアツーピア複製セットアップでは、プライマリー・マスターに障害が発生すると、プロキシ・サーバーは要求をバックアップ・マスター・サーバーに送信します。ただし、プロキシ・サーバーは、バックアップ・マスター・サーバーに障害が発生するまでは、プライマリー・マスターにフォールバックしません。

以下の図に、ピアツーピア複製の例を示します。

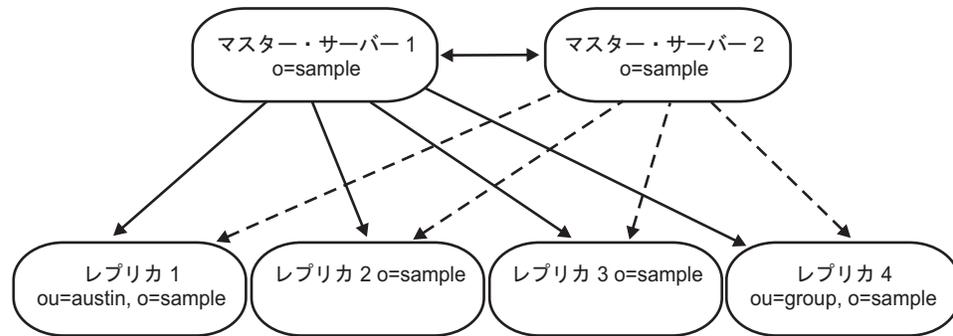


図9. ピアツーピア複製

ゲートウェイ複製

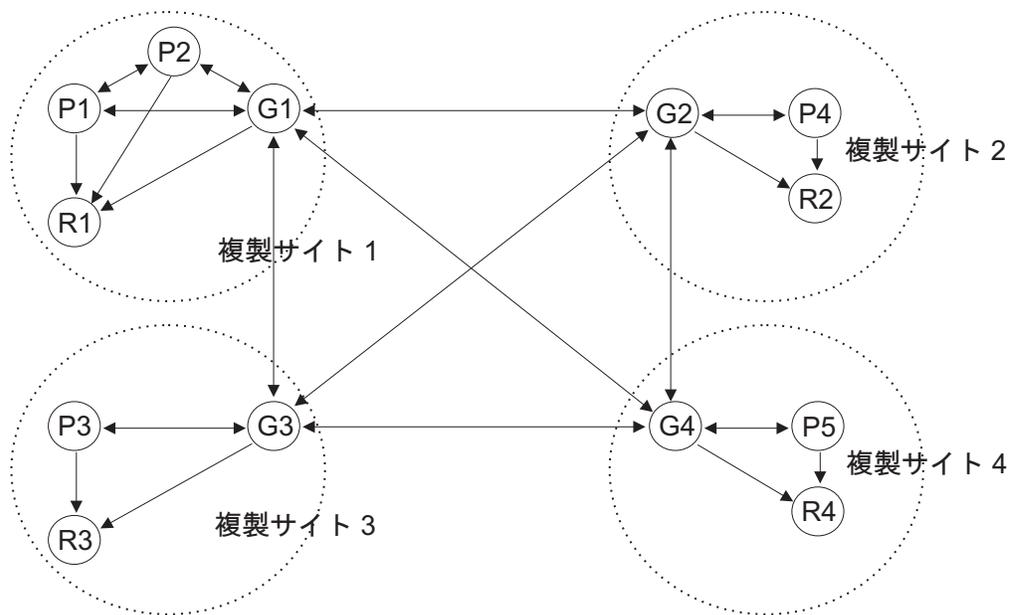
ゲートウェイ複製は、ピアツーピア複製をさらに高度に応用したもので、ネットワーク全体に複製機能を展開します。ここで提供する情報および例により、それについて詳しく知ることができます。

もっとも注目すべき相違点は、ゲートウェイ・サーバーが、他のピア・サーバーからゲートウェイを介して受け取った変更を複製するという点です。

ゲートウェイ・サーバーはマスター・サーバー、つまり書き込み可能である必要があります。ゲートウェイ・サーバーは、所有する複製サイト内ではピア・サーバーとして動作します。つまりゲートウェイ・サーバーは、複製サイト内では、クライアント更新を受け取って複製することも、他のピア・マスター・サーバーから更新を受け取ることもできます。ゲートウェイ・サーバーは、他のピア・サーバーから受け取った更新を、所有する複製サイト内の他のどのサーバーにも複製しません。

ゲートウェイ・サーバーは、ゲートウェイ・ネットワーク内では、両方向の転送サーバーとして動作します。ある場合は、複製サイト内のピアがゲートウェイ・サーバーのサプライヤーとして動作し、他のゲートウェイ・サーバーがコンシューマーとして動作します。またある場合は、両者の役割が逆になります。つまり、コンシューマーとして動作していたゲートウェイ・サーバーがサプライヤーとして動作し、複製サイト内でサプライヤーとして動作していたサーバーがコンシューマーとして動作します。

ゲートウェイ複製では、ゲートウェイ・サーバーを使用して、複製情報を複製ネットワークを介して効果的に収集および配布します。ゲートウェイ複製の主な利点はネットワーク・トラフィックの軽減です。例:



P=ピア・サーバー
 G=ゲートウェイ・サーバー
 R=読み取り専用レプリカ

図 10. ゲートウェイ複製

部分複製

ここで提供する情報およびリンクにより、それについて詳しく知ることができます。

部分複製は、指定された項目およびサブツリー内の指定された項目の属性サブセットのみを複製する複製機能です。部分複製を使用すると、管理者はデプロイメントの要件に応じて複製の処理能力を向上させることができます。複製される属性は複製フィルターを使用して指定されます。部分複製について詳しくは、380 ページの『部分複製』を参照してください。

複製の競合解決

ここでは、複製の競合、およびそれらを解決するための方法について詳しく説明します。

DN の削除または変更操作に関連する複製競合が発生した場合、結果として人的な介入が必要なエラーとなります。例えば、あるサーバーで項目を変更している間に、別のサーバーでその項目の名前を変更した場合、変更がレプリカに届く前に、名前の変更 (modifyDN) がレプリカに届いてしまう場合があります。この場合、変更がレプリカに到着しても、エラーとなってしまいます。このケースでは、管理者は、新規の DN を持つ項目に変更を適用することで、エラーに対応する必要があります。正しい名前の変更を再実行するのに必要な情報は、すべて複製ログおよびエラー・ログに保存されます。複製エラーは、正しく構成された複製トポロジーではほとんど発生しませんが、決して発生しないと仮定するのは危険です。

注: 複製競合が検出されると、その複製競合を解決するために項目が再追加され、再追加の前の元の項目は `lostandfound.log` ファイルに書き込まれます。これにより、元の項目のすべての側面の復元が可能になります。グループ項目に競合が検出された場合も、グループ項目全体がこのログ・ファイルに記録されます。

ピアツーピア複製で、追加操作および変更操作を行った場合に発生する競合は、タイム・スタンプを基にして解決されます。マルチ・マスター複製環境の各サーバーでは、最新の変更タイム・スタンプを持つ項目更新が一番優先順位が上です。複製された削除要求および名前変更要求は、競合解決なしで受け取った順番で適用されます。複製競合が検出された場合、後でリカバリーできるように、置き換えられた項目は逸失および検出ログにアーカイブとして保存されます。詳細については、476 ページの『ロギングのユーティリティ』を参照してください。

複数のサーバーによる同じ項目の更新が、ディレクトリー・データの不整合を発生させる場合があります。これは、競合解決が項目のタイム・スタンプを基に行われるからです。最新の変更タイム・スタンプが一番優先順位が上です。サーバー上のデータで不整合が発生した場合、サーバーの再同期については、「*IBM Security Directory Server Version 6.3 Command Reference*」の `ldapdiff` コマンド情報を参照してください。

複製競合の解決メカニズムを拡張するには、タイム・スタンプの細分度をマイクロ秒に設定します。Security Directory Server では、ピア間で同一項目に対する変更が異なる時刻に行われた場合、クロック・スキューが原因でそれらの変更が収束しない可能性があるということも考慮されます。したがって、収束を確実にし、更新後の項目のタイム・スタンプが更新操作の前のタイム・スタンプより小さくならないように確保するために、更新のたびに各項目のタイム・スタンプが単調増加されます。これにより、クロック・スキューがあったとしても、確実に項目を収束させることができます。このようにして、複製トポロジーに含まれているマシンのシステム・クロックが同期していない場合でも、複製競合の解決が正しく機能します。

注:

- パスワード・ポリシーの運用属性では、これらの属性にタイム・スタンプ値が含まれている場合でも、タイム・スタンプの細分度は重要ではありません。
- Security Directory Server 6.2 以降のバージョンでは、Windows プラットフォームで追加または変更される項目のタイム・スタンプ細分度はミリ秒です。ただし、Windows 以外のプラットフォームの場合、タイム・スタンプ細分度はマイクロ秒です。これは、非 Windows マシンから Windows マシンに項目を複製すると、その項目のタイム・スタンプはマイクロ秒レベルの細分度になるということです。逆に、Windows マシンから非 Windows マシンに項目を複製した場合は、その項目のタイム・スタンプはミリ秒レベルの細分度になります。

IBM Security Directory Server 6.0 以降のバージョンでは、複製競合を解決するため、サプライヤーで項目が更新される前に、サプライヤーが項目のタイム・スタンプを提供する必要があります。サプライヤーとして稼働している旧バージョンのディレクトリー・サーバーには、この種の情報を提供できる機能はありません。したがって、サプライヤーが下位レベルのサーバーの場合には、複製競合の解決は適用不能になります。コンシューマー・サーバー (この説明では IBM Security Directory Server バージョン 6.0 サーバー) は、複製されたタイム・スタンプと更新を受け取り、競合チェックを行わずにそれを適用します。

注:

1. 古いバージョンの IBM Security Directory Server は、タイム・スタンプ競合の解決をサポートしません。トポロジーに古いバージョンの IBM Security Directory Server が含まれている場合、そのネットワークでのデータの整合性は確保されません。使用しているサーバーが競合解決をサポートしている場合、623 ページの『付録 B. ルート DSE 内部のオブジェクト ID (OID) および属性』および 625 ページの『サポートされ、使用可能になっている機能の OID』を参照して解決方法を確認してください。
2. 複製競合を解決するために、新しいタイム・スタンプを持つ通常のデータベース項目は、古いタイム・スタンプを持つ複製された項目によって置き換えられることはありません。ただし、競合解決は項目 `cn=schema` には適用されません。項目 `cn=schema` は、複製された項目 `cn=schema` に必ず置き換えられます。
3. 複製競合の解決は、複製トポロジーに複数のサプライヤーが指定されていない場合は、コンシューマーで使用不可に設定できます。このような複製トポロジーの場合、`ibmslapd.log` ファイルに記録される競合操作関連のメッセージは単純な警告メッセージとみなすことができます。これらのメッセージのロギングを停止するための予備手段として、`ldapmodify` コマンドを使用して構成ファイルパラメーター `ibm-slapdNoReplConflictResolution` を `true` に設定することができます。

ロード・バランサーを設定することも、データの競合を解決する方法の 1 つです。

IBM WebSphere Edge Server などのロード・バランサーは、ディレクトリーに更新を送信する際、仮想ホスト名を使用します。アプリケーションは、この仮想ホスト名を使用します。ロード・バランサーは、それらの更新を 1 つのサーバーにのみ送信するように構成されます。このサーバーがダウンしたり、ネットワーク障害により使用不可になった場合、このサーバーが再度オンラインになって使用可能になるまで、ロード・バランサーは使用可能な次のピア・サーバーに更新を送信します。ロード・バランシング・サーバーのインストール方法および構成方法については、ロード・バランサーの製品資料を参照してください。

競合解決が使用可能にされているときに、1 つのグループのメンバーシップに対する変更が 2 つのサーバーで同時に行われた場合、競合解決が繰り返トリガーされ、グループが大きい場合にはサーバーのパフォーマンスに影響が出ることがあります。

Security Directory Server を使用すると、複製競合の解決を選択的に使用可能または使用不可に設定し、構成ファイルの「`cn=Replication, cn=configuration`」項目下位の「`ibm-slapdEnableConflictResolutionForGroups`」属性の値を定義して、グループ項目を変更することができます。

属性「`ibm-slapdEnableConflictResolutionForGroups`」を `FALSE` に設定すると、グループ項目に対する操作 (タイプが `member` または `uniquemember` の属性の追加、削除、または名前変更など) で競合が検出された場合でも、競合解決は実行されません。

ただし、単一の変更要求で複数の属性をターゲットにできます。その場合、単一の変更要求で `member` または `uniquemember` 以外の属性が使用されていると、属性「`ibm-slapdEnableConflictResolutionForGroups`」が `FALSE` に設定されていても、複製の競合解決が実行されます。

グループ項目の変更の場合に複製の競合解決を使用可能または使用不可にするには、以下のいずれかの方法を使用します。

Web 管理ツールの使用:

ここで説明する手順に従い、Web 管理ツールを使用して複製競合を処理することができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「サーバー・プロパティの管理」をクリックします。「競合解決」タブをクリックします。

グループ・メンバーの複製競合解決を構成するには、以下のステップを実行します。

1. 「グループ・メンバーの複製競合解決を有効にする」チェック・ボックスを選択します。デフォルトではこのチェック・ボックスは選択されていません。構成ファイル内の dn "cn=Replication, cn=configuration" の下にある「ibm-slapdEnableConflictResolutionForGroups」属性は、このコントロールに関連付けられています。この属性は、グループ項目に対する不要な競合解決を回避することによって複製の速度を高めるために、すべての複製トポロジーで使用できます。「ibm-slapdEnableConflictResolutionForGroups」属性のデフォルト値は FALSE です。
2. 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして変更を適用し、このパネルを終了します。
 - 「適用」をクリックして変更内容を適用し、このパネルを表示させたままにします。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

コマンド行の使用:

ここで説明するコマンドを発行することにより、グループ・メンバーの複製競合の解決を使用可能または使用不可にすることができます。

このタスクについて

```
ldapmodify -h <ldaphost> -p <ldap port> -D <bindDN> -w <password> -f <file>
```

where *file* contains:

```
dn:cn=Replication, cn=Configuration
changetype: modify
replace: ibm-slapdEnableConflictResolutionForGroups
ibm-slapdEnableConflictResolutionForGroups: <value to be set as either TRUE or FALSE>
```

複製競合の解決機能を使用不可に設定:

Security Directory Server 6.1 以降のバージョンでは、以下に示すさまざまな方法で、複製競合の解決機能を使用不可にすることができます。

このタスクについて

手順

1. 構成ファイルの手動編集:

構成ファイルを手動で編集して、項目「cn=master server, cn=configuration」下の属性「ibm-slappedNoReplConflictResolution」を TRUE に設定します。

変更した内容を有効にするには、この属性値を TRUE に設定した後で、サーバーを再始動するか、readconfig 操作を発行する必要があります。

2. ldapmodify ユーティリティーの使用:

以下に示すように、ldapmodify ユーティリティーを使用して、属性「ibm-slappedNoReplConflictResolution」の値を TRUE に設定することができます。-ldapmodify -D <admin_dn> -w <admin_pwd> dn: cn=master server, cn=configuration changetype: replace replace: ibm-slappedNoReplConflictResolution ibm-slappedNoReplConflictResolution: TRUE変更を有効にするには、サーバーを再始動するか、readconfig 操作を実行する必要があります。

3. Web 管理ツールの使用:

ナビゲーション領域で「複製管理」カテゴリを展開し、「複製プロパティの管理」をクリックします。

- a. 「サプライヤー情報」リストから「デフォルトの資格情報と参照」を選択して、「編集」をクリックします。
- b. 「複製の競合解決」コンボ・ボックスから、値 FALSE を選択します。
- c. 「OK」をクリックして、設定を保存します。

複製エラーの処理

複製された更新で、コンシューマーから LDAP_SUCCESS 以外の結果が戻された場合、複製エラーが発生しています。複製競合エラーでは、LDAP_OTHER と特殊なコントロールが戻されますが、サーバー構成が許容しているよりも大きいデータでない限り、エラーとしては扱われません。以下に示す情報により、その詳細を把握できます。

複製エラーのログは、データベースに保存できます。この複製エラー・ログのサイズはサーバー構成 (ibm-slappedReplMaxErrors) で設定でき、動的に更新できます。複製エラーは、複製合意ごとに保管および管理されます。したがって、2 つの合意が存在し、一方の合意でエラーが記録された場合でも、もう一方の合意ではエラーが記録されていないという場合もあります。

エラーの解決方法は複製方式によって異なります。単一スレッドの複製の場合、結果は以下ようになります。

- `ibm-slappedReplMaxErrors: 0` を指定すると、エラーはログに記録されません。また最初のエラーは成功するまで毎分再試行されるか、スキップされます。
- 複製合意のエラー数が制限に達した場合、次のエラーが成功するまで再試行されるか、スキップされるか、その複製合意のエラー数の制限が増加されるか、ログからエラーが消去されます。複製ステータス属性 `ibm-replicationChangeLDIF` により、再試行が行われている項目のデータが表示されます。
- 複製合意のステータスは以下ようになります。

```
ibm-replicationStatus: retrying
```

マルチスレッド複製の場合、以下のような処理が行われます。

- `ibm-slapdReplMaxErrors: 0` を指定すると、エラーはログに記録されません。ただし、エラーが発生した場合、すべてのエラーがクリアされるまで複製は中断されます。
- 複製合意のエラー数が制限を超えた場合、少なくとも 1 つのエラーがクリアされるまで複製は中断されるか、複製合意のエラー数の制限が増加されます。
- 複製合意のステータスは以下ようになります。

```
ibm-replicationStatus: error log full
```

複製エラーの表示について詳しくは、IBM Security Directory Server の資料の『トラブルシューティングとサポート』セクションを参照してください。

複製合意

以下に示す情報により、複製合意についての詳細を把握できます。

複製合意は、レプリカ・サブエントリーの下に作成されたオブジェクト・クラス **ibm-replicationAgreement** のディレクトリーの項目であり、サブエントリーによって表されたサーバーから別のサーバーへの複製を定義します。これらのオブジェクトは、以前のバージョンの IBM Security Directory Server で使用していた `replicaObject` 項目に似ています。複製合意は、以下の項目で構成されます。

- 合意の命名属性として使用される、わかりやすい名前。
- LDAP サーバー、ポート番号、および SSL を使用するかどうかを指定する LDAP URL。
- コンシューマー・サーバーの ID (既知の場合) -- サーバー ID が不明の場合は「unknown」。
- サプライヤーがコンシューマーにバインドするために使用する資格情報を含むオブジェクトの DN。
- (オプション) 複製のためのスケジュール情報を含むオブジェクトへの DN ポインター。この属性が存在しない場合は、変更が直ちに複製されます。
- 複製方式 (単一スレッド、またはマルチスレッド)。
- コンシューマーの数: 単一スレッド複製方式を使用する複製合意の場合、コンシューマー接続の数は必ず 1 つで、属性値は無視されます。マルチスレッド複製を使用する合意の場合、接続の数は 1 から 32 の間で構成できます。合意でこの値を指定しない場合、コンシューマー接続の数は 1 に設定されます。

注: `cn=ibmpolicies` サブツリーでは、すべての複製合意は単一スレッド複製方式、単一のコンシューマー接続を使用し、属性値は無視されます。

分かりやすい名前は、コンシューマー・サーバー名などの説明的なストリングです。

データの正確性を確保するために、サプライヤーは、コンシューマーにバインドするときにサーバー ID をルート DSE から取得し、合意の値と比較します。サーバー ID が一致しない場合は、警告がログに記録されます。

コンシューマー・サーバー ID は、トポロジーを全探索するために Web 管理ツールによって使用されます。コンシューマー・サーバー ID を指定すると、Web 管理ツールは、対応するサブエントリーとそれについての合意を検索できます。

複製合意は複製が可能であるため、資格情報オブジェクトに対する DN が使用されます。これにより、資格情報はディレクトリーの非複製領域に保管できます。資格情報オブジェクト（「平文」資格情報を取得可能なもの）を複製すると、機密漏れのリスクが生じます。cn=localhost サフィックスは、資格情報オブジェクトを作成するのにふさわしいデフォルト場所です。個別のオブジェクトを使用することによっても、さまざまな認証方法をより簡単にサポートできます。多数のオプション属性について、それぞれの意味を把握しなくとも、新しいオブジェクト・クラスを作成できます。

オブジェクト・クラスは、サポートされている認証方法ごとに定義されます。

- 単純なバインド
- SSL を使用した SASL EXTERNAL メカニズム
- Kerberos 認証

レプリカ・サブエントリーを定義せずに `ibm-replicationContext` 補助クラスをサブツリーのルートに追加することによって、複製されたサブツリーの一部を複製しないことを指定できます。

複製を構成する前に考慮する事項

LDAP 複製構成を設定する前に、考慮すべき管理責任がいくつかあります。ここで提供する情報およびリンクを活用して、それについて詳しく知ることができます。

複製が円滑に運用され、レプリカが最新の状態に保たれるようにするため、管理者は、複製状況をモニターする操作を定期的に行う必要があります。複製が正しく構成されると、更新はすべての定義済みレプリカ・サーバーに自動的に伝搬され続けます。ただし、エラーが発生すると、問題を完全に修正するために人的な介入が必要になる場合があります。

複製するためにキューに入れられた更新についての情報を表示し、特定のレプリカに対する複製を中断または再開することができるようにするインターフェースが用意されています。詳しくは、419 ページの『キューの管理』を参照してください。これらの複製キューについては、エラーがないかどうか定期的に検査してください。特定のコンシューマー・サーバーへの複製時に発生した可能性があるエラーの検査方法を理解するには、413 ページの『サーバー・エラーの表示』を参照してください。

また管理者は、複製合意の運用属性を参照することによって、詳細な状況およびエラーの情報を入手できます。入手可能な情報について詳しくは、422 ページの『複製状況のモニター』を参照してください。

複数のマスター・サーバーを構成すると、管理者が認識しておく必要がある潜在的なエラー事例の数が増えます。同じ項目がほぼ同時に 2 つの異なるマスター・サーバーで更新されると、それらの更新は、トポロジー内のその他のサーバーに複製されるときに競合する確率が高くなります。複製アルゴリズムは、追加と追加の間、または変更と変更の間における複製競合をすべて検出して解決するように設計されています。320 ページの『複製の競合解決』を参照してください。

また時刻同期製品を使用すると、LDAP サーバーを常に同期化させることができます。このようなユーティリティを、IBM Security Directory Server は提供していません。

重要: 新規のディレクトリー・サーバー・インスタンスを作成する場合、以下の情報に注意してください。複製を使用して最高のパフォーマンスを得るには、サーバー・インスタンスの暗号鍵を同期化させる必要があります。

既存のディレクトリー・サーバー・インスタンスと暗号同期化させる必要のあるディレクトリー・サーバー・インスタンスを作成する場合は、サーバーでサーバー暗号鍵が生成されるため、以下のいずれかの手順を行う前に、サーバー・インスタンス上の暗号鍵を同期させる必要があります。

- 2 番目のサーバー・インスタンスの始動
- 2 番目のサーバー・インスタンスからの、**idsbulkload** コマンドの実行
- 2 番目のサーバー・インスタンスからの、**idsldif2db** コマンドの実行

ディレクトリー・サーバー・インスタンスの同期化については、703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』を参照してください。

サブツリーに複製合意が含まれている場合、サーバーはそのサブツリーの削除を許可しません。項目の削除は任意の順番で行えるので、削除項目の複製も任意の順番で行えます。例えば、サブツリーで最初に複製合意が削除された場合、その削除操作を複製することはできません。この制約は、**-s** オプションを指定してコンテキストを削除する場合にのみ有効になります。サブツリーを削除する場合、最初に複製合意を削除する必要があります。

注: 複製を開始する前に、複製トポロジー項目を同期化させる必要があります。ネットワークでサーバーをセットアップします。

レプリカ・サーバーを構成するときは、マスター DN をレプリカ・サーバーの管理 DN の ID とは異なる ID に設定したことを確認してください。両者の DN ID を同じにすると、結合された **adminDN-masterDN ID** を使用してレプリカにバインドし、更新がレプリカに直接行われる可能性があります。そして、レプリカ・サーバーがマスター・サーバーと非同期になる可能性があります。これにより、マスターにエラーが生じ、サーバー間でのデータの不整合をもたらします。レプリカに対するすべての変更は、**masterDN** を使用してバインドするマスター・サーバーが行う必要があります。レプリカ・サーバーに対して変更を試行すると、更新プロセスを実行するために、マスター・サーバーに転送されます。

スキーマ更新およびパスワード・ポリシー更新の複製

スキーマおよびパスワード・ポリシーの更新は、**cn=ibmpolicies** サブツリーを使用した場合のみ複製されます。ここで提供する情報およびリンクを活用して、それについて詳しく知ることができます。

スキーマとパスワード・ポリシーをすべてのサーバーで同期化させるには、**cn=ibmpolicies** の追加複製コンテキストを作成する必要があります。この複製コンテキストには、ディレクトリー・トポロジー内のすべてのサーバーを含める必要があります。パスワード・ポリシー属性の複製について詳しくは、672 ページの『パスワード・ポリシー運用属性の複製』を参照してください。

注: プロキシ・サーバーを使用している場合、パスワード・ポリシーの更新は複製されます。Security Directory Server は、プロキシ・サーバーがサービスを提供する対象のすべてのバックエンド・サーバー間で複製が CN=IBMPOLICIES コンテキスト用にセットアップされている場合、複製トポロジー内でのスキーマ更新のコンシューマー・サーバーへの複製もサポートします。グローバル管理グループ・メンバーは、スキーマの更新の要求をプロキシ・サーバーを介してバックエンド・サーバーに送信できます。スキーマに対する更新について詳しくは、448 ページの『分散ディレクトリーでのスキーマの更新』を参照してください。

複製に関する以下の要件について考慮してください。

- 最適な結果を得るために、データの変更を複製する前にスキーマの変更を複製します。
- **idsldapdiff** ユーティリティを使用すると、スキーマの相違点を確認できます。ただし **idsldapdiff** ユーティリティでは、スキーマの相違点の自動訂正は行えません。
- ディレクトリー・トポロジー内のすべてのサーバー間で **cn=ibmpolicies** 項目が複製される場合は、スキーマを同期したままにすることができます。分散ディレクトリーがセットアップされている場合、ユーザーはスキーマ更新がプロキシ・サーバーを介して行われるようにする必要があります。

マスター - レプリカ・トポロジーの作成

ここで提供する情報および例に従って、マスター - レプリカ・トポロジーを作成することができます。

注: 複製トポロジーを設定する前に、**ibmslapd.conf**、**ibmslapdcfg.ksf**、および **ibmslapddir.ksf** ファイルのバックアップ・コピーを作成してください。複製で問題が発生した場合、このバックアップ・コピーを使用すれば元の構成を復元できます。

以下の図は、基本的なマスター - レプリカ・トポロジーを表しています。

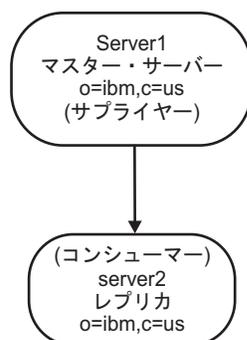


図 11. 基本的なマスター - レプリカ・トポロジー

基本的なマスター - レプリカ・トポロジーを定義するには、以下の手順を実行します。

1. マスター・サーバーを作成し、内容を定義します。複製するサブツリーを選択し、サーバーをマスターとして指定します。
2. サプライヤーが使用する資格情報を作成します。

- レプリカ・サーバーを作成します。
- レプリカにデータをエクスポートします。

注: 新規レプリカのセットアップ時に、データをレプリカにエクスポートする際、パスワード・ポリシー項目もコピーする必要があります。

以下のセクションでは、上述のタスクを実行する方法を説明します。

注: 新規の複製コンテキストのルートにする項目がサーバーのサフィックスでない場合、「サブツリーの追加」機能を使用して複製の構成情報を追加する前に、その ACL を以下のように定義しておく必要があります。

フィルターに掛けられていない ACL の場合:

```
ownersource : <the entry DN>
ownerpropagate : TRUE
aclsource : <the entry DN>
aclpropagate: TRUE
```

フィルターに掛けられた ACL の場合:

```
ownersource : <the entry DN>
ownerpropagate : TRUE
ibm-filteraclinherit : FALSE
ibm-filteraclentry : <any value>
```

ACL 要件を満たすには、項目がサーバーのサフィックスでない場合に、「項目の管理」パネルでその項目の ACL を編集します。

- 左側のナビゲーション・パネルで、「ディレクトリー管理」->「項目の管理」をクリックします。
- 項目を選択し、「アクションの選択」メニューを開きます。
- 「ACL の編集」を選択し、「実行」をクリックします。フィルターに掛けられていない ACL を追加する場合は、タブを選択し、ACL と所有者の両方について、役割が **access-id** の項目 **cn=this** を追加します。
- 「ACL の伝搬」および「所有者の伝搬」に確実にチェック・マークを付けます。「フィルターに掛けられた ACL」を追加する場合は、そのタブを選択し、ACL と所有者の両方について、役割が **access-id** の項目 **cn=this** を追加します。
- 必ず「フィルターに掛けられた ACL の累算」のチェック・マークを外し、「所有者の伝搬」にチェック・マークを付けてください。詳細については、558 ページの『ACL の処理』を参照してください。

Web 管理の使用

ここで提供される情報は、Web 管理ツールを使用してマスター・レプリカを作成しようとするときに参照できます。

このタスクについて

注: これらの手順は、関連するすべてのサーバーが IBM Security Directory Server バージョン 5.x および 6.x サーバーであることを前提としています。また、Web 管理ツールがインストール済みであること、Web 管理ツールを使用できる管理権限があることが前提となります。Web 管理ツールのインストールについて詳しくは、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。

マスター・サーバー (複製されたサブツリー) の作成:

以下に示すコマンドを発行することにより、マスター・サーバー (複製されたサブツリー) を作成することができます。

このタスクについて

注: この作業を実行するには、サーバーが稼働している必要があります。

このタスクでは、単独で複製されるサブツリーのルートを表す項目を指定し、その下に該当サーバーをそのサブツリーの単一マスターとして表す **ibm-replicasubentry** 項目を作成します。複製されたサブツリーを作成するには、複製元のサブツリーをサーバーに指定する必要があります。

注: Linux、Solaris、および HP-UX プラットフォームでは、参照を追跡しているときにクライアントがハングした場合、システム環境で環境変数 **LDAP_LOCK_REC** が設定されていることを確認します。特定の値を指定する必要はありません。

```
set LDAP_LOCK_REC=anyvalue
```

手順

1. Web 管理ツールを使用してマスター・サーバーへログオンします。
2. Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。
3. 「サブツリーの追加」をクリックします。
4. 複製するサブツリーの DN を入力するか、「参照」をクリックして項目を展開し、サブツリーのルートにする項目を選択します。この例では、「o=sample」を使用します。

注: 複製するサブツリーがサフィックスでない場合、最初にサブツリーの親をレプリカに複製する必要があります。

5. マスター・サーバー参照 URL は、LDAP URL の形式で表示されます。例を以下に示します。非 SSL の場合:

```
ldap://<myservername>.<mylocation>.<mycompany>.com:<port>
```

SSL の場合:

```
ldaps://<myservername>.<mylocation>.<mycompany>.com:<port>
```

デフォルトの URL は `ldap://localhost:389` です。

注: マスター・サーバー参照 URL はオプションです。これは以下の場合にのみ使用されます。

- サーバーが読み取り専用サブツリーを含む場合。
 - サーバーの読み取り専用サブツリーに対する更新のために戻される参照 URL を定義する場合。
6. 「OK」をクリックします。
 7. ヘッダー「複製サブツリー」の下にある「トポロジーの管理」パネルに、新しいサブツリーが表示されます。
 8. 「複製サブツリー」テーブルからサブツリーを選択し、「トポロジーの表示」をクリックします。トポロジーは、「選択されたサブツリーのトポロジー」見出し

の下に表示されます。デフォルトでは、「複製サブツリー」テーブルでサブツリーが選択可能な場合、テーブル内の最初のサブツリーのトポロジは「**選択されたサブツリーのトポロジ**」見出しの下に表示されます。トポロジ・ツリーでのノードの選択に応じて、ノード上で許可される操作は異なります。ルート以外のノードを選択したときのみ適用される操作もあります。また、ノードのタイプ (マスター・サーバー、転送サーバー、複製サーバー、ゲートウェイ・サーバーなど) に固有の操作もあります。

資格情報の作成:

資格情報は、サプライヤーがコンシューマーへのバインドに使用するメソッドおよび DN やパスワードなどの必須情報を識別します。これについての詳細は、以下の手順に示すステップを使用することで把握できます。

このタスクについて

1. まだ行っていない場合は、Web 管理ツールを使用してマスター・サーバーへログオンします。
2. Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「資格情報の管理」をクリックします。
3. 資格情報を保管する場所のリストから、**cn=replication,cn=IBMpolicies** を選択します。**注:** Web 管理ツールでは、資格情報を 3 つの場所で定義できます。397 ページの『資格情報の追加』に、作成できるその他のタイプの資格情報についての追加情報が掲載されているので参照してください。
4. 「追加」をクリックします。
5. 作成する資格情報の名前 (例: **mycreds**) を入力します。フィールドには「cn=」が事前に入力されています。
6. 認証のタイプとして「**単純なバインド**」を選択し、「次へ」をクリックします。**注:** 「**Kerberos**」または「**証明書付き SSL**」も選択できます。
 - サーバーがレプリカへのバインドに使用する DN を入力します (cn=any など)。**注:** この DN は、ご使用のサーバー管理 DN と同じにしないでください。
 - サーバーがレプリカにバインドするときに使用するパスワード (例えば、secret) を入力します。
 - タイプミスがないことを確認するため、再度パスワードを入力します。
 - 必要に応じて、資格情報の要旨を入力します。
 - 「完了」をクリックします。

注: 資格情報のバインド DN およびパスワードは、後で参照できるように記録しておいてください。

レプリカ・サーバーの作成:

以下に示す指示により、Web 管理ツールを使用してレプリカ・サーバーを作成することができます。

このタスクについて

注: このタスクを実行するには、サーバーを実行していなければなりません。

マスター・サーバー上では、以下を実行します。

1. まだ行っていない場合は、Web 管理ツールを使用してマスター・サーバーへログオンします。
2. Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。
3. 複製するサブツリーを選択して、「トポロジーの表示」をクリックします。
4. サプライヤー・サーバーを選択して、「レプリカの追加」をクリックします。
5. 「レプリカの追加」ウィンドウの「サーバー」タブで、以下の手順を実行します。

- 「サーバーのホスト名:ポート」ドロップダウン・リストから、レプリカ・サーバー用の LDAP サーバーを選択します。

コンソール・サーバーに登録されていない別のサーバーをレプリカ・サーバーとして指定する場合は、「サーバーのホスト名:ポート」ドロップダウン・リストから「以下からの項目を使用します」項目を選択し、レプリカ・サーバーのホスト名およびポート番号を `hostname:port` の形式でフィールドに入力します。デフォルトのポートは、非 SSL の場合 389、SSL の場合 636 です。

- 「SSL を使用可能にする」チェック・ボックスは未チェックのままにしておきます。
- レプリカ名を入力するか、ホスト名を使用する場合はフィールドを空白にします。
- レプリカ ID を入力します。レプリカを作成する対象のサーバーが実行中の場合、「レプリカ ID の取得」をクリックすると、このフィールドが自動的に設定されます。これは必須フィールドです。レプリカ ID が不明の場合は、**unknown** を入力します。
- レプリカ・サーバーの説明を入力します。
- マスターと通信するためにレプリカが使用する資格情報を指定します。
 - a. 「選択」をクリックします。
 - b. 「**cn=replication,cn=IBMpolicies**」の隣にあるラジオ・ボタンをクリックします。
 - c. 「資格情報の表示」をクリックします。
 - d. 「**cn=replication,cn=ibmpolicies**」を選択します。
 - e. 「資格情報の表示」をクリックします。
 - f. 「OK」をクリックします。

合意資格情報の詳細については、397 ページの『資格情報の追加』を参照してください。

6. 「追加」タブをクリックします。
 - a. 「複製スケジュールの選択または DN の入力 (オプション)」の設定は、「なし」のままにしておきます。これにより即時の複製がデフォルトとして設定されます。

- b. どの機能も選択解除しないでください。405 ページの『レプリカ・サーバーの追加』を参照してください。
- c. 「複製方式」の設定は「単一スレッド」のままにしておきます。

注: IBM Security Directory Server 6.0 以降のバージョンでのみ、複製方式を単一スレッドまたはマルチスレッドに設定できます。IBM Security Directory Server 5.x では、単一スレッドしか選択できません。

- d. 「コンシューマーに関する資格情報の追加」チェック・ボックスをクリックして選択します。

注: 資格情報が外部にある場合、IBM WebSphere Application Server 環境変数を設定する必要があります。注にある情報を参照してください。

- e. コンシューマー (レプリカ) サーバーの管理者 DN を入力します。例: cn=root。

注: サーバーの構成プロセスで作成した管理者 DN が cn=root の場合、省略せずに完全な管理者 DN を入力します。root のみを入力しないよう注意してください。

- f. コンシューマー (レプリカ) の管理者パスワードを入力します。例: secret。

注: コンシューマー・サーバーが実行されている必要があります。

- g. レプリカを作成するには、「OK」をクリックします。

注: 資格情報が存在する場合、そのことを知らせるメッセージが表示されます。資格情報が存在しない場合、資格情報が追加され、メッセージ・プロンプトが表示されます。また、サーバーを再始動するよう要求されます。さらにパネルに、2 つのポート番号、サーバーのポート番号 (このポート番号は編集できません) と管理サーバーのポート番号が表示されます。特定インスタンス用の管理サーバーのポート番号が正しいことを確認してください。誤った管理サーバーのポート番号が指定されている場合、管理サーバーはサーバーを再始動できません。

- h. 「OK」をクリックします。

注: サーバーがコンシューマーにトポロジーの追加を試行したことを知らせるメッセージが表示されます。このメッセージで追加試行が成功したかどうか確認できます。

- i. 「OK」をクリックします。

詳細については、405 ページの『レプリカ・サーバーの追加』を参照してください。

レプリカへのデータのコピー:

ここで説明する手順に従って、データをレプリカにコピーすることができます。

このタスクについて

サーバーを同期化させるには、最初にマスターを静止させる必要があります。つまり、クライアントからの更新をマスターが受信できないようにします。

手順

1. まだ行っていない場合は、Web 管理ツールを使用してマスター・サーバーへログオンします。
2. Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。
3. 複製したサブツリーを選択します。
4. サブツリーを静止するには、「静止/静止解除」をクリックします。
5. 「OK」をクリックします。

タスクの結果

次にマスターのデータをレプリカにエクスポートする必要があります。これは手動で行う手順です。

マスター・サーバーで、データの LDIF ファイルを作成します。マスター・サーバーに格納されているすべてのデータをコピーするには、`idsdb2ldif -o <masterfile.ldif> -I <instance_name> -k <key seed> -t <key salt>` コマンドを発行します。注: インスタンスが複数存在する場合は、`-I` オプションを使用する必要があります。サーバー上の鍵が同期されていない場合は、`-k` および `-t` オプションを使用する必要があります。1 つのサブツリーのデータのみをコピーする場合のコマンドは、`idsdb2ldif -o <masterfile.ldif> -s <subtreeDN> -I <instance_name> -k <key seed> -t <key salt>` です。注: インスタンスが複数存在する場合は、`-I` オプションを使用する必要があります。サーバーの鍵を同期化していない場合は、`-k` および `-t` オプションを使用する必要があります。注: `-j` オプションを指定しない場合は、`createTimestamp`、`creatorsName`、`modifiersName`、および `modifyTimestamp` の 4 つの運用属性が LDIF ファイルにエクスポートされます。

レプリカを作成しているコンピューターで、以下の手順を実行します。

1. マスターが使用するサフィックスが `ibmslapd.conf` ファイルで定義されていることを確認します。
2. レプリカ・サーバーを停止します。
3. `<masterfile.ldif>` ファイルをレプリカにコピーし、コマンド `idsldif2db -r no -i <masterfile.ldif> -I <instance name>` を発行します。複製合意、スケジュール、資格情報 (複製されたサブツリーに格納されている場合)、および項目データがレプリカにロードされます。
4. サーバーを開始します。

重要: Advanced Encryption Standard (AES) が使用可能になっているサーバーにインポートするデータをエクスポートする場合で、2 つのサーバーが暗号同期化されていない場合は、「**AES 対応宛先サーバーにデータをエクスポート**」チェックボックスを選択します。その後、「**暗号化シード**」および「**暗号化ソルト**」フィールドに入力します。(サーバーの暗号同期化については、703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』を参照してください。)

ソース・サーバー (データをエクスポートするサーバー) および宛先サーバー (データをインポートするサーバー) が一致しないディレクトリー・キー stash ファイルを使用していて、宛先サーバーの暗号化シード値および暗号化ソルト値を指定している場合、AES で暗号化されたデータはソース・サーバーの AES 鍵で暗号化解除され、さらに宛先サーバーの暗号化シード値および暗号化ソルト値で再度暗号化されます。暗号化されたデータは、LDIF ファイルに保管されます。

暗号化シードは、AES 共通鍵の値セットの生成に使用します。これらの値は、ディレクトリー stash ファイルに格納され、ディレクトリーに格納されたパスワードと共通鍵属性の暗号化および暗号化解除に使用されます。暗号化シードに含まれる文字は、33 以上 126 以下の範囲の値を持つ印刷可能な ISO-8859-1 ASCII 文字のみでなければなりません。また、最小文字数は 12、最大文字数は 1016 です。これらの文字については、647 ページの『付録 D. 33 番から 126 番までの ASCII 文字』を参照してください。

暗号化ソルトは、AES 暗号化鍵の生成に使用されたランダムに生成された値です。宛先サーバーのソルト値は、(**idsldapsearch** ユーティリティーを使用して) 宛先サーバーの「cn=crypto,cn=localhost」項目を検索することにより取得できます。属性タイプは `ibm-slapdCryptoSalt` です。

レプリカへのサブライヤー情報の追加:

以下に示す情報を使用することで、Web 管理ツール経由でサブライヤー情報をレプリカに追加することができます。

このタスクについて

コンシューマー (レプリカ) への資格情報の追加を選択しなかった場合、またはレプリカへの資格情報の追加で問題が発生した場合、レプリカの構成を変更して、どのサブライヤーがレプリカに対する変更を複製できる権限を持つかを識別できるようにする必要があります。また参照をマスターに追加する必要があります。

1. Web 管理ツールを使用して、レプリカを作成するコンピューターにディレクトリー管理者としてログオンします。
2. Web 管理ツールのナビゲーション領域で「複製管理」を展開して、「複製プロパティーの管理」をクリックします。
3. サブライヤー情報の下の「追加」をクリックします。
4. 「複製されたサブツリー」ドロップダウン・メニューからサブライヤーを選択し、「下の項目を使用してください」を選択して、サブライヤー資格情報を構成する複製サブツリーの名前を入力します。
5. 複製バインド DN を入力します。この例では `cn=any` が使用されます。
6. 資格情報パスワードを入力して確認します。この例では、`secret` を使用します。397 ページの『資格情報の追加』を参照してください。

7. 「OK」をクリックします。
8. 変更した内容を有効にするには、レプリカを再始動する必要があります。
サブライヤー情報については、414 ページの『レプリカへのサブライヤー情報の追加』を参照してください。

複製の開始:

Web 管理ツールを使用して複製を開始できます。

このタスクについて

レプリカは中断状態であり、複製は行われていません。複製トポロジーの設定が完了したら、マスターで以下の操作を行う必要があります。

1. まだ行っていない場合は、Web 管理ツールを使用してマスター・サーバーへログオンします。
2. Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「キューの管理」をクリックします。
3. 新規レプリカを選択します。
4. 「キューの詳細」をクリックします。
5. 「変更の保留」をクリックします。
6. 変更の保留がある場合、「すべてスキップ」をクリックします。変更の保留がない場合、「キャンセル」をクリックします。これにより、<masterfile.ldif> ファイルを使用してロードされたトポロジー情報の重複を防ぐことができます。新規のレプリカを複数作成した場合は、各新規サーバーに対してステップ 1 から 6 を繰り返します。
7. ナビゲーション領域で「複製管理」カテゴリの「トポロジーの管理」をクリックします。
8. 複製したサブツリーを選択します。ステータスは「静止」になるはずですが。
9. サブツリーを静止解除するには、「静止/静止解除」をクリックします。
10. 「OK」をクリックします。これでマスターはクライアントから更新を受け取り、複製キューに格納します。
11. ナビゲーション領域で「複製管理」カテゴリの「キューの管理」をクリックします。
12. レプリカを選択します。
13. 「中断/再開」をクリックして、そのサーバーの複製更新の受信を開始します。中断状態の各サーバーに対して、ステップ 10 から 13 を繰り返します。

注: マスターにプロモートする場合、マスターのキューを再開する必要があります。

キューの管理については、419 ページの『キューの管理』を参照してください。

コマンド・ラインの使用

コマンド行を使用して、以下に示すコマンドを発行することで、レプリカを作成できます。

このタスクについて

このシナリオは、複製されるサブツリーを新規に作成すること、および `server1` のみ項目データを含むことが前提となります。他のサーバーはすべて新しくインストールし、構成済みのデータベースを所有させます。

注:

```
dn: o=sample
objectclass: organization
objectclass: ibm-replicationContext
o: sample
```

上記は作成するサブツリーです。この項目がすでに存在する場合は、項目全体を追加する代わりに **objectclass=ibm-replicationContext** を追加するように変更してください。

サブツリーのレプリカを作成するには、マスターとレプリカの間に複製合意を作成する必要があります (325 ページの『複製合意』を参照)。この合意は、マスターとレプリカの両方にロードする必要があります。

2 つのサーバーは、マスターがレプリカへのサプライヤーであり、レプリカがマスターのコンシューマーであるという関係になっています。

サブツリー **o=sample** のマスター (`server1`) およびレプリカ (`server2`) を作成するには、以下のようにします。

1. マスターが存在するマシンで、合意情報を格納するファイル (*myreplicainfofile* など) を作成します。ここで、*myreplicainfofile* の内容は以下のとおりです。注: 以下のファイルで `<server1-uuid>` が出現する箇所はすべて、マスター・サーバーの **cn=Configuration** 項目の **ibm-slappedServerId** 属性に置き換えてください。この値は、サーバーを最初に始動したときにサーバーによって生成されます。また、UNIX ベースのシステムの場合は、**cn=Configuration** 項目の **idsldapsearch** を実行するか、**ibmslapd.conf** ファイルに対して **grep** コマンドを使用することによって検索できます。同様に、`<server2-uuid>` が出現する箇所はすべて、すべてレプリカ・サーバーの **cn=Configuration** 項目の **ibm-slappedServerId** 属性の値で置き換えてください。###Replication Context-needs to be on all suppliers and consumers dn:
cn=replication,cn=IBMpolicies objectclass: containerdn: o=sample
objectclass: organization objectclass: ibm-replicationContext###Copy the following setting to servers at v5.x and above.###Replica Group dn:
ibm-replicaGroup=default, o=sample objectclass: top objectclass:
ibm-replicaGroup ibm-replicaGroup: default ###Bind Credentials/method to replica server - replication agreement ###points to this. dn:
cn=server2 BindCredentials,cn=replication,cn=IBMpolicies objectclass:
ibm-replicationCredentialsSimple cn: server2 BindCredentials
replicaBindDN: cn=any replicaCredentials: secret description: Bind method of the master (server1) to the replica (server2)###Replica SubEntry dn: ibm-replicaServerId=<server1-uuid>,ibm-replicaGroup=default,o=sample objectclass: top objectclass:
ibm-replicaSubentry ibm-replicaServerId: <server1-uuid>
ibm-replicationServerIsMaster: true cn: server1 description: master server###Replication Agreement to the replica server dn:

```
cn=server2,ibm-replicaServerId=<server1-uuid>,ibm-
replicaGroup=default,o=sample objectclass: top objectclass:
ibm-replicationAgreement cn: server2 ibm-replicaConsumerId:
<server2-uuid> ibm-replicaUrl: ldap://server2:389 ibm-
replicaCredentialsDN: cn=server2 BindCredentials,cn=replication,
cn=IBMpolicies description: replica server (server2)
```

2. マスターがまだ停止していない場合は、停止します。ibmdirctl -h server1 -D <adminDN> -w <adminPW> -p 389 stop
3. マスターに新規の複製トポロジをロードするには、次のコマンドを発行します。idsldif2db -r no -i <myreplicainfofile> -I <instance name>
4. 新規レプリカを同期するために必要なすべてのデータを持つファイルを生成するには、次のコマンドを発行します。idsdb2ldif -o <masterfile.ldif> -I <instance_name> -s o=sample -k <key seed> -t <key salt>注: 複数のインスタンスがある場合は -I オプションを使用する必要があります。サーバーの鍵を同期化していない場合は、-k および -t オプションを使用する必要があります。
重要: Advanced Encryption Standard (AES) が使用可能になっているサーバーにインポートするデータをエクスポートする場合において、2 つのサーバーが暗号同期化されていない場合は、サーバーの暗号同期化について、703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』を参照してください。また、注も参照してください。
詳しくは、「IBM Security Directory Server Version 6.3 Command Reference」の **idsdb2ldif** コマンド情報を参照してください。注: **ステップ 5 からステップ 9** は、server2 が配置されているマシンで実行してください。
5. <masterfile.ldif> をレプリカにコピーします。
6. 構成専用モードで、レプリカの server2 を始動させます。idsslapd -I <instance name> -a
7. 元の ibmslapd.conf、ibmslapdcfg.ksf、および ibmslapddir.ksf ファイルのバックアップがあるか確認します。
8. server2 を構成してレプリカ・サーバーにする必要があります。**idsldapadd** コマンドを使用し、server2 の **ibmslapd.conf** ファイルに以下の項目を追加します。server2 で、次のコマンドを発行します。idsldapadd -D <adminDN> -w<adminPW> -i<filename> ここで、<filename> は次のとおりです。dn: cn=Master Server, cn=configuration objectclass: ibm-slapdReplication cn: Master Server ibm-slapdMasterDN: cn=any ibm-slapdMasterPW: secret ibm-slapdMasterReferral: ldap://server1:389/注: ibm-slapdMasterDN 値および ibm-slapdMasterPW 値は、ステップ 1 の項目「cn=server2 BindCredentials」で、マスター・サーバーである server1 に格納されている値と一致している必要があります。
9. レプリカ server2 を停止します。サーバーを停止するには、次のコマンドを発行します。ibmdirctl -h server2 -D <AdminDN> -w <Adminpwd> -p 389 stop
10. **ibmslapd.conf** ファイルを新規バックアップとして保管します。
11. 次のコマンドを発行します。idsldif2db -r no -i <masterfile.ldif> -I <instance name>

12. マスター (server1) およびレプリカ (server2) を始動します。各サーバーで、次のコマンドを発行します。idsslapd -I <LDAPinstance>

パスワード・ポリシー運用属性の複製

複製トポロジー内に一貫性を確保してパスワード・ポリシーをインプリメントするには、トポロジー内のすべてのサーバーに対して、特定のパスワード・ポリシー運用属性を複製する必要があります。

複製環境内にパスワード・ポリシーをインプリメントするには、cn=ibmpolicies サブツリーのすべてのコンシューマーに対して、グローバル・パスワード・ポリシー項目 cn=pwdpolicy, cn=ibmpolicies を複製する必要があります。ユーザーのパスワード・ポリシー関連の詳細は、ユーザー項目のパスワード・ポリシー運用属性内に格納されます。これらの運用属性は、ユーザー項目のアカウント・アクセス操作およびロックアウト操作を管理します。すべてのサーバーのパスワード・ポリシー項目を同一にするには、cn=ibmpolicies 項目の下でパスワード・ポリシー項目を定義します。すべてのサーバーに対して、パスワード・ポリシー運用属性が複製されます。これらの複製更新を受け取ったサーバーは、これらの更新を記録するかどうかを決定します。

マスターが読み取り専用のレプリカに対して、ユーザー項目のパスワード・ポリシー運用属性 (pwdAccountLockedTime、pwdExpirationWarned、pwdFailureTime、pwdGraceUseTime など) を複製する際には、これらの値は記録されません。同様に、読み取り専用レプリカ・サーバー上でユーザー項目のこれらの属性に変更を加えても、個別のマスター・サーバー上では更新されません。書き込みレプリカ (ピア・サーバー) 間でパスワード・ポリシーに一貫性を持たせる場合は、書き込みレプリカがこれらの運用属性を複製して記録します。このため、これらの属性の複製は、現在のディレクトリー・サーバーの要件に基づいて考慮する必要があります。

6.3.0.10 より前のサーバーでは、パスワード失敗、猶予ログイン、およびアカウント・ロックの数は、各読み取り専用レプリカでユーザーに対して個別に更新されます。複製トポロジーの場合、ユーザーは、実施されているパスワード・ポリシーで定義されている回数を超えてサーバーに対してバインド操作を実行できます。また、一部のサーバーでバインドが失敗した場合でも、これらの追加バインド操作を使用できます。

ユーザーに設定されているパスワード失敗の有効なカウントが M (pwdMaxFailure 属性の値) である場合、マスター・レプリカ・トポロジー上のユーザーは $N * M$ 回試行することができます。N はサーバーの数で、M は pwdMaxFailure 属性の値です。サーバーの数 N のうち、書き込みレプリカのカウントは 1 と見なされます。ピア・サーバーでユーザー項目のパスワード・ポリシー運用属性が更新されると、それらの更新はすべての書き込みレプリカに複製されます。残りの N-1 のサーバーは、読み取り専用レプリカのカウントです。各読み取り専用レプリカでは、ユーザー項目のパスワード・ポリシー運用属性に対する更新が独自のデータベースに格納されます。

管理者は、パスワード・ポリシー運用属性の複製を使用して、複製トポロジー内で強力なパスワード・ポリシーを実施できます。ユーザーのパスワード・ポリシー運用属性が、読み取り専用レプリカ・サーバーを含む、すべてのサーバーで更新されていることを確認できます。この機能により、資格情報が無効であるため

LDAP_INVALID_CREDENTIAL エラーが発生したバインドは、無効なバインドであると見なされます。資格情報が有効で成功したバインドは、有効なバインドであると見なされます。

パフォーマンスを向上させるために、複製トポロジー内のサーバー・インスタンスを暗号同期化する必要があります。

すべてのサーバー間で一貫性を確保してパスワード・ポリシー運用属性を複製するには、複製が以下の条件を満たしている必要があります。

- 複製トポロジー内のすべてのサーバーで必要なサブツリーすべてに対して、リアルタイム複製が設定されている。
- すべてのサーバーにおいてパスワード・ポリシーが設定されている。
- 複製トポロジー内のすべてのサーバーにおいて、ユーザーがバインドの試行に失敗したカウントが同期化されている。
- 複製に参加しているすべてのサーバーにおいて機能が有効になっている。また、以下の属性も設定する必要があります。
 - 読み取り専用レプリカに必要な複製コンテキストに対して `ibm-replicareferralURL` 属性を追加します (存在しない場合)。
 - 複製に参加しているすべてのサーバーにおいて、`ibm-slapdReplicateSecurityAttributes` 属性を `true` に設定します。

注: この機能において、`ibm-slapdMasterReferral` 属性の使用方法に関して変更はありません。

ルート DSE 検索結果

複製トポロジー内のサーバーが以下の操作をサポートしている場合、ルート DSE 検索により `1.3.18.0.2.32.105` という OID 値を持つ `ibm-supportedCapabilities` 属性が返されます。

- 読み取り専用レプリカは、パスワード・ポリシー運用属性の複製の更新を受け入れます。読み取り専用レプリカは、ユーザーのパスワード・ポリシー運用属性に影響するバインド操作をマスター・サーバーに通知できます。
- マスター・サーバーは、ユーザーのパスワード・ポリシー運用属性に影響するバインド操作に関する通知を読み取り専用レプリカから受け取ることができます。

この機能がサーバーで正常に構成されている場合は、ルート DSE 検索を実行すると、`1.3.18.0.2.32.105` という OID 値を持つ `ibm-enabledCapabilities` 属性が返されます。

また、ルート DSE 検索を実行して、`ibm-slapdReplicateSecurityAttributes` 属性に割り当てられている値を確認することもできます。この属性値が `true` である場合、サーバーはパスワード・ポリシー運用属性の複製をサポートしています。

複製トポロジーにおけるサーバーのパフォーマンス

ユーザーが読み取り専用レプリカに対してバインド操作を試みると、以下の操作が行われます。

1. バインド操作がユーザーのパスワード・ポリシー運用属性に影響を与えるかどうかを確認します。

2. マスター・サーバーを識別し、バインド操作に関して通知します。
3. バインド操作を読み取り専用レプリカからマスター・サーバーに伝搬します。

これらの操作を完了するために、読み取り専用レプリカ・サーバーはさらに処理を行います。この結果、セキュリティ機能拡張に対するトレードオフとして、読み取り専用レプリカ・サーバーのパフォーマンスが低下する場合があります。

監査およびログの情報

サーバーは、パスワード・ポリシー運用属性の複製に関連する情報を以下のログ・ファイルに記録します。

- 監査機能が設定されている場合、読み取り専用レプリカは、以下の情報を `audit.log` ファイルに記録します。
 - 失敗したバインド操作および成功したバインド操作を含む、バインド操作の詳細。
- 読み取り専用レプリカは、読み取り専用レプリカに対してバインドおよびマスター・サーバーへの通知を要求する以下の操作を `audit.log` ファイルに記録します。
 - 読み取り専用レプリカ・サーバー上のユーザーのパスワード・ポリシー運用属性に影響を与えるすべてのバインド要求。

管理者はこれらのログを使用して、サーバーが開始して完了した操作を確認することができます。

- サーバーは、`ibm-slapdReplicateSecurityAttributes` 属性値を `ibmslapd.log` および `traceibmslapd.log` ファイルに記録します。
- 読み取り専用レプリカにバインドの通知先となるマスターのリストが含まれていない場合、サーバーは該当するメッセージを `ibmslapd.log` ファイルに記録します。
- また、読み取り専用レプリカは、ユーザー項目に対して更新された、パスワード失敗のタイム・スタンプを `traceibmslapd.log` ファイルに記録します。読み取り専用レプリカが記録するパスワード失敗のタイム・スタンプのソースは以下のとおりです。
 - 読み取り専用レプリカが最後に生成したタイム・スタンプ。
 - マスター・サーバーからの応答制御内のタイム・スタンプ。
 - マスター・サーバーから複製されたタイム・スタンプ。
- 複製トポロジー内のサーバーは、すべての失敗パス・エラー・メッセージを `traceibmslapd.log` ファイルに記録します。

パスワード・ポリシー運用属性の複製用に構成する属性

複製トポロジー内のすべてのサーバー間でパスワード・ポリシー運用属性を複製するには、`ibm-replicareferralURL` および `ibm-slapdReplicateSecurityAttributes` 属性を構成します。サーバー間で複製を構成する場合は、これらの属性を設定する必要があります。

パスワード・ポリシー運用属性を複製するには、`ibm-slapdReplicateSecurityAttributes` 属性を `TRUE` に設定します。複製トポロジー内のすべてのサーバーにおいて、`ibm-slapdReplicateSecurityAttributes` 属性を設定

する必要があります。この属性を設定すると、デフォルトの動作が上書きされ、マスター・サーバーと読み取り専用レプリカ・サーバーの間でパスワード・ポリシーの運用属性が伝搬されます。構成ファイル内の `cn=Replication`, `cn=configuration` 項目の下に `ibm-slapdReplicateSecurityAttributes` 属性を追加する必要があります。

複製のコンテキストでは、1 つの読み取り専用レプリカ・サーバーに対して複数のマスター・サーバーを構成することができます。読み取り専用レプリカに対するバインドがユーザーのパスワード・ポリシー運用属性に影響を与えることをマスターに通知するには、読み取り専用レプリカで `ibm-replicareferralURL` 属性を追加します。読み取り専用レプリカは `ibm-replicareferralURL` 属性を使用して、通知する必要があるマスター・サーバーを識別します。必要なすべての複製コンテキストにおいて、読み取り専用レプリカで `ibm-replicareferralURL` 属性を追加する必要があります。読み取り専用レプリカ・サーバーの `ibm-replicareferralURL` 属性には、マスター・サーバーの有効な IP アドレスまたは完全修飾ドメイン・ネームをポートとともに設定します。マスター・サーバーがセキュアな接続と非セキュアな接続の両方を受け入れている場合は、属性においてセキュアな URL (`ldaps://server`) および非セキュアな URL (`ldap://server`) を構成することができます。読み取り専用レプリカは、鍵データベース・ファイル、ラベル、および証明書を使用して、マスター・サーバーとの間でセキュアな接続を確立します。読み取り専用レプリカおよびマスター・サーバーは、両方のサーバーに共通で最もセキュアなプロトコルを使用して、セキュアな接続を確立します。読み取り専用レプリカおよびマスター・サーバーは、両方のサーバーにおいてセキュアなプロトコル用にサポートされている最もセキュアな暗号に対してネゴシエーションを行います。

ネットワーク障害またはその他の理由により、リスト内の最初のマスターが使用できない場合、要求は次のマスターに送信されます。リスト内のマスター・サーバーのいずれかに到達できる場合でも、読み取り専用レプリカは、そのマスター・サーバーに対してバインド要求に関する通知を行います。以下の例は、2 つのマスター・サーバー項目を持つ `ibm-replicareferralURL` 属性を示しています。

```
ibm-replicareferralURL: ldap://server1:port ldaps://server1:sec_port ldaps://server2:sec_port
```

重要: 機能を適切に動作させるために、`ibm-slapdReplicateSecurityAttributes` および `ibm-replicareferralURL` の両方の属性を設定する必要があります。

パスワード・ポリシー運用属性の複製の構成:

マスターと読み取り専用レプリカの間でパスワード・ポリシー運用属性を同期化するために、複製トポロジー内で機能を構成します。

始める前に

パスワード・ポリシー運用属性を複製するには、以下のタスクを完了する必要があります。

- パスワード・ポリシーを構成します。『グローバル・パスワード・ポリシーの設定』を参照してください。
- トポロジー内でマスターおよび読み取り専用レプリカを含む複製を構成します。『マスター - レプリカ・トポロジーの作成』を参照してください。

手順

1. インスタンス所有者としてログインします。
2. 複製トポロジー内のすべてのサーバーにおいて、`ibm-slapdReplicateSecurityAttributes` 属性を構成します。

```
idsldapmodify -h host_name -p port -D adminDN -w adminDN -i file.ldif
```

`file.ldif` には、以下の項目が格納されています。

```
dn: cn=Replication, cn=configuration
changetype: modify
add: ibm-slapdReplicateSecurityAttributes
ibm-slapdReplicateSecurityAttributes: true
```

3. 複製コンテキストに対して、`ibm-replicareferralURL` 属性が構成されているかどうかを確認します。

```
idsldapsearch -h host_name -p port -D adminDN -w adminDN
-s one -b replication_context objectclass=*
```

4. 読み取り専用レプリカ・サーバーでは、複製コンテキストごとに、すべてのマスター・サーバーの IP アドレスとポートを使用して `ibm-replicareferralURL` 属性を構成します。

- `ibm-replicareferralURL` 属性が構成されていない場合は、以下のコマンドを実行します。

```
idsldapmodify -l -h host_name -p port -D adminDN -w adminDN -i ref_file.ldif
```

`ref_file.ldif` には、以下の項目が格納されています。

```
dn: cn=ibmpolicies
changetype: modify
add: ibm-replicareferralURL
ibm-replicareferralURL: ldap://server1:port1 ldaps://server2:port2
```

- `ibm-replicareferralURL` 属性が構成されている場合は、以下のコマンドを実行します。

```
idsldapmodify -l -h host_name -p port -D adminDN -w adminDN -i ref_file1.ldif
```

`ref_file1.ldif` には、以下の項目が格納されています。

```
dn: cn=ibmpolicies
changetype: modify
replace: ibm-replicareferralURL
ibm-replicareferralURL: ldap://server1:port1 ldaps://server2:port2
```

5. ディレクトリー・サーバーおよび管理サーバーを再始動します。

```
ibmslapd -I dsrdbm01 -k
ibmdiradm -I dsrdbm01 -k
ibmslapd -I dsrdbm01 -n
ibmdiradm -I dsrdbm01
```

パスワード・ポリシー運用属性の複製を使用したバインド・シナリオ

一貫性を確保してパスワード・ポリシー運用属性の複製を構成するには、サーバーがバインド試行に対して応答する方法について理解しておく必要があります。

ユーザーによるバインド操作がユーザーのパスワード・ポリシー属性に影響を与える場合、マスター・サーバーはユーザー項目の更新をデータベースに記録します。次にマスター・サーバーは、複製トポロジー内の他のサーバーに更新を複製します。読み取り専用レプリカでこの機能が有効になっている場合、サーバーは複製の更新で受け取ったパスワード・ポリシー運用属性を更新します。読み取り専用レプリカでこの機能が無効になっている場合、サーバーは複製の更新で受け取ったパスワード・ポリシー運用属性を更新しません。

マスター・サーバーおよび読み取り専用レプリカ・サーバーでこの機能が有効になっているかどうかに応じた、以下のバインド・シナリオを想定することができます。

シナリオ 1: パスワード・ポリシー運用属性を更新した、読み取り専用レプリカでの無効なバインド

読み取り専用レプリカでユーザーが無効なバインドを試みた場合、レプリカは識別したマスター・サーバーに対して以下の値を通知します。

- ユーザー資格情報。
- 複製バインド失敗のタイム・スタンプ・コントロール。

マスター・サーバーは、ユーザーのパスワード・ポリシー運用属性に対する更新をデータベースに記録し、次にその更新を他のサーバーに複製します。同時に、マスター・サーバーは、読み取り専用レプリカに対する応答で、コントロール内のパスワード失敗のタイム・スタンプを送信します。読み取り専用レプリカは、データベース内にあるユーザーのパスワード・ポリシー運用属性を、マスター・サーバーから受信したタイム・スタンプで更新します。

シナリオ 2: パスワード・ポリシー運用属性を更新した、読み取り専用レプリカでの有効なバインド

ユーザーがマスターまたは読み取り専用レプリカでのバインドに成功した場合、そのバインドにより、ユーザーのパスワード・ポリシー運用属性が更新されている可能性があります。ユーザー項目にパスワード失敗のタイム・スタンプが含まれている場合、以下の条件がすべて満たされると、そのユーザーについてバインドが成功したときに、その値がリセットされます。

- ユーザー・アカウントがロックされていない。
- ユーザー項目内に最低 1 つのパスワード失敗のタイム・スタンプがある。

無効なバインドが何回も行われた後に読み取り専用レプリカでユーザーがバインドを行い、さらにアカウントがロックされていない場合、サーバーはパスワード・ポリシー運用属性を更新します。バインドに成功すると、読み取り専用レプリカ・サーバー上のユーザーのパスワード失敗のタイム・スタンプの記録がクリアされます。同時に、読み取り専用レプリカは、ユーザー資格情報を使用してマスターに通知します。マスター・サーバーは、データベースにあるユーザーのパスワード・ポリシー運用属性を更新します。バインドに成功すると、マスター・サーバー上のユーザーのパスワード失敗のタイム・スタンプの記録がクリアされます。

ユーザーがバインド操作を試みた場合、ユーザー項目のタイム・スタンプは変更されません。このため、マスター・サーバーと読み取り専用レプリカ・サーバーの間で複製の競合は発生しません。パスワード・ポリシーが設定されている場合、バインド操作のパスワード・ポリシー運用属性が変更されます。これらの変更により、`modifyTimestamp` 属性が更新されることはありません。ユーザー項目の `modifyTimestamp` 属性は変更されないため、複製の競合は発生しません。

機能を持たないサーバーまたは機能が無効であるサーバーとの互換性

以下のバージョンまたは構成のマスター・サーバーでは、複製のバインド失敗のタイム・スタンプ・コントロールは認識されません。

- 6.3.0.10 より前のバージョンのマスター・サーバー
- 6.3.0.10 以降で機能が無効であるマスター・サーバー

このため、マスター・サーバーは、読み取り専用レプリカ・サーバーに対してコントロールによってパスワード失敗のタイム・スタンプは返しません。マスター・サーバーからのタイム・スタンプが受信されない場合、読み取り専用レプリカは、ユーザー項目内のパスワード失敗のタイム・スタンプをそれ自体のタイム・スタンプで更新します。読み取り専用レプリカがそれ自体のタイム・スタンプを記録することにより、ユーザー試行が、設定された最大の失敗カウントに制限されます。読み取り専用レプリカ・サーバーがマスター・サーバーからタイム・スタンプを受信していない場合、ユーザーは、読み取り専用レプリカ・サーバーにおいて追加のバインド操作を試行することができます。

ユーザーが最大の失敗カウントに到達する前に、読み取り専用レプリカにおいてユーザー・アカウントがロックされてしまうことがあります。例えば、サーバーで有効な最大失敗カウントが 2 に設定されているとします。読み取り専用レプリカでユーザーが無効なバインドを 1 回試みると、パスワード失敗のタイム・スタンプが記録され、失敗カウントが 1 に設定されます。複製のスケジュールが設定されている場合は、スケジュール済み時間に従って、マスター・サーバーからの更新が複製トポロジ内の他のサーバーに複製されます。パスワード失敗のタイム・スタンプがユーザー項目に記録されているタイム・スタンプと異なる場合は、複製の更新によりパスワード失敗のカウントが 2 に設定されることがあります。この例では、許可されている最大失敗カウントが 2 であるため、ユーザー・アカウントがロックされます。

この機能は、以前のバージョンでは使用できません。パスワード・ポリシー運用属性への更新は、マスター・サーバーと読み取り専用レプリカ・サーバーの両方において既存の設計に従って処理されます。

ibm-replicateSecurityAttribute 属性を持つ複製トポロジ内のサーバー:

読み取り専用レプリカは、ibm-replicateSecurityAttribute 属性に設定されている値に基づくマスターからのパスワード・ポリシー運用属性による複製の更新を記録します。

マスターと読み取り専用レプリカ間のパスワード・ポリシー運用属性の更新を要約すると、以下の条件を設定します。

- 複製を構成します。
- パスワード・ポリシーを構成します。
- 読み取り専用レプリカ・サーバーにおいて、ibm-replicareferralURL 属性を、すべてのマスター・サーバーの IP アドレスまたは完全修飾ドメイン名およびポートで設定します。

読み取り専用レプリカがタイム・スタンプをそれ自体のデータベースに記録するソースは、以下の条件に応じて異なる場合があります。

- マスター・サーバーの可用性。
- マスター・サーバーおよび読み取り専用レプリカ・サーバーでの `ibm-replicateSecurityAttribute` 値。
- バインドの結果。

表 34. マスター・サーバーでの無効なバインドの場合の、*ibm-replicateSecurityAttribute* 値とパスワード・ポリシー運用属性の更新の間の関係

シナリオ	ibm-replicateSecurityAttribute 属性値		パスワード・ポリシー運用属性に対する更新	
	マスター・サーバー	読み取り専用レプリカ・サーバー	マスター・サーバー	読み取り専用レプリカ・サーバー
1	TRUE	TRUE	YES	YES*
2	TRUE	FALSE/設定なし	YES	NO
3	FALSE/設定なし	TRUE	YES	YES*
4	FALSE/設定なし	FALSE/設定なし	YES	NO

注: YES* は、読み取り専用レプリカがマスター・サーバーからの複製の更新を記録して、パスワード・ポリシー運用属性を記録することを示します。

表 35. 読み取り専用レプリカ・サーバーでの無効なバインドの場合の、*ibm-replicateSecurityAttribute* 値とパスワード・ポリシー運用属性の更新の間の関係

シナリオ	ibm-replicateSecurityAttribute 属性値		コントロールによる無効なバインドの通知	コントロール内のタイム・スタンプによる読み取り専用レプリカへの応答	パスワード・ポリシー運用属性に対する更新	
	マスター・サーバー	読み取り専用レプリカ・サーバー			マスター・サーバー	読み取り専用レプリカ・サーバー
1	TRUE	TRUE	YES	YES	YES	YES
2	TRUE	FALSE/設定なし	NO	NO	NO	YES*
3	FALSE/設定なし	TRUE	YES	NO	YES	YES**
4	FALSE/設定なし	FALSE/設定なし	NO	NO	NO	YES*

注:

- YES* は、読み取り専用レプリカが、読み取り専用レプリカでのバインド結果に基づいてパスワード・ポリシー運用属性を更新することを示しています。読み取り専用レプリカ・サーバーは、マスター・サーバーにパスワード・ポリシー運用属性の更新を通知しません。このため、マスター・サーバーは、複製トポロジー内の他のサーバーにこれらの更新を複製しません。
- YES** は、読み取り専用レプリカが、読み取り専用レプリカでのバインド結果に基づいてパスワード・ポリシー運用属性を更新することを示しています。読み取り専用レプリカ・サーバーは、マスター・サーバーにパスワード・ポリシー運用属性の更新を通知します。このため、マスター・サーバーは、複製トポロジー内の他のサーバーにこれらの更新を複製します。

表 36. マスター・サーバーでの有効なバインドの場合の、*ibm-replicateSecurityAttribute* 値とパスワード・ポリシー運用属性の更新の間の関係

シナリオ	ibm-replicateSecurityAttribute 属性値		パスワード・ポリシー運用属性に対する更新	
	マスター・サーバー	読み取り専用レプリカ・サーバー	マスター・サーバー	読み取り専用レプリカ・サーバー
1	TRUE	TRUE	YES	YES*
2	TRUE	FALSE/設定なし	YES	NO
3	FALSE/設定なし	TRUE	YES	YES*
4	FALSE/設定なし	FALSE/設定なし	YES	NO

注: YES* は、読み取り専用レプリカがマスター・サーバーからの複製の更新を記録して、パスワード・ポリシー運用属性を記録することを示します。

表 37. 読み取り専用レプリカ・サーバーでの有効なバインドの場合の、`ibm-replicateSecurityAttribute` 値とパスワード・ポリシー運用属性の更新の間の関係

シナリオ	ibm-replicateSecurityAttribute 属性値		コントロールによる無効なバインドの通知	コントロール内のタイムスタンプによる読み取り専用レプリカへの応答	パスワード・ポリシー運用属性に対する更新	
	マスター・サーバー	読み取り専用レプリカ・サーバー			マスター・サーバー	読み取り専用レプリカ・サーバー
1	TRUE	TRUE	YES	YES	YES	YES
2	TRUE	FALSE/設定なし	NO	NO	NO	YES*
3	FALSE/設定なし	TRUE	YES	NO	YES	YES**
4	FALSE/設定なし	FALSE/設定なし	NO	NO	NO	YES*

注:

- YES* は、読み取り専用レプリカが、読み取り専用レプリカでのバインド結果に基づいてパスワード・ポリシー運用属性を更新することを示しています。読み取り専用レプリカ・サーバーは、マスター・サーバーにパスワード・ポリシー運用属性の更新を通知しません。このため、マスター・サーバーは、複製トポロジー内の他のサーバーにこれらの更新を複製しません。
- YES** は、読み取り専用レプリカが、読み取り専用レプリカでのバインド結果に基づいてパスワード・ポリシー運用属性を更新することを示しています。読み取り専用レプリカ・サーバーは、マスター・サーバーにパスワード・ポリシー運用属性の更新を通知します。このため、マスター・サーバーは、複製トポロジー内の他のサーバーにこれらの更新を複製します。

パスワード・ポリシー運用属性の複製のトラブルシューティング

複製環境に関するトラブルシューティングを行うには、パスワード・ポリシー運用属性の複製機能を使用して問題を特定し、修正する必要があります。

- 複製トポロジー内の一部のサーバーで機能を設定していない場合は、パスワード・ポリシー運用属性値で不整合が生じる場合があります。
- パスワード・ポリシー運用属性の複製を構成する場合は、すべてのユーザーのパスワード失敗のカウントを同期化する必要があります。パスワード失敗のカウントを同期化しないと、サーバーでのユーザーによるバインドが成功しても、他のサーバーでの失敗のカウントがリセットされない場合があります。例えば、マスターに 2 回の無効なバインド試行が含まれており、読み取り専用レプリカにはユーザーの無効なバインド試行が含まれていないとします。機能を有効にすると、読み取り専用レプリカでユーザーによるバインドが成功しても、マスターでのパスワード失敗のカウントはリセットされません。マスターでパスワード失敗のカウントがリセットされないのは、読み取り専用レプリカでのパスワード失敗のカウントが 0 であったためです。
- 以下のいずれかの条件で、サーバーはユーザーのパスワード失敗のカウントをリセットします。
 - ユーザー・アカウントがロックされていないときに、ユーザーによるバインドが成功した場合。
 - 管理者がマスター・サーバーでユーザー・アカウントをアンロックした場合。これにより、他のすべてのサーバーでユーザー・アカウントがアンロックされます。

例外的なケースとして、パスワード管理者が特定のサーバーでユーザー・アカウントをアンロックすることが必要になる場合があります。例えば、複製トポロジ

ーがマスターおよび読み取り専用レプリカから構成されているとします。両方のサーバーで機能は有効になっています。最大の失敗試行は 3 に設定されています。この場合、2 回の無効なバインド試行後、マスターおよび読み取り専用レプリカでは、それぞれのサーバーでユーザーのパスワード失敗のカウン트가 2 と記録されます。マスター・サーバーに障害が発生した場合、読み取り専用レプリカで無効なバインドが行われるとパスワード失敗のカウン트가 3 になるため、ユーザー・アカウントがロックされます。マスターではそのユーザーのパスワード失敗のカウン트는 2 のままです。マスター・サーバーが使用可能になったときに、マスター・サーバーでユーザーによるバインドが成功すると、パスワード失敗のカウン트가 0 にリセットされます。ただし、マスター・サーバーでバインドが成功しても、読み取り専用レプリカではこのユーザーのパスワード失敗のカウン트는 0 にはリセットされません。これは、ユーザー・アカウントが既にロックされているためです。このシナリオでは、パスワード管理者が読み取り専用レプリカでのユーザー・アカウントをアンロックして、ユーザーがサーバーにアクセスできるようにする必要があります。

- ユーザーがマスター・サーバーで連続して無効なバインドを試みると、サーバーは、ユーザーについて同じタイム・スタンプを持つ複数の `pwdFailureTime` 項目を記録します。マスター・サーバーがこれらの更新を複製すると、読み取り専用レプリカは、そのユーザーについて異なるタイム・スタンプ値を持つ `pwdFailureTime` 項目のみを記録します。このため、マスター・サーバーに同じタイム・スタンプ値を持つ複数の `pwdFailureTime` 項目が含まれている場合、読み取り専用レプリカはユーザーについて 1 つの `pwdFailureTime` 項目のみを記録します。読み取り専用レプリカでは、同じタイム・スタンプ値を持つ残りの項目は記録されません。以下の例は、ポート 389 上のマスター・サーバーおよびポート 2389 上の読み取り専用レプリカからの、複数の `pwdFailureTime` 項目を持つユーザー項目を示しています。

```
#idsldapsearch -p 389 -D adminDN -w adminPWD -s sub -b cn=user02,o=sample%
objectclass=* +ibmpwdpolicy
cn=user02,o=sample
pwdChangedTime=20110914053218.807758Z
pwdAccountLockedTime=20111014080533.000000Z
pwdFailureTime=20111014080532.000000Z
pwdFailureTime=20111014080532.000000Z
pwdFailureTime=20111014080533.000000Z
#
#idsldapsearch -p 2389 -D adminDN -w adminPWD -s sub -b cn=user02,o=sample%
objectclass=* +ibmpwdpolicy
cn=user02,o=sample
pwdChangedTime=20110914053218.807758Z
pwdAccountLockedTime=20111014080533.000000Z
pwdFailureTime=20111014080532.000000Z
pwdFailureTime=20111014080533.000000Z
#
```

- マスターで `pwdGraceLoginLimit` 属性が設定されていて、パスワードの期限が切れた後にユーザーがこのサーバーでバインドを行った場合、サーバーは `pwdGraceUseTime` 項目を記録します。マスター・サーバーがこれらの更新を複製すると、読み取り専用レプリカは、ユーザー項目内で異なるタイム・スタンプ値を持つ `pwdGraceUseTime` 項目のみを記録します。このため、マスター・サーバーに同じタイム・スタンプ値を持つ複数の `pwdGraceUseTime` 項目が含まれている場合、読み取り専用レプリカはそのユーザーについて 1 つの `pwdGraceUseTime` 項目のみを記録します。読み取り専用レプリカでは、同じタイム・スタンプ値を持つ残りの項目は記録されません。以下の例は、ポート 3389 上のマスター・サーバーおよびポート 13389 上の読み取り専用レプリカからの、複数の `pwdGraceUseTime` レコードを持つユーザー項目を示しています。

```
#idsldapsearch -p 3389 -D adminDN -w adminPWD -s sub -b cn=user01,o=sample%
objectclass=* +ibmpwdpolicy
cn=user01,o=sample
pwdChangedTime=20111014103004.000000Z
pwdExpirationWarned=20111014103143.000000Z
pwdHistory=20111014102507Z#2.5.4.35#32#{AES256}gXurNKCz6CYR0t8miTtVRw==
pwdHistory=20111014103004Z#2.5.4.35#32#{AES256}lyfDaLmvJ7RpW42kDKSN+A==
pwdGraceUseTime=20111014103305.000000Z
pwdGraceUseTime=20111014103308.000000Z
pwdGraceUseTime=20111014103308.000000Z
#
#idsldapsearch -p 3389 -D adminDN -w adminPWD -s sub -b cn=user01,o=sample%
objectclass=* +ibmpwdpolicy
cn=user01,o=sample
pwdChangedTime=20111014103004.000000Z
pwdExpirationWarned=20111014103143.000000Z
pwdGraceUseTime=20111014103305.000000Z
pwdGraceUseTime=20111014103308.000000Z
#
```

ピア複製を持つ単純なトポロジーのセットアップ

ピア複製は、複数のサーバーがマスターである複製トポロジーです。ここで提供する情報に従って、ピア複製を行う単純なトポロジーをセットアップできます。

ピア複製は、更新ベクトルが既知の環境のみで使用してください。ディレクトリー内の特定のオブジェクトに対する更新は、1つのピア・サーバーのみで行う必要があります。これは、あるサーバーがオブジェクトを削除した後に、別のサーバーがそのオブジェクトに対して変更操作を行うのを防ぐためです。このようなことが発生すると、ピア・サーバーはオブジェクトの削除コマンドを受信した後に、その同じオブジェクトに対する変更コマンドを受信し、結果として競合が発生してしまいます。複製された削除要求および名前変更要求は、競合解決なしで受け取った順番で適用されます。競合解決の詳細については、417ページの『複製スケジュールの作成』を参照してください。

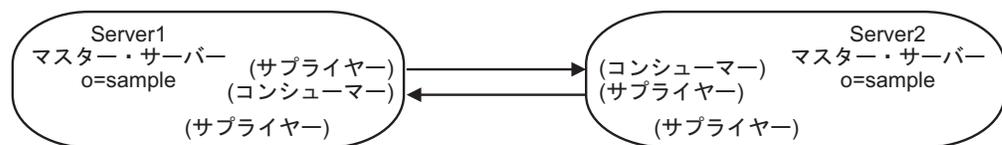


図 12. 基本的なピアツーピア・トポロジー

このセクションでは、2つのサーバー間のみで複製トポロジーを設定する方法を説明します。

Web 管理の使用

ここで提供する情報に従い、Web 管理ツールを使用してサブツリーを作成することができます。

このタスクについて

開始する前に、以下の点を確認してください。

1. 両方のサーバーが稼働中であること。
2. 両方のサーバーが暗号同期化されていること (必要な場合)。IBM Security Directory Server の資料の『管理』セクションで、『703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』』を参照してください。
3. Web 管理ツールで、該当のサーバーの 1 つにログインしていること。(この手順では、2つのうちの最初のサーバーである server1 にログインするとします。)

2 つのピア・マスターをセットアップするには、以下のようになります。

手順

1. Web 管理ツールのナビゲーション領域で「複製管理」カテゴリーを展開し、「トポロジーの管理」をクリックします。
2. 複製するサブツリーを選択し、「トポロジーの表示」をクリックします。既存のトポロジーを表示する場合は、既存のサーバーの横のボックスをクリックして、サプライヤー・サーバーのリストを展開します。
3. 「複製トポロジー」をクリックして強調表示し、次に「マスターの追加」をクリックします。
4. 「マスターの追加」ウィンドウの「サーバー」タブで、以下の手順を実行します。
 - a. このサーバーをゲートウェイ・サーバーにするには、「サーバーはゲートウェイです」を選択し、サーバーをマスター・サーバーとして追加するには、「サプライヤー・ゲートウェイ」を選択してから、ドロップダウン・リストからサーバーを選択します。
 - b. 「サーバーのホスト名:ポート」ドロップダウン・リストから、マスター・サーバー用の LDAP サーバーを選択します。コンソール・サーバーに登録されていない別のサーバーをマスター・サーバーとして指定する場合は、「サーバー・ホスト名:ポート」ドロップダウン・リストから「以下からの項目を使用します」項目を選択し、マスター・サーバーのホスト名とポート番号をフィールドに `hostname:port` 形式で入力します。注: デフォルト・ポートは、非 SSL の場合は 389、SSL の場合は 636 です。
 - c. SSL 通信を使用可能にするには、「SSL 暗号化を使用可能にする」チェック・ボックスを選択します。
 - d. 「ピア・マスター名」フィールドにサーバー名を入力するか、ホスト名を使用する場合はフィールドをブランクにします。
 - e. サーバー ID を入力します。ピア・マスターを作成しているサーバーが実行中の場合は、「サーバー ID の取得」をクリックすると、自動的にこのフィールドが事前に入力されます。サーバー ID が不明の場合は、**unknown** を入力します。
 - f. サーバーの説明を入力します (オプション)。
 - g. マスター・サーバーと通信するためにサーバーが使用する資格情報を指定する必要があります。「資格情報オブジェクト」フィールドの横にある「選択」をクリックします。「資格情報の選択」ウィンドウが表示されます。「資格情報の選択」ウィンドウでは、以下を実行します。
 - 1) 使用する資格情報の場所を選択します。`cn=replication,cn=localhost` がよく使用されます。Web 管理ツールでは、以下の場所で資格情報を定義できます。
 - **cn=replication,cn=localhost** は、その資格情報を使用するサーバーのみに資格情報を保持します。資格情報は `cn=replication,cn=localhost` に置くほうが安全です。
 - **cn=replication,cn=IBMpolicies** は、Web 管理ツールを使用して接続しているサーバーが、レプリカを追加しようとするサーバーと同じでない場合であっても使用可能です。この場所に配置された資格情報はサーバー

に複製されます。場所 `cn=replication,cn=IBMpolicies` を使用できるのは、`IBMpolicies` をサポートする OID 1.3.18.0.2.32.18 がルート DSE の `ibm-supportedcapabilities` の下にある場合のみです。

- 複製されたサブツリー内の場合、資格情報は他のサブツリーで複製されます。複製されたサブツリーに置かれる資格情報は、そのサブツリーの **ibm-replicagroup=default** 項目の下に作成されます。
 - 2) すでに資格情報のセットがある場合は、以下のようにします。
 - 「**資格情報の表示**」をクリックします。既存の資格情報のリストは、「**資格情報の選択**」フィールドに表示されています。
 - 資格情報のリストを展開して、使用する資格情報を選択します。
 - 3) 既存の資格情報がない場合は、「**資格情報の追加**」をクリックして資格情報を追加します。合意資格情報について詳しくは、IBM Security Directory Server の資料の『**管理**』セクションで、397 ページの『**資格情報の追加**』を参照してください。
 - 4) 「**OK**」をクリックします。
5. 「**追加**」タブで以下の手順を実行します。
- a. 既存の複製スケジュールを使用する場合、ドロップダウン・リストから複製スケジュールを選択します。新規の複製スケジュールを作成するには、以下の手順を実行します。
 - 1) 「**追加**」をクリックします。
 - 2) 複製スケジュールについて詳しくは、IBM Security Directory Server の資料の『**管理**』セクションで、『417 ページの『**複製スケジュールの作成**』』を参照してください。「**マスターの追加**」パネルに戻ったら、スケジュールのリストから作成したスケジュールを選択します。
 - b. 「**コンシューマーに複製する機能**」リストから、コンシューマーに複製しない機能を選択解除できます。リリースの異なるサーバーがネットワークに混在する場合は、古いリリースでは使用できない機能が新しいリリースで使用できます。ACL のフィルター操作やパスワード・ポリシーのような一部の機能では、他の変更と共に複製される運用属性を利用します。これらの機能を使用する場合は、ほとんどの場合、すべてのサーバーでそれらの機能がサポートされるようにすることができます。その機能をサポートしないサーバーがある場合は、その機能を使用しないようにすることができます。例えば、各サーバーで異なる ACL が有効にならないようにすることができます。ただし、ある機能をサポートするサーバーでその機能を使用し、その機能をサポートしないサーバーにその機能に関連した変更を複製したくない場合があります。そのような場合は、機能リストを使用して、特定の機能が複製されないようにマークを付けることができます。
 - c. 「**コンシューマーに関する資格情報についての情報の追加**」チェック・ボックスにチェック・マークを付けます。これを選択すると、コンシューマー・サーバーの構成ファイルのサプライヤー資格情報が自動的に更新されます。これにより、トポロジー情報を `server2` に複製できるようになります。
 - コンシューマー・サーバー (`server2`) の管理者 DN を入力します (例: `cn=root`)。サーバーの構成プロセスで作成した管理者 DN が `cn=root` の場合、省略せずに完全な管理者 DN を入力します。`root` のみを使用しないでください。

- コンシューマー・サーバーの管理者パスワードを入力します (例: secret)。
 - d. 「OK」をクリックします。
 - e. 「追加のサプライヤー合意の作成」パネルに、新規マスター・サーバーと既存のサーバー間のサプライヤー合意およびコンシューマー合意がリスト表示されます。作成しない合意のチェック・ボックスのチェック・マークを外してください。
 - f. 「継続 (Continue)」をクリックします。
 - g. server2 を再始動するかどうかを尋ねるメッセージが表示されたら、「はい」をクリックします。必要な追加アクションを知らせるその他のメッセージが表示される場合があります。適切なアクションを実行するか、確認します。完了したら、「OK」をクリックします。
 - h. server2 から server1 への合意を構成するために適切な資格情報を追加します。
 - 1) 使用する資格情報の場所を選択します。cn=replication,cn=localhost がよく使用されます。
 - 2) すでに資格情報のセットがある場合は、以下のようになります。
 - a) 「資格情報の表示」をクリックします。既存の資格情報のリストは、「資格情報の選択」フィールドに表示されています。
 - b) 資格情報のリストを展開して、使用する資格情報を選択します。
 - 3) 「OK」をクリックします。
- 注: 場合によっては、「資格情報の選択」パネルが開き、cn=replication,cn=localhost 以外の場所に置かれている資格情報を入力するよう求められます。このような場合は、cn=replication,cn=localhost 以外の場所に存在する資格情報オブジェクトを指定する必要があります。既存の資格情報セットからサブツリーで使用する資格情報を選択するか、新規の資格情報を作成します。資格情報について詳しくは、『管理』で、397 ページの『資格情報の追加』を参照してください。
- i. ピア・マスターを作成するには、「OK」をクリックします。
 - j. 必要な追加アクションを知らせるメッセージが表示される場合があります。適切なアクションを実行するか、確認します。完了したら、「OK」をクリックします。

コマンド・ラインの使用

ここで説明するコマンドをコマンド行で発行することにより、サブツリーを作成することができます。

このシナリオは、複製されるサブツリーを新規に作成すること、および server1 のみ項目データを含むことが前提となります。ほかのサーバーはすべて新しくインストールされ、構成済みのデータベースを所有し、初期化のために少なくとも 1 回は始動されているとします。(サーバー・インスタンスを始動する前に、IBM Security Directory Server の資料の『管理』セクションで、『703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』』を必ずお読みください)。

注: 作成するサブツリーを以下に示します。

```
dn: o=sample
objectclass: organization
objectclass: ibm-replicationContext
o: sample
```

この項目がすでに存在する場合は、項目全体を追加する代わりに **objectclass=ibm-replicationContext** を追加するように変更してください。

server1 および server2 はピア・マスター・サーバーです。すなわち、相互に更新を受信しますが、複製するのはクライアントから受信した項目のみです。両方のマスターの項目の内容は同じですが、項目を複製するのはクライアント要求を受信したサーバーのみです。両方のマスターは、互いにサプライヤーおよびコンシューマーであり、他のサーバーに対するサプライヤーです。

サブツリー **o=sample** のピア・マスター (server1 および server2) を作成するには、以下のようにします。

1. 構成専用モードでサーバー server1 および server2 を始動します。各サーバーで、以下のコマンドを発行します。

```
idsslapd -I <LDAPinstance> -a
```

2. 各インスタンス用の管理サーバー (**idsdiradm**) が実行されていない場合は、**idsdiradm** を始動させます。

```
idsdiradm -I <LDAP_instance>
```

3. server1 および server2 を構成してピア・サーバーにする必要があります。

idsldapadd コマンドを使用し、server1 および server2 の `ibmslapd.conf` ファイルに以下の項目を追加します。server1 および server2 で、以下のコマンドを発行します。

```
idsldapadd -D <adminDN> -w<adminPW> -i<filename>
```

where <filename> contains:

```
dn: cn=Master Server, cn=configuration
objectclass: ibm-slapdReplication
cn: Master Server
ibm-slapdMasterDN: cn=any
ibm-slapdMasterPW: secret
```

注: この例ではすべてのサーバーで共用する資格情報オブジェクトを使用するため、これらの項目は両方のサーバーで完全に同じでなければなりません。パスワードは入力時には平文ですが、ファイルでは暗号化されます。

4. server1 および server2 を停止します。サーバーを停止させるには、各サーバーで以下のコマンドを発行します。

```
idsslapd -I <instancename> -k
```

ここで、<instancename> は、停止するディレクトリー・サーバー・インスタンスの名前です。

```
ibmdirctl -h <serverx> -D <adminDN>-w <adminPW>-p 389 stop
```

<serverx> にはサーバーの名前を指定します。

5. `ibmslapd.conf` ファイルを保存します。
6. マスター・サーバー server1 が存在するコンピューターで、合意情報の更新に使用するファイル (例えば `mycredentialsfile`) を作成します。`mycredentialsfile` の内容は以下のとおりです。

```
dn: cn=replication,cn=IBMpolicies
objectclass: container
```

```

###Bind Credentials/method to peer server - replication agreement
###points to this.
dn: cn=simple,cn=replication,cn=IBMpolicies
objectclass:ibm-replicationCredentialsSimple
cn:simple
replicaBindDN:cn=any
replicaCredentials:secret
description:Bind method of the peer master (server1)to the peer (server2)

```

7. 以下のコマンドを発行します。

```
idsldif2db -r no -i<mycredentialsfile> -I <instance_name>
```

8. <mycredentialsfile> を server2 が存在するコンピューターにコピーして、以下のコマンドを発行します。

```
idsldif2db -r no -i<mycredentialsfile> -I <instance_name>
```

9. server1 が存在するコンピューターでファイル <mytopologyfile> を作成します。ここで、<mytopologyfile> には以下の設定が含まれます。

注: 以下のファイルの <server1-uuid> の箇所は、すべてのマスター・サーバーの **cn=Configuration** 項目の **ibm-slappedServerId** 属性の値で置き換えてください。この値は、サーバーを最初に始動したときにサーバーによって生成されます。また、AIX、Linux、または Solaris システムの場合は、**cn=Configuration** 項目の **idsldapsearch** を実行するか、ibmslapd.conf ファイルに対して **grep** コマンドを使用することによって検索できます。同様に、出現する <serverx-uuid> (x は 1 または 2 を表す) はすべて、それぞれのサーバーの **cn=Configuration** 項目の **ibm-slappedServerId** 属性の値に置き換えてください。

```

dn: o=sample
o: sample
objectclass: top
objectclass: container
objectclass: ibm-replicationContext

dn: ibm-replicaGroup=default, o=sample
objectclass: top
objectclass: ibm-replicaGroup
ibm-replicaGroup: default

dn: ibm-replicaServerId=<server1-uuid>,ibm-replicaGroup=default,o=sample
objectclass: top
objectclass: ibm-replicaSubentry
ibm-replicaServerId: <server1-uuid>
ibm-replicationServerIsMaster: true
cn: server1
description: server 1 (peer master) ibm-replicaSubentry

dn: ibm-replicaServerId=<server2-uuid>,ibm-replicaGroup=default,o=sample
objectclass: top
objectclass: ibm-replicaSubentry
ibm-replicaServerId: <server2-uuid>
ibm-replicationServerIsMaster: true
cn: server2
description: server2 (peer master) ibm-replicaSubentry

#server1 to server2 agreement
dn: cn=server2,ibm-replicaServerId=<server1-uuid>,
ibm-replicaGroup=default,o=sample
objectclass: top
objectclass: ibm-replicationAgreement
cn: server2
ibm-replicaConsumerId: <server2-uuid>
ibm-replicaUrl: ldap://server2:389
ibm-replicaCredentialsDN: cn=simple,cn=replication,cn=IBMpolicies
description: server1(master) to server2(master) agreement

#server2 to server1 agreement
dn: cn=server1,ibm-replicaServerId=<server2-uuid>,
ibm-replicaGroup=default,o=sample
objectclass: top
objectclass: ibm-replicationAgreement
cn: server1
ibm-replicaConsumerId: <server1-uuid>
ibm-replicaUrl: ldap://server1:389
ibm-replicaCredentialsDN: cn=simple,cn=replication,cn=IBMpolicies
description: server2(master) to server1(master) agreement

```

10. このトポロジーをロードするには、以下のコマンドを発行します。

```
idsldif2db -r no -i<mytopologyfile> -I <instance_name>
```

ここで、`-r no` は項目のセットの複製を防止するオプションです。

11. この時点で、サブツリーに追加のデータをロードできます。

注: `-r no` フラグを使用すると、項目セットの複製を防げます。

12. データのロードが完了したら、その他のサーバーに取り込むトポロジおよび複製コンテキストの追加データをエクスポートできるようにするために、以下のコマンドを発行します。

```
idsdb2ldif-s"o=sample" -o <mymasterfile.ldif>-I <instance_name>
-k <key seed> -t <key salt>
```

注: 複数のインスタンスが存在する場合、`-I` オプションを使用する必要があります。サーバーの鍵を同期化していない場合は、`-k` および `-t` オプションを使用する必要があります。詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の `idsdb2ldif` コマンド情報を参照してください。

重要: Advanced Encryption Standard (AES) が使用可能になっているサーバーにインポートするデータをエクスポートする場合で、2 つのサーバーが暗号同期化されていない場合は、サーバーの暗号同期化について、703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』を参照してください。

ソース・サーバー (データをエクスポートするサーバー) および宛先サーバー (データをインポートするサーバー) が一致しないディレクトリー・キー stash ファイルを使用していて、宛先サーバーの暗号化シード値および暗号化ソルト値を指定している場合、AES で暗号化されたデータはソース・サーバーの AES 鍵で暗号化解除され、さらに宛先サーバーの暗号化シード値および暗号化ソルト値で再度暗号化されます。暗号化されたデータは、LDIF ファイルに保管されます。

暗号化シードは、AES 共通鍵の値セットの生成に使用します。これらの値は、ディレクトリー stash ファイルに格納され、ディレクトリーに格納されたパスワードと共通鍵属性の暗号化および暗号化解除に使用されます。暗号化シードに含まれる文字は、33 以上 126 以下の範囲の値を持つ印刷可能な ISO-8859-1 ASCII 文字のみでなければなりません。また、最小文字数は 12、最大文字数は 1016 です。これらの文字について詳しくは、IBM Security Directory Server の資料の『管理』セクションで、『647 ページの『付録 D. 33 番から 126 番までの ASCII 文字』』を参照してください。

暗号化ソルトは、AES 暗号化鍵の生成に使用されたランダムに生成された値です。宛先サーバーのソルト値は、(`idsldapsearch` ユーティリティを使用して) 宛先サーバーの「`cn=crypto,cn=localhost`」項目を検索することにより取得できます。属性タイプは `ibm-slapdCryptoSalt` です。

13. `server1` を再始動します。
14. `server2` が存在するコンピューターに `<mymasterfile.ldif>` ファイルをコピーします。
15. `server2` が存在するコンピューターで、以下のコマンドを発行します。

```
idsldif2db -r no -i <mymasterfile.ldif> -I <instance_name>
```

16. `server2` を開始します。

```
idsslapd -I <instance_name>
```

マスター - 転送 - レプリカ・トポロジーの作成

ここで提供する情報に従って、マスター - 転送 - レプリカ・トポロジーを作成できます。

以下の図は、マスター - 転送 - レプリカ・トポロジーを示します。

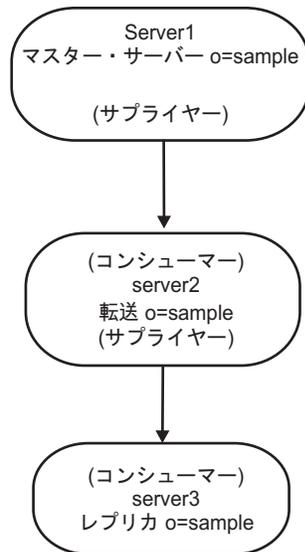


図 13. マスター - 転送サーバー - レプリカ・トポロジー

マスター - 転送 - レプリカ・トポロジーを定義するには、以下の手順を実行します。

1. マスター・サーバーおよびレプリカ・サーバーを作成します。すでにこれらを作成している場合は、328 ページの『マスター - レプリカ・トポロジーの作成』を参照してください。
2. 元のレプリカに対する新しいレプリカ・サーバーを作成します。405 ページの『レプリカ・サーバーの追加』を参照してください。
3. データをレプリカにコピーします。333 ページの『レプリカへのデータのコピー』を参照してください。

注: cn=schema などのグローバル更新を複製するには、cn=ibmpolicies 下のトポロジーにすべてのサーバーが追加済みであることを確認してください。

レプリカの転送サーバーへの変更

ここで提供する情報に従って、レプリカを転送サーバーに変更することができます。

このタスクについて

注: 複製トポロジーの設定を開始する前に、各サーバーの `ibmslapd.conf` ファイルのバックアップ・コピーを作成してください。複製で問題が発生した場合、このバックアップ・コピーを使用すれば元の構成を復元できます。

マスター (server1) およびレプリカ (server2) を持つ複製トポロジーをセットアップした場合、server2 の役割を転送サーバーの役割に変更できます。これを行うには、

server2 の下に新しいレプリカ (server3) を作成する必要があります。

Web 管理の使用:

Web 管理ツールを使用して、レプリカを転送サーバーに変更することができます。ここで説明する手順に従って、同じ操作を実行します。

手順

1. すべてのサーバーを始動します。
2. Web 管理ツールを使用してマスター・サーバー (server1) にログオンしていない場合は、ログオンします。
3. ナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。
4. 複製するサブツリーを選択して、「トポロジーの表示」をクリックします。
5. 「server1」選択の隣にあるボックスをクリックし、サーバーのリストを展開します。
6. server2 を選択して、「レプリカの追加」をクリックします。
7. 「レプリカの追加」ウィンドウの「サーバー」タブで、以下の手順を実行します。
 - 「サーバーのホスト名:ポート」ドロップダウン・リストから、レプリカ・サーバー用の LDAP サーバーを選択します。

コンソール・サーバーに登録されていない別のサーバーをレプリカ・サーバーとして指定する場合は、「サーバーのホスト名:ポート」ドロップダウン・リストから「以下からの項目を使用します」項目を選択し、レプリカ・サーバーのホスト名およびポート番号を `hostname:port` の形式でフィールドに入力します。デフォルトのポートは、非 SSL の場合 389、SSL の場合 636 です。

- 「SSL を使用可能にする」チェック・ボックスは未チェックのままにしておきます。
- レプリカ名を入力するか、ホスト名を使用する場合はフィールドを空白にします。
- レプリカ ID を入力します。レプリカを作成する対象のサーバーが実行中の場合、「レプリカ ID の取得」をクリックすると、このフィールドが自動的に設定されます。これは必須フィールドです。
- レプリカ・サーバーの説明を入力します。
- マスターと通信するためにレプリカが使用する資格情報を指定します。
 - a. 「選択」をクリックします。
 - b. 「cn=replication,cn=IBMpolicies」の隣にあるラジオ・ボタンをクリックします。

注: cn=ibmpolicies を複製する場合を除いて、mycreds 資格情報を、フォワルダー (転送サーバー) の cn=replication, cn=ibmpolicies の下に作成する必要があります。

- c. 「資格情報の表示」をクリックします。
- d. 資格情報のリストを展開して、「mycreds」を選択します。

- e. 「OK」をクリックします。

合意資格情報の詳細については、397 ページの『資格情報の追加』を参照してください。

8. 「追加」タブをクリックします。

- a. 「複製スケジュールの選択または DN の入力 (オプション)」の設定は、「なし」のままにしておきます。これにより即時の複製がデフォルトとして設定されます。
- b. どの機能も選択解除しないでください。
- c. 「複製方式」の設定は「単一スレッド」のままにしておきます。
- d. 「コンシューマーに関する資格情報の追加」チェック・ボックスをクリックして選択します。
- e. コンシューマー (レプリカ) サーバーの管理者の DN を入力します。例:
cn=root。

注: サーバーの構成プロセスで作成した管理者 DN が cn=root の場合、省略せずに完全な管理者 DN を入力します。root のみを入力しないよう注意してください。

- f. コンシューマー (レプリカ) の管理者のパスワードを入力します。例:
secret。
- g. レプリカを作成するには、「OK」をクリックします。レプリカ・サーバーの再始動など、必要な追加アクションを知らせるメッセージが表示されません。適切なアクションを実行します。
- h. 「OK」をクリックします。

9. データを server1 から新規レプリカ server3 にコピーします。この方法の詳細については、333 ページの『レプリカへのデータのコピー』を参照してください。

注: トポロジーの変更は、マスターである server1 により server2 に複製されます。

10. サプライヤー合意を server3 に追加し、server2 を server3 のサプライヤーに、server3 を server2 のコンシューマーにします。この方法の詳細については、414 ページの『レプリカへのサプライヤー情報の追加』を参照してください。

注: 「コンシューマーに関する資格情報の追加」チェック・ボックスを選択しなかった場合、またはコンシューマーの構成ファイルにサプライヤー情報を追加できなかった場合に限り、このステップを実行する必要があります。

タスクの結果

Web 管理ツールでは、サーバーの役割がアイコンで示されます。以上で、トポロジーは以下ようになります。

- server1 (マスター)
 - server2 (転送)
 - server3 (レプリカ)

コマンド・ラインの使用:

ここで説明するコマンドをコマンド行で発行することにより、サブツリーを作成することができます。

このタスクについて

このシナリオは、複製されるサブツリーを新規に作成すること、および `server1` のみ項目データを含むことが前提となります。ほかのサーバーはすべて新しくインストールされ、構成済みのデータベースを所有し、初期化のために少なくとも 1 回は始動されているとします。(サーバー・インスタンスを始動する前に、IBM Security Directory Server の資料の『管理』セクションで、『703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』』を必ずお読みください)。

注: 作成するサブツリーを以下に示します。

```
dn: o=sample
objectclass: organization
objectclass: ibm-replicationContext
o: sample
```

この項目がすでに存在する場合は、項目全体を追加する代わりに **objectclass=ibm-replicationContext** を追加するように変更してください。

この手順は単一のマスターおよびレプリカの場合と似ていますが、トポロジー全体を各サーバーに追加する必要があり、合意情報ファイルの内容が複雑になります。現在、ファイルには転送サーバーの情報およびサプライヤーとコンシューマーの情報が格納されています。

このシナリオのサプライヤーとコンシューマーの関係は以下のとおりです。

- マスターは転送に対するサプライヤーです。
- 転送は以下の 2 つの役割を持ちます。
 1. マスターのコンシューマー
 2. レプリカに対するサプライヤー
- レプリカは転送のコンシューマーです。

サブツリー **o=sample** のマスター (`server1`)、転送 (`server2`)、およびレプリカ (`server3`) を作成するには、以下のようになります。

手順

1. マスター・サーバーが存在するコンピューターで、合意情報を格納するファイル (例: `myreplicainfofile`) を作成します。ここで、`myreplicainfofile` には以下の設定が含まれます。

注: 以下のファイルにおいて、`<server1-uuid>` の箇所すべてを、マスター・サーバーの **cn=Configuration** 項目の **ibm-slapdServerId** 属性の値で置き換えてください。この値は、サーバーを最初に始動したときにサーバーによって生成されます。また、AIX、Linux、または Solaris システムの場合は、**cn=Configuration** 項目の **idsldapsearch** を実行するか、`ibmslapd.conf` ファイルに対して **grep** コマンドを使用することによって検索できます。同様に、

<server2-uuid> および <server3-uuid> の箇所すべてを、各サーバーの **cn=Configuration** 項目の **ibm-slappedServerId** 属性の値で置き換える必要があります。

```
dn: cn=replication,cn=IBMpolicies
objectclass: containerdn: o=sample
objectclass: organization
objectclass: ibm-replicationContextdn: ibm-replicaGroup=default, o=sample
objectclass: top objectclass: ibm-replicaGroup
ibm-replicaGroup: defaultdn: cn=server2 BindCredentials,
    cn=replication,cn=IBMpolicies
objectclass: ibm-replicationCredentialsSimple
#or ibm-replicationCredentialsExternal or
#ibm-replicationCredentialsKerberos
cn: server2 BindCredentials
replicaBindDN: cn=any replicaCredentials: secret
description: Bindmethod of server 1 (the master)to server2
dn: cn=server3 BindCredentials,cn=replication,cn=IBMpolicies
objectclass: ibm-replicationCredentialsSimplecn: server3 BindCredentials
    replicaBindDN: cn=any replicaCredentials: secret description:
        Bindmethod of server2 (the forwarder) to
server3 (the replica)dn: ibm-replicaServerId=server1-uuid,
ibm-replicaGroup=default,o=sample objectclass: top
objectclass: ibm-replicaSubentry ibm-replicaServerId: server1-uuid
#whatever the ID is in the config ibm-replicationServerIsMaster: true
#true if master, false if forwarder
cn: server1 description: master
ibm-replicaSubentrydn: ibm-replicaServerId=server2-uuid,
ibm-replicaGroup=default,o=sample objectclass: top
objectclass: ibm-replicaSubentry ibm-replicaServerId: server2-uuid
ibm-replicationServerIsMaster: false
cn: server2 description: forwarder
ibm-replicaSubentrydn: cn=forwarder1,ibm-replicaServerId=<server1-uuid>,
ibm-replicaGroup=default,o=sample objectclass: top
objectclass: ibm-replicationAgreement cn: server2
ibm-replicaConsumerId: <server2-uuid>
ibm-replicaUrl: ldap://server2:389
ibm-replicaCredentialsDN: cn=server2 BindCredentials,
    cn=replication,cn=IBMpolicies
description: server1 (the master) to server2 (the forwarder) agreement
dn: cn=server3,ibm-replicaServerId=<server2-uuid>,
ibm-replicaGroup=default,o=sample objectclass: top
objectclass: ibm-replicationAgreement cn: server3
ibm-replicaConsumerId: <server3-uuid>-uuid
ibm-replicaUrl: ldap://server3:389 ibm-replicaCredentialsDN: cn=server3
BindCredentials,cn=replication,cn=IBMpolicies
description: server2 (the forwarder) to server3 (the replica) agreement
```

2. マスターがまだ停止していない場合は、次のコマンドを使用して停止します。
`ibmdirctl -h server1 -D <adminDN> -w <adminPW> -p 389 stop`
3. マスターに新規の複製トポロジをロードするには、次のコマンドを発行します。`idsldif2db -r no -i<myreplicainfofile> -I <instance_name>`
4. 新規レプリカの同期化に必要なデータをすべて含むファイルを生成するには、以下のコマンドを発行します。`idsdb2ldif -o <masterfile.ldif>-I <instance_name> -s o=sample -k <key seed> -t <key salt>` ディレクトリー・サーバーのインスタンスが複数存在する場合は、`-I` オプションを使用する必要があります。サーバーの鍵を同期化していない場合は、`-k` および `-t` オプションを使用する必要があります。詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の `idsdb2ldif` コマンド情報を参照してください。

重要: Advanced Encryption Standard (AES) が使用可能になっているサーバーにインポートするデータをエクスポートする場合で、2 つのサーバーが暗号同期化されていない場合は、サーバーの暗号化同期について、IBM Security Directory Server の資料の『管理』セクションで、『703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』』を参照してください。ソース・サーバー (データをエクスポートするサーバー) および宛先サーバー (データをインポートするサーバー) が一致しないディレクトリー・キー stash ファイルを使用していて、宛先サーバーの暗号化シード値および暗号化ソルト値を指定している場合、AES で暗号化されたデータはソース・サーバーの AES 鍵で暗号化解除され、さらに宛先サーバーの暗号化シード値および暗号化ソルト値で再度暗号化されます。暗号化されたデータは、LDIF ファイルに保管されます。

暗号化シードは、AES 共通鍵の値セットの生成に使用します。これらの値は、ディレクトリー stash ファイルに格納され、ディレクトリーに格納されたパスワードと共通鍵属性の暗号化および暗号化解除に使用されます。暗号化シードに含まれる文字は、33 以上 126 以下の範囲の値を持つ印刷可能な ISO-8859-1 ASCII 文字のみでなければなりません。また、最小文字数は 12、最大文字数は 1016 です。これらの文字について詳しくは、IBM Security Directory Server の資料の『管理』セクションで、『647 ページの『付録 D. 33 番から 126 番までの ASCII 文字』』を参照してください。

暗号化ソルトは、AES 暗号化鍵の生成に使用されたランダムに生成された値です。宛先サーバーのソルト値は、(idsldapsearch ユーティリティーを使用して) 宛先サーバーの「cn=crypto,cn=localhost」項目を検索することにより取得できます。属性タイプは ibm-slappedCryptoSalt です。

5. server2 が存在するコンピューターに <masterfile.ldif> ファイルをコピーします。
6. 構成専用モードでフォワーダー server2 を始動します。idsslapd -I <LDAPinstance> -a
7. server2 を構成してレプリカ・サーバーにする必要があります。idslapadd コマンドを使用し、server2 の ibmslapd.conf ファイルに以下の項目を追加します。server2 で、次のコマンドを発行します。idslapadd -D <adminDN> -w<adminPW> -i<filename>ここで、<filename> には、dn: cn=Master Server, cn=configuration objectclass: ibm-slappedReplication cn: Master Server ibm-slappedMasterDN: cn=any ibm-slappedMasterPW: secret ibm-slappedMasterReferral: ldap://server1:389/#referral to master when trying to add to consumer.#Referral can also be added to replicaContext, which would be#checked first for a valid server が含まれます。注: ibm-slappedMasterDN と ibm-slappedMasterPW の値は、マスター・サーバー server1 の項目「cn=server2 BindCredentials」に格納されている値と一致する必要があります。
8. server2 を停止します。ibmdirctl -h server2 -D <adminDN> -w <adminPW> -p 389 stop
9. **ibmslapd.conf** ファイルを保管します。
10. server3 が存在するコンピューターに <masterfile.ldif> ファイルをコピーします。
11. 構成専用モードでレプリカ server3 を始動します。idsslapd -I <LDAPinstance> -a

12. server3 を構成してレプリカ・サーバーにする必要があります。 **idsldapadd** コマンドを使用し、server3 の **ibmslapd.conf** ファイルに以下の項目を追加します。server3 で、次のコマンドを発行します。idsldapadd -D <adminDN> -w<adminPW> -i<filename>ここで、<filename> には、dn: cn=Master Server, cn=configuration objectclass: ibm-slapdReplication cn: Master Server ibm-slapdMasterDN: cn=any ibm-slapdMasterPW: secret ibm-slapdMasterReferral: ldap://server2:389/ が含まれます。注: ibm-slapdMasterDN と ibm-slapdMasterPW の値は、マスター・サーバー server1 の項目「cn=server3 BindCredentials」に格納されている値と一致する必要があります。
13. server3 を停止します。ibmdirctl -h server3 -D <adminDN> -w <adminPW> -p <port> stop
14. **ibmslapd.conf** ファイルを保管します。
15. server2 および server3 が存在するコンピューターで、次のコマンドを発行します。idsldif2db -r no -i <masterfile.ldif> -I <instance_name>
16. マスター (server1)、フォワーダー (server2)、およびレプリカ (server3) を始動します。各サーバーで、次のコマンドを発行します。idsslapd -I <LDAPinstance>

ピア複製を持つ複雑なトポロジーのセットアップ

ここで提供する情報に従って、ピア複製を使用する複雑なトポロジーをセットアップできます。

この処理によって作成された **ibm-replicagroup** オブジェクトは、最初は、複製されたサブツリーのルート項目の ACL を継承します。これらの ACL は、ディレクトリーの複製情報に対するアクセス・コントロールに不適切な場合があります。

追加する項目 DN がサーバーのサフィックスではない場合にサブツリー追加操作を正常に終了させるには、その項目 DN に正しい ACL が必要です。

フィルターに掛けられていない ACL の場合:

```
ownersource : <the entry DN>
ownerpropagate : TRUE
aclsource : <the entry DN>
aclpropagate: TRUE
```

フィルターに掛けられた ACL の場合:

```
ownersource : <the entry DN>
ownerpropagate : TRUE
ibm-filteraclinherit : FALSE
ibm-filteraclentry : <any value>
```

Web 管理ツールの「**ACL の編集**」機能を使用し、新しく作成した複製されるサブツリーに関連付ける複製情報の ACL を設定します (396 ページの『サブツリーのアクセス・コントロール・リストの編集』を参照)。

356 ページの『レプリカの転送サーバーへの変更』で作成した転送トポロジーを使用して、2 つのピア・マスター・サーバー、2 つの転送サーバー、および 4 つのレプリカから構成されるピア転送レプリカ・トポロジーを作成します。このトポロジーを作成するには、以下の操作を実行する必要があります。

1. マスター・サーバーに対するレプリカ・サーバーをさらに 2 つ作成します。405 ページの『レプリカ・サーバーの追加』を参照してください。

2. 新規作成した 2 つのレプリカ・サーバーの下に、それぞれ 2 つのレプリカを作成します。
3. 新しいピア・マスター・サーバーを追加します。402 ページの『ピア・マスターまたはゲートウェイ・サーバーの追加』を参照してください。

注: マスターにプロモートするサーバーは、従属レプリカを持たないリーフ・レプリカでなければなりません。

4. マスターから新しいマスターおよびレプリカにデータをコピーします。333 ページの『レプリカへのデータのコピー』を参照してください。
5. 複製を開始します。419 ページの『キューの管理』を参照してください。

コマンド・ラインの使用

ここで提供する情報に従い、ここで説明するコマンドをコマンド行で発行することにより、新規の複製されたサブツリーを作成することができます。

このタスクについて

このシナリオは、複製されるサブツリーを新規に作成すること、および server1 のみ項目データを含むことが前提となります。ほかのサーバーはすべて新しくインストールされ、構成済みのデータベースを所有し、初期化のために少なくとも 1 回は始動されているとします。(サーバー・インスタンスを始動する前に、IBM Security Directory Server の資料の『管理』セクションで、『703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』』を必ずお読みください)。

注:

```
dn: o=sample
objectclass: organization
objectclass: ibm-replicationContext
o: sample
```

上記は作成するサブツリーです。この項目がすでに存在する場合は、項目全体を追加する代わりに **objectclass=ibm-replicationContext** を追加するように変更してください。

この例ではトポロジーがより複雑になります。2 つのピア・マスター (server1 および server5)、2 つの転送 (server2 および server4)、および 4 つのレプリカ (server3、server6、server7、および server8) があります。サーバーの関係は以下のとおりです。

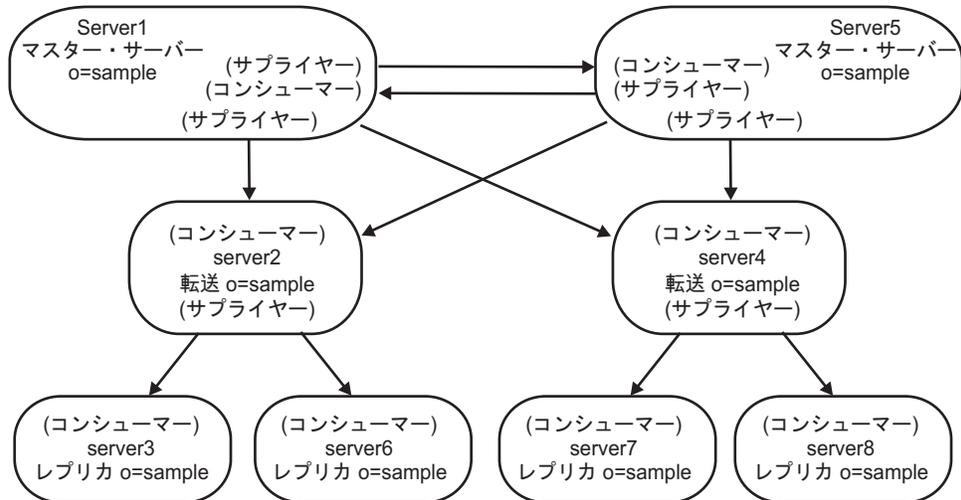


図 14. ピアツーピア・トポロジー

- server1 および server5 はピア・マスター・サーバーです。すなわち、相互に更新を受信しますが、複製するのはクライアントから受信した項目のみです。両方のマスターの項目の内容は同じですが、項目を複製するのはクライアント要求を受信したサーバーのみです。両方のマスターは、互いにサプライヤーおよびコンシューマーであり、転送サーバーに対するサプライヤーです。
- server2 および server4 は 2 つの役割があります。これらはともに server1 および server5 のコンシューマーであり、各レプリカに対するサプライヤーです。クライアント更新は行いません。複製された更新をコンシューマーに渡します。このシナリオでは、
 - server2 は server3 および server6 に対するサプライヤーです。
 - server4 は server7 および server8 に対するサプライヤーです。
 server2 と server4 の間の対話はありません。
- replica 1 および replica 2 は server2 のコンシューマーであり、server7 および server8 は server4 のコンシューマーです。

サブツリー **o=sample** のピア・マスター (server1 および server5)、転送サーバー (server2 および server4)、およびレプリカ (server3、server6、server7、および server8) を作成するには、以下の手順を実行します。

1. 構成モードでサーバー server1 および server5 を始動します。各サーバーで、次のコマンドを発行します。 `idsslapd -I <LDAPinstance> -a`

2. server1 および server5 を構成してピア・サーバーにする必要があります。

idsldapadd コマンドを使用し、server1 および server5 の `ibmslapd.conf` ファイルに以下の項目を追加します。server1 および server5 で、次のコマンドを発行します。 `idsldapadd -D <adminDN> -w<adminPW> -i<filename>`。ここで、`<filename>` には、`dn: cn=Master Server, cn=configuration objectclass: ibm-slapdReplication cn: Master Server ibm-slapdMasterDN: cn=any ibm-slapdMasterPW: secret` が含まれます。注: この例では、すべてのサーバーで共有する資格情報オブジェクトを使用するため、これらの項目は両方のサーバーで完全に同じでなければなりません。

3. server1 および server5 を停止します。サーバーを停止するには、各サーバーで次のコマンドを発行します。ibmdirctl -h <serverx> -D <adminDN>-w <adminPW>-p 389 stop。ここで、<serverx> はサーバーの名前です。
4. ibmslapd.conf ファイルのバックアップがあることを確認します。
5. マスター・サーバー server1 が存在するコンピュータで、合意情報を格納するファイル (例: mycredentialsfile) を作成します。ここで、mycredentialsfile には以下の情報が含まれます。dn: cn=replication,cn=IBMpolicies objectclass: container###Bind Credentials/method to peer/forwarder server - replication agreement ###points to this. dn: cn=simple,cn=replication,cn=IBMpolicies objectclass:ibm-replicationCredentialsSimple cn:simple replicaBindDN:cn=any replicaCredentials:secret description:Bind method of the master to the peer/forwarder
6. 次のコマンドを発行します。idsldif2db -r no -i<mycredentialsfile> -I <instance_name>
7. server2 および server4 を停止します。サーバーを停止するには、各サーバーで次のコマンドを発行します。ibmdirctl -h <serverx> -D <adminDN>-w <adminPW>-p 389 stopここで、<serverx> はサーバーの名前です。
8. <mycredentialsfile> ファイルを、server5、server2、および server4 が存在するコンピュータにコピーし、各コンピュータで次のコマンドを発行します。idsldif2db -r no -i<mycredentialsfile> -I <instance_name>
9. server1 が存在するコンピュータでファイル <mytopologyfile>> を作成します。ここで、<mytopologyfile>> の内容は以下のとおりです。

注: 以下のファイルの <master-uuid> の箇所は、すべてマスター・サーバーの **cn=Configuration** 項目の **ibm-slapdServerId** 属性の値で置き換えてください。この値は、サーバーを最初に始動したときにサーバーによって生成されます。また、AIX、Linux、または Solaris システムの場合は、**cn=Configuration** 項目の **idsldapsearch** を実行するか、ibmslapd.conf ファイルに対して **grep** コマンドを使用することによって検索できます。同様に、<serverx-uuid> (x は番号を表す) は、すべてそれぞれのサーバーの **cn=Configuration** 項目の **ibm-slapdServerId** 属性の値に置き換えてください。

```
dn: o=sample
o: sample
objectclass: top
objectclass: container
objectclass: ibm-replicationContext
dn: ibm-replicaGroup=default, o=sample
objectclass: top
objectclass: ibm-replicaGroup
ibm-replicaGroup: default
dn: ibm-replicaServerId= server1-uuid ,ibm-replicaGroup=default,o=sample
objectclass: top
objectclass: ibm-replicaSubentry
ibm-replicaServerId: server1-uuid
ibm-replicationServerIsMaster: true
cn: server1
description: server 1 (peer master) ibm-replicaSubentry
dn: ibm-replicaServerId= server2-uuid ,ibm-replicaGroup=default,o=sample
objectclass: top
objectclass: ibm-replicaSubentry
ibm-replicaServerId: server2-uuid
ibm-replicationServerIsMaster: true
```

```

cn: server2
description: server2 (peer master) ibm-replicaSubentry
#server1 to server2 agreement
dn: cn=server2,ibm-replicaServerId= server1-uuid ,
ibm-replicaGroup=default,o=sample
objectclass: top
objectclass: ibm-replicationAgreement
cn: server2
ibm-replicaConsumerId: server2-uuid
ibm-replicaUrl: ldap://server2:389
ibm-replicaCredentialsDN: cn=simple,cn=replication,cn=IBMpolicies
description: server1(master) to server2(master) agreement
#server2 to server1 agreement
dn: cn=server1,ibm-replicaServerId= server2-uuid ,
ibm-replicaGroup=default,o=sample
objectclass: top
objectclass: ibm-replicationAgreement
cn: server1
ibm-replicaConsumerId: server1-uuid
ibm-replicaUrl: ldap://server1:389
ibm-replicaCredentialsDN: cn=simple,cn=replication,cn=IBMpolicies
description: server2(master) to server1(master) agreement

```

10. このトポロジーをロードするには、次のコマンドを発行します。idsldif2db -r no -i<mytopologyfile> -I <instance_name>。ここで、-r no により、項目セットの複製を防止します。
11. この時点で、サブツリーに追加のデータをロードできます。
12. データのロードが終了したら、トポロジーをエクスポートして他のサーバーに値を取り込むことができるようにするため、次のコマンドを発行します。
idsdb2ldif -s"o=sample" -o <mymasterfile.ldif>-I <instance_name> -k <key seed> -t <key salt>注: インスタンスが複数存在する場合は、-I オプションを使用する必要があります。サーバーの鍵を同期化していない場合は、-k および -t オプションを使用する必要があります。詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の **idsdb2ldif** コマンドを参照してください。

重要: Advanced Encryption Standard (AES) が使用可能になっているサーバーにインポートするデータをエクスポートする場合で、2 つのサーバーが暗号同期化されていない場合は、サーバーの暗号同期化について、IBM Security Directory Server の資料の『管理』セクションで、『703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』』を参照してください。ソース・サーバー (データをエクスポートするサーバー) および宛先サーバー (データをインポートするサーバー) が一致しないディレクトリー・キー stash ファイルを使用していて、宛先サーバーの暗号化シード値および暗号化ソルト値を指定している場合、AES で暗号化されたデータはソース・サーバーの AES 鍵で暗号化解除され、さらに宛先サーバーの暗号化シード値および暗号化ソルト値で再度暗号化されます。暗号化されたデータは、LDIF ファイルに保管されます。

暗号化シードは、AES 共通鍵の値セットの生成に使用します。これらの値は、ディレクトリー stash ファイルに格納され、ディレクトリーに格納されたパスワードと共通鍵属性の暗号化および暗号化解除に使用されます。暗号化シードに含まれる文字は、33 以上 126 以下の範囲の値を持つ印刷可能な ISO-8859-1 ASCII 文字のみでなければなりません。また、最小文字数は 12、最大文字数は 1016 です。これらの文字について詳しくは、IBM Security Directory Server の資料の『管理』セクションで、『647 ページの『付録 D. 33 番から 126 番までの ASCII 文字』』を参照してください。

暗号化ソルトは、AES 暗号化鍵の生成に使用されたランダムに生成された値です。宛先サーバーのソルト値は、(idsldapsearch ユーティリティを使用して) 宛先サーバーの「cn=crypto,cn=localhost」項目を検索することにより取得できます。属性タイプは ibm-slappedCryptoSalt です。

13. 構成専用モードで server2、server3、server4、server6、server7、および server8 を始動します。各サーバーで、次のコマンドを発行します。idsldapd -I <LDAPinstance> -a
14. server2 および server4 は転送サーバーとして、server3、server6、server7、および server8 はレプリカ・サーバーとして構成する必要があります。idsldapadd コマンドを使用して、次の項目を各サーバーの ibmslapd.conf ファイルに追加します。idsldapadd -D <adminDN> -w<adminPW> -p <port> -i<filename>。ここで、<filename> には次が含まれます。dn: cn=Master Server, cn=configuration objectclass: ibm-slappedReplication cn: Master Server ibm-slappedMasterDN: cn=any ibm-slappedMasterPW: secret ibm-slappedMasterReferral: ldap://server1:389/注: これにより、クライアントからのすべての更新が server1 で参照されるようにします。
15. server2、server3、server4、server6、server7、および server8 を停止します。サーバーを停止するには、各サーバーで次のコマンドを発行します。ibmdirctl -h <serverx> -D <adminDN>-w <adminPW> -p <port> stop。ここで、<serverx> はサーバーの名前です。
16. ibmslapd.conf ファイルを新規バックアップとして保管します。
17. server2、server3、server4、server5、server6、server7、および server8 が存在するコンピューターに <mymasterfile.ldif> をコピーします。
18. これらのコンピューターのそれぞれで、次のコマンドを発行します。idsldif2db -r no -i <mymasterfile.ldif> -I <instance_name>

19. server1、server2、server3、server4、server5、server6、server7、および server8 を始動します。各サーバーで、次のコマンドを発行します。idsslapd -I <instance_name>

マスター/レプリカ構成の構成解除

マスター (サプライヤー)/レプリカ (コンシューマー) トポロジーからレプリカ・サーバーを除去する方法は複数あります。ここで説明するコマンドを使用して、両方のマシンで LDAP サーバーのデータベースを構成解除して再構成することにより、すべてのマスター/レプリカ情報を除去することができます。

このタスクについて

```
idsucfgdb -I <instance_name>
```

メッセージ・ボックスが表示されて、データベースおよびデータベース・インスタンスを除去するかどうか尋ねられます。「はい」をクリックします。

注: このプロセスにより、レプリカ・サーバーのデータベース全体が構成解除され、すべてのデータが消去されます。

また以下の手順でも、トポロジーからレプリカを除去できます。このオプションでは、1 つのサーバー (レプリカ) のみ構成解除および再構成できます。

手順

1. レプリカ・サーバーを停止します。
2. マスター・サーバーを中断します。
3. マスター・サーバーからサプライヤー情報を除去します。「複製管理」->「トポロジーの管理」に移動します。
4. レプリカ・サーバーを削除します。
 - a. 「トポロジーの表示」をクリックします。
 - b. レプリカを選択します。
 - c. 「削除」をクリックします。
5. マスター・サーバーを削除します。
 - a. 「トポロジーの表示」をクリックします。
 - b. マスターを選択します。
 - c. 「削除」をクリックします。
6. マスター・サーバーからサブツリーを除去します。
 - a. 「トポロジーの表示」をクリックします。
 - b. サブツリーを選択します。
 - c. ドロップダウン・リストから「サブツリーの削除」を選択します。
 - d. 「実行 (Go)」をクリックする。
7. マスター・サーバーから資格情報を除去します。
 - a. 「資格情報の管理」をクリックします。
 - b. サブツリーを選択します。
 - c. 「資格情報の表示」をクリックします。
 - d. 資格情報を選択します。

- e. 「削除」をクリックします。
 - f. 「OK」をクリックします。
8. レプリカ・サーバーで次のコマンドを実行してデータベースを構成解除し、すべてのデータを除去します。idsucfgdb -I <instance_name>メッセージ・ボックスが表示され、データベースとデータベース・インスタンスを除去するかどうか尋ねられます。「はい」をクリックします。データベースのそれぞれで、すべての情報または項目が失われます。

タスクの結果

以下の手順を実行し、データベース全体を構成解除することなくレプリカ・サーバーを構成解除することもできます。

1. マスター・サーバーからサプライヤー情報を除去します。「複製管理」->「トポロジーの管理」に移動します。
2. レプリカ・サーバーを削除します。
 - a. 「トポロジーの表示」をクリックします。
 - b. レプリカを選択します。
 - c. 「削除」をクリックします。
3. マスター・サーバーを削除します。
 - a. 「トポロジーの表示」をクリックします。
 - b. マスターを選択します。
 - c. 「削除」をクリックします。
4. マスター・サーバーからサブツリーを除去します。
 - a. 「トポロジーの表示」をクリックします。
 - b. サブツリーを選択します。
 - c. ドロップダウン・リストから「サブツリーの削除」を選択します。
 - d. 「実行 (Go)」をクリックする。
5. マスター・サーバーから資格情報を除去します。
 - a. 「資格情報の管理」をクリックします。
 - b. サブツリーを選択します。
 - c. 「資格情報の表示」をクリックします。
 - d. 資格情報を選択します。
 - e. 「削除」をクリックします。
 - f. 「OK」をクリックします。
6. レプリカ・サーバーから資格情報を除去します。
 - a. 「資格情報の管理」をクリックします。
 - b. サブツリーを選択します。
 - c. 「資格情報の表示」をクリックします。
 - d. 資格情報を選択します。
 - e. 「削除」をクリックします。
 - f. 「OK」をクリックします。

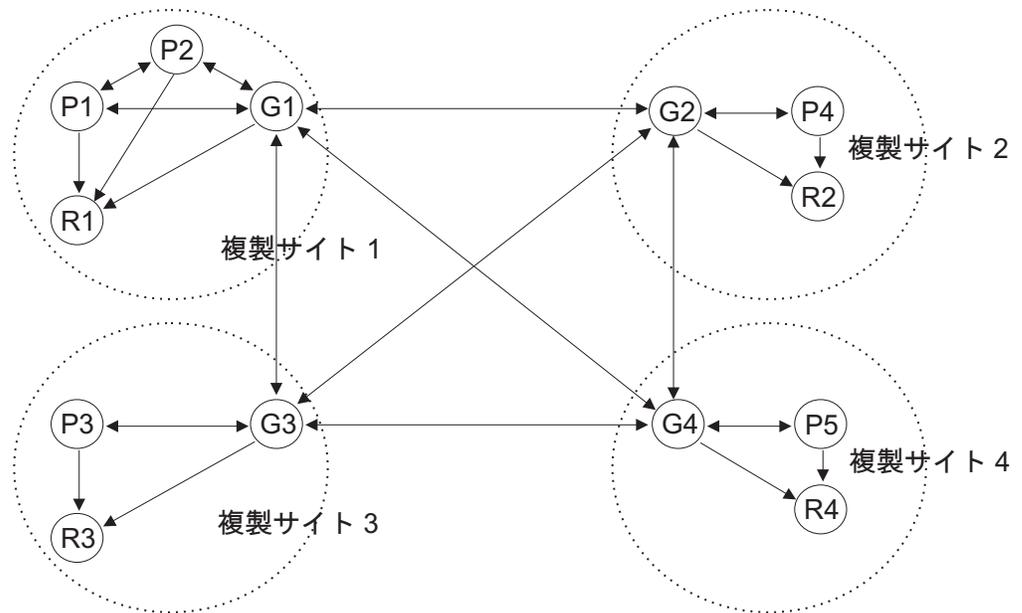
7. レプリカ・サーバーからサプライヤー情報を削除します。「複製プロパティの管理」をクリックします。「削除」をクリックします。
8. 「ディレクトリー管理」に移動します。
9. サブツリーを選択して展開します。
10. 「**ibm-replica Group=default**」を選択して展開します。
11. 「**replicaSubentry**」項目を選択して展開します。
12. すべての合意を削除します。
13. **replicaSubentry** 項目を縮小表示して削除します。
14. **ibm-replica Group=default** 項目を縮小表示して削除します。
15. サブツリーを選択します。ドロップダウン・リストから、「補助オブジェクト・クラスの削除」を選択し「実行」をクリックします。
16. 新規パネルが表示されます。このパネルで、`ibm-replicationContext` を選択し「削除」をクリックします。
17. 「OK」をクリックします。
18. レプリカ・サーバーで以下の検索を実行して、サーバーに複製情報がないか確認します。2 番目の検索では何も返されないはずですが。最初の検索で空のコンテナが返された場合、これは許容されます。`idsldapsearch -D cn=root -w secret -b " " -s sub objectclass=ibm-repl*`この操作では、ディレクトリーに残っているすべての複製トポロジーが返されます。**注:** トポロジーにレプリカが残されていない場合は、マスターでこのステップを実行することができます。

ゲートウェイ・トポロジーのセットアップ

ゲートウェイ複製の詳しい仕組み、およびゲートウェイをセットアップするための手順について説明します。

ゲートウェイ複製では、ゲートウェイ・サーバーを使用して、複製情報を複製ネットワークを介して効果的に収集および配布します。ゲートウェイ複製の主な利点はネットワーク・トラフィックの軽減です。

ゲートウェイ・サーバーはマスター (書き込み可能) にする必要があります。次の図は、ゲートウェイ複製がどのように機能するかを示しています。



P=ピア・サーバー
 G=ゲートウェイ・サーバー
 R=読み取り専用レプリカ

図 15. ゲートウェイ・サーバーを持つ複製ネットワーク

上記の図の複製ネットワークは 4 つの複製サイトで構成されており、各サイトにゲートウェイ・サーバーが 1 つずつあります。ゲートウェイ・サーバーの機能は次のとおりです。

- 各ゲートウェイ・サーバーが存在する複製サイトのピア・サーバーやマスター・サーバーから複製の更新情報を収集して、この更新情報を複製ネットワーク内部にあるその他のすべてのゲートウェイ・サーバーに送信します。
- 複製ネットワーク内部にある他のゲートウェイ・サーバーから複製の更新情報を収集して、これらの更新情報を、このゲートウェイ・サーバーが存在する複製サイトのピア・サーバー、マスター・サーバーおよびレプリカ・サーバーに送信します。

ゲートウェイ・サーバーは、サーバー ID とコンシューマー ID を使用して、複製ネットワーク内の他のゲートウェイ・サーバーに送信する更新情報と、複製サイト内部のローカル・サーバーに送信する更新情報を判別します。

ゲートウェイ複製をセットアップするには、2 つ以上のゲートウェイ・サーバーを作成する必要があります。ゲートウェイ・サーバーを作成すると、複製サイトが確立されます。次に、このゲートウェイ・サーバーと、このゲートウェイ・サーバーの複製サイト内に組み込むマスター、ピア、およびレプリカの各サーバー間の複製合意を作成します。

ゲートウェイ・サーバーはマスター (書き込み可能) にする必要があります。マスターではないサブエントリにゲートウェイ・オブジェクト・クラス (ibm-replicaGateway) を追加しようとすると、エラー・メッセージが戻されます。

ゲートウェイ・サーバーを作成するには 2 つの方法があります。以下を実行できます。

- 新規のゲートウェイ・サーバーを作成する
- 既存のマスター・サーバーをゲートウェイ・サーバーに変換する

注: 複製サイトごとに割り当てるゲートウェイの数を 1 つだけにすることは非常に重要です。複製サイト内のマスター・サーバーおよびレプリカ・サーバーが合意を結べるのは、そのサイトのゲートウェイ・サーバーのみです。

Web 管理の使用

ここで説明する手順に従い、Web 管理ツールを使用してゲートウェイ・トポロジーをセットアップすることができます。

このタスクについて

注: 複製トポロジーの設定を開始する前に、元の構成ファイル (ibmslapd.conf) および鍵 stash ファイル (ibmslapddir.ksf および ibmslapdcfg.ksf) のバックアップ・コピーを作成してください。複製で問題が発生した場合、このバックアップ・コピーを使用すれば元の構成を復元できます。また、ディレクトリーに格納されている複製トポロジー情報も保管する必要があります。**idsdb2ldif** ユーティリティを使用すると、複製サブツリーの `ibm-replicagroup=default` サブツリーをエクスポートできます。例えば、サブツリー `o=sample` のトポロジーを変更する場合、サブツリー `ibm-replicagroup=default,o=sample` をエクスポートする必要があります。

重要: 復元を行う場合、障害が発生したオペレーティング・システムと同じオペレーティング・システムにデータをリストアする必要があります。同じオペレーティング・システムにリストアしないと、エラーが発生する場合があります。

前述のシナリオからのピア複製を持つ複雑なトポロジーを使用してゲートウェイをセットアップするには、以下の手順を実行します。

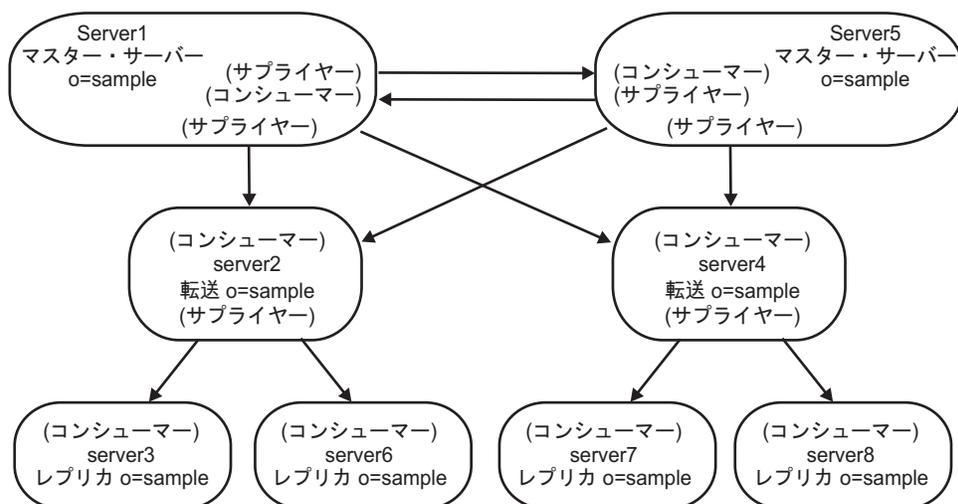


図 16. 先のシナリオで作成したピアツーピア・トポロジー

- 既存のピア・サーバー (peer1) をゲートウェイ・サーバーに変換し、複製サイト 1 を作成します。

- 複製サイト 2 用の新しいゲートウェイ・サーバー、および peer1 との合意を作成します。
- 複製サイト 2 のトポロジーを作成します (この例には示されていません)。
- マスターからトポロジー内のすべてのマシンにデータをコピーします。

手順

1. Web 管理ツールを使用して、マスター (server1) へログオンします。
2. ナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。
3. 所要のサブツリーを選択して、「トポロジーの表示」をクリックします。
4. 既存のサーバーをゲートウェイ・サーバーに変換する場合、「ゲートウェイ・サーバーの管理」をクリックします。「server1」またはそのピアの「server5」を選択します。この例では「server1」を使用し、「ゲートウェイの作成」をクリックします。
5. 「OK」をクリックします。注: ゲートウェイとして使用するサーバーがまだマスターとなっていない場合、そのサーバーは従属レプリカを持たないリーフ・レプリカである必要があります。そのリーフ・レプリカは、まずマスターにプロモートしてからゲートウェイとして指定することができます。
6. 新しいゲートウェイ・サーバーを作成するには、「サーバーの追加」をクリックします。
7. ゲートウェイ・サーバーとして新しいサーバー **server9** を作成します。この方法の詳細については、402 ページの『ピア・マスターまたはゲートウェイ・サーバーの追加』を参照してください。
8. 「追加のサプライヤー合意の作成」パネルが表示されます。「サプライヤー合意 (supplier agreement)」チェック・ボックスで server1 のみをチェックします。他の合意を選択解除します。

選択	サプライヤー	コンシューマー
✓	server1	server9
✓	server9	server1
	server2	server9
	server9	server2
	server4	server9
	server9	server4
	server9	server5
	server5	server9

9. 「**継続 (Continue)**」をクリックします。
10. 「**OK**」をクリックします。
11. 適切な資格情報とコンシューマー情報を追加します。注: 場合によっては、「資格情報の選択」パネルが開き、cn=replication,cn=localhost 以外の場所に置かれている資格情報を入力するよう求められます。このような場合は、cn=replication,cn=localhost 以外の場所に存在する資格情報オブジェクトを指定す

る必要があります。既存の資格情報セットからサブツリーで使用する資格情報を選択するか、新規の資格情報を作成します。397 ページの『資格情報の追加』を参照してください。

12. 「OK」をクリックします。Web 管理ツールでは、サーバーの役割がアイコンで示されます。以上で、トポロジーは以下のようになります。

- server1 (複製サイト 1 のマスター - ゲートウェイ)
 - server2 (転送)
 - server3 (レプリカ)
 - server6 (レプリカ)
- server4 (転送)
 - server7 (レプリカ)
 - server8 (レプリカ)
- server5 (マスター)
- server9 (複製サイト 2 のマスター - ゲートウェイ)
- server5 (マスター)
 - server1 (マスター)
 - server2 (転送)
 - server3 (レプリカ)
 - server6 (レプリカ)
- server4 (転送)
 - server7 (レプリカ)
 - server8 (レプリカ)
- server9 (マスター - ゲートウェイ)
 - server1 (マスター - ゲートウェイ)

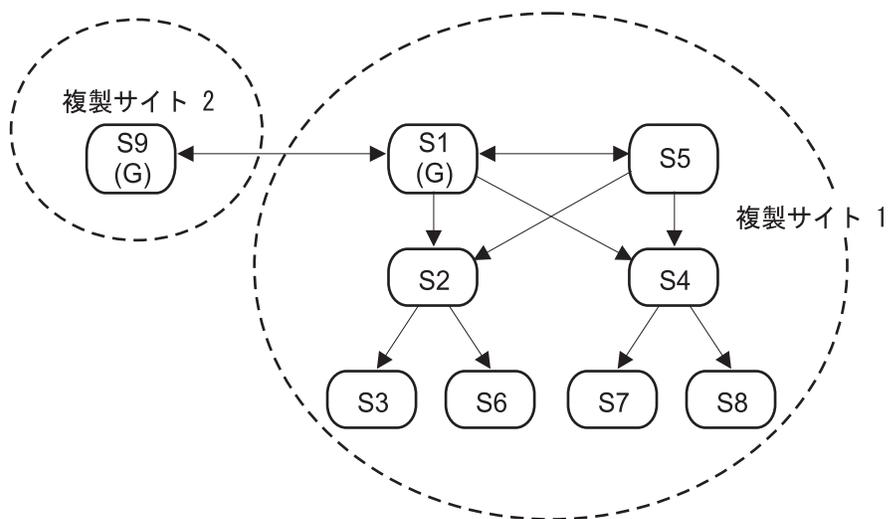


図 17. 2 つの複製サイトを持つゲートウェイ・トポロジー

13. サーバーを **server9** に追加して複製サイト 2 のトポロジを作成します。複製サイト 2 の外部にあるサーバーと新規サーバーとの合意は、必ず選択解除してください。
14. 複製サイトをさらに作成する場合は、この手順を繰り返します。複製サイトごとに作成するゲートウェイ・サーバーの数は 1 つだけにするのを忘れないでください。ただし、トポロジ内の各ゲートウェイ・サーバーは、他のゲートウェイ・サーバーと合意を結ぶ必要があります。
15. トポロジの作成が完了したら、server1 のデータをすべての複製サイトのすべての新規サーバーにコピーします。また必要な場合は、サプライヤーの資格情報をすべての新規サーバーに追加します。この方法の詳細については、333 ページの『レプリカへのデータのコピー』および 414 ページの『レプリカへのサプライヤー情報の追加』を参照してください。

コマンド・ラインの使用

ここで説明するコマンドを発行することにより、ゲートウェイ・トポロジをセットアップすることができます。

このタスクについて

この例では、前述の 2 つのピア、2 つの転送、および 4 つのレプリカ・シナリオを変更し、以下のことを行います。

- server1 の役割をそのトポロジのゲートウェイ・サーバー (複製サイト 1) に変更します。
- 複製サイト 2 用の新しいゲートウェイ・サーバー (server9) を作成します。複製サイト 2 は、ゲートウェイ・サーバーとして server9 を持つ独自のトポロジを備えています。この複製トポロジは、この例では示されていません。複製サイト 1 のトポロジをモデルとして使用できます。ただし、実際のトポロジ・セットアップでは、すべての複製サイトにすべてのトポロジを含める必要があります。

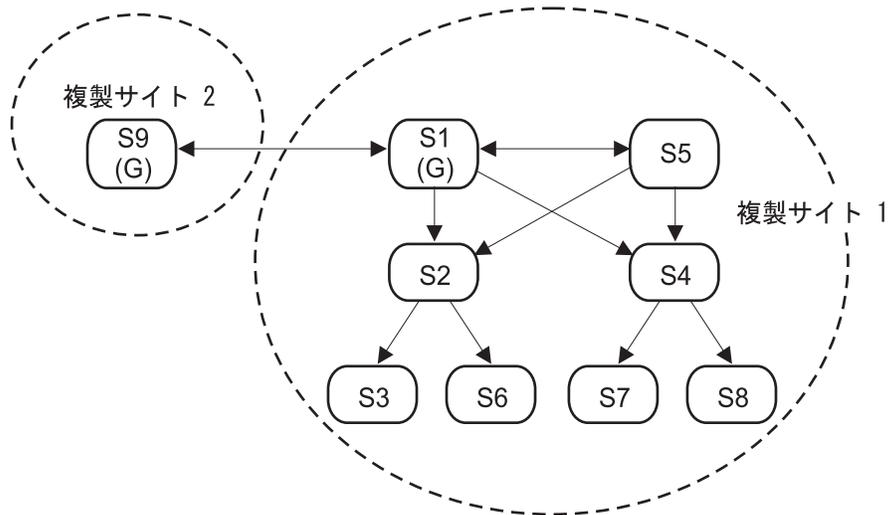


図 18. 2 つの複製サイトを持つゲートウェイ・トポロジ

手順

1. server9 を作成します。server9 のインスタンスを作成します。IBM Security Directory Server の資料の『インストールと構成』セクションで、『インスタンスの作成および管理』を参照してください。このインスタンスのサーバー ID を控えておいてください。このタスクで後ほど使用します。
2. server9 を server1 のコンシューマーに構成します。idsldapmodify コマンドを使用して次の項目を server9 の **ibmslapd.conf** ファイルに追加します。
idsldapmodify -D <adminDN> -w<adminPW> -p <port> -i <filename>、ここで、<filename> には、dn: cn=Master Server, cn=configuration objectclass: ibm-slapdReplication cn: Master Server ibm-slapdMasterDN: cn=any ibm-slapdMasterPW: secret が含まれます。
3. server1 をゲートウェイに構成します。objectclass: ibm-replicaGateway 属性を追加することにより、server1 の次の項目を変更します。dn:
ibm-replicaServerId=<server1-uuid>,ibm-replicaGroup=default,
ou=test,o=sample objectclass: top objectclass: ibm-replicaSubentry
objectclass: ibm-replicaGateway ibm-replicaServerId: <server1-uuid>
ibm-replicationServerIsMaster: true cn: server1 description: server1
(gateway server from replication site 1 to replication site 2)
4. server9 サブエントリを server1 に追加します。dn: **ibm-replicaServerId=<server9-uuid>,ibm-replicaGroup=default,ou=test,o=sample objectclass: top objectclass: ibm-replicaSubentry objectclass: ibm-replicaGateway ibm-replicaServerId: <server9-uuid> ibm-replicationServerIsMaster: true cn: server9 description: server9 (gateway server from replication site 2 to replication site 1)**
5. server5 から server1 へのキューを中断します。idsldapexop -D <adminDN> -w <admin_password> -h server5 -p <port> -op controlrepl -action suspend -rc "ou=test,o=sample"
6. server1 で server9 から server1 への複製合意を追加します。**#server9 to server1 agreement dn: cn=server1,ibm-replicaServerId=<server9-uuid>,ibm-replicaGroup=default,ou=test,o=sample objectclass: top objectclass: ibm-replicationAgreement cn: server1 ibm-replicaConsumerId: <server1-uuid> ibm-replicaUrl: ldap://server1:389 ibm-replicaCredentialsDN: cn=simple,cn=replication,cn=IBMPolicies description: supplier agreement from replication site2 to replication site 1**
7. server1 で server1 から server9 への複製合意を追加します。**#server1 to server9 agreement dn: cn=server9,ibm-replicaServerId=<server1-uuid>,ibm-replicaGroup=default,ou=test,o=sample objectclass: top objectclass: ibm-replicationAgreement cn: server9 ibm-replicaConsumerId: <server9-uuid> ibm-replicaUrl: ldap://server9:389 ibm-replicaCredentialsDN: cn=simple,cn=replication,cn=IBMPolicies description: supplier agreement from replication site1 to replication site2**
8. server1 を静止させます。idsldapexop -D <adminDN> -w <admin_password> -h server1 -p <port> -op quiesce -rc "ou=test,o=sample"

9. server1 から server9 へのキューをフラッシュします。idsldapexop -D <adminDN> -w <admin_password> -h server1 -p <port> -op controlqueue -skip all -ra "cn=server9,ibm-replicaServerId=<server1-uuid>, ibm-replicaGroup=default,ou=test,o=sample"
10. idsdb2ldif コマンドを実行して、server1 で LDIF ファイルを作成します。idsdb2ldif -s "ou=test,o=sample" -o <filename1>.ldif -I <instance_name> -k <key seed> -t <key salt>。ここで、<filename1>.ldif は最初の LDIF ファイルです。ファイルの内容についての詳細は、『<filename1>.ldif』 ページを参照してください。
11. idsdb2ldif コマンドを実行して、server1 で 2 番目の LDIF ファイルを作成します。idsdb2ldif-s "cn=replication,cn=ibmpolicies" -o <filename2>.ldif -I <instance_name> -k <key seed> -t <key salt>。ここで、<filename2>.ldif は 2 番目の LDIF ファイルです。ファイルの内容についての詳細は、380 ページの『<filename2>.ldif』 ページを参照してください。
12. server1 を静止解除します。idsldapexop -D <adminDN> -w <admin_password> -h server1 -p <port> -op quiesce -end -rc "ou=test,o=sample"
13. server5 で server5 から server1 へのキューを再開します。idsldapexop -D <adminDN> -w <admin_password> -h server5 -p <port> -op controlrepl -action resume -rc "ou=test,o=sample"。この時点で、server5 および server1 は完全に機能する状態になります。
14. <filename1>.ldif ファイルを server9 にコピーします。
15. <filename1>.ldif を server9 にロードします。idsldif2db -r no -i <filename1>.ldif -I <instance_name>
16. <filename2>.ldif ファイルを server9 にコピーします。
17. <filename2>.ldif を server9 にロードします。idsldif2db -r no -i <filename2>.ldif -I <instance_name>
18. server9 を始動します。idsslapd -I <instance_name> -a

タスクの結果

注: グローバル・ポリシー情報を複製する場合は、cn=ibmpolicies の下のトポロジーにすべてのサーバーが追加されているか必ず確認してください。

以下のファイル内容は、server9 にロードされる最初と 2 番目の両方の LDIF ファイルの内容を部分的に示しています。

<filename1>.ldif

注: 太字の項目は、このゲートウェイ・トポロジーを作成するために変更または追加した項目です。

```
dn: cn=ou=test,o=sample o: sample objectclass: top objectclass:
organization objectclass: ibm-replicationContextdn:
ibm-replicaGroup=default,ou=test,o=sample objectclass: top
objectclass: ibm-replicaGroup ibm-replicaGroup: default #Make
server1 a gateway server for site 1 dn: ibm-
replicaServerId=<server1-uuid>,ibm-replicaGroup=default,
ou=test,o=sample objectclass: top objectclass: ibm-replicaSubentry
objectclass: ibm-replicaGateway ibm-replicaServerId: <server1-uuid>
```

```

ibm-replicationServerIsMaster: true cn: server1 description: server1
(gateway server from replication site 1 to replication site 2)#Add
server9 as a gateway server for site 2 dn: ibm-
replicaServerId=<server9-uuid>,ibm-replicaGroup=default,
ou=test,o=sample objectclass: top objectclass: ibm-replicaSubentry
objectclass: ibm-replicaGateway ibm-replicaServerId: <server9-uuid>
ibm-replicationServerIsMaster: true cn: server9 description: server9
(gateway server from replication site 2 to replication site 1)dn:
ibm-replicaServerId=<server5-uuid>,ibm-replicaGroup=default,
ou=test,o=sample objectclass: top objectclass: ibm-replicaSubentry
ibm-replicaServerId: <server5-uuid> ibm-replicationServerIsMaster:
true cn: server5 description: server5 (master)dn:
ibm-replicaServerId=<server2-uuid>,ibm-
replicaGroup=default,ou=test,o=sample objectclass: top objectclass:
ibm-replicaSubentry ibm-replicaServerId: <server2-uuid>
ibm-replicationServerIsMaster: false cn: server2 description:
server2 (forwarder server number one)dn: ibm-
replicaServerId=<server4-uuid>, ibm-
replicaGroup=default,ou=test,o=sample objectclass: top objectclass:
ibm-replicaSubentry ibm-replicaServerId: <server4-uuid>
ibm-replicationServerIsMaster: false cn: server4 description:
server4 (forwarder server number two)#server1 to server9 agreement
dn: cn=server9,ibm-replicaServerId=<server1-uuid>,
ibm-replicaGroup=default,ou=test,o=sample objectclass: top
objectclass: ibm-replicationAgreement cn: server9
ibm-replicaConsumerId: <server9-uuid> ibm-replicaUrl:
ldap://server9:389 ibm-replicaCredentialsDN:
cn=simple,cn=replication,cn=IBMPolicies description: supplier
agreement from replication site1 to replication site2#server9 to
server1 agreement dn: cn=server1,ibm-replicaServerId=<server9-
uuid>,ibm-replicaGroup=default,ou=test,o=sample objectclass: top
objectclass: ibm-replicationAgreement cn: server1
ibm-replicaConsumerId: <server1-uuid> ibm-replicaUrl:
ldap://server1:389 ibm-replicaCredentialsDN:
cn=simple,cn=replication,cn=IBMPolicies description: supplier
agreement from replication site2 to replication site 1#server1 to
server5 agreement dn: cn=server5,ibm-replicaServerId=<server1-
uuid>,ibm-replicaGroup=default,ou=test,o=sample objectclass: top
objectclass: ibm-replicationAgreement cn: server5
ibm-replicaConsumerId: <server5-uuid> ibm-replicaUrl:
ldap://server5:389 ibm-replicaCredentialsDN:
cn=simple,cn=replication,cn=IBMPolicies description: server1
(gateway-master) to server5 (peer-master) agreement #server1 to
server2 agreement dn: cn=server2,ibm-replicaServerId=<server1-
uuid>,ibm-replicaGroup=default,ou=test,o=sample objectclass: top
objectclass: ibm-replicationAgreement cn: server2
ibm-replicaConsumerId: <server2-uuid> ibm-replicaUrl:
ldap://server2:389 ibm-replicaCredentialsDN:

```

```

cn=simple,cn=replication,cn=IBMPolicies description: server1
(gateway-master) to server2 (forwarder) agreement #server1 to
server4 agreement dn: cn=server4,ibm-replicaServerId=<server1-
uuid>ibm-replicaGroup=default,ou=test,o=sample objectclass: top
objectclass: ibm-replicationAgreement cn: server4
ibm-replicaConsumerId: <server4-uuid> ibm-replicaUrl:
ldap://server4:389 ibm-replicaCredentialsDN:
cn=simple,cn=replication,cn=IBMPolicies description: server1
(gateway-master) to server4 (forwarder) agreement #server5 to
server1 agreement dn: cn=server1,ibm-replicaServerId=<server5-
uuid>,ibm-replicaGroup=default,ou=test,o=sample objectclass: top
objectclass: ibm-replicationAgreement cn: server1
ibm-replicaConsumerId: <server1-uuid> ibm-replicaUrl:
ldap://server1:389 ibm-replicaCredentialsDN:
cn=simple,cn=replication,cn=IBMPolicies description: server5
(peer-master) to server1 (gateway-master) agreement #server5 to
server2 agreement dn: cn=server2,ibm-replicaServerId=<server5-
uuid>ibm-replicaGroup=default,ou=test,o=sample objectclass: top
objectclass: ibm-replicationAgreement cn: server2
ibm-replicaConsumerId: server2-uid ibm-replicaUrl:
ldap://server2:389 ibm-replicaCredentialsDN:
cn=simple,cn=replication,cn=IBMPolicies description: server5
(peer-master) to server2 (forwarder) agreement #server5 to server4
agreement dn: cn=server4,ibm-replicaServerId=<server5-uuid>,ibm-
replicaGroup=default,ou=test,o=sample objectclass: top objectclass:
ibm-replicationAgreement cn: server4 ibm-replicaConsumerId:
<server4-uuid> ibm-replicaUrl: ldap://server4:389
ibm-replicaCredentialsDN: cn=simple,cn=replication,cn=IBMPolicies
description: server5 (peer-master) to server4 (forwarder) agreement
#server2 to server3 agreement dn: cn=server3,ibm-
replicaServerId=<server2-uuid>,ibm-
replicaGroup=default,ou=test,o=sample objectclass: top objectclass:
ibm-replicationAgreement cn: server3 ibm-replicaConsumerId:
<server3-uuid> ibm-replicaUrl: ldap://server3:389
ibm-replicaCredentialsDN: cn=simple,cn=replication,cn=IBMPolicies
description: server2 (forwarder) to server3 (replica)
agreement#server2 to server6 agreement dn: cn=server6,ibm-
replicaServerId=<server2-uuid>,ibm-
replicaGroup=default,ou=test,o=sample objectclass: top objectclass:
ibm-replicationAgreement cn: server6 ibm-replicaConsumerId:
<server6-uuid> ibm-replicaUrl: ldap://server6:389
ibm-replicaCredentialsDN: cn=simple,cn=replication,cn=IBMPolicies
description: server2 (forwarder) to server6 (replica)
agreement#server4 to server7 agreement dn: cn=server7,ibm-
replicaServerId=<server4-uuid>,ibm-
replicaGroup=default,ou=test,o=sample objectclass: top objectclass:
ibm-replicationAgreement cn: server7 ibm-replicaConsumerId:
<server7-uuid> ibm-replicaUrl: ldap://server7:389

```

```
ibm-replicaCredentialsDN: cn=simple,cn=replication,cn=IBMPolicies
description: server4 (forwarder) to server7 (replica)
agreement#server4 to server8 agreement dn: cn=server8,ibm-
replicaServerId=<server4-uuid>,ibm-
replicaGroup=default,ou=test,o=sample objectclass: top objectclass:
ibm-replicationAgreement cn: server8 ibm-replicaConsumerId:
<server8-uuid> ibm-replicaUrl: ldap://server8:389
ibm-replicaCredentialsDN: cn=simple,cn=replication,cn=IBMPolicies
description: server4 (forwarder) to server8 (replica)agreement
```

<filename2>.ldif

```
dn: cn=replication,cn=ibmpolicies o: sample objectclass: top
objectclass: container objectclass: ibm-replicationContextdn:
cn=simple,cn=replication,cn=ibmpoliciesobjectclass:
ibm-replicationCredentialsSimple cn: simplereplicaBindDN:
cn=anyreplicaCredentials: secret
```

部分複製

部分複製は、指定された項目およびサブツリー内の指定された項目の属性サブセットのみを複製する複製機能です。ここで提供する情報により、部分複製について詳しく知ることができます。

複製される項目および属性は LDAP 管理者によって指定されます。部分複製を使用すると、管理者はデプロイメントの要件に応じて複製の処理能力を向上させることができます。例えば、管理者は、cn、sn、および userPassword 属性が複製され、description 属性が複製されないオブジェクト・クラス person の項目を選択できます。

複製される属性は複製フィルターを使用して指定されます。複製フィルターは、特定の複製合意に関連付けることができ、オブジェクト・クラスに基づきます。複製フィルターは、1 つのオブジェクト・クラスに関連する一連の属性で構成されます。1 つのオブジェクト・クラスに対して選択した属性のリストを、組み込みリストまたは除外リストの一部として指定できます。組み込みリストは、複製用に選択する属性のリストです。これに対して、除外リストは、複製用に選択しない属性のリストです。ただし、管理者は、オブジェクト・クラスの MUST 属性を除外しないようにする必要があります。オブジェクト・クラスで MUST 属性を除外すると、このオブジェクト・クラスを含む項目の複製は失敗する可能性があり、複製状態が再試行中に設定されます。このため、この特定の複製合意のための複製がブロックされる可能性があります。例えば、dn: cn=replicationfilter1,cn=localhost objectclass: ibm-replicationfilter ibm-replicationFilterattr: (objectclass=person) : !(sn) ibm-replicationFilterattr: (objectclass=*) : (*) という設定について検討してみます。この場合、フィルターを ibm-replicationFilterattr:(objectclass=person) : !(sn) と指定すると、オブジェクト・クラスが person の項目は複製に失敗し、複製がブロックされます。これは、sn が person オブジェクト・クラスの MUST 属性であるためです。

以下の属性は、除外リストに指定されていても、常に複製されます。

- 項目のオブジェクト・クラス属性
- 命名属性

- すべての運用属性

部分複製の既知の制約については、IBM Security Directory Server の資料の『トラブルシューティングおよびサポート』セクションで、『一般情報、既知の制限、および一般的なトラブルシューティング』を参照してください。

部分複製機能は、Web 管理ツールを使用するか、コマンド行から管理できます。

Web 管理ツールの使用

ここで提供する情報に従い、Web 管理ツールを使用してフィルターを管理することができます。

このタスクについて

まだ行っていない場合は、Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「フィルターの管理」をクリックします。このパネルは、サーバーがフィルター・ベースの複製機能をサポートする場合にのみ使用可能です。

このパネルで、以下を行うことができます。

- 複製フィルターを保管するサブツリーの表示
- フィルターの追加
- フィルターの編集
- フィルターの削除
- フィルターのコピー
- フィルターの表示

フィルターの追加:

ここで説明する手順に従って、フィルターを追加することができます。

このタスクについて

複製フィルターを追加するには、まず「フィルターの管理」で「サブツリーの選択」ボックスからサブツリーを選択し、次に「追加」をクリックして、「複製フィルターの追加」パネルを表示します。

複製フィルターの追加 - 一般:

このパネルには、複製フィルターに関する詳細情報を追加するためのコントロールがあります。ここで説明する手順に従って、複製フィルターを追加することができます。

このタスクについて

手順

1. 「フィルター名」ボックスに、フィルターする名前を入力します。例えば、myfilter1 など。
2. 「使用可能なオブジェクト・クラス」ボックスから、フィルターを作成するオブジェクト・クラスを選択します。

3. 「追加」をクリックして、「選択されたオブジェクト・クラス」ボックスに「使用可能なオブジェクト・クラス」ボックスのオブジェクト・クラスを取り込みます。
4. 「残りのオブジェクト・クラスのフィルターを定義する」チェック・ボックスを選択します。
5. フィルター対象属性の複製フィルターの追加を続行するには、「次へ」をクリックします。

複製フィルターの追加 - フィルター対象属性:

ここで説明する手順に従って、複製フィルター - フィルター対象属性を追加することができます。

このタスクについて

このパネルは、選択したオブジェクト・クラスの複製する属性を選択する機能を提供します。このパネルは、「複製フィルターの追加」の「一般」パネルで「次へ」ボタンをクリックして起動します。

あるオブジェクト・クラスについて複製する属性を指定するには、以下のようになります。

手順

1. 属性の複製を指定するオブジェクト・クラス行の「選択」列をクリックします。
2. 「フィルター属性の管理」ボタンをクリックするか、「アクションの選択」リストから「フィルター属性の管理」を選択して、「実行」をクリックします。

フィルター属性の管理:

「フィルター属性の管理」パネルは、複製フィルターのオブジェクト・クラス属性を指定するために使用します。ここで説明する手順に従って、複製フィルターの属性を指定することができます。

このタスクについて

手順

1. 「すべての属性をフィルター対象属性として選択」チェック・ボックスをクリアします。注:1 つの複製フィルターで選択対象オブジェクト・クラスのすべての属性を指定する場合は、「すべての属性をフィルター対象属性として選択」チェック・ボックスを選択します。
2. 「使用可能な属性」ボックスで必須属性を選択します。
3. 「追加」をクリックして、選択した属性を「使用可能な属性」から「フィルター対象属性」に移動させます。
4. 「フィルター対象属性」ボックス内の属性を複製フィルターに組み込むには、「選択したフィルター対象属性を組み込む」をクリックします。
5. 「フィルター対象属性」ボックス内の属性を複製フィルターから除外するには、「選択したフィルター対象属性を除外」をクリックします。
6. 「OK」をクリックします。

- 複製フィルターを保管するには、「複製フィルターの追加」の「フィルター対象属性」パネルで「完了」をクリックします。

フィルターの削除:

ここで説明する手順に従って、フィルターを削除することができます。

このタスクについて

複製フィルターを削除するには、「フィルターの管理」パネルの「選択したサブツリーのフィルター」ボックスで複製フィルターを選択して、「削除」をクリックします。

フィルターの編集:

複製フィルターは、「フィルターの管理」パネルで選択したサブツリー・ボックスの「フィルター」からフィルターを選択し、「編集」をクリックすることによって編集できます。

このタスクについて

複製フィルターの編集 - 一般:

このパネルには、選択済みのフィルターの内容を変更するためのコントロールがあります。ここで提供する情報に従って、複製フィルターを編集することができます。

このタスクについて

手順

- 「使用可能なオブジェクト・クラス」ボックスから、フィルターに追加するオブジェクト・クラスを選択します。
- 既存のフィルターを編集するには、以下の手順を実行します。
 - 「追加」をクリックして、「選択されたオブジェクト・クラス」ボックスに「使用可能なオブジェクト・クラス」ボックスのオブジェクト・クラスを取り込みます。
 - 「除去」をクリックして、「選択されたオブジェクト・クラス」ボックスから選択したオブジェクト・クラスを除去します。
- 「残りのオブジェクト・クラスのフィルターを定義する」チェック・ボックスを選択します。
- フィルター対象属性の複製フィルターの編集を続行するには、「次へ」をクリックします。

複製フィルターの編集 - フィルター対象属性:

ここで説明する手順に従って、複製フィルター - フィルター対象属性を編集することができます。

このタスクについて

このパネルは、フィルターが選択されている場合に、複製する属性を選択する機能を提供します。このパネルは、「複製フィルターの編集」の「一般」パネルで「次へ」ボタンをクリックして起動します。

あるオブジェクト・クラスについて複製する属性を指定するには、以下のようになります。

手順

1. 複製フィルター内の選択済みオブジェクト・クラスについて既存の属性リストを編集するには、対象のオブジェクト・クラス行の「**選択**」列をクリックします。
2. 「**フィルター属性の管理**」ボタンをクリックするか、「アクションの選択」リストから「フィルター属性の管理」を選択し、「**実行**」をクリックして、「フィルター属性の管理」パネルを表示します。
3. 「フィルター属性の管理」パネルで、複製フィルター定義に組み込むまたは除外する属性を指定します。

フィルターのコピー:

ここで提供する情報に従って、フィルターをコピーすることができます。

このタスクについて

複製フィルターの詳細を別の複製フィルターにコピーするには、まず「サブツリーの選択」ボックスからサブツリーを選択し、次に、「フィルターの管理」パネルの「選択したサブツリーのフィルター」からそのサブツリーの下に格納されているフィルターを選択して、「**コピー**」をクリックします。

複製フィルターのコピー - 一般:

ここで説明する手順に従って、複製フィルターをコピーすることができます。

このタスクについて

手順

1. 「フィルター・ロケーション」ボックスから、選択された複製フィルターをコピーするサブツリーを選択します。
2. 「フィルター名」ボックスに、フィルターする名前を入力します。例えば、myfilter2 など。
3. 「使用可能なオブジェクト・クラス」ボックスから、既存のフィルターに追加するオブジェクト・クラスを選択します。
4. 「**追加**」をクリックして、「選択されたオブジェクト・クラス」ボックスに「使用可能なオブジェクト・クラス」ボックスのオブジェクト・クラスを取り込みます。
5. 「**残りのオブジェクト・クラスのフィルターを定義する**」チェック・ボックスを選択します。
6. フィルター対象属性のフィルターのコピーを続行するには、「**次へ**」をクリックします。

複製フィルターのコピー - フィルター対象属性:

ここで説明する手順に従って、複製フィルターをコピーする場合にオブジェクト・クラスで複製される属性を指定することができます。

このタスクについて

このパネルは、選択したオブジェクト・クラスの複製する属性を選択する機能を提供します。このパネルは、「複製フィルターのコピー」の「一般」パネルで「次へ」ボタンをクリックして起動します。

1. 属性の複製を指定するオブジェクト・クラス行の「**選択**」列をクリックします。
2. 「**フィルター属性の管理**」ボタンをクリックするか、「アクションの選択」リストから「フィルター属性の管理」を選択し、「**実行**」をクリックして、「フィルター属性の管理」パネルを表示します。
3. 「フィルター属性の管理」パネルで、複製フィルター定義に組み込むまたは除外する属性を指定します。

コマンド行の使用

ここで説明するコマンドをコマンド行で発行することにより、複製フィルターを追加することができます。

このタスクについて

次のコマンドを発行して複製フィルターを追加します。`ldapadd -D cn=root -w rootdn: cn=replicationfilter,cn=localhost objectclass: ibm-replicationfilter ibm-replicationFilterAttr: (objectclass=person):(cn,sn,description) ibm-replicationFilterAttr: (objectclass=printer):!(cn,color) ibm-replicationFilterAttr: (objectclass=*): (*)`。この例では、タイプが「person」の項目の場合に、属性 `cn`、`sn`、および `description` がレプリカに送信されるよう指定しています。この項目に存在している残りの属性は送信されません。タイプ「printer」の項目については、`cn` および `color` 以外のすべての属性が送信されます。その他の項目については、すべての属性が送信されます。

ここで、複製合意を変更して、フィルター項目の DN を追加します。それには、次のコマンドを発行します。`ldapmodify -D cn=root -w rootdn: cn=replica1,ibm-replicaServerId=master-uuid,ibm-replicaGroup=default,o=sample changetype: modify add: ibm-replicationFilterDN ibm-replicationFilterDN: cn=replicationfilter,cn=localhost`

複製フィルターの例

以下に、複製フィルターの使用方法を説明した例をいくつか示します。

注: Security Directory Server 6.2 以降のバージョンは、複製フィルターにおける代替名をサポートしていません。

例 1: `dn: cn=replicationfilter, cn=localhost objectclass: ibm-replicationFilter ibm-replicationFilterAttr: (objectclass=person):(*) ibm-replicationFilterAttr: (objectclass=*): !(*)` この例の最初のフィルター属性では、項目タイプが「person」のすべての属性を複製するように指定されていま

す。2 番目のフィルター属性は、タイプ「person」以外の属性はいずれも複製しないことを指定します。つまり、タイプが「person」の項目のみが複製され、その他の項目は複製されないということです。

```
例 2: dn: cn=replicationfilter, cn=localhost objectclass:
ibm-replicationFilter ibm-replicationFilterAttr: (objectclass=person):
(cn,sn,userPassword) ibm-replicationFilterAttr: (objectclass=managerOf):
(managerOfDept) ibm-replicationFilterAttr: (objectclass=*):
```

!(managerOfDept)この例の場合は、タイプが「person」の項目「cn=Ricardo Garcia,o=sample」について考慮します。新規の補助オブジェクト・クラス「managerOf」が、この項目に付加されます。したがって、項目「cn=Ricardo Garcia,o=sample」には、「person」と「managerOf」の両方のオブジェクト・クラスが含まれることとなります。

最初のフィルター属性は、項目タイプ「person」の属性 cn、sn、および userpassword を複製することを指定します。2 番目のフィルター属性は、項目タイプ「managerOf」の属性 managerOfDept を複製することを指定します。3 番目のフィルター属性は、タイプが「person」または「managerOf」の項目以外の項目については、属性 managerOfDept を複製しないことを指定します。

したがって、項目タイプ「person」の場合は、属性 cn、sn、および userPassword が複製されます。項目「cn=Ricardo Garcia,o=sample」にはオブジェクト・クラス person と managerOf が含まれているため、属性 cn、sn、userPassword、および managerOfDept が複製されます。タイプが「person」でも「managerOf」でもないほかのすべての項目については、managerOfDept 以外のすべての属性が複製されます。

```
例 3: dn: cn=replicationfilter, cn=localhost objectclass:
ibm-replicationFilter ibm-replicationFilterAttr: (objectclass=person):
(cn,sn,userPassword) ibm-replicationFilterAttr: (objectclass=inetOrgPerson)
:!(userPassword,employeeNumber) ibm-replicationFilterAttr: (objectclass=*):
!(*)この例の場合は、タイプが「person」の項目「cn=Ricardo Garcia,o=sample」と、
タイプが「inetOrgperson」の別の項目「cn=Jane Smith,o=sample」について考慮します。
項目「cn=Jane Smith,o=sample」には、「person」と「inetOrgPerson」の両方のオブジェクト・クラスが含まれることとなります。
```

最初のフィルター属性は、項目タイプ「person」の属性 cn、sn、および userpassword を複製することを指定します。2 番目のフィルター属性は、項目タイプ「inetOrgPerson」の属性 userPassword および employeeNumber を複製しないことを指定します。3 番目のフィルター属性は、タイプが「person」または「inetOrgPerson」の項目以外の項目の属性はいずれも複製しないことを指定します。

したがって、項目「cn=Ricardo Garcia,o=sample」については、属性 cn、sn、および userPassword が複製されます。項目「cn=Jane Smith,o=sample」は最初と 2 番目の複製フィルターに一致するため、属性 cn と sn のみが複製されます。組み込みリストと除外リストの両方に存在している属性 userPassword は、除外の方が組み込みより優先されるため、除外されます。タイプが「person」でも「inetOrgPerson」でもないほかのすべての項目については、いずれの属性も複製されません。

複製トポロジー情報の除外

以下に示す情報を使用することにより、複製トポロジー情報を除外することができます。

IBM Security Directory Server 構成では、複製トポロジー情報は複製に関与するすべてのディレクトリー・サーバー・インスタンスの DB2 データベースに存在しています。この複製環境で、ディレクトリー・サーバー・インスタンスの DB2 データベースの内容は LDIF ファイルにエクスポートするが、複製トポロジー関連のデータを除外することが必要な状況が考えられます。Security Directory Server では、`replfilterdn.ldif` という名前のファイルが、ロケーション `<IDS_LDAP_HOME>/examples` に用意されています。このファイル内の項目を使用して、複製トポロジー情報が結果の `ldif` ファイルに出力されないように抑止できます。`replfilterdn.ldif` ファイルの例を以下に示します。

```
dn: cn=replicationfilter,cn=localhost
objectclass: ibm-replicationfilter ibm-replicationFilterAttr:
(objectclass=ibm-replicaGateway):!(*) ibm-replicationFilterAttr:
(objectclass=ibm-replicaGroup):!(*) ibm-replicationFilterAttr:
(objectclass=ibm-replicaSubentry):!(*) ibm-replicationFilterAttr:
(objectclass=ibm-replicationAgreement):!(*) ibm-replicationFilterAttr:
(objectclass=ibm-replicationCredentials):!(*) ibm-replicationFilterAttr:
(objectclass=ibm-replicationCredentialsExternal):!(*) ibm-
replicationFilterAttr: (objectclass=ibm-replicationCredentialsKerberos)
:!(*) ibm-replicationFilterAttr: (objectclass=ibm-
replicationCredentialsSimple):!(*) ibm-replicationFilterAttr:
(objectclass=ibm-replicationDailySchedule):!(*) ibm-replicationFilterAttr:
(objectclass=ibm-replicationWeeklySchedule):!(*) ibm-replicationFilterAttr:
(objectclass=*) : (*)複製トポロジー情報を抑止するには、まず、データのエク
スポート元のディレクトリー・サーバー・インスタンス内に項目を作成する必要があ
ります。この項目で、エクスポート時に使用するフィルター・プロパティを指定
します。ibm-replicationFilterAttr の値で、除外する項目と組み込む項目を指定しま
す。
```

例として、すべての「`ibm-replicagroup`」項目を除外する場合を考えてみましょう。これらの項目は、`objectclass` 属性に値「`ibm-replicaGroup`」があることで識別されます。この除外は、上に示す `ibm-replicationFilterAttr` の 2 番目の値によって実行されます。`ibm-replicationFilterAttr` の最後の値は、その他のすべての項目（複製トポロジーに関連する項目の条件に一致しない項目）のすべての属性を組み込む必要があることを示します。

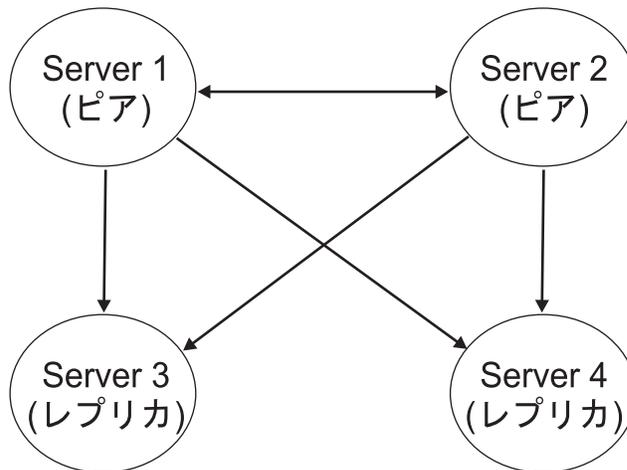
次のようにして、上記の項目を持つファイル `filterdn.ldif` を作成し、`ldapadd` コマンドを発行して、項目をディレクトリー・サーバー・インスタンスに追加します。

```
idsldapadd -D <binddn> -w <password> -f filterdn.ldif ディレクトリー・サー
バー・インスタンスから DB2 データベース情報をエクスポートし、複製関連デー
タを除外するには、次のように、新規に作成されたフィルター項目
cn=replicationfilter,cn=localhost の DN を、-n オプションを使用して指定します。
idsdb2ldif -I <instance_name> -o <output_file> -n
"cn=replicationfilter,cn=localhost" 生成される出力ファイルには、複製トポロ
ジー関連の項目は含まれません。
```

リカバリー手順

ここで説明する手順は、2 つのピア・マスター・サーバー (server 1、server 2) と 2 つのレプリカ・サーバー (server 3、server 4) から成るシステム・トポロジーに基づいています。

server 2 はフェイルオーバー・マスターとして動作します。したがって、server 1 がオフラインにならない限り、クライアント・マシンから直接更新を受信することはありません。



必要なリカバリー情報

複製トポロジーを作成した後、ここで説明する手順を実行する必要があります。

1. 各サーバーの構成ファイル (ibmslapd.conf) および鍵 stash ファイル (ibmslapddir.ksf および ibmslapdcfg.ksf) のコピーを作成し、それらのファイルを安全な場所に保管します。安全な場所とは、複製トポロジーに属さないバックアップ・マシンや、ディスケット、CD、テープなどのオフライン・メディアです。これらのファイルの情報は、トポロジーを変更する場合、または構成パラメーター (cn=Configuration 以下の項目) を変更する場合に限り更新する必要があります。既存のスキーマに変更を加えた場合、または新規のスキーマを追加した場合、スキーマ・ファイル (V3.* files) のコピーも同様に作成する必要があります。
2. **idsdbback** ユーティリティを使用して、毎日夜間にバックアップ・ディレクトリーを作成します。このディレクトリーを tar または zip 処理して、安全な場所に保管します。安全な場所とは、複製トポロジーに属さないバックアップ・マシンや、CD、テープなどのオフライン・メディアです。このバックアップ・ディレクトリーには、ディレクトリー内の全項目、サーバーの構成情報、およびスキーマ・ファイルを含めます。このバックアップ・ディレクトリーにより、24 時間分より価値のあるデータは失わずにすむことになります。また非ピーク時間には、このユーティリティを server 3 または server 4 に対して実行し、最新のデータを保管します。

重要: 復元を行う場合、障害が発生したオペレーティング・システムと同じオペレーティング・システムにデータをリストアする必要があります。同じオペレーティング・システムにリストアしないと、エラーが発生する場合があります。

データベース・バックアップ・ファイルの作成:

構成ツールかコマンド行ユーティリティーのいずれかを使用することで、バックアップ・ファイルを作成できます。

バックアップ・ファイルを作成する前に、すべてのデータをコピーできるだけの十分な容量があるか確認してください。必要なおおよその容量は、次のディレクトリーのサイズを合計すれば算出できます。

- `<dblocation>/<dbname>`
- `<dblocation>/ldap32kcont_/<dbname>`

デフォルトでは `<dblocation>` は、データベース・インスタンスのインストール・パスです。

サーバーを停止してからでないと、データベースのバックアップは作成できません。データベースをバックアップするには、以下のようにします。

バックアップ・ディレクトリーを作成したら、ディレクトリーとその内容を圧縮して、安全な場所に保管します。安全な場所とは、複製トポロジーに属さないバックアップ・マシンや、CD、テープなどのオフライン・メディアです。

構成ツールの使用:

構成ツールでは、以下に説明する手順を使用できます。

このタスクについて

手順

1. コマンド・プロンプトで `idsxcfg -I <instance_name>` と入力し、構成ツールを始動させます。
2. 左側のタスク・リストで「データベースのバックアップ」をクリックします。
3. 右の「データベースのバックアップ」ウィンドウで、「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・データおよび構成設定をバックアップするディレクトリーのパスを入力します。また、「ブラウズ」をクリックして、ディレクトリー・パスを探し出すこともできます。このバックアップ・ディレクトリーの正確なディレクトリー・パスをメモします。データを正常に復元するためには、この場所を正確に指定する必要があります。
4. バックアップ・ディレクトリーが存在していなくて、新しく作成する場合は、「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。
5. 「バックアップ」をクリックします。

コマンド・ラインの使用:

以下に示すコマンドをコマンド行ユーティリティーで使用することにより、バックアップ・ファイルを作成することができます。

このタスクについて

バックアップ・ディレクトリーがない場合は、ソース・サーバーとして使用しているサーバーにバックアップ・ディレクトリー、`<backupdir>` を作成します。次に、コマンド `idsdbback -k <backupdir> -I <instance_name>` を発行します。ここで、

backupdir は、作成するバックアップ・ディレクトリーの名前です。このバックアップ・ディレクトリーの正確なディレクトリー・パスをメモします。データを正常に復元するためには、この場所を正確に指定する必要があります。

データベースの復元:

構成ツールかコマンド行ユーティリティーのいずれかを使用して、データベースおよび構成情報を復元することができます。

最新のバックアップ・ディレクトリー・ファイルをサーバーにコピーし、解凍します。

注: このファイルは、バックアップした元のディレクトリーがあった正確な場所にコピーする必要があります。それ以外の場合、**idsdbrestore** は失敗します。

データベースを復元する前に、必ずサーバーを停止してください。データベースを復元するには、以下のようにします。

データベースおよび構成情報が復元されます。

構成ツールの使用:

Web 管理ツールで、ここに示されている手順を使用します。

このタスクについて

手順

1. コマンド・プロンプトで `idsxcfg -I <instance_name>` と入力し、構成ツールを始動させます。
2. 左側のタスク・リストで「データベースの復元」をクリックします。
3. 右側の「データベースの復元」ウィンドウの「バックアップ・ディレクトリー」フィールドに、バックアップしたディレクトリーのパスを入力します。代わりに、「参照」をクリックしてパスを指定することもできます。
4. 「データのみ復元する (構成設定は復元しない)」チェック・ボックスを選択します。
5. 「復元」をクリックします。

コマンド・ラインの使用:

データを復元するサーバーで、以下に示すコマンドを使用できます。

このタスクについて

1. 以下のコマンドを発行します。

```
idsdbrestore -k <backupdir> -I <instance_name> -n
```

backupdir には、復元に使用するバックアップ・ディレクトリーの名前を指定します。

シングル・サーバー障害からのリカバリー

ここで説明する手順に従って、シングル・サーバー障害からリカバリーできます。

このタスクについて

この手順を使用すると、例えばハード・ディスクを交換したサーバーなど、修復したサーバーを復元できます。この例では、server 3 を復元します。また Server 2 を server 3 の復元に使用します。

注: サーバーを新しいマシンに取り替える場合、前のマシンと同じホスト名を使用する必要があります。

重要: 以下の説明は、障害が発生したオペレーティング・システムと同じオペレーティング・システムにデータをリカバリーすることを前提としています。同じオペレーティング・システムにリカバリーしないと、エラーが発生してしまいます。

手順

1. server 3 に IBM Security Directory Server をインストールします。
2. server 3 で新規データベースを構成します。server 3 で以前に使用していたのと同じインスタンス所有者名、データベース名を使用します。
3. server 3 のバックアップ構成ファイル (ibmslapd.conf) と鍵 stash ファイル (ibmslapddir.ksf および ibmslapdfg.ksf) をリカバリー・ソース・メディアから server 3 にコピーします。**注:** リカバリーする場合は、障害が発生したときのオペレーティング・システムと同じオペレーティング・システムにリカバリーする必要があります。同じオペレーティング・システムにリカバリーしないと、エラーが発生する場合があります。
4. server 1 を静止します。idsldapexop -D <admin_dn> -w <admin_pw> -op quiesce -rc o=sample
5. server 1 が保留中の更新すべてを server 2 に複製するまで (ibm-replicationpendingchangeount が 0 になるまで) 待機します。
idsldapsearch -D <admin_dn> -w <admin_pw> -h <server1> -b <dn of agreement with server2> -s base objectclass=* ibm-replicationpendingchangeount
6. server 1 で、server 3 用の複製キューを消去します。idsldapexop -D <admin_dn> -w <admin_pw> -op controlqueue -skip all -ra <dn of agreement with server3>
7. server 1 で、server 3 との複製で記録されたすべてのエラーをクリアします。
idsldapexop -D <admin_dn> -w <admin_pw> -op controlreplerr -delete all -ra <dn of agreement with server3>
8. server 1 で、server 2 および server 3 への複製を中断します。idsldapexop -D <admin_dn> -w <admin_pw> -op controlrepl -action suspend -ra <dn of agreement with server2> idsldapexop -D <admin_dn> -w <admin_pw> -op controlrepl -action suspend -ra <dn of agreement with server3>
9. server 1 を静止解除し、更新の受け入れを再開できるようにします。
idsldapexop -D <admin_dn> -w <admin_pw> -op quiesce -end -rc o=sample
10. server 3 を停止します。
11. server 2 を停止します。
12. DB2 バックアップを使用して、server 2 のデータをバックアップします。

13. server 2 を始動し、server 1 でその複製キューを再開します。idsldapexop -op controlrepl -action resume -ra <dn of agreement with server2>
14. DB2 データを server 3 に復元します。
15. server 3 を始動し、server 1 に対する複製キューを再開します。 idsldapexop -op controlrepl -action resume -ra <dn of agreement with server3>

大規模障害からのリカバリー

この手順は、トポロジー内のすべてのサーバーで障害が発生し、すべてのサーバーを取り替える場合に使用できます。

このタスクについて

1. 新規のマシンに、以前使用していたのと同じホスト名が使用されているか確認します。
2. IBM Security Directory Server バージョン 6.3 を、すべての新規サーバーに再インストールします。
3. 各サーバーで新規データベースを構成します。以前と同じインスタンス所有者名およびデータベース名を使用します。
4. すべてのサーバーが停止していることを確認してください。
5. 最新のバックアップ・ディレクトリー・ファイルを各サーバーにコピーします。

注: このファイルは、バックアップした元のディレクトリーがあった正確な場所にコピーする必要があります。正確な場所にコピーしないと、**idsdbrestore** コマンドは失敗してしまいます。

6. 構成ツール、または **idsdbrestore** コマンドを使用して、各サーバーにデータベースを復元します。390 ページの『データベースの復元』を参照してください。
7. すべてのサーバーを再始動します。

トポロジーおよびデータは、障害が発生する前の状態 (障害発生前の 24 時間以内の状態) に復元されます。

マルチスレッド複製

ここで提供する情報および例により、マルチスレッド複製について詳しく知ることができます。

マルチスレッド複製機能は、現在の単一複製スレッドを最小で 3 つのスレッドに置き換え、複製合意を提供します。

- メイン・スレッド
- 送信側スレッド
- 受信側スレッド

マルチスレッド複製では、1 から 32 のコンシューマー接続をどこでも行えます。コンシューマー接続の数は、マシンのプロセッサの数と同じに設定します。

マルチスレッドを使用すると、サプライヤーは、コンシューマーからの応答を待つことなく、更新をコンシューマーに送信できます。

複製のバックログがある場合は、マルチスレッド複製への切り替えを検討することをお勧めします。候補となる環境の条件には、以下のようなものがあります。

- 更新率が高い
- 下位レベルのサーバーがない
- 共通 AES ソルトおよび同期化を使用している (暗号化が AES でパスワードが頻繁に更新される)
- 分岐が少ない (例えば、24 の各レプリカに対して 8 つの接続が合意を結んでいる場合などは分岐が多すぎる)
- 使用可能なサーバーおよび信頼できるネットワークがある
- データの整合性が重要でない
- すべての複製スケジュールを即時に実行する必要がある
- マルチプロセッサ・マシンを使用している

サーバーまたはネットワークの信頼性が低い場合、マルチスレッド複製は管理が難しくなります。

エラーが発生した場合、そのエラーはログに記録されるため、管理者はエラーを再現できます。ただし、エラー・ログはこまめにモニターする必要があります。以下の検索により、1 つのサーバーによって提供されるすべての合意の複製バックログが表示されます。

```
idsldapsearch -h supplier-host -D cn=admin -w ? -s sub
objectclass=ibm-replicationagreement
ibm-replicationpendingchangeount ibm-replicationstate
```

複製の状態がアクティブで保留カウントが増加している場合、更新率が低下しない限りバックログは減少しません。

複製エラー・テーブル

以下に示す情報を使用することにより、複製エラー・テーブルについて詳細を把握できます。

複製エラー・テーブルには、後でリカバリーが行えるように更新の失敗が記録されます。複製が開始されると、各複製合意ごとに記録された失敗の数がカウントされます。更新が失敗に終わると、このカウントは増加し、新しい項目がテーブルに追加されます。

複製エラー・テーブルの各項目には、以下の情報が記録されます。

- 複製合意の ID。
- 複製変更の ID。
- 更新が試行された時刻を示すタイム・スタンプ。
- 更新が試行された回数 (デフォルト値は 1 で更新が試行されるたびに 1 が加算されます)。
- コンシューマーからの結果コード。
- 更新に関連する複製操作の各種情報。例えば、DN、実際のデータ、コントロール、フラグなど。

サーバー構成の属性 `ibm-slapdReplMaxErrors` に指定されている値が **0** の場合、複製による更新処理はエラーが発生しても続行されます。属性 `ibm-slapdReplMaxErrors` は、複製構成項目の属性で動的に変更できます。

属性 `ibm-slapdReplMaxErrors` で指定した値が **0** より大きい場合に、複製合意のエラー件数とその値を超えると、複製では以下のいずれかのアクションが実行されます。

単一スレッド

複製はループ状態になり、失敗した更新の複製試行が繰り返されます。

マルチスレッド

複製が中断されます。

サーバーが単一接続を使用するように構成されている場合、60 秒待った後に同じ複製更新の送信が試行され、複製が成功するまで、または管理者が更新をスキップするまでこれが繰り返されます。

サーバーが複数の接続を使用するように構成されている場合、該当する合意の複製は中断されます。受信側スレッドは、送信された更新のステータスをポーリングし続けますが、更新は複製されません。複製を再開するには、ディレクトリー管理者が該当合意のエラーを少なくとも 1 つクリアするか、サーバー構成の動的変更を使用して制限値を大きくする必要があります。

詳しくは、「*IBM Security Directory Server Version 6.3 Programming Reference*」の『Replication error log extended operation』を参照してください。

複製を管理するための Web 管理タスク

Web 管理ツールを使用することにより、以下に示すタスクを実行できます。

このタスクについて

複製サブツリー

Web 管理ツールを使用することにより、複製サブツリーに対し以下のタスクを実行できます。

サブツリーの追加:

以下に示す指示により、サブツリーを追加することができます。

このタスクについて

注: この作業を実行するには、サーバーが稼働していることが必要です。

ナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。

- 「サブツリーの追加」をクリックします。
- 複製するサブツリーの DN を入力するか、「ブラウズ」をクリックして項目を展開し、サブツリーのルートにする項目を選択します。
- LDAP URL の形式でマスター・サーバー参照 URL を入力します。以下は入力例です。

非 SSL の場合:

```
ldap://<myservername>.<mylocation>.<mycompany>.com:<port>
```

SSL の場合:

```
ldaps://<myservername>.<mylocation>.<mycompany>.com:<port>
```

デフォルトの URL は ldap://localhost:389 です。

注: マスター・サーバー参照 URL はオプションです。これは以下の場合にのみ使用されます。

- サーバーが読み取り専用サブツリーを含む場合。
- サーバーの読み取り専用サブツリーに対する更新のために戻される参照 URL を定義する場合。
- 「**OK**」をクリックします。
- ヘッダー「複製サブツリー」の下にある「トポロジーの管理」パネルに、新しいサーバーが表示されます。

注: Linux、Solaris、および HP-UX プラットフォームでは、参照を追跡しているときにクライアントがハングした場合、システム環境で環境変数 LDAP_LOCK_REC が設定されていることを確認します。特定の値を指定する必要はありません。

```
set LDAP_LOCK_REC=anyvalue
```

サブツリーの編集:

このサブツリーとレプリカが更新を送信する宛先となるマスター・サーバーの URL を変更するには、このオプションを使用します。この処理は、マスター・サーバーのポート番号またはホスト名を変更し、マスターを別のサーバーに変更する場合に行う必要があります。以下に示す指示により、このことについて詳細を把握できます。

このタスクについて

手順

1. 編集するサブツリーを選択します。
2. 「アクションの選択」メニューを展開して、「サブツリーの編集」を選択し、「実行」をクリックします。
3. マスター・サーバーの参照 URL を入力します。これは、以下のような LDAP URL の形式にする必要があります。

```
ldap://<mynewservername>.<mylocation>.<mycompany>.com:<port>
```

4. このサブツリーのサーバーが担っていた役割 (マスター、レプリカ、転送のいずれであるか) に応じて、異なるラベルおよびボタンがパネルに表示されます。
 - サブツリーの役割がレプリカの場合は、サーバーがレプリカまたはフォワーダーの役目を果たすことを示すラベルが「サーバーをマスターにする」ボタンとともに表示されます。このボタンをクリックすると、Web 管理ツールの接続先サーバーがマスターになります。
 - 補助クラス (デフォルト・グループもサブエントリも存在しない) を追加することによってのみサブツリーが複製用に構成されている場合は、ラベル「このサブツリーは複製されていません」がボタン「サブツリーの複製」とともに

表示されます。このボタンをクリックすると、デフォルト・グループおよびサブエントリーが追加され、Web 管理ツールの接続先サーバーがマスターになります。

- マスター・サーバーのサブエントリーが見つからない場合は、ラベル「このサブツリーにはマスター・サーバーが定義されていません」がボタン「サーバーをマスターにする」とともに表示されます。このボタンをクリックすると、欠落しているサブエントリーが追加され、Web 管理ツールの接続先サーバーがマスターになります。

サブツリーの除去:

以下に記載されている手順により、サブツリーの除去ができます。

手順

1. 除去するサブツリーを選択します。
2. 「アクションの選択」メニューを展開して、「サブツリーの削除」を選択し、「実行」をクリックします。
3. 削除の確認を要求されたら、「OK」をクリックします。

タスクの結果

サブツリーが、「複製されたサブツリー」リストから除去されます。

注: この操作は、ibm-replicaGroup=default が空の項目の場合にのみ正常に終了します。

サブツリーの静止:

以下に示す情報により、サブツリーの静止を実行することができます。

このタスクについて

この機能は、保守を実行したり、トポロジーを変更したりする場合に便利です。この機能を使用すると、サーバーに対して行われる更新の数を最小化したり、更新を停止したりできます。静止されたサーバーは、クライアント要求を受け入れません。静止されたサーバーは、サーバー管理制御を使用する管理者からの要求のみを受け入れます。

この機能はブールです。

1. サブツリーを静止するには、「静止/静止解除」をクリックします。
2. 処理の確認を要求されたら、「OK」をクリックします。
3. サブツリーを静止解除するには、「静止/静止解除」をクリックします。
4. 処理の確認を要求されたら、「OK」をクリックします。

サブツリーのアクセス・コントロール・リストの編集:

以下に記述する情報を参照することにより、サブツリーのアクセス制御リストの編集について詳細を把握できます。

このタスクについて

複製情報 (レプリカ・サブエントリ、複製合意、スケジュール、場合によっては資格情報) は、特別なオブジェクト **ibm-replicagroup=default** に格納されます。ibm-replicagroup オブジェクトは、複製されたサブツリーのルート項目の直下に存在します。デフォルトでは、このサブツリーは、複製されたサブツリーのルート項目から ACL を継承します。この ACL は、複製情報へのアクセスの制御に不適切な場合があります。

必要な権限は以下のとおりです。

- 複製制御: ibm-replicagroup=default オブジェクトに対する書き込みアクセスを持つ (または所有者/管理者である) 必要があります。
- カスケード複製制御: ibm-replicagroup=default オブジェクトに対する書き込みアクセスを持つ (または所有者/管理者である) 必要があります。
- キュー制御: 複製合意への書き込みアクセスが必要です。

Web 管理ツール・ユーティリティーを使用して ACL プロパティを表示させたり、ACL を処理したりするには、以下を行います。

1. ACL を編集するサブツリーを選択します。
2. 「アクションの選択」メニューを展開して、「ACL の編集」を選択し、「実行」をクリックします。

ACL の編集方法については 558 ページの『ACL の処理』を、ACL の追加情報については 546 ページの『アクセス制御リスト』を参照してください。

資格情報

Web 管理ツールを使用することで、資格情報を定義、変更、または除去することができます。

資格情報の追加:

以下に示す指示により、Web 管理ツールを使用して資格情報を追加することができます。

このタスクについて

Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「資格情報の管理」をクリックします。

1. 資格情報の格納に使用する場所を、サブツリーのリストから選択します。Web 管理ツールでは、資格情報を 3 つの場所で定義できます。
 - **cn=replication,cn=localhost**: 資格情報を現在のサーバーにのみ保持します。注: 通常の複製では、cn=replication,cn=localhost に資格情報を配置することが推奨されます。これは、複製された資格情報をサブツリーに配置するよりも高いセキュリティが得られるためです。しかし、状況によっては、cn=replication,cn=localhost に配置した資格情報が使用できない場合もあります。
例えば serverA というサーバーの下にレプリカを追加しようとする場合、ユーザーが Web 管理ツールを使用して別のサーバー (serverB) に接続していると、「資格情報の選択」フィールドにオプション **cn=replication,cn=localhost**

が表示されません。これは、serverB に接続していると、serverA の **cn=localhost** の下の情報を読み取ったり更新したりできないからです。 **cn=replication,cn=localhost** を使用できるのは、 Web 管理ツールを使用して接続しているサーバーが、レプリカを追加しようとするサーバーと同じ場合に限られます。

- **cn=replication,cn=IBMpolicies** は、 Web 管理ツールを使用して接続しているサーバーが、レプリカを追加しようとするサーバーと同じでない場合であっても使用可能です。この場所に配置された資格情報はサーバーに複製されます。注：場所 **cn=replication,cn=IBMpolicies** を使用できるのは、 **IBMpolicies** をサポートする OID 1.3.18.0.2.32.18 がルート DSE の **ibm-supportedcapabilities** の下にある場合のみです。
- 複製されたサブツリー内の場合、資格情報は他のサブツリーで複製されます。複製されたサブツリーに配置する資格情報は、そのサブツリーの **ibm-replicagroup=default** 項目の下に作成されます。注：サブツリーが表示されない場合は、 394 ページの『サブツリーの追加』を参照し、複製するサブツリーの作成に関する詳細を確認してください。

2. 「追加」をクリックします。
3. 作成する資格情報の名前 (例: **mycreds**) を入力します。フィールド内では **cn=** が前に付加されます。
4. 使用する認証方式のタイプを選択し、「次へ」をクリックします。
 - 単純なバインド認証を選択した場合は、以下の手順を実行します。
 - a. **cn=any** など、サーバーがレプリカへのバインドに使用する DN を入力します。
 - b. **secret** など、サーバーがレプリカにバインドするときに使用するパスワードを入力します。
 - c. タイプミスがないことを確認するため、再度パスワードを入力します。
 - d. 必要に応じて、資格情報の要旨を入力します。
 - e. 「完了」をクリックします。

注：資格情報のバインド DN およびパスワードは、後で参照できるように記録しておいてください。レプリカ合意を作成する場合は、このパスワードが必要です。

- Kerberos 認証を選択した場合は、以下の手順を実行します。
 - a. Kerberos バインド DN を入力します。
 - b. **keyfile** を入力します (鍵データベース・ファイルの完全修飾ファイル仕様)。このフィールドを空白にすると、サーバーの LDAP サービス名が使用されます。注：このサーバーの LDAP サービス・プリンシパル名は **service/hostname@realm** です。これは標準 Kerberos 規約から取得されません。**service** は常に **ldap** です。例えば、Kerberos レルム「**MYTOWN.MYCOMPANY.COM**」内のホスト **myserver.mytown.mycompany.com** の場合、サーバーのプリンシパル名は **ldap/myserver.mytown.mycompany.com@MYTOWN.MYCOMPANY.COM** です。サーバーはシステム TCP/IP 構成からホスト名を取得します。レルム名は、「**セキュリティー・プロパティー (Security properties)**」パネルの「**Kerberos**」タブで構成されたレルム名から取得されます。

- c. 必要に応じて、資格情報の要旨を入力します。その他の情報は必要ありません。詳細については、254 ページの『Kerberos のセットアップ』を参照してください。
- d. 「完了」をクリックします。

「Kerberos」パネルには、`ibm-kn=xxx@realm` の形式でバインド DN を指定できるオプション、鍵タブ・ファイル名 (Web 管理ツールで鍵ファイルとして参照される) を指定できるオプションがあります。バインド DN が指定された場合、サーバーは指定されたプリンシパル名を使用して、コンシューマー・サーバーに対して認証を行います。それ以外の場合、サーバーの Kerberos サービス名 (`ldap/host-name@realm`) が使用されます。

鍵タブ・ファイルを使用する場合、サーバーはその鍵タブ・ファイルを使用して、指定したプリンシパル名の資格情報を取得します。鍵タブ・ファイルを指定しないと、サーバーは、サーバーの Kerberos 構成で指定されている鍵タブ・ファイルを使用します。

デフォルトでは、サプライヤーは独自のサービス・プリンシパルを使用してコンシューマーとバインドします。例えば、サプライヤーの名前が `master.our.org.com` であり、レルムが `SOME.REALM` の場合の DN は、**`ibm-Kn=ldap/master.our.org.com@SOME.REALM`** です。レルムの値には、大文字小文字の区別はありません。

注: 複数のサプライヤーが Kerberos 認証を使用して同じコンシューマーに対して複製を行う場合、すべてのサプライヤーが同じ Kerberos プリンシパルを使用するように構成する必要があります。デフォルトのままだとそれぞれの Kerberos サービス名を使用してしまうので注意してください。

- 証明書認証を使用した SSL を選択して、サーバーの証明書を使用している場合は、追加情報を指定する必要はありません。サーバーの証明書以外の証明書を使用する場合は、以下を行います。
 - a. 鍵ファイル名を入力します。
 - b. 鍵ファイル・パスワードを入力します。
 - c. 確認のため、鍵ファイル・パスワードを再入力します。
 - d. 鍵ラベルを入力します。
 - e. 必要に応じて、要旨を入力します。
 - f. 暗号ハードウェアの PKCS#11 サポートを使用可能にする場合は、「**PKCS#11 インターフェース・サポートを使用可能にする**」チェック・ボックスを選択します。
 - g. 「完了」をクリックします。

詳細については、154 ページの『Secure Sockets Layer』を参照してください。

注: Web 管理ツールで追加マスター操作を行ってコンシューマーに資格情報を追加する際、外部の資格情報オブジェクトを選択する場合は、Web サーバーが実行されているマシンで以下の設定を構成する必要があります。

- JCE プロバイダーと CMS プロバイダーを登録するための以下の 2 つの項目が `JAVA_HOME\jre\lib\security\java.security` ファイルに存在するかどうかを確認します。項目が存在しない場合、次の項目を `java.security` ファイルに追加します。

```
security.provider.X=com.ibm.crypto.provider.IBMJCE
security.provider.X+1=com.ibm.security.cmskeystore.CMSProvider
```

ここで、**X** は所定の順序の次の番号です。

- GSKit をインストールし、プラットフォームに応じて `<install_location>gsk8¥lib` または `<install_location>gsk8¥lib64` をシステム・パスに追加する必要があります。
- マスター・サーバーは、レプリカに接続してレプリカに資格情報を作成する際、鍵ファイルに含まれている資格情報を使用します。この鍵ファイルを Web 管理ツールで読み取れるようにするために、Windows プラットフォームの場合は `C:¥temp` に、UNIX の場合は `/tmp` に鍵ファイルを格納する必要があります。

資格情報の変更:

以下に示す指示により、Web 管理ツールで資格情報を変更することができます。

このタスクについて

Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「資格情報の管理」をクリックします。

1. サブツリーを選択して、「資格情報の表示」をクリックします。
2. 選択したサブツリーの資格情報ボックスで、変更する資格情報を選択し「編集」をクリックします。
 - 資格情報がシンプル認証の場合。「資格情報の編集」パネルで変更できます。
 - バインド DN
 - パスワード
 - 資格情報の説明
 - 資格情報が Kerberos 認証の場合。「資格情報の編集」パネルで変更できます。
 - バインド DN
 - 鍵ファイル
 - 資格情報の説明
 - 資格情報が証明書認証付きの SSL の場合。
 - a. 「資格情報の編集」パネルで変更できます。
 - 鍵ファイル
 - パスワード
 - 鍵ラベル
 - 資格情報の説明
 - b. 暗号ハードウェアの PKCS#11 サポートを使用可能にする場合は、「PKCS#11 インターフェース・サポートを使用可能にする」チェック・ボックスを選択します。
3. 完了したら、「OK」をクリックします。

資格情報の除去:

以下に示す指示により、Web 管理ツールで資格情報を除去することができます。

このタスクについて

Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「資格情報の管理」をクリックします。

手順

1. サブツリーを選択して、「資格情報の表示」をクリックします。
2. 選択したサブツリーの資格情報ボックスで、除去する資格情報を選択し「除去」をクリックします。
3. 資格情報オブジェクトを除去するかどうか確認するメッセージが表示されます。「OK」をクリックして資格情報を除去するか、「キャンセル」をクリックして「資格情報の管理」パネルに戻ります。後者を選択した場合、変更は保存されません。

資格情報 ACL の管理:

以下に示す指示により、Web 管理ツールを使用して資格情報 ACL を管理することができます。

このタスクについて

他のユーザーに資格情報の操作を許可する場合、この情報を使用します。この機能を使用可能にするには、ACL を割り当てる必要があります。

Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「資格情報の管理」をクリックします

1. サブツリーを選択して、「資格情報の表示」をクリックします。
2. 選択したサブツリーの資格情報ボックスで、ACL を変更する資格情報を選択し「ACL の編集」をクリックします。
3. ACL の編集については、558 ページの『ACL の処理』を参照してください。

トポロジー管理

IBM Security Directory Server は、複製トポロジー内のコンシューマー・サーバーに対するスキーマの更新の複製をサポートしています。トポロジーは複製されたサブツリーに固有のものです。

トポロジーの表示:

以下に示す指示により、トポロジーを表示することができます。

このタスクについて

注: この作業を実行するには、サーバーが稼働していることが必要です。

ナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。

1. 表示するサブツリーを選択して、「トポロジーの表示」をクリックします。
- 複製トポロジー・リストにトポロジーが表示されます。トポロジーを展開します。このリストから、以下のことができます。
- マスターの追加

- レプリカの追加
- ゲートウェイ・サーバーの管理
- 合意の編集
- 複製スケジュールの表示
- 複製エラーの表示
- サーバーに対するトポロジー内での別の役割の割り当て
- サーバーの削除

ピア・マスターまたはゲートウェイ・サーバーの追加:

以下に示す指示により、ピア・マスターまたはゲートウェイ・サーバーを追加する方法を把握できます。

このタスクについて

注: この作業を実行するには、サーバーが稼働していることが必要です。

ナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。

1. 複製するサブツリーを選択して、「トポロジーの表示」をクリックします。
2. 既存のトポロジーを表示する場合は、「複製トポロジー」の隣のボックスをクリックして、サプライヤー・サーバーのリストを展開します。
3. 「マスターの追加」をクリックします。

「マスターの追加」ウィンドウの「サーバー」タブで、以下の手順を実行します。

- このサーバーをゲートウェイ・サーバーにするには、「サーバーはゲートウェイです」を選択し、サーバーをマスター・サーバーとして追加するには、「サプライヤー・ゲートウェイ」を選択してから、ドロップダウン・リストからサーバーを選択します。
- 「サーバーのホスト名:ポート」ドロップダウン・リストから、マスター・サーバー用の LDAP サーバーを選択します。

コンソール・サーバーに登録されていない別のサーバーをマスター・サーバーとして指定する場合は、「サーバーのホスト名:ポート」ドロップダウン・リストから「以下からの項目を使用します」項目を選択し、マスター・サーバーのホスト名およびポート番号を `hostname:port` の形式でフィールドに入力します。

注: デフォルトのポートは、非 SSL の場合 389、SSL の場合 636 です。

- SSL 通信を使用可能にするには、「SSL 暗号化を使用可能にする」チェック・ボックスを選択します。
- サーバー名を入力するか、ホスト名を使用する場合はフィールドを空白にします。
- サーバー ID を入力します。ピア・マスターを作成しているサーバーが実行中の場合は、「サーバー ID の取得」をクリックすると、自動的にこのフィールドが事前に入力されます。
- サーバーの説明を入力します。

- 他のマスター・サーバーと通信するためにサーバーが使用する資格情報を指定する必要があります。「**選択**」をクリックします。

注: Web 管理ツールでは、以下の場所で資格情報を定義できます。

- **cn=replication,cn=localhost** は、その資格情報を使用するサーバーのみに資格情報を保持します。資格情報は **cn=replication,cn=localhost** に置くほうが安全です。
- **cn=replication,cn=IBMpolicies** は、Web 管理ツールを使用して接続しているサーバーが、レプリカを追加しようとするサーバーと同じでない場合であっても使用可能です。この場所に配置された資格情報はサーバーに複製されます。

注: 場所 **cn=replication,cn=IBMpolicies** を使用できるのは、**IBMpolicies** をサポートする OID 1.3.18.0.2.32.18 がルート DSE の **ibm-supportedcapabilities** の下にある場合のみです。

- 複製されたサブツリー内の場合、資格情報は他のサブツリーで複製されます。複製されたサブツリーに置かれる資格情報は、そのサブツリーの **ibm-replicagroup=default** 項目の下に作成されます。
1. 使用する資格情報の場所を選択します。**cn=replication,cn=localhost** がよく使用されます。
 2. すでに資格情報のセットがある場合は、「**資格情報の表示**」をクリックします。
 3. 資格情報のリストを展開して、使用する資格情報を選択します。
 4. 「**OK**」をクリックします。
 5. 既存の資格情報がない場合は、「**追加**」をクリックして資格情報を追加します。合意資格情報の詳細については、397 ページの『資格情報の追加』を参照してください。

「**追加**」タブで以下の手順を実行します。

1. ドロップダウン・リストから複製スケジュールを指定するか、または「**追加**」をクリックして複製スケジュールを作成します。417 ページの『複製スケジュールの作成』を参照してください。
2. サプライヤー機能のリストから、コンシューマーに複製しない機能を選択解除できます。

リリースの異なるサーバーがネットワークに混在している場合は、古いリリースで使用不能な機能が新しいリリースで使用可能です。フィルター ACL (547 ページの『フィルターに処理された ACL』) やパスワード・ポリシー (235 ページの『パスワード・ポリシー設定』) などの一部の機能は、他の変更と共に複製される運用属性を利用します。ほとんどの場合、これらの機能を使用するには、すべてのサーバーでこの機能がサポートされていることが必要です。すべてのサーバーがこの機能をサポートしない場合は、この機能を使用しないことが推奨されます。例えば、サーバーごとに異なる ACL を有効にすることが必要ない場合があります。しかし、ある機能をサポートしているサーバーでその機能を使用し、その機能をサポートしていないサーバーにはその機能に関連する変更を複製しない場合もあります。このような場合、機能リストを使用して、複製しない機能にマークを付けることができます。

3. サプライヤーの資格情報の動的更新を使用可能にする場合は、「**コンシューマーに関する資格情報の追加**」チェック・ボックスをチェックします。これを選択すると、作成するサーバーの構成ファイルのサプライヤー情報が自動的に更新されます。これにより、トポロジー情報をサーバーに複製できるようになります。
 - このコンシューマー・サーバーの管理者 DN を入力します。例: cn=root。

注: サーバーの構成プロセスで作成した管理者 DN が cn=root の場合、省略せずに完全な管理者 DN を入力します。root のみを入力しないよう注意してください。
 - このコンシューマー・サーバーの管理者パスワードを入力します。例: secret。
4. 「**OK**」をクリックします。
5. 新規マスター・サーバーと既存のサーバー間のサプライヤー合意およびコンシューマー合意がリスト表示されます。作成しない合意のチェック・マークを外してください。ゲートウェイ・サーバーを作成する場合、これは特に重要です。
6. 「**継続 (Continue)**」をクリックします。
7. 必要な追加アクションを知らせるメッセージが表示される場合があります。適切なアクションを実行するか、確認します。完了したら、「**OK**」をクリックします。
8. 適切な資格情報を追加します。

注: 場合によっては、「資格情報の選択」パネルが開き、cn=replication,cn=localhost 以外の場所に存在する資格情報が要求されます。このような場合は、cn=replication,cn=localhost 以外の場所に存在する資格情報オブジェクトを指定する必要があります。既存の資格情報セットからサブツリーで使用する資格情報を選択するか、新規の資格情報を作成します。397 ページの『資格情報の追加』を参照してください。

9. サプライヤーの資格情報の動的更新を使用可能にする場合は、「**コンシューマーに関する資格情報の追加**」チェック・ボックスをチェックします。これを選択すると、作成するサーバーの構成ファイルのサプライヤー情報が自動的に更新されます。これにより、トポロジー情報をサーバーに複製できるようになります。
 - このコンシューマー・サーバーの管理者 DN を入力します。例: cn=root。

注: サーバーの構成プロセスで作成した管理者 DN が cn=root の場合、省略せずに完全な管理者 DN を入力します。root のみを入力しないよう注意してください。
 - このコンシューマー・サーバーの管理者パスワードを入力します。例: secret。
10. ピア・マスターを作成するには、「**OK**」をクリックします。
11. 必要な追加アクションを知らせるメッセージが表示される場合があります。適切なアクションを実行するか、確認します。完了したら、「**OK**」をクリックします。336 ページの『複製の開始』を参照してください。

注: Web 管理ツールで追加マスター操作を行ってコンシューマーに資格情報を追加する際、外部の資格情報オブジェクトを選択する場合は、IBM WebSphere Application Server が実行されているマシンで以下の設定を構成する必要があります。

•

JCE プロバイダーと CMS プロバイダーを登録するための以下の 2 つの項目が `JAVA_HOME¥jre¥lib¥security¥java.security` ファイルに存在するかどうかを確認します。項目が存在しない場合、次の設定を入力して、この項目を `java.security` ファイルに追加します。

```
security.provider.X=com.ibm.crypto.provider.IBMJCE
security.provider.X+1=com.ibm.security.cmskeystore.CMSProvider
```

ここで、**X** は所定の順序の次の番号です。

- IBM WebSphere Application Server を再始動します。
- GSKit をインストールし、プラットフォームに応じて `gsk8¥lib` または `gsk8¥lib64` をシステム・パスに追加する必要があります。
- マスター・サーバーは、レプリカに接続してレプリカに資格情報を作成する際、鍵ファイルに含まれている資格情報を使用します。この鍵ファイルを Web 管理ツールで読み取れるようにするために、Windows プラットフォームの場合は `C:¥temp` に、UNIX の場合は `/tmp` に鍵ファイルを格納する必要があります。

レプリカ・サーバーの追加:

以下に示す情報により、レプリカ・サーバーを追加する方法を把握できます。

このタスクについて

注: この作業を実行するには、サーバーが稼働していることが必要です。

ナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。

手順

1. 複製するサブツリーを選択して、「トポロジーの表示」をクリックします。
2. 既存のサーバーの隣のボックスをクリックして、サプライヤー・サーバーのリストを展開します。
3. サプライヤー・サーバーを選択して、「レプリカの追加」をクリックします。

タスクの結果

「レプリカの追加」ウィンドウの「サーバー」タブで、以下の手順を実行します。

- 「サーバーのホスト名:ポート」ドロップダウン・リストから、レプリカ・サーバー用の LDAP サーバーを選択します。
コンソール・サーバーに登録されていない別のサーバーをレプリカ・サーバーとして指定する場合は、「サーバーのホスト名:ポート」ドロップダウン・リストから「以下からの項目を使用します」項目を選択し、レプリカ・サーバーのホスト名およびポート番号を `hostname:port` の形式でフィールドに入力します。デフォルトのポートは、非 SSL の場合 389、SSL の場合 636 です。
- SSL 通信を使用可能にするかどうかを選択します。

- レプリカ名を入力するか、ホスト名を使用する場合はフィールドをブランクにします。
 - レプリカ ID を入力します。レプリカを作成する対象のサーバーが実行中の場合、「**レプリカ ID の取得**」をクリックすると、このフィールドが自動的に設定されます。
 - レプリカ・サーバーの説明を入力します。
 - マスターと通信するためにレプリカが使用する資格情報を指定する必要があります。「**選択**」をクリックします。注: Web 管理ツールでは、以下の場所で資格情報を定義できます。
 - **cn=replication,cn=localhost** は、その資格情報を使用するサーバーのみに資格情報を保持します。資格情報は **cn=replication,cn=localhost** に置くほうが安全です。
 - **cn=replication,cn=IBMpolicies** は、Web 管理ツールを使用して接続しているサーバーが、レプリカを追加しようとするサーバーと同じでない場合であっても使用可能です。この場所に配置された資格情報はサーバーに複製されます。場所 **cn=replication,cn=IBMpolicies** を使用できるのは、**IBMpolicies** をサポートする **OID 1.3.18.0.2.32.18** がルート **DSE** の **ibm-supportedcapabilities** の下にある場合のみです。
 - 複製されたサブツリー内の場合、資格情報は他のサブツリーで複製されます。複製されたサブツリーに置かれる資格情報は、そのサブツリーの **ibm-replicagroup=default** 項目の下に作成されます。
1. 使用する資格情報の場所を選択します。 **cn=replication,cn=localhost** がよく使用されます。
 2. すでに資格情報のセットがある場合は、「**資格情報の表示**」をクリックします。
 3. 資格情報のリストを展開して、使用する資格情報を選択します。
 4. 「**OK**」をクリックします。
 5. 既存の資格情報がない場合は、「**追加**」をクリックして資格情報を追加します。合意資格情報の詳細については、397 ページの『資格情報の追加』を参照してください。

「**追加**」タブで以下の手順を実行します。

1. ドロップダウン・リストから複製スケジュールを指定するか、または「**追加**」をクリックして複製スケジュールを作成します。417 ページの『複製スケジュールの作成』を参照してください。
2. サプライヤー機能のリストから、コンシューマーに複製しない機能を選択解除できます。

リリースの異なるサーバーがネットワークに混在している場合は、古いリリースで使用不能な機能が新しいリリースで使用可能です。ACL のフィルター操作 (547 ページの『フィルターに処理された ACL』) やパスワード・ポリシー (235 ページの『パスワード・ポリシー設定』) などの一部の機能は、他の変更と共に複製される運用属性を利用します。ほとんどの場合、これらの機能を使用するには、すべてのサーバーでこの機能がサポートされていることが必要です。すべてのサーバーがこの機能をサポートしない場合は、この機能を使用しないことが推奨されます。例えば、サーバーごとに異なる ACL を有効にすることが必要ない場合があります。しかし、ある機能をサポートしているサーバーでその機能

を使用し、その機能をサポートしていないサーバーにはその機能に関連する変更を複製しない場合もあります。このような場合、機能リストを使用して、複製しない機能にマークを付けることができます。

- 複製方式として「単一スレッド」または「マルチスレッド」を選択します。「マルチスレッド」を選択する場合、複製で使用する接続数 (2 から 32 の間) を指定する必要があります。デフォルトの接続数は 2 です。
- サプライヤーの資格情報の動的更新を使用可能にする場合は、「**コンシューマーに関する資格情報の追加**」チェック・ボックスをチェックします。これを選択すると、作成するサーバーの構成ファイルのサプライヤー情報が自動的に更新されます。これにより、トポロジー情報をサーバーに複製できるようになります。
 - このコンシューマー・サーバーの管理者 DN を入力します。例えば、cn=root と指定します。**注:** サーバーの構成プロセスで作成した管理者 DN が cn=root の場合、省略せずに完全な管理者 DN を入力します。root のみを入力しないよう注意してください。
 - このコンシューマー・サーバーの管理者パスワードを入力します。例: secret。
- レプリカを作成するには、「**OK**」をクリックします。
- 追加のアクションが必要であることを示すメッセージが表示されます。「**OK**」をクリックします。

注:

- サーバーを追加レプリカとしてさらに追加する場合、または複雑なトポロジーを作成する場合は、マスター・サーバー上のトポロジーの定義を完了するまでは、333 ページの『レプリカへのデータのコピー』 または 414 ページの『レプリカへのサプライヤー情報の追加』 を実行しないでください。トポロジーの完成後に *masterfile.ldif* を作成すると、そのファイルにトポロジー合意の完全なコピーとマスター・サーバーのディレクトリー項目が含まれます。このファイルを各サーバーにロードすれば、それぞれのサーバーは同じ情報を持つようになります。
- Web 管理ツールを使用した「レプリカの追加」操作でコンシューマーに資格情報を追加する際、外部の資格情報オブジェクトを選択する場合は、注にある情報を参照してください。

サーバーの除去:

ここで説明する手順に従って、サーバーを除去することができます。

このタスクについて

ナビゲーション領域で「複製管理」カテゴリーを展開し、「トポロジーの管理」をクリックします。

手順

- 所要のサブツリーを選択して、「トポロジーの表示」をクリックします。
- トポロジーから除去するサーバーを選択します。
- 「削除」をクリックします。
- 削除の確認を要求されたら、「**OK**」をクリックします。

タスクの結果

注: トポロジーからレプリカを除去する際、サプライヤー資格情報項目を再度使用するマスター・サーバーがない場合は、必ずコンシューマーからその資格情報項目を削除してください。マスター・サーバーはその下の合意はどれも使用しません。400 ページの『資格情報の除去』を参照してください。

サーバーの移動またはプロモート:

ここで説明する手順に従って、サーバーを移動またはプロモートすることができます。

このタスクについて

ナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。

手順

1. 所要のサブツリーを選択して、「トポロジーの表示」をクリックします。
2. 必要なサーバーを選択し、「移動」をクリックします。
3. レプリカを移動するサーバーを選択するか、「複製トポロジー」を選択し、レプリカをマスターにプロモートします。「移動」をクリックします。
4. 「追加のサプライヤー合意の作成」が表示されます。サーバーの役割に適さないサプライヤー合意を選択解除します。作成するそれぞれの新規サプライヤー合意の資格情報およびコンシューマー情報を選択するよう要求されます。他のサーバーから新規プロモートされたサーバーへの既存のサプライヤー合意は依然として有効であり、再作成する必要はありません。注: 場合によっては、「資格情報の選択」パネルが開き、cn=replication,cn=localhost 以外の場所に置かれている資格情報を入力するよう求められます。このような場合は、cn=replication,cn=localhost 以外の場所に存在する資格情報オブジェクトを指定する必要があります。サブツリーが資格情報の既存のセットの形成に使用する資格情報を選択するか、または新しい資格情報を作成します。資格情報項目は、他のマスターに存在するか作成するかする必要があります。397 ページの『資格情報の追加』を参照してください。
5. 「OK」をクリックします。

タスクの結果

トポロジー・ツリーの変更はサーバーの移動に反映されます。

詳細については、362 ページの『ピア複製を持つ複雑なトポロジーのセットアップ』を参照してください。

マスターのデモート:

ここで提供する情報に従って、マスターをサーバーにデモートすることができます。

このタスクについて

サーバーの役割をマスターからレプリカへ変更する場合は、ナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。

1. Web 管理ツールをデモート対象のサーバーに接続します。
2. 「トポロジーの管理」をクリックします。
3. サブツリーを選択し、「トポロジーの表示」をクリックします。
4. デモートするサーバーを選択し、「移動」をクリックします。
5. デモートするサーバーを置くサーバーを選択し、「移動」をクリックします。
6. デモートするサーバーの合意をすべて削除します。「はい」をクリックします。

マスター・サーバーのダウン時にレプリカ・サーバーをマスターにプロモートする
:

ここで説明する手順に従って、マスター・サーバーのダウン時にレプリカ・サーバーをマスター・サーバーにプロモートすることができます。

このタスクについて

:

Web 管理の使用:

ここで説明する手順に従い、Web 管理ツールを使用してレプリカ・サーバーをプロモートすることができます。

このタスクについて

まず Web 管理ツールを使用して、マスターに変更するレプリカ・サーバーにログインします。

1. Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。
2. 既存のレプリカの役割を編集するには、該当する行を選択し、「アクションの選択」リストから「サブツリーの編集」を選択して、「実行」をクリックします。
3. 「サーバーをマスターにする」ボタンをクリックして、サーバーの役割をマスターに変更します。
4. 「OK」をクリックして、設定を保存します。

コマンド・ラインの使用:

ここで説明するコマンドをコマンド行で発行することにより、レプリカ・サーバーをプロモートすることができます。

このタスクについて

レプリカ・サーバーをマスターにプロモートするには、まず以下のようにして `ldif` レコードを作成する必要があります。`ldif` レコードでは、`ibm-replicaServerId` 属性の値をレプリカ・サーバーまたはコンシューマー・サーバーのサーバー ID と同じにする必要があります。この値は、レプリカの `ibmslapd.conf` ファイルから、または

レプリカに対して rootDSE 検索を実行することによって取得できます。次に、以下に示すように ldapadd コマンドを実行して、この値をレプリカ/コンシューマーに追加します。

```
ldapadd -h <ldaphost> -p <port> -D cn=root -w root -f promote.ldif -k
```

```
where promote.ldif file contains :
dn: cn=<any_name>,ibm-replicaGroup=default,o=sample
objectclass: top
objectclass: ibm-replicaSubentry
ibm-replicaServerId: <server ID of replica or consumer server>
ibm-replicationServerIsMaster: true
cn: master
description: master server
```

レプリカをマスターにプロモートした後に再度デモートする場合は、前に追加した項目を除去する必要があります。

ゲートウェイ・サーバーの管理:

ここで提供する情報に従って、ゲートウェイ・サーバーを管理することができます。

このタスクについて

複製サイトのゲートウェイ・サーバーの役割をマスター・サーバーに持たせるかどうかを指定できます。

マスターをゲートウェイ・サーバーに指定するには、ナビゲーション領域の「複製管理」カテゴリーを展開して、「トポロジーの管理」をクリックします。

1. 表示するサブツリーを選択して、「トポロジーの表示」をクリックします。
2. 「ゲートウェイ・サーバーの管理」をクリックします。
3. 「マスター・サーバー」ボックスから、ゲートウェイ・サーバーにするサーバーを選択します。
4. 「ゲートウェイの作成」をクリックします。サーバーが「マスター・サーバー」ボックスから「ゲートウェイ・サーバー」ボックスに移動します。
5. 「OK」をクリックします。

ゲートウェイ・サーバーの役割をマスター・サーバーから除去するには、以下の手順を実行します。

1. 「ゲートウェイ・サーバーの管理」をクリックします。
2. 「ゲートウェイ・サーバー」ボックスから、マスター・サーバーにするサーバーを選択します。
3. 「マスターの作成」をクリックします。サーバーが「ゲートウェイ・サーバー」ボックスから「マスター・サーバー」ボックスに移動します。
4. 「OK」をクリックします。

注: 各複製サイトに作成できるゲートウェイ・サーバーの数は 1 つだけです。トポロジーに追加ゲートウェイ・サーバーを作成する場合、Web 管理ツールはそのゲートウェイをピア・サーバーとして扱い、トポロジー内のすべてのサーバーに対する合意を作成します。他のゲートウェイ・サーバーが所有していない合意、または複製サイト内のゲートウェイ内に存在しない合意は必ず選択解除してください。

詳細については、370 ページの『ゲートウェイ・トポロジーのセットアップ』を参照してください。

合意の編集:

レプリカについては、以下に示す情報を変更できます。

このタスクについて

「サーバー」タブで変更可能な情報は以下に限られます。

- ホスト名およびポート

注: SSL 使用不可から SSL 使用可能に切り替える場合、またはその逆の切り替えを行う場合のみ、ポートは編集可能です。

- SSL を使用可能にする
- 説明
- 資格情報 - 397 ページの『資格情報の追加』を参照してください。

「追加」タブでは、以下の情報を変更できます。

- 複製スケジュール - 417 ページの『複製スケジュールの作成』を参照してください。
- コンシューマー・レプリカに複製される機能を変更します。サプライヤー機能のリストから、コンシューマーに複製しない機能を選択解除できます。
- 複製方式
- コンシューマー情報
- 完了したら、「OK」をクリックします。

複製スケジュールの表示:

ここで説明する手順に従って、複製スケジュールを表示することができます。

このタスクについて

Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。

手順

1. 表示するサブツリーを選択して、「トポロジーの表示」をクリックします。
2. 表示するマスター・サーバーまたはゲートウェイ・サーバーを選択します。
3. 「スケジュールの表示」をクリックします。

タスクの結果

選択したサーバーとそのコンシューマー間に複製スケジュールが存在する場合は、そのスケジュールが表示されます。これらのスケジュールを変更および削除できません。スケジュールが存在していなくて作成する場合は、Web 管理ツールのナビゲーション領域にある「スケジュールの管理」機能を使用する必要があります。スケジュールの管理については、417 ページの『複製スケジュールの作成』を参照してください。

サーバー情報の表示:

Web 管理ツールを使用して、サーバーの情報を表示できます。

このタスクについて

Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします

手順

1. 表示するサブツリーを選択して、「トポロジーの表示」をクリックします。
2. 表示するサーバーを選択します。
3. 「サーバーの表示」をクリックして、「サーバーの表示」パネルを表示します。

タスクの結果

「サーバーの表示」パネルには、以下の情報が表示されます。

サーバー名

このフィールドには、ディレクトリー・サーバー・インスタンスが稼働しているサーバーの名前が表示されます。この情報は、hostname:port の形式で表示されます。

ホスト名

このフィールドには、ディレクトリー・サーバー・インスタンスが稼働しているマシンのホスト名が表示されます。

ポート このフィールドには、サーバーが listen している非セキュア・ポートが表示されます。

サーバー ID

このフィールドには、サーバーの最初の始動時にサーバーに割り当てられる固有の ID が表示されます。この ID は、サーバーの役割を判別するために複製トポロジーで使用されます。

役割 このフィールドには、複製トポロジー内のサーバーの構成済みの役割が表示されます。

構成モード

このフィールドは、サーバーが構成モードで稼働しているかどうかを示します。TRUE の場合、サーバーは構成モードです。FALSE の場合、サーバーは構成モードではありません。

インスタンス名

このフィールドには、サーバーで稼働しているディレクトリー・サーバー・インスタンスの名前が表示されます。

セキュリティー

このフィールドには、サーバーが listen しているセキュア SSL ポートが表示されます。

サーバー名、ID、役割、およびコンシューマー情報が表示されます。

サーバー・エラーの表示:

Web 管理ツールを使用して、サーバーのエラーを表示することができます。

このタスクについて

複製中に発生したエラーのために完了しなかった複製の更新を表示させることができます。

Web 管理ツールのナビゲーション領域で「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします

手順

1. 表示するサブツリーを選択して、「トポロジーの表示」をクリックします。
2. 表示するサーバー (レプリカ合意) を選択します。
3. 「エラーの表示」をクリックします。

タスクの結果

サブツリー、サプライヤー、およびコンシューマー情報が表示されます。複製エラーが表示されるテーブルでは、以下の情報が提供されます。

ID の変更

失敗した更新に割り当てられた ID。

最終更新時刻

項目の複製を最後に試行した時刻を示します。

試行回数

項目を複製しようとした試行の回数を示します。

結果コード

項目の複製を最後に試行したときに取得した結果コード。

注: これらの情報は、障害番号順に表示されます。障害番号は、障害が発生すると割り当てられます。障害番号と変更 ID は同じではありません。変更 ID が定数なのに対して、障害番号は試行の失敗ごとに変更されます。

エラーを選択後、以下のアクションを実行できます。

- 「詳細の表示」をクリックすると、エラーについての詳細な情報が表示されます。
- 「再試行」をクリックして、更新を再度試行します。
- 「除去」をクリックして、複製エラー管理テーブルからエラーを除去します。

以下を行うこともできます。

- 「すべて再試行」をクリックして、すべての更新を再度試行します。
- 「すべて除去」をクリックして、複製エラー管理テーブルからすべてのエラーを除去します。

詳細については、419 ページの『キューの管理』を参照してください。

レプリカへのサプライヤー情報の追加:

以下に示す情報を使用することにより、サプライヤー情報をレプリカに追加することができます。

このタスクについて

コンシューマー (レプリカ) への資格情報の追加を選択しなかった場合、またはレプリカへの資格情報の追加で問題が発生した場合、レプリカの構成を変更して、どのサプライヤーがレプリカに対する変更を複製できる権限を持つかを識別できるようにする必要があります。また参照をマスターに追加する必要があります。

レプリカを作成しているマシンで、以下の手順を実行します。

1. ナビゲーション領域で「複製管理」を展開し、「複製プロパティの管理」をクリックします。
 2. 「追加」をクリックします。
 3. 「複製されたサブツリー」ドロップダウン・メニューからサプライヤーを選択するか、サプライヤー資格情報を構成する複製されたサブツリーの名前を入力します。 サプライヤー資格情報を編集している場合は、このフィールドは編集できません。
 4. 複製バインド DN を入力します。この例では `cn=any` です。注: 状況に応じて、以下の 2 つのいずれかのオプションを使用できます。
 - 「デフォルトの資格情報と参照」を使用して、サーバーに複製されたすべてのサブツリーの複製バインド DN (およびパスワード) ならびにデフォルト参照を設定します。これは、すべてのサブツリーを同じサプライヤーから複製するときに使用される場合があります。
 - 各サブツリーのサプライヤー情報を追加して、複製されたサブツリーごとに独立して複製バインド DN およびパスワードを設定します。これは、サブツリーごとにサプライヤーが異なる場合 (サブツリーごとにマスター・サーバーが異なる場合) に使用される場合があります。
 5. 資格情報のタイプに応じて資格情報パスワードを入力し、確認します。(将来使用するときのために以前に記録しています。)
 - **単純なバインド** - DN およびパスワードを指定します。
 - **Kerberos** - サプライヤーの資格情報がプリンシパルおよびパスワードを識別しない場合 (サーバーの独自のサービス・プリンシパルを使用する場合) のバインド DN は `ibm-kn=ldap/<yourservername@yourrealm>` になります。資格情報のプリンシパル名が `<myprincipal@myrealm>` などの場合は、その名前を DN として使用します。いずれの場合も、パスワードは不要です。
 - **EXTERNAL バインドの SSL** - 証明書のサブジェクト DN およびパスワードなしを指定します。
- 397 ページの『資格情報の追加』を参照してください。
6. 「OK」をクリックします。
 7. 変更した内容を有効にするには、レプリカを再始動する必要があります。
詳細については、415 ページの『複製プロパティの変更』を参照してください。

レプリカは中断状態であり、複製は行われていません。複製トポロジーのセットアップが完了したら、「キューの管理」をクリックし、レプリカを選択し、「中断/再開」をクリックし、複製を開始する必要があります。詳細については、419 ページの『キューの管理』を参照してください。以上で、レプリカがマスターから更新を受信するようになります。

複製プロパティの変更

ここで提供する情報に従って、複製プロパティを変更することができます。

このタスクについて

ナビゲーション領域で「複製管理」カテゴリを展開し、「複製プロパティの管理」をクリックします。

このパネルで、以下を行うことができます。

- 複製状況照会から戻す保留変更の最大数を変更します。デフォルトは 200 です。
- 更新を複製中にサーバーが許容する複製エラーの最大数を設定します。これを設定するには、「エラー」をクリックし、フィールドに数値を入力します。あるいは、コンシューマーに更新を複製するときにサーバーが許容する複製エラーの最大数を無制限として設定するには、「無制限」をクリックします。

注: 0 より大きい値を指定すると、ロギングが使用可能になります。

- 複製コンテキスト・キャッシュのサイズをバイト単位で変更できます。デフォルトは 100000 バイトです。
- 競合する複製項目の最大サイズをバイト単位で設定できます。競合する複製項目の合計サイズ (バイト) がこのフィールドの値を超えた場合、競合した複製はサブライヤーによって再送されず、コンシューマーによる複製の競合の解決は行われません。デフォルトは 0、つまり無制限です。
- 複製トポロジーへのアクセスを制限するかどうかを指定する場合は、「アクセスを複製トポロジーに制限」フィールドから値を選択します。
- サプライヤー情報の追加、編集、または削除を実行します。

サプライヤー情報の追加:

以下の手順に示すステップにより、サプライヤー情報を追加することができます。

手順

1. 「追加」をクリックします。
2. ドロップダウン・メニューからサプライヤーを選択するか、サプライヤーとして追加する複製されたサブツリーの名前を入力します。
3. 資格情報の複製バインド DN を入力します。注: 状況に応じて、以下の 2 つのいずれかのオプションを使用できます。
 - 「デフォルトの資格情報と参照」を使用して、サーバーに複製されたすべてのサブツリーの複製バインド DN (およびパスワード) ならびにデフォルト参照を設定します。これは、すべてのサブツリーを同じサプライヤーから複製するときに使用される場合があります。
 - 各サブツリーのサプライヤー情報を追加して、複製されたサブツリーごとに独立して複製バインド DN およびパスワードを設定します。これは、サブツリ

ーごとにサブライヤーが異なる場合 (サブツリーごとにマスター・サーバーが異なる場合) に使用される場合があります。

4. 資格情報のタイプに応じて資格情報パスワードを入力し、確認します。(将来使用するときのために以前に記録しています。)
 - **単純なバインド** - DN およびパスワードを指定します。
 - **Kerberos** - パスワードなしで `ibm-kn=LDAP-service-name@realm` の形式の疑似 DN を指定します。
 - **EXTERNAL バインドの SSL** - 証明書のサブジェクト DN およびパスワードなしを指定します。

397 ページの『資格情報の追加』を参照してください。

5. 「**OK**」をクリックします。

タスクの結果

サブライヤーのサブツリーがサブライヤー情報リストに追加されます。

サブライヤー情報の編集:

以下に示す指示により、サブライヤー情報を編集することができます。

手順

1. 編集するサブライヤー・サブツリーを選択します。
2. 「**編集**」をクリックします。
3. 「**デフォルトの資格情報と参照**」を編集し、それを使用して `cn=configuration` に `cn=Master Server` 項目を作成する場合は、「**デフォルト・サブライヤーの LDAP URL**」フィールドに、クライアントでレプリカの更新を受信するサーバーの URL を入力します。これは、有効な LDAP URL (`ldap://`) である必要があります。それ以外の場合は、ステップ 4 にスキップしてください。
4. サーバーが競合する複製の解決をサポートするかどうかを指定するには、「**複製の競合解決**」コンボ・ボックスから値を選択します。
5. 使用する新規資格情報の複製バインド DN を入力します。

注: 複製されたサブツリーごとに、各サブツリーのサブライヤー情報を追加することにより、独自に複製バインド DN およびパスワードを設定します。これは、サブツリーごとにサブライヤーが異なる場合 (つまり、サブツリーごとにマスター・サーバーが異なる場合) に使用される場合があります。

6. 資格情報パスワードを入力して確認します。
7. 「**OK**」をクリックします。

サブライヤー情報の除去:

ここで提供する情報に従って、サブライヤー情報を除去することができます。

手順

1. 除去するサブライヤー・サブツリーを選択します。
2. 「**削除**」をクリックします。
3. 削除の確認を要求されたら、「**OK**」をクリックします。

タスクの結果

サブツリーが「サプライヤー情報」リストから除去されます。

複製スケジュールの作成

以下に示す情報を使用することにより、複製スケジュールの作成について詳細を把握できます。

このタスクについて

オプションで複製スケジュールを定義すると、特定の時間に複製するように、または特定の時間に複製しないようにスケジュールできます。スケジュールを使用しない場合、サーバーは、変更が行われた時点で複製をスケジュールします。これは、スケジュールで毎日午前 12:00 に直ちに複製を開始するよう指定することと同等です。

ナビゲーション領域で「複製管理」カテゴリを展開し、「スケジュールの管理」をクリックします。

「週次スケジュール」タブで、スケジュールを作成するサブツリーを選択し、「スケジュールの表示」をクリックします。スケジュールが存在する場合は、「週次スケジュール」ボックスに表示されます。新規のスケジュールを作成または追加するには、以下の手順を実行します。

1. 「追加」をクリックします。
2. スケジュールの名前を入力します。例えば、**schedule1** などです。
3. 日曜から土曜までの毎日の日次スケジュールは、「なし」として指定します。したがって、複製更新イベントはスケジュールされません。最後の複製イベント(ある場合)がまだ有効になっています。これは新規のレプリカであるため、前の複製イベントは存在しません。したがって、スケジュールのデフォルトは、即時複製に設定されます。
4. 日次複製スケジュールを作成するには、日を選択して、「日次スケジュールの追加」をクリックします。日次スケジュールを作成すると、その日次スケジュールが各曜日のデフォルトのスケジュールになります。以下を実行できます。
 - 日次スケジュールをそれぞれの日のデフォルトとして保持するか、または特定の日を選択して、その日のスケジュールをなしに戻します。スケジュールされた複製イベントがない日については、最後に発生した複製イベントがまだ有効になっていることに注意してください。
 - 日を選択して、「日次スケジュールの編集」を選択することで、日次スケジュールを変更します。日次スケジュールを変更すると、選択した日以外にも、そのスケジュールを使用するすべての日に影響することに注意してください。
 - 日を選択して、「日次スケジュールの追加」をクリックすることで、別の日次スケジュールを作成します。このスケジュールを作成すると、「日次スケジュール」ドロップダウン・メニューに追加されます。スケジュールを使用する日ごとにこのスケジュールを選択する必要があります。

日次スケジュール設定の詳細については、418 ページの『日次スケジュールの作成』を参照してください。

5. 完了したら、「OK」をクリックします。

日次スケジュールの作成:

以下に示すステップを使用することにより、日次スケジュールを作成することができます。

このタスクについて

ナビゲーション領域で「複製管理」カテゴリを展開し、「スケジュールの管理」をクリックします。

「日次スケジュール」タブで、スケジュールを作成するサブツリーを選択し、「スケジュールの表示」をクリックします。スケジュールが存在する場合は、「日次スケジュール」ボックスに表示されます。新規のスケジュールを作成または追加するには、以下の手順を実行します。

1. 「追加」をクリックします。
2. スケジュールの名前を入力します。例えば、**monday1** などです。
3. 時間帯設定 (UTC またはローカル) を選択します。
4. ドロップダウン・メニューから複製のタイプを選択します。

即時 最後の複製イベント以降、保留されていた項目更新を実行してから、次にスケジュールされた更新イベントに達するまで継続的に更新します。

1 回 開始時刻より前に保留されていた更新をすべて実行します。開始時刻以降に行われた更新は、次にスケジュールされた複製イベントまで待機します。

5. 複製イベントの開始時刻を選択します。
6. 「追加」をクリックします。複製イベントのタイプと時刻が表示されます。
7. イベントを追加または除去し、スケジュールを完成させます。イベントのリストは、日時順に再表示されます。
8. 完了したら、「OK」をクリックします。

例:

複製タイプ	開始時刻
即時	12:00 AM
1 回	10:00 AM
1 回	2:00 PM
即時	4:00 PM
1 回	8:00 PM

このスケジュールでは、最初の複製イベントは真夜中に発生し、その時刻より前に保留されていた変更がすべて更新されます。複製更新は、10:00 AM まで続行されます。10:00 AM から 2:00 PM までに行われた更新は、2:00 PM まで複製するのを待機します。2:00 PM から 4:00 PM までに行われた更新は、4:00 PM にスケジュールされた複製イベントを待機します。その後、次にスケジュールされた 8:00 PM の複製イベントまで、複製更新は続行されます。8:00 PM 以降に行われた更新は、次にスケジュールされた複製イベントまで待機します。

注: 複製イベントの間隔を密にスケジュールすると、次のイベントがスケジュールされたときに前のイベントの更新が進行中の場合、複製イベントが失われることがあります。

キューの管理

キューの管理により、このサーバーが使用する複製合意 (キュー) ごとに複製の状況をモニターできます。ここで説明する情報を使用できます。

ナビゲーション領域で「複製管理」カテゴリを展開し、「キューの管理」をクリックします。

「キューの管理」テーブルの列には、次の情報が格納されます。

選択 アクションを実行するレプリカを選択します。

レプリカ

複製キューのレプリカの名前を指定します。

サブツリー

レプリカが位置するサブツリーを指定します。

最終結果

最後の戻りコード/ステータス (成功/失敗) を示します。

状態 コンシューマーとの複製の状態を示します。

アクティブ

コンシューマーにアクティブに送られている更新。

作動可能

即時複製モード。発生時に更新を送信可能。

Waiting

次にスケジュールされた複製時刻を待機中。

Binding

コンシューマーへのバインド処理中。

接続中。

コンシューマーへの接続処理中。

On Hold

この複製合意が中断または「保留」されている。

Error Log Full

サーバーが複数の接続を使用するように構成されている場合、該当する合意の複製は中断されます。受信側スレッドは、送信された更新のステータスをポーリングし続けますが、更新は複製されません。

Retrying

サーバーが単一接続を使用するように構成されている場合、60 秒待った後に同じ複製更新の送信が試行され、複製が成功するまで、または管理者が更新をスキップするまでこれが繰り返されます。

キュー・サイズ

複製状況の照会時に戻す保留中の変更の数を指定します。

- キューを管理する対象となるレプリカを選択します。
- レプリカの状況に応じて、「**中断/再開**」をクリックして複製を中止または開始できます。
- 「**複製の強制**」をクリックすると、次の複製がいつスケジュールされているかに無関係に、すべての保留変更が複製されます。
- レプリカのキューの詳細については、「**キューの詳細**」をクリックします。この選択項目からキューを管理することもできます。
- 「**再表示**」をクリックすると、キューが更新され、現在のステータスを取得し、サーバー・メッセージがクリアされます。

キューの詳細:

ここで提供する情報を読むことにより、キューについて詳しく知ることができます。

「**キューの詳細**」をクリックすると、以下の 3 つのタブが表示されます。

- 状況
- 最終試行の詳細
- 変更の保留

「**ステータス**」タブには、レプリカ名、そのサブツリー、その複製状況、および複製時間のレコードが表示されます。このパネルで「**中断**」をクリックすると複製を中断でき、「**再開**」をクリックすると複製を再開できます。変更不可能なステータス・フィールドには、このステータスの変化が反映されます。「**再表示**」をクリックするとキュー情報が更新されます。

「**最終試行の詳細**」タブには、選択したレプリカに対する最後の更新試行に関する以下の情報が表示されます。

- **レプリカ** - 複製キューのレプリカの名前。
- **サブツリー** - レプリカが位置するサブツリー。
- **項目 DN** - 更新された項目の DN。
- **最終複製時刻** - 項目が最後に複製された時刻。
- **更新タイプ** - 更新のタイプ (追加、削除、変更など)。
- **最終結果** - エラーに割り当てられたエラー・コード。
- **LDIF の失敗** - LDIF 形式の更新。
- **追加のエラー・メッセージ** - エラーに関する追加情報。

項目をロードできない場合は、「**ブロッキング項目のスキップ**」を押し、次の保留中の項目から複製を継続します。「**再表示**」をクリックするとキュー情報が更新されます。

注: 複製を介して完了する変更のデフォルトのタイムアウトは、60 秒です。複製の更新に大量の変更 (例えば、大きなグループ項目の追加) が伴う場合は、更新操作が完了するまでに 60 秒を超える時間が必要になる場合があります。複製を介した単一の更新 (add、delete、modify、または modifydn) 操作に 60 秒を超える時間がかかる場合は、サプライヤーのサーバーで、その更新操作がタイムアウトになり、複製を介した同じ更新の送信が再試行されます。複製の更新操作のタイムアウト期間を

長くするには、IBMSLDAP_REPL_UPDATE_EXTRA_SECS 環境変数を使用します。この環境変数の使用方法については、IBM Security Directory Server の資料の『トラブルシューティングおよびサポート』セクションを参照してください。

「変更の保留」タブには、レプリカに対するすべての保留変更が表示されます。表示される保留変更の数は、「複製プロパティの管理」パネルに入力した値によって決まります。デフォルトは 200 です。

複製がブロックされる場合は、「すべてスキップ」をクリックすると、保留変更をすべて削除できます。「再表示」をクリックすると、保留変更のリストが更新され、処理済みの新規の更新が反映されます。

注: ブロックしている変更をスキップした場合は、必ず最終的にコンシューマー・サーバーを更新する必要があります。詳しくは、「IBM Security Directory Server Version 6.3 Command Reference」の **ldapdiff** コマンド情報を参照してください。

複製を管理するためのコマンド行タスク

これらのコマンド行タスクを実行することで、複製の管理ができます。

サブツリーのサプライヤー DN およびパスワードの指定

特定のサブツリーのサプライヤー DN およびパスワードを指定できます。ここで説明する手順に従って、同じ操作を実行することができます。

このタスクについて

手順

1. コンシューマー・サーバーを始動します。
2. `replica1` を構成してレプリカ・サーバーにする必要があります。以下の手順を実行して、`replica1` の `ibmslapd.conf` ファイルに項目を追加します。 `idsldapmodify -D <admin_dn> -w <admin_pw> -I <instance_name> -i <LDIF_file>` ここで、`<LDIF_file>` には、次の設定が含まれます。
dn: cn=Master Server,
cn=configuration cn: Master Server ibm-slapdMasterDN: cn=master
ibm-slapdMasterPW: <masterserverpassword> ibm-slapdMasterReferral:
ldap://<masterhostname:masterport> objectclass: ibm-slapdReplication
dn: cn=Supplier s1, cn=configuration cn: Supplier s1 ibm-slapdMasterDN:
cn=s1 ibm-slapdMasterPW: s1 ibm-slapdReplicaSubtree: ou=Test, o=sample
objectclass: ibm-slapdSupplier
3. `ibmslapd.conf` ファイルを保管します。
4. `replica1` を再始動します。

複製構成情報の表示

以下に示す指示およびコマンドにより、複製構成情報を表示できます。

検索を使用して、複製アクティビティに関連する大量の情報を利用できます。特定の複製されたサブツリーに関連する複製トポロジー情報を参照するには、ベースをサブツリーの DN に設定してフィルターを (`objectclass=ibm-repl*`) に設定したサブツリー検索を実行することで、トポロジー情報のベースであるサブエントリを検索できます。この複製コンテキストが Web 管理インターフェース経由で作成された場合、項目の名前は `ibm-replicaGroup=default` となります。

```
idsldapsearch -D <adminDN> -w <adminPW> -p <port> -b <suffixentryDN>
objectclass=ibm-repl*
```

返されるオブジェクトには、レプリカ・グループ自体に加え、以下の結果が含まれます。

- このコンテキスト内でデータを複製する各サーバーの **objectclass=ibm-replicaSubentry** のオブジェクト。レプリカ・サブエントリーには、サーバー ID 属性およびサーバーの役割 (**ibm-replicationServerIsMaster**) が示されます。
- レプリカ・サブエントリーごとに、レプリカ・サブエントリーによって記述されたサーバーから複製更新を受信する各コンシューマー・サーバーの複製合意オブジェクトがあります。各複製合意には以下の情報があります。
 - **ibm-replicaConsumerId**: コンシューマー・サーバーのサーバー ID。
 - **ibm-replicaURL**: コンシューマー・サーバーの LDAP URL。
 - **ibm-replicaCredentialsDN**: コンシューマーへのバインドに使用する資格情報を含む項目の DN。

合意には、以下の情報を含む場合もあります。

- **ibm-replicaScheduleDN**: 複製更新がこのコンシューマーに送信されるタイミングを決定するスケジュール項目の DN。スケジュールが指定されていない場合は、複製はデフォルトで「即時」モードになります。
- **ibm-replicationOnHold**: このコンシューマーへの複製が中断されているかどうかを示すブール値。
- **ibm-replicationExcludedCapability**: この属性の値は、コンシューマーがサポートしていない機能の OID をリストします。これにより、これらの機能に関連した操作は、このコンシューマーに送信された更新から除外されます。
- **ibm-replicationMethod**: 単一スレッドまたはマルチスレッド。
- **ibm-replicationConsumerConnections**: 単一スレッド複製方式を使用する複製合意の場合、コンシューマー接続の数は必ず 1 つで、属性値は無視されます。マルチスレッド複製を使用する合意の場合、接続の数は 1 から 32 の間で構成できます。合意でこの値を指定しない場合、コンシューマー接続の数は 1 に設定されます。

複製状況のモニター

ここで提供する情報に従って、複製状況をモニターすることができます。

さらに、検索時に明示的に要求した場合に、複製状況情報を提供する多くの操作可能な属性があります。これらの属性の中の 1 つは、複製されたサブツリーのベースの項目 (**ibm-replicationContext** オブジェクト・クラスが追加された項目) に関連付けられます。その項目のベース検索を行う場合は、**ibm-replicationIsQuiesced** 属性を戻すように要求します。この属性は、サブツリーが静止したかどうかを示すブール値です。サブツリーが静止すると、クライアントの更新は許可されません (複製サブライヤーからの更新のみが受け入れられます)。サブツリーを静止するために使用できる拡張操作について詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の **ldapexop** コマンド情報を参照してください。

状況関連の操作可能な残りの属性は、すべて複製合意オブジェクトに関連するものです。これらの属性は、検索時に明示的に要求された場合にのみ戻されます。使用可能な属性は以下のとおりです。

- **ibm-replicationLastActivationTime:** このサプライヤーとコンシューマーの間の最後の複製セッションが開始された時刻。
- **ibm-replicationLastFinishTime:** このサプライヤーとコンシューマーの間の最後の複製セッションが完了した時刻。
- **ibm-replicationLastChangeId:** このコンシューマーに送信された最後の更新の変更 ID。
- **ibm-replicationState:** このコンシューマーとの複製の現在の状態。可能な値は以下のとおりです。

アクティブ

コンシューマーにアクティブに送られている更新。

作動可能

即時複製モード。発生時に更新を送信可能。

Retrying

サーバーが単一接続を使用するように構成されている場合、60 秒待った後に同じ複製更新の送信が試行され、複製が成功するまで、または管理者が更新をスキップするまでこれが繰り返されます。

Waiting

次にスケジュールされた複製時刻を待機中。

Binding

コンシューマーへのバインド処理中。

接続中。

コンシューマーへの接続処理中。

On Hold

この複製合意が中断または「保留」されている。

Error Log Full

サーバーが複数の接続を使用するように構成されている場合、該当する合意の複製は中断されます。受信側スレッドは、送信された更新のステータスをポーリングし続けますが、更新は複製されません。

エラー xxxx

エラーが発生しました。ここで、xxxx はエラーを説明するメッセージの ID です。

- **ibm-replicationLastResult** このコンシューマーに対する最後に試行された更新の結果。形式は以下のとおりです。

`<time stamp> <change ID> <result code> <operation> <entry DN>`

注: この情報は、単一スレッド複製を使用している場合のみ取得できます。

- **ibm-replicationLastResultAdditional:** 最後の更新についてコンシューマーから戻された追加のエラー情報。

注: この情報は、単一スレッド複製を使用している場合のみ取得できます。

- **ibm-replicationPendingChangeCount:** このコンシューマーに複製するためにキューに入れられた更新の数。
- **ibm-replicationPendingChanges:** この属性のそれぞれの値は、以下の形式で保留変更の 1 つに関する情報を提供します。

<change ID> <operation> <entry DN>

この属性を要求すると、多くの値が戻される場合があります。この属性を要求する前に変更カウントを検査してください。

- **ibm-replicationChangeLDIF**: LDIF で最後に失敗した更新の詳細。

注: この情報は、単一スレッド複製を使用している場合のみ取得できます。

- **ibm-replicationFailedChanges**: **ibm-replicationPendingChanges** と同じく、指定した複製合意で記録された障害の ID、DN、更新タイプ、結果コード、タイム・スタンプ、試行の数をリストします。表示される障害の数は、**ibm-slapdMaxPendingChangesDisplayed** 以下です。
- **ibm-replicationFailedChangeCount**: **ibm-replicationPendingChangeCount** と同じく、指定した複製合意で記録された障害の数が返されます。
- **ibm-replicationPerformance**: マルチスレッド複製についての情報。

以下のユーザーのみが、**ibm-replicationPendingChanges**、**ibm-replicationPendingChangesCount**、**ibm-replicationFailedChanges**、および **ibm-replicationChangeLDIF** を表示できます。

- 管理者
- 管理グループのメンバー
- グローバル管理グループのメンバー
- 複製トポロジー項目に対する更新アクセス権を、ACL を介して明示的に与えられたユーザー

ゲートウェイ・サーバーの作成

ここに示す情報により、ゲートウェイ・サーバーの作成、およびそこでの処理についての詳細を知ることができます。

新規のゲートウェイ・サーバーの作成:

以下に示す例を使用することで、新規のゲートウェイ・サーバーを作成することができます。

このタスクについて

注: ゲートウェイ・サーバーを作成したら、新規の複製合意を作成して、新しいトポロジーを反映させる必要があります。詳細については、325 ページの『複製合意』を参照してください。

新規のレプリカ・コンテキスト、レプリカ・グループ、およびレプリカ・サブエントリーを DIT に作成します。レプリカのサブエントリーには、**ibm-replicaSubentry** オブジェクト・クラスと **ibm-replicaGateway** 補助オブジェクト・クラスを格納する必要があります。**ibm-replicaSubentry** オブジェクト・クラスと **ibm-replicaGateway** 補助オブジェクト・クラスは、次の例では太字になっています。

```
dn: o=sample
objectclass: top
objectclass: organization
objectclass: ibm-replicationContext

dn: ibm-replicagroup=default,o=sandbox
objectclass: top
objectclass: ibm-replicaGroup
ibm-replicagroup: default
```

```
dn: ibm-replicaServerId=<serverid>,ibm-replicagroup=default,o=sandbox
objectclass: top
objectclass: ibm-replicaSubentry
objectclass: ibm-replicaGatewayibm-replicaServerId:<serverid>
ibm-replicationServerIsMaster: TRUE
cn: <servername>
```

ここで、<servername> はサーバーの名前、<serverid> はサーバーの最初の始動時に割り当てられる 37 文字のストリングです。サーバー ID は、コマンド・プロンプトに以下のコマンドを入力すると表示されます。

```
idsldapsearch -p <port> -b "" -s base objectclass=*
```

既存のピア・サーバーからゲートウェイ・サーバーへの変換:

ピア・サーバーをゲートウェイ・サーバーに変換する前に、サブツリーが静止状態であり、保留中の変更がないことを確認します。以下に示す例では、ゲートウェイ・サーバーとして構成されていないレプリカのサブエントリを示します。

このタスクについて

```
dn: ibm-replicaServerId=<serverid>,ibm-replicagroup=default,o=sandbox
objectclass: top
objectclass: ibm-replicaSubentry
ibm-replicaServerId: <serverid>
ibm-replicationServerIsMaster: TRUE
cn: <servername>
```

このピア・サーバーをゲートウェイ・サーバーに変換するには、DIT 内で、**ibm-replicaGateway** 補助オブジェクト・クラスを、それを必要とするレプリカ・サブエントリに追加します。**ibm-replicaGateway** 補助オブジェクト・クラスは、次の例では太字になっています。

```
dn: ibm-replicaServerId=<serverid>,ibm-replicagroup=default,o=sandbox
changetype: modify
add: objectclass
objectclass: ibm-replicaGateway
```

ここで、<servername> はサーバーの名前、<serverid> はサーバーの最初の始動時に割り当てられる 37 文字のストリングです。サーバー ID は、コマンド・プロンプトに以下のコマンドを入力すると表示されます。

```
idsldapsearch -p <port> -b "" -s base objectclass=*
```

補助オブジェクト・クラスの除去については、540 ページの『補助オブジェクト・クラスの削除』を参照してください。

分散ディレクトリー

分散ディレクトリーとは、複数のディレクトリー・サーバー間でデータが分割されるディレクトリー環境です。

分散ディレクトリーは、リレーショナル・データベース管理 (RDBM) サーバーを組み込んだマシンと、トポロジーを管理するプロキシー・サーバーとの集合として構成されている必要があります。

プロキシー・サーバー

プロキシー・サーバーは、特殊なタイプの IBM Security Directory Server で、要求のルーティング、ロード・バランシング、フェイルオーバー、分散認証、分散/メンバーシップ・グループのサポート、コンテナの分割化などを実行します。これら

の機能のほとんどは、新規のバックエンド、プロキシ・バックエンドで提供されます。IBM Security Directory Proxy Server は RDBM バックエンドを所有しないので、複製には参加できません。

ディレクトリー・プロキシ・サーバーは分散ディレクトリーのフロントエンドに位置し、ユーザー要求を効率的にルーティングすることで、特定の状況のパフォーマンスを改善し、さらに統合されたディレクトリー・ビューをクライアントに提供します。プロキシ・サーバーは、フェイルオーバーおよびロード・バランシングを提供するサーバー・クラスターのフロントエンドとして使用することもできます。

プロキシ・サーバーは、読み取り要求と書き込み要求を、構成に応じて別個に送付します。単一区画に対する書き込み要求は、単一の 1 次書き込みサーバーに送信されます。競合を避けるためにピア・サーバーは使用されません。読み取り要求は、負荷のバランスを取るためにラウンドロビン方式で送付されます。ただし高い整合性が有効な場合、読み取り要求は 1 次書き込みサーバーに送付されます。

またプロキシ・サーバーは、別の区画に定義されたグループに基づいて ACL を定義するためのサポートも提供します。さらには、フラット・ネームスペースの分割化をサポートします。プロキシ・サーバーは、LDAP 準拠のロード・バランサーとして使用することもできます。

プロキシ・サーバーを構成する場合、プロキシ・サーバーが代理する、各バックエンド・サーバーに接続するための接続情報が必要になります。この接続情報には、ホスト・アドレス、ポート番号、バインド DN、資格情報、および接続プール・サイズが含まれます。各バックエンド・サーバーを構成する場合、プロキシ・サーバーがバックエンド・サーバーに接続する際使用する DN および資格情報についての情報が必要になります。DN は、グローバル管理グループのメンバー、dirData 権限を持つローカル管理グループのメンバー、または 1 次管理者でなければなりません。

プロキシ・サーバーをデプロイする前に、ご使用の環境に必要なすべての操作がサポート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、625 ページの『サポートされ、使用可能になっている機能の OID』、636 ページの『拡張操作の OID』、および 638 ページの『コントロールの OID』

注: を参照してください。ユーザーがプロキシ・サーバーに対する操作の管理制御を指定すると、プロキシ・サーバーはその管理制御をバックエンド・サーバーに伝搬します。

プロキシ・サーバーは、バックエンド・サーバーをターゲットにした新規要求を送付する際に、空いているバックエンド接続のみを使用します。使用可能な空いているバックエンド接続がない場合、プロキシ・サーバーは一時的にクライアントからの要求の読み取りを中断します。プロキシ・サーバーは、バックエンド接続が空き状態になったときのみクライアントからの読み取りを再開します。また、クライアントからバックエンドへの保留要求がある場合、クライアントからの新規要求は前の要求で使用されたものと同じバックエンド接続を使用して送付されます。

注: **ibm-slapdProxyBackendServer** オブジェクト・クラスの **ibm-slapdProxyMaxPendingOpsPerClient** 属性は、バックエンド接続内で保持されるクライアント接続からの未処理要求数のしきい値限度を構成するために使用されます。このしきい値限度に達すると、バックエンド接続の保留要求数が、指定されたしきい値限度より少ない値になるまで、クライアント接続からの要求は読み取られません。この属性を指定していない場合、保留クライアント操作の最大数はデフォルトで 5 になります。

最後に、プロキシ・サーバーは、独自のスキーマを使用して構成します。プロキシ・サーバーが代理するバックエンド・サーバーのスキーマと同じスキーマを使用して、プロキシ・サーバーを構成する必要があります。またプロキシ・サーバーの構成には、区画情報も必要です。

注: サーバーは、ディレクトリー・サーバーとプロキシ・サーバーのどちらとして構成されていても、同じデフォルト構成ファイルを使用します。ただし、サーバーがプロキシ・サーバーとして構成されている場合、プロキシ・サーバーでサポートされていない機能の構成設定は無視されます。プロキシ・サーバーで無視される構成ファイル内の項目のリストは以下のとおりです。

- cn=Event Notification, cn=Configuration
- cn=Persistent Search, cn=Configuration
- cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
- cn=Replication, cn=configuration
- cn=Bulkload, cn=Log Management, cn=Configuration
- cn=DB2CLI, cn=Log Management, cn=Configuration

項目「cn=Front End, cn=configuration」では、この項目の下に設定される環境変数はプロキシ・サーバーでサポートされます。プロキシ・サーバーでサポートされる環境変数には、以下の変数が含まれます。

表 38. プロキシ・サーバーでサポートされる環境変数

変数	説明
<i>PROXY_CACHE_GAG_PW</i>	パスワード・キャッシングが使用可能か使用不可かを指定します。プロキシ・サーバーには、グローバル管理者のパスワードをローカル側でキャッシュに入れる機能があります。パスワード・ポリシーが使用可能な場合、グローバル管理グループ・メンバーのパスワードのキャッシングは使用不可です。パスワード・ポリシーが使用不可の場合、グローバル管理グループ・メンバーのキャッシングは使用可能です。 <i>PROXY_CACHE_GAG_PW</i> 環境変数は、このデフォルトの動作をオーバーライドできます。 <i>PROXY_CACHE_GAG_PW</i> を YES に設定すると、パスワード・キャッシングが使用可能になります。 <i>PROXY_CACHE_GAG_PW</i> をその他の値に設定すると、パスワード・キャッシングは使用不可になります。環境変数を設定解除すると、デフォルトの動作はパスワード・ポリシー設定によって管理されます。
<i>PROXY_GLOBAL_GROUP_PERIOD</i>	プロキシ間隔スレッドがウェイクアップするまでの間隔を指定します。この変数のデフォルト値は 30 秒です。

表 38. プロキシ・サーバーでサポートされる環境変数 (続き)

変数	説明
<i>PROXY_USE_SINGLE_SENDER</i>	単一の送信側スレッドが操作に使用されるかどうかを指定します。デフォルトでは false です。
<i>PROXY_RECONNECT_TIME</i>	ダウンしたバックエンド・サーバーへの再接続をプロキシが試行するまでの間隔を指定します。デフォルトでは 5 秒です。
<i>LDAP_LIB_WRITE_TIMEOUT</i>	ソケットの書き込み準備が完了するのを待機する時間 (秒) を指定します。
<i>FLOW_CONTROL_SLEEP_TIME</i>	フロー制御において、使用可能な空いているバックエンド接続がない場合、プロキシ・サーバーは一時的にソケットからの読み取りを中断します。次に、使用可能になった空いているバックエンド接続がないかどうかを定期的に検査します。この検査が実行される頻度は、環境変数 <i>FLOW_CONTROL_SLEEP_TIME</i> によって決まります。この環境変数は整数値に設定する必要があり、プロキシ・サーバーによって検査が行われる頻度がミリ秒単位で指定されます。環境変数を設定しない場合、デフォルトで 5 に設定されます。

プロキシ・サーバーでは Security Directory Server の一部の機能がサポートされる一方で、サポートされない機能もあります。プロキシ・サーバーでサポートされる機能のリストは以下のとおりです。

- ログ・アクセスの拡張操作
- サポートされる属性の動的構成
- サーバーの始動および停止
- TLS
- バインドされた DN のアンバインド
- 動的トレース
- 属性タイプの拡張操作
- ユーザー・タイプの拡張操作
- ソース IP 制御の監査
- サーバー管理のコントロール
- 項目のチェックサム
- 項目 UUID
- ACL のフィルター操作
- 管理グループの代行
- サービス妨害の防止
- 管理サーバーの監査
- 動的グループ
- 操作カウントのモニター
- ログイン・カウントのモニター
- アクティブ・ワーカーの接続モニター

- トレースのモニター
- SSL FIPS モード
- 項目の名前変更によって項目が区画をまたいで移動しない限り DN を変更する。
- 複数インスタンス
- AES パスワード暗号化
- 管理パスワード・ポリシー
- 項目検出拡張操作
- 役割の再開拡張操作
- LDAP ファイル取得
- 属性値の制限数
- パフォーマンスの監査 - パフォーマンスの監査はプロキシ・サーバーでサポートされます。プロキシ・サーバーでは、監査レコードごとに以下のパフォーマンス情報フィールドが有効です。プロキシ・サーバーの RDBM ロック待ち時間は常に 0 です。
 - 操作の応答時間
 - 作業キューで費やされる時間
 - クライアントの入出力時間
- ダイジェスト MD-5 バインド
- 管理役割
- preoperation プラグイン
- グローバル管理グループ
- ページ検索およびソート検索
- ibm-allmembers 検索
- トランザクション

注：トランザクションがサポートされるのは、トランザクション要求の一部である項目がすべて単一ディレクトリー・サーバーにある場合のみです。

プロキシ・サーバーでサポートされない機能のリストは以下のとおりです。

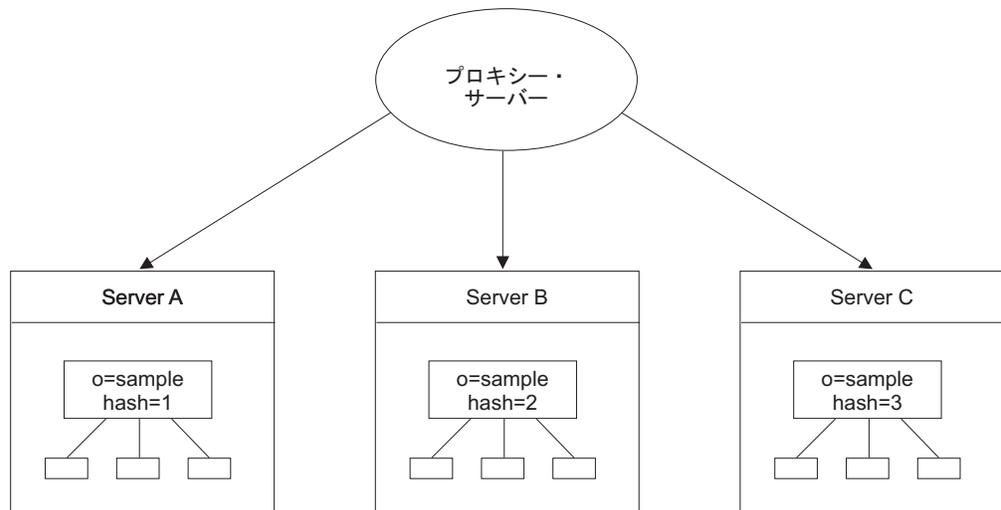
- イベント通知
- 複製管理拡張操作
- グループ評価拡張操作
- アカウント・ステータス拡張操作
- サブツリーの削除
- プロキシ許可のコントロール
- グループ許可のコントロール
- グループの参照整合性の省略
- 固有属性
- 有効なパスワード・ポリシー
- オンライン・バックアップ拡張操作
- パスワード事前結合の拡張操作
- パスワード事後結合の拡張操作

- 事後操作プラグイン
- ヌル・ベースの検索

サブツリー内のデータの分割

RDN ハッシュに基づくサブツリー内のデータは、プロキシ・サーバーを使用して分割することができます。

この設定では、3 つのサーバーが「コンテナ (ディレクトリー・ツリーの項目の下)」内に分割されたデータを保持します。プロキシ・サーバーは要求を適切なサーバーにルーティング処理するので、参照は使用しません。クライアント・アプリケーションが認識する必要があるのはプロキシ・サーバーのみです。クライアント・アプリケーションは、サーバー A、B、または C で認証される必要はありません。



データは RDN ハッシュにより等分割され、各ディレクトリーの分割のベースの下に格納されます。この例では、サブツリー内のデータが RDN のハッシュ値に基づき分割されます。ハッシュ処理できるのは、コンテナ下のツリー内の 1 レベル内の RDN のみです。区画のネストは許可されています。複合 RDN の場合、正規化された複合 RDN 全体がハッシュ処理されます。このハッシュ・アルゴリズムでは、各項目の DN に索引値が割り当てられます。この値は、項目を使用可能なサーバーに均等に配布する際に使用されます。

注:

1. 複数のサーバーの親項目は、この場合でも、同期化させる必要があります。親項目の保守は管理者の責任です。
2. ACL は、各サーバーの区画ベース・レベルに定義する必要があります。

注: 区画の数および区画レベルは、プロキシ・サーバーを構成する際、およびデータを分割する際に決定されます。トポロジーを拡張または縮小するには、再度区画化する以外方法はありません。

プロキシ・サーバーは、ハッシュ値を使用して項目の探索および項目の取得を行います。

例: **o=sample** の下位のデータが 3 つのサーバーに分割されます。つまり、**o=sample** の直後の RDN 値をハッシュ処理して 3 つのサーバー (すなわち「器」) 間で分割されるようにプロキシー・サーバーを構成します。また、**o=sample** から、1 より大きい RDN 値を、**o=sample** の直後の値として同じサーバーにマップします。例えば、**cn=test,o=sample** および **cn=user1,cn=test,o=sample** は必ず同じサーバーにマップします。ServerA はハッシュ値 1 の項目をすべて保持し、server B はハッシュ値 2 の項目をすべて保持し、ServerC はハッシュ値 3 の項目をすべて保持します。プロキシー・サーバーは、DN **cn=Test,o=sample** である項目の追加要求を受け取ります。プロキシー・サーバーは、内部のハッシュ関数への入力値として、構成情報 (具体的に言うと、ベース **o=sample** の 3 つの区画があるという情報) と **cn=Test** RDN を使用します。この関数が 1 を返した場合、その項目は ServerA にあり、追加要求はそこに転送されます。

項目のハッシュ処理は、その項目の RDN に基づいて行われます。分割ポイントのすぐ左の DN の一部のみがハッシュ・アルゴリズムに使用されます。また、値だけでなく、正規化された文字列全体がハッシュに使用されます。例えば、分割ポイントが **o=sample** で、3 つの区画に分割する場合、以下のような処理が行われます。

- **cn=example,o=sample** は単一のサーバー、例えば serverA にハッシュします。これは、**cn=example** が 3 つの区画の 1 つにハッシュすることで決定されます。
- **dc=example, o=sample** は別のサーバー、例えば ServerB にハッシュします。これは、**dc=example** がハッシュされることで決定されます。
- **cn=foo,cn=example,o=sample** は、ServerA にハッシュします。これは、ハッシュ・アルゴリズムに **cn=example** のみを使用されるからです。
cn=example,o=sample 以下のすべての項目は、**cn=example,o=sample** と同じサーバーに解決されます。

注: プロキシー・サーバーのバージョン 6.1 以降とバックエンド・サーバーのバージョン 6.0 を共に使用する場合、**cn=pwdpolicy** サブツリーを分割ポイントとして構成する必要があります。ただし、6.1 以降のバージョンのバックエンド・サーバーを使用するバージョン 6.1 以降のプロキシー・サーバーには、**cn=pwdpolicy** サブツリーがありません。

DN 区画化プラグイン

Security Directory Server には、カスタマー作成の区画化関数をサーバー実行時にロードするオプションがあります。データの区画化に使用する既存のハッシュ・アルゴリズムは、Security Directory Server によって静的にリンクされます。ただし、DN 区画化関数がプラグインとしてインプリメントされている場合、ハッシュ・アルゴリズムを容易に置き換えられるため、Security Directory Server はより柔軟で最適になります。

ただし、既存のハッシュ・アルゴリズムはデフォルトの区画化プラグインとして残ります。既存のハッシュ・アルゴリズムは、使用可能なカスタマイズされたコードがない場合に、サーバーの始動時にロードされます。この機能では、

ibm-slapdDNPartitionPlugin という属性を **objectclass ibm-slapdProxyBackend** に取り込みます。これは必須の単一値属性であり、1 つのプロキシー・サーバー・バックエンドに対して許可される DN 区画化プラグインは 1 つのみです。属性値は、カスタマイズされた DN 区画化モジュールのロードに使用するパスと、ユーザー提供の DN 区画化関数の登録に使用する初期化関数から構成されます。

プロキシ・サーバーの始動時に DN 区画化プラグインをロードするときに、初期化関数が呼び出されます。動的にロード可能なプラグイン・モジュールをロードすることにより、ローダーは、モジュールに定義された関数を関数アドレスに割り当てます。この初期化関数を実行すると、初期化関数に登録された区画化関数のアドレスがプロキシ・サーバー・バックエンドに保管されます。登録された DN 区画化関数は、要求をターゲット・サーバーに送付するために後でプロキシ・ルーターに呼び出されます。

注:

- ある区画化アルゴリズムを使用するプロキシ・サーバーによって取り込まれた DIT は、別の区画化アルゴリズムを使用するプロキシ・サーバーからはアクセス不能になります。DIT の取り込み後は、区画化プラグインを変更してはいけません。区画化プラグインを変更する必要がある場合は、データを再ロードしてください。IBM Security Directory Server バージョン 6.0 以前用にロードされたデータは、デフォルトのプラグインがバージョン 6.1 以降で使用されていない限り、バージョン 6.1 以降のカスタム DN 区画化プラグインとは連携しません。
- カスタマイズされたプラグインを使用するには **ddsetup** コマンドを実行する前にそのプラグインを設定する必要がある、ということに注意してください。

コマンド・ラインの使用

以下のコマンドを発行することで、`ibm-slapdDNPartitionPlugin` 属性を変更し、カスタマイズされたプラグインを追加できます。

このタスクについて

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where *<filename>* contains:

```
dn: cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
changetype: modify
replace: ibm-slapdDNPartitionPlugin
ibm-slapdDNPartitionPlugin: <customized DN partitioning plug-in library>
<plug-in initialization function>
```

分散ディレクトリーのセットアップ・ツール

分散ディレクトリー・セットアップ (ddsetup) ツールは、LDIF ファイルを、個々のディレクトリー・サーバーにロードできる個別の LDIF ファイルに分割します。

LDIF ファイルを単に個々の断片に分割するだけなら、非分散環境でも ddsetup ツールを使用できます。また、DN で分割ポイントを指定することで、1 つ以上のサブツリーの DIT を分割することもできます。このツールでは、プロキシ・サーバーの `ibmslapd.conf` ファイルを使用して項目を区画化します。データは、構成ファイルの `ibm-slapdDNPartitionPlugin` 属性に指定された区画化アルゴリズムを使用して分割されます。

注: ddsetup ツールは最適なパフォーマンスを得るよう設計されているため、`objectclass` のスキーマ検査を実施しません。

データの追加および分割化:

ここで示す方法および説明を使用することにより、データを追加および区画化することができます。

このタスクについて

項目を追加するには、Web 管理ツール (詳細は、526 ページの『項目の追加』を参照) または **idsldapadd** コマンドおよび **idsldapmodify** コマンド (「*IBM Security Directory Server Version 6.3 Command Reference*」のコマンド情報を参照) を使用します。

多数の項目を持つ既存のデータベースがある場合、それらの項目を 1 つの LDIF ファイルにエクスポートする必要があります。これを行う方法について詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の **idsdb2ldif** コマンドの情報を参照してください。

1. LDIF ファイルを作成するには、次のコマンドを発行します。idsdb2ldif-o mydata.ldif -s o=sample-I <instance_name>
2. 次のコマンドを発行します。ddsetup -I proxy -B "o=sample" -I mydata.ldif
ここで、

proxy: プロキシ・サーバー・インスタンス

重要: 新規のディレクトリー・サーバー・インスタンスを作成する場合、以下の情報に注意してください。分散ディレクトリーを使用して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同期化させる必要があります。AES 形式のデータを含む既存のディレクトリーを分散ディレクトリーに分割する場合、区画サーバーと元の非区画サーバーを同期化させる必要があります。これを行わないと、ddsetup ツールが生成する LDIF エクスポート・ファイルをインポートできません。

既存のディレクトリー・サーバー・インスタンスと暗号同期化する必要があるディレクトリー・サーバー・インスタンスを作成する場合は、以下のいずれかのアクションを行う**前に** サーバー・インスタンスを同期化する必要があります。

- 2 番目のサーバー・インスタンスの始動
- 2 番目のサーバー・インスタンスからの、**idsbulkload** コマンドの実行
- 2 番目のサーバー・インスタンスからの、**idsldif2db** コマンドの実行

ディレクトリー・サーバー・インスタンスの同期化については、703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』を参照してください。

3. idsldif2db または idsbulkload を使用して、データを適切なバックエンドにロードします。
 - ServerA (区画索引 1) - ServerA.ldif
 - ServerB (区画索引 2) - ServerB.ldif
 - ServerC (区画索引 3) - ServerC.ldif
 - ServerD (区画索引 4) - ServerD.ldif
 - ServerE (区画索引 5) - ServerE.ldif

注: 対応する区画索引値を持つサーバーに LDIF 出力をロードする必要があります。これを行わないと、プロキシ・サーバーは項目を取得できません。

ddsetup ユーティリティについての詳細は、「*IBM Security Directory Server Command Reference*」を参照してください。

情報の同期化

分散ディレクトリーのサーバー間では、主に 2 つの種類の構成情報を同期化させる必要があります。

サブツリー・ポリシー

ACL は現在のところ、唯一のサブツリー・ポリシー・タイプです。ACL は、ローカル・サーバーでのみ遵守されます。データをフラット・コンテナ間で分割する場合、各サーバーにはその親項目を格納します。ACL をその親項目に定義する場合、それぞれの親項目に定義する必要があります。親レベルまたはその下位レベルに定義する ACL が、そのツリーの親項目よりも上位の項目に依存してはいけません。サーバーは別のサーバーで定義されている ACL は実行しません。

ddsetup を使用して設定を行う際、親項目全体の正確なコピーを各サーバーに追加します。または、ユーザーの責任で親項目全体のコピーをサーバーに追加します。親項目に ACL を定義する場合、初期構成を行った後、各サーバーの親の下の子項目にも同じ ACL を定義します。初期構成をしてから親項目に変更を加えた場合、その変更は当該親項目を含む各サーバーに、プロキシ・サーバーを使用せずに送信する必要があります。各サーバー間で親項目 (親の ACL を含む) の同期を保つことは、管理者の責任となります。

スキーマおよびパスワード・ポリシーを含むグローバル・ポリシー

cn=ibmpolicies および **cn=schema** サブツリーは、グローバル構成を保管しているため、分散ディレクトリーのサーバー間で複製する必要があります。サーバーが複製を所有する場合は、変更がそれらの個々のレプリカに渡されるように、**cn=ibmpolicies** サブツリーの下でゲートウェイ複製合意を設定します。**cn=ibmpolicies** 複製合意を使用すると、**cn=schema** および **cn=pwdpolicy** サブツリーは自動的に複製されます。グローバル・ポリシーには、**cn=ibmpolicies** の下に保管されているグローバル管理グループ項目が含まれます。詳細については、436 ページの『グローバル管理グループ』を参照してください。

注:

1. グローバル・ポリシーはプロキシ・サーバーに複製されません。
2. **cn=schema** への変更は、プロキシ・サーバーに複製されません。

重要: 新規のディレクトリー・サーバー・インスタンスを作成する場合は、以下の情報に注意してください。分散ディレクトリーを使用して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同期化させる必要があります。

ディレクトリー・サーバー・インスタンスを作成し、それを既存のディレクトリー・サーバー・インスタンスと暗号同期化する必要がある場合は、以下の手順を実行する前に、サーバー・インスタンスを同期する必要があります。

- 2 番目のサーバー・インスタンスの始動
- 2 番目のサーバー・インスタンスからの、**idsbulkload** コマンドの実行
- 2 番目のサーバー・インスタンスからの、**idsldif2db** コマンドの実行

ディレクトリー・サーバー・インスタンスの同期化については、703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』を参照してください。

区画項目

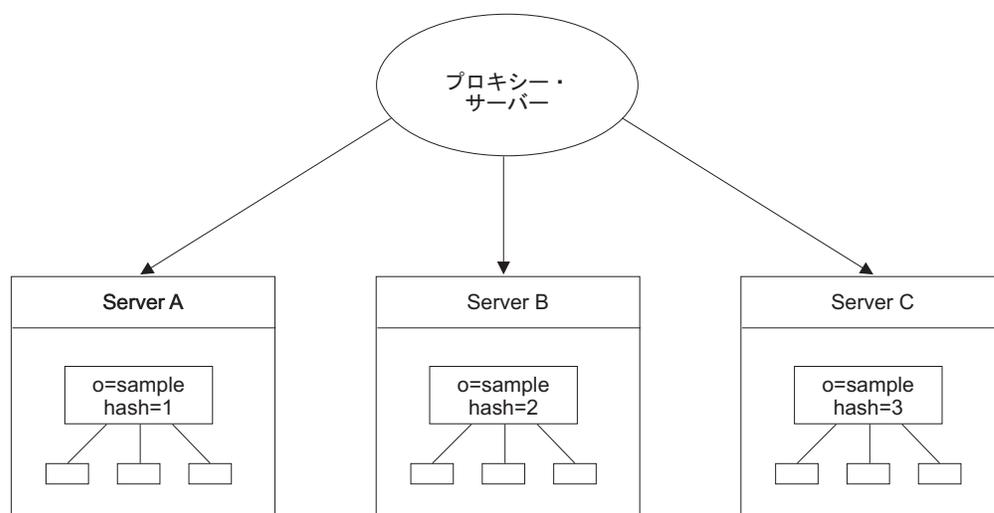
区画項目は、区画のベースとして存在する項目です (例: o=sample)。これらの項目は、プロキシ・サーバー経由では変更できません。

プロキシ・サーバーは、検索時 (重複プロキシ検索、項目はランダムに返される) にこれらの項目を 1 つ返すことができますが、これらの項目はプロキシ・サーバーを使用して変更できません。

プロキシ・サーバーを持つ分散ディレクトリーのセットアップ

以下に示す情報と例により、プロキシ・サーバーを使用して分散ディレクトリーをセットアップする方法について詳しく説明します。

次のシナリオでは、プロキシ・サーバーと、サブツリー o=sample の 3 つの区画を持つ分散ディレクトリーを設定する方法を説明します。



バックエンド・サーバーのセットアップ

バックエンド・サーバーをセットアップするには、以下のいずれかの方法を使用します。

Web 管理の使用:

Web 管理ツールを使用して、バックエンド・サーバーをセットアップするためのいくつかのタスクを実行できます。

バックエンド・サーバーへのサフィックスの追加:

以下に示す説明に従うことにより、Web 管理ツールで、バックエンド・サーバーにサフィックスを追加できます。

このタスクについて

サフィックスを追加するには、以下のいずれかの方法を使用します。

1. Server にログオンするには、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「サーバー・プロパティの管理」をクリックします。次に、「サフィックス」タブをクリックします。
2. サフィックス DN `o=sample` を入力します。
3. 「追加」をクリックします。
4. 追加するサフィックスの数だけこのプロセスを繰り返します。
5. 完了したら、終了せずに変更を保存する場合は「適用」をクリックし、変更を適用して終了する場合は「OK」をクリックします。
6. この手順を ServerB および ServerC に対しても繰り返します。

詳しくは、137 ページの『サフィックスの追加または除去』を参照してください。

グローバル管理グループ:

グローバル管理グループを使用すると、ディレクトリー管理者は、分散環境の管理権限をデータベース・バックエンドに委任できます。

グローバル管理グループ・メンバーとは、データベース・バックエンドの項目へのアクセスに関して管理グループと同じ特権セットが付与されているユーザーです。これらのメンバーは、ディレクトリー・サーバー・バックエンドに完全アクセスできます。すべてのグローバル管理グループ・メンバーは同じ特権セットを所有します。グローバル管理グループ・メンバーは、監査ログにアクセスできません。したがって、ローカル管理者は、セキュリティ管理のために、監査ログを使用してグローバル管理グループ・メンバーのアクティビティをモニターできます。

グローバル管理グループ・メンバーは、ディレクトリー・サーバーの構成設定に関連するデータまたは操作にアクセスする権限または特権は所有していません。これは一般的に構成バックエンドと呼ばれます。

グローバル管理グループ・メンバーは、スキーマの更新の要求をプロキシ・サーバーを介してバックエンド・サーバーに送信できます。この場合は、スキーマの更新がプロキシ・サーバーに適用された後に、変更がバックエンド・サーバーに伝搬されます。詳細については、448 ページの『分散ディレクトリーでのスキーマの更新』を参照してください。

注: 管理資格情報を使用してプロキシ・サーバーと通信するアプリケーションまたは管理者は、グローバル管理グループを使用する必要があります。例えば、プロキシ・サーバーを介してディレクトリー項目を変更する場合、命令 `cn=manager,cn=ibmpolicies` を使用して設定したメンバーを、ローカル管理者 (`cn=root`) の代わりに使用する必要があります。`cn=root` でプロキシ・サーバーにバインドすると、管理者にはプロキシ・サーバーの構成への全アクセス権限が与えられますが、ディレクトリー項目には匿名アクセスしかできません。

グローバル管理者グループのメンバーシップ用ユーザー項目の作成:

ここで説明する手順に従うことにより、グローバル管理者グループにメンバーシップ用ユーザー項目を作成することができます。

手順

1. ServerA にログオンします。このサーバーは、cn=ibmpolicies の区画として指定したサーバーです。
2. サーバーを開始します。
3. ナビゲーション領域から「ディレクトリー管理」トピックを展開します。
4. 「項目の追加」をクリックします。詳細については、526 ページの『項目の追加』を参照してください。
5. 「構造化オブジェクト・クラス」ドロップダウン・メニューから「個人 (person)」を選択します。
6. 「次へ」をクリックします。
7. 「次へ」をクリックして、「補助オブジェクト・クラスの選択」パネルへスキップします。
8. 「相対 DN」フィールドに「cn=manager」と入力します。
9. 「親 DN」フィールドに「cn=ibmpolicies」と入力します。
10. 「cn」フィールドに「manager」と入力します。
11. 「sn」フィールドに「manager」と入力します。
12. 「オプションの属性」タブをクリックします。
13. 「userPassword」フィールドにパスワードを入力します。例えば、mysecret などです。
14. 「完了」をクリックします。

グローバル管理グループへのユーザー項目の追加:

ここで説明する手順に従うことにより、グローバル管理グループにユーザー項目を追加することができます。

このタスクについて

以下のステップを実行して、グローバル管理グループに cn=manager を追加します。

1. ナビゲーション領域の「項目の管理」をクリックします。

注: 「現在の場所」フィールドには、DIT ツリーの現行レベルの項目が URL 形式で表示されます。DIT のサフィックス・ノードは ldap://hostname:port の形式で表示されます。「項目の管理」テーブルの RDN 列で RDN をクリックすると、次のレベルが表示されます。これにより、そのレベルの DIT が表示されず、表示されている DIT ツリーの上位レベルに移動するには、「現在の場所」フィールドで必要な URL をクリックします。

2. cn=ibmpolicies のラジオ・ボタンを選択し、「展開」をクリックします。

注: 展開可能な項目は、その項目に子項目があることを示します。展開可能な項目の場合は、「展開」列の項目の隣にプラス記号「+」が付いています。項目の隣にある「+」記号をクリックすると、選択した項目の子項目を表示できます。

3. globalGroupName=GlobalAdminGroup のラジオ・ボタンを選択し、「アクションの選択」ドロップダウン・メニューから「メンバーの管理」を選択して「実行」をクリックします。

4. グループごとの返すメンバーの最大数を指定します。「返すメンバーの最大数」をクリックした場合は、数字を入力してください。選択しない場合は「無制限」をクリックします。
5. テーブルにメンバーをロードするには、「ロード」をクリックするか、「アクションの選択」から「ロード」を選択して、「実行」をクリックします。
6. メンバー・フィールドに「cn=manager,cn=ibmpolicies」と入力し、「追加」をクリックします。
7. 次のメッセージが表示されます。「サーバーから項目をロードしていません。表には変更内容のみが表示されます。続行しますか?」。「OK」をクリックします。
8. 表には cn=manager が表示されます。「OK」をクリックします。cn=manager がグローバル管理グループのメンバーになりました。

コマンド・ラインの使用:

以下の作業は、コマンド行を使用して実行できます。

バックエンド・サーバーへのサフィックスの追加:

以下に示すリンクを参照することで、コマンド行を使用して、バックエンド・サーバーにサフィックスを追加することができます。

このタスクについて

コマンド行の使用によるバックエンド・サーバーへのサフィックスの追加については、137 ページの『サフィックスの追加または除去』を参照してください。

グローバル管理者グループのメンバーシップ用ユーザー項目の作成および追加:

以下に示すコマンドを発行することで、必要なアクションを実行できます。

このタスクについて

以下のコマンドを発行します。

```
idsldapadd -h <ServerA> -D <admin_dn> -w <admin_pw> -f <LDIF1>
idsldapmodify -h <ServerA> -D <admin_dn> -w <admin_pw> -f <LDIF2>
```

ここで、<LDIF1> の内容は以下のとおりです。

```
dn: cn=manager,cn=ibmpolicies
objectclass: person
sn: manager
cn: manager
userpassword: secret
```

ここで、<LDIF2> の内容は以下のとおりです。

```
dn: globalGroupName=GlobalAdminGroup,cn=ibmpolicies
changetype: modify
add: member
member: cn=manager,cn=ibmpolicies
```

プロキシ・サーバーのセットアップ

以下のいずれかの方法を使用することで、プロキシ・サーバーをセットアップできます。

Web 管理の使用:

Web 管理ツールを使用してプロキシ・サーバーをセットアップするためのさまざまなタスクで、以下に示す情報を使用することができます。

プロキシ・サーバーの構成:

以下に説明する手順に従うことにより、プロキシ・サーバーを構成できます。

このタスクについて

注: プロキシ・サーバーとして構成するサーバーに、ディレクトリーに配布する項目データが含まれている場合は、サーバーを構成する前にその項目データを LDIF ファイル内に抽出する必要があります。サーバーをプロキシ・サーバーに構成した後では、サーバーの RDBM に含まれているデータにアクセスできません。サーバーの RDBM 内のデータにアクセスする必要がある場合は、そのサーバーのプロキシ・サーバー構成を解除するか、そのサーバーのデータベースとして RDBM をポイントする新規のディレクトリー・サーバー・インスタンスを作成します。

手順

1. プロキシ・サーバーとして使用するサーバーにログオンします。
2. 構成専用モードでサーバーを始動します。
3. ナビゲーション領域から「プロキシ管理」を展開します。
4. 「プロキシ・プロパティの管理」をクリックします。
5. 「プロキシ・サーバーとして構成」チェック・ボックスを選択します。
6. 「サフィックス DN」フィールドに「**cn=ibmpolicies**」と入力して、「追加」をクリックします。
7. 「サフィックス DN」フィールドに「**o=sample**」と入力して、「追加」をクリックします。
8. すべてのグループ処理を使用可能にするには、「分散グループを使用可能にする」チェック・ボックスを選択します。デフォルトではこのチェック・ボックスが選択されています。構成ファイル内の `ibm-slapdProxyBackend` オブジェクト・クラスの `ibm-slapdProxyEnableDistGroups` 属性は、このコントロールに関連付けられています。**注:** 分散グループとは、グループ項目とメンバー DN が異なる区画に存在するグループです。すべてのグループ処理が使用不可である場合、プロキシ・サーバーは分散グループ評価をまったく行いません。これは、分散ディレクトリーにグループまたは分散グループが含まれない場合に、プロキシ・サーバーが追加のグループ処理を回避できるため有用です。ただし、グループがプロキシ・サーバー・レベルで使用不可であり、バックエンド・サーバー上のデータに分散グループが含まれている場合、動作はサポートされず、未定義になります。これはプロキシ・サーバーでは検出できないため、警告やエラーは発行されません。
9. 動的グループ処理を使用可能にするには、「分散動的グループを使用可能にする」チェック・ボックスを選択します。デフォルトではこのチェック・ボックスが選択されています。構成ファイル内の `ibm-slapdProxyBackend` オブジェクト・クラスの `ibm-slapdProxyEnableDistDynamicGroups` 属性は、このコントロールに関連付けられています。**注:** 分散動的グループとは、一部またはすべてのメンバーが異なる区画に存在する場合に定義される動的グループです。分散動

動的グループが存在しない場合、動的グループ処理を回避できます。この設定を有効にするには、動的グループを使用可能にする必要があります。「動的グループを使用可能にする (Enable dynamic group)」チェック・ボックスを選択またはクリアすると、動的グループ処理を使用可能または使用不可にすることができます。

10. 「OK」をクリックして変更を保存し、「概要」パネルに戻ります。注: Web 管理からいったんログオフし、再度ログインする必要があります。これを行うと、ナビゲーション領域が更新されます。ログオフ、再ログインを行わないと、ナビゲーション領域にはプロキシー・サーバー用の更新が行われません。

プロキシー・サーバーに分散ディレクトリー・サーバーを識別させる:

ここで説明する手順に従うことにより、プロキシー・サーバーに分散ディレクトリー・サーバーを識別させることができます。

手順

1. ナビゲーション領域から「プロキシー管理」を展開して、「バックエンド directory server の管理」をクリックします。
2. 「追加」をクリックします。
3. ServerA のホスト名を「ホスト名」フィールドに入力します。
4. ServerA のポート番号を入力します (この例では、すべてのサーバーがポート 389 を使用します)。
5. 「接続プール・サイズ」フィールドに、プロキシー・サーバーが最大で何台のバックエンド・サーバーと接続できるようにするかを入力します。最小値は 1 で最大値は 100 です。この例では、値を 5 に設定します。

注:

- 「接続プール・サイズ」フィールドに 5 より小さい値は設定しないでください。
 - バックエンド・サーバーへの接続の数は、バックエンド・サーバーに構成されているワーカーの数以下にしてください。
6. サーバーがヘルス・チェックの実行をスケジュールする間隔を秒単位で入力します。

注: この編集ボックスが表示されるのは、バージョン 6.1 以降のプロキシー・サーバーのみです。

7. 「接続ごとの最大保留クライアント操作数」フィールドに、接続ごとの最大保留クライアント操作数の数値を入力します。ibm-slapdProxyBackendServer オブジェクト・クラスの ibm-slapdProxyMaxPendingOpsPerClient 属性は、このフィールドに関連付けられています。この属性は、バックエンド接続のクライアント接続から保留要求数のしきい値制限を構成するために使用します。ibm-slapdProxyMaxPendingOpsPerClient 属性のデフォルト値は 5 です。ibm-slapdProxyMaxPendingOpsPerClient 属性に値「0」を割り当てると、接続ごとの保留クライアント操作数は無制限になります。

注: 「接続ごとの最大保留クライアント操作数」フィールドに割り当てることができるのは、正の数値だけです。負の値を割り当てると、該当するエラー・メッセージが表示されます。

8. バックエンド・ディレクトリー・サーバーの認証方式は、デフォルトでは「簡易」に設定されています。「SSL 暗号化を使用可能にする」チェック・ボックスが選択されていないことを確認してください。
9. 「ヘルス・チェック未処理制限を有効にする」チェック・ボックスを選択して、サーバーが待機している未処理ヘルス・チェック要求数を確認します。
10. 「ヘルス・チェック未処理制限」の値を入力します。
11. 「次へ」をクリックします。
12. 「バインド DN」フィールドに、管理者 DN、ローカル管理者のメンバー DN、またはグローバル管理者グループのメンバーを指定します。例えば、**cn=root** です。
13. 「バインド・パスワード」フィールドに、管理者パスワードを指定し確認します。例えば、**secret** です。
14. 「完了」をクリックします。
15. ServerB および ServerC に対して、ステップ 2 から 10 を繰り返します。
16. 完了したら、「閉じる」をクリックして変更を保管し、「概要」パネルに戻ります。
17. バックエンド・サーバーがすべて始動していることを確認してください。

注: プロキシ・サーバーが始動時に 1 つ以上のバックエンド・サーバーと接続できない場合、そのプロキシ・サーバーは構成モードで始動しています。サーバー・グループを設定しない限り、プロキシ・サーバーは構成モードで始動します。456 ページの『サーバー・グループ』を参照してください。

グローバル・ポリシーの同期化:

以下に示す手順に従うことにより、グローバル・ポリシーを同期することができます。

このタスクについて

以下のステップでは、単一の区画として **cn=ibmpolicies** を設定します。これは、すべてのサーバーでグローバル・ポリシーを同期化させる場合に必要です。グローバル管理グループ・メンバーは、スキーマの更新の要求をプロキシ・サーバーを介してバックエンド・サーバーに送信できます。スキーマの更新について詳しくは、448 ページの『分散ディレクトリーでのスキーマの更新』を参照してください。

手順

1. ナビゲーション領域から「区画ベースの管理」をクリックします。
2. 「区画ベース」テーブルで、「追加」をクリックします。
3. 「分割名」フィールドに分割名を入力します。注: この値は、区画ベース DN を区画に分割する分割ポイントに指定されている分割名を表します。
ibm-slapdProxyBackendSplitContainer オブジェクト・クラスの **ibm-slapdProxySplitName** 属性は、この分割名に関連付けられています。
ibm-slapdProxySplitName 属性の値は、プロキシ・サーバーの構成ファイル内で固有であり、英数字の値のみが含まれている必要があります。例えば、ディレクトリーが DN 「o=sample」で 2 つの区画に分割されている場合、分割名

は o=sample 分割とこの 2 つの区画に関連付けられます。分割区画を一意的に識別するには、ibm-slapdProxySplitName および ibm-slapdProxyPartitionIndex 属性を使用する必要があります。

4. 「区画ベース DN」フィールドに **cn=ibmpolicies** と入力します。
 5. 「区画数」フィールドに **1** を入力します。注: cn=ibmpolicies の場合、**1** より大きい値はサポートされていません。
 6. 自動フェイルバックを使用可能にするには、「**自動フェイルバックが使用可能**」チェック・ボックスを選択します。
 - a. 自動フェイルバック・キューを使用可能にするには、「**自動フェイルバック・キューが使用可能 (Auto fail-back queue enabled)**」チェック・ボックスを選択します。ibm-slapdProxyBackendSplitContainer オブジェクト・クラスの ibm-slapdProxyFailbackBasedOnQueueEnabled 属性は、このコントロールに関連付けられています。
「**自動フェイルバック・キューが使用可能 (Auto fail-back queue enabled)**」チェック・ボックスを選択すると、フェイルバックは複製キュー・サイズに基づいて実行されます。このチェック・ボックスを選択しない場合、自動フェイルバック・キューのしきい値サイズの値は無視されます。
 - b. 「**自動フェイルバック・キューのしきい値サイズ (Auto fail-back queue threshold size)**」フィールドに自動フェイルバック・キューのしきい値サイズを入力します。ibm-slapdProxyBackendSplitContainer オブジェクト・クラスの ibm-slapdProxyFailbackQueueThresholdSize 属性は、このコントロールに関連付けられています。
自動フェイルバック・キューのしきい値サイズのデフォルト値は **5** です。自動フェイルバック・キューのしきい値サイズは、複製状態が安定しているかどうかを判別する複製キューのサイズを示します。**0** の値は、変更の保留がない場合にのみ、複製キューは安定していると見なされることを示します。負の値は許可されていません。
- 注: バックエンド・サーバーの再始動時に自動フェイルバックも使用可能である場合、プロキシ・サーバーはそのバックエンド・サーバーを使用して自動的に始動します。
7. プロキシの高い整合性を使用可能にするには、「**プロキシの高い整合性**」チェック・ボックスを選択します。詳しくは、453 ページの『高い整合性とフェイルオーバー』を参照してください。
 8. 「**OK**」をクリックします。
 9. cn=ibmpolicies のラジオ・ボタンを選択し、「**サーバーの表示**」をクリックします。
 10. cn=ibmpolicies が「**区画ベース DN**」フィールドに表示されていることを確認してください。
 11. 「**区画ベースのバックエンド・ディレクトリー・サーバー**」テーブルで、「**追加**」をクリックします。
 12. 「**バックエンド・ディレクトリー・サーバー**」メニューから、ServerA を選択します。
 13. 「**区画索引**」フィールドに **1** を入力します。
 14. 「**サーバー役割**」リストから、バックエンド・ディレクトリー・サーバーの役割を選択します。注: **使用可能であり**、バックエンド・ディレクトリー・サー

バーに割り当てることができる役割は、primarywrite および any です。1 次書き込みサーバーは、書き込み要求の送信先であるマスター・サーバーまたはピア・サーバーに設定してください。

15. 「プロキシ層」リストから、割り当てる優先順位を選択します。詳細については、454 ページの『バックエンド・サーバーの重みによる優先順位付け』を参照してください。
16. 「OK」をクリックします。

データの区画への分割:

以下に示すステップを使用することで、サブツリー `o=sample` 内のデータを 3 つの区画に分割することができます。

このタスクについて

1. 「区画ベース」テーブルで、「追加」をクリックします。
2. 「分割名」フィールドに分割名を入力します。
3. 「区画ベース DN」フィールドに `o=sample` と入力します。
4. 「区画数」フィールドに `3` を入力します。
5. 自動フェイルバックを使用可能にするには、「自動フェイルバックが使用可能」チェック・ボックスを選択します。
 - 自動フェイルバック・キューを使用可能にするには、「自動フェイルバック・キューが使用可能 (Auto fail-back queue enabled)」チェック・ボックスを選択します。ibm-slapdProxyBackendSplitContainer オブジェクト・クラスの `ibm-slapdProxyFailbackBasedOnQueueEnabled` 属性は、このコントロールに関連付けられています。

「自動フェイルバック・キューが使用可能 (Auto fail-back queue enabled)」チェック・ボックスを選択すると、フェイルバックは複製キュー・サイズに基づいて実行されます。このチェック・ボックスを選択しない場合、自動フェイルバック・キューのしきい値サイズの値は無視されます。
 - 「自動フェイルバック・キューのしきい値サイズ (Auto fail-back queue threshold size)」フィールドに自動フェイルバック・キューのしきい値サイズを入力します。ibm-slapdProxyBackendSplitContainer オブジェクト・クラスの `ibm-slapdProxyFailbackQueueThresholdSize` 属性は、このコントロールに関連付けられています。

自動フェイルバック・キューのしきい値サイズのデフォルト値は `5` です。自動フェイルバック・キューのしきい値サイズは、複製状態が安定しているかどうかを判別する複製キューのサイズを示します。`0` の値は、変更の保留がない場合にのみ、複製キューは安定していると見なされることを示します。負の値は許可されていません。
6. プロキシの高い整合性を使用可能にするには、「プロキシの高い整合性」チェック・ボックスを選択します。
7. 「OK」をクリックします。

サーバーへの区画索引値の割り当て:

ここで説明する手順を使用することで、サーバーに区画索引値を割り当てることができます。

このタスクについて

以下のステップでは、各サーバーに区画値を割り当てます。

手順

1. o=sample のラジオ・ボタンを選択し、「サーバーの表示」をクリックします。
2. o=sample が「区画ベース DN」フィールドに表示されていることを確認してください。
3. 「区画ベースのバックエンド・ディレクトリー・サーバー」テーブルで、「追加」をクリックします。
4. 「バックエンド・ディレクトリー・サーバー」ドロップダウン・メニューから、ServerA を選択します。
5. 「区画索引」フィールドに 1 が表示されていることを確認してください。
6. 「サーバー役割」ドロップダウン・メニューから、該当するサーバー役割を選択します。注: この値は、特定の区画内のバックエンド・ディレクトリー・サーバーの役割を表します。ibm-slapdProxyBackendSplit オブジェクト・クラスの ibm-slapdProxyServerRole 属性は、この値に関連付けられています。この属性に割り当てることができる値は、primarywrite などです。
7. 「プロキシ層」リストから、割り当てる優先順位を選択します。
8. 「OK」をクリックします。
9. 「区画ベースのバックエンド・ディレクトリー・サーバー」テーブルで、「追加」をクリックします。
10. 「バックエンド・ディレクトリー・サーバー」ドロップダウン・メニューから、ServerB を選択します。
11. 「区画索引」フィールドに 2 が表示されているようにしてください。注: この数値は自動的に増加します。区画索引番号は手動で変更できますが、ベースの実際の区画数以下でなければなりません。例えば、区画ベースに区画が 3 つしかない場合は、区画索引として 4 は使用できません。区画索引の重複は、そのサブツリーの複製に参加しているサーバーでのみ許可されます。
12. 「OK」をクリックします。
13. 「区画ベースのバックエンド・ディレクトリー・サーバー」テーブルで、「追加」をクリックします。
14. 「バックエンド・ディレクトリー・サーバー」ドロップダウン・メニューから、ServerC を選択します。
15. 「区画索引」フィールドに 3 が表示されていることを確認してください。
16. 「サーバー役割」ドロップダウン・メニューから、該当するサーバー役割を選択します。注: この値は、特定の区画内のバックエンド・ディレクトリー・サーバーの役割を表します。ibm-slapdProxyBackendSplit オブジェクト・クラスの ibm-slapdProxyServerRole 属性は、この値に関連付けられています。この属性に割り当てることができる値は、primarywrite などです。
17. 「プロキシ層」リストから、割り当てる優先順位を選択します。

18. 「OK」をクリックします。
19. 完了したら、「閉じる」をクリックします。
20. 変更した内容を有効にするには、プロキシ・サーバーを再始動します。

区画ベースの表示:

ここに示す手順を実行することにより、区画ベースを表示することができます。

このタスクについて

1. ナビゲーション領域から「区画ベースの表示」をクリックします。
2. 「分割の選択」コンボ・ボックスから分割を選択します。
3. 「区画の表示」をクリックします。これにより、選択された分割で使用可能な区画が「区画項目」テーブルに取り込まれます。

区画のサーバー項目を表示するには、以下のステップを行います。

1. 「区画項目」テーブルから区画項目を選択します。
2. 「サーバーの表示」をクリックします。これにより、分割の選択された区画に関連付けられたサーバー情報が「サーバー項目」テーブルに取り込まれます。

項目の場所の表示:

Web 管理ツールを使用することで、項目の場所を表示することができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域で、「プロキシ管理」をクリックし、展開されたリストで「項目の場所の表示」をクリックします。このパネルの「場所の詳細」テーブルには、分散ディレクトリー内の単一 DN 項目または複数 DN 項目の場所の詳細が取り込まれます。「場所の詳細」テーブルに情報を取り込むために、項目検索拡張操作が呼び出されます。

分散ディレクトリー内の単一 DN 項目の場所を表示する場合は、以下のステップを行います。

1. 分散ディレクトリー内の DN 項目の場所を検索するには、「項目 DN」を選択してフィールドに有効な DN を入力するか、「参照」ボタンをクリックして項目 DN のロケーションを指定します。
2. 「項目の詳細の表示」ボタンをクリックします。これにより、指定された項目 DN のロケーション情報が「場所の詳細」テーブルに取り込まれます。
3. 「閉じる」ボタンをクリックして、「概要」パネルにナビゲートします。

分散ディレクトリー内の複数の DN 項目の場所を表示する場合は、以下のステップを行います。

1. 分散ディレクトリー内の複数の DN 項目の場所を検索するには、「複数の DN を含むファイルを選択する」を選択します。
2. 複数の DN 項目を含むテキスト・ファイルの絶対パスを「ファイル名」フィールドに入力します。あるいは、「参照」ボタンをクリックして、DN 項目を含むテキスト・ファイルの場所を指定します。
3. 「ファイルの実行依頼」ボタンをクリックします。

4. 「項目の詳細の表示」ボタンをクリックして、DN 項目のロケーション情報を「場所の詳細」テーブルに取り込みます。
5. 「閉じる」ボタンをクリックして、「概要」パネルにナビゲートします。

プロキシー・サーバーの構成:

以下に示すコマンドを発行することで、プロキシー・サーバーを構成することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -h <Proxy Server> -D <admin_dn> -w <admin_pw> -i <LDIF1>
idsldapmodify -h <Proxy Server> -D <admin_dn> -w <admin_pw> -i <LDIF2>
```

ここで、<LDIF1> の内容は以下のとおりです。

```
dn: cn=Configuration
changetype: modify
replace: ibm-slapdServerBackend
ibm-slapdServerBackend: PROXY
```

ここで、<LDIF2> の内容は以下のとおりです。

```
dn: cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
changetype: modify
add: ibm-slapdSuffix
ibm-slapdSuffix: cn=ibmpolicies
ibm-slapdSuffix: o=sample
-
replace: ibm-slapdProxyEnableDistDynamicGroups
ibm-slapdProxyEnableDistDynamicGroups: true
-
replace: ibm-slapdProxyEnableDistGroups
ibm-slapdProxyEnableDistGroups: true
```

プロキシー・サーバーの構成:

以下に示すコマンドを発行することで、プロキシー・サーバーを構成することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -h <Proxy Server> -D <admin_dn> -w <admin_pw> -i <LDIF1>
idsldapmodify -h <Proxy Server> -D <admin_dn> -w <admin_pw> -i <LDIF2>
```

ここで、<LDIF1> の内容は以下のとおりです。

```
dn: cn=Configuration
changetype: modify
replace: ibm-slapdServerBackend
ibm-slapdServerBackend: PROXY
```

ここで、<LDIF2> の内容は以下のとおりです。

```
dn: cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
changetype: modify
add: ibm-slapdSuffix
ibm-slapdSuffix: cn=ibmpolicies
ibm-slapdSuffix: o=sample
-
replace: ibm-slapdProxyEnableDistDynamicGroups
ibm-slapdProxyEnableDistDynamicGroups: true
-
replace: ibm-slapdProxyEnableDistGroups
ibm-slapdProxyEnableDistGroups: true
```

プロキシ・サーバーに分散ディレクトリー・サーバーを識別させる:

ここにリストするコマンドを発行することにより、コマンド行を使用して、プロキシ・サーバーに分散ディレクトリー・サーバーを識別させることができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapadd -h <Proxy Server> -D <admin_dn> -w <admin_pw> -f <LDIF1>
```

ここで、<LDIF1> の内容は以下のとおりです。

```
dn: cn=Server1, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory, cn=Schemas,
cn=Configuration
cn: Server1
ibm-slapdProxyBindMethod: Simple
ibm-slapdProxyConnectionPoolSize: 5
ibm-slapdProxyMaxPendingOpsPerClient: <value to be set in numerals>
ibm-slapdProxyDN: cn=root
ibm-slapdProxyPW: secret
ibm-slapdProxyTargetURL: ldap://ServerA:389
objectClass: top
objectClass: ibm-slapdProxyBackendServer
objectClass: ibm-slapdConfigEntry
```

```
dn: cn=Server2, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory, cn=Schemas,
cn=Configuration
cn: Server2
ibm-slapdProxyBindMethod: Simple
ibm-slapdProxyConnectionPoolSize: 5
ibm-slapdProxyMaxPendingOpsPerClient: <value to be set in numerals>
ibm-slapdProxyDN: cn=root
ibm-slapdProxyPW: secret
ibm-slapdProxyTargetURL: ldap://ServerB:389
objectClass: top
objectClass: ibm-slapdProxyBackendServer
objectClass: ibm-slapdConfigEntry
```

```
dn: cn=Server3, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory, cn=Schemas,
cn=Configuration
cn: Server3
ibm-slapdProxyBindMethod: Simple
ibm-slapdProxyConnectionPoolSize: 5
ibm-slapdProxyMaxPendingOpsPerClient: <value to be set in numerals>
ibm-slapdProxyDN: cn=root
ibm-slapdProxyPW: secret
ibm-slapdProxyTargetURL: ldap://ServerC:389
objectClass: top
objectClass: ibm-slapdProxyBackendServer
objectClass: ibm-slapdConfigEntry
```

データの区画への分割およびサーバーへの区画索引値の割り当て:

以下に示すコマンドを使用することで、データを区画に分割し、区画索引値をサーバーに割り当てることができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapadd -h <Proxy Server> -D <admin_dn> -w <admin_pw> -f <LDIF2>
```

<LDIF2> には、以下の情報が格納されています。

```
dn: cn=cn%=ibmpolicies split, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory,
cn=Schemas, cn=Configuration
cn: cn=ibmpolicies split
ibm-slapdProxyNumPartitions: 1
ibm-slapdProxyPartitionBase: cn=ibmpolicies
ibm-slapdProxySplitName: ibmpolicysplit
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdProxyBackendSplitContainer

dn: cn=split1, cn=cn%=ibmpolicies split, cn=ProxyDB, cn=Proxy Backends,
cn=IBM Directory, cn=Schemas, cn=Configuration
cn: split1
```

```

ibm-slapdProxyBackendServerDN: cn=Server1,cn=ProxyDB,cn=Proxy Backends,
cn=IBM Directory,cn=Schemas,cn=Configuration
ibm-slapdProxyPartitionIndex: 1
ibm-slapdProxyBackendServerRole: any
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdProxyBackendSplit
dn: cn=o%=sample split, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory,
cn=Schemas, cn=Configuration
cn: o=sample split
ibm-slapdProxyNumPartitions: 3
ibm-slapdProxyPartitionBase: o=sample
ibm-slapdProxySplitName: samplesplit
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdProxyBackendSplitContainer

dn: cn=split1, cn=o%=sample split, cn=ProxyDB, cn=Proxy Backends,
cn=IBM Directory, cn=Schemas, cn=Configuration
cn: split1
ibm-slapdProxyBackendServerDN: cn=Server1,cn=ProxyDB,cn=Proxy Backends,
cn=IBM Directory,cn=Schemas,cn=Configuration
ibm-slapdProxyPartitionIndex: 1
ibm-slapdProxyBackendServerRole: any
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdProxyBackendSplit

dn: cn=split2, cn=o%=sample split, cn=ProxyDB, cn=Proxy Backends,
cn=IBM Directory, cn=Schemas, cn=Configuration
cn: split2
ibm-slapdProxyBackendServerDN: cn=Server2,cn=ProxyDB,cn=Proxy Backends,
cn=IBM Directory,cn=Schemas,cn=Configuration
ibm-slapdProxyPartitionIndex: 2
ibm-slapdProxyBackendServerRole: any
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdProxyBackendSplit

dn: cn=split3, cn=o%=sample split, cn=ProxyDB, cn=Proxy Backends,
cn=IBM Directory, cn=Schemas, cn=Configuration
cn: split3
ibm-slapdProxyBackendServerDN: cn=Server3,cn=ProxyDB,cn=Proxy Backends,
cn=IBM Directory,cn=Schemas,cn=Configuration
ibm-slapdProxyPartitionIndex: 3
ibm-slapdProxyBackendServerRole: any
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdProxyBackendSplit

```

分散ディレクトリーでのスキーマの更新

グローバル管理グループ・メンバーがスキーマの更新を要求した場合、そのスキーマの更新は、最初に Security Directory Proxy Server に適用され、次にバックエンド・サーバーに伝搬されます。また、グローバル管理者グループ・メンバーは、バックエンド・サーバーに対して直接、スキーマの更新を要求できます。ただし、1次管理者、SchemaAdmin 役割を備えたローカル管理グループ・メンバー、またはマスター・サーバー DN がプロキシ・サーバーに対してスキーマの更新を要求した場合、スキーマの更新は、そのプロキシ・サーバーにのみ適用されます。

プロキシ・サーバーがサービスを提供しているすべてのバックエンド・サーバーにスキーマの更新を強制的に適用するには、グローバル・ポリシーを同期させる必要があります。Security Directory Server は、複製トポロジー内のコンシューマー・サーバーに対する、スキーマの更新の複製をサポートしています（ただし、プロキシ・サーバーがサービスを提供しているすべてのバックエンド・サーバー間で CN=IBMPOLICIES コンテキストに複製がセットアップされている場合）。これを実装するには、プロキシ・サーバーがサービスを提供しているすべてのバックエンド・サーバー間で、CN=IBMPOLICIES コンテキストに複製をセットアップする必要があります。1次書き込みサーバーに障害が発生した場合でもスキーマが正常に更新されるようにするには、ディレクトリー管理者が、CN=IBMPOLICIES コンテキストの複製トポロジーに、少なくとも 1 つの別の書き込みサーバーを含める必要があります。1次書き込みサーバーに障害が発生した場合、プロキシは、次に使用可

能な書き込みサーバーに、スキーマの更新を再送付します。1 次書き込みサーバーが復元されると、2 次書き込みサーバーは、1 次書き込みサーバーが不在のときに受信したスキーマの更新を 1 次書き込みサーバーにプッシュします。このセットアップを作成するには、以下のアクションを考慮する必要があります。

1. プロキシ・サーバーを持つ分散ディレクトリーをセットアップします。438 ページの『プロキシ・サーバーのセットアップ』を参照してください。
2. `cn=ibmpolicies` サブツリー用の複製トポロジーを作成します。複製のセットアップについて詳しくは、310 ページの『レプリカ生成』および460 ページの『グローバル・ポリシーのトポロジーの設定』を参照してください。

注: 書き込みサーバーがすべてオフラインの場合、プロキシ・サーバーは、該当するエラー・メッセージを LDAP クライアントに返します。

スキーマの更新を伝搬するプロキシ・サーバーの構成例を抜粋して示します。

```
cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
cn=Proxy Backend
ibm-slapdDNPartitionPlugin=libldapnhash.so dnHashInit
ibm-slapdPagedResAllowNonAdmin=TRUE
ibm-slapdPagedResLmt=3
ibm-slapdPlugin=database libback-proxy.so proxy_backend_init
ibm-slapdPlugin=extendedoplibback-proxy.so initResumeRole
ibm-slapdProxyEnabledDistDynamicGroups=true
ibm-slapdProxyEnabledDistGroups=true
ibm-slapdSuffix=o=sample
ibm-slapdSuffix=cn=ibmpolicies
objectclass=top
objectclass=ibm-slapdConfigEntry
objectclass=ibm-slapdProxyBackend

cn=Server1, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory,
cn=Schemas, cn=Configuration
cn=Server1
ibm-slapdProxyBindMethod=Simple
ibm-slapdProxyConnectionPoolSize=5
ibm-slapdProxyDN=cn=root
ibm-slapdProxyHealthCheckOlimit=24
ibm-slapdProxyMaxPendingOpsPerClient=5
ibm-slapdProxyPW={AES256}LM3NvpMr0FvYhTnEdmeTbw==
ibm-slapdProxyTargetURL=ldap://ServerA:389
ibm-slapdServerID=Bc440640-6e1f-102e-88a8-ff9133d50edd
ibm-slapdStatusInterval=5
objectclass=top
objectclass=ibm-slapdProxyBackendServer
objectclass=ibm-slapdConfigEntry

cn=Server2, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory,
cn=Schemas, cn=Configuration
cn=Server2
ibm-slapdProxyBindMethod=Simple
ibm-slapdProxyConnectionPoolSize=5
ibm-slapdProxyDN=cn=root
ibm-slapdProxyHealthCheckOlimit=24
ibm-slapdProxyMaxPendingOpsPerClient=5
ibm-slapdProxyPW={AES256}LM3NvpMr0FvYhTnEdmeTbw==
ibm-slapdProxyTargetURL=ldap://ServerB:389
ibm-slapdServerID=aaaa01c0-6e1f-102e-8ea9-8d957fd1611f
ibm-slapdStatusInterval=5
objectclass=top
objectclass=ibm-slapdProxyBackendServer
objectclass=ibm-slapdConfigEntry

cn=cn%=ibmpolicies split, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory,
cn=Schemas, cn=Configuration
cn=cn%=ibmpolicies split
ibm-slapdProxyAutoFailBack=true
ibm-slapdProxyFailbackBasedOnQueueEnabled=true
ibm-slapdProxyFailbackQueueThreshold=5
ibm-slapdProxyHighConsistency=true
ibm-slapdProxyNumPartitions=1
ibm-slapdProxyPartitionBase=cn=ibmpolicies
ibm-slapdProxySplitName=ibmpoliciesplit
objectclass=ibm-slapdConfigEntry
objectclass=ibm-slapdProxyBackendSplitContainer
objectclass=top

cn=split1, cn=cn%=ibmpolicies split, cn=ProxyDB, cn=Proxy Backends,
cn=IBM Directory, cn=Schemas, cn=Configuration
cn=split1
```

```

ibm-slapdProxyBackendServerDN=cn=Server1,cn=ProxyDB,cn=Proxy Backends,
cn=IBM Directory,cn=Schemas,cn=Configuration
ibm-slapdProxyBackendServerRole=primarywrite
ibm-slapdProxyPartitionIndex=1
ibm-slapdProxyTier=1
objectclass=top
objectclass=ibm-slapdConfigEntry
objectclass=ibm-slapdProxyBackendSplit

cn=split2,cn=cn%=ibmpolicies split,cn=ProxyDB,cn=Proxy Backends,
cn=IBM Directory,cn=Schemas,cn=Configuration
cn=split2
ibm-slapdProxyBackendServerDN=cn=Server2,cn=ProxyDB,cn=Proxy Backends,
cn=IBM Directory,cn=Schemas,cn=Configuration
ibm-slapdProxyBackendServerRole=any
ibm-slapdProxyPartitionIndex=1
ibm-slapdProxyTier=1
objectclass=top
objectclass=ibm-slapdConfigEntry
objectclass=ibm-slapdProxyBackendSplit

```

分散ディレクトリーのパスワード・ポリシー

分散ディレクトリーのパスワード・ポリシーは、プロキシー・サーバーに多少の追加オーバーヘッドを与えて、バックエンド・サーバーに対して実施されます。

ユーザー・パスワード・ポリシーには、グローバル・パスワード・ポリシーと複数のパスワード・ポリシーの 2 種類があります。複数のパスワード・ポリシーが分散ディレクトリー環境でサポートされるのは、すべてのグループ、メンバー、およびポリシー・データが単一区画に対してローカルである場合のみです。一方、グローバル・パスワード・ポリシーは、ユーザーやグループが分散していてもサポートされます。

プロキシー・サーバーでパスワード・ポリシーがサポートされるには、すべてのバックエンド・サーバーでパスワード・ポリシーが使用可能である必要があります。プロキシー・サーバーは、すべての必要な要求に対するパスワード・ポリシー制御を送信します。大多数のパスワード・ポリシーはバックエンド・サーバーでローカルに実施されるため、非分散環境の場合と同様に機能します。場合によっては、一貫性のあるパスワード・ポリシーを実施するために、プロキシー・サーバー・レベルでさらに検査を行う必要があります。

注:

1. 管理者がパスワード・ポリシーを使用可能または使用不可にする場合、プロキシー・サーバーを再始動する必要があります。
2. プロキシー・サーバーでは、有効パスワード・ポリシー拡張操作はサポートされません。

プロキシー・サーバーは 2 つの拡張操作を使用して、外部バインドに対してパスワード・ポリシーを実施できるようにします。これらは、パスワード・ポリシー初期化およびバインド検証拡張操作と、パスワード・ポリシー・ファイナライズおよびバインド検証拡張操作です。これらの 2 つの拡張操作について詳しくは、「*IBM Security Directory Server Version 6.3 Programming Reference*」を参照してください。

フェイルオーバーおよびロード・バランシング

プロキシー・サーバーは、高い整合性が使用不可の場合に読み取り要求のロード・バランシングを実行します。高い整合性が使用可能な場合、フェイルオーバーが発生しない限り、すべての読み取り要求と書き込み要求は 1 次書き込みサーバーに送

信されます。バックエンド・サーバーが使用不可の場合、この操作ではエラーが表示されます。以降のすべての操作は、使用可能な別のサーバーにフェイルオーバーします。

プロキシ・サーバーは、所定の区画のレプリカをすべて認識し、読み込んだ要求の処理をそれらのオンライン・レプリカに均等に配分します (ロード・バランシング)。また、プロキシ・サーバーは所定の区画のマスターをすべて認識し、そのうちの 1 つをプライマリ・マスターとして使用する必要があります。1 次書き込みサーバーとして構成されているサーバーがプライマリ・マスターです。1 次書き込みサーバーが構成されていない場合は、最初のマスター・サーバーまたはピア・サーバーが 1 次書き込みサーバーです。プライマリ書き込みサーバーがダウンした場合、プロキシ・サーバーは、そのプライマリ書き込みサーバーの機能を、バックアップ・サーバー (他のマスター・サーバーまたはピア・サーバーの 1 つ) にフェイルオーバーできます。要求された操作が現在オンライン中のサーバーで実行できない場合、プロキシ・サーバーは操作エラーを返します。

注:

- 適切なパフォーマンスを得るためには、すべてのバックエンド・サーバーおよびプロキシ・サーバー・インスタンスを暗号同期する必要があります。ディレクトリー・サーバー・インスタンスの同期化については、703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』を参照してください。
- 比較操作ではロード・バランスは取られません。

詳細については、453 ページの『高い整合性とフェイルオーバー』を参照してください。

自動フェイルバック

Security Directory Server には、自動フェイルバックを使用可能または使用不可にするオプションがあります。

自動フェイルバックが使用可能な場合、プロキシ・サーバーは、サーバーが使用可能になるとすぐにそのサーバーを使用します。ただし、自動フェイルバックが使用不可の場合、サーバーは役割の再開拡張操作を使用して復元する必要がありますが、自動フェイルバックが常に使用可能な以下の場合を除きます。

常に自動フェイルバックを開始するケースと実行されるアクション

- 区画内のすべてのバックエンド・サーバーがダウンしている。

実行アクション:

- 読み取りサーバーがオンライン状態に戻る最初のサーバーである場合、プロキシ・サーバーはそのサーバーを自動復元します。読み取りサーバーは書き込み操作を処理できないため、オンライン状態になっている最初の書き込みサーバーも復元されます。
 - 書き込みサーバーがオンライン状態に戻る最初のサーバーである場合、プロキシ・サーバーはその書き込みサーバーを自動復元します。書き込みサーバーは読み取り要求と書き込み要求の両方を処理できるため、この他のサーバーで自動復元されるものではありません。
- 区画内のすべての書き込み可能バックエンド・サーバーがダウンしている。

実行されるアクション:

- 最初にオンライン状態に戻る書き込みサーバーがプロキシー・サーバーによって自動復元されます。

注:

- 自動フェイルバックは、**ibm-slapdEnableAutoFailBack** 属性の値を true または false に設定することで、使用可能または使用不可にできます。
- **ibm-slapdEnableAutoFailBack** のデフォルト値は true です。

Security Directory Server には、構成可能な複製キュー・サイズに基づいたフェイルバックを使用可能にするオプションもあります。この機能では、現在の書き込みサーバーからフェイルバックされるサーバーへの複製キュー・サイズが、構成された複製キュー・サイズ以下である場合にのみ、フェイルバックが自動的に実行されます。

Web 管理ツールを使用して、構成可能な複製キュー・サイズに基づいたフェイルバックを使用可能にする場合は、443 ページの『データの区画への分割』を参照してください。

コマンド行を使用して、構成可能な複製キュー・サイズに基づいたフェイルバックを使用可能にする場合は、以下のようにします。

- 以下のコマンドを実行して、**ibm-slapdProxyFailbackBasedOnQueueEnabled** 属性の値を TRUE に設定します。

```
ldapmodify -D <admin DN of proxy server> -w <admin PW of proxy server> %  
-p <port of proxy server> -i modify.ldif  
  
where modify.ldif contains  
dn: <RDN of Backend Split Container>, cn=ProxyDB, cn=Proxy Backends,  
cn=IBM Directory, cn=Schemas, cn=Configuration  
changetype: modify  
replace: ibm-slapdProxyFailbackBasedOnQueueEnabled  
ibm-slapdProxyFailbackBasedOnQueueEnabled : <value to be set as either TRUE or FALSE>
```

- 以下のコマンドを実行して、**ibm-slapdProxyFailbackQueueThreshold** 属性の値を必要な値に設定します。

```
ldapmodify -D <admin DN of proxy server> -w <admin PW of proxy server> %  
-p <port of proxy server> -i modify.ldif  
  
where modify.ldif contains  
dn: <RDN of Backend Split Container>, cn=ProxyDB, cn=Proxy Backends,  
cn=IBM Directory, cn=Schemas, cn=Configuration  
changetype: modify  
replace: ibm-slapdProxyFailbackQueueThreshold  
ibm-slapdProxyFailbackQueueThreshold : <value to be set in numerals>
```

正常性チェック機能

正常性チェック機能では、バックエンド・サーバーが応答しなくなった時点を検出します。この機能を使用可能にするには、**ibm-slapdProxyHealthCheck01limit** 属性を設定します。この属性の値は、バックエンド・サーバーが応答しないことをプロキシー・サーバーが判別するまでの、未処理の正常性チェック要求数のしきい値を示します。

プロキシー・サーバー・バックエンドは、正常性チェックというスレッドを使用して、使用可能なサーバーとダウンしているサーバーとを識別します。正常性チェック・スレッドは、各バックエンド・サーバーに対して **ibm-slapdisconfigurationmode** 属性のルート DSE 検索を開始することにより、正常性チェックを実行します。サーバーがダウンしているか、サーバーが構成専用モード

であることが原因で、いずれかのサーバーに対するルート DSE 検索が失敗した場合、スレッドはフェイルオーバー処理を開始し、そのサーバーに使用不可とマークを付けます。サーバーが使用不可と識別されると、適切なエラー・メッセージもエラー・ログに書き込まれます。

例えば、正常性チェック間隔が 5 秒に設定され、**olimit** が 5 に設定されているとします。この場合、バックエンド・サーバーが正常性チェック検索に 25 から 30 秒以内に応答しない場合、プロキシ・サーバーはそのバックエンド・サーバーに切断状態のマークを付け、次に使用可能なサーバーにフェイルオーバーします。続いて、メッセージも記録されます (GLPPXY044E)。

このメッセージがログに記録されるのは、バックエンド・サーバーが過負荷状態でありパフォーマンスの調整またはハードウェアのアップグレードが必要である場合か、バックエンド・サーバーが対処を要する何らかのエラー状態に陥っている場合です。バックエンド・サーバーがルート DSE 検索に正常に回答できるようになると、プロキシ・サーバーはバックエンド・サーバーの状態を更新します。自動フェイルバックが使用可能な場合、サーバーが復元されます。自動フェイルバックが使用不可の場合、管理者は役割の再開拡張操作を使用して、サーバーの使用を再開できます。

注: **ibm-slapdProxyHealthCheckOlimit** 属性を構成するときには注意が必要です。この属性は、正常性チェックに対する **olimit** を指定するために使用します。プロキシ・サーバーに重い負荷がかかる場合に **olimit** 値の設定が小さすぎると、プロキシ・サーバーはバックエンド・サーバーが応答不能であると誤って報告する可能性があります。この問題を修正するには、**olimit** の値を大きくする必要があります。ただし、**olimit** の値は、接続プール・サイズの値より少なくとも 3 は小さくする必要があります。

正常性チェック・ステータス間隔の構成

ibm-slapdStatusInterval 属性を使用して、サーバーによってスケジュールされた正常性チェックの実行の時間間隔を構成します。

この属性は動的属性ではなく、デフォルト値は 0 に設定されます。値 0 では、正常性チェックは使用不可になります。管理者は環境に合わせてこの属性の値を変更できます。

高い整合性とフェイルオーバー

整合性が高い環境では、プロキシ・サーバーはラウンドロビン読み取り操作を行いません。代わりに、プロキシ・サーバーは単一区画のすべての読み取りおよび書き込み操作を単一のバックエンド・サーバーに送信します。

アプリケーションには、高い整合性が必要となることがあります。例えば、アプリケーションであるデータを書き込んでからすぐに検索を実行して、更新が正しく行われているようにする、といった場合などです。高整合性は分割ベースごとに構成できます。

高い整合性を使用可能にするには、**ibm-slapdProxyHighConsistency** 属性を **true** に設定する必要があります。

以下のサンプル項目は、区画ベース `o=sample` を持つ分割コンテナに対して高い整合性を使用可能に指定します。

```
Sample Entry
dn: cn=o=sample split, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory,
cn=Schemas, cn=Configuration
cn: o=sample split
ibm-slapdProxyNumPartitions: 1
ibm-slapdProxyPartitionBase: o=sample
ibm-slapdProxySplitName: samplesplit
ibm-slapdEnableAutoFailBack: true
ibm-slapdProxyHighConsistency: true
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdProxyBackendSplitContainer
```

単一区画のすべての読み取りおよび書き込み操作は、単一のバックエンド・サーバーに送信されます。1 次バックエンド・サーバーがダウンすると、プロキシ・サーバーは構成されている 2 次サーバーにフェイルオーバーします。1 次サーバーが復元されるまで、すべての読み取りおよび書き込み操作はそのサーバーに送信されます。

バックエンド・サーバーの重みによる優先順位付け

プロキシ・サーバーは、バックエンド・サーバーを考えられる 5 つの層に優先順位付けします。プロキシ・サーバーが一度に使用するのは、1 つの層内のサーバーのみです。層内のすべての書き込みサーバーに障害が起こると、プロキシ・サーバーは 2 次層にフェイルオーバーします。2 次層に障害が起こると 3 次層に、というように順次フェイルオーバーします。

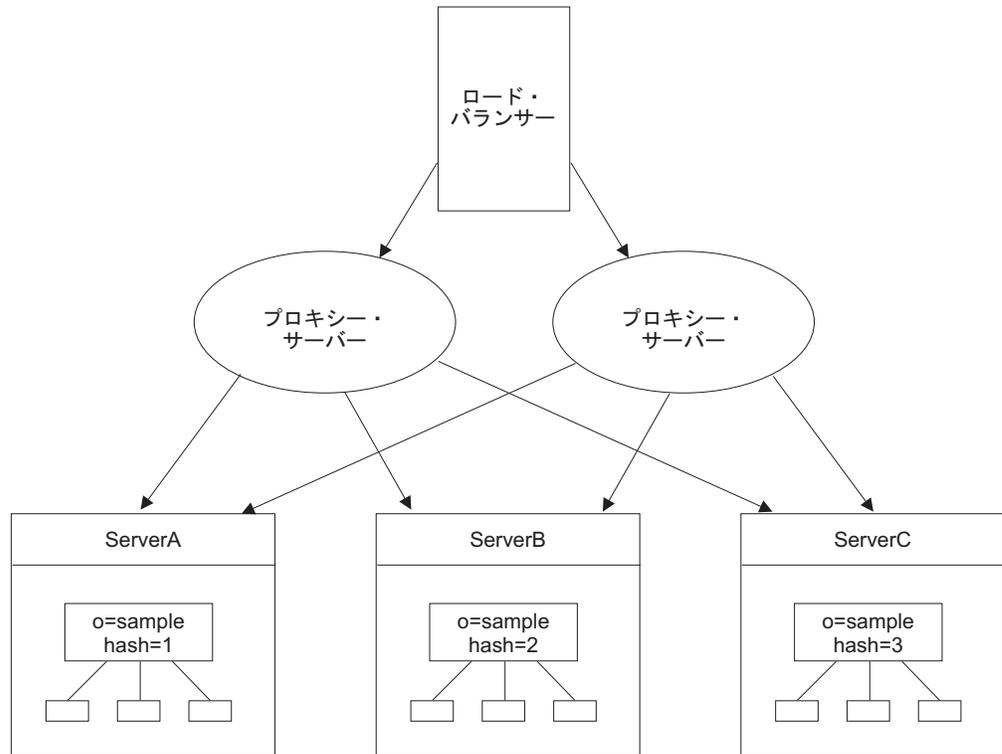
分割内の各バックエンド・サーバーに対して、重みによる優先順位を構成できます。これを行うには、`ibm-slapdProxyTier` 属性の値を設定します。この属性のデフォルト値が 1 であり、この属性が存在しない場合、プロキシはバックエンド・サーバーを層 1 のサーバーとして扱います。この属性の有効な値の範囲は 1 から 5 です。

始動時には、すべての層内のすべてのサーバーが接続されます。管理者がプロキシ・サーバーを始動する場合、層が異なる一部のバックエンド・サーバーが使用不可であっても、サーバー・グループは使用できます。サーバー・グループについての詳細は、456 ページの『サーバー・グループ』 ページを参照してください。

プロキシ・サーバー間のフェイルオーバー

最初のプロキシ・サーバーと同一の追加プロキシ・サーバーを作成することにより、プロキシ間でフェイルオーバーを行うことができます。これらのプロキシ・サーバーは、ピア・マスターとは異なりお互いの情報を所有しないため、ロード・バランサーを介して管理する必要があります。

IBM WebSphere Edge Server などのロード・バランサーは、ディレクトリーに更新を送信する際、仮想ホスト名を使用します。アプリケーションは、この仮想ホスト名を使用します。ロード・バランサーは、これらの更新を 1 つのサーバーにのみ送信するように構成されています。ネットワーク障害によりこのサーバーがダウンまたは使用不可になった場合、このサーバーが再度オンラインになり使用可能になるまで、ロード・バランサーは更新を使用可能な別のプロキシ・サーバーに送信します。ロード・バランシング・サーバーのインストール方法および構成方法については、ロード・バランサーの製品資料を参照してください。

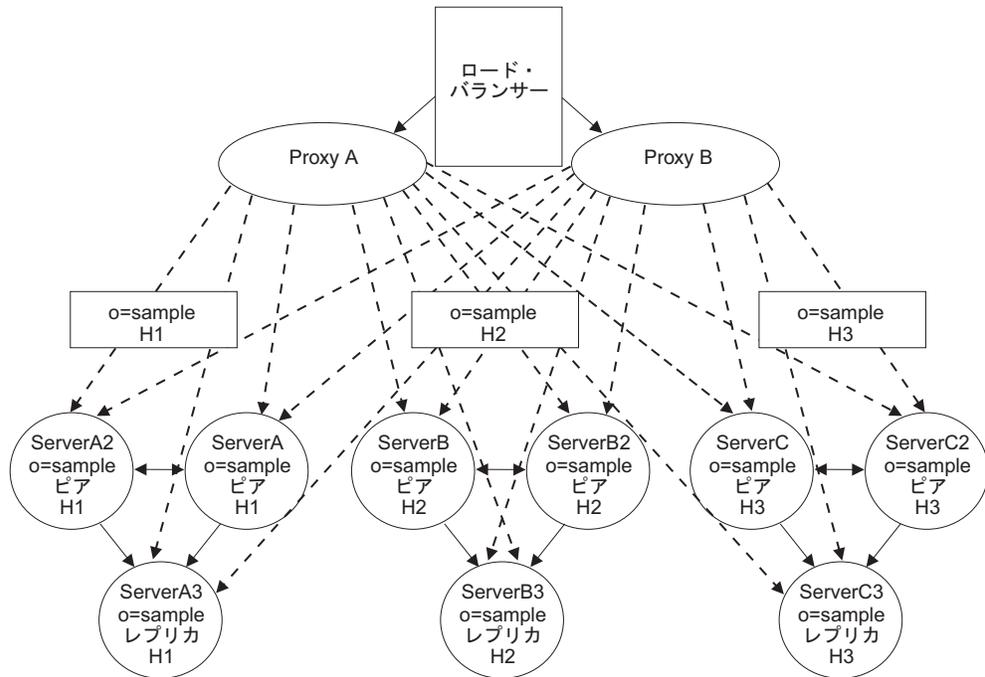


注: ロード・バランス・プロキシ環境では、プロキシ・サーバーに障害が発生すると、そのプロキシ・サーバーに送信された最初の操作は失敗し、エラーが返されます。以降のすべての操作は、フェイルオーバー・プロキシ・サーバーに送信されます。失敗した最初の操作は、再試行できます。ただし、フェイルオーバー・サーバーに自動的に送信されません。

プロキシ・サーバーを使用した分散ディレクトリーのバックアップ複製の設定

以下に示す情報と例により、プロキシ・サーバーを使用して分散ディレクトリーのバックアップ複製をセットアップする方法について詳しく説明します。

この例では、分散ディレクトリーの設定と、複製を使用したバックアップの読み取り機能、書き込み機能の構成を行います。サフィックスが `o=sample` の 3 つの区画は、対応するハッシュ値 (H1、H2、または H3) を所有します。各区画は、2 つのピア・サーバーと 1 つのレプリカで構成される複製サイトを所有し、読み取りおよび書き込みバックアップ機能を提供します。各プロキシ・サーバーは、トポロジー内のすべてのサーバーの情報を所有します (破線で示されています)。各複製サイト内のサーバー間の関係は実線で示されています。



このシナリオを作成するには、以下のことを実行します。

1. 区画するデータの LDIF ファイルを作成する必要があります。458 ページの『データ項目用の LDIF ファイルの作成』を参照してください。
2. データ・サブツリー用の複製トポロジーを作成する必要があります。458 ページの『複製トポロジーのセットアップ』を参照してください。
3. **cn=ibmpolicies** サブツリー用の別の複製トポロジーを作成する必要があります。460 ページの『グローバル・ポリシーのトポロジーの設定』を参照してください。
4. プロキシ・サーバーをセットアップします。461 ページの『プロキシ・サーバーのセットアップ』を参照してください。
5. 既存のデータを分割します。461 ページの『データの分割化』を参照してください。
6. データをロードします。461 ページの『分割したデータのロード』を参照してください。
7. 複製を開始します。465 ページの『複製の開始』を参照してください。

複製のセットアップについて詳しくは、310 ページの『レプリカ生成』を参照してください。

注: スキーマの変更は、プロキシ・サーバーでは複製されません。スキーマを更新する項目を、**cn=ibmpolicies** トポロジー内のプロキシ・サーバーおよびピア・サーバーの 1 つに作成する必要があります。

サーバー・グループ

サーバーのグループ化機能により、ユーザーは、複数のバックエンド・サーバーを互いのミラーとして定義できます。また、プロキシ・サーバーは、グループに属する 1 つ以上のバックエンド・サーバーがダウンした場合でも、少なくとも 1 つ

のバックエンド・サーバーがオンライン状態である限りは、処理を続行できます。接続が何らかの理由 (例えば、リモート・サーバーの停止または再始動など) でクローズした場合、接続は定期的に再始動されます。

プロキシ・サーバーがバックエンド・サーバーに接続できない場合、または認証が失敗した場合、プロキシ・サーバーの始動は失敗します。プロキシ・サーバーはデフォルトの場合、構成ファイルでサーバーのグループ化を定義している場合を除き、構成専用モードで始動します。

プロキシ構成ファイルは特殊な項目セットをサポートしており、ディレクトリー管理者はそれらを使用することで構成ファイルでサーバー・グループを定義できます。各グループには、バックエンド・サーバーのリストが設定されます。プロキシ・サーバーは、各グループに属する少なくとも 1 つのバックエンド・サーバーに接続できれば、正常に始動し、クライアント要求に対してサービスを提供します (ただしパフォーマンスは低下することがあります)。項目内の各バックエンド・サーバーには OR 関係が定義され、さらにすべての項目には AND 関係が定義されま

す。ディレクトリー管理者は、**idsldapadd** および **idsldapmodify** を使用して、サーバー・グループを定義したり、必要な項目を追加および変更する必要があります。またディレクトリー管理者は、各バックエンド・サーバーを適切なサーバー・グループに配置し、さらに各サーバー・グループのバックエンド・サーバーにディレクトリー・データベースの同一の区画を組み込む必要があります。例えば、**server1** と **server2** がお互いにピア関係で、**server3** と **server4** が分離したピア関係だったとします。つまり、**server1** と **server2** には、**server3** と **server4** とは異なるデータが格納されます。このケースでは、ユーザーは、**server1** と **server2** を **cn=configuration** サフィックスの下のサーバー・グループ項目に追加して、**server3** と **server4** を別のサーバー・グループ項目に追加するでしょう。**server1** と **server2** のどちらか一方が作動している場合、プロキシ・サーバーは、**server3** または **server4** がオンラインになっているかのチェックに進むことができます。**server3** と **server4** の両方がダウンしている場合、プロキシ・サーバーは構成専用モードで始動することになります。

管理者は、サーバー・グループ項目に、サーバー・グループだけでなく各バックエンド・サーバーのサーバー ID も追加する必要があります。サーバーがダウンした場合、ルート DSE 情報が取得できないため、トポロジー全体のサプライヤー/コンシューマー関係を判断するためにサーバー ID が必要になります。

サーバー・グループに属さないバックエンド・サーバーが、プロキシ・サーバーの始動時にオフラインだった場合、プロキシ・サーバーは構成専用モードで始動します。

以下の例は、ユーザー定義のサーバー・グループを示しています。

```
dn: cn=serverGroup, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory, cn=Schemas,
   cn=Configuration
cn: serverGroup
ibm-slapdProxyBackendServerDN: cn=Server1,cn=ProxyDB,cn=Proxy Backends,
   cn=IBM Directory, cn=Schemas,cn=Configuration
ibm-slapdProxyBackendServerDN: cn=Server2,cn=ProxyDB,cn=Proxy Backends,
   cn=IBM Directory, cn=Schemas,cn=Configuration
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdProxyBackendServerGroup
```

注:

1. `ibm-slappdProxyBackendServerDn` の各項目には、属性 `ibm-slappdServerId` を追加して、対応するバックエンド・サーバーの値と同一の値を指定する必要があります。
2. Web 管理ツールは、サーバーのグループ化をサポートしていません。分散構成でこれらの項目を同期させたり訂正するのは管理者の責任です。これらの項目の保守には、LDAP プロトコルを使用する必要があります。

データ項目用の LDIF ファイルの作成

以下に示すコマンドを発行することで、データ項目用の LDIF ファイルを作成することができます。

このタスクについて

現在サーバーにある、サブツリー `o=sample` のデータ項目用の LDIF ファイル (`mydata.ldif`) を作成するには、以下の手順を実行します。

- 以下のコマンドを発行します。

```
idsdb2ldif-o mydata.ldif -s o=sample-I <instance_name>  
-k <key seed> -t <key salt>
```

注: 複数のインスタンスが存在する場合、`-I` オプションを使用する必要があります。サーバーの鍵を同期化していない場合は、`-k` および `-t` オプションを使用する必要があります。

重要:

- Advanced Encryption Standard (AES) が使用可能になっているサーバーにインポートするデータをエクスポートする場合で、2 つのサーバーが暗号同期化されていない場合は、サーバーの暗号同期化について、703 ページの『付録 J. サーバー・インスタンス間の両方向の暗号化の同期』を参照してください。
- 分散ディレクトリー環境のすべてのバックエンド・サーバーが SHA-2 アルゴリズム・ファミリー (SHA-224, SHA-256, SHA-384, SHA-512)、または salted バージョンの SHA-2 アルゴリズム・ファミリー (SSHA-224, SSHA-256, SSHA-384, SSHA-512) 用に構成されていない場合は、これらのアルゴリズム・ファミリーを使用して暗号化したデータをプロキシ・サーバーを介して追加してはなりません。なぜなら、これらのアルゴリズム・ファミリー用に構成されていないバックエンド・サーバーに、これらのアルゴリズム・ファミリーを使用して暗号化したデータを追加すると、サーバーは、データが平文形式であると想定するので、データが破損する可能性があります。

詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の `idsdb2ldif` コマンド情報を参照してください。

複製トポロジーのセットアップ

以下に示す情報を使用して、複製トポロジーを実行する方法を説明します。

このタスクについて

このシナリオを作成する前に、複製の概念と用語をよく理解しておく必要があります。複製の概念を理解していない場合は、310ページの『レプリカ生成』を参照してください。

Web 管理ツールを使用して作成するこのトポロジーでは、各区画は個別の複製サイトとして扱われます。ただし、このトポロジーにゲートウェイ・サーバーは存在しません。これは、分割したデータを他の区画に複製する利点がないからです。

注: ここからはトポロジーを作成します。項目データはロードしないでください。

1. ServerA にログオンしていない場合はログオンし、サブツリー o=sample を追加します。これを行うことで ServerA を o=sample のマスター・サーバーにします。394ページの『サブツリーの追加』を参照してください。
2. トポロジーの資格情報セットを作成します。397ページの『資格情報の追加』を参照してください。
3. ピア・マスター・サーバーとして ServerA2 を追加します。402ページの『ピア・マスターまたはゲートウェイ・サーバーの追加』を参照してください。
4. レプリカとして ServerA3 を追加します。ServerA2 とのサプライヤー合意が選択されていることを確認してください。405ページの『レプリカ・サーバーの追加』を参照してください。

注: ServerB と ServerC のどちらか一方にログオンして、ServerA で作成したのと同様のトポロジーを作成することも、ServerA からトポロジーの作成を引き続き行うこともできます。ServerA から引き続きトポロジーの追加を行う場合、Web 管理ツールが合意を作成しようとしませんが、トポロジーに不適切な合意は選択解除してください。例えば、"A" グループのサーバーと、"B" または "C" グループのサーバー間に合意を持つことはできません。同様に、"B" グループのサーバーと、"C" または "A" グループのサーバー間にも、合意を持つことはできません。

5. サブツリー o=sample のマスター・サーバーとして ServerB を追加します。402ページの『ピア・マスターまたはゲートウェイ・サーバーの追加』を参照してください。ServerA、Server A2、および ServerA3 との合意は必ず選択解除してください。
6. Server B のピア・マスター・サーバーとして ServerB2 を追加します。402ページの『ピア・マスターまたはゲートウェイ・サーバーの追加』を参照してください。ServerA、Server A2、および ServerA3 との合意は必ず選択解除してください。
7. レプリカとして ServerB3 を追加します。ServerA および ServerA2 とのサプライヤー合意が選択されている場合は、選択解除してください。405ページの『レプリカ・サーバーの追加』を参照してください。
8. サブツリー o=sample のマスター・サーバーとして ServerC を追加します。402ページの『ピア・マスターまたはゲートウェイ・サーバーの追加』を参照してください。ServerA、Server A2、ServerA3、ServerB、ServerB2、および ServerB3 との合意は必ず選択解除してください。
9. Server C のピア・マスター・サーバーとして ServerC2 を追加します。402ページの『ピア・マスターまたはゲートウェイ・サーバーの追加』を参照してく

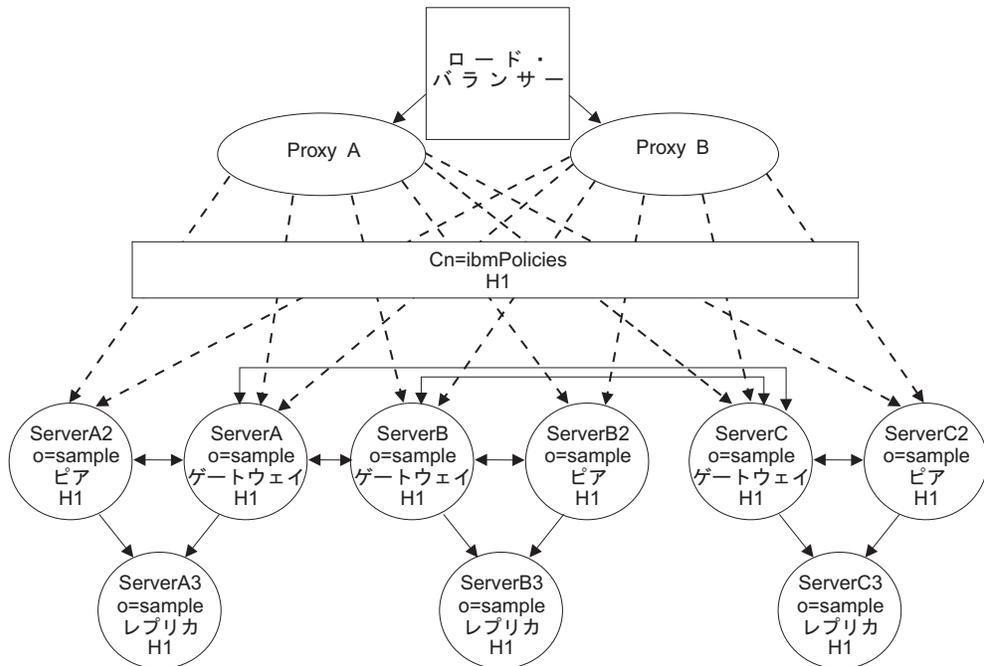
ださい。ServerA、Server A2、ServerA3、ServerB、ServerB2、および ServerB3 との合意は必ず選択解除してください。

- レプリカとして ServerC3 を追加します。ServerA、ServerA2、ServerB、および ServerB2 とのサプライヤー合意は選択解除してください。405 ページの『レプリカ・サーバーの追加』を参照してください。

複製のセットアップについて詳しくは、310 ページの『レプリカ生成』を参照してください。

グローバル・ポリシーのトポロジーの設定

グローバル・ポリシーの更新を複製するためには、**cn=ibmPolicies** サブツリー用の 2 番目のトポロジーを設定する必要があります。例えば、o=sample 用に作成した同一のトポロジー設定を使用して、ServerA、ServerB、および ServerC をゲートウェイ・サーバーにすることが可能です。



このトポロジーでは、いずれか 1 つのサーバーに対する更新により、すべてのサーバーが更新されます。

複製サイト間で適切な合意を作成する必要があります。この種類のトポロジーの設定方法については、370 ページの『ゲートウェイ・トポロジーのセットアップ』および 410 ページの『ゲートウェイ・サーバーの管理』を参照してください。

データ・サブツリー用に設定した同じトポロジー・モデルを使用する必要はありません。サーバー A、A2、B、B2、C、および C2 をすべてピア・サーバーにし、それらのサーバーとレプリカ・サーバー A3、B3、および C3 との間で合意を結び、といったトポロジーを作成することも可能です。唯一の要件は、データ・サブツリー・トポロジー内のすべてのサーバーが、**cn=ibmpolicies** サブツリー・トポロジーに含まれていることです。

プロキシ・サーバーのセットアップ

以下に説明する手順に従うことにより、プロキシ・サーバーをセットアップできます。

手順

1. プロキシ・サーバー Proxy A をセットアップします。438 ページの『プロキシ・サーバーのセットアップ』の指示に従って、プロキシ・サーバーをセットアップします。ServerB および ServerC に対してステップを繰り返すよう指示された場合、そのステップは ServerA2、ServerA3、ServerB2、ServerB3、ServerC2、および ServerC3 に対しても実行する必要がある、ということを留意してください。**注:** バックエンド・サーバーに区画値を割り当てる場合は、必ず正確な区画値を割り当ててください。

サーバー名	区画索引値
ServerA	1
ServerA2	1
ServerA3	1
ServerB	2
ServerB2	2
ServerB3	2
ServerC	3
ServerC2	3
ServerC3	3

2. 2 番目のプロキシ・サーバー、Proxy B を、Proxy A を設定した場合と同じ方法で設定します。
3. IBM WebSphere Edge Server などのロード・バランサーを追加します。

データの分割化

ここに示すコマンドを発行することにより、サブツリー o=sample 用に作成した mydata.ldif ファイル内に含まれるデータを分割できます。

このタスクについて

```
ddsetup -I ProxyA -B "o=sample" -i mydata.ldif
```

ここで、
ProxyA:Is the proxy server instance

分割したデータのロード

データの容量に従い **idsldif2db** または **idsbulkload** を使用して、データを適切なバックエンド・サーバーにロードします。データを複製するよりも、該当する LDIF ファイルを各サーバーにロードする方が効率的な場合があります。

区画索引値が正しく対応するサーバーに対し、正しい LDIF 出力をロードする必要があります。これを行わないと、プロキシ・サーバーは項目を取得できません。

- ServerA (区画索引 1) - ServerA.ldif
- ServerA2 (区画索引 1) - ServerA.ldif
- ServerA3 (区画索引 1) - ServerA.ldif

- ServerB (区画索引 2) - ServerB.ldif
- ServerB2 (区画索引 2) - ServerB.ldif
- ServerB3 (区画索引 2) - ServerB.ldif
- ServerC (区画索引 3) - ServerC.ldif
- ServerC2 (区画索引 3) - ServerC.ldif
- ServerC3 (区画索引 3) - ServerC.ldif

モニター検索

モニター検索は、ステータスの照会をアクティブには行いませんが、現在のステータスを簡単に報告し、それをプロキシ・サーバーが使用できます。バックエンド・サーバーがダウンし、そのことをプロキシ・サーバーがまだディスカバーしていない場合、検索結果では報告されません。

管理者はモニター検索を使用して、プロキシ・サーバーの現在のステータスを判別できます。**cn=partitions, cn=proxy, cn=monitor** のモニター検索では、分割ポイント、区画、各区画内のサーバーごとに 1 つの項目が返されます。

注:

- プロキシ・サーバーの **cn=monitor** 検索では、実際に操作が完了する前に、完了と表示されます。実際に完了した操作を検出するために操作カウントが必要な場合は、**cn=proxy, cn=monitor** 検索を使用する必要があります。
- プロキシ・サーバー環境では、クライアントからの単一要求を、プロキシ・サーバー環境内のさまざまな種類の複数の要求にマップできます。例えば、あるバインドを、比較、検索および一連の拡張操作にマップして、グループ・メンバーシップを評価できます。

検索ベース **cn=partitions, cn=proxy, cn=monitor** のモニター検索の例は以下のとおりです。

```
idsldapsearch -D <adminDN> -w <adminpw> -h <servername> -p <portnumber>
-b cn=partitions,cn=proxy,cn=monitor -s base objectclass=*
```

このコマンドは、以下の情報を戻します。

```
Split Point Entry:
ibm-slapdProxySplitName= <configured name>, cn=partitions, cn=proxy, cn=monitor
ibm-slapdProxyPartitionBase= <configured base>
ibm-slapdProxyHighConsistencyEnabled = <true|false>
ibm-slapdProxyCurrentTier = <tier number> the current tier that the proxy
server uses to process operations.

Partition Entry:
ibm-slapdProxyPartitionIndex= <index value>,ibm-slapdProxySplitName= <configured name>,
cn=partitions,cn=proxy, cn=monitor
ibm-slapdProxyPartitionStatus : (active, readonly, unavailable)
ibm-slapdProxyPartitionIndex= <index value>

Server Entry:
ibm-slapdPort= <port> + ibm-slapdProxyBackendServerName= <server URL>,
ibm-slapdProxyPartitionIndex= <index value> ibm-slapdProxySplitName= <configured name>,
cn=partitions, cn=proxy, cn=monitor
ibm-slapdServerStatus: (active, unavailable)
ibm-slapdProxyCurrentServerRole: (primarywriteserver, readonlyserver, writeserver, notactive)
ibm-slapdProxyConfiguredRole: (primarywriteserver, readonlyserver, writeserver)
ibm-slapdProxyNumberOfActiveConnections: <connection count>
```

ここで、

- **ibm-slapdProxyPartitionStatus:**
 - active: 1 つ以上の書き込みサーバーがアクティブである。

- readonly: 書き込みサーバーは 1 つもアクティブではないが、1 つ以上の読み取りサーバーはアクティブである。
- unavailable: 区画内のどのサーバーもアクティブではない。
- **ibm-slapdServerStatus:**
 - active: サーバーが始動していて、プロキシ・サーバーがサーバーへの接続を確立している。
 - unavailable: サーバーが構成モードで始動しているか、プロキシ・サーバーが適切な権限を使用してサーバーへの接続を確立できない。
- **ibm-slapdProxyCurrentRole:**
 - primarywriteserver: サーバーがアクティブで、すべての書き込み要求を受け取っている。高い整合性が使用可能な場合、サーバーはすべての読み取り要求も受け取っている。
 - readonlyserver: サーバーがアクティブで、読み取り専用要求用に使用可能である。サーバーが使用されるのは、高い整合性が使用不可であるか、すべての書き込みサーバーがダウンしている場合のみです。
 - writeserver: サーバーがアクティブで、使用可能である。高い整合性が使用可能な場合、このサーバーはフェイルオーバーが発生するまで使用されません。高い整合性が使用不可の場合、このサーバーはフェイルオーバー状態までは読み取りサーバーとして使用されます。
 - notactive: サーバーがこの区画内で現在使用されていない。これは、サーバーにアクセスできないか、サーバーは始動しているがこの区画に復元されていない、のいずれかを意味します。
- **ibm-slapdProxyConfiguredRole:** サーバーに構成された役割。役割が具体的に構成されていない場合、この値は、プロキシ・サーバー独自の始動時のディスカバリー・アルゴリズムに基づいて設定されます。
- **ibm-slapdProxyNumberofActiveConnections:** バックエンド・サーバーに対して開かれている接続の実際の数。

注: 接続が保護されている場合、**ibm-slapdPort** 属性の代わりに **ibm-slapdSecurePort** 属性が使用されます。

cn=proxy,cn=monitor のモニター検索では、プロキシ・バックエンドによって要求および完了された各操作のカウンターが提供されます。この検索でサポートされているフィルターは **objectclass=*** です。プロキシ・サーバーに構成されているすべてのバックエンド・サーバーに関連するカウンターは、モニター検索の出力として提供されます。プロキシ・バックエンドのモニター検索で返されるカウンターは以下のとおりです。

- **ops_requested** - プロキシ・バックエンドによって要求された操作の数。
- **ops_completed** - プロキシ・バックエンドによって完了された操作の数。
- **search_requested** - プロキシ・バックエンドによって要求された検索操作の数。
- **search_completed** - プロキシ・バックエンドによって完了された検索操作の数。
- **binds_requested** - プロキシ・バックエンドによって要求されたバインド操作の数。
- **binds_completed** - プロキシ・バックエンドによって完了されたバインド操作の数。

- unbinds_requested - プロキシー・バックエンドによって要求されたアンバインド操作の数。
- unbinds_completed - プロキシー・バックエンドによって完了されたアンバインド操作の数。
- adds_requested - プロキシー・バックエンドによって要求された追加操作の数。
- adds_completed - プロキシー・バックエンドによって完了された追加操作の数。
- deletes_requested - プロキシー・バックエンドによって要求された削除操作の数。
- deletes_completed - プロキシー・バックエンドによって完了された削除操作の数。
- modrdns_requested - プロキシー・バックエンドによって要求された modrdn 操作の数。
- modrdns_completed - プロキシー・バックエンドによって完了された modrdn 操作の数。
- modifies_requested - プロキシー・バックエンドによって要求された変更操作の数。
- modifies_completed - プロキシー・バックエンドによって完了された変更操作の数。
- compares_requested - プロキシー・バックエンドによって要求された比較操作の数。
- compares_completed - プロキシー・バックエンドによって完了された比較操作の数。
- abandons_requested - プロキシー・バックエンドによって要求された中止操作の数。
- abandons_completed - プロキシー・バックエンドによって完了された中止操作の数。
- extops_requested - プロキシー・バックエンドによって要求された拡張操作の数。
- extops_completed - プロキシー・バックエンドによって完了された拡張操作の数。
- unknownops_requested - プロキシー・バックエンドによって要求された不明操作の数。
- unknownops_completed - プロキシー・バックエンドによって完了された不明操作の数。
- total_connections - プロキシー・サーバー用に構成されたプロキシー・バックエンド・サーバーとバックエンド・サーバーとの間の使用中の接続の数。
- total_ssl_connections - プロキシー・サーバー用に構成されたプロキシー・バックエンド・サーバーとバックエンド・サーバーとの間の SSL 接続の数。
- used_connections - プロキシー・サーバー用に構成されたプロキシー・バックエンド・サーバーとバックエンド・サーバーとの間の使用中の接続の数。
- used_ssl_connections - プロキシー・サーバー用に構成されたプロキシー・バックエンド・サーバーとバックエンド・サーバーとの間の使用中の SSL 接続の数。
- total_result_sent - プロキシー・サーバーの始動後にプロキシー・バックエンドによってクライアントに送信された結果の数。
- total_entries_sent - プロキシー・サーバーの始動後にプロキシー・バックエンドによってクライアントに送信された項目の数。

- `total_success_result_sent` - プロキシ・サーバーの始動後にプロキシ・バックエンドによってクライアントに送信されて成功した結果の数。
- `total_failed_result_sent` - プロキシ・サーバーの始動後にプロキシ・バックエンドによってクライアントに送信されて失敗した結果の数。
- `total_references_sent` - プロキシ・サーバーの始動後にプロキシ・バックエンドによってクライアントに送信された参照の数 (参照に関連)。
- `transactions_requested` - プロキシ・バックエンドによって要求されたトランザクション操作の数。
- `transactions_completed` - プロキシ・バックエンドによって完了されたトランザクション操作の数。
- `transaction_prepare_requested` - プロキシ・バックエンドによって要求されたトランザクション準備操作の数。
- `transaction_prepare_completed` - プロキシ・バックエンドによって完了されたトランザクション準備操作の数。
- `transaction_commit_requested` - プロキシ・バックエンドによって要求されたトランザクションのコミット操作の数。
- `transaction_committed` - プロキシ・バックエンドによって完了されたトランザクションのコミット操作の数。
- `transaction_rollback_requested` - プロキシ・バックエンドによって要求されたトランザクションのロールバック操作の数。
- `transaction_rollbacked` - プロキシ・バックエンドによって完了されたトランザクションのロールバック操作の数。

プロキシ・サーバーでのトランザクション

トランザクションにより、アプリケーションは一連の項目更新をグループ化できます。プロキシ・サーバーは、すべての操作が単一のバックエンド・サーバーをターゲットとする同時トランザクション要求を処理できます。

プロキシ・サーバーはバックエンド・サーバーのトランザクション機能を使用して、トランザクション要求を完了します。プロキシ・サーバーでトランザクションが使用可能になるのは、それらのトランザクションがバックエンド・サーバーで使用可能な場合のみです。バックエンド・サーバーでトランザクションが使用可能な場合、始動時にメッセージがログに記録されます。また、トランザクション準備拡張操作が使用可能になるのは、それがバックエンド・サーバーで使用可能な場合のみです。バックエンド・サーバーでトランザクションの準備要求がサポートされない場合、始動時にメッセージがログに記録されます。

最良の結果を得るため、プロキシ・サーバーで構成するトランザクションの最大数は、1 以上で、各バックエンド・サーバーで使用可能な接続数より少ない数にする必要があります。例えば、接続プール値が 10 に設定されている場合、トランザクションの最大数は 9 以下に設定します。また、バックエンド・サーバーのタイムアウト値が小さい場合、プロキシ・サーバーのトランザクションはより小さいトランザクション・タイムアウト値でロールバックされます。

複製の開始

以下に示す情報とリンクを使用して、複製を開始できます。

複製が自動的に開始されない場合、サブツリーを静止解除して各サーバーのキューを再始動する必要があります。これらのタスクの実行方法については、396 ページの『サブツリーの静止』 および 419 ページの『キューの管理』を参照してください。

ディレクトリー・サーバーをバックアップおよびリストアする

この機能により、ディレクトリー・サーバーをバックアップおよび復元することができます。

Security Directory Server では、ディレクトリー・サーバー・インスタンス情報のバックアップ/リストア方式があります。ディレクトリー・サーバー・インスタンスの情報を完全にバックアップする方法と、データベース内のデータのみをバックアップする方法があります。バックアップおよび復元の方式を選択するときには、『ディレクトリー・サーバー・インスタンス情報全体のバックアップ』および 468 ページの『データベース情報のみのバックアップ』の情報を参照してください。

ディレクトリー・サーバー・インスタンス情報全体のバックアップ

この機能により、ディレクトリー・サーバー・インスタンス情報全体をバックアップおよび復元することができます。

Security Directory Server には、ディレクトリー・サーバー・インスタンス情報全体をバックアップおよび復元するメカニズムが 2 つ用意されています。

- 基本
- 拡張

この 2 つのメカニズムでは、ディレクトリー・サーバー・インスタンス・データ (DB2 データベースに格納されているデータ) に加え、ディレクトリー・サーバー・インスタンスの関連構成ファイルおよびスキーマ・ファイルもバックアップできます。

基本方式についての情報は、IBM Security Directory Server の資料の『インストールと構成』のセクションにあります。『すべての設定を指定する新規インスタンスの作成』および『ディレクトリー・サーバー・インスタンスのバックアップ』のセクションを参照してください。また、基本方式についての情報は、IBM Security Directory Server の資料の『コマンド解説書』セクションにもあります。idsdbback コマンドおよび idsdbrestore コマンドに関する情報を参照してください。

拡張方式についての情報は、このセクションおよび「*IBM Security Directory Server Version 6.3 Command Reference*」に含まれています (ldapexop ユーティリティおよび拡張操作オプション **-op backuprestore** に関する情報を参照してください)。

どちらの方式にも、以下を実行するためのオプションがあります。

- オンライン・バックアップ: オンライン・バックアップはサーバーの実行中にも停止中にも実行できます。
- オフライン・バックアップ: オフライン・バックアップは、サーバーの停止中に実行する必要があります。

バックアップは、常にそのバックアップが取られたサーバーに保管されます。ただし、ユーザーがバックアップを要求できる場所および方法はさまざまです。

2 つの方式のどちらでも、バックアップで以下のファイルは対象にならないため、個別にバックアップする必要があります。

- idsinstances.ldif
- SSL 関連ファイル: 鍵、鍵 stash ファイル、 CRL ファイル
- Security Directory Integrator ソリューション・ファイル

これらの方式について詳しく確認したら、いずれか 1 つの方式を選択してその方式のみを使用します。2 つの方式を混用しないでください。

以下の表に、2 つの方式の比較を示します。

表 39. バックアップおよび復元の基本方式および拡張方式の比較

フィーチャー	基本方式	拡張方式
要求元	ローカル・サーバー	リモート・サーバーおよびローカル・サーバー
使用するインターフェース	インスタンス管理ツールまたは idsdbback および idsdbrestore コマンド	Web 管理ツールまたは ldapexop ユーティリティ
バックアップ・ロケーション	その都度異なるロケーションで実行できます。そのため、前のバックアップが上書きされるのは、前のバックアップと同じロケーションでバックアップを実行する場合のみです	このメカニズムで要求されるすべてのバックアップに使用される、バックアップ・ロケーションおよびバックアップ方式を構成する方法が提供されます
1 つまたは複数のバックアップの保管	複数のバックアップ	一度に 1 つのバックアップのみが保管され、新規バックアップが正常に実行されると、前のバックアップは上書きされます。
復元	管理者はディスク上の任意のバックアップ・ロケーションから選択できます。	実行された最新のバックアップからの復元のみが許可されます。
スケジューリング	バックアップ時に指定した特定のロケーションにバックアップまたは復元を行う一回限りの要求	一回限り、日次、または週次のバックアップをスケジュールするためのオプションがあります
オンラインまたはオフライン	オンライン・バックアップもオフライン・バックアップも実行できます。	オンライン・バックアップもオフライン・バックアップも実行できます。
ディレクトリー・サーバー・データおよび関連する構成ファイルとスキーマ・ファイルのバックアップ	構成ファイルのみをバックアップするためのオプションがあります。	データおよび関連する構成ファイルとスキーマ・ファイルをバックアップします。
管理者による管理	必要な管理作業が多い。管理者はディスク・スペースの管理を改善する必要があります。	必要な管理作業が少ない。1 つのバックアップ・ロケーションのみを管理します。
DB2 パラメーターのバックアップおよび復元	DB2 構成パラメーターおよびデータベース最適化パラメーターのバックアップおよび復元	DB2 構成パラメーターおよびデータベース最適化パラメーターのバックアップおよび復元

データベース情報のみのバックアップ

この機能により、データベース情報のみをバックアップおよび復元することができます。

Security Directory Server の完全バックアップ/リストア・メカニズムの代わりに、DB2 データベースに格納されているディレクトリー・サーバー・インスタンス・データのみをバックアップおよびリストアする方式が 2 つあります。これらのバックアップ方式では、DB2 データがバックアップされますが、スキーマなどの Security Directory Server 固有の構成はバックアップされません。1 つの方式では、DB2 構成も保存されます。この 2 つの方式について以下で説明します。

- Security Directory Server LDAP LDIF のエクスポートおよびインポート・コマンド、idsdb2ldif および idsldif2db を使用して、データを LDIF ファイルにエクスポートし、それを LDIF ファイルから復元できます。構成ツールの使用については IBM Security Directory Server の資料の『インストールと構成』セクションの『構成ツールの使用による LDIF データのインポート』セクションを、コマンドについては IBM Security Directory Server の資料の『コマンド解説書』セクションを参照してください。これらのコマンドでは、DB2 構成は保存されません。これらのコマンドは異種ハードウェア・プラットフォーム間で機能しますが、処理時間が比較的長くかかります。
- DB2 のバックアップ/リストア・コマンドを使用してデータをバックアップおよびリストアできます。この方式では、DB2 構成が保存されます。また、処理時間が短いです。この方式は、一部の異種ハードウェアおよびプラットフォーム間で機能します。これは DB2 でのハードウェアまたはプラットフォームのサポートに基づきます。詳細については、717 ページの『付録 M. IBM Security Directory Server のバックアップおよび復元』を参照してください。

最良の結果を得るため、対処するべき特別な事情 (異なるハードウェア・プラットフォームをまたいだデータのバックアップや復元など) がない限り、466 ページの『ディレクトリー・サーバー・インスタンス情報全体のバックアップ』に説明されている基本方式か拡張方式のいずれかを使用してください。

拡張バックアップ

拡張バックアップ方式を使用すると、ディレクトリー・サーバー・インスタンス・データと、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構成ファイルおよびスキーマ・ファイルをバックアップできます。

拡張バックアップ方式には、オンラインとオフラインの両方のバックアップを実行するオプションがあります。

注:

- オンライン・バックアップ構成は、初期のデータベース構成時に行うことも、データベース・バックアップ・ツールから行うこともできます。
- オンライン・バックアップがサーバーの構成ファイル内に構成されており、管理者がバックアップ・ロケーション・パスを変更する場合は、変更が続いて最初のバックアップを行うため、サーバーを停止してください。後続のバックアップでは、サーバーがオンライン状態で実行できます。

- オンライン・バックアップ用に構成されたサーバーでは、循環バックアップをスケジューリングすることが重要です。そうしないと、ログがファイル・システムに対して大きくなりすぎます。
- オンライン・バックアップ構成の削除は、データベース構成ツールを使用することで可能です。
- バックアップされたデータベースおよびサーバー・ファイルは、バックアップが成功するたびに置き換えられます。ただし、バックアップ操作が失敗した場合、前のバックアップはまだ使用可能です。
- プロキシ・サーバーは、基本方式を使用してバックアップする必要があります。詳細については、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。
- 必要な場合は、変更ログ・データをバックアップできます。
- 複数のパスにバックアップまたは復元するには、インスタンス管理ツールを使用する必要があります。詳細については、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。
- すべてのバックアップ操作において、管理サーバーが実行されていることを確認してください。

バックアップおよび復元用にディレクトリー・サーバーを構成するには、以下のいずれかの方法を使用します。

Web 管理の使用

Web 管理ツールを使用することで、ディレクトリー・サーバー・インスタンス・データと、それに関連する構成ファイルおよびスキーマ・ファイルをバックアップおよび復元することができます。

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「バックアップ/復元の管理」をクリックします。「バックアップ/復元の管理」パネルで、「バックアップ/復元ステータス」タブはデフォルトで選択されています。

「バックアップ/復元ステータス」タブには、以下の情報が表示されます。

バックアップ有効

ディレクトリー・サーバー・インスタンス用にバックアップが有効になっているかどうかを示します。このフィールドの値は、true または false です。**backupenabled** 属性は、このフィールドに関連付けられています。

有効な変更ログのバックアップ

変更ログのバックアップが構成されているかどうかを示します。このフィールドの値は、true または false です。**backupchange log** 属性は、このフィールドに関連付けられています。

バックアップ・タイプ

ディレクトリー・サーバー・インスタンスでオンライン・バックアップまたはオフライン・バックアップを構成するかどうかを指定します。バックアップ・タイプがオンラインの場合、このフィールドの値は ONLINE です。バックアップ・タイプがオフラインの場合、このフィールドの値は OFFLINE です。

バックアップ頻度

ディレクトリー・サーバー・インスタンスで実行されるバックアップの頻度を指定します。このフィールドの値は、「**directory server のバックアップのスケジュール**」タブでユーザーが構成したスケジュールのタイプに応じて、「1 回」、「日次」、「週次」、または「1 回と繰り返し」になります。ユーザーがオプションを何も選択しない場合は、フィールドに「なし」と表示されます。

バックアップ・ステータス

バックアップのステータスを示します。バックアップのステータスは以下のオプションのいずれかです。

- スケジュール済み
- 未スケジュール
- バックアップ進行中

backupstatus 属性は、このフィールドに関連付けられています。

前の正常バックアップ

最終正常バックアップが実行された日時を YYYY-MM-DD-hh:mm 形式で示します。ディレクトリー・サーバー・インスタンスのバックアップを一度も実行していない場合は、**none** と表示されます。**backuplastdone** 属性は、このフィールドに関連付けられています。

前のバックアップ・ロケーション

最後のバックアップが実行されたときの構成済みパスを指定します。ディレクトリー・サーバー・インスタンスのバックアップが構成されていない場合は、このフィールドに **none** と表示されます。

次のスケジュール済みバックアップ

次のバックアップのスケジュールされた日時を YYYY-MM-DD-hh:mm 形式で示します。ディレクトリー・サーバー・インスタンスのバックアップが構成されていない場合は、このフィールドに **none** と表示されます。

backupnextscheduled 属性は、このフィールドに関連付けられています。

次のバックアップ・ロケーション

次のバックアップが実行されるロケーションを指定します。ディレクトリー・サーバー・インスタンスのバックアップが構成されていない場合は、このフィールドに **none** と表示されます。

復元ステータス

現在の復元ステータスを示します。復元ステータスは以下のオプションのいずれかです。

- 復元進行中
- 復元完了 yyyy-MM-dd-hh:mm
- なし

restorestatus 属性は、このフィールドに関連付けられています。

「再表示」をクリックすると、このパネルの情報を更新できます。

directory server のバックアップの構成

ここで説明する手順に従うことにより、Web 管理ツールを使用して、ディレクトリー・サーバーのバックアップを構成することができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「バックアップ/復元の管理」をクリックします。「directory server のバックアップの構成」タブをクリックします。

注: ディレクトリー・サーバーが稼働していない場合で、Web 管理ツールが管理サーバーに接続している場合は、「管理サーバーに接続しました。一部の値は使用できません。」などのメッセージが表示されます。

このタブで、以下のアクションを実行できます。

- ディレクトリー・サーバーのバックアップを有効または無効にする
- 変更ログのバックアップを有効または無効にする
- バックアップ・タイプを設定する
- バックアップおよび復元用のパスを設定する

ディレクトリー・サーバー・バックアップは、以下のユーザーが構成できます。

- プライマリー・ディレクトリー管理者
- DirDataAdmin、ServerStartStopAdmin、ServerConfigGroupMember、および SchemaAdmin のすべての役割を持つローカル管理グループ・メンバー

Directory Server インスタンスのバックアップおよび復元の設定を構成するには、以下のステップを行います。

1. 「directory server のバックアップを有効にする」チェック・ボックスを選択して、選択したディレクトリー・サーバー・インスタンスのバックアップを有効にします。
2. 「変更ログのバックアップを有効にする」チェック・ボックスを選択して、変更ログ・データベースのバックアップを有効にします。**注:** このチェック・ボックスは、そのディレクトリー・サーバー・インスタンスで変更ログが構成されている場合にのみ有効になります。
3. バックアップ・タイプを指定するには、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」をクリックして、ディレクトリー・サーバー・インスタンスのオンライン・バックアップを有効にします。
 - 「オフライン・バックアップ」をクリックして、ディレクトリー・サーバー・インスタンスのオフライン・バックアップを有効にします。

注: オンライン・バックアップはサーバーの実行中または停止中に実行できるのに対し、オフライン・バックアップはサーバーの停止中に実行する必要があります。

4. 「バックアップ/復元ロケーション」フィールドで、バックアップおよび復元操作に必要なパスを指定します。コンピューターに指定されたロケーションが存在しない場合は、そのパスが作成されます。**注:**

- インスタンス所有者は、指定したバックアップ・ロケーションに対する書き込み許可を持っている必要があります。
 - ディレクトリー・サーバー・バックアップのパスを指定する場合は、指定したパスにディレクトリー・バックアップ 2 つ分の十分なスペースがあることを確認する必要があります。これは、現在のバックアップが正常に完了するまで前のバックアップが保存されるためです。オンライン・バックアップがスケジュールされている場合、最大 1 週間分の非アクティブ・アーカイブ・ログ・ファイル用の十分なスペースがあることを確認する必要があります。オンライン・バックアップがスケジュールされていない場合、ディレクトリー管理者は、非アクティブ・ログによって使用されるスペースをモニターし、定期的にそれらのログを除去する必要があります。
5. 完了したら、以下のステップのいずれかを行います。
- 「OK」をクリックして変更内容を適用し、このパネルを終了します。
 - 「適用」をクリックして変更内容を適用し、このパネルを表示させたままにします。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

directory server のバックアップの実行

ここで提供する情報により、ディレクトリー・サーバーのバックアップの実行方法について詳しく学ぶことができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「バックアップ/復元の管理」をクリックします。「directory server のバックアップの実行」タブをクリックします。

このタブは、サーバーが以下の結果を返す場合にのみ表示されます。

- ルート DSE 検索時でサーバー機能 OID 1.3.18.0.2.32.87 が返される場合。これは、サーバーがバックアップおよび復元構成項目を構成可能であることを示します。
- ルート DSE 検索で管理サーバーの supportedextension に ServerBackupRestore LDAP 拡張操作 OID 1.3.18.0.2.12.81 が返される場合。

管理サーバーは `idsdbback` コマンドを使用して、バックアップ要求を処理します。`idsdbback` コマンドを使用して、ディレクトリー・サーバー・インスタンスのデータおよび構成ファイルのバックアップが実行されます。ディレクトリー・サーバー・インスタンスのバックアップを初めて実行する場合は、バックアップを実行する前にディレクトリー・サーバー・インスタンスを停止する必要があります。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ない場合に、初めてオンライン・バックアップを行うには、ディレクトリー・サーバーを停止する必要があります。これは、オンライン・バックアップでは、データベース構成の変更を行う必要があるためです。初期バックアップ後、ディレクトリー・サーバー・インスタンスの状態は、オンライン・バックアップの実行時は、実行中でも停止でも構いません。ただし、オフライン・バックアップの場合、ディレクトリー・サーバー・インスタンスを停止する必要があります。Web 管理ツールの指示に従ってサーバーを停止してください。

バックアップ操作を実行できるユーザーは、以下のとおりです。

- プライマリー・ディレクトリー管理者
- DirDataAdmin、ServerStartStopAdmin、ServerConfigGroupMember、および SchemaAdmin のすべての役割を持つローカル管理グループ・メンバー

その他のユーザーに対しては、「**directory server のバックアップの実行**」タブは表示されません。

「directory server のバックアップの実行」タブには、以下の情報が表示されます。

バックアップ・タイプ

ディレクトリー・サーバー・インスタンス用に構成されたバックアップのタイプを指定します。構成されているバックアップのタイプに応じて、このフィールドの値は「ONLINE」または「OFFLINE」になります。backuponline 属性は、このフィールドに関連付けられています。

バックアップ・ステータス

バックアップの現在のステータスを示します。バックアップのステータスは以下のステップのいずれかです。

- スケジュール済み
- 未スケジュール
- バックアップ進行中

backupstatus 属性は、このフィールドに関連付けられています。

前の正常バックアップ

最終正常バックアップが実行された日時を YYYY-MM-DD-hh:mm 形式で示します。

バックアップ・ロケーション

バックアップを格納するパスを示します。backuplocation 属性は、このフィールドに関連付けられています。バックアップ・ロケーションが構成されていない場合は、「directory server のバックアップの実行」タブは有効になりません。

以下の手順を実行します。

- 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ない場合に、初めてオンライン・バックアップを行うには、「**サーバーを停止して今すぐバックアップ**」をクリックします。
- 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、ディレクトリー・サーバー・インスタンスのオンライン・バックアップを行うには、「**今すぐバックアップ**」をクリックします。
- サーバーの実行中にオフライン・バックアップを行うには、「**サーバーを停止して今すぐバックアップ**」をクリックします。
- サーバーの停止中にオフライン・バックアップを行うには、「**今すぐバックアップ**」をクリックします。
- バックアップ操作に関連したログを表示するには、「**ログの表示**」をクリックします。

注: Web 管理ツールは、現在の状態に応じて上のオプションのいずれか 1 つのみを表示します。

「再表示」をクリックすると、このパネルの情報を更新できます。

directory server のバックアップのスケジュール

ここで説明する手順に従って、ディレクトリー・サーバーのバックアップをスケジュールすることができます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「バックアップ/復元の管理」をクリックします。「directory server のバックアップのスケジュール」タブをクリックします。

注: オフライン・バックアップをスケジュールすると、サーバーは実行するバックアップを停止し、再始動します。ただし、スケジュールされたオンライン・バックアップではサーバーは停止しません。

このタブでは、ディレクトリー・サーバー・インスタンスのバックアップ操作を実行するスケジュールを構成できます。バックアップのスケジュールリングを構成するには、以下の手順を実行します。

1. ディレクトリー・サーバー用にバックアップを 1 回実行するには、「1 回」セクションの下にあるチェック・ボックスを選択して日時を指定します。カレンダー・アイコンを使用して、日付を選択することができます。**注:**
 - ユーザーは、バックアップ操作をスケジュールする場合に、「1 回」、「繰り返し」またはその両方のオプションを選択できます。
 - バックアップ・タイプがオンラインであるが、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ない場合は、「1 回」セクションと「繰り返し」セクションでの制御が無効になり、「directory server のバックアップの実行」タブを使用して最初のバックアップを実行しない限り、バックアップのスケジュールは許可されません。
2. 一定の間隔でディレクトリー・サーバーのバックアップを繰り返し実行するには、「繰り返し」セクションでそのためのチェック・ボックスを選択し、期間を指定します。ここでの期間は、日次または曜日にすることができます。
3. 完了したら、以下のステップのいずれかを行います。
 - 「OK」をクリックして変更を適用し、このパネルを終了します。
 - 「適用」をクリックして変更内容を適用し、このパネルを表示させたままにします。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。

directory server の復元の実行

Web 管理ツールを使用して、ディレクトリー・サーバーの復元を実行できます。

このタスクについて

まだ行っていない場合は、Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「バックアップ/復元の管理」をクリックします。「directory server の復元の実行」タブをクリックします。

管理サーバーは、idsdbrestore コマンドを使用して復元要求を処理します。このコマンドは、ディレクトリー・サーバー・インスタンスのデータおよび構成ファイルを復元します。復元操作を実行するには、ディレクトリー・サーバー・インスタンスを停止する必要があります。

復元操作を実行できるユーザーは、以下のとおりです。

- プライマリー・ディレクトリー管理者
- DirDataAdmin、ServerStartStopAdmin、ServerConfigGroupMember、および SchemaAdmin のすべての役割を持つローカル管理グループ・メンバー

その他のユーザーに対しては、「**directory server の復元の実行**」タブは表示されません。

「directory server の復元の実行」タブには、以下の情報が表示されます。

復元ステータス

復元操作のステータスを示します。

復元ロケーション

バックアップの復元の構成済みパスを指定します。 backuplocation 属性は、このフィールドに関連付けられています。

バックアップから復元

前のバックアップの日時を yyyy-MM-dd-hh:mm 形式で指定します。

以下の手順を実行します。

- サーバーの実行中にディレクトリー・サーバー・インスタンスを復元するには、「**サーバーを停止して今すぐ復元**」をクリックします。
- サーバーの停止中にディレクトリー・サーバー・インスタンスを復元するには、「**今すぐ復元**」をクリックします。
- 復元操作に関連したログを表示するには、「**ログの表示**」をクリックします。

注: Web 管理ツールは、サーバーの状態に応じて上のオプションのいずれか 1 つのみを表示します。

「再表示」をクリックすると、このパネルの情報を更新できます。

コマンド・ラインの使用

以下に示すコマンドをコマンド行で使用することにより、ディレクトリー・サーバーの復元を実行することができます。

このタスクについて

バックアップ・ステータスを表示するには、以下のコマンドを使用します。

```
idsldapsearch -h <ldaphost> -p <admin port> -D <binddn> -w <password>
-s base -b cn=backup,cn=monitor objectclass=*
```

バックアップを構成するには、以下のコマンドを使用します。

```
idsldapmodify -h <ldaphost> -p <ldap port> -D <binddn> -w <password> -i backup.ldif
```

Where backup.ldif contains:

```
dn: cn=RDBM Backup, cn=Configuration
ibm-slapdBackupAt: 2008-04-14-16:55
ibm-slapdBackupChangeLog: <value to be set as either TRUE or FALSE>
```

```
ibm-slapdBackupEnabled: <value to be set as either TRUE or FALSE>
ibm-slapdBackupEvery: 6-01:17
ibm-slapdBackupLocation: <specify the required backup location>
ibm-slapdBackupOnline: <value to be set as either TRUE or FALSE>
```

この例で、1 回および繰り返しのバックアップをスケジュールするには、それぞれ `ibm-slapdBackupAt` 属性と `ibm-slapdBackupEvery` 属性を設定します。

`ibm-slapdBackupAt` 属性と `ibm-slapdBackupEvery` 属性は、以下の形式で設定する必要があります。

- `ibm-slapdBackupAt` : <YYYY-MM-DD-hh:mm>
- `ibm-slapdBackupEvery`: <D-hh:mm>。ここで、0 = 日曜日、6 = 土曜日、7 = 毎日

注: バックアップがオンラインで実行されるよう構成されている場合、最初のバックアップではディレクトリー・サーバーをオフラインにして実行する必要があります。オンライン・バックアップをスケジュールする場合は、まず最初のバックアップをオフラインで実行する必要があります。これを行わない場合、バックアップは失敗します。

管理サーバーにサーバー構成の変更について通知するには、以下のコマンドを実行します。

```
idsldapexop -h <ldaphost> -p <admin port> -D <binddn> -w <password>
-op readconfig -scope subtree 'CN=RDBM BACKUP, CN=CONFIGURATION'
```

ディレクトリー・サーバー・インスタンスのバックアップ要求をリモート側で開始するには、以下のコマンドを実行します。

```
idsldapexop -h <ldaphost> -p <admin port> -D <binddn> -w <password>
-op backuprestore -action backup
```

注: バックアップのタイプおよびバックアップ・ロケーションは、サーバーのバックアップがどのように構成されているかによって決まります。構成を行うのは、`idsldapexop` コマンドを実行する前にしてください。

ディレクトリー・サーバー・インスタンスをリモート側で復元するには、以下のコマンドを実行します。

```
idsldapexop -h <ldaphost> -p <ldap port> -D <binddn> -w <password>
-op backuprestore -action restore
```

注: `ldapexop` ユーティリティーを拡張操作オプション `-op backuprestore` と共に使用して、ディレクトリー・サーバー・インスタンス情報をバックアップおよびリストアする方法については、「*IBM Security Directory Server Version 6.3 Command Reference*」を参照してください。

ロギングのユーティリティー

IBM Security Directory Server で提供されているロギング・ユーティリティーは、**Web 管理ツール**とシステム・コマンド行のいずれでも表示できます。

- 480 ページの『グローバル・ログ設定の変更』
- 481 ページの『管理サーバー・ログ設定の変更』
- 484 ページの『管理サーバー監査ログの使用可能化と管理監査ログ設定の変更』
- 488 ページの『サーバーの監査ログ設定』
- 499 ページの『Bulkload ログ設定の変更』
- 501 ページの『構成ツール・ログ設定の変更』

- 503 ページの『DB2 ログ設定の変更』
- 504 ページの『逸失および検出ログ設定の変更』
- 506 ページの『サーバー・ログの変更』

注:

1. **Web 管理ツール**では、それぞれのタスク・タイトル・バーの「**ログ・ファイル**」リンクから Web 管理コンソールのログ・ファイルにアクセスします。IBM Security Directory Server のログ・ファイルにアクセスするには、以下のセクションに示す手順を使用します。
2. **Windows** のシステムでは、パスがドライブ名およびコロンで開始する場合は、絶対パスとします。ドライブ名のないパスはインストール・ツリーから開始します。例えば、`c:%tmp%mylog` は絶対パスであり、`%tmp%mylog` は `c:%idsldap-<instancename>%tmp%mylog` と解釈されます。

管理者または管理グループのメンバーのみがログ情報の表示またはアクセスを実行できます。

idslogmgmt アプリケーションはデフォルトで、以下のファイルにデータを記録します。

UNIX

```
/var/idsldap/V6.3/idslogmgmt.log
```

Windows

```
<SDS install_directory>%var%idslogmgmt.log
```

以下のリストは、idslogmgmt.log のログ管理のデフォルト値を示しています。

- デフォルトのしきい値は 10 MB です。
- アーカイブ・ファイルの最大数は 3 です。
- アーカイブの場所は、元のログの場所と同じです。

デフォルト・ログのパス

ディレクトリー・サーバーに対して実行されているさまざまな操作を追跡するためにログ・ファイルを構成することができます。ログ・ファイルを構成していない場合、ログの詳細はデフォルト・ログ・パスに記録されます。

ディレクトリー・サーバーは、ログを以下のデフォルト・ログ・パスに記録します。

AIX、Linux、および Solaris

```
instance_directory/idsldapd-instance_name/logs
```

変数は、以下の目的に使用されます。

- *instance_directory*: ディレクトリー・サーバー・インスタンス所有者のホーム・ディレクトリーを指定します。
- *instance_name*: ディレクトリー・サーバー・インスタンスの名前を指定します。

Windows

```
drive%idsldapd-instance_name%logs
```

変数は、以下の目的に使用されます。

- *drive*: ディレクトリー・サーバー・インスタンスが作成されたドライブを指定します。
- *instance_name*: ディレクトリー・サーバー・インスタンスの名前を指定します。

注: デフォルトのエラー・ログ・パス (ディレクトリー・サーバーでは `ibmslapd.log`、管理サーバーでは `idsdiradm.log`) を変更した場合、サーバーは以下のアクションを実行します。

1. サーバーが再始動された時間から `ibm-slapdLog` 属性を解析するまでは、ログ・メッセージをデフォルト・ログ・ファイルに書き込みます。
2. カスタム・ログ・パスを含む `ibm-slapdLog` 属性をサーバーが解析した後は、ログ・メッセージをカスタム・ログ・パスに書き込みます。

ログ管理ツール

ログ管理ツールを使用すると、LDAP 管理者は、ログ・ファイルのサイズを制限できます。

ツール `idslogmgmt` は、15 分ごとにウェイクアップして、ログ・ファイルのサイズをチェックし、最大ログ・サイズしきい値を超過しているファイルをアーカイブ・ファイルに移動します。このアーカイブ・ログの数も制限できます。ログの構成設定は、管理ツールおよび `idslogmgmt` のログの構成設定を除いて、`ibmslapd` 構成ファイル内にあります。詳細については、IBM Security Directory Server の資料の『コマンド解説書』セクションに記載されている `idslogmgmt` コマンド情報を参照してください。

注: ログ管理ツールを使用する場合、IBM Security Directory Integrator がインストールされている必要があります。

重要: いずれかのログ・ファイルのサイズがシステム・ファイル・サイズ制限を超えると、IBM Security Directory Server は破損する場合があります。このような状態が発生しやすいのは、サーバーでトレースが使用可能になっている場合です。

インスタンスの `idslogmgmt.log` ファイルのカスタム・ロケーションの指定

インスタンスの `idslogmgmt.log` ファイルのカスタム・ロケーションを指定することができます。

このタスクについて

デフォルトでは、`-I <instance>` オプションを指定してインスタンス所有者として `idslogmgmt` ツールを実行するか、または `-I` オプションを指定せずにルートとして `idslogmgmt` ツールを実行すると、以下のファイルに情報が記録されます。

UNIX ベースのシステムの場合

```
/var/idsldap/V6.3/idslogmgmt.log
```

Windows システムの場合

```
<TDS_install_directory>%var%idslogmgmt.log
```

ただし、ルート権限を備えたユーザーがツールを実行すると、idslogmgmt.log ファイルの他のユーザーのアクセス権が読み取り専用へとオーバーライドされます。これにより、インスタンス所有者は、インスタンスに固有の idslogmgmt.log ファイルに情報を記録できなくなります。

idslogmgmt -I <instance> コマンドを使用するときに、情報を記録する idslogmgmt.log ファイルのカスタム・ロケーションを指定するには、環境変数 IDSLMG_LOG_PATH を設定する必要があります。idslogmgmt.log ファイルのカスタム・ロケーションを指定するには、以下の手順を実行します。

1. idslogmgmt ファイルを保管するディレクトリーを作成します。インスタンス所有者がこのディレクトリーに対して必要なアクセス権を持っていることを確認します。
2. インスタンス所有者の資格情報を使用して、システムにログインします。

注: UNIX の場合、ユーザーがインスタンス所有者とは異なる資格情報を使用してログインした場合は、su - <instance_owner> を実行してください。

3. 環境変数 IDSLMG_LOG_PATH を設定して、その変数をエクスポートします。
例:

UNIX ベースのシステムの場合

```
export IDSLMG_LOG_PATH=/directoryForLog
```

Windows システムの場合

```
set IDSLMG_LOG_PATH=C:¥directoryForLog
```

4. 同じコンソールから idslogmgmt ツールを始動します。例:

```
idslogmgmt -I <instance_name>
```

これにより、IDSLMG_LOG_PATH 環境変数で指定したロケーションの下に idslogmgmt.log ファイルが作成されます。ただし、Security Directory Integrator AssemblyLine の始動メッセージは、<instance_home>/idsslapd-<instance>/etc/logmgmt/idslogmgmt.log ファイルに記録されます。

環境変数を設定せず、idslogmgmt コマンドの実行時に -I <instance> オプションを指定した場合は、<instance_home>/idsslapd-<instance>/etc/logmgmt/idslogmgmt.log ファイルに情報が記録されます。

デフォルトのログ管理

デフォルトのログ・ファイル管理用の新規の構成項目が作成されます。この項目には、ibm-slapdLog 属性を除く、すべてのログのデフォルト・ログ設定が含まれません。

デフォルト・ログ設定は、次のセクションで説明する特定のログ管理項目でオーバーライドできます。デフォルトでは、項目に属性がありません。そのため、ログの制限は適用されません。ここではログ管理用の項目について説明します。

```
dn: cn=default, cn=Log Management, cn=Configuration
ibm-slapdLogSizeThreshold:
ibm-slapdLogMaxArchives:
ibm-slapdLogArchivePath:
objectclass: top
objectclass: ibm-slapdLogConfig
objectclass: ibm-slapdConfigEntry
objectclass: container
```

以下の属性が定義されています。

ibm-slapdLogSizeThreshold

このサイズしきい値 (MB) を超過したファイルはアーカイブされます。

ibm-slapdLogMaxArchives

アーカイブ・ログの最大数。

ibm-slapdLogArchivePath

アーカイブ・ログの保存先のパス。

グローバル・ログ設定の変更

IBM Security Directory Integrator をインストールしたら、**ログ管理ツール**を使用してグローバル・ログ設定を変更できます。デフォルトの最大ログ・サイズしきい値、ログ・アーカイブの最大数、およびログ・アーカイブ・パス値を設定できます。

例えば、維持するアーカイブ・ログを、各ログに 3 つのみにする場合は、すべてのログの最大ログ・アーカイブ値を 3 に設定します。グローバル・ログ設定はすべてのログに適用されます。グローバル・ログ設定は、個別のログ項目の設定を明示的に指定してオーバーライドしない限り、すべてのログ管理項目に適用されます。

グローバル・ログ設定を編集するには、以下のいずれかの方法を使用します。

Web 管理ツールの使用

以下に示す指示により、Web 管理ツールを使用してグローバル・ログ設定を編集することができます。

このタスクについて

手順

1. 「**グローバル・ログ設定**」を選択して「**設定の編集**」ボタンをクリックするか、「**アクションの選択**」ドロップダウン・リストから「**設定の編集**」を選択して「**実行**」をクリックします。
2. 「**ログ・サイズしきい値 (MB)**」にログのしきい値サイズを MB 単位で指定します。サイズ制限を MB 単位で指定する場合、オプションを選択して、フィールドに数値を指定します。選択しない場合は「**無制限**」を選択します。
3. アーカイブするログの最大数を指定します。アーカイブするログの最大数を指定する場合、オプションを選択して、フィールドに数値を指定します。ログをアーカイブしない場合には、「**アーカイブなし**」を選択します。無制限に設定するには「**無制限**」を選択します。
4. アーカイブするログのパス名を指定します。パス名を指定する場合、オプションを選択して、アーカイブするログの絶対パス名を入力します。ログ・ファイルと同じアーカイブ・パスを指定するには、「**ログ・ファイルと同じディレクトリー**」を選択します。
5. 「**頻度の選択**」チェック・ボックスから項目を選択して、イベントの 2 つのサイクルの頻度を指定します。
6. 「**開始日**」フィールドに、イベントの開始日および開始時刻を指定します。カレンダー・アイコンをクリックして開始日を指定することもできます。開始時刻は 12:30:00 PM の形式で指定します。
7. 完了したら、以下のステップのいずれかを行います。

- 「次へ」をクリックし、ログ設定の構成を続行します。
- 「完了」をクリックして変更内容を保管し、「ログ設定の変更」パネルに戻ります。
- 「キャンセル」をクリックしてこのパネルで行った変更を破棄し、「ログ設定の変更」パネルにナビゲートします。

コマンド・ラインの使用

以下に示すコマンドを発行することにより、グローバル・ログ設定を編集することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Default, cn=Log Management, cn=Configuration
changetype: modify
replace: ibm-slapdLogSizeThreshold
ibm-slapdLogSizeThreshold: <size threshold in MB>
-
replace: ibm-slapdLogMaxArchives
ibm-slapdLogMaxArchives: <number of log archives to save>
-
replace: ibm-slapdLogArchivePath
ibm-slapdLogArchivePath: <archived logs path>
```

管理サーバー・ログ設定の変更

管理サーバーは、拡張操作を受け入れ、LDAP サーバーを停止、始動、および再始動する限定された LDAP サーバーです。管理サーバー・ログ (デフォルトのファイル名は `idsdiradm.log`) を使用して、管理サーバーによって検出された状況およびエラーを参照できます。

管理サーバー・ログ設定を変更するには、以下のいずれかの方法を使用します。個々のログ設定により、デフォルト・ログ設定がオーバーライドされます。

Web 管理ツールの使用

以下に示す指示により、管理サーバー・ログを変更することができます。

手順

1. ナビゲーション領域の「ログ」を展開して、「ログ設定の変更」をクリックします。
2. 「管理サーバー・ログ」をクリックします。
3. 管理サーバー・エラー・ログのパスおよびファイル名を入力します。ファイルが LDAP サーバー上に存在し、パスが有効であることを確認してください。デフォルト・ログのパスについては、477 ページの『デフォルト・ログのパス』を参照してください。**注:** 受け入れ可能なファイル名でないファイルを指定した場合 (構文が無効な場合や、ファイルの作成や変更を行う権限がサーバーにない場合など)、操作はエラー「LDAP サーバーは操作の実行を望んでいません」で失敗します。

4. 「ログ・サイズしきい値 (MB)」で 1 番目のラジオ・ボタンを選択し、最大ログ・サイズを MB 単位で入力します。ログ・サイズを制限しない場合には、代わりに「無制限」ラジオ・ボタンを選択します。
5. 「最大ログ・アーカイブ」で、以下のオプションのいずれかを選択します。
 - アーカイブ・ログの最大数を指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択します。保管するアーカイブの最大数を入力します。1 つのアーカイブ・ログは、そのサイズしきい値に達した古いログです。
 - ログをアーカイブしない場合には、「アーカイブなし」を選択します。
 - アーカイブ・ログの数を制限しない場合には、「無制限」を選択します。
6. 「ログ・アーカイブ・パス」の下で、以下のいずれかの手順を実行します。
 - アーカイブの保管先パスを指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択し、必要なパスを入力します。
 - ログ・ファイルがあるディレクトリーにアーカイブを保管する場合は、「ログ・ファイルと同じディレクトリー (Same directory as log file)」ラジオ・ボタンを選択します。
7. 「ログ・スケジュール」の下で、以下の手順を実行します。
 - a. 「頻度の選択」チェック・ボックスから項目を選択して、イベントの 2 つのサイクルの頻度を指定します。
 - b. 「開始日」フィールドに、イベントの開始日および開始時刻を指定します。カレンダー・アイコンをクリックして開始日を指定することもできます。開始時刻は 12:30:00 PM の形式で指定します。
8. 変更を適用してログ操作を続行する場合は「適用」を、変更を保管して IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「OK」をクリックします。変更を保管せずに IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「キャンセル」をクリックします。
9. 変更した内容を有効にするには、サーバーを停止する必要があります。86 ページの『サーバーの開始と停止』を参照してください。サーバーを停止したら、管理サーバーをローカル・マシン上で停止および始動して、ポートを再同期化する必要があります。

オプション	説明
AIX、Linux、Solaris および Windows	<pre> 次のコマンドを発行します。ibmdirctl -D <AdminDN> -w <AdminPW> -p <admin server portnumber> stopibmdirctl -D <AdminDN> -w <AdminPW> -p <admin server portnumber> admstopidsdiradmbmdirctl -D <AdminDN> -w <AdminPW>-p <admin server portnumber> start </pre>

オプション	説明
Windows	<ol style="list-style-type: none"> 1. 「コントロール パネル」->「管理ツール」->「サービス」に移動します。 2. 「IBM Security Directory Admin Server V6.3 - <InstanceName>」を選択します。 3. 以下のステップのいずれかを実行します。 <ul style="list-style-type: none"> • 「アクション (Action)」->「停止」をクリックします。 • 「サービスの停止」をクリックします。 4. 「IBM Security Directory Admin Server V6.3 - <InstanceName>」を選択します。 5. 以下のステップのいずれかを実行します。 <ul style="list-style-type: none"> • 「アクション (Action)」->「始動」をクリックします。 • 「サービスの開始」をクリックします。

10. サーバーを再始動します。

コマンド・ラインの使用

以下で示すコマンドを発行することにより、管理サーバー・ログ設定を変更することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Admin, cn=Log Management, cn=Configuration
changetype: modify
replace: ibm-slapdLog
ibm-slapdLog: <newpathname>
-
replace: ibm-slapdLogSizeThreshold
ibm-slapdLogSizeThreshold: <size threshold in MB>
-
replace: ibm-slapdLogMaxArchives
ibm-slapdLogMaxArchives: <number of log archives to save>
-
replace: ibm-slapdLogArchivePath
ibm-slapdLogArchivePath: <archived logs path>
```

変更した内容を有効にするには、サーバーを停止する必要があります。サーバーを停止したら、管理サーバーをローカル・マシン上で停止および始動して、ポートを再同期化する必要があります。サーバーを開始します。

```
ibmdirctl -D <AdminDN> -w <AdminPW> -p <portnumber> stop
```

```
ibmdirctl -D <AdminDN> -w <AdminPW> admstop
```

```
idsdiradm
```

```
ibmdirctl -D <AdminDN> -w <AdminPW> -p <portnumber> start
```

管理サーバー監査ログの使用可能化と管理監査ログ設定の変更

この機能では、管理サーバー監査ログを使用可能にし、その設定を変更することができます。

監査ログは、ディレクトリー・サーバーのセキュリティーを高めるために使用されます。AuditAdmin 役割または ServerConfigGroupMember 役割を割り当てられているディレクトリー管理者および管理グループ・メンバーは、監査ログに格納された記録を使用して、試行中に疑わしいアクティビティーのパターンがないかどうか検査し、セキュリティーの違反を検出できます。セキュリティー違反が発生した場合、管理サーバー監査ログ (デフォルトのファイル名は adminaudit.log) を参照すれば、問題が発生した経緯、発生時刻を確認できます。損害の程度を確認できる場合もあります。

注:

- 管理サーバー監査ログ設定にアクセスできるユーザーは、プライマリー・ディレクトリー管理者と、監査管理者役割およびサーバー構成グループ・メンバー役割を持つ管理グループのメンバーのみです。
- 接続試行の失敗は、それらが LDAP サーバーに到達して失敗した場合のみ監査されます。SSL 層、ネットワーク層、またはオペレーティング・システム層で失敗した接続は監査されません。

管理監査ログ設定を変更するには、以下のいずれかの方法を使用します。個々のログ設定により、デフォルト・ログ設定がオーバーライドされるということに注意してください。

注: 管理サーバー監査ログでは、バインド、アンバインド、検索、および拡張操作を監査します。

Web 管理ツールの使用

Web 管理ツールを使用することで、管理サーバー監査ログを使用し、その設定を変更することができます。

手順

1. ナビゲーション領域の「ログ」を展開して、「ログ設定の変更」をクリックします。
2. 「管理サーバーの監査ログ」をクリックします。
3. 管理サーバーで監査ログ・ユーティリティーを使用するには、「管理サーバーの監査ログ作成の使用可能化 (Enable admin server audit logging)」を選択します。注: デフォルトの設定は使用可能です。以前に管理サーバー監査ログを使用不可にしてある場合は、チェック・ボックスを選択するだけで済みます。
4. 管理サーバー監査ログのパスおよびファイル名を入力します。LDAP サーバー上にこのファイルが存在していることと、パスが有効であることを確認します。デフォルト・ログのパスについては、477 ページの『デフォルト・ログのパス』を参照してください。注: 受け入れ可能なファイル名でないファイルを指定した場合 (構文が無効な場合や、ファイルの作成や変更を行う権限がサーバーにない場合など)、操作はエラー 「LDAP サーバーは操作の実行を望んでいません」で失敗します。

5. 「**ログ・サイズしきい値 (MB)**」で 1 番目のラジオ・ボタンを選択し、最大ログ・サイズを MB 単位で入力します。ログ・サイズを制限しない場合には、代わりに「**無制限**」ラジオ・ボタンを選択します。
6. 「**最大ログ・アーカイブ**」で、以下のオプションのいずれかを選択します。
 - アーカイブ・ログの最大数を指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択します。保管するアーカイブの最大数を入力します。1 つのアーカイブ・ログは、そのサイズしきい値に達した古いログです。
 - ログをアーカイブしない場合には、「**アーカイブなし**」を選択します。
 - アーカイブ・ログの数を制限しない場合には、「**無制限**」を選択します。
7. 「**ログ・アーカイブ・パス**」の下で、以下のいずれかの手順を実行します。
 - アーカイブの保管先パスを指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択し、必要なパスを入力します。
 - ログ・ファイルがあるディレクトリーにアーカイブを保管する場合は、「**ログ・ファイルと同じディレクトリー (Same directory as log file)**」ラジオ・ボタンを選択します。
8. 「**ログ・スケジュール**」の下で、以下の手順を実行します。
 - a. 「**頻度の選択**」チェック・ボックスから項目を選択して、イベントの 2 つのサイクルの頻度を指定します。
 - b. 「**開始日**」フィールドに、イベントの開始日および開始時刻を指定します。カレンダー・アイコンをクリックして開始日を指定することもできます。開始時刻は 12:30:00 PM の形式で指定します。
9. 「**ログに記録する操作**」の下で、以下の手順を実行します。
 - a. バインド操作のロギングを使用可能にするには、「**バインド**」チェック・ボックスを選択します。バインド操作のロギングを使用不可にするには、チェック・ボックスをクリアします。
 - b. アンバインド操作のロギングを使用可能にするには、「**アンバインド**」チェック・ボックスを選択します。アンバインド操作のロギングを使用不可にするには、チェック・ボックスをクリアします。
 - c. 「**検索**」チェック・ボックスを選択して、クライアントによって行われた LDAP 検索操作を記録します。検索を使用不可にするには、チェック・ボックスをクリアします。
 - d. LDAP への追加を記録するには、「**追加**」チェック・ボックスを選択します。このフィーチャーを使用不可にするには、チェック・ボックスをクリアします。
 - e. LDAP への変更を記録するには、「**変更**」チェック・ボックスを選択します。このフィーチャーを使用不可にするには、チェック・ボックスをクリアします。
 - f. LDAP からの削除を記録するには、「**削除**」チェック・ボックスを選択します。このフィーチャーを使用不可にするには、チェック・ボックスをクリアします。
 - g. RDN への変更を記録するには、「**RDN の変更**」チェック・ボックスを選択します。このフィーチャーを使用不可にするには、チェック・ボックスをクリアします。

- h. 「イベント通知」チェック・ボックスを選択して、イベント通知を記録します。このフィーチャーを使用不可にするには、チェック・ボックスをクリアします。
 - i. 拡張操作のロギングを使用可能にするには、「拡張操作」チェック・ボックスを選択します。拡張操作のロギングを使用不可にするには、チェック・ボックスをクリアします。
10. 変更を適用してログ操作を続行する場合は「適用」を、変更を保管して IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「OK」をクリックします。変更を保管せずに IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「キャンセル」をクリックします。

コマンド・ラインの使用

以下に示すコマンドをコマンド行で使用することにより、管理サーバー監査ログを使用可能にし、その設定を変更することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Admin Audit, cn=Log Management, cn=Configuration
changetype: modify
replace: ibm-audit
ibm-audit: true
-
replace: ibm-slapdLog
ibm-slapdLog: <newpathname>
-
replace: ibm-slapdLogSizeThreshold
ibm-slapdLogSizeThreshold: <size threshold in MB>
-
replace: ibm-slapdLogMaxArchives
ibm-slapdLogMaxArchives: <number of log archives to save>
-
replace: ibm-slapdLogArchivePath
ibm-slapdLogArchivePath: <archived logs path>
-
replace: ibm-auditbind
ibm-auditbind: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditunbind
ibm-auditunbind: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditsearch
ibm-auditsearch: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditadd
ibm-auditadd: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditmodify
ibm-auditmodify: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditdelete
ibm-auditdelete: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditmodifydn
ibm-auditmodifydn: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditextopevent
ibm-auditextopevent: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
```

```
-
replace: ibm-auditExtOp
ibm-auditExtOp: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
```

設定を動的に更新するには、以下のコマンドを発行します。

```
idsldapexop -p <instance port> -D <adminDN> -w <adminPW> -op readconfig ¥
-scope entire
```

```
idsldapexop -p <administration server port> -D <adminDN> -w <adminPW> ¥
-op readconfig -scope entire
```

管理サーバー監査ログの使用不可化

この機能により、管理サーバー監査ログを使用不可にすることができます。

監査ログ記録を使用不可にするには、以下の手順を実行します。

Web 管理の使用

Web 管理ツールを使用することで、管理サーバー監査ログを使用不可にし、その設定を変更することができます。

手順

1. ナビゲーション領域の「ログ」を展開して、「ログ設定の変更」をクリックします。
2. 「管理サーバーの監査ログ」をクリックします。
3. 「管理サーバーの監査ログ作成の使用可能化 (Enable admin server audit logging)」の選択を解除します。
4. 変更を適用してログ操作を続行する場合は「適用」を、変更を保管して IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「OK」をクリックします。変更を保管せずに IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「キャンセル」をクリックします。

コマンド・ラインの使用

以下に示すコマンドをコマンド行で使用することにより、管理サーバー監査ログを使用不可にし、その設定を変更することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Admin Audit, cn=Log Management, cn=Configuration
changetype: modify
replace: ibm-audit
ibm-audit: false
```

設定を動的に更新するには、以下のコマンドを発行します。

```
idsldapexop -p <instance port> -D <adminDN> -w <adminPW> -op readconfig -scope entire
```

```
idsldapexop -p <administration server port> -D <adminDN> -w <adminPW>
-op readconfig -scope entire
```

事前監査レコードの構成

操作が完了する前に、その操作を監査するよう監査を構成できます。これは事前監査といいます。ここで説明する手順を使用することにより、事前監査レコードを構成することができます。

このタスクについて

事前監査レコードが使用可能な場合、監査プラグインが呼び出され、操作が完了する前に監査レコードが更新されます。事前監査を使用可能にするには、**IBMSLDAPD_PREOP_AUDIT** 環境変数の値を "YES" に設定する必要があります。これを行うには、環境変数にアクセスするか、以下の形式で `ldapmodify` コマンドを使用します。

```
ldapmodify -D <adminDN> -w <adminPW>
dn: cn=Front End, cn=configuration
changetype: modify
add: ibm-slapdSetEnv
ibm-slapdSetEnv: IBMSLDAPD_PREOP_AUDIT=YES
```

注:

- 変更内容を有効にするには、サーバーを再始動する必要があります。
- 事前監査を使用するのは、デバッグの目的のみにする必要があります。事前監査ではフォーマットが変更され、ログを解析するツールが中断されます。

事前監査が使用可能な場合の診断監査レコードのペアの例は以下のとおりです。ここで、シーケンス ID は 3、つまり <"PREOP: 3" および "POSTOP: 3">、です。

```
AuditV3--2007-08-29-11:44:32.912-06:00DST--V3 PREOP: 3 threadId:1161116592
Search--bindDN: cn=root--client: 127.0.0.1:1044--connectionID:
3--received: 2007-08-29-11:44:32.912-06:00DST--Success
controlType: 1.3.6.1.4.1.42.2.27.8.5.1
criticality: false
base: o=sample
scope: baseObject
derefAliases: neverDerefAliases
typesOnly: false
filter: (objectclass=*)
```

```
AuditV3--2007-08-29-11:44:33.092-06:00DST--V3 POSTOP: 3 threadId:1161116592
Search--bindDN: cn=root--client: 127.0.0.1:1044--connectionID:
3--received: 2007-08-29-11:44:32.912-06:00DST--Success
controlType: 1.3.6.1.4.1.42.2.27.8.5.1
criticality: false
base: o=sample
scope: baseObject
derefAliases: neverDerefAliases
typesOnly: false
filter: (objectclass=*)
```

サーバーの監査ログ設定

監査ログは、ディレクトリー・サーバーのセキュリティーを高めるために使用されます。サーバーには、デフォルトの監査プラグインが提供されています。このプラグインは、サーバーが処理した各 LDAP 操作ごとに、監査項目をデフォルトまたは指定された監査ログに記録します (ログの記録先は、監査構成パラメーターで決まります)。

管理者は、セキュリティーの違反を検出できるよう、監査ログに格納されているアクティビティーを使用して、疑わしいアクティビティーのパターンがないかどうかを検査します。セキュリティー違反が発生した場合、監査ログを使用すると、問題がいつどのようにして起きたのかを特定できます。また、監査ログから、受けた損害の程度がわかることもあります。この情報は、違反からリカバリーする場合にも、また今後発生しうる問題を防止するために強化されたセキュリティー対策を開

発する場合にも役立ちます。監査プラグインを独自に作成して、デフォルトの監査プラグインと置き換えたり、デフォルトの監査プラグインにより多くの機能を追加したりすることもできます。プラグインについては、「*IBM Security Directory Server Version 6.3 Server Plug-ins Reference*」を参照してください。

注: 接続試行の失敗は、それらが LDAP サーバーに到達して失敗した場合のみ監査されます。SSL 層、ネットワーク層、またはオペレーティング・システム層で失敗した接続は監査されません。

監査が使用可能な場合、以下のサーバー・イベントが監査されます。

- 監査の開始
- 監査の停止
- 監査構成の変更
- サーバーの始動
- サーバーの停止

サーバー・イベントの監査では、以下のフォーマットが使用されます。

<Time>--<Message Text in local code page>

以下に例を示します。

```
2009-08-05-14:06:20.957-06:00--GLPSRV009I IBM Security Directory (SSL),
Version 6.3Server started.
```

監査ログには、ログ項目が日時順に表示されます。非メッセージ項目にはそれぞれ一般情報ヘッダーが含まれ、その後には操作固有のデータが続きます。例:

```
2000-03-23-16:01:01.345-06:00--V3 Bind--bindDN:cn=root
--client:9.1.2.3:12345--
ConnectionID:12--received:2000-03-23-16:01:01.330-06:00
--success
name:cn=root
authenticationChoice: simple
```

監査バージョンがバージョン 2 である場合、ヘッダーには「AuditV2--」が含まれます。

```
AuditV2--2003-07-22-09:39:54.421-06:00DST--V3 Bind--bindDN: cn=root--client: 127
.0.0.1:8196--connectionID: 3--received: 2003-07-22-09:39:54.421-06:00DST--Success
```

監査バージョンがバージョン 3 である場合、ヘッダーには「AuditV3--」が含まれます。

```
AuditV3--2003-07-22-09:39:54.421-06:00DST--V3 Bind--bindDN: cn=root--client: 127
.0.0.1:8196--connectionID: 3--received: 2003-07-22-09:39:54.421-06:00DST--Success
UniqueID:
```

監査バージョンが 1 に設定されている場合、追加情報は監査されません。

監査バージョンが 2 以降に設定されている場合は、以下の条件が TRUE になります。

- 制御がプロキシ許可制御である場合、以下の追加情報が監査されます。
 - ProxyDN: Proxy Auth DN
- 制御がグループ許可制御であり、グループ許可制御で送信されるグループを監査するよう構成されている場合、以下の追加情報が監査されます。
 - Group: Group Name
 - Group: Group Name 2 (これ以降の Group Name も監査されます)

- Normalized: TRUE または FALSE
- 制御が監査制御であり、監査制御の追加情報を監査するよう構成されている場合、以下の追加情報が監査されます。
 - RequestID: request ID 1
 - RequestID: request ID 2 (これ以降の request ID も監査されます)
 - ClientIP: 監査コントロールで送信される client IP
- 制御が複製更新 ID 制御であり、複製更新 ID 制御を監査するよう構成されている場合、以下の追加情報が監査されます。
 - value: コントロールで送信される値

注: 操作については、以下のいずれかのタイプが印刷されます。

- 不明
- バインド
- アンバインド
- 検索
- 追加
- 変更
- 削除
- ModifyDN
- イベント通知: 登録
- イベント通知: 登録抹消
- 拡張操作
- 比較

ヘッダーの形式は以下のとおりです。

タイム・スタンプ 1 "--"

項目をログに記録したときの現地時間 (要求が処理された時刻)。タイム・スタンプの形式は、YYYY-MM-DD-HH:MM:SS.mmm=(または -)HH:MM です。(または -)HH:MM は UTC オフセットです。mmm はミリ秒です。

バージョン番号 +[SSL/TLS]+[unauthenticated または anonymous] 操作 "--"

受信して処理された LDAP 要求を示します。バージョン番号は、V2 か V3 です。SSL は、接続で SSL が使用されたときにのみ表示されます。TLS は、接続で TLS が使用されるときにのみ表示されます。要求が非認証クライアントからのものである場合は unauthenticated、無名クライアントからのものである場合は anonymous が表示されます。要求が認証済みクライアントからのものである場合は、unauthenticated も anonymous も表示されません。

bindDN:

バインド DN を示します。V3 の非認証要求や匿名要求の場合、このフィールドは <*CN=NULLDN*> になります。

client: クライアント IP アドレス: ポート番号 "--"

クライアント IP アドレスとポート番号を示します。

ConnectionID: xxxx "--"

同じ接続で (バインドとアンバインド間で、共に) 受信されるすべての項目をグループ化するために使用されます。

received: タイム・スタンプ 2 "--"

要求を受信したときの現地時間。厳密に言えば、要求の処理が開始された時刻です。形式はタイム・スタンプ 1 と同じです。

結果またはステータス・ストリング

LDAP 操作の結果またはステータスを示します。結果ストリングの場合は、テキスト形式の LDAP resultCode が記録されます。例えば、0 や 1 ではなく、success や operationsError が記録されます。

UniqueID

uniqueID は、コントロールに保管される固有の要求 ID です。clientIP は、コントロールに保管されるクライアントの元の IP です。critical が true の場合は、コントロールの criticality も true に設定され、critical が false の場合は、コントロールの criticality も false に設定されます。

操作固有のデータは、ヘッダーに続いて以下のように表示されます。

- バインド:
 - name: <bindDN string>
 - authenticationChoice: unknown、simple、krbv42LDAP、krbv42DSA、sasl
 - authenticationMechanism: CRAM-MD5
 - Admin Acct Status: Not Locked、Locked、Lock Cleared
 - username: adminusername (DIGEST-MD5 の場合のみ)
 - mappedname: cn=root (authzid 付きの DIGEST-MD5 の場合のみ)
 - authzId: u: username (authzid 付きの DIGEST-MD5 の場合のみ)
- 検索:
 - base: o=ibm_us, c=us
 - scope: unknown、baseObject、singleLevel、または wholeSubtree
 - derefAliases:
 - unknown、neverDerefAliases、derefInSearching、derefFindingBaseObj、または derefAlways
 - typesOnly: FALSE
 - filter: (&(cn=c*)(sn=a*))
 - attributes: cn, sn, title (属性がない場合、このアイテムはありません)
- 比較:
 - entry: cn=Joe Smith, o=ibm_us, c=us
 - attribute: cn

注: この属性値は書き込まれていません。
- 追加:
 - entry: cn=Joe Smith, o=ibm_us, c=us
 - attributes: cn, sn

注: この属性値は書き込まれていません。

- 変更:
 - object: cn=Joe Smith, o=ibm_us, c=us
 - add: mail
 - delete: title
 - replace: telephonenumber (各操作/属性のペアが監査されます)変更のタイプは、以下のいずれかです。
 - unknown
 - add
 - delete
 - replace
- 削除:
 - entry: cn=Joe Smith, o=ibm_us, c=us
- ModifyDN:
 - entry: cn=Joe Smith, ou=Austin, o=ibm_us, c=us
 - newrdn: Joe S. Smith
 - deleteoldrdn: true
 - newSuperior: ou=rochester (newSuperior 値がない場合、このアイテムは存在しません)
- イベント通知: イベント登録:
 - eventID: LDAP_change
 - base: o=ibm_us, c=us
 - scope: wholeSubtree
 - type: unknown、changeAdd、changeDelete、changeModify、またはchangeModDN
- イベント通知: イベント登録抹消:
 - ID: hostname.uuid

デフォルトでは、監査ログは使用不可です。

注: 管理グループのメンバーは監査ログと設定を表示できますが、これらを変更することはできません。監査ログ・ファイルのアクセス、変更、または消去ができるのは、管理者のみです。

監査ログを使用可能にして、ログ設定を変更するには、以下の方法を使用します。個々のログ設定により、デフォルト・ログ設定がオーバーライドされます。

Web 管理の使用

ここで説明する手順に従って、Web 管理ツールを使用してサーバー監査ログを設定できます。

このタスクについて

手順

1. ナビゲーション領域の「ログ」を展開して、「ログ設定の変更」をクリックします。
2. 「サーバーの監査ログ」をクリックします。注:
 - このパネルにアクセスできるユーザーは、ディレクトリー管理者および管理グループのメンバーのみです。
 - 一部のプラットフォームでは、ロギングは、標準のオペレーティング・システムのロギング・メカニズムによって提供されます。これらのプラットフォームでは、このパネルを使用してディレクトリー・サーバー・ログの構成を行うことはできません。例えば、OS/400® プラットフォームでは、サーバー・メッセージはすべてディレクトリー・サーバー・ジョブ・ログに記録されます。ただし、i5/OS ディレクトリー・サーバー、バージョン 6.1 以上の場合、「監査ログ」パネルが表示され、監査用のディレクトリー・サーバー・ログを構成できます。
 - ログ管理ツールをインストールしている場合には、「ログ・サイズしきい値」、「最大ログ・アーカイブ」、および「ログ・アーカイブ・パス」の値を設定できます。ログ管理ツールがインストールされていない場合、これらのフィールドに入力された値は有効にはなりません。ログ管理ツールについて詳しくは、IBM Security Directory Server の資料の『トラブルシューティングとサポート』セクションを参照してください。
3. 監査ログ・ユーティリティーを使用するには、「サーバー監査ログを使用可能にする」を選択します。
4. 監査ログの「パスおよびファイル名」を入力します。監査ログは、ライン・プリンターなどファイル以外の場所にも送信することもできます。LDAP サーバー上にこのファイルが存在していることと、パスが有効であることを確認します。デフォルト・ログのパスについては、477 ページの『デフォルト・ログのパス』を参照してください。注: 受け入れ可能なファイル名でないファイルを指定した場合 (構文が無効な場合や、ファイルの作成や変更を行う権限がサーバーにない場合など)、操作はエラー「LDAP サーバーは操作の実行を望んでいません」で失敗します。
5. 「ログ・サイズしきい値 (MB)」で 1 番目のラジオ・ボタンを選択し、最大ログ・サイズを MB 単位で入力します。ログ・サイズを制限しない場合には、代わりに「無制限」ラジオ・ボタンを選択します。
6. 「最大ログ・アーカイブ」で、以下のオプションのいずれかを選択します。
 - アーカイブ・ログの最大数を指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択します。保管するアーカイブの最大数を入力します。1 つのアーカイブ・ログは、そのサイズしきい値に達した古いログです。
 - ログをアーカイブしない場合には、「アーカイブなし」を選択します。
 - アーカイブ・ログの数を制限しない場合には、「無制限」を選択します。
7. 「監査バージョン」の下で、使用する監査バージョンを選択します。バージョン 1 では、監査ログを解析するすべてのアプリケーションに対して、前回の監査のロギング機能を維持します。バージョン 2 を使用すると、拡張操作のログが可能になりますが、監査ログを解析する既存のアプリケーションの変更が必要な場合があります。デフォルト値のバージョン 3 を使用すると、サーバーが

要求の固有 ID を生成した場合、それも書き出されます。この固有 ID は、プロキシー・サーバーでのみ生成され、ヘッダー情報と各種制御データの間に出力されます。

8. 「**監査ログ・レベル**」の下で、以下のいずれかの手順を実行します。
 - 失敗した試行のみをログに記録するには、「**失敗した試行のみ**」ラジオ・ボタンを選択します。
 - すべての試行をログに記録するには、「**すべての試行**」ラジオ・ボタンを選択します。
9. 「**ログ・アーカイブ・パス**」の下で、以下のいずれかの手順を実行します。
 - アーカイブの保管先パスを指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択し、必要なパスを入力します。
 - ログ・ファイルがあるディレクトリーにアーカイブを保管する場合は、「**ログ・ファイルと同じディレクトリー (Same directory as log file)**」ラジオ・ボタンを選択します。
10. ログに記録する操作を選択します。ログに記録できるさまざまな操作の追加情報については、フィールドのヘルプを参照してください。
 - **バインド (Bind)** - サーバーへの接続を記録します。
 - **アンバインド (Unbind)** - サーバーからの切断を記録します。
 - **検索 (Search)** - クライアントによって行われた LDAP 検索操作を記録します。
 - **追加 (Add)** - LDAP への追加を記録します。
 - **変更 (Modify)** - LDAP に対する変更を記録します。
 - **削除 (Delete)** - LDAP からの削除を記録します。
 - **比較** - 比較操作を記録します。
 - **RDN の変更** - RDN に対する変更を記録します。
 - **イベント通知 (Event notification)** - イベント通知を記録します。
 - **拡張操作 (Extended operations)** - サーバーに対して実行された拡張操作を記録します。
 - **グループ制御で送信されたグループ値** - グループ制御で定義されたグループを記録します。
 - **グループ評価拡張操作で送信された属性** - グループ評価拡張操作で送信された属性を記録します。
11. 「**ログ・スケジュール**」の下で、以下の手順を実行します。
 - a. 「**頻度の選択**」チェック・ボックスから項目を選択して、イベントの 2 つのサイクルの頻度を指定します。
 - b. 「**開始日**」フィールドに、イベントの開始日および開始時刻を指定します。カレンダー・アイコンをクリックして開始日を指定することもできます。開始時刻は 12:30:00 PM の形式で指定します。
12. 変更を適用してログ操作を続行する場合は「**適用**」を、変更を保管して IBM Security Directory Server の Web 管理ツールの「**概要**」パネルに戻る場合は、「**OK**」をクリックします。変更を保管せずに IBM Security Directory Server の Web 管理ツールの「**概要**」パネルに戻る場合は、「**キャンセル**」をクリックします。

コマンド・ラインの使用

ここで説明する手順に従うことにより、サーバー監査ログを設定できます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Audit, cn=Log Management, cn=Configuration
changetype: modify
replace: ibm-audit
ibm-audit: true
-
replace: ibm-slapdLog
ibm-slapdLog: <newpathname>
-
replace: ibm-slapdLogSizeThreshold
ibm-slapdLogSizeThreshold: <size threshold in MB>
-
replace: ibm-slapdLogMaxArchives
ibm-slapdLogMaxArchives: <number of log archives to save>
-
replace: ibm-slapdLogArchivePath
ibm-slapdLogArchivePath: <archived logs path>
-
replace: ibm-auditadd
ibm-auditadd: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditbind
ibm-auditbind: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditdelete
ibm-auditdelete: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditextopevent
ibm-auditextopevent: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditfailedoonly
ibm-auditfailedoonly: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditmodify
ibm-auditmodify: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditmodifydn
ibm-auditmodifydn: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditsearch
ibm-auditsearch: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditunbind
ibm-auditunbind: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditversion
ibm-auditversion: {1|2|3}
#select 2 or 3, if you are enabling audit of additional information on controls
-
replace: ibm-auditExtOp
ibm-auditExtOp: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditCompare
ibm-auditCompare: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditGroupsOnGroupControl
ibm-auditGroupsOnGroupControl: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
-
replace: ibm-auditAttributesOnGroupEvalOp
ibm-auditAttributesOnGroupEvalOp: {TRUE|FALSE}
#select TRUE to enable, FALSE to disable
```

監査ログを使用不可にする

監査ログを使用不可にするには、以下のいずれかの方法を使用します。

このタスクについて

Web 管理の使用

ここで説明する手順に従うことにより、Web 管理ツールを使用して、監査ログを使用不可にすることができます。

このタスクについて

Web 管理ナビゲーション領域の「サーバー管理」をクリックしてから、展開されたリスト上で「ログ」をクリックします。

手順

1. 「ログ設定の変更」をクリックします。
2. 「サーバーの監査ログ」をクリックします。
3. 「監査ログ記録を使用可能にする」を選択解除します。
4. 変更を適用してログ操作を続行する場合は「適用」を、変更を保管して IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「OK」をクリックします。変更を保管せずに IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「キャンセル」をクリックします。

コマンド・ラインの使用

以下に示すコマンドをコマンド行で使用することにより、監査ログを使用不可にすることができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Audit, cn=Log Management, cn=Configuration
changetype: modify
replace: ibm-audit
ibm-audit: false
```

パフォーマンスのプロファイル作成

IBM Security Directory Server は、独立トレース機能 (**ldtrc**) に基づくパフォーマンス・トレースを使用して、サーバーのランタイム・パフォーマンスに関する情報を提供します。

また、IBM Security Directory Server は、各操作の監査レコードに、操作実行時におけるパフォーマンスのホット・スポットを示す情報を提供します。したがって、サーバーはパフォーマンス情報を以下の場所にパブリッシュできます。

- 独立トレース機能に基づくパフォーマンス・トレース。
- 監査ログ。

独立トレース機能によるパフォーマンスのプロファイル作成

トレース内のパフォーマンス・プロファイル情報は、ユーザーによるパフォーマンスの問題の診断に役立つことを目的としています。独立トレース機能を使用することで、パフォーマンスのプロファイル作成はサーバー・パフォーマンスへの影響を最小限に抑えて実施されます。

独立トレース機能では、実行中のサーバー・インスタンスについて操作実行時に通過するキーポイントのタイム・スタンプから構成される、操作パフォーマンスのプロファイルが作成されます。様々なステージで、以下のタイム・スタンプのプロファイルが作成されます。

- RDBM 検索処理
- RDBM バインド処理
- RDBM 比較処理
- RDBM 書き込み処理

注: 個々の操作のタイム・スタンプ・コレクション・ポイントは、RDBM バックエンドのみに提供されます。

インスタンス構成オプション `ibm-slapdStartupTraceEnabled` は、サーバーの始動時のパフォーマンス・レコードのトレースを制御します。動的トレース (`ldaptrace` クライアント・ユーティリティー) を使用すると、独立トレース機能でサーバーの始動後にパフォーマンス・レコードの収集を開始または停止できます。パフォーマンス・レコードの動的トレースを活動化するには、以下のステップを実行します。

1. パフォーマンス・レコードのトレースを活動化します。以下の形式で `ldaptrace` コマンドを実行します。

```
ldaptrace -h <hostname> -p <port number> -D <adminDN> -w <adminpwd> -l on ¥  
-t start -- -perf
```

2. トレースをバイナリー・トレース・ファイルにダンプします。次のコマンドを実行します。

```
ldtrc dmp trace.bin
```

3. トレースをフォーマット設定します。次のコマンドを実行します。

```
ldtrc fmt trace.bin trace.txt
```

トレースのフォーマット設定後、トレースの分析およびパフォーマンス上の問題の診断を実行できます。トレースをオフにするには、以下のコマンドを実行します。

```
ldtrc off
```

フォーマット設定されたパフォーマンス・トレースの例を以下に示します。

```
prf_entry LD PERF FrontEnd::operation_in_workQ (3.100.98.1.1.0)  
pid 10255; tid 1167334320; sec 1159183071; nsec 84815000  
En-queue bind op; Worker thread ID 1133718448;  
Work Q size now = 1; client conn (9.124.231.39: conn ID 1)
```

パフォーマンスのプロファイル作成の監査

この機能により、詳細なパフォーマンス・プロファイルを提供する独立トレース機能を使用して、タイム・スタンプをトレースできます。

独立トレース機能を使用したタイム・スタンプのトレースでは、詳細なパフォーマンス・プロファイルが提供されます。ただし、操作実行時のパフォーマンスのボトルネックを識別するには、監査ログでパフォーマンスのホット・スポットを示す要

約図を調べることもできます。こうしたホット・スポットは、要約として提供される最良のものです。例えば、操作の応答時間、作業キューで費やされた時間、RDBM ロックの累積待ち時間、操作あたりのクライアント I/O に費やされた時間などです。以下のホット・スポットが、監査用に識別されます。

- ワーカー・スレッドが実際に操作の実行を開始するまでに、操作がワーカー・スレッド・キュー内で長時間待つ必要がある場合。
- バックエンド内のキャッシュ競合に費やされる時間を追跡する必要がある場合。
- クライアント I/O の処理に費やされる時間。つまり、要求の受け取りおよび結果の戻しに費やされる時間。この値は、処理速度が遅いクライアントまたはネットワークの問題が原因であるボトルネックの検出にも使用できます。

各操作において、監査レコード内のパフォーマンス・データ・フィールドは、構成オプション「ibm-auditPerformance」を使用して制御されます。

「ibm-auditPerformance」フィールドの値は、デフォルトでは「false」です。したがって、デフォルトではパフォーマンス・データの収集およびパブリッシュは行われません。

「ibm-auditPerformance」フィールドの値を「true」に設定すると、監査が使用可能になっている操作ごとにパフォーマンス・データが収集され、監査ログにパブリッシュされます。

「ibm-auditPerformance」フィールドを「true」に設定して使用可能にすると、監査レコード・セクション内の 4 つのパフォーマンス・データ・フィールド (operationResponseTime、timeOnWorkQ、rdbmLockWaitTime、および clientIOTime) が監査されます。これらのパフォーマンス・データ・フィールドの値はミリ秒単位です。パフォーマンス・データ・フィールドについて以下に説明します。

- **operationResponseTime** – このフィールドは、操作を受け取った時刻とその応答を送信した時刻の時差をミリ秒で表します。操作の受け取り時刻と応答の送信時刻は、監査 v3 ヘッダーにパブリッシュされます。
- **timeOnWorkQ** – このフィールドは、操作の実行が開始されるまでにワーカー・キュー内で費やされた時間をミリ秒で表します。このフィールドの値は、実行が開始された時刻と操作が受け取られた時刻の差です。
- **rdbmLockWaitTime** – このフィールドは、操作実行時に RDBM キャッシュに対するロックの獲得に費やされた時間をミリ秒で表します。このフィールドの値を使用すると、管理者は実際の作業に対するキャッシュ競合に費やされる時間を判別できます。

以下のリソースに対するロックの待ち時間も考慮されます。

- リソース・キャッシュ
- DN キャッシュ
- 項目キャッシュ
- フィルター・キャッシュ
- 属性キャッシュ

注: IBM Security Directory Server 6.3 リリース以降、属性キャッシュは非推奨になりました。今後は、属性キャッシュの使用を避けてください。

- デッドロック検出機能

– RDBM ロック

- **clientIOTime** – このフィールドは、完全な操作要求の受け取りおよび完全な操作応答の戻りに費やされた時間をミリ秒で表します。このフィールドは操作構造内にインプリメントされ、操作要求の完全な BER の受け取り時、および操作の応答 BER メッセージの正常な戻し時に更新されます。

以下の例では、`ibm-auditPerformance` が使用可能な場合に発行される、検索操作の監査バージョン 3 形式を示します。

```
AuditV3--2006-09-09-10:49:01.863-06:00DST--V3 Search--bindDN:  
cn=root--client: 127.0.0.1:40722--connectionID: 2--received:  
2006-09-09-10:49:01.803-06:00DST--Success  
controlType: 1.3.6.1.4.1.42.2.27.8.5.1  
criticality: false  
base: o=sample  
scope: wholeSubtree  
derefAliases: neverDerefAliases  
typesOnly: false  
filter: (&(cn=C*)(sn=A*))  
operationResponseTime: 591  
timeOnWorkQ: 1  
rdmLockWaitTime: 0  
clientIOTime: 180
```

パフォーマンス・データの監査を使用可能にするには、以下のいずれかの方法を使用します。

Web 管理の使用:

ここで説明する手順に従うことで、Web 管理ツールを使用して、パフォーマンス・データの監査を使用可能にすることができます。

手順

1. ナビゲーション領域の「サーバー管理」で「ログ」を展開して、「ログ設定の変更」をクリックします。
2. 「サーバーの監査ログ」をクリックします。
3. 「パフォーマンス・データの監査」の下で、「パフォーマンス・データの監査を使用可能にする」チェック・ボックスを選択して、サーバーに関連したパフォーマンス・データを監査ログに記録します。

コマンド行の使用:

以下に示すコマンドを発行することで、パフォーマンス・データの監査を使用可能にすることができます。

このタスクについて

```
ldapmodify -h <hostname> -p <port number> -D <adminDN>-w <adminpwd>  
dn: cn=Audit,cn=Log Management,Configuration  
changetype: modify  
replace: ibm-auditPerformance  
ibm-auditPerformance: true
```

Bulkload ログ設定の変更

`bulkload` は項目のロードに使用します。`Bulkload` ログを使用することで、`Bulkload` に関連する状況およびエラーを参照できます。

IBM Security Directory Server の資料の『コマンド解説書』セクションに記載されている `idsbulkload` コマンド情報を参照してください。

bulkload ログ設定を変更するには、以下のいずれかの方法を使用します。個々のログ設定により、デフォルト・ログ設定がオーバーライドされます。

Web 管理の使用

以下に示す指示により、Web 管理ツールを使用してログ設定を変更することができます。

手順

1. ナビゲーション領域の「ログ」を展開して、「ログ設定の変更」をクリックします。
2. 「Bulkload ログ」をクリックします。
3. エラー・ログのパスとファイル名を入力します。LDAP サーバー上にこのファイルが存在していることと、パスが有効であることを確認します。デフォルト・ログのパスについては、477 ページの『デフォルト・ログのパス』を参照してください。注: 受け入れ可能なファイル名でないファイルを指定した場合 (構文が無効な場合や、ファイルの作成や変更を行う権限がサーバーにない場合など)、操作はエラー「LDAP サーバーは操作の実行を望んでいません」で失敗します。
4. 「ログ・サイズしきい値 (MB)」で 1 番目のラジオ・ボタンを選択し、最大ログ・サイズを MB 単位で入力します。ログ・サイズを制限しない場合には、代わりに「無制限」ラジオ・ボタンを選択します。
5. 「最大ログ・アーカイブ」で、以下のオプションのいずれかを選択します。
 - アーカイブ・ログの最大数を指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択します。保管するアーカイブの最大数を入力します。1 つのアーカイブ・ログは、そのサイズしきい値に達した古いログです。
 - ログをアーカイブしない場合には、「アーカイブなし」を選択します。
 - アーカイブ・ログの数を制限しない場合には、「無制限」を選択します。
6. 「ログ・アーカイブ・パス」の下で、以下のいずれかの手順を実行します。
 - アーカイブの保管先パスを指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択し、必要なパスを入力します。
 - ログ・ファイルがあるディレクトリーにアーカイブを保管する場合は、「ログ・ファイルと同じディレクトリー (Same directory as log file)」ラジオ・ボタンを選択します。
7. 「ログ・スケジュール」の下で、以下の手順を実行します。
 - a. 「頻度の選択」チェック・ボックスから項目を選択して、イベントの 2 つのサイクルの頻度を指定します。
 - b. 「開始日」フィールドに、イベントの開始日および開始時刻を指定します。カレンダー・アイコンをクリックして開始日を指定することもできます。開始時刻は 12:30:00 PM の形式で指定します。
8. 変更を適用してログ操作を続行する場合は「適用」を、変更を保管して IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「OK」をクリックします。変更を保管せずに IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「キャンセル」をクリックします。

コマンド・ラインの使用

以下に示すコマンドを発行することにより、一括ログを使用してサーバー・ログ設定を変更することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
cn=Bulkload, cn=Log Management, cn=Configuration
changetype: modify
replace: ibm-slapdLog
ibm-slapdLog: <newpathname>
-
replace: ibm-slapdLogSizeThreshold
ibm-slapdLogSizeThreshold: <size threshold in MB>
-
replace: ibm-slapdLogMaxArchives
ibm-slapdLogMaxArchives: <number of log archives to save>
-
replace: ibm-slapdLogArchivePath
ibm-slapdLogArchivePath: <archived logs path>
-
```

設定を動的に更新するには、以下の **idsldapexop** コマンドを発行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readconfig -scope single
"cn=Bulkload, cn=Log Management, cn=Configuration" ibm-slapdLog
```

idsldapexop コマンドでは、これらの属性のうち動的に変更可能なもののみが更新されます。他の変更内容を有効にするには、サーバーを停止して再始動する必要があります。動的に更新可能な属性のリストについては、713 ページの『付録 L. 動的に変更される属性』を参照してください。

構成ツール・ログ設定の変更

構成ツール・ログを使用することにより、**idscfgdb**、**idsucfgdb**、**idscfgchlog**、**idsucfgchlog**、**idscfgsuf**、**idsucfgsuf**、**idsdnpw**、および **idsxcfg** の構成ツールに関連する状況およびエラー・メッセージを確認できます。

構成ツールのログ設定を変更するには、以下のいずれかの方法を使用します。個々のログ設定により、デフォルト・ログ設定がオーバーライドされます。

Web 管理の使用

以下に示す指示により、Web 管理ツールを使用して構成ツール・ログ設定を変更することができます。

手順

1. ナビゲーション領域の「ログ」を展開して、「ログ設定の変更」をクリックします。
2. 「ツール・ログ」をクリックします。
3. エラー・ログのパスおよびファイル名を入力します。このファイルが LDAP サーバー上に存在しているようにし、また、パスが有効であるようにします。デフォルト・ログのパスについては、477 ページの『デフォルト・ログのパス』を参照してください。注: 受け入れ可能なファイル名でないファイルを指定した場合

(構文が無効な場合や、ファイルの作成や変更を行う権限がサーバーにない場合など)、操作はエラー「LDAP サーバーは操作の実行を望んでいません」で失敗します。

4. 「**ログ・サイズしきい値 (MB)**」で 1 番目のラジオ・ボタンを選択し、最大ログ・サイズを MB 単位で入力します。ログ・サイズを制限しない場合には、代わりに「**無制限**」ラジオ・ボタンを選択します。
5. 「**最大ログ・アーカイブ**」で、以下のオプションのいずれかを選択します。
 - アーカイブ・ログの最大数を指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択します。保管するアーカイブの最大数を入力します。1 つのアーカイブ・ログは、そのサイズしきい値に達した古いログです。
 - ログをアーカイブしない場合には、「**アーカイブなし**」を選択します。
 - アーカイブ・ログの数を制限しない場合には、「**無制限**」を選択します。
6. 「**ログ・アーカイブ・パス**」の下で、以下のいずれかの手順を実行します。
 - アーカイブの保管先パスを指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択し、必要なパスを入力します。
 - ログ・ファイルがあるディレクトリーにアーカイブを保管する場合は、「**ログ・ファイルと同じディレクトリー (Same directory as log file)**」ラジオ・ボタンを選択します。
7. 「**ログ・スケジュール**」の下で、以下の手順を実行します。
 - a. 「**頻度の選択**」チェック・ボックスから項目を選択して、イベントの 2 つのサイクルの頻度を指定します。
 - b. 「**開始日**」フィールドに、イベントの開始日および開始時刻を指定します。カレンダー・アイコンをクリックして開始日を指定することもできます。開始時刻は 12:30:00 PM の形式で指定します。
8. 変更を適用してログ操作を続行する場合は「**適用**」を、変更を保管して IBM Security Directory Server の Web 管理ツールの「**概要**」パネルに戻る場合は、「**OK**」をクリックします。変更を保管せずに IBM Security Directory Server の Web 管理ツールの「**概要**」パネルに戻る場合は、「**キャンセル**」をクリックします。

コマンド・ラインの使用

以下に示すコマンドを発行することにより、構成ツール・ログ設定を変更することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Tools, cn=Log Management, cn=Configuration
changetype: modify
replace: ibm-slapdLog
ibm-slapdLog: <newpathname>
-
replace: ibm-slapdLogSizeThreshold
ibm-slapdLogSizeThreshold: <size threshold in MB>
-
replace: ibm-slapdLogMaxArchives
```

```
ibm-slapdLogMaxArchives: <number of log archives to save>
-
replace: ibm-slapdLogArchivePath
ibm-slapdLogArchivePath: <archived logs path>
```

DB2 ログ設定の変更

DB2 エラー・ログ (デフォルトのファイル名は db2cli.log) には、LDAP 操作の結果発生したデータベース・エラーが記録されます。

DB2 ログ設定を変更するには、以下のいずれかの方法を使用します。個々のログ設定により、デフォルト・ログ設定がオーバーライドされます。

Web 管理の使用

以下に示すステップを使用することにより、DB2 ログ設定を変更することができます。

手順

1. ナビゲーション領域で「**サーバー管理**」を展開して、「**ログ**」をクリックし、「**ログ設定の変更**」をクリックして、「**DB2 ログ**」をクリックします。
2. DB2 ログのパスおよびファイル名を入力します。パスは有効なものであるようにしてください。ファイルが存在しない場合は作成されます。エラー・ログは、ライン・プリンターなどファイル以外の場所にも送信することもできます。デフォルト・ログのパスについては、477 ページの『デフォルト・ログのパス』を参照してください。注: 受け入れ可能なファイル名でないファイルを指定した場合 (構文が無効な場合や、ファイルの作成や変更を行う権限がサーバーにない場合など)、操作はエラー「LDAP サーバーは操作の実行を望んでいません」で失敗します。
3. 「**ログ・サイズしきい値 (MB)**」で 1 番目のラジオ・ボタンを選択し、最大ログ・サイズを MB 単位で入力します。ログ・サイズを制限しない場合には、代わりに「**無制限**」ラジオ・ボタンを選択します。
4. 「**最大ログ・アーカイブ**」で、以下のオプションのいずれかを選択します。
 - アーカイブ・ログの最大数を指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択します。保管するアーカイブの最大数を入力します。1 つのアーカイブ・ログは、そのサイズしきい値に達した古いログです。
 - ログをアーカイブしない場合には、「**アーカイブなし**」を選択します。
 - アーカイブ・ログの数を制限しない場合には、「**無制限**」を選択します。
5. 「**ログ・アーカイブ・パス**」の下で、以下のいずれかの手順を実行します。
 - アーカイブの保管先パスを指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択し、必要なパスを入力します。
 - ログ・ファイルがあるディレクトリーにアーカイブを保管する場合は、「**ログ・ファイルと同じディレクトリー (Same directory as log file)**」ラジオ・ボタンを選択します。
6. 「**ログ・スケジュール**」の下で、以下の手順を実行します。
 - a. 「**頻度の選択**」チェック・ボックスから項目を選択して、イベントの 2 つのサイクルの頻度を指定します。

- b. 「開始日」フィールドに、イベントの開始日および開始時刻を指定します。カレンダー・アイコンをクリックして開始日を指定することもできます。開始時刻は 12:30:00 PM の形式で指定します。
7. 変更を適用してログ操作を続行する場合は「適用」を、変更を保管して IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「OK」をクリックします。変更を保管せずに IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「キャンセル」をクリックします。

コマンド・ラインの使用

コマンド行を使用して、以下に示すコマンドを発行することで、DB2 ログ設定を変更することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=DB2CLI, cn=Log Management, cn=Configuration
changetype: modify
replace: ibm-slapdLog
ibm-slapdLog: <newpathname>
-
replace: ibm-slapdLogSizeThreshold
ibm-slapdLogSizeThreshold: <size threshold in MB>
-
replace: ibm-slapdLogMaxArchives
ibm-slapdLogMaxArchives: <number of log archives to save>
-
replace: ibm-slapdLogArchivePath
ibm-slapdLogArchivePath: <archived logs path>
-
```

設定を動的に更新するには、以下の **idsldapexop** コマンドを発行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readconfig -scope single
"cn=DB2CLI, cn=Log Management, cn=Configuration" ibm-slapdLog
```

idsldapexop コマンドでは、これらの属性のうち動的に変更可能なもののみが更新されます。他の変更内容を有効にするには、サーバーを停止して再始動する必要があります。動的に更新可能な属性のリストについては、713 ページの『付録 L. 動的に変更される属性』を参照してください。

逸失および検出ログ設定の変更

逸失および検出ログ (デフォルトのファイル名は LostAndFound.log) には、複製競合の結果発生したエラーが記録されます。

逸失および検出ログ設定を変更するには、以下のいずれかの方法を使用します。個々のログ設定により、デフォルト・ログ設定がオーバーライドされます。

Web 管理の使用

以下に示す指示により、逸失および検出ログ設定を変更することができます。

手順

1. ナビゲーション領域の「ログ」を展開して、「ログ設定の変更」をクリックします。

2. 「逸失および検出ログ」をクリックします。 注:
 - このパネルにアクセスできるユーザーは、ディレクトリー管理者および管理グループのメンバーのみです。
 - 一部のプラットフォームでは、ロギングは、標準のオペレーティング・システムのロギング・メカニズムによって提供されます。これらのプラットフォームでは、このパネルを使用してディレクトリー・サーバー・ログの構成や表示を行うことはできません。例えば、OS/400 プラットフォームでは、サーバー・メッセージはすべてディレクトリー・サーバー・ジョブ・ログに記録されます。ただし、i5/OS ディレクトリー・サーバー、バージョン 6.1 以上の場合、「逸失および検出ログ」パネルが表示され、複製の競合の結果として発生したエラーに関連するログを逸失および検出ログに記録できます。
 - ログ管理ツールをインストールしている場合には、「ログ・サイズしきい値」、「最大ログ・アーカイブ」、および「ログ・アーカイブ・パス」の値を設定できます。ログ管理ツールがインストールされていない場合、これらのフィールドに入力された値は有効にはなりません。ログ管理ツールについて詳しくは、IBM Security Directory Server の資料の『トラブルシューティングとサポート』セクションを参照してください。
3. エラー・ログのパスとファイル名を入力します。LDAP サーバー上にこのファイルが存在していることと、パスが有効であることを確認します。デフォルト・ログのパスについては、477 ページの『デフォルト・ログのパス』を参照してください。注: 受け入れ可能なファイル名でないファイルを指定した場合 (構文が無効な場合や、ファイルの作成や変更を行う権限がサーバーにない場合など)、操作はエラー「LDAP サーバーは操作の実行を望んでいません」で失敗します。
4. 「競合に関係しているグループ項目のメンバーをログに記録する」チェック・ボックスを選択して、複製競合の解決中に、グループ項目のメンバーを逸失および検出ログに記録します。項目「cn=Replication, cn=Log Management, cn=Configuration」の「ibm-slapdLogMembers」属性は、このコントロールに関連付けられています。グループ・メンバー項目を逸失および検出ログに記録する必要がある場合は、パフォーマンス上の理由により、グループ・メンバーのキャッシュを有効にする必要があります。グループに大量のメンバー項目が含まれている場合は、すべてのメンバーのログ記録を無効にすることが推奨されます。注: ibm-slapdLogMembers 属性が重要なのは、「cn=Replication, cn=Log Management, cn=Configuration」項目の場合のみです。その他すべてのログ設定では、ibm-slapdLogMembers 属性は重要ではありません。
5. 「ログ・サイズしきい値 (MB)」で 1 番目のラジオ・ボタンを選択し、最大ログ・サイズを MB 単位で入力します。ログ・サイズを制限しない場合には、代わりに「無制限」ラジオ・ボタンを選択します。
6. 「最大ログ・アーカイブ」で、以下のオプションのいずれかを選択します。
 - アーカイブ・ログの最大数を指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択します。保管するアーカイブの最大数を入力します。1 つのアーカイブ・ログは、そのサイズしきい値に達した古いログです。
 - ログをアーカイブしない場合には、「アーカイブなし」を選択します。
 - アーカイブ・ログの数を制限しない場合には、「無制限」を選択します。
7. 「ログ・アーカイブ・パス」の下で、以下のいずれかの手順を実行します。

- アーカイブの保管先パスを指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択し、必要なパスを入力します。
 - ログ・ファイルがあるディレクトリーにアーカイブを保管する場合は、「**ログ・ファイルと同じディレクトリー (Same directory as log file)**」ラジオ・ボタンを選択します。
8. 「**ログ・スケジュール**」の下で、以下の手順を実行します。
 - a. 「**頻度の選択**」チェック・ボックスから項目を選択して、イベントの 2 つのサイクルの頻度を指定します。
 - b. 「**開始日**」フィールドに、イベントの開始日および開始時刻を指定します。カレンダー・アイコンをクリックして開始日を指定することもできます。開始時刻は 12:30:00 PM の形式で指定します。
 9. 変更を適用してログ操作を続行する場合は「**適用**」を、変更を保管して IBM Security Directory Server の Web 管理ツールの「**概要**」パネルに戻る場合は、「**OK**」をクリックします。変更を保管せずに IBM Security Directory Server の Web 管理ツールの「**概要**」パネルに戻る場合は、「**キャンセル**」をクリックします。

コマンド・ラインの使用

以下に示すコマンドを発行することにより、逸失および検出ログを変更することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=Replication, cn=Log Management, cn=Configuration
changetype: modify
replace: ibm-slapdLog
ibm-slapdLog: <newpathname>
-
replace: ibm-slapdLogSizeThreshold
ibm-slapdLogSizeThreshold: <size threshold in MB>
-
replace: ibm-slapdLogMaxArchives
ibm-slapdLogMaxArchives: <number of log archives to save>
-
replace: ibm-slapdLogArchivePath
ibm-slapdLogArchivePath: <archived logs path>
```

サーバー・ログの変更

エラー・ログ `ibmslapd.log` (デフォルトのファイル名) は、デフォルトで使用可能になっています。このエラー・ログを使用することにより、サーバーに関連する状況およびエラー・メッセージを参照することができます。

エラー・ログ設定を変更するには、以下のいずれかの方法を使用します。個々のログ設定により、デフォルト・ログ設定がオーバーライドされます。

Web 管理の使用

以下に示す指示により、Web 管理ツールを使用してサーバー・ログ設定を変更することができます。

このタスクについて

1. ナビゲーション領域で「サーバー管理」を展開し、「ログ」をクリックし、「ログ設定の変更」をクリックします。
2. 「サーバー・ログ」をクリックします。
3. エラー・ログのパスとファイル名を入力します。パスが有効なことを確認してください。ファイルが存在しない場合は作成されます。エラー・ログは、ライン・プリンターなどファイル以外の場所に送信することもできます。デフォルト・ログのパスについては、477 ページの『デフォルト・ログのパス』を参照してください。

注: 受け入れ可能なファイル名でないファイルを指定した場合 (構文が無効な場合や、ファイルの作成や変更を行う権限がサーバーにない場合など)、操作はエラー「LDAP サーバーは操作の実行を望んでいません」で失敗します。

4. 「ログ・サイズしきい値 (MB)」で 1 番目のラジオ・ボタンを選択し、最大ログ・サイズを MB 単位で入力します。ログ・サイズを制限しない場合には、代わりに「無制限」ラジオ・ボタンを選択します。
5. 「最大ログ・アーカイブ」で、以下のオプションのいずれかを選択します。
 - アーカイブ・ログの最大数を指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択します。保管するアーカイブの最大数を入力します。1 つのアーカイブ・ログは、サイズしきい値に達した古いログです。
 - ログをアーカイブしない場合には、「アーカイブなし」を選択します。
 - アーカイブ・ログの数を制限しない場合には、「無制限」を選択します。
6. 「ログ・アーカイブ・パス」の下で、次のいずれかのタスクを実行します。
 - アーカイブの保管先パスを指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択し、必要なパスを入力します。
 - ログ・ファイルがあるディレクトリーにアーカイブを保管する場合は、「ログ・ファイルと同じディレクトリー (Same directory as log file)」ラジオ・ボタンを選択します。
7. 「ログ・スケジュール」で、以下のタスクを実行します。
 - 「頻度の選択」チェック・ボックスから項目を選択して、イベントの 2 つのサイクルの頻度を指定します。
 - 「開始日」フィールドに、イベントの開始日および開始時刻を指定します。カレンダー・アイコンをクリックして開始日を指定することもできます。開始時刻は 12:30:00 PM の形式で指定する必要があります。
8. エラー・ログ記録のレベルとして、「低 (low)」、「中 (medium)」、または「高 (high)」を選択します。
 - 低 (low) の場合、ログに記録されるエラー情報の量が最も少なくなり、例えば「Oct 06 10:33:02 2009 GLPSRV009I IBM Security Directory (SSL), Version 6.3 Server started.」となります。
 - 中 (medium) の場合、中程度の量のエラー情報が記録され、例えば「Oct 06 10:35:41 2009 GLPCOM024I The extended Operation plug-in is successfully loaded from libloga.dll.Oct 06 10:35:41 2009 GLPCOM003I Non-SSL port initialized to 389.Oct 06 10:35:44 2009 GLPSRV009I IBM Security Directory (SSL), Version 6.3Server started.」となります。

- 高 (high) の場合、ログに記録されるエラー情報の量が最も多くなり、例えば
「Oct 06 10:37:48 2009 GLPSRV047W Anonymous binds will be allowed.Oct 06 10:37:48 2009 GLPCOM024I The extended Operation plug-in is successfully loaded from libloga.dll.Oct 06 10:37:48 2009 GLPSRV003I Configuration file successfully read.Oct 06 10:37:48 2009 GLPCOM003I Non-SSL port initialized to 389.Oct 06 10:37:51 2009 GLPSRV009I IBM Security Directory (SSL), Version 6.3Server started. 」となります。
9. 変更を適用してログ操作を続行する場合は「適用」を、変更を保管して IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「OK」をクリックします。変更を保管せずに IBM Security Directory Server の Web 管理ツールの「概要」パネルに戻る場合は、「キャンセル」をクリックします。

コマンド・ラインの使用

以下に示すコマンドを発行することにより、サーバー・ログを変更することができます。

このタスクについて

以下のコマンドを発行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

where <filename> contains:

```
dn: cn=ibmslapd, cn=Log Management, cn=Configuration
changetype: modify
replace: ibm-slapdLog
ibm-slapdLog: <newpathname>
-
replace: ibm-slapdLogSizeThreshold
ibm-slapdLogSizeThreshold: <size threshold in MB>
-
replace: ibm-slapdLogMaxArchives
ibm-slapdLogMaxArchives: <number of log archives to save>
-
replace: ibm-slapdLogArchivePath
ibm-slapdLogArchivePath: <archived logs path>
-
replace: ibm-slapdLogOptions
ibm-slapdLogOptions: {l | m | h}
```

設定を動的に更新するには、以下の **idsldapexop** コマンドを発行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readconfig -scope entire
```

idsldapexop コマンドでは、これらの属性のうち動的に変更可能なもののみが更新されます。他の変更内容を有効にするには、サーバーを停止して再始動する必要があります。動的に更新可能な属性のリストについては、713 ページの『付録 L. 動的に変更される属性』を参照してください。

サーバー・トレースの開始と終了

サーバー・トレースの開始と停止を行う場合は、以下の情報を参照してください。

サーバー・トレースを開始または停止するには、以下の方法を使用します。

Web 管理の使用

Web 管理ツールを使用してサーバーのトレースを開始または停止するには、以下の手順を実行します。

このタスクについて

Web 管理ナビゲーション領域の「**サーバー管理**」をクリックし、展開されたリスト上で「**ログ**」をクリックします (この操作をまだ実行していない場合)。「**サーバーのトレースの開始/停止**」をクリックします。

このパネルで、以下を行うことができます。

- サーバーのトレースを使用可能にする
- 収集するトレース・デバッグ・データのレベルを設定する
- トレース情報を送信するデバッグ出力ファイルを指定する

トレース機能を使用可能にするには、以下を行います。

1. 「**サーバーのトレースを使用可能にする**」チェック・ボックスを選択して、このサーバー・インスタンスのトレースを使用可能にします。
2. 「**トレースのデバッグ・レベル**」フィールドに、トレースのデバッグ・レベルを指定します。
3. 「**トレースのデバッグ・ファイル**」フィールドに、トレース情報を送信するファイルを指定します。
4. 完了したら、以下のステップのいずれかを行います。
 - 「**OK**」をクリックして変更内容を保存し、「**概要**」パネルに戻ります。
 - 「**キャンセル**」をクリックして変更内容を廃棄し、「**概要**」パネルに戻ります。

IBM Security Directory Server ログの表示

IBM Security Directory Server のログを表示するには、**Web 管理**ツールまたはコマンド行を使用します。

以下のセクションでは、IBM Security Directory Server のログの表示方法を説明します。選択されたログ・ファイルでは、「**ログの表示**」パネルに「**ログの表示**」テーブルの最新のログが昇順に表示されます。「**ログの表示**」テーブルに表示されるのは 20 行です。ログ記録された項目は、1 行以上に渡って表示されることがあります。テーブルのステータス・バーにあるナビゲーション矢印をクリックすると、「**ログの表示**」テーブル内のページにナビゲートすることができます。また、ステータス・バー上のフィールドにページ番号を入力して「**実行**」をクリックすることもできます。

Web 管理ツールを使用したログの表示

Web 管理ツールを使用してログを表示するには、以下の手順を実行します。

このタスクについて

1. Web 管理ナビゲーション領域の「**サーバー管理**」をクリックしてから、展開されたリスト上で「**ログ**」をクリックします。「**ログの表示**」をクリックします。

注:

 - このパネルにアクセスできるユーザーは、ディレクトリー管理者および管理グループのメンバーのみです。
 - 一部のプラットフォームでは、ロギングは、標準のオペレーティング・システムのロギング・メカニズムによって提供されます。これらのプラットフォーム

では、このパネルを使用してディレクトリー・サーバー・ログの表示を行うことはできません。例えば、OS/400 プラットフォームでは、サーバー・メッセージはすべてディレクトリー・サーバー・ジョブ・ログに記録されます。ただし、i5/OS Directory Server バージョン 6.0 以上の場合、ルート DSE 検索で監査ログと逸失および検出ログの `ibm-supportedCapability` OID に `1.3.18.0.2.32.80` および `1.3.18.0.2.32.52` がそれぞれ表示される場合、「ログの選択」フィールドには監査ログと逸失および検出ログのみが表示されます。

- Web 管理ツールを使用して管理サーバーにアクセスする場合は、以下のようになります。
 - 「ログの表示」パネルのステータス・バーに、ツールが管理サーバーに接続していることを示すメッセージが表示されます。管理サーバーでサポートされていないパネルにアクセスすると、そのパネルの機能がサポート外であることを示すメッセージが表示されます。
 - 「ログの表示」パネルは、`rootDSE` の `ibm-supportedcapabilities` 属性にある機能に基づいて使用可能になります。
 - 管理サーバーではログのクリア要求はサポートされないため、「ログの表示」パネルの「クリア」ボタンは使用不可になります。
- 2. 「ログの選択」ドロップダウン・メニューから、表示するログを選択します。例えば、「逸失および検出ログ」などを選択します。
- 3. 以下を実行できます。
 - パネル下部のナビゲーション矢印「次へ」を使用すると次のページに、「前へ」を使用すると前のページに移動できます。
 - 「編集」メニューから特定のページ (例えば「ページ 6/16」) を選択して、「実行」をクリックすると、そのページのエラー・ログを表示できます。
 - 「再表示」をクリックして、ログの項目を更新します。
 - 「ログのクリア」をクリックすると、ログ内の項目がすべて削除されます。注：管理グループ・メンバーは監査ログをクリアできません。
- 4. 「閉じる」をクリックして、IBM Security Directory Server Web 管理ツールの「概要」パネルに戻ります。

コマンド行を使用したログの表示

コマンド行を使用してログを表示するには、以下の手順を実行します。

管理サーバー・エラー・ログの表示:

デフォルトの場所にある管理サーバー・エラー・ログを表示するには、以下のコマンドを実行します。

このタスクについて

UNIX オペレーティング・システムの場合。

```
more <instance base directory>/idsldapd-<instance name>/logs/idsdiradm.log
```

各部の意味を以下に示します。

- `instance base directory` は、ディレクトリー・サーバー・インスタンスの所有者のホーム・ディレクトリー、またはディレクトリー・サーバー・インスタンス作成時に指定したディレクトリーです。

- *instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

Windows オペレーティング・システムの場合。

```
more <drive>%idsslapd-<instance name>%logs
```

drive は、ディレクトリー・サーバー・インスタンス作成時に指定したドライブです。*instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

IBM Security Directory Server クライアントが存在するシステムから管理サーバー・エラー・ログを表示するには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readlog -logidsdiradm-lines all
```

管理サーバー・エラー・ログをクリアするには、以下のステップを実行します。

```
ldapexop -D <adminDN> -w <adminPW> -op clearlog -logidsdiradm
```

管理サーバー監査ログ設定の表示:

デフォルトの場所にある管理サーバー監査ログを表示するには、以下のコマンドを実行します。

このタスクについて

UNIX オペレーティング・システムの場合。

```
more <instance base directory>/idsslapd-<instance name>/logs/adminaudit.log
```

各部の意味を以下に示します。

- *instance base directory* は、ディレクトリー・サーバー・インスタンスの所有者のホーム・ディレクトリー、またはディレクトリー・サーバー・インスタンス作成時に指定したディレクトリーです。
- *instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

Windows オペレーティング・システムの場合。

```
more <drive>%idsslapd-<instance name>%logs%adminaudit.log
```

drive は、ディレクトリー・サーバー・インスタンス作成時に指定したドライブです。*instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

IBM Security Directory Server クライアントが存在するシステムから管理サーバー・ログを表示するには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readlog -logadminAudit-lines all
```

管理サーバー・ログをクリアするには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op clearlog -logadminAudit
```

監査ログの表示:

デフォルトの場所にある監査ログを表示するには、以下のコマンドを実行します。

このタスクについて

UNIX オペレーティング・システムの場合。

```
more <instance base directory>/idsslapd-<instance name>/logs/audit.log
```

各部の意味を以下に示します。

- *instance base directory* は、ディレクトリー・サーバー・インスタンスの所有者のホーム・ディレクトリー、またはディレクトリー・サーバー・インスタンス作成時に指定したディレクトリーです。
- *instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

Windows オペレーティング・システムの場合。

```
more <drive>%idsslapped-<instance name>%logs%audit.log
```

drive は、ディレクトリー・サーバー・インスタンス作成時に指定したドライブです。*instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

IBM Security Directory Server クライアントが存在するシステムから監査ログを表示するには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readlog -log audit -lines all
```

監査ログをクリアするには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op clearlog -log audit
```

Bulkload ログの表示:

デフォルトの場所にある Bulkload ログを表示するには、以下のコマンドを実行します。

このタスクについて

UNIX オペレーティング・システムの場合。

```
more <instance base directory>/idsslapped-<instance name>/logs/bulkload.log
```

各部の意味を以下に示します。

- *instance base directory* は、ディレクトリー・サーバー・インスタンスの所有者のホーム・ディレクトリー、またはディレクトリー・サーバー・インスタンス作成時に指定したディレクトリーです。
- *instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

Windows オペレーティング・システムの場合。

```
more <drive>%idsslapped-<instance name>%logs%bulkload.log
```

drive は、ディレクトリー・サーバー・インスタンス作成時に指定したドライブです。*instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

IBM Security Directory Server クライアントが存在するシステムから bulkload エラー・ログを表示するには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readlog -log bulkload -lines all
```

Bulkload エラー・ログをクリアするには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op clearlog -log bulkload
```

構成ツールのログの表示:

デフォルトの場所にある構成ツールのログを表示するには、以下のコマンドを実行します。

このタスクについて

UNIX オペレーティング・システムの場合。

```
more <instance base directory>/idsslapd-<instance name>/logs/idstools.log
```

各部の意味を以下に示します。

- *instance base directory* は、ディレクトリー・サーバー・インスタンスの所有者のホーム・ディレクトリー、またはディレクトリー・サーバー・インスタンス作成時に指定したディレクトリーです。
- *instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

Windows オペレーティング・システムの場合。

```
more <drive>%idsslapd-<instance name>%logs%idstools.log
```

drive は、ディレクトリー・サーバー・インスタンス作成時に指定したドライブです。*instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

IBM Security Directory Server クライアントが存在するシステムから構成ツール・ログを表示するには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readlog -log config -lines all
```

構成ツール・ログをクリアするには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op clearlog -log config
```

DB2 ログの表示:

デフォルトの場所にある DB2 ログを表示するには、以下のコマンドを実行します。

このタスクについて

UNIX オペレーティング・システムの場合。

```
more <instance base directory>/idsslapd-<instance name>/logs/db2cli.log
```

各部の意味を以下に示します。

- *instance base directory* は、ディレクトリー・サーバー・インスタンスの所有者のホーム・ディレクトリー、またはディレクトリー・サーバー・インスタンス作成時に指定したディレクトリーです。
- *instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

Windows オペレーティング・システムの場合。

```
more <drive>%idsslapd-<instance name>%logs%db2cli.log
```

drive は、ディレクトリー・サーバー・インスタンス作成時に指定したドライブです。*instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

IBM Security Directory Server クライアントが存在するシステムから DB2 エラー・ログを表示するには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readlog -logcli-lines all
```

DB2 エラー・ログをクリアするには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op clearlog -logcli
```

逸失および検出エラー・ログの表示:

デフォルトの場所にある逸失および検出ログを表示するには、以下のコマンドを使用します。

このタスクについて

UNIX オペレーティング・システムの場合。

```
more <instance base directory>/idsslapd-<instance name>/logs  
/LostAndFound.log
```

各部の意味を以下に示します。

- *instance base directory* は、ディレクトリー・サーバー・インスタンスの所有者のホーム・ディレクトリー、またはディレクトリー・サーバー・インスタンス作成時に指定したディレクトリーです。
- *instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

Windows オペレーティング・システムの場合。

```
more <drive>%idsslapd-<instance name>%logs%LostAndFound.log
```

drive は、ディレクトリー・サーバー・インスタンス作成時に指定したドライブです。*instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

IBM Security Directory Server クライアントが存在するシステムから逸失および検出エラー・ログを表示するには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readlog -log LostAndFound -lines all
```

逸失および検出エラー・ログをクリアするには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op clearlog -log LostAndFound
```

サーバー・エラー・ログの表示:

デフォルトの場所にある構成ツールのログを表示するには、以下のコマンドを実行します。

このタスクについて

UNIX オペレーティング・システムの場合。

```
more <instance base directory>/idsslapd-<instance name>/logs/ibmslapd.log
```

各部の意味を以下に示します。

- *instance base directory* は、ディレクトリー・サーバー・インスタンスの所有者のホーム・ディレクトリー、またはディレクトリー・サーバー・インスタンス作成時に指定したディレクトリーです。
- *instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

Windows オペレーティング・システムの場合。

```
more <drive>%idsslapd-<instance name>%logs%ibmslapd.log
```

drive は、ディレクトリー・サーバー・インスタンス作成時に指定したドライブです。*instance name* は、ディレクトリー・サーバー・インスタンスの名前です。

IBM Security Directory Server クライアントが存在するシステムからエラー・ログを表示するには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op readlog -logslapd-lines all
```

エラー・ログをクリアするには、以下のステップを実行します。

```
idsldapexop -D <adminDN> -w <adminPW> -op clearlog -logslapd
```

CBE および CARS フォーマットへのログの統合

問題判別アーキテクチャー用のデータ・フォーマットを標準化するため、IBM では、Common Base Event (CBE) フォーマットという、ログおよびトレース情報の共通フォーマットを導入しました。このフォーマットにより、類似するフィールド間で整合性が生まれ、複数のログ間の相関性が向上します。

注: Security Directory Server ログの CBE および CARS との統合は、非推奨となりました。

IBM は、自己管理環境を形成するために、「オートノミック・コンピューティング」を導入しました。オートノミック・コンピューティングとは、オープン・スタンダード・ベースのアーキテクチャーであり、これを取り入れたシステムはシステム自体を構成、修復、最適化、および保護できます。システムのさまざまなコンポーネントの状態を判別するために、イベント・データのフォーマットを標準化し、システムが現在の状態を解決できるようにすることが必要です。

CBE は 3-tuple 構造化フォーマットに基づいています。

- 状態によって影響を受けるコンポーネント (ソース)
- 状態を監視するコンポーネント
- 状態データ (関連情報を使用して状態を説明するプロパティ)

3-tuple フォーマットを使用すると、障害が起こったコンポーネントを分離できるリソース独立管理関数を作成および実装できるようになります。

IBM Security Directory Server をオートノミック・コンピューティング・スペース向けに調整するには、エラー・ログや監査ログなどのログを IBM Security Directory Server 製品で生成し、これらのログが CBE フォーマットで提供されるようにします。

IBM Common Auditing and Reporting Service (CARS) コンポーネントは、IBM が提案するイベントの共通フォーマットである CBE と、IBM Common Event Infrastructure (CEI) テクノロジーとを活用して、監査インフラストラクチャーを提供します。CBE の目的は、企業内で異なるコンポーネント間の効果的な相互通信を促進することです。監査データを効果的に処理するために、CARS コンポーネントには CBE フォーマットの監査データが必要です。CEI は、CBE イベントの送信、永続的ストレージ、照会、およびサブスクリプション用の IBM の戦略イベント・インフラストラクチャーです。CARS コンポーネントは、イベントの送信に CEI インターフェースを使用します。これらのイベントは、CEI サーバーで構成オプションを使用することにより、監査可能と示すことができます。CEI サーバーは監査要件を満たす CEI XML イベント・ストアにイベントを保管します。

CARS コンポーネントでは、CEI XML イベント・ストアからレポート・テーブルにデータをステージングできます。IBM の製品およびお客様は、レポート・テーブ

ルにステージングされた監査可能イベントに基づく監査レポートを提供できます。CARS コンポーネントでは、監査可能イベントのライフ・サイクルの管理もサポートされます。これには、アーカイブ、復元、および復元されたアーカイブについてのレポートの監査が含まれます。

IBM Security QRadar SIEM は、ネットワーク全体に分散された多数のデバイス、エンドポイント、およびアプリケーションからのログ・ソース・イベント・データを統合します。さらに、生データを即時に正規化して相関させ、真の脅威を誤検出から区別します。大規模な IT システムとネットワークの観点で、Security Directory Server でのアクティビティを相互に関連付けるには、Security Directory Server インスタンスの監査ログ・ファイルを QRadar サーバー・インスタンスの監査ログと統合する必要があります。

CBE、CEI、および CARS 機能のログ管理ツール

IBM Security Directory Server インスタンスに対して CBE、CEI、および CARS の各機能を開始するには、IBM Security Directory Server ログ管理ツールである **idslogmgmt** を実行する必要があります。

注: 1 つの IBM Security Directory Server インスタンス上で実行できる **idslogmgmt** インスタンスは 1 つのみです。また、管理ツール・ログを管理する **idslogmgmt** インスタンスは、1 つのみ実行できます。

CBE、CEI、CARS、および QRadar の各機能をインプリメントするには、**idslogmgmt** ラッパーを使用して、IBM Security Directory Integrator サーバーおよびアセンブリ・ラインを起動する必要があります。ログ管理アセンブリ・ラインは、まずラッパー・スクリプトによって渡されたパラメーターを読み取り、処理します。次に、ログ管理アセンブリ・ラインは、Security Directory Server インスタンスのリポジトリ・ファイルを読み取ります。アセンブリ・ラインは、インストールされているサーバーに関連付けられたログ管理ツールのバージョンを判別します。サーバーのリスト用に、`ibmslapd.conf` が読み取られ、ログ管理設定が取得されます。ツールは、IBM Security Directory Server インスタンスの構成ファイル内の設定更新を定期的な間隔で検査します。デフォルトの間隔は 5 分です。`IDSLMG_CHECK_INTERVAL` 変数が設定されている場合、この変数に設定されている値が優先されます。CARS のインストールおよび構成についての詳細は、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。

`ibmslapd.conf` ファイルからログ管理の構成設定が読み取られると、ツールはログの場所を検索し、適切なログ管理アクティビティを実行します。アクティビティには、ログ・ディスク・スペースの使用量の管理や、専有フォーマットのログ・データを CBE フォーマットに変換し、そのデータをファイルまたは CEI サーバーに送信することも含まれます。また、アクティビティには、サーバー監査ログ・データを QRadar が使用する `syslog` 形式に変換することも含まれます。

注: 管理サーバーの監査ログ・データは、QRadar との統合の場合、`syslog` に変換されません。

idslogmgmt ツールの実行中には、プロセス ID が含まれる `pid` ファイル `idslogmgmt.pid` が作成され、`<instance home>%tmp` ディレクトリー内で更新されません。この `pid` ファイルは、ステータス・アクションがログ管理拡張操作で指定され

ている場合に、IBM Security Directory Server インスタンスで実行または停止される **idslogmgmt** を判別するのに役立ちます。このプロセスはインスタンス固有の **idslogmgmt** の実行のみに適用され、管理ツール・パラメーターが指定されている場合の実行には適用されません。Common Base Event (CBE) に関する特殊なケースのシナリオについて詳しくは、IBM Security Directory Server の資料の『トラブルシューティングとサポート』セクションで、Common Base Event (CBE) 機能についてのセクションを参照してください。

ログ管理の項目

CBE、CEI、および CARS 機能に関連付けられているログ管理属性は、属性に応じて各種ログ項目の下に置かれます。

cn=default, cn=Log Management, cn=configuration

個々のログ項目内で明示的に設定を指定することにより上書きしない限り、すべてのログ管理項目に適用されます。

cn=<specific_log_name>, cn=Log Management, cn=configuration

項目で指定されたログのみに適用されます。このログのデフォルト設定は、この項目の設定を指定することにより上書きできます。 <specific_log_name> の値は、ibmslapd、audit、tools、bulkload、admin、admin audit、db2cli、replication、および ddsetup です。

QRadar の統合に関連付けられている構成属性は、cn=Audit、cn=Log Management、cn=Configuration の下でのみ配置できます。

CARS レポート

この機能では、CARS レポートを生成します。

CARS レポートでは必須の CBE プロパティが生成されます。CBE プロパティにマップされている Security Directory Serve ログ項目は、以下のプロパティに分類されます。

- **基本プロパティ**：基本プロパティ・テーブルには、CBE v1.0.1 仕様の一部であるプロパティがリストされます。
- **セキュリティー拡張プロパティ**：セキュリティー拡張プロパティ・テーブルには、Security Events v0.21 仕様の CBE 拡張の一部であるプロパティがリストされます。

プロパティは XPath 文で表されます。これは、CBE 内のどの位置にそのプロパティがあるのかを記述したものです。

CBE フォーマット化された出力例:

監査レコードの CBE フォーマット化された出力の以下の例を参照してください。

```
AuditV3--2005-11-14-18:27:37.444-06:00--V3 Bind--bindDN:
cn=root--client: 127.0.0.1:1193--connectionID:
1--received: 2005-11-14-18:27:37.444-06:00--Success
controlType: 1.3.6.1.4.1.42.2.27.8.5.1
criticality: false
name: cn=root
authenticationChoice: simple
Admin Acct Status: Not Locked

<?xml version="1.0" encoding="UTF-8"?>
<CommonBaseEvent creationTime="2005-11-14T12:27:37"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonbaseevent1_0.xsd"
```

```

globalInstanceId="i00000000000000000000000000000000"
sequenceNumber="00000000000000000000000000000001"
extensionName="SECURITY_AUDIT_AUTHN">
<sourceComponentId component="Official Product Name"
subcomponent="audit"
componentIdType="ProductName"
componentType="http://www.ibm.com/namespace/autonomic/Security_componentTypes"
location="127.0.0.1:389"
locationType="IPV6"
instanceId="ldapdev"/>
<situation categoryName="ConnectSituation">
<situationType reasoningScope="EXTERNAL"
successDisposition="SUCCESSFUL"
situationDisposition="AVAILABLE"/>
</situation>
<extendedDataElements name="action">
<values>authentication</values>
</extendedDataElements>
<extendedDataElements name="authnType">
<values>ldap_3.0</values>
</extendedDataElements>
<extendedDataElements name="outcome">
<result>SUCCESSFUL</result>
</extendedDataElements>
<extendedDataElements name="outcome">
<failureReason>authenticationFailure</failureReason>
</extendedDataElements>
<extendedDataElements name="resourceInfo">
<children name="type">
<values>application</values>
</children>
<children name="nameInPolicy">
<values>ldap</values>
</children>
<children name="nameInApp">
<values>ldap</values>
</children>
</extendedDataElements>
<extendedDataElements name="userInfo">
<children name="appUserName">
<values>cn=root</values>
</children>
<children name="proxyUserName">
<values>NOT AVAILABLE</values>
</children>
<children name="registryUserName">
<values>NOT AVAILABLE</values>
</children>
<children name="sessionId">
<values>1</values>
</children>
<children name="location">
<values>127.0.0.1:1193</values>
</children>
<children name="locationType">
<values>IPV6</values>
</children>
</extendedDataElements>
</CommonBaseEvent>

```

CBE、CARS、および QRadar のログ管理属性の構成

以下に示す手順を使用することにより、CBE、CARS、および QRadar のログ管理属性を構成することができます。

Web 管理の使用:

以下に示す手順に従うことにより、Web 管理ツールを使用して、CBE および CARS 機能のログ管理属性を構成することができます。

このタスクについて

ここでは、管理サーバー・ログの例を考えます。選択するログに応じて、パネルに表示されるコントロールは多少異なる場合があります。

以下をまだ実行していない場合には、実行します。

手順

1. Web 管理ナビゲーション領域の「**サーバー管理**」をクリックしてから、展開されたリスト上で「**ログ**」をクリックします。
2. 「**ログ設定の変更**」をクリックします。
3. ログのリストから、「**管理サーバー・ログ**」を選択します。

タスクの結果

管理サーバー・ログを変更するには、以下を行います。

1. 管理サーバー・ログのパスおよびファイル名を入力します。
2. 「**ログ・サイズしきい値 (MB)**」で、以下のオプションのいずれかを選択します。
 - 横にある編集フィールド付きのラジオ・ボタンを選択し、最大ログ・サイズをメガバイト単位で入力します。
 - デフォルトの制限を使用する場合は、ドロップダウン・メニューの横にあるラジオ・ボタンを選択します。ドロップダウン・メニューから「**デフォルト**」を選択します。
 - ログ・サイズに制限を設定しない場合は、ドロップダウン・メニューの横にあるラジオ・ボタンを選択します。ドロップダウン・メニューから「**無制限**」を選択します。
3. 「**最大ログ・アーカイブ**」で以下のオプションのいずれかを選択します。
 - 横にある編集フィールド付きのラジオ・ボタンを選択し、保存するアーカイブの最大数を入力します。1 つのアーカイブ・ログは、サイズしきい値に達した古いログです。
 - デフォルトの最大ログ・アーカイブ値を使用する場合は、ドロップダウン・メニューの横にあるラジオ・ボタンを選択します。ドロップダウン・メニューから「**デフォルト**」を選択します。
 - ログをアーカイブしない場合は、ドロップダウン・メニューの横にあるラジオ・ボタンを選択します。ドロップダウン・メニューから「**アーカイブなし**」を選択します。
 - アーカイブ・ログの数を制限しない場合は、ドロップダウン・メニューの横にあるラジオ・ボタンを選択します。ドロップダウン・メニューから「**無制限**」を選択します。
4. 「**ログ・アーカイブ・パス**」で以下のオプションのいずれかを選択します。
 - アーカイブの保管先パスを指定する場合は、編集ウィンドウの隣にあるラジオ・ボタンを選択し、必要なパスを入力します。
 - ログ・ファイルがあるディレクトリーにアーカイブを保管する場合は、「**デフォルト・パス**」ラジオ・ボタンを選択します。
5. 「**頻度の選択**」チェック・ボックスから項目を選択して、CBE 機能の 2 つのサイクルの頻度を指定します。
6. 「**開始日**」フィールドに、CBE 機能の開始日および開始時刻を指定します。カレンダー・アイコンをクリックして開始日を指定することもできます。開始時刻は **12:30:00 PM** の形式で指定します。
7. 完了したら、以下のステップのいずれかを行います。

- 「次へ」をクリックし、ログ設定の構成を続行します。
- 「完了」をクリックして変更内容を保管し、「ログ設定の変更」パネルに戻ります。
- 「キャンセル」をクリックしてこのパネルで行った変更を破棄し、「ログ設定の変更」パネルにナビゲートします。

イベント形式のログ・ファイルのログ設定を構成するには、以下のステップを実行します。

- 「ログ・レコードをイベント形式のログ・ファイルに送信」チェック・ボックスを選択して、ユーザーが CBE 形式のログ・ファイルを使用できるようにします。
- CBE 形式のログ・ファイルを格納するパス名を「ファイル・パス」フィールドに指定します。
- CBE 形式のログのファイル名を「ファイル名接頭部」フィールドに指定します。
- 「ログ・サイズしきい値 (MB)」に、CBE 形式のログ・ファイルのしきい値サイズを MB 単位で指定します。サイズ制限を MB 単位で指定する場合、オプションを選択して、フィールドに数値を指定します。選択しない場合は「無制限」を選択します。
- CBE 形式のログをアーカイブする最大数を指定します。アーカイブするログの最大数を指定する場合、オプションを選択して、フィールドに数値を指定します。無制限に設定するには「無制限」を選択します。
- CBE 形式のログをアーカイブするパス名を指定します。パス名を指定する場合、オプションを選択して、アーカイブするログの絶対パス名を入力します。ログ・ファイルと同じアーカイブ・パスを指定するには、「ログ・ファイルと同じディレクトリー」を選択します。
- CBE 形式のログのログ・レベルを指定します。使用可能なログ・レベルは、「高」、「中」、「低」です。
- 完了したら、以下のステップのいずれかを行います。
 - 「戻る」をクリックし、前のパネルに戻ります。
 - 「次へ」をクリックし、ログ設定の構成を続行します。
 - 「完了」をクリックして変更内容を保管し、「ログ設定の変更」パネルに戻ります。
 - 「キャンセル」をクリックしてこのパネルで行った変更を破棄し、「ログ設定の変更」パネルにナビゲートします。

注:

- ログ・アーカイブ・パスに値を入力しないと、デフォルト値が割り当てられません。
- 数値の指定が必要なフィールドに 0 を設定すると、「最大ログ・アーカイブ」以外は「無制限」とみなされます。「最大ログ・アーカイブ」では、0 は「アーカイブなし」とみなされます。

共通監査およびレポート・サービスを構成するには、以下を実行します。

- 「ログ・レコードを共通監査およびレポート・サービスに送信」チェック・ボックスを選択して、CBE 機能で Security Directory Server 専有形式のログを読み取り、CBE 形式に変換して CEI サーバーに書き込みできるようにします。
- 「ホスト」フィールドに、CEI サーバーのホスト名を入力します。
- 「ポート」フィールドに、CEI サーバーが listen するポート番号を入力します。
- CBE 形式のログのログ・レベルを指定します。使用可能なログ・レベルは、「高」、「中」、「低」です。
- 完了したら、以下のステップのいずれかを行います。
 - 「戻る」をクリックし、前のパネルに戻ります。
 - 「完了」をクリックして変更内容を保管し、「ログ設定の変更」パネルに戻ります。
 - 「キャンセル」をクリックしてこのパネルで行った変更を破棄し、「ログ設定の変更」パネルにナビゲートします。

注: Web 管理ツールを使用した QRadar 統合機能の構成は、サポートされていません。

Web 管理ツールを使用してログ管理を開始または停止するには:

Web 管理ツールを使用してログの管理を開始または停止するには、以下の手順を実行します。

このタスクについて

Web 管理ナビゲーション領域の「サーバー管理」の「ログ」をクリックし、展開されたリスト上で「ログ管理の開始/停止」をクリックします (この操作をまだ実行していない場合)。

AuditAdmin または ServerConfigGroupMember の役割を持つ 1 次管理者グループおよびローカル管理グループのメンバーは、このパネルを使用してログ管理サービスを開始および停止できます。

ログ管理サービスを開始または停止するには、以下を実行します。

- 以下のステップのいずれかを実行します。
 - ログ管理サービスが実行中の場合は、「停止」をクリックしてサービスを停止します。
 - ログ管理サービスが停止している場合は、「開始」をクリックしてサービスを開始します。
- 「概要」パネルに戻るには「閉じる」をクリックします。

コマンド・ラインの使用:

コマンド行を使用して CBE 昨日と CARS 機能の属性値を設定するには、以下の手順を実行します。

このタスクについて

CBE および CARS 機能の属性値を設定するには、以下のようになります。

```
#idsldapmodify -h <host_name> -p <portnumber>-D <cn=RDN_value> -w <password> ¥  
-f <file_name>
```

ここで、<file_name> の内容は以下のとおりです。

```
dn: cn=<specific_log_name>,cn=Log Management, cn=configuration  
ibm-slapdLogEventFileEnabled: true  
-  
add: ibm-slapdLogCARSEnabled  
ibm-slapdLogCARSEnabled: false  
-  
add: ibm-slapdLogEventFormat  
ibm-slapdLogEventFormat: CBE  
-  
add: ibm-slapdLogMgmtStartTime  
ibm-slapdLogMgmtStartTime: 200609010000  
-  
add: ibm-slapdLogMgmtFrequency  
ibm-slapdLogMgmtFrequency: 20  
-  
add: ibm-slapdLogEventFileSizeThreshold  
ibm-slapdLogEventFileSizeThreshold: 2  
-  
add: ibm-slapdLogEventFileMaxArchives  
ibm-slapdLogEventFileMaxArchives: 2  
-  
add: ibm-slapdLogEventFileArchivePath  
ibm-slapdLogEventFileArchivePath: <path_name>/TempDir  
-  
add: ibm-slapdLogEventFileOptions  
ibm-slapdLogEventFileOptions: <h|m|l>  
-  
add: ibm-slapdLogEventFilePath  
ibm-slapdLogEventFilePath: /home/inst1/idsslapd-<instance_name>/logs  
-  
add: ibm-slapdLogEventFilePrefix  
ibm-slapdLogEventFilePrefix: <log_name>  
-  
add: ibm-slapdLogSizeThreshold  
ibm-slapdLogSizeThreshold: 1  
-  
add: ibm-slapdLogMaxArchives  
ibm-slapdLogMaxArchives: 1  
-  
add: ibm-slapdLogArchivePath  
ibm-slapdLogArchivePath: <path_name>/TempDir1
```

QRadar 統合の属性値を設定するには、まず次のようにして、補助オブジェクト・クラス `ibm-slapdQRadarConfig` を `cn=Audit, cn=Log Management, cn=Configuration` に追加します。

```
#idsldapmodify -h host_name -p portnumber -D cn=RDN_value -w password ¥  
-f file_name
```

ここで、file_name の内容は以下のとおりです。

```
dn: cn=Audit, cn=Log Management, cn=Configuration  
changetype: modify  
add: objectclass  
objectclass: ibm-slapdQRadarConfig
```

QRadar 統合の属性値を設定するには、以下のようになります。

```
#idsldapmodify -h host_name -p portnumber -D cn=RDN_value -w password ¥  
-f file_name
```

ここで、file_name の内容は以下のとおりです。

```
dn: cn= specific_log_name ,cn=Log Management, cn=configuration  
ibm-slapdLogEventQRadarEnabled: true  
-  
add: ibm-slapdLogEventQRadarHostName  
ibm-slapdLogEventQRadarHostName: host_name_of_qradar_instance  
-  
add: ibm-slapdLogEventQRadarPort  
ibm-slapdLogEventQRadarPort: port_of_qradar_instance
```

```
-  
add: ibm-slapdLogEventQRadarMapFilesLocation  
ibm-slapdLogEventQRadarMapFilesLocation: directory_location_of_qradar_mapfiles
```

インスタンスを開始するには、以下のようにします。

```
ibmslapd -I <instance_name> -n
```

ログ管理はローカル側でもリモート側でも開始できます。ログ管理を開始するには、以下のコマンドを実行します。

```
idslogmgmt -I <instance_name>
```

リモート側でログ管理を開始して、ステータスを取得し、停止するには、以下のコマンドを実行します。

```
ibmdirctl -D <adminDN> -w <password> -h <host_name> %  
-p <administration server port number> startlogmgmt
```

```
ibmdirctl -D <adminDN> -w <password> -h <host_name> %  
-p <administration server port number> statuslogmgmt
```

```
ibmdirctl -D <adminDN> -w <password> -h <host_name> %  
-p <administration server port number> stoplogmgmt
```


第 3 章 ディレクトリー管理

ここで提供されている情報を使用して、ディレクトリー管理についての詳細を知ることができます。さらに、ディレクトリー項目の処理、アクセス制御、検索制限の管理、およびプロキシー許可の管理についてもここで詳しく説明します。

ディレクトリー項目

「項目の管理」を選択すると、実行するすべてのディレクトリー項目タスクにアクセスできます。

Web 管理ツールのナビゲーション領域の「ディレクトリー管理」カテゴリを展開します。項目の追加および項目の検索の特定のタスクには、ナビゲーション領域に 2 つのショートカットが追加されています。

ディレクトリー項目に対しては、以下の操作を実行できます。

- ディレクトリー・ツリーのブラウズ
- 項目の追加または除去
- 項目への補助オブジェクト・クラスの追加または除去
- 項目の属性の編集
- 項目のコピー
- メンバーの管理
- メンバーシップの管理
- ACL の編集
- 項目の検索

ツリーのブラウズ

Web 管理ツールのナビゲーション・ツリーをブラウズすると、実行するすべてのディレクトリー項目タスクにアクセスできます。

手順

1. ナビゲーション領域で「ディレクトリー管理」カテゴリを展開します。
2. 「項目の管理」をクリックします。

「項目の管理」テーブルには以下の列情報が表示されます。

オプション	説明
選択	表示、編集、コピー、または削除する属性の名前の横にあるラジオ・ボタンを選択します。
展開	拡張可能な項目を示します。拡張可能な項目とは、子項目を持つ項目です。 注: + 記号が表示されている場合でも、ACL で子項目の参照が許可されていない場合は、その子項目は参照できません。

オプション	説明
RDN	項目の相対識別名 RDN を表示します。
オブジェクト・クラス	項目のオブジェクト・クラスを表示します。
作成	項目が作成された日付をリストします。
変更	項目が最後に変更された日付をリストします。
変更者	最後に項目を変更したユーザーの ID をリストします。

- サブツリーを選択して「**拡張**」をクリックすると、サブツリーの 1 つ下のレベルを表示できます。
- 「**縮小表示/移動**」をクリックして、サブツリー階層の 1 つ上のレベルに移動します。
- 「**検索**」をクリックして、作業対象の項目を検索します。

詳細については、541 ページの『ディレクトリー項目の検索』を参照してください。

- 項目を選択し、ツールバーまたは「**アクションの選択**」ドロップダウン・メニューから、実行する操作を選択します。

項目の追加

この機能を使用すると、項目を追加できます。

Web 管理を使用した項目の追加

Web 管理ツールを使用して、ユーザー項目を追加します。

このタスクについて

ナビゲーション領域で「**ディレクトリー管理**」カテゴリーを展開します。

手順

- 「**項目の追加**」をクリックします。
- メニューからフィルター・オブジェクト・クラスを選択して、「**再表示**」をクリックします。
- リスト・ボックスから**構造化オブジェクト・クラス**を 1 つ選択します。
- 「**次へ**」をクリックします。
- メニューからフィルター・オブジェクト・クラスを選択して、「**再表示**」をクリックします。
- 「**使用可能**」ボックスから、使用する任意の「**補助オブジェクト・クラス**」を選択して、「**追加**」をクリックします。追加する補助オブジェクト・クラスごとにこのプロセスを繰り返します。補助オブジェクト・クラスを選択して、「**除去**」をクリックすることで、「**選択済み**」ボックスから補助オブジェクト・クラスを削除することもできます。
- 「**次へ**」をクリックする。
- 「**相対 DN**」フィールドに、追加する項目の相対識別名 (RDN) を入力します。例えば、cn=John Doe です。

9. 「親 DN」フィールドに、選択したツリー項目の識別名を入力します。例えば、ou=Austin, o=sample です。「ブラウズ」をクリックして、リストから「親 DN」を選択することもできます。選択を展開して、サブツリーの下位にある他の選択項目を表示することもできます。選択項目を指定して「選択」をクリックし、必要な「親 DN」を指定します。デフォルトでは、「親 DN」には、ツリー内で選択されている項目が設定されます。

注: このタスクを「項目の管理」パネルから開始した場合、このフィールドは事前に入力されています。「親 DN」を選択してから、「追加」をクリックして項目の追加プロセスを開始します。ただし、サーバーが **modifyDN** 操作をサポートしている場合 (IBM Security Directory Server バージョン 6.0 以降)、項目がリーフ・ノードでもそのフィールドは変更可能です。つまり、下位に項目がない場合、その項目は別の「親 DN」項目に移動できます。

10. 「必須属性」タブで、属性の値を入力します。
 - a. 属性が複数值で、特定の属性に複数の値を追加する場合は、「複数值」をクリックします。528 ページの『属性の複数值の追加』を参照してください。
 - b. 属性がバイナリー・データを必要とする場合は、「バイナリー・データ」をクリックします。528 ページの『属性のバイナリー・データ』を参照してください。
 - c. サーバーで言語タグが使用可能な場合は、「言語タグ値」をクリックして言語タグ記述子を追加または除去します。詳細については、530 ページの『言語タグ』および 532 ページの『言語タグ値の追加』を参照してください。
 - d. 属性に参照が含まれる場合は、「参照の管理」をクリックします。詳細については、301 ページの『参照』および 306 ページの『デフォルト参照の作成』を参照してください。
11. 「オプションの属性」をクリックします。
12. 「オプションの属性」タブで、他の属性の値を必要に応じて入力します。
13. 「完了」をクリックすると、項目が作成されます。
14. 項目が正常に追加されると、類似の項目を追加するためのプロンプトが出されます。類似の項目を追加するには「はい」をクリックします。終了して「項目の管理」パネルに戻るには、「いいえ」をクリックします。

コマンド行を使用した項目の追加

コマンド行を使用して、項目を追加できます。

手順

次のコマンドを実行します。

```
idsldapadd -D adminDN -w adminPW -i  
filename
```

ここで、*filename* には、以下の情報が含まれます。

```
dn: cn=John Doe, ou=Austin, o=sample  
cn: John Doe  
objectclass: inetOrgPerson  
objectclass: organizationalPerson  
objectclass: person  
objectclass: top  
sn: Doe
```

属性の複数値の追加

属性が複数値をサポートしている場合は、特定の属性に複数の値を追加できます。

このタスクについて

手順

1. 「複数値」をクリックします。
2. 属性の追加の値を指定します。
3. 「追加」をクリックします。
4. 追加する各値に対してこのステップを繰り返します。
5. 完了したら、「OK」をクリックします。

これらの値は、属性の下に表示されるドロップダウン・メニューに追加されます。特定の属性の値を 1 つ以上除去することもできます。

6. 値を除去するには、「複数値」をクリックします。
7. 除去する値を選択します。
8. 「除去」をクリックします。
9. 除去する各追加値について、このステップを繰り返します。
10. 「OK」をクリックします。

これらの値は、属性の下に表示されるドロップダウン・メニューから除去されます。ドロップダウン・メニューには、残りの値が表示されます。属性に割り当てられている値が 1 つのみであるか、全くない場合、ドロップダウン・メニューは表示されなくなります。

注: 「言語タグ付きで表示」メニューで言語値タグを選択すると、追加または除去する属性にその言語タグが関連付けられます。言語値タグの追加についての詳細は、532 ページの『言語タグ値の追加』を参照してください。

属性のバイナリー・データ

以下の説明を参照して、以下の手順を実行すると、属性のバイナリー・データを処理できます。

Web 管理の使用

Web 管理ツールを使用して、以下の手順を実行すると、属性のバイナリー・データを処理できます。

このタスクについて

属性がバイナリー・データを必要とする場合は、「バイナリー・データ」 ボタンが属性フィールドの横に表示されます。属性にデータが含まれていない場合、フィールドはブランクです。バイナリー属性は表示できないので、属性にバイナリー・データが含まれる場合は、フィールドに「バイナリー・データ 1」と表示されます。属性に複数の値が含まれる場合は、フィールドがドロップダウン・リスト形式で表示されます。

バイナリー属性を処理するには、「バイナリー・データ」ボタンをクリックします。

バイナリー・データをインポート、エクスポート、または除去することができます。

属性にバイナリー・データを追加するには、以下の手順を実行します。

手順

1. 「バイナリー・データ」ボタンをクリックします。
2. 「インポート」をクリックします。
3. 該当するファイルのパス名を入力するか、「ブラウズ」をクリックして、バイナリー・ファイルを検索して選択します。
4. 「ファイルの実行依頼」をクリックします。「ファイルがアップロードされました」というメッセージが表示されます。
5. 「閉じる」をクリックします。「バイナリー・データ項目」の下の表に「バイナリー・データ 1」が表示されます。
6. 追加するバイナリー・ファイルの数だけインポート・プロセス (ステップ 2 から 5) を繰り返します。以降の項目は、「バイナリー・データ 2」、「バイナリー・データ 3」などとしてリストされます。
7. バイナリー・データの追加が完了したら、「OK」をクリックします。

タスクの結果

最初のバイナリー・データ・ファイルのインポート後、2 つの追加操作を実行できるようになります。バイナリー・データのエクスポートと除去です。

バイナリー・データをエクスポートするには、以下の手順を実行します。

1. まだ行っていない場合は、「バイナリー・データ」ボタンをクリックします。
2. エクスポートするバイナリー・ファイルを選択します。
3. 「エクスポート」をクリックします。
4. 「ダウンロードするバイナリー・データ」リンクをクリックします。
5. バイナリー・ファイルを表示、または新しい場所に保存するには、ウィザードの指示に従います。
6. 「閉じる」をクリックします。
7. エクスポートするバイナリー・ファイルの数だけエクスポート・プロセスを繰り返します。
8. データのエクスポートが完了したら、「OK」をクリックします。

バイナリー・データを除去するには、以下の手順を実行します。

1. まだ行っていない場合は、「バイナリー・データ」ボタンをクリックします。
2. 除去するバイナリー・データ・ファイルにチェック・マークを付けます。このタスクの場合は、複数のファイルを選択できます。
3. 「削除」をクリックします。
4. 削除を確認するプロンプトが出されたら、「OK」をクリックします。削除のマークが付けられたバイナリー・データがリストから除去されます。

5. データの削除が完了したら、「OK」をクリックします。

注: バイナリー属性は検索できません。

コマンド行の使用による属性へのバイナリー・データの追加

属性がバイナリー・データを必要とする場合は、コマンド行を使用して、属性のバイナリー・データを追加できます。

手順

バイナリー・データを追加するには、以下のコマンドを実行します。

```
idsldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

ここで、*filename* には、以下の詳細情報が含まれます。

```
dn: cn=Bob Garcia, ou=deptABC, ou=Austin, o=sample
changetype: modify
add: jpegphoto
jpegphoto:< file:///usr/local/directory/photos/Bob.jpg
```

言語タグ

言語タグについては、以下の説明で詳細を把握できます。

注:

1. 言語タグを正しく機能させるには、データベースを UTF-8 データベースとして構成する必要があります。
2. 言語タグを使用可能にしてから、言語タグを項目の属性に関連付けると、サーバーは言語タグが付いた項目を返します。後で言語タグ機能を使用不可にした場合でも、言語タグ付きの項目が戻されます。言語タグ機能を使用可能にしてからは、使用不可にしないでください。

言語タグという用語は、自然言語コードとディレクトリー内に格納されている値とをディレクトリーが関連付けるための仕組みや、自然言語の特定の要件に合致する値をクライアントがディレクトリーで照会できるようにする仕組みと定義されています。言語タグは、属性記述子のコンポーネントです。言語タグは、接頭辞 **lang-**を持ち、英字の基本サブタグと、ハイフン (-) でつながれたサブタグが続く場合もあります。後置のサブタグには、任意の英数字を組み合わせることができます。英字にする必要があるのは、先頭の基本サブタグのみです。サブタグの長さに制限はありませんが、タグ全体の長さは 240 文字以下にしてください。言語タグでは大/小文字は区別されないため、en-us、en-US、EN-US は同一とみなされます。言語タグを DN または RDN のコンポーネントに組み込むことはできません。属性記述子当たりに許可される言語タグは 1 つのみです。

注: 言語タグは、固有属性と相互に排他的です。特定の属性を固有属性として指定した場合、その属性に言語タグを関連付けることはできません。

ディレクトリーに追加されたデータに言語タグが含まれている場合、特定の言語では、その言語タグを検索操作で使用することで選択的に属性値を取得できます。検索で要求された属性リストの属性の説明に言語タグが指定されている場合は、同じ言語タグを持つディレクトリー項目の属性値が返されます。したがって、以下のような検索を実行した場合、

```
idsldapsearch -b "o=sample" (objectclass=organization) description;lang=en
```

サーバーは属性「description;lang-en」の値を返しますが、属性 **description** や **description;lang-fr** の値は返しません。

言語タグなしで属性を指定して要求を行った場合は、すべての属性値がその言語タグとは無関係に戻されます。

属性タイプと言語タグは、セミコロン (;) 文字で分離されています。

注: RFC2252 では、AttributeType の「NAME」パートにセミコロン文字を使用することが許されています。しかし、この文字は AttributeType と言語タグを分離するために使用されるため、現在 AttributeType の「NAME」パートで使用することは許されていません (draft-ietf-ldapbis-models-07.txt を参照)。

例えば、クライアントが「description」属性を要求し、一致する項目に以下の内容が含まれていた場合、

```
objectclass: top
objectclass: organization
o: Software GmbH
description: software
description;lang-en: software products
description;lang-de: Softwareprodukte
postalAddress: Berlin 8001 Germany
postalAddress;lang-de: Berlin 8001 Deutschland
```

サーバーは、以下の内容を返します。

```
description: software
description;lang-en: software products
description;lang-de: Softwareprodukte
```

検索で「**description;lang-de**」属性を要求した場合、サーバーは以下の内容を返します。

```
description;lang-de: Softwareprodukte
```

このタイプのサーバー処理により、マルチリンガル・データを含むディレクトリーが使用可能になり、各種の言語で動作するクライアントがサポートされます。アプリケーションが正しくインプリメントされている場合、ドイツ語クライアントには属性 **lang-de** で入力されたデータのみが表示され、フランス語クライアントには **lang-fr** 属性で入力されたデータのみが表示されます。

言語タグ機能が使用可能であるかどうかを確認するには、属性 **ibm-enabledCapabilities** を指定してルート DSE 検索を発行します。

```
idsldapsearch -b "" -s base objectclass=* ibm-enabledCapabilities
```

OID 「1.3.6.1.4.1.4203.1.5.4」が戻された場合は、言語タグ機能は使用可能です。

言語タグ・サポートが使用可能でない場合は、言語タグを属性に関連付ける LDAP 操作が拒否され、以下のエラー・メッセージが表示されます。

```
LDAP_NO_SUCH_ATTRIBUTE
```

言語タグを関連付けられない属性

以下を参照して、言語タグを関連付けられない属性のリストを把握します。

以下の属性には言語タグを関連付けられません。

- objectclass
- member

- uniquemember
- memberURL
- ibm-memberGroup
- userpassword
- secretkey
- ref
- 運用属性
- 構成属性
- バイナリー属性

言語タグを関連付けられない属性のリストを生成するには、次のコマンドを使用します。

```
idsldapexop -op getattributes -attrType language_tag -matches true
```

言語タグ値の追加

属性でサポートされている場合には、言語タグ値を追加する必要があります。言語タグを使用すると、自然言語コードとディレクトリー内に格納されている値とを、ディレクトリーで関連付けることができます。

手順

1. 「言語タグ値」をクリックします。
2. 「言語タグ」フィールドに、作成するタグの名前を入力します。タグは、接頭部 lang- で始まっている必要があります。
3. 「値」フィールドにタグの値を入力します。
4. 「追加」をクリックします。
5. 属性の「複数值」機能が使用可能になっている場合は、必要に応じて値の追加を繰り返します。「複数值」ボタンが使用不可の場合、入力できる言語タグ値は 1 つのみです。528 ページの『属性の複数值の追加』を参照してください。
6. 「OK」をクリックして値を適用します。

注: 「OK」をクリックしないと、属性値は保管されません。

タスクの結果

「言語タグ付きで表示」メニューに値が追加されます。「言語タグ付きで表示」メニューを展開し、言語タグを選択します。「表示の変更」をクリックすると、その言語タグに対して入力した属性値が表示されます。この表示画面で追加または除去した値は、選択した言語タグにのみ適用されます。属性が言語タグ値をサポートしていて、特定の属性の言語タグ値を 1 つ以上除去したい場合は、533 ページの『言語タグ記述子の項目からの除去』を参照してください。

言語タグ付き属性を含む項目の検索

以下の情報を使用して、言語タグ付き属性を含む項目を検索します。

手順

1. 次のコマンドを入力します。

```
idsldapsearch -b "o=sample" "cn=Mark Anthony" sn
```

以下の結果が返されます。

```
cn=Mark Anthony,o=sample
sn=Anthony
sn;lang-spanish=Antonio
```

注: 出力には `sn;lang-spanish` のみが表示されます。

2. 次のコマンドを入力します。

```
idsldapsearch -b "o=sample" "sn;lang-spanish=Antonio"
```

以下の結果が返されます。

```
cn=Mark Anthony,o=sample
sn;lang-spanish=Antonio
```

注: 出力には `sn;lang-spanish` のみが表示されます。

3. 次のコマンドを入力します。

```
idsldapsearch -b "o=sample" "sn;lang-spanish=Antonio"
```

返される項目全体は以下のとおりです。

```
cn=Mark Anthony,o=sample
objectclass=person
objectclass=top
cn=Mark Anthony
sn=Anthony
sn;lang-spanish=Antonio
```

言語タグ記述子の項目からの除去

項目から言語タグ記述子を除去するには、以下のいずれかの方法を使用します。

手順

1. 項目全体を削除します。項目全体を削除する場合は、534 ページの『項目の削除』を参照してください。
2. オプション: 情報を表示して、項目全体が削除されていることを確認します。

Web 管理の使用:

以下の手順を実行することにより、項目からの言語タグ記述子の除去が、Web 管理ツールで実行できます。

手順

1. 「項目の管理」 > 「属性の編集」パス、または「項目の追加」 > 「構造化オブジェクト・クラスを選択」 > 「補助オブジェクト・クラスを選択」 > 「属性の入力」パスから、
2. 言語タグを除去する属性を選択します。
3. 「言語タグ値」をクリックして、「言語タグ値」パネルを表示します。
4. 「言語タグ」フィールドで、除去する言語タグをクリックします。
5. 「除去」をクリックします。言語タグとその値がメニュー・リストから除去されます。
6. 除去の対象となる言語タグごとに、手順 3 および 4 を繰り返します。
7. 完了したら、「OK」をクリックします。

コマンド・ラインの使用:

項目の属性を変更するには、`idsldapmodify` コマンドが使用できます。

手順

1. 次のコマンドを入力します。

```
idsldapmodify -D adminDN -w adminPW -i filename
```

ここで、*filename* には、以下の情報が含まれます。

```
dn: cn=Mark Anthony, o=sample  
changetype: modify  
delete:sn;lang-spanish  
sn;lang-spanish: Antonio
```

2. オプション: コマンドを実行したら、情報を表示して、内容を確認します。

タスクの結果

このアクションにより、値 Antonio を持つ属性 sn;lang-spanish が項目から除去されます。

項目の削除

この機能を使用すると、項目を削除できます。

コンソールにログインした際、「**Web 管理ツール**」では、ログオンしている項目の削除は許可されません。

次の詳細を使用してログオンしている場合、

```
cn=John Doe
```

```
ou=mylocale
```

```
o=mycompany,
```

```
c=mycountry
```

項目 cn=John Doe をツリーから削除しようとする、エラー・メッセージが表示されます。

注: John Doe の項目を削除する場合は、別のユーザーとしてログオンする必要があります。

Web 管理の使用

以下の説明を参照し、Web 管理を操作して、項目を削除します。

手順

1. ナビゲーション領域の「**ディレクトリー管理**」カテゴリーがまだ展開されていなければ展開します。続いて、「**項目の管理**」をクリックします。個々のサブツリーを展開すると、作業する項目 John Doe などを選択できます。
2. 「**削除**」をクリックします。
3. 「**OK**」をクリックして削除を確認します。

タスクの結果

項目が項目から削除され、項目のリストに戻ります。

コマンド・ラインの使用

idsldapdelete コマンドを使用して、リーフまたは非リーフ項目を削除します。

手順

1. 次のコマンドを入力します。

```
idsldapdelete -D adminDN -w adminPW "cn=John Doe, ou=Austin, o=sample"
```

削除する項目 "cn=John Doe, ou=Austin, o=sample" がリーフ項目でない場合、**delete** コマンドは失敗します。

2. 非リーフ項目を削除するには、以下のように **idsldapdelete** ユーティリティの **-s** オプションを使用します。

```
idsldapdelete -D adminDN -w adminPW -s "cn=John Doe, ou=Austin, o=sample"
```

タスクの結果

このコマンドにより、項目 "cn=John Doe, ou=Austin, o=sample" とそれに続くすべての項目が削除されます。

項目の変更

項目は、Web 管理とコマンド行を使用することで変更できます。

Web 管理の使用

以下の情報により、項目の変更を Web 管理で実行できます。

手順

1. ナビゲーション領域の「ディレクトリー管理」カテゴリがまだ展開されていない場合は展開します。続いて、「項目の管理」をクリックします。個々のサブツリーを展開すると、作業する項目を選択できます。「属性の編集」をクリックするか、RDN 列の項目の RDN 名をクリックして「属性の編集」パネルを開きます。
2. 「オブジェクト・クラス」メニューには、項目のオブジェクト・クラス継承が表示されます。オブジェクト・クラスは継承でソートされます。
3. 「相対 DN」フィールドで、編集する項目の相対識別名 (RDN) を変更します。例えば、cn=Bob Garcia を cn=Robert Garcia に変更します。
4. 「親 DN」フィールドに、選択したツリー項目の識別名が表示されます。サーバーが (IBM Security Directory Server バージョン 6.0 でサポート開始された) modifyDN 操作をサポートしている場合は、親 DN とリーフ・ノードの新規上位属性を変更できます。このフィールドを編集することも、以下のステップを実行して項目の親 DN を変更することもできます。
 - a. 「参照」をクリックします。
 - b. リストから親 DN を選択し、「選択」をクリックします。
5. 「必須属性」タブで、想定している属性の値を入力します。

注:

- a. 属性が複数值で、特定の属性に複数の値を追加する場合は、「複数值」をクリックします。528 ページの『属性の複数值の追加』を参照してください。

- b. 複数値属性の場合、属性が持つ値の数が、各属性に対して返す値の最大数の制限より多いと、属性の値は組み合わせボックスを使用して表示されます。表示される値の数は、この制限の値と同じになります。また、この属性の場合、「複数値」ボタンは表示されず、この属性値について切り捨てがあったことを示すメッセージが表示されます。
 - c. 属性がバイナリー・データを必要とする場合は、「バイナリー・データ」をクリックします。528 ページの『属性のバイナリー・データ』を参照してください。
 - d. サーバーで言語タグが使用可能な場合は、「言語タグ値」をクリックして言語タグ記述子を追加または除去します。詳しくは、530 ページの『言語タグ』 および 532 ページの『言語タグ値の追加』を参照してください。
 - e. 属性に参照が含まれる場合は、「参照の管理」をクリックします。詳しくは、301 ページの『参照』 および 306 ページの『デフォルト参照の作成』を参照してください。
6. 「オプションの属性」をクリックします。
 7. 「オプションの属性」タブで、他の属性の値を必要に応じて入力します。
 8. 「OK」をクリックすると、項目が変更されます。

注: 項目が持つ属性の数が、各項目に対して返す属性の最大数の制限より多い場合、その項目は属性のすべての値とともに返されます。この項目は、各項目に対して返す属性の最大数の制限に達するまで返されます。値が返されない属性は、パネルの下部に表示されます。これらの属性とともに、この項目が完全でないことを示すメッセージが表示されます。

コマンド・ラインの使用

RDN 項目を変更するには、`idsldapmodrdn` コマンドを使用します。

手順

1. 次のアクションを実行して、項目の名前を変更します。

項目の名前変更

項目の名前を変更する場合、例えば RDN を `cn=Bob Garcia` から `cn=Robert Garcia` に変更する場合は、次のコマンドを入力します。

```
idsldapmodrdn -D adminDN -w adminPW
-r "cn=Bob Garcia, ou=deptABC, ou=Austin, o=sample" "cn=Robert Garcia"
```

注: `-r` オプションでは、前の名前が除去されます。

2. 次のアクションを実行して、項目を移動します。

項目の移動

項目を移動する場合、例えば Bob を新規の部門に移動する場合、以下のコマンドを入力します。

```
idsldapmodrdn -D adminDN -w adminPW -s "ou=deptXYZ, ou=Austin,
o=sample" "cn=Bob Garcia, ou=deptABC, ou=Austin, o=sample" "cn=Bob Garcia"
```

項目は、次のコマンドを入力して移動することもできます。

```
idsldapmodify -D adminDN -w adminPW -i filename
```

ここで、`filename` には、以下の情報が含まれます。

```
dn: cn=Bob Garcia, ou=deptABC, ou=Austin, o=sample
changetype: modrdn
newrdn: cn=Bob Garcia
deleteoldrdn: 0
newsuperior: ou=deptXYZ, ou=Austin, o=sample
```

注: プロキシ環境で項目の名前変更または移動がサポートされるのは、区画をまたがって項目を移動しない場合のみです。

3. 項目の属性を変更するには、次のアクションを実行します。

項目の属性の変更

項目の属性を変更する場合、例えば `roomNumber` 属性値を置き換える場合は、次のコマンドを入力します。

```
idsldapmodify -D adminDN -w adminPW -i filename
```

ここで、`filename` には、以下の情報が含まれます。

```
dn: cn=Bob Garcia, ou=deptABC, ou=Austin, o=sample
changetype: modify
replace: roomNumber
roomNumber: 4B-014
```

項目の再作成

この機能を使用すると、項目をコピーできます。

この機能は、類似した項目を作成する場合に役に立ちます。コピーは、元の項目の属性をすべて継承します。新しい項目に名前を付けるには、いくつかの変更を行う必要があります。

Web 管理ツールの使用による項目のコピー

Web 管理ツールを使用して、項目をコピーできます。コピーは、元の項目の属性をすべて継承します。

手順

1. ナビゲーション領域で「ディレクトリー管理」カテゴリを展開します。
2. 「項目の管理」をクリックします。個々のサブツリーを展開すると、作業する項目 John Doe などを選択できます。
3. 「アクションの選択」ドロップダウン・メニューを展開します。
4. 「コピー」を選択します。
5. 「実行」をクリックします。
6. 「DN」フィールドの RDN 項目を変更します。例えば、`cn=John Doe` を `cn=Jim Smith` に変更します。
7. サーバーが (IBM Security Directory Server バージョン 6.0 でサポート開始された) `modifyDN` 操作をサポートしている場合は、親 DN とリーフ・ノードの新規上位属性を変更できます。このフィールドを変更することも、「ブラウズ」をクリックしてリストから親 DN を選択することもできます。また「選択」をクリックして項目の親 DN を変更することもできます。
8. 「必須属性」タブで、`cn` 項目を新しい RDN に変更します。この例では Jim Smith です。
9. 必要に応じて、他の必須属性を変更します。この例では、`sn` 属性を Doe から Smith に変更します。
10. 「次へ」をクリックして、「オプションの属性」タブを表示します。

11. 必要に応じて、オプションの属性を変更し、「次へ」をクリックして「静的メンバーシップ」タブを表示します。
12. 「静的メンバーシップ」タブで、コピーした項目をメンバーにするグループ・メンバーシップを選択します。このタブで、コピーした項目のメンバーシップを編集することもできます。

注: 項目をコピーするときに「静的メンバーシップ」タブが表示されるのは、コピー対象の項目が静的グループのメンバーである場合のみです。項目が静的グループのメンバーでない場合は、項目のコピー操作の場合でも「静的メンバーシップ」タブは表示されません。

13. 必要な変更を完了してから「完了」をクリックすると、新しい項目が作成されます。
14. 新しい項目 **Jim Smith** が項目リストの下部に追加されます。

注: この手順は、項目の属性のみをコピーします。元の項目のグループ・メンバーシップは、新しい項目にはコピーされません。585 ページの『項目のメンバーシップの管理』を参照して項目にメンバーシップを追加します。

コマンド行の使用による項目のコピー

コマンド行を使用して、項目をコピーできます。コピーは、元の項目の属性をすべて継承します。

手順

1. 検索を行い LDIF 形式の現在の項目を取得します。次のコマンドを実行します。

```
idsldapsearch -L -s base -b "cn=Bob Garcia,
ou=deptABC, ou=Austin, o=sample" (objectclass=*)
```

以下の情報が返されます。

```
dn: cn=Bob Garcia, ou=deptABC, ou=Austin, o=sample
cn: Bob Garcia
cn: Robert Garcia
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
sn: Garcia
roomNumber: 4B-014
```

2. 項目を編集して新規の項目の名前および部屋番号に変更します。

```
DNdn: Matt Morris, ou=deptABC, ou=Austin, o=sample
cn: Matt Morris
cn: Matthew Morris
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
sn: Morris
roomNumber: 2B-001
```

3. 新規項目を追加します。以下のコマンドを実行します。

```
idsldapadd -D adminDN -w adminPW -i
filename
```

項目のアクセス・コントロール・リストの編集

以下の説明を参照して、項目のアクセス制御リスト (ACL) を編集します。

手順

1. ナビゲーション領域の「ディレクトリー管理」カテゴリーがまだ展開されていない場合は展開します。

2. 「**項目の管理**」をクリックします。
3. さまざまなサブツリーを展開して、cn=Robert Garcia,ou=Austin,o=sample など、作業対象の項目を選択します。
4. 「**アクションの選択**」メニューを展開します。
5. 「**ACL の編集**」を選択します。
6. 「**実行**」をクリックします。

タスクの結果

Web 管理ツール・ユーティリティーを使用して ACL プロパティを表示させたり ACL を処理したりするには、558 ページの『ACL の処理』を参照してください。

詳細については、546 ページの『アクセス制御リスト』を参照してください。

補助オブジェクト・クラスの追加

この機能を使用すると、補助オブジェクト・クラスを追加できます。

Web 管理ツールを使用した補助オブジェクト・クラスの追加

Web 管理ツールを使用して、補助オブジェクト・クラスを追加できます。補助オブジェクト・クラスに必要な属性を、同じ変更操作の一部として項目に追加する必要があります。

手順

1. ナビゲーション領域で「**ディレクトリー管理**」カテゴリーを展開します。
2. 「**項目の管理**」をクリックします。
3. 個々のサブツリーを展開すると、作業する項目 John Doe などを選択できます。
4. 「**アクションの選択**」ドロップダウン・メニューから、スクロールダウンして「**補助クラスの追加**」を選択し、
5. 「**実行**」をクリックします。
6. ドロップダウン・メニューからフィルター・オブジェクト・クラスを選択して、「**再表示**」をクリックします。
7. 「**使用可能**」ボックスから、使用する任意の「**補助オブジェクト・クラス**」を選択して、「**追加**」をクリックします。追加する補助オブジェクト・クラスごとにこのプロセスを繰り返します。補助オブジェクト・クラスを選択して、「**除去**」をクリックすることで、「**選択済み**」ボックスから補助オブジェクト・クラスを削除することもできます。
8. 「**次へ**」をクリックします。
9. 「**必須属性**」タブで、必要な属性の値を入力します。
 - a. 属性が複数值で、特定の属性に複数の値を追加する場合は、「**複数值**」をクリックします。528 ページの『属性の複数值の追加』を参照してください。
 - b. 属性がバイナリー・データを必要とする場合は、「**バイナリー・データ**」をクリックします。528 ページの『属性のバイナリー・データ』を参照してください。

- c. サーバーで言語タグが使用可能な場合は、「**言語タグ値**」をクリックして言語タグ記述子を追加または除去します。詳細については、530 ページの『言語タグ』および 532 ページの『言語タグ値の追加』を参照してください。
 - d. 属性に参照が含まれる場合は、「**参照の管理**」をクリックします。詳細については、301 ページの『参照』および 306 ページの『デフォルト参照の作成』を参照してください。
10. 「**オプションの属性**」をクリックします。
 11. 「**オプションの属性**」タブで、他の属性の値を必要に応じて入力します。
 12. 「**完了**」をクリックすると、項目が変更されます。

コマンド行を使用した補助オブジェクト・クラスの追加

コマンド行を使用して、補助オブジェクト・クラスを追加できます。補助オブジェクト・クラスに必要な属性を、同じ変更操作の一部として項目に追加する必要があります。

このタスクについて

手順

次のコマンドを実行します。

```
idsldapmodify -D adminDN -w adminPW -i  
filename
```

ここで、*filename* には、以下の情報が含まれます。

注: 5 番目の行のハイフン (-) は重要です。

```
dn: cn=Bob Garcia, ou=deptABC, ou=Austin, o=sample  
changetype: modify  
add: objectclass  
objectclass: uniquelyIdentifiedUser  
-  
add: serialNumber  
serialNumber: 738393
```

補助オブジェクト・クラスの削除

この機能を使用すると、単一の補助オブジェクト・クラスを削除できます。

補助オブジェクト・クラスの削除を使用して、項目から単一の補助オブジェクト・クラスを削除します。

補助オブジェクト・クラスの追加の手順を実行して、補助オブジェクト・クラスを削除することもできます。詳細については、539 ページの『補助オブジェクト・クラスの追加』を参照してください。項目から複数の補助クラスを削除する場合は、補助クラスの追加の手順を実行します。

Web 管理の使用

以下の説明を参照し、Web 管理を操作して、補助オブジェクト・クラスを削除します。

手順

1. ナビゲーション領域の「ディレクトリー管理」カテゴリーがまだ展開されていなければ展開します。続いて、「項目の管理」をクリックします。個々のサブツリーを展開すると、作業する項目 John Doe などを選択できます。
2. 「アクションの選択」メニューから、スクロールダウンして「補助クラスの削除」を選択します。
3. 「実行」をクリックします。
4. 補助オブジェクト・クラスのリストから、削除する補助オブジェクト・クラスを選択して「OK」を押します。
5. 「OK」をクリックして削除を確認します。

タスクの結果

補助オブジェクト・クラスが項目から削除され、項目のリストに戻ります。

コマンド・ラインの使用

`idsldapmodify` コマンドを使用して、補助オブジェクト・クラスを変更します。

手順

1. 以下のコマンドを入力します。

```
idsldapmodify -D adminDN -w adminPW -i filename
```

ここで、*filename* には、以下の情報が含まれます。

注: 5 番目の行のハイフン (-) は重要です。

```
dn: cn=Bob Garcia, ou=deptABC, ou=Austin, o=sample
changetype: modify
delete: objectclass
objectclass: uniquelyIdentifiedUser
-
delete: serialNumber
serialNumber: 738393
```

補助オブジェクト・クラスによってのみ項目内で許可されている属性は、同じ変更操作の一部として項目から除去する必要があります。

2. 表示して、変更された情報を確認します。

ディレクトリー項目の検索

ディレクトリー項目には、事前定義またはユーザー定義の照会を使用できます。

ディレクトリー・ツリーの検索には、3 つのオプションがあります。

- 事前に定義した一連の検索基準を使用する簡易検索
- ユーザーが定義した一連の検索基準を使用する拡張検索
- 手動検索

これらのオプションを利用するには、ナビゲーション領域の「ディレクトリー管理」カテゴリーを展開して、「項目の検索」をクリックします。以下のタブのいずれかを選択します。

注: 検索可能な属性は、`userpassword` などのバイナリー属性のみです (それらが実際に存在している場合に限る)。

検索について詳しくは、122 ページの『検索設定』を参照してください。

検索フィルター

提供されている検索タイプのいずれかを選択できます。

簡易検索の実行:

以下の情報により、簡易検索を実行できます。

このタスクについて

簡易検索では、以下に示すデフォルトの検索基準が使用されます。

- 基本 DN は、すべてのサフィックス
- 検索スコープは、サブツリー
- 検索サイズは、500
- 時間制限は、900
- 別名の参照解除は、なし
- 追跡参照は、クリア (オフ)

手順

1. 「**検索フィルター**」タブで、「**簡易**」をクリックします。
2. クラス・リストからオブジェクト・クラスを選択します。
3. サーバーで言語タグが使用可能になっている場合は、言語タグを指定できます。詳細については、530 ページの『言語タグ』を参照してください。
4. 選択した項目タイプの特定の属性を選択します。特定の属性を検索する場合は、リストから属性を選択し、「**等しい**」ボックスにその属性値を入力します。属性を指定しないと、検索は、選択した項目タイプのディレクトリー項目をすべて戻します。
5. 「**OK**」をクリックします。

検索 - 拡張:

拡張検索では、検索の制約と検索フィルターを指定することができます。デフォルトの検索条件は、簡易検索の場合と同じです。

手順

1. 「**検索フィルター**」タブで、「**拡張**」をクリックします。
2. 「**追加**」をクリックします。
3. ドロップダウン・リストから「**属性**」を選択します。
4. サーバーで言語タグが使用可能になっている場合は、言語タグを指定できます。詳細については、530 ページの『言語タグ』を参照してください。
5. 「**比較**」演算子を選択します。

オペレーター	説明
等しい	属性は値と等しい。
等しくない	属性は値と等しくない。
より小か等しい	属性は値よりより小か等しい。

オペレーター	説明
より大か等しい	属性は値よりより大か等しい。
ほぼ等しい	属性は値とほぼ等しい。

6. 比較する値を入力します。
7. すでに少なくとも 1 つの検索フィルターを追加している場合は、追加の基準を指定し、「演算子」ドロップダウン・メニューから演算子を選択します。**AND** コマンドは、検索フィルター基準の両方のセットに一致する項目を戻します。**OR** コマンドは、検索フィルター基準のいずれかのセットに一致する項目を戻します。デフォルトの演算子は **AND** です。
8. 拡張検索に検索フィルター基準を追加するには、「**OK**」をクリックします。「検索結果」テーブルには以下の列があります。

列	説明
選択	追加、編集、または削除するフィルターの名前の横にあるラジオ・ボタンを選択します。
属性	フィルター実行対象の属性です。例えば objectclass などです。
比較	フィルターの比較基準（「次に等しい」など）です。
値	比較に使用する値（ワイルドカード値 (*) など）です。
オペレーター	指定した検索演算子 (AND など) です。

9. 検索に使用するフィルターごとにチェック・ボックスを選択します。
10. 「オプション」タブのいずれかのデフォルト設定を変更します。544 ページの『ディレクトリー・オプション』を参照してください。
11. 「**OK**」をクリックして検索を開始します。「検索結果」テーブルには以下の列があります。

列	説明
選択	操作する項目の名前の横のラジオ・ボタンを選択します。
RDN	項目の RDN。
オブジェクト・クラス	項目が属するオブジェクト・クラス。
作成	項目が作成された日付。
最終変更日時	項目が最後に変更された日付。
最終変更者	最後に項目を変更したユーザーの ID。

12. 検索結果を表示すれば、項目属性を変更できます（525 ページの『ディレクトリー項目』を参照）。「閉じる」をクリックすると、「項目の検索」パネルに戻ります。
13. 検索フィルターを変更するには、以下の手順を実行します。
 - a. 変更するフィルターを選択します。
 - b. 「編集」をクリックします。
 - c. 検索フィルターを追加した場合は、設定されているフィールドを変更します。
 - d. 「**OK**」をクリックします。

14. 検索フィルターを除去するには、以下の手順に従います。
 - a. 除去するフィルターごとにチェック・ボックスを選択します。
 - b. 拡張検索からフィルター基準を除去するには、「**除去**」をクリックします。
 - c. 検索フィルターをすべて消去する場合は、「**すべて除去**」をクリックします。

コマンド行の使用:

idsldapsearch コマンドを使用することで、簡易検索と拡張検索が実行できます。

このタスクについて

簡易検索または拡張検索のいずれを実行することもできます。以下の手順は、簡易検索項目または拡張検索項目の例を示しています。

手順

1. 簡易検索を実行する場合は、次のコマンドを入力します。

```
idsldapsearch -D userDN -w userPW -b Subtree DN -s SUBcn=John
```

2. 拡張検索を実行する場合は、次のコマンドを入力します。

```
idsldapsearch -D userDN -w userPW -b Subtree DN -s SUB (&(cn=John)(sn=Smith))
```

この例では、cn=John と sn=Smith がある項目が検索されます。ここでは、AND (&) 論理演算子を使用して、2 つの検索条件を 1 つのフィルターに結合しています。

- 3.

手動検索:

手動検索については、以下の説明で詳細を把握できます。

注:

1. ワイルドカード検索では、ワイルドカードを単語の先頭または末尾以外の場所で使用しないでください。次のような先行文字を使用してワイルドカード検索を実行します。

```
sn=*term
```

または、次の末尾の文字を使用して実行します。

```
sn=term*
```

2. また、ワイルドカードを先頭と末尾に同時に使用することもできません。

この方法を使用して、検索フィルターを作成します。デフォルトの検索条件は、単純検索の検索条件と同じです。例えば、名字を検索するには、フィールドに **sn=*** と入力します。複数の属性を検索する場合は、検索フィルター構文を使用する必要があります。例えば、特定の部門の名字を検索するには、以下のように入力します。

```
(&(sn=*)(dept=<departmentname>))
```

ディレクトリー・オプション

ディレクトリー内の検索で使用できる、使用可能なディレクトリー・オプションを把握します。

「オプション」タブで以下の手順を実行します。

- **検索ベース DN** - いずれかのラジオ・ボタンを選択することで、検索ベースを選択します。
 - **DN** - 検索ベースを明示的に指定する場合は、「DN」ラジオ・ボタンを選択します。「DN」フィールドに検索ベース (o=sample など) を入力します。
 - **サフィックス** - 特定のサフィックス内のみを検索する場合は、「サフィックス」ドロップダウン・メニューからそのサフィックスを選択します。このタスクを「項目の管理」パネルから開始した場合、このフィールドは事前に入力されています。
 - **すべてのサフィックス** - ツリー全体を検索するには、「すべてのサフィックス」を選択します。
- **検索スコープ**
 - 選択したオブジェクトの中だけで検索する場合は、「オブジェクト」を選択します。
 - 選択したオブジェクトの直接の子の範囲内のみで検索する場合は、「単一レベル」を選択します。
 - 選択したオブジェクトのすべての子孫を検索する場合は、「サブツリー」を選択します。
- **検索サイズ上限** - 検索する項目の最大数を入力します。「無制限」を選択することもできます。
- **検索時間制限** - 検索の最大時間数 (秒) を入力します。「無制限」を選択することもできます。
- サーバーが別名の参照解除をサポートしている場合は、ドロップダウン・リストから「別名の参照解除」のタイプを選択します。
 - **しない**: 選択した項目が別名の場合、その項目は検索で参照解除されません。つまり、検索では、その別名への参照は無視されます。また、検索で検出された項目は参照解除されません。
 - **検出** - 選択した項目が別名の場合、検索では別名が参照解除され、その別名のロケーションから検索されます。
 - **検索** - 選択した項目は参照解除されませんが、検索で検出された項目は参照解除されます。
 - **常時** - 検索で検出された別名は、すべて参照解除されます。
- 検索で参照が戻された場合、別のサーバーへの参照を追跡するには、「追跡参照」チェック・ボックスを選択します。参照により別のサーバーへの検索が指示される場合、そのサーバーへの接続には現在の資格情報が使用されます。無名でログインしている場合は、認証済みの DN を使用して、サーバーにログインしなければならない場合があります。

参照サーバーで項目が検出された場合、「検索結果」パネルには、項目の DN のみが表示されます。「オブジェクト・クラス」や「変更されたタイム・スタンプ (modified timestamp)」などのその他の列は表示されません。参照項目に対して「ACL の編集」、「削除」、「補助の追加 (Add auxiliary)」、または「補助の削除 (Delete auxiliary)」などの操作を実行することはできません。

詳細については、301 ページの『参照』および『アクセス制御リスト』を参照してください。

- 「削除された項目を含める」チェック・ボックスを選択して、削除された項目が検索操作で返されるようにします。

アクセス制御リスト

この機能を使用すると、アクセス制御リストを管理できます。

以下のセクションでは、アクセス制御リスト (ACL) とその管理方法について説明します。

概説

アクセス制御リスト (ACL) では、LDAP ディレクトリーに保管された情報を保護します。

管理者は ACL を使用して、ディレクトリーのさまざまな部分へのアクセスや、特定のディレクトリー項目へのアクセスを制限します。LDAP のディレクトリー項目は、階層ツリー構造によって相互に関連しています。各ディレクトリー項目 (またはオブジェクト) には、一連の属性やそれに対応する値のみではなく、オブジェクトの識別名も含まれています。

アクセス制御モデルでは、以下の 2 つの属性セットが定義されます。

- entryOwner 情報
- アクセス・コントロール情報 (ACI)

ACI 情報と entryOwner 情報は、LDAP モデルに従って、属性 - 値ペアの形式で表現されます。LDIF 構文を使用すると、これらの値を管理できます。

entryOwner 情報

entryOwner 情報により、ACL を定義するサブジェクトが制御され、さらに、ターゲット・オブジェクトへの完全なアクセス権が獲得されます。

以下の属性は、項目の所有権を定義します。

- entryOwner - 項目の所有者を明示的に定義します。
- ownerPropagate - アクセス権セットをサブツリー子孫項目に伝搬させるかどうかを指定します。

項目の所有者には、aclEntry に関係なく、オブジェクトに対して任意の操作を実行するためのアクセス権があります。それに加えて、特定のオブジェクトの aclEntry の管理を許可されているのは、項目の所有者だけです。entryOwner は、アクセス制御のサブジェクトであり、個人、グループ、または役割として定義できます。

注: ディレクトリー管理者、および DirDataAdmin 役割に割り当てられているローカル管理グループ・メンバーは、デフォルトではディレクトリー内のすべてのオブジェクトの entryOwners であり、この entryOwnership はいずれのオブジェクトからも除去できません。

アクセス・コントロール情報

アクセス制御情報は、特定の LDAP オブジェクトに対して実行するサブジェクトのアクセス権を明示的に定義します。

フィルターに処理されていない ACL:

非フィルター ACL は、この ACL を含むディレクトリー項目に明示的に適用されますが、子孫項目にまったく伝搬しない場合も、すべての子孫項目に伝搬する場合があります。

フィルターに処理されていない ACL のデフォルトの振る舞いは、伝搬することです。以下の属性は、非フィルター ACL を定義します。

- `aclEntry` - アクセス権セットを定義します。
- `aclPropagate` - アクセス権セットをサブツリー子孫項目に伝搬させるかどうかを指定します。

フィルターに処理された ACL:

フィルター ACL は、ターゲット・オブジェクトとそれらに適用される有効なアクセスとを突き合わせるために、指定されたオブジェクト・フィルターを使用してフィルター・ベースの比較を行う、という点で異なります。

これらは同じ機能を実行しますが、2 種類の ACL の振る舞いは異なります。フィルター・ベース ACL は、非フィルター・ベース ACL が現在行っているのと同じ方法では伝搬しません。フィルター・ベースの ACL は本質的に、関連するサブツリーで比較が一致したオブジェクトに伝搬します。このような理由から、`aclPropagate` 属性 (フィルターに掛けられていない ACL の伝搬の停止に使用します) は新しいフィルター・ベースの ACL には適用されません。

フィルター・ベースの ACL のデフォルト動作では、最下位の収容項目から、祖先項目チェーンを上に向かって、DIT の最上位の収容項目まで累算します。有効なアクセスは、構成する祖先項目によって付与または否認されたアクセス権の共用体として計算されます。この動作には例外があります。サブツリー複製機能との互換性のために、また管理制御を強化するために、上限属性を使用して、上限属性が含まれる項目での累算が停止されます。

一連の独立したアクセス・コントロール属性は、フィルター・ベースの特性を既存の非フィルター・ベースの ACL にマージするのではなく、フィルター・ベースの ACL をサポートすることに主眼を置いています。

- `ibm-filterAcEntry`
- `ibm-filterAcInherit`

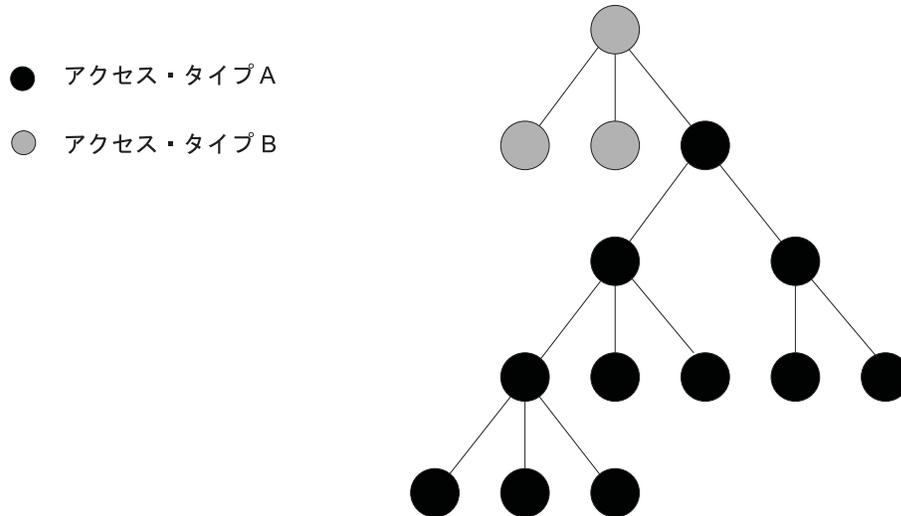
`ibm-filterAcEntry` 属性は、オブジェクト・フィルター・コンポーネントを追加することにより、`aclEntry` と同じ形式になります。関連する上限属性は、`ibm-filterAcInherit` です。デフォルトでは `true` に設定されています。`false` に設定すると、累算が停止します。

ACL タイプの使用法のシナリオ

非フィルター ACL の目的は、ディレクトリーのアクセス接続形態が同種のアクセス権サブツリー分布を必要とする状況で役立つことです。

以下の例では、ツリー内の一様な分布内にあるディレクトリー・オブジェクトにアクセス権を適用する必要がある場合について説明します。

図 19. 非フィルター処理 ACL のシナリオ



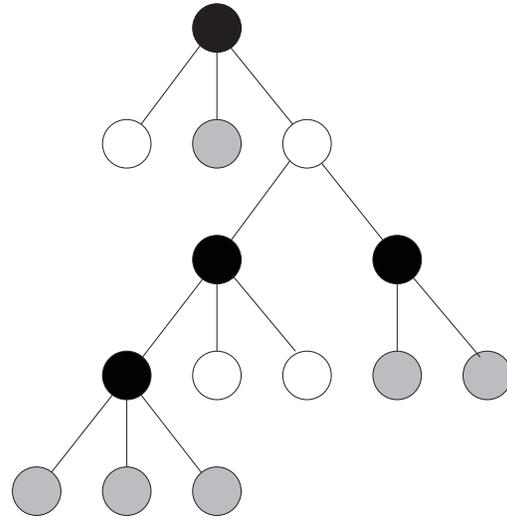
例 1: 非フィルター ACL のシナリオ

これを実現するには、非フィルター処理 ACL 仕様一式をディレクトリーの最上位項目 (またはその付近の項目) で定義します。ACL は、ディレクトリーのサブツリー全体にわたって均一に伝搬できるため、すべてのサブツリー・オブジェクトに適用できます。このタイプの ACL に関連付けられている照合は存在しないため、処理も少なくなります。

フィルター・ベース ACL の目的は、以下の例で示すように、ディレクトリーのアクセス接続形態が異種のアクセス権サブツリー分布を必要とする状況で役立つことです。このシナリオではいくつかのアクセス権タイプが必要であり、より分散した分布のディレクトリー・オブジェクトにアクセス権タイプを適用する必要があります。

図 20. フィルター・ベース ACL のシナリオ

- アクセス・タイプ A
- アクセス・タイプ B
- アクセス・タイプ C



例 2: フィルター・ベース ACL のシナリオ

これを実現するには、必要な各アクセス権タイプと関連付けられているフィルターを使用して、フィルター・ベース ACL の仕様一式をディレクトリーのサフィックス項目で定義します。フィルターは、ディレクトリー・ツリー全体にわたって分布しているさまざまなオブジェクト内にある属性に対応しています。

特定のディレクトリー・オブジェクト内にある属性との照合が正常に行われることにより、そのオブジェクトに対して正しいアクセス権が適用されます。サフィックスの場所が単一であるため、ACL 管理は簡略化されます。対照的に、非フィルター処理 ACL を使用して同じ ACL 一式を実現するには、ツリー内のすべてのディレクトリー・オブジェクトに ACL 仕様が必要になります。

アクセス制御属性の構文

新しいフィルター・ベース ACL 属性の構文は、現在の非フィルター・ベース ACL 属性の変更バージョンです。

これらの各属性は、LDIF 表記を使用して管理できます。バックス正規形式 (BNF) を使用した ACI 属性および entryOwner 属性の構文を定義する項目を以下に示します。

```
<aclEntry> ::= <subject> [ ":" <rights> ]
<aclPropagate> ::= "true" | "false"
<ibm-filterAclEntry> ::= <subject> ":" <object filter> [ ":" <rights> ]
<ibm-filterAclInherit> ::= "true" | "false"
<entryOwner> ::= <subject>
<ownerPropagate> ::= "true" | "false"
<subject> ::= <subjectDnType> ':' <subjectDn> |
<pseudoDn>
<subjectDnType> ::= "role" | "group" | "access-id"
<subjectDn> ::= <DN>
```

```

<DN> ::= distinguished name as described in RFC 2251, section 4.1.3.

<pseudoDn> ::= "group:cn=anybody" | "group:cn=authenticated" |
"access-id:cn=this"

<object filter> ::= string search filter as defined in RFC 2254, section 4
(extensible matching is not supported).

<rights> ::= <accessList> [ ":" <rights> ]

<accessList> ::= <objectAccess> | <attributeAccess> |
<attributeClassAccess>

<objectAccess> ::= "object:" [<action> ":"] <objectPermissions>

<action> ::= "grant" | "deny"

<objectPermissions> ::= <objectPermission> [ <objectPermissions> ]

<objectPermission> ::= "a" | "d" | ""

<attributeAccess> ::= "at." <attributeName> ":" [<action> ":"]
<attributePermissions>

<attributeName> ::= attributeType name as described in RFC 2251, section 4.1.4.
(OID or alpha-numeric string with leading
alphabet, "-" and ";" allowed)

<attributePermissions> ::= <attributePermission>
[ <attributePermissions> ]

<attributePermission> ::= "r" | "w" | "s" | "c" | ""

<attributeClassAccess> ::= <class> ":" [<action> ":"]
<attributePermissions>

<class> ::= "normal" | "sensitive" | "critical" | "system" | "restricted"

```

サブジェクトの概要

サブジェクトとは、オブジェクトに対して操作するためのアクセス権を要求するエンティティです。

サブジェクトは、DN (識別名) タイプと DN との組み合わせから構成されます。有効な DN タイプは、アクセス ID、グループ、および役割です。

DN は、特定のアクセス ID、役割、またはグループを識別します。例えば、1 つのサブジェクトは `access-id: cn=personA, o=sample` or `group: cn=deptXYZ, o=sample` のようになります。

フィールドの区切り文字はコロン (:) です。したがって、DN にコロンが含まれている場合は、二重引用符 ("") で囲む必要があります。DN に二重引用符で囲まれた文字が既に入っている場合は、円記号 (¥) を使用して、該当する文字をエスケープする必要があります。

ディレクトリー・グループはすべて、アクセス・コントロールで使用できます。

注: `AccessGroup`、`GroupOfNames`、`GroupofUniqueNames`、または `groupOfURLs` の各構造化オブジェクト・クラス、または `ibm-dynamicGroup`、`ibm-staticGroup` の補助オブジェクト・クラスは、いずれもアクセス制御に使用できます。

アクセス制御モデル内で使用されるもう 1 つの DN タイプは、役割です。役割とグループは、インプリメンテーション上はよく似ていますが、概念的には異なります。ユーザーに役割を割り当てるときは、その役割に関連するジョブの実行に必要な権限がセットアップ済みである、という暗黙の了解があります。グループ・メンバーシップには、そのグループのメンバーになることで得られるあるいは否認される許可に固有の前提条件はありません。

役割とグループは、ディレクトリー内でオブジェクトにより表現されるという点では同じです。役割には、さらに DN のグループも含まれています。アクセス・コントロールで使用する役割は、AccessRole のオブジェクト・クラスを持っている必要があります。

疑似 DN

疑似 DN は、アクセス・コントロールの定義および評価で使用されます。

ディレクトリーには、いくつかの疑似 DN が含まれています。例えば、`group:cn=Anybody` や `access-id:cn=this` があります。これらの疑似 DN は、実行される操作または操作が実行されているオブジェクトのいずれかに関して、共通の特性を共有する多数の DN を参照するために使用されます。

LDAP バージョン 3 では、以下の 3 つの疑似 DN がサポートされます。

access-id:cn=this

ACL の一部として指定されると、この DN は操作が実行される DN と同じ bindDN を参照します。例えば、オブジェクト `cn=personA, o=sample` に対して操作が実行され、bindDn が `cn=personA, o=sample` の場合、与えられる許可は、`cn=this` に与えられる許可と `cn=personA, o=sample` に与えられる許可の組み合わせとなります。

group:cn=anybody

ACL の一部として指定されると、この DN は、認証されていないユーザーも含めて、すべてのユーザーを参照します。このグループからユーザーを除去することはできません。また、データベースからこのグループを除去することもできません。

group: cn=Authenticated

この DN は、ディレクトリーによって認証された DN を参照します。認証の方式は考慮されません。

注: `cn=Authenticated` は、DN を表すオブジェクトがどこにあるかにかかわらず、サーバーの任意の場所で認証された DN を参照します。ただし、これを使用するには注意が必要です。例えば、あるサフィックスの下で、`cn=Secret` は `cn=Confidential Material` と呼ばれるノードとなっており、`group:cn=Authenticated:normal:rsc` の acl 項目を持つことがあります。別のサフィックスの下で、`cn=Common` はノード `cn=Public Material` になることがあります。これらの 2 つのツリーが同じサーバー上にある場合、`cn=Public Material` へのバインドは認証済みと見なされ、`cn=Confidential Material` オブジェクト上の標準クラスに対する許可が取得されます。

疑似 DN の例:

ご参考までに、疑似 DN の例を以下に示します。

例 1 `object:cn=personA, o=sample AclEntry` に対して、以下の ACL を考えてみます。

```
access-id: cn = this:critical:rWSC
AclEntry: group: cn=Anybody: normal:rsc
AclEntry: group: cn=Authenticated: sensitive:rsc
```

ユーザー・バインド	受け取る内容
cn=personA, o=sample	normal:rsc:sensitive:rcs:critical:rwsc
cn=personB, o=sample	normal:rsc:sensitive:rsc
NULL (認証されていない)	normal:rsc

この例で personA が受け取るのは、cn=this ID に与えられた許可、および cn=Anybody 疑似 DN グループと cn=Authenticated 疑似 DN グループの両方に与えられた許可です。

例 2 object:cn=personA, o=sample AclEntry に対して、以下の ACL を考えてみます。

```
access-id:cn=personA, o=sample: object:ad
AclEntry: access-id: cn = this:critical:rwsc
AclEntry: group: cn=Anybody: normal:rsc
AclEntry: group: cn=Authenticated: sensitive:rcs
```

cn=personA, o=sample に対して実行する操作は、以下のようになります。

ユーザー・バインド	受け取る内容
cn=personA, o=sample	object:ad:critical:rwsc
cn=personB, o=sample	normal:rsc:sensitive:rsc
NULL (認証されていない)	normal:rsc

この例で personA が受け取るのは、cn=this ID に与えられた許可、および DN 自体 cn=personA, o=sample に与えられた許可です。バインド DN cn=personA, o=sample に対して、より具体的な acl 項目 access-id:cn=personA, o=sample があるため、グループ許可は与えられません。

例 3 オブジェクト cn=personA, o=sample AclEntry に対して、以下の ACL を考えてみます。ユーザーに自身のパスワードを変更する権限を与えます。

```
access-id:cn=this:at.userpassword:rwsc
```

ユーザー・バインド	受け取る内容
cn=personA, o=sample	at.userpassword:rwsc

オブジェクト・フィルター

RFC 2254 で定義されているストリング検索フィルターは、オブジェクト・フィルター形式として使用されます。

このパラメーターは、フィルターに処理された ACL にのみ適用されます。ターゲット・オブジェクトは既知であるため、ストリングは実際の検索の実行には使用されません。代わりに、問題となっているターゲット・オブジェクトでのフィルター・ベースの比較が実行され、ibm-filterAclEntry 値のセットがそれに適用されるかどうか判别されます。

アクセス権

アクセス権は、オブジェクト全体またはオブジェクトの属性に適用されます。

LDAP のアクセス権はそれぞれ独立しています。つまり、1 つの権限が別の権限を伴うことはありません。規則のセットに従うことにより、権限を 1 つに結合すると、必要な権限のリストを提供できます。権限には値を指定しないこともできま

す。権限に値を指定しないと、ターゲット・オブジェクト上のサブジェクトにはアクセス権が付与されません。権限は、以下の 3 つの部分から構成されます。

処置 定義される値は **grant** または **deny** です。このフィールドがない場合、デフォルトは **grant** に設定されます。

権限 ディレクトリー・オブジェクト上で実行できる基本操作は 6 つです。これらの操作から、ACI 許可の基本セットが処理されます。

- 項目の追加
- 項目の削除
- 属性値の読み取り
- 属性値の書き込み
- 属性の検索
- 属性値の比較

以下に示すのは、属性で可能な許可です。

- 読み取り **r**
- 書き込み **w**
- 検索 **s**
- 比較 **c**

また、オブジェクトの許可は、項目全体に適用されます。それらの許可は以下のとおりです。

- 子項目の追加 **a**
- この項目の削除 **d**

以下の表は、各 LDAP 操作の実行に必要なとされる許可をまとめたものです。

操作	必要な許可
idsldapadd	追加 (親に対する)
idsldapdelete	削除 (オブジェクトに対する)
idsldapmodify	書き込み (変更された属性に対する)
idsldapsearch	<ul style="list-style-type: none"> • 検索、読み取り (RDN 内の属性に対する) • 検索 (検索フィルターで指定された属性に対する) • 検索 (正確な名前とともに返された属性に対する) • 検索、読み取り (値とともに戻された属性に対する)
idsldapmodrdn	書き込み (RDN 属性に対する)

検索操作の場合、サブジェクトは、検索フィルター内のすべての属性への検索 **s** アクセス権を持っている必要があります。検索アクセス権を持っていないと、項目は戻されません。検索から戻される項目について、サブジェクトは、戻される項目の RDN のすべての属性に対して、検索 **s** および読み取り **r** アクセス権を持っている必要があります。これらのアクセス権を持っていないと、項目は戻されません。

以下の例では、at.telephoneNumber:rsc 許可セットで、cn=Bowling Team, ou=Groups, o=sample のメンバーが、この項目に含まれる telephoneNumber

属性のみに読み取り専用でアクセスできるようにしています。at.cn:rsc 許可セットでは、RDN 検索条件が満たされるようにしています。この例の場合、cn または telephoneNumber 属性のみが検索フィルターで使用できます。title 属性を検索フィルターで使用する場合、検索を成功させるために at.title:rsc 許可を追加します。

```
dn: cn=Bonnie Daniel, ou=Widget Division, ou=Austin, o=sample
objectclass: person
objectclass: organizationalPerson
cn: Bonnie Daniel
sn: Daniel
telephonenumber: 1-812-855-7453
internationalISDNNumber: 755-7453
title: RISC Manufacturing
seealso: cn=Mary Burnnet, ou=Widget Division, ou=Austin, o=sample
postalcode: 1515
aclentry: group: cn=Bowling Team, ou=Groups, o=sample: at.cn:rsc:
at.telephoneNumber:r
```

Access Target:

これらの許可は、オブジェクト全体 (子項目の追加、項目の削除) や項目内の個々の属性に適用できます。あるいは、属性グループ (属性アクセス・クラス) に適用できます。

同様のアクセス権を必要としている属性は、クラス内にグループ化されません。属性は、ディレクトリー・スキーマ・ファイル内の属性クラスにマッピングされます。これらのクラスは明確に区別されています。あるクラスにアクセスしても、それによって、別のクラスへのアクセスが発生することはありません。許可は、属性アクセス・クラス全体に対して設定されます。ある特定の属性クラスに設定された許可は、個々の属性アクセス権が指定されない限り、このアクセス・クラス内のすべての属性に適用されます。

IBM では、ユーザー属性へのアクセスの評価に使用する属性クラスとして normal、sensitive、critical、system、および restricted の 5 つを定義しています。例えば、属性 commonName は normal クラスに属し、属性 userPassword は critical クラスに属します。ユーザー定義属性は、特に指定がない限り、normal アクセス・クラスに属します。

アクセス制御が適用される system クラス属性は、以下のとおりです。

- aclSource
- ibm-effectiveAcl
- ownerSource

これらの属性は、LDAP サーバーによって保持されており、ディレクトリーのユーザーおよび管理者に対しては、読み取り専用で設定されています。OwnerSource と aclSource については、『伝搬』のセクションを参照してください。

アクセス制御を定義する restricted クラス属性は、以下のとおりです。

- aclEntry
- aclPropagate
- entryOwner
- ibm-filterAclEntry
- ibm-filterAclInherit
- ownerPropagate

デフォルトでは、すべてのユーザーが `restricted` 属性への読み取りアクセス権を保有していますが、これらの属性を作成、変更、および削除できるのは `entryOwners` のみです。

伝搬の概要

伝搬属性である `aclPropagate` と `ownerPropagate` では、同じ項目内に格納できる値は 1 つに限られます。

`aclEntry` が配置されている項目は、明示的な `aclEntry` を持っている項目と見なされます。同様に、`entryOwner` が特定の項目に対して設定されている場合、その項目は、明示的な所有者を持っているものと見なされます。この 2 つは、互いに関連しているわけではありません。明示的な所有者を持つ項目が、明示的な `aclEntry` を持つとは限りませんが、明示的な `aclEntry` を持つ項目は、明示的な所有者を持つことがあります。これらの値のいずれかが項目上に明示的に存在していない場合、欠落している値は、ディレクトリー・ツリー内の祖先ノードから継承されます。

明示的な `aclEntry` または `entryOwner` は、それらが設定されている項目にそれぞれ適用されます。また、値は、明示的に設定された値を持たないすべての子孫に適用できます。これらの値は伝搬されるものと見なされ、ディレクトリー・ツリーを通じて伝搬されます。特定の値の伝搬は、別の伝搬中の値が到達するまで続けられます。

注: フィルター・ベースの ACL は、非フィルター・ベースの ACL と同じ方法では伝搬しません。フィルター・ベースの ACL は、関連するサブツリーで比較が一致したオブジェクトに伝搬します。詳細については、547 ページの『フィルターに処理された ACL』を参照してください。

`aclEntry` と `entryOwner` は、伝搬値を "false" に指定して、特定の項目にのみ適用するように設定することができます。また、伝搬値を "true" に指定して、その項目およびそのサブツリーに適用するように設定することもできます。`aclEntry` と `entryOwner` はいずれも伝搬できますが、それらの伝搬はリンクされません。

`aclEntry` 属性と `entryOwner` 属性では、同じ項目内での複数値が許可されます。

`system` 属性の `aclSource` と `ownerSource` には、`aclEntry` または `entryOwner` を評価する、有効なノードの DN が含まれています。そのようなノードが存在しない場合は、値として `default` が割り当てられます。

オブジェクトの有効なアクセス・コントロール定義は、以下のロジックによって得ることができます。

- オブジェクトに明示的な一連のアクセス・コントロール属性がある場合は、それがオブジェクトのアクセス・コントロール定義になります。
- 明示的に定義されたアクセス・コントロール属性がない場合は、一連の伝搬アクセス・コントロール属性を持つ祖先ノードに達するまで、ディレクトリー・ツリーを上方向に検索します。
- そのような祖先ノードが見つからない場合は、556 ページの『アクセス評価』で説明するデフォルト・アクセスがサブジェクトに付与されます。

アクセス評価

特定の操作のためのアクセスが認可されるかどうかは、ターゲット・オブジェクト上でその操作を行うための、サブジェクトのバインド DN によって決まります。アクセスが決定されると、処理はただちに停止されます。

アクセスの検査は、まず有効な **entryOwnership** と **ACI** 定義を検索し、次に項目の所有権を検査してから、オブジェクトの **ACI** の値を評価することで行われます。

フィルター・ベースの **ACL** では、最下位の収容項目から、祖先項目チェーンを上に向かって、**DIT** の最上位の収容項目まで累算します。有効なアクセスは、構成する祖先項目によって付与または否認されたアクセス権の共用体として計算されます。特定規則と結合規則の既存のセットは、フィルター・ベースの **ACL** の有効なアクセスを評価します。

フィルター・ベースの属性と非フィルター・ベースの属性は、単一の収容ディレクトリー項目内では相互に排他的です。両方のタイプの属性を同じ項目に入れることはできません。制約違反になります。この条件が検出されると、ディレクトリー項目の作成または更新に関連する操作は失敗します。

有効なアクセスを計算する場合、ターゲット・オブジェクト項目の祖先チェーンで検出される最初の **ACL** タイプにより、計算のモードが設定されます。フィルター・ベース・モードでは、有効なアクセスを計算するときに非フィルター・ベースの **ACL** は無視されます。同様に、非フィルター・ベース・モードでは、有効なアクセスを計算するときにフィルター・ベースの **ACL** は無視されます。

有効なアクセスを計算するときに、フィルター・ベースの **ACL** の累算を制限するには、値を *false* に設定した **ibm-filterAclInherit** 属性を、サブツリーの **ibm-filterAclEntry** の最上位と最下位の間にある項目に配置します。この方法により、ターゲット・オブジェクトの祖先チェーンでそれより上にある **ibm-filterAclEntry** 属性のサブセットが無視されます。

有効なアクセスを計算するときに、フィルター・ベースの **ACL** の累算を除外するには、値を *false* に設定した **ibm-filterAclInherit** 属性を、サブツリーの **ibm-filterAclEntry** の最下位の間にあるいずれかの項目に配置します。この方法により、ターゲット・オブジェクトの祖先チェーンでそれより上にあるすべての **ibm-filterAclEntry** 属性が無視されます。結果のアクセスは、デフォルトのフィルター **ACL** 値に解決されます。

デフォルトでは、ディレクトリー管理者、**DirDataAdmin** 役割に割り当てられているローカル管理グループのメンバー、およびマスター・サーバー (複製の場合はピア・サーバー) は、ディレクトリー内のすべてのオブジェクトに対するフル・アクセス権を取得します。ただし、システム属性に対する書き込み権限は除きます。その他の **entryOwner** は、**system** 属性への書き込みアクセスを除き、その所有権の下でのオブジェクトへのアクセス権をすべて取得します。デフォルトでは、すべてのユーザーが **normal**、**system**、**restricted** の各属性に対する読み取りアクセス権を持っています。要求を出しているサブジェクトに **entryOwnership** が付与されている場合、アクセス権はデフォルト設定によって決定され、アクセス処理は停止されません。

注: 項目に明示的に ACL を設定し、システム属性には明示的に ACL を設定しない場合、リクエスターには自動的に読み取り、検索、比較許可が付与されます。アクセスを拒否するには、明示的に拒否する必要があります。デフォルトではアクセス権は拒否されていません。

要求を出しているサブジェクトが `entryOwner` でない場合は、オブジェクト項目の ACI の値が検査されます。ACI 内で定義されている、ターゲット・オブジェクトに対するアクセス権は、特定規則と結合規則によって計算されます。

特定規則

最も特定の `aclEntry` 定義は、ユーザーへの許可の付与または否認を評価するときに使用される `aclEntry` 定義です。特定性のレベルは以下のとおりです。

- アクセス ID は、グループまたは役割よりも特定のものです。グループと役割は、同じレベルです。
- 同じ `dnType` レベル内では、個々の属性レベルの許可の方が、属性クラス・レベルの許可よりも特定のものです。
- 同じ属性または属性クラス・レベル内では、`deny` の方が `grant` よりも特定のものです。

結合規則

同じ特定性を持つ複数のサブジェクトに付与されている許可は、結合されません。同じ特定性のレベル内でアクセスを決定できない場合は、特定性のレベルがより低いアクセス定義が使用されます。定義済みの ACI がすべて適用されてもアクセスが決定されない場合は、アクセスが否認されます。

注: アクセス評価の際に、一致するアクセス ID レベルの `aclEntry` が見つかると、グループ・レベルの `aclEntry` は、アクセス計算に含まれません。ただし、例外として、一致するアクセス ID レベルの `aclEntry` が `cn=this` の下ですべて定義されている場合は、一致するグループ・レベルの `aclEntry` も、評価の際にすべて結合されます。

つまり、オブジェクト項目内において、バインド DN と同じアクセス ID サブジェクト DN が、定義済みの ACI 項目に含まれている場合、許可は、最初にその `aclEntry` に基づいて評価されます。同じサブジェクト DN の下で、一致する属性レベルの許可が定義されていると、それらの許可は、属性クラスの下で定義されている許可に取って代わります。同じ属性または属性クラス・レベル定義の下で、競合する許可がある場合は、`deny` (否認) された許可が `grant` (付与) された許可をオーバーライドします。

注: ヌル値許可を定義すると、特定性のより低い許可定義は含まれなくなります。

アクセスがまだ決定できず、見つかった `aclEntry` のうち一致するものがすべて `cn=this` の下で定義されている場合は、グループ・メンバーシップが評価されます。ユーザーが複数のグループに属している場合、ユーザーはそれらのグループから、組み合わされた許可を受け取ります。また、ユーザーは自動的に `cn=Anybody` グループに属します。ユーザーが認証済みのバインドを実行した場合は、`cn=Authenticated` グループに属することがあります。これらのグループに対して許可が定義されている場合、ユーザーは、指定された許可を受け取ります。

注: グループおよび役割メンバーシップは、バインド時に決定されます。これらは、別のバインドが発生するまで、またはアンバインド要求を受け取るまで続きます。ネストされたグループおよび役割 (すなわち、別のグループまたは役割のメンバーとして定義されたグループまたは役割) は、メンバーシップの決定やアクセス評価では解決されません。

例えば、attribute1 が sensitive 属性クラス内にあり、ユーザー cn=Person A, o=sample が group1 と group2 の両方に属しており、以下の aclEntry が定義されていると想定します。

1. aclEntry: access-id: cn=Person A, o=sample:
at.attribute1:grant:rsc:sensitive:deny:rsc
2. aclEntry: group: cn=group1,o=sample:critical:deny:rwc
3. aclEntry: group: cn=group2, o=sample:critical:grant:r:normal:grant:rsc

このユーザーのアクセス権は以下のとおりです。

- rsc から attribute1 へのアクセス権を取得します (1. より。属性レベル定義は、属性クラス・レベル定義に取って代わります)。
- ターゲット・オブジェクト内の他の sensitive クラス属性へのアクセス権は取得しません (1. より)。
- その他の権限は与えられません (2. および 3. は、アクセス評価に含まれません)。

別の例として、以下の aclEntry が定義されていると想定します。

1. aclEntry: access-id: cn=this: sensitive
2. aclEntry: group: cn=group1, o=sample:sensitive:grant:rsc:normal:grant:rsc

このユーザーのアクセス権は以下のとおりです。

- sensitive クラス属性へのアクセス権は付与されません (1. より。access-id の下にヌル値が定義されているため、group1 の sensitive クラス属性へのアクセス権を含めることはできません)。
- rsc から normal クラス属性へのアクセス権は持ちます (2. より)。

ACL の処理

この機能によって、ACL を処理できます。

以下のセクションでは、ACL を管理するために実行できるさまざまなタスクについて説明します。

Web 管理ツールを使用した ACL のプロパティーの表示

Web 管理ツールを使用して、ACL のプロパティーを表示したり、ACL を処理したりできます。

手順

1. 「ディレクトリー管理」をクリックします。
2. 「項目の管理」をクリックします。
3. ディレクトリー項目を選択します。例えば、ou=Widget Division,ou=Austin,o=sample です。

4. 「アクションの選択」メニューを展開します。
5. 「ACL の編集」を選択します。
6. 「実行 (Go)」をクリックする。

注: 「ACL の編集」パネルは、「有効な ACL」タブが事前に選択されて表示されます。このパネルには、以下の 5 つのタブがあります。

- 有効な ACL
- 有効所有者
- フィルターに処理されていない ACL
- フィルターに処理された ACL
- 所有者

「有効な ACL」タブと「有効所有者」タブには、ACL に関する読み取り専用情報が表示されます。

有効なアクセス制御リスト:

有効なアクセス制御リストとは、選択された項目についての、明示的でありかつ継承されたアクセス制御リストです。

選択した項目について有効なアクセス制御リストを表示するには、テーブル上部の「ロード」ボタンをクリックします。有効なアクセス制御リストのテーブルには、以下の列に読み取り専用の情報があります。

- **選択** - 表示する ACL の名前を選択します。
- **対象 DN** - アクセス権を付与または拒否する項目の識別名。
- **対象タイプ** - ACL のタイプ。以下の 3 つの対象タイプがあります。
 - **アクセス ID** - ユーザーにアクセスを関連付けます。
 - **グループ** - 選択したグループのメンバーであるユーザーにアクセスを関連付けます。
 - **役割** - 選択した役割が割り当てられているユーザーにアクセスを関連付けます。

「ロード」をクリックして、ACL をロードします。ACL のロードが完了してからは、いつでも「再表示」をクリックしてテーブルを再表示することができます。テーブルの下のタイム・スタンプは、テーブルの最終更新時刻を記録したものです。

アクセス権の表示:

Web 管理ツールを使用して、以下の手順を実行すると、アクセス権を表示できます。

このタスクについて

特定の有効な ACL に対するアクセス権を表示させるには、その ACL を選択し、「表示」をクリックします。「アクセス権の表示」パネルが開きます。

- 「対象 DN」セクションには、表示する項目の識別名が表示されます。
- 「対象タイプ」セクションには、項目が関連付けられている ACL のタイプが表示されます。

- 「**権限**」セクションには、サブジェクトの追加権限と削除権限が表示されます。
 - 「**子の追加**」では、選択した項目の下にディレクトリー項目を追加する権限をサブジェクトに対して許可または否認します。
 - 「**項目の削除**」では、選択された項目を削除する権限をサブジェクトに対して許可または否認します。
- 「**セキュリティー・クラス・アクセス権**」セクションでは、セキュリティー・クラスのアクセス権を定義します。属性は、以下のようなセキュリティー・クラスにグループ化されます。
 - **Normal** - Normal 属性では、最低限のセキュリティーが要求されます (例: commonName 属性)。
 - **Sensitive** - Sensitive 属性では、中程度のセキュリティーが要求されます (例: homePhone 属性)。
 - **Critical** - Critical 属性では、最高レベルのセキュリティーが要求されます (例: userpassword 属性)。
 - **System** - System 属性は、サーバーによって管理される読み取り専用属性です。
 - **Restricted** - Restricted 属性は、アクセス制御の定義に使用します。

属性を表示して、そのセキュリティー・クラスを判断できます。この方法の詳細が必要な場合は、51 ページの『属性の表示』を参照してください。

注: システム・セキュリティー・クラスおよび制限付きセキュリティー・クラスのオプションは、サーバーがシステム ACL および制限付き ACL をサポートする場合にのみ表示されます。システム・セキュリティー・クラスを書き込み可能に設定することはできません。

- 「**属性アクセス権**」セクションには、個別に許可が設定された属性がリスト表示されます。属性が所属するセキュリティー・クラス・セットを使用することはありません。
 - **読み取り** - サブジェクトは属性を読み取ることができます。
 - **書き込み** - サブジェクトは属性を変更することができます。
- 注:** System 属性に書き込みをすることはできません。
- **検索** - サブジェクトは属性を検索することができます。
 - **比較** - サブジェクトは属性を比較することができます。
- 「**閉じる**」をクリックして、「有効な ACL」パネルに戻ります。

有効所有者:

有効所有者とは、選択された項目についての、明示的でありかつ継承された所有者です。

「有効な所有者」テーブルには、対象 DN および有効な所有者の対象タイプについての読み取り専用情報が含まれます。

フィルターに処理されていない ACL:

新規の非フィルター ACL を項目に追加することも、既存の非フィルター ACL を編集することもできます。

フィルターに処理されていない ACL を伝搬できます。ある項目に対して定義されたアクセス制御情報は、その下位の項目すべてに適用できます。「ACL ソース」は、選択した項目に対する現在の ACL のソースです。項目に ACL がない場合、その項目は、親オブジェクトの ACL 設定に基づいて、親オブジェクトから ACL を継承します。

直接、または継承によってディレクトリー・オブジェクトに適用する ACL がない場合は、以下のデフォルト・アクセスが適用されます。

```
aclentry:group:CN=ANYBODY:normal:rsc:system:rsc:restricted:rsc
```

フィルターに掛けられていない ACL の追加または編集:

フィルターに処理されていない ACL を項目に追加またはフィルターに処理されていない既存の ACL を編集したりできます。フィルターに処理されていない ACL を伝搬できます。ある項目に対して定義されたアクセス制御情報は、その下位の項目すべてに適用できます。

手順

1. 「フィルターに掛けられていない ACL」タブを選択します。

注: 項目に、非フィルター ACL が存在しない場合、「ACL の伝搬」チェック・ボックスは事前選択され、変更できません。

2. 「伝搬 (Propagate)」チェック・ボックスを選択して、明示的に定義された ACL を持たない子孫がこの項目から継承することを許可します。このチェック・ボックスが選択されている場合、子孫はこの項目から ACL を継承します。また、子項目に対して ACL が明示的に定義されていれば、親から継承された ACL は、追加された新しい ACL に置換されます。このチェック・ボックスが選択されていない場合、明示的に定義された ACL がない子孫項目は、このオプションがオンにされている、その項目の親から、ACL を継承します。
3. 項目の新規アクセス権を作成する場合は「追加」をクリックします。既存の ACL を変更する場合は、既存の対象 DN を選択して「編集」をクリックします。
 - a. 「対象 DN」を指定します。選択した項目に対して操作を実行するためのアクセス権を要求するエンティティの DN を入力します。例えば、`cn=Ricardo Garcia,ou=austin,o=sample` です。ACL を編集の場合、このフィールドは変更できません。
 - b. 「対象タイプ」を指定します。ACL のタイプを選択します。例えば、DN がユーザーの場合は、「アクセス ID」を選択します。ACL を編集の場合、このフィールドは変更できません。
 - c. 「子の追加」メニューでは、選択した項目の下にディレクトリーを追加する権限を対象に付与するか、その権限を否認するかを選択します。この例で付与を選択した場合、Ricardo Garcia は `ou=Widget` 部門の下に子項目を追加できるようになります。
 - d. 「項目の削除」メニューでは、選択した項目を除去する権限を対象に付与するか、またはその権限を否認するかを選択します。この例の場合、`cn=Ricardo Garcia` に `ou=Widget Division` とその子項目の削除権を付与するか、またはその権限を否認するかを選択することになります。

- e. 「セキュリティ・クラス・アクセス権」では、各セキュリティ・クラスに対するアクセス権を設定します。個別に権限を付与することもできますし、「すべて許可」または「すべて拒否」をクリックすれば、グローバルに許可を付与または否認することもできます。この例の場合、Ricardo Garcia に各セキュリティ・クラスの全属性へのアクセス権を付与するかどうかを選択することになります。詳細については、559 ページの『アクセス権の表示』を参照してください。

注: 「すべて許可」を選択すると、Ricardo Garcia には ACL 自体を含む制限された属性へのアクセス権が付与されます。Ricardo Garcia は、項目への追加アクセス権を自分自身に対して付与できます。

例えば、管理者が Ricardo Garcia について、項目 ou=Widget

Division,ou=austin,o=sample に対する「項目の削除」権を否認した場合、Ricardo Garcia は、この項目やその子項目を削除することはできません。管理者が、セキュリティ・クラス許可の「すべて許可」もクリックした場合、Ricardo Garcia は ACL を変更できるようになります。Ricardo Garcia は ou=Widget Division,ou=austin,o=sample の子項目および親項目自体の削除権を自分自身に付与できるようになります。ACL 作成時にどうしても「すべて許可」を選択するという場合は、セキュリティを保護するために、制限されたクラスへの書き込み権を明示的に否認することが推奨されます。

- f. また、アクセス権は、属性が所属するセキュリティ・クラスではなく、属性に基づいて指定することもできます。
- 「属性の定義」ドロップダウン・リストから属性を選択します。
 - 「定義」をクリックします。属性は、許可表に表示されます。
 - 属性に関連付けられた 4 つの各セキュリティ・クラスそれぞれについて許可の付与または否認を指定するか、「すべて許可」または「すべて拒否」をクリックして、グローバルに許可を付与または否認します。
 - 複数の属性について、この手順を繰り返すことができます。
 - 属性を除去するには、属性を選択して、「削除」をクリックします。
 - 「OK」をクリックし、「ACL の編集」パネルに戻ります。
- g. 「OK」をクリックして、変更を保管し終了します。

フィルターに掛けられていない ACL の除去:

フィルターに掛けられていない ACL を項目から除去することができます。フィルターに処理されていない ACL を伝搬できます。ある項目に対して定義されたアクセス制御情報は、その下位の項目すべてに適用できます。

手順

1. 「フィルターに掛けられていない ACL」タブを選択します。
2. 削除する ACL の隣にあるラジオ・ボタンをクリックします。
3. 「除去」または「すべて除去」をクリックして、リストからすべての対象 DN を削除します。
4. 「OK」をクリックし、変更内容を保管します。

フィルターに処理された ACL:

フィルター・ベースの ACL は、ターゲット・オブジェクトとそれらのオブジェクトに適用される有効なアクセスとを突き合わせるために、指定されたオブジェクト・フィルターを使用してフィルター・ベースの比較を行います。

新規のフィルター ACL を項目に追加することも、既存のフィルター ACL を編集することもできます。

フィルター・ベースの ACL のデフォルト動作では、DIT での最下位の収容項目から、祖先項目チェーンを上に向かって、最上位の収容項目まで累算します。有効なアクセスは、構成する祖先項目によって付与または否認されたアクセス権の共用体として計算されます。この動作には例外があります。サブツリー複製機能との互換性のために、また管理制御を強化するために、上限属性を使用して、上限属性が含まれる項目で累算が停止されます。

直接、または継承によってディレクトリー・オブジェクトに適用する ACL がない場合は、以下のデフォルト・アクセスが適用されます。

```
ibm-filteraclentry:group:CN=ANYBODY:(objectclass=*)normal:rsc:system:rsc:restricted:rsc
```

フィルターに掛けられた ACL の追加および編集:

フィルター・ベースの比較を使用するには、フィルター ACL を項目に追加する必要があります。

手順

1. 「フィルターに掛けられた ACL」タブを選択します。
2. 「フィルターに処理された ACL」タブで、以下の情報を入力します。
 - a. 選択した項目から `ibm-filterACLInherit` 属性を除去するには、「指定なし」を選択します。
 - b. 選択した項目に対して ACL を許可するには、「**True**」を選択します。ACL は、DIT でのその項目から、祖先項目チェーンを上に向かって、最上位のフィルター ACL 収容項目まで累算します。
 - c. 選択した項目でのフィルター ACL の累算を停止するには、「**False**」を選択します。
3. 項目の新規アクセス権を作成する場合は「追加」をクリックします。既存のフィルターに掛けられた ACL を変更する場合は、既存の対象 DN を選択して「編集」をクリックします。
 - a. 「対象 DN」を指定します。選択した項目に対して操作を実行するためのアクセス権を要求するエンティティの DN を入力します。例えば、`cn=Ricardo Garcia,ou=austin,o=sample` です。ACL を編集中の場合は、このフィールドは変更できません。
 - b. 「対象タイプ」を指定します。ACL のタイプを選択します。例えば、DN がユーザーの場合は、「アクセス ID」を選択します。ACL を編集中の場合は、このフィールドは変更できません。

- c. 「子の追加」メニューでは、選択した項目の下にディレクトリーを追加する権限を対象に付与するか、その権限を否認するかを選択します。この例で付与を選択した場合、Ricardo Garcia は ou=Widget Division 部門の下に子項目を追加できるようになります。
- d. 「項目の削除」メニューでは、選択した項目を除去する権限を対象に付与するか、またはその権限を否認するかを選択します。この例の場合、cn=Ricardo Garcia に ou=Widget Division とその子項目の削除権を付与するか、またはその権限を否認するかを選択することになります。
- e. 「オブジェクト・フィルター」フィールドには、選択した ACL のフィルターを指定します。ACL は、このフィールドで指定したフィルターに一致する関連サブツリーの子孫オブジェクトに伝搬します。例えば、フィルターとして sn=Campbell を指定した場合、Ricardo Garcia には ou=Widget Division,ou=austin,o=sample の下位の項目 cn=David Campbell, cn=David Campbell, cn=James Campbell, cn=Michael Campbell+postalcode=4609 および cn=Michael Campbell へのアクセス権が付与されます。これは各項目に値が Campbell の sn 属性が含まれているからです。検索フィルター・ストリングの構成には、「フィルターの編集」をクリックします。
- f. 「セキュリティー・クラス・アクセス権」では、各セキュリティー・クラスに対するアクセス権を設定します。個別に権限を付与することもできますし、「すべて許可」または「すべて拒否」をクリックすれば、グローバルに許可を付与または否認することもできます。この例の場合、Ricardo Garcia に各セキュリティー・クラスの全属性へのアクセス権を付与するかどうかを選択することになります。詳細については、559 ページの『アクセス権の表示』を参照してください。

注: 「すべて許可」を選択すると、Ricardo Garcia には、ACL 自体を含む制限された属性へのアクセス権が付与されます。Ricardo Garcia は、項目への追加アクセス権を自分自身に対して付与することができます。例えば、管理者が Ricardo Garcia について、項目 ou=Widget Division,ou=austin,o=sample に対する「項目の削除」権を否認した場合、Ricardo Garcia は、この項目やその子項目を削除することはできません。管理者が、セキュリティー・クラス許可の「すべて許可」を同時にクリックした場合、Ricardo Garcia は ACL を変更できるようになり、ou=Widget Division,ou=austin,o=sample の子項目および親項目自体の削除権を自分自身に付与できるようになります。ACL 作成時にどうしても「すべて許可」を選択するという場合は、セキュリティーを保護するために、制限されたクラスへの書き込み権を明示的に否認することが推奨されます。

- g. また、アクセス権の指定は、属性が所属するセキュリティー・クラスではなく、属性に基づいて行うこともできます。
 - 「属性の定義」ドロップダウン・リストから属性を選択します。
 - 「定義」をクリックします。属性は、許可表に表示されます。
 - 属性に関連付けられた 4 つの各セキュリティー・クラスそれぞれについて許可の付与または否認を指定するか、「すべて許可」または「すべて拒否」をクリックして、グローバルに許可を付与または否認します。
 - 複数の属性について、この手順を繰り返すことができます。
 - 属性を除去するには、属性を選択して、「削除」をクリックします。

- 「OK」をクリックし、「ACL の編集」パネルに戻ります。
4. 「OK」をクリックして、変更を保管し終了します。

フィルターに掛けられた ACL の除去:

フィルター ACL を項目から除去することができます。フィルター・ベースの ACL は、フィルター・ベースの比較を行います。この比較の実行には、指定されたオブジェクト・フィルターが使用され、ターゲット・オブジェクトとそれらのオブジェクトに適用される有効なアクセスとが突き合わせられます。

手順

1. 「フィルターに掛けられた ACL」タブを選択します。
2. 削除する ACL の隣にあるラジオ・ボタンをクリックします。
3. 「除去」または「すべて除去」をクリックして、リストからすべての対象 DN を削除します。
4. 「OK」をクリックし、変更内容を保管します。

所有者:

項目の所有者は、オブジェクトに対するすべての操作を実行できる完全な許可を持っています。項目の所有者は、明示的にすることも、伝搬する (継承する) こともできます。所有者は、選択した項目の現在の所有者のソースです。

項目が所有者を祖先から継承しない場合は、このフィールドには、この項目はデフォルトから所有者を継承することを示すメッセージが表示されます。この項目に所有者を追加すると、継承された所有者がすべて上書きされます。デフォルトでは、ディレクトリー管理者はディレクトリーの全項目の所有者です。

所有者の追加:

以下の説明を参照して、所有者を追加します。

手順

1. 「所有者」タブを選択します。
2. 明示的に定義された所有者を持たない子孫がこの項目から継承するのを許可するには、「所有者の伝搬」チェック・ボックスを選択します。このチェック・ボックスが選択されていない場合、明示的に定義された所有者のない子孫項目は、このオプションが使用可能であるその項目の親から、所有者を継承します。
3. 「対象 DN」を指定します。選択した項目に対する所有者アクセスを許可しているエンティティの識別名 (DN) を入力します。例えば、cn=Ricardo Garcia,ou=austin,o=sample です。
4. DN の「対象タイプ」を選択します。たとえば、DN がユーザーの場合は「アクセス ID」を選択します。
5. 「追加」をクリックします。
6. さらに所有者を作成する場合は、この手順を繰り返します。
7. 完了したら、「OK」をクリックして変更を保管し、「項目の管理」パネルを終了します。

所有者の除去:

以下の説明を参照して、項目から所有者を除去します。

手順

1. 「所有者」タブを選択します。
2. 項目のリストから、削除する所有者を選択します。
3. 「除去」をクリックします。 リストからすべてのサブジェクト DN を削除するには、「すべて除去」をクリックします。
4. 「OK」をクリックし、変更内容を保管します。

コマンド行ユーティリティーによる ACL の管理

LDIF ユーティリティーの使用による ACL の管理については、以下の説明で詳細を把握できます。

ACI と項目の所有者の定義:

以下に示す例を使用すると、ACL と項目の所有者を定義できます。

このタスクについて

以下の 2 つの例は、設定中の管理サブドメインを示しています。最初の例は、ドメイン全体の entryOwner として割り当てられている単一ユーザーを示しています。2 番目の例は、entryOwner として割り当てられているグループを示しています。

```
entryOwner: access-id:cn=Person A,o=sample
ownerPropagate: true

entryOwner: group:cn=System Owners, o=sample
ownerPropagate: true
```

次の例は、アクセス ID "cn=Person 1, o=sample" に対して、attribute1 の読み取り、検索、および比較の許可を与える方法を示しています。許可は、サブツリー全体のすべてのノード、"(objectclass=groupOfNames)" 比較フィルターと一致するこの ACI を含むノード、またはそのノードの下に適用されます。祖先ノードで一致する ibm-filteraclentry 属性の累算は、ibm-filterAclInherit 属性を "false" に設定することで、この項目で終了しています。

```
ibm-filterAclEntry: access-id:cn=Person 1,o=sample:(objectclass=groupOfNames):
at.attribute1:grant:rsc

ibm-filterAclInherit: false
```

次の例は、グループ "cn=Dept XYZ, o=sample" に対して、attribute1 の読み取り、検索、および比較の許可を与える方法を示しています。この許可は、この ACI を含むノードの下のサブツリー全体に適用されます。

```
aclEntry: group:cn=Dept XYZ,o=sample:at.attribute1:grant:rsc
aclPropagate: true
```

次の例は、役割 "cn=System Admins,o=sample" に対して、このノードの下にオブジェクトを追加する許可と、attribute2 と critical 属性クラスの読み取り、検索、および比較の許可を与える方法を示しています。この許可は、この ACI を含むノードにしか適用されません。

```
aclEntry: role:cn=System Admins,o=sample:object:grant:a:at.
attribute2:grant:rsc:critical:grant:rsc
aclPropagate: false
```

ACI 値と項目の所有者値の変更:

ACI の値や entryOwner の値の変更は、以下の情報に従って実行します。

手順

1. 属性の値を作成または置換します。

Modify-replace

Modify-replace は、他のすべての属性と同じように機能します。属性値が存在しない場合は、値を作成します。属性値が存在する場合は、値を置換します。以下に例を示します。

項目での元の ACI:	実行する変更:	結果としての ACI:
aclEntry: group:cn=Dept ABC,o=sample:normal:grant:rsc aclPropagate: true	dn: cn=some entry changetype: modify replace: aclEntry aclEntry: group:cn=Dept XYZ,o=sample:normal:grant:rsc	aclEntry: group:cn=Dept XYZ,o=sample:normal:grant:rsc aclPropagate: true この置換アクションにより、Dept ABC の ACI 値は失われます。
ibm-filterAclEntry: group:cn=Dept ABC,o=sample: (cn=Manager ABC):normal :grant:rsc ibm-filterAclInherit: true	dn: cn=some entry changetype: modify replace: ibm-filterAclEntry ibm-filterAclEntry: group:cn=Dept XYZ,o=sample: (cn=Manager XYZ):normal :grant:rsc dn: cn=some entry changetype: modify replace: ibm-filterAclInherit ibm-filterAclInherit: false	ibm-filterAclEntry: group:cn=Dept XYZ,o=sample: (cn=Manager XYZ):normal :grant:rsc ibm-filterAclInherit: false この置換アクションにより、Dept ABC の ACI 値は失われます。

2. ACI または entryOwner に値を追加します。

Modify-add

idsldapmodify-add の実行中に、ACI または entryOwner が存在しない場合は、特定の値を持った ACI または entryOwner が作成されます。ACI または entryOwner が存在する場合は、指定された値を ACI または entryOwner に追加します。以下に例を示します。

項目での元の ACI:	加える変更:	生成される複数値 aclEntry:
aclEntry: group:cn=Dept XYZ,o=sample: normal:grant:rsc	dn: cn=some entry changetype: modify add: aclEntry aclEntry: group:cn=Dept ABC,o=sample: at.attributel:grant:rsc	aclEntry: group:cn=Dept XYZ,o=sample: normal:grant:rsc aclEntry: group:cn=Dept ABC,o=sample: at.attributel:grant:rsc
ibm-filterAclEntry: group:cn=Dept XYZ,o=sample: (cn=Manager XYZ):normal :grant:rsc	dn: cn=some entry changetype: modify add: ibm-filterAclEntry ibm-filterAclEntry: group:cn=Dept ABC,o=sample: (cn=Manager ABC) :at.attributel:grant:rsc	ibm-filterAclEntry: group:cn=Dept XYZ,o=sample: (cn=Manager XYZ):normal :grant:rsc ibm-filterAclEntry: group:cn=Dept ABC,o=sample: (cn=Manager ABC):at.attributel :grant:rsc

同じ属性または属性クラスの下での許可は、基本的なビルディング・ブロックと見なされます。また、アクションは、修飾子と見なされます。同じ許可値が複数回追加されている場合でも、保管される値は 1 つのみです。同じ許可値が複数回追加されていても、アクション値がそれぞれ異なる場合、最後のアクション値が使用されます。結果の許可フィールドが空 ("") の場合、この許可値はヌルに設定され、アクション値は grant に設定されます。以下に例を示します。

項目での元の ACI:	加える変更:	生成される複数値 aclEntry:
aclEntry: group:cn=Dept XYZ,o=sample:normal:grant:rsc	dn: cn=some entry changetype: modify add: aclEntry aclEntry: group:cn=Dept XYZ,o=IBM:normal:deny:r:critical: deny::sensitive :grant:r	aclEntry: group:cn=Dept XYZ,o=sample:normal:grant:sc: normal:deny:r:critical :grant::sensitive:grant:r
ibm-filterAclEntry: group:cn=Dept XYZ,o=sample: (cn=Manager XYZ):normal :grant:rsc	dn: cn=some entry changetype: modify add: ibm-filterAclEntry ibm-filterAclEntry: group:cn=Dept XYZ,o=sample: (cn=Manager XYZ):normal :deny:r:critical:deny::sensitive:grant:r	ibm-filterAclEntry: group:cn=Dept XYZ,o=sample: (cn=Manager XYZ):normal :grant:sc:normal:deny:r:critical:grant::sensitive :grant:r

3. 特定の ACI 値を削除します。

Modify-delete

特定の ACI 値を削除するには、通常の `idsldapmodify-delete` 構文を使用します。

項目での元の ACI:	生成されサーバー上で存続する ACI
<code>aciEntry: group:cn=Dept XYZ,o=sample:object:grant:ad aciEntry: group:cn=Dept XYZ,o=sample:normal:grant:rws dn: cn = some entry changetype: modify delete: aciEntry aciEntry: group:cn=Dept XYZ,o=sample:object:grant:ad</code>	<code>aciEntry: group:cn=Dept XYZ,o=sample:normal:grant:rws</code>
<code>ibm-filterAciEntry: group:cn=Dept XYZ,o=sample:(cn=Manager XYZ):object:grant:ad ibm-filterAciEntry: group:cn=Dept XYZ,o=sample:(cn=Manager XYZ):normal:grant:rws dn: cn = some entry changetype: modify delete: ibm-filterAciEntry ibm-filterAciEntry: group:cn=Dept XYZ,o=sample:(cn=Manager XYZ):object:grant:ad</code>	<code>ibm-filterAciEntry: group:cn=Dept XYZ,o=sample:(cn=Manager XYZ):normal:grant:rws</code>

存在しない ACI 値または `entryOwner` 値を削除しても、ACI または `entryOwner` は変更されず、属性値が存在しないことを示す戻りコードが返されます。

ACI 値または項目の所有者値の削除:

以下の説明を参照して、ACI 値または項目の所有者値を削除します。

手順

1. 以下の値を指定し、`idsldapmodify-delete` 操作を使用して、`entryOwner` を削除します。

```
dn: cn = some entry  
changetype: modify  
delete: entryOwner
```

項目からは、明示的な `entryOwner` がなくなります。 `ownerPropagate` も自動的に除去されます。この項目は、伝搬規則に従って、ディレクトリー・ツリー内の祖先ノードからその `entryOwner` を継承します。

2. `aciEntry` を完全に削除します。次のアクションを実行します。

```
dn: cn = some entry  
changetype: modify  
delete: aciEntry
```

最後の ACI 値または `entryOwner` 値を項目から削除することと、ACI または `entryOwner` を削除することとは異なります。項目には、値を持たない ACI または `entryOwner` を含めることができます。ACI や `entryOwner` を照会しても、クライアントには何も返されません。また、設定は、オーバーライドされるまでは、子孫ノードに伝搬されます。いずれのユーザーもアクセスできないような懸垂項目を防止するため、ディレクトリー管理者は、項目にヌルの ACI 値または `entryOwner` 値がある場合であっても、その項目への完全なアクセス権を常に所有します。

ACI 値または項目の所有者値の取得:

以下の情報により、ACI 値または項目の所有者値を取得できます。

手順

1. 有効な ACI 値または `entryOwner` 値は、想定している ACL または `entryOwner` 属性を検索で指定して取得します。以下に例を示します。

```
idslapsearch -b "cn=object A, o=sample" -s base "objectclass=*"
aclentry aclpropagate aclsource entryowner ownerpropagate ownersource
ibm-filterAclEntry ibm-filterAclInherit ibm-effectiveAcl
```

このアクションにより、オブジェクト A に対するアクセス評価で使用される ACL または entryOwner の情報がすべて返されます。

注: 戻り値は、最初に定義した値と異なる場合があります。値は、元の形式と同等です。

ibm-filterAclEntry 属性のみを検索すると、収容項目固有の値のみが返されません。

読み取り専用の運用属性 ibm-effectiveAcl は、累算された有効なアクセスを表示するために使用されます。ibm-effectiveAcl の検索要求では、非フィルター ACL またはフィルター ACL が DIT 内にどのように分散されているかによって、非フィルター ACL またはフィルター ACL に基づいて、ターゲット・オブジェクトに適用される有効なアクセスが返されます。

フィルター・ベースの ACL は、複数の祖先ソースから発生することがあるため、aclSource 属性の検索により、関連するソースのリストが作成されます。

2. オプション: 情報を表示して、ACI 値または entryOwner 値が取得されていることを確認します。

サブツリー複製に関する考慮事項

サブツリー複製では、すべての aclEntry 属性と ibm-filterAclEntry 属性について、フィルター・ベースまたは非フィルター・ベースのアクセスに関する考慮事項があります。

サブツリー複製に関する、以下の 2 つのタイプの考慮事項があります。

- サブツリー複製に組み込まれる非フィルター・ベースのアクセスでは、すべての aclEntry 属性が、関連する ibm-replicationContext 項目に存在する必要があります。複製されたサブツリーの上位にある祖先項目から有効なアクセス権を伝搬できないため、aclPropagate 属性の値を **true** に設定する必要があります。
- サブツリー複製に組み込まれるフィルター・ベースのアクセスでは、すべての ibm-filter AclEntry 属性が、関連する ibm-replicationContext 項目または項目の下に存在する必要があります。複製されたサブツリーの上位にある祖先項目から有効なアクセス権を累算できないため、ibm-filterAclInherit 属性は、値を **false** に設定して、関連する ibm-replicationContext 項目に常駐させる必要があります。

グループと役割

グループと役割には、sample.Idif ファイルに含まれている項目を使用します。このファイルは、IBM Security Directory Server の **examples** ディレクトリーにあります。

ランチ・クラブを編成する 3 つのグループを作成します。

- 1 番目のグループは静的グループで、月曜日に一緒にランチを食べる人をリストします。

- 2 番目のグループは動的グループで、火曜日に一緒にランチを食べる人をリストします。このグループは、部門 (ウィジェット部門) のすべてのメンバーをリストします。動的グループの利点は、新規のユーザー項目の追加など、サブツリー項目に変更を行うと、グループでも同様の変更が動的に行われる点です。
- 3 番目のグループは、他の 2 つのグループのコンテナとなるネストされたグループです。

グループ (Groups)

グループは、名前の集合などのリストです。これは、静的、動的、または、ネストされた、です。

グループは、アクセスを制御するために **aclentry**、**ibm-filterAclEntry**、および **entryowner** の各属性で使用したり、メーリング・リストなどのアプリケーション固有の用途で使用したりすることができます。546 ページの『アクセス制御リスト』を参照してください。

静的グループ

静的グループは、構造化オブジェクト・クラス `groupOfNames`、`groupOfUniqueNames`、`accessGroup`、または `accessRole`、あるいは、補助オブジェクト・クラス `ibm-staticgroup` または `ibm-globalAdminGroup` を使用して、各メンバーを個別に定義します。

構造化オブジェクト・クラス `groupOfNames` または `groupOfUniqueNames` を使用する静的グループには、少なくとも 1 つの `member` または `uniqueMember` が必要です。

IBM Security Directory Server は、静的グループの部分的な参照整合性を強制的に維持します。参照整合性はデータベースの概念で、テーブル間の関係が常に一貫することを保証します。静的グループをディレクトリーに追加した場合、メンバーはそのディレクトリーに存在する必要がなくなります。ただし、オブジェクトをディレクトリーから削除すると、そのオブジェクトをメンバーとして所有していたすべての静的グループは自動的に更新され、グループのメンバーのリストからそのオブジェクトは除去されます。また、ディレクトリー内のオブジェクトの名前を変更すると、そのオブジェクトをメンバーとして所有していたすべての静的グループおよびネストされたグループは自動的に更新され、グループのメンバーのリスト内のそのオブジェクトの名前が変更されます。

注: この概念は動的グループには適用されません。これは動的グループが検索ベースだからです。また、ディレクトリーからオブジェクトを削除すると、検索結果からそのオブジェクトは自動的に除外されます。

一般的なグループ項目を以下に示します。

```
DN: cn=Dev.Staff,ou=Austin,o=sample
objectclass: accessGroup
cn: Dev.Staff
member: cn=John Doe,ou=Austin,o=sample
member: cn=Jane Smith,ou=Austin,o=sample
member: cn=James Smith,ou=Austin,o=sample
```

各グループ・オブジェクトには、メンバー DN からなる複数値の属性が含まれません。

アクセス・グループを削除すると、そのアクセス・グループは、適用されているすべての ACL から削除されます。

注: 参照整合性により、メンバーが属するグループ項目の `modifyTimeStamp` が更新されます。複製環境では、型削除の `ldap` 操作である `modrdn`、つまり一方のツリーから他方のツリーへのメンバー項目の移動を行うと、マスター (サプライヤー) とレプリカ (コンシューマー) の両方の参照整合性が呼び出されます。マスターおよびレプリカ上のグループ項目では、異なるタイム・スタンプ値が記録されることにより発生する可能性があるレプリカ生成上の競合を防止するため、影響を受けるグループの `modifyTimeStamp` を、前回の操作で影響を受けたメンバー項目の `modifyTimeStamp` の値に設定します。ただし、前回の操作の `modifyTimeStamp` がグループの既存の `modifyTimeStamp` より後の時刻であることが条件です。

動的グループ

動的グループは、静的グループとは別の方法でメンバーを定義します。動的グループは、個々にメンバーをリストするのではなく、LDAP 検索を使用してメンバーを定義します。

動的グループは、構造化オブジェクト・クラス `groupOfURLs` (または補助オブジェクト・クラス `ibm-dynamicGroup`) と属性 `memberURL` を使用して、簡略 LDAP URL 構文を使った検索を定義します。

```
ldap:///<base DN of search> ? ? <scope of search> ? <searchfilter>
```

注: この例に示すように、構文にホスト名は指定しないでください。その他のパラメーターは、LDAP の通常の URL 構文と同じように指定します。パラメーターを指定しない場合でも、各パラメーター・フィールドを「?」で区切る必要があります。一般に、戻される一連の属性は、基本 DN と検索範囲の間に含まれています。このパラメーターは、動的メンバーシップの判別時にはサーバーで使用されないため、除外することができます。分離文字 ? が必要です。

説明:

base DN of search

ディレクトリー内の検索の開始点です。サフィックスやディレクトリーのルート (`ou=Austin` など) を指定できます。このパラメーターは必須です。

scope of search

検索の範囲を指定します。デフォルトの有効範囲は `sub` です。

基本 URL に指定された基本 DN についての情報のみを戻します。

1 URL に指定された基本 DN の 1 レベル下の項目について情報を戻します。これには、基本項目は含まれません。

サブ 基本 DN とその下にあるすべてのレベルの項目について情報を戻します。

searchfilter

検索の有効範囲内の項目に適用するフィルターです。検索フィルターの構文について詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の `idsldapsearch` コマンドの情報を参照してください。デフォルトは `objectclass=*` です。

動的メンバーの検索は常にサーバー内部で行われます。そのため、完全な LDAP URL を指定する場合とは異なり、ホスト名とポート番号は指定されません。また、プロトコルは常に **ldap** が使用されます (**ldaps** ではありません)。**memberURL** 属性には各種の URL が含まれますが、サーバーは、**ldap:///** で始まる **memberURL** のみを使用して、動的メンバーを判別します。

例:

以下に示す例を参照して、動的グループ内の項目を処理できます。

スコープが **sub** にデフォルト設定され、フィルターが **objectclass=*** にデフォルト設定される単一項目の場合:

```
ldap:///cn=John Doe, cn=Employees, o=Acme, c=US
```

cn=Employees の 1 レベル下にあり、フィルターが **objectclass=*** にデフォルト設定されるすべての項目の場合:

```
ldap:///cn=Employees, o=Acme, c=US??one
```

o=Acme の下にあり、**objectclass=person** が指定されているすべての項目の場合:

```
ldap:///o=Acme, c=US??sub?objectclass=person
```

ユーザー項目を定義するオブジェクト・クラスにもよりますが、項目には、グループ・メンバーシップの判別に適した属性が含まれない場合があります。補助オブジェクト・クラス **ibm-dynamicMember** を使用すると、ユーザー項目を拡張して **ibm-group** 属性を含めることができます。この属性を使用すると、動的グループのフィルターのターゲットとして機能するユーザー項目に任意の値を追加できます。

例: 以下の動的グループのメンバーは、**cn=users,ou=Austin** 項目の直下にある項目であり、**GROUP1** という **ibm-group** グループ属性があります。

```
dn: cn=GROUP1,ou=Austin
objectclass: groupOfURLs
cn: GROUP1
memberURL: ldap:///cn=users,ou=Austin??one?(ibm-group=GROUP1)
```

以下に **cn=GROUP1,ou=Austin** のメンバーの例を示します。

```
dn: cn=Group 1 member, cn=users, ou=austin
objectclass: person
objectclass: ibm-dynamicMember
cn: Group 1 member
sn: member
userpassword: memberpassword
ibm-group: GROUP1
```

ネストされたグループ

グループをネストすると、階層関係を作成できます。階層関係を使用すると、継承されたグループ・メンバーシップを定義できます。ネストされたグループは、親グループ項目として定義されます。グループ項目は、その親グループ項目のメンバーに属します。

ネストされたグループは、**ibm-nestedGroup** 補助オブジェクト・クラスを追加して、構造化グループ・オブジェクト・クラスの 1 つを拡張することで作成されます。ネストされたグループを拡張すると、ゼロ個以上の **ibm-memberGroup** 属性を追加できます。**ibm-memberGroup** の値には、ネストされた子グループの DN を設定できます。例:

```
dn: cn=Group 2, cn=Groups, o=sample
objectclass: groupOfNames
objectclass: ibm-nestedGroup
objectclass: top
cn: Group 2
description: Group composed of static, and nested members.
member: cn=Person 2.1, cn=Dept 2, cn=Employees, o=sample
member: cn=Person 2.2, cn=Dept 2, cn=Employees, o=sample
ibm-memberGroup: cn=Group 8, cn=Nested Static, cn=Groups, o=sample
```

ネストされた静的なグループ階層に循環を導入することは許されていません。ネストされた静的なグループ操作によって循環参照が直接的にまたは継承を介して発生したことが確認された場合、それは制約違反と見なされるため、項目は更新されません。

混成グループ

本書で説明する構造化グループ・オブジェクト・クラスは、静的、動的、およびネストされたメンバー型の組み合わせでグループ・メンバーシップが記述されるように拡張できます。

```
dn: cn=Group 10, cn=Groups, o=sample
objectclass: groupOfURLs
objectclass: ibm-nestedGroup
objectclass: ibm-staticGroup
objectclass: top
cn: Group 10
description: Group composed of static, dynamic, and nested members.
memberURL: ldap:///cn=Austin, cn=Employees, o=sample??one?objectClass=person
ibm-memberGroup: cn=Group 9, cn=Nested Dynamic, cn=Groups, o=sample
member: cn=Person 10.1, cn=Dept 2, cn=Employees, o=sample
member: cn=Person 10.2, cn=Dept 2, cn=Employees, o=sample
```

グループ・メンバーシップの判別

この機能を使用すると、グループ・メンバーシップを判別できます。

2 つの運用属性が、集合グループ・メンバーシップの照会に使用できます。

ibm-allMembers 運用属性は、特定のグループ項目について、一連の集合グループ・メンバーシップを列挙します (これには、ネストされたグループ階層によって記述された、静的メンバー、動的メンバー、およびネストされたメンバーが含まれます)。**ibm-allGroups** 運用属性は、特定のユーザー項目について、グループのセットの集合を列挙します (これには、そのユーザーにメンバーシップがある祖先グループが含まれます)。

注:

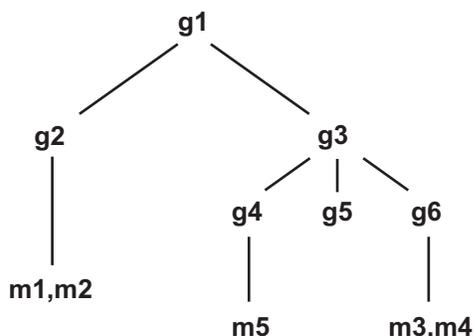
- **ibm-allMembers** 運用属性は、分散環境でも処理されます。
- ネストされたグループの動的なメンバーがプロキシ・サーバーによって取得されるのは、メンバーが同じバックエンド・サーバーに存在する場合に限られます。また、プロキシ・サーバーの場合は、グローバル管理グループのメンバーのみが **ibm-allMembers** を検索できます。
- **ibm-allMembers** 検索は、ベース検索の場合にのみサポートされます。
- **ibm-allMembers** および **ibm-allGroups** 運用属性の値は、実行時に判別されます。したがって大規模なディレクトリーの場合、操作時間が長くなる場合があります。

要求者は、データに対する ACL の設定に応じて、要求したデータの一部しか受け取れないことがあります。運用属性 **ibm-allMembers** と **ibm-allGroups** はいずれのユーザーでも要求できますが、戻されるデータ・セットには、その要求者がアクセス権を持っている LDAP 項目と属性のデータしか含まれません。**ibm-allMembers**

属性または **ibm-allGroups** 属性を要求するユーザーの場合、静的メンバーを参照するには、そのグループおよびネストしたグループの **member** 属性値または **uniquemember** 属性値へのアクセス権を持っている必要があります。また、動的メンバーを参照するには、**memberURL** 属性値に指定されている検索を実行する権限を持っている必要があります。

階層の例:

以下に示す例を参照して、グループ・メンバーシップの判別の詳細を把握できます。



この例の場合は、ディレクトリーに以下の項目があると想定しています。

```

dn: cn=g1,cn=groups,o=sample
objectclass: groupOfNames
objectclass: ibm-nestedGroup
cn: g1
ibm-memberGroup: cn=g2,cn=groups,o=sample
ibm-memberGroup: cn=g4,cn=groups,o=sample
ibm-memberGroup: cn=g5,cn=groups,o=sample

dn: cn=m1, cn=users,o=sample
objectclass: person
cn: m1
sn: one
aclentry: access-id:cn=user1,cn=users,o=sample:normal:rsc
aclentry: access-id:cn=user2,cn=users,o=sample:normal:rsc

dn: cn=m2, cn=users,o=sample objectclass: person
cn: m2
sn: two
aclentry: access-id:cn=user1,cn=users,o=sample:normal:rsc
aclentry: access-id:cn=user2,cn=users,o=sample
  
```

m1 および **m2** は、**g2** の **member** 属性に属していると想定します。**g2** の ACL により、**user1** はメンバー属性を読み取ることができますが、**user2** にはメンバー属性へのアクセス権がありません。**g2** 項目の項目 LDIF は、以下のとおりです。

```

dn: cn=g2,cn=groups,o=sample
objectclass: accessGroup
cn: g2
member: cn=m1,cn=users,o=sample
member: cn=m2,cn=users,o=sample
aclentry: access-id:cn=user1,cn=users,o=sample:normal:rsc
aclentry: access-id:cn=user2,cn=users,o=sample:normal:rsc:at.member:deny:rsc
  
```

g4 項目ではデフォルトの **aclentry** が使用されますが、これにより、**user1** と **user2** は、ともに **g4** のメンバー属性を読み取ることができます。**g4** 項目の LDIF は、以下のとおりです。

```

dn: cn=g4, cn=groups,o=sample
objectclass: accessGroup
cn: g4
member: cn=m5, cn=users,o=sample
  
```

g5 項目は動的グループであり、その 2 つのメンバーを `memberURL` 属性から取得します。**g5** 項目の LDIF は、以下のとおりです。

```
dn: cn=g5, cn=groups, o=sample
objectclass: container
objectclass: ibm-dynamicGroup
cn: g5
memberURL: ldap:///cn=users, o=sample??sub?(|(cn=m3)(cn=m4))
```

項目 **m3** および **m4** は、`memberURL` が一致するので、グループ **g5** のメンバーです。**m3** 項目の ACL は、**user1** および **user2** に対してこの項目の検索を許可していません。**m4** 項目の ACL は、**user2** に対してこの項目の検索を許可していません。**m4** 項目の LDIF を以下に示します。

```
dn: cn=m3, cn=users, o=sample
objectclass: person
cn: m3
sn: three
aclentry: access-id:cn=user1, cn=users, o=sample:normal:rsc
aclentry: access-id:cn=user2, cn=users, o=sample:normal:rsc
```

```
dn: cn=m4, cn=users, o=sample
objectclass: person
cn: m4
sn: four
aclentry: access-id:cn=user1, cn=users, o=sample:normal:rsc
aclentry: access-id:cn=user2, cn=users, o=sample
```

例 1: **user1** が、グループ **g1** のすべてのメンバーを取得するために、検索を実行します。**user1** はすべてのメンバーに対するアクセス権を持っているので、すべてのメンバーが戻ります。

```
idsldapsearch -D cn=user1, cn=users, o=sample -w user1pwd -s base -b cn=g1,
cn=groups, o=sample objectclass=* ibm-allmembers
```

```
cn=g1, cn=groups, o=sample
ibm-allmembers: CN=M1, CN=USERS, o=sample
ibm-allmembers: CN=M2, CN=USERS, o=sample
ibm-allmembers: CN=M3, CN=USERS, o=sample
ibm-allmembers: CN=M4, CN=USERS, o=sample
ibm-allmembers: CN=M5, CN=USERS, o=sample
```

例 2: **user2** が、グループ **g1** のすべてのメンバーを取得するために、検索を実行します。**user2** はグループ **g2** メンバー属性に対するアクセス権を持っていないので、メンバー **m1** および **m2** にアクセスできません。**user2** は **g4** のメンバー属性に対するアクセス権を持っているので、メンバー **m5** にアクセスすることができます。**user2** は、グループ **g5** の `memberURL` で項目 **m3** に対する検索を実行し、メンバーをリストすることができますが、**m4** に対する検索を実行することはできません。

```
idsldapsearch -D cn=user2, cn=users, o=sample -w user2pwd -s base -b cn=g1,
cn=groups, o=sample objectclass=* ibm-allmembers
```

```
cn=g1, cn=groups, o=sample
ibm-allmembers: CN=M3, CN=USERS, o=sample
ibm-allmembers: CN=M5, CN=USERS, o=sample
```

例 3: ユーザー 2 は、検索を実行して、**m3** がグループ **g1** のメンバーであるかどうかを確認します。ユーザー 2 にはこの検索に対するアクセス権があるので、検索では、**m3** がグループ **g1** のメンバーであることが示されます。

```
idsldapsearch -D cn=user2, cn=users, o=sample -w user2pwd -s base -b cn=m3,
cn=users, o=sample objectclass=* ibm-allgroups
```

```
cn=m3, cn=users, o=sample
ibm-allgroups: CN=G1, CN=GROUPS, o=sample
```

例 4: ユーザー 2 は、検索を実行して、**m1** がグループ **g1** のメンバーであるかどうかを確認します。ユーザー 2 にはメンバー属性に対するアクセス権がないので、検索では、**m1** がグループ **g1** のメンバーであることは示されません。

```
idsldapsearch -D cn=user2,cn=users,o=sample -w user2pwd -s base -b
cn=m1,cn=users,o=sample objectclass=* ibm-allgroups
```

```
cn=m1,cn=users,o=sample
```

例 5: ユーザーに関連付けられている ACL によっては、動的グループの **ibm-allMembers** 運用属性を構成している検索の評価結果が変動する場合があります。この例では、アクセス制御が動的グループの **ibm-allMembers** 運用属性の評価にどのように影響するかを示します。

LDIF の 2 つのグループの項目が以下のように定義されたとします。

```
dn: cn=claims,cn=groups,o=sample
objectclass: top
objectclass: groupOfURLs
memberURL: ldap:///cn=users,o=sample??sub?((ibm-group=claims)
cn: claims
```

```
dn: cn=departmentNum, cn=groups, o=sample
objectclass: top
objectclass: groupOfURLs
memberURL: ldap:///cn=users,o=sample??one?((departmentnumber=2001)
(departmentnumber=2002))
```

LDIF のユーザーの項目が以下のように定義されたとします。

```
dn: uid=adavid, cn=users, o=sample
objectclass: top
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: ibm-dynamicMember
cn: Al
sn: David
departmentnumber: 2001
ibm-group: claims
```

```
dn: uid=jchevy, cn=users, o=sample
objectclass: top
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: ibm-dynamicMember
cn: Jerry
sn: Chevy
departmentnumber: 2002
ibm-group: claims
```

ここでは、デフォルトのアクセス制御である **cn=anybody** を使用します。これには読み取り、検索、比較という 3 つの権限があります。この DN のアクセス・クラスは「normal」と定義されています。

必須の管理特権を持つユーザーが、これらのグループの **ibm-allMembers** を返す検索を実行すると、次の結果が返されます。

```
idsldapsearch -D cn=root -w ? -b "cn=groups, o=sample" -s one objectclass=*
ibm-allMembers
```

```
cn=departmentNum,cn=groups,o=sample
ibm-allMembers=uid=adavid,cn=users,o=sample
ibm-allMembers=uid=jchevy,cn=users,o=sample
```

```
cn=claims,cn=groups,o=sample
ibm-allMembers=uid=adavid,cn=users,o=sample
ibm-allMembers=uid=jchevy,cn=users,o=sample
```

結果として、検索条件 **departmentnumber=2001** または **departmentnumber=2002** および **ibm-group=claims** に合致する項目が表示されます。

同じ検索を匿名で実行すると、次のような検索結果が返されます。

```
idsldapsearch -b "cn=groups, o=sample" -s one objectclass=* ibm-allMembers
```

```
cn=departmentNum,cn=groups,o=sample
ibm-allMembers=uid=adavid,cn=users,o=sample
ibm-allMembers=uid=jchevy,cn=users,o=sample
```

```
cn=claims,cn=groups,o=sample
```

表示された結果を見ると、**departmentNum** グループのメンバーで、検索条件 **departmentnumber=2001** または **departmentnumber=2002** に合致する項目が返されており、**claims** グループのメンバーとして返された項目はありません。

この理由は、IBM-group 属性のアクセス・クラスは「critical」と定義されているのに対して、departmentnumber 属性のアクセス・クラスは「normal」と定義されているためです。さらに匿名ユーザーには、アクセス・クラスが「critical」の属性に対する検索権限がありません。

動的グループでは、メンバーを LDAP 検索を使用して定義します。このため、動的メンバーの検索とグループ・メンバーシップの決定はディレクトリー・サーバーの内部で行われ、アクセス制御は適用されません。

ただし、クライアント・アプリケーションが他のアプリケーション内部での権限を管理するために IBM-allGroups を取得する場合は、必ず、必要な権限を備えた ID を使用してこれらの検索が行われるようにする必要があります。

グループ・オブジェクト・クラス

各種の使用可能なグループ・オブジェクト・クラスを把握します。

ibm-dynamicGroup

この補助クラスでは、オプションの属性の memberURL を使用できます。静的メンバーと動的メンバーの両方を持つ混成グループを作成するには、これを groupOfNames などの構造化クラスとともに使用します。

ibm-dynamicMember

この補助クラスでは、オプションの属性の ibm-group を使用できます。これは、動的グループ用のフィルター属性として使用します。

ibm-nestedGroup

この補助クラスでは、オプションの属性の ibm-memberGroup を使用できます。親グループ内でサブグループをネストできるようにするには、これを groupOfNames などの構造化クラスとともに使用します。

ibm-staticGroup

この補助クラスでは、オプションの属性の member を使用できます。静的メンバーと動的メンバーの両方を持つ混成グループを作成するには、これを groupOfURLs などの構造化クラスとともに使用します。

注: **ibm-staticGroup** は、member がオプションである唯一のクラスです。member を使用するそれ以外のすべてのクラスでは、最低 1 つのメンバーが必要です。

groupOfNames

グループ名の項目を定義します。順序不問の名前のリストを含むリストを示します。

groupOfUniqueNames

固有の名前のグループの項目を定義します。

accessGroup

アクセス・コントロールに使用されるグループ。

groupOfURLs

URL のグループを示します。

グループ属性タイプ

各種の使用可能なグループ属性タイプを把握します。

ibm-allGroups

項目が属しているグループをすべて表示します。項目は、member 属性、uniqueMember 属性、または memberURL 属性によって直接メンバーにすることができます。あるいは、ibm-memberGroup 属性によって間接的にメンバーにすることができます。検索フィルターでは、Read-only 運用属性を使用することはできません。

ibm-allMembers

グループのメンバーをすべて表示します。項目は、member 属性、uniqueMember 属性、または memberURL 属性によって直接メンバーにすることができます。あるいは、ibm-memberGroup 属性によって間接的にメンバーにすることができます。検索フィルターでは、Read-only 運用属性を使用することはできません。

ibm-group

補助クラス ibm-dynamicMember で使用される属性です。動的グループ内にある項目のメンバーシップを制御する任意の値を定義するには、この属性を使用します。例えば、フィルター `ibm-group=Bowling Team` がある任意の memberURL に項目を含めるには、値 `Bowling Team` を追加します。

ibm-memberGroup

補助クラス `ibm-nestedGroup` で使用される属性です。親グループ項目のサブグループを識別します。このようなサブグループのメンバーは、ACL、または運用属性の `ibm-allMembers` と `ibm-allGroups` を処理する際に、親グループのメンバーと見なされます。サブグループ項目それ自体は、メンバーではありません。ネストされたメンバーシップは再帰的です。

member

グループのメンバーごとに識別名を示します。

uniquemember

各名前に `uniqueIdentifier` を与えてその固有性を保証する項目と関連する名前グループを示します。`uniqueMember` 属性の値は DN でその後に `uniqueIdentifier` が続きます。

memberURL

グループの各メンバーに関連する URL を示します。あらゆるタイプのラベル付き URL を使用できます。

静的グループ項目の作成

Web 管理ツールを使用して、以下の手順を実行すると、静的グループ項目を作成できます。

このタスクについて

ナビゲーション領域の「ディレクトリー管理」カテゴリーがまだ展開されていない場合は、それを展開します。

手順

1. 「項目の追加」をクリックします。
2. ドロップダウン・メニューから**グループ**のフィルター・オブジェクト・クラスを選択して、「再表示」をクリックします。

3. リスト・ボックスから**構造化オブジェクト・クラス**を 1 つ選択します。この例では、**GroupOfNames** を使用します。
4. 「次へ」をクリックします。
5. ドロップダウン・メニューから**グループ**のフィルター・オブジェクト・クラスを選択して、「再表示」をクリックします。
6. 「使用可能」ボックスから、使用する**補助オブジェクト・クラス**を選択します。この例では **ibm-staticGroup** を選択して、「追加」をクリックします。追加する補助オブジェクト・クラスごとにこのプロセスを繰り返します。補助オブジェクト・クラスを選択して、「除去」をクリックすることで、「選択済み」ボックスから補助オブジェクト・クラスを削除することもできます。
7. 「次へ」をクリックします。
8. 追加する項目の**相対識別名 (RDN)** を「**相対 DN**」フィールドに入力します (cn=Monday など)。
9. 選択したツリー項目の**識別名**を「**親 DN**」フィールドに入力します (ou=Groups,o=sample など)。「参照」をクリックして、リストから親 DN を選択することもできます。選択を展開して、サブツリーの下位にある他の選択項目を表示することもできます。選択項目を指定して「**選択**」をクリックし、必要な親 DN を指定します。デフォルトでは、「**親 DN**」には、ツリー内で選択されている項目が設定されます。**注: このタスクを「項目の管理」パネルから開始した場合、このフィールドは事前に入力されています。「親 DN」を選択してから、「追加」をクリックして項目の追加プロセスを開始します。**
10. 「**必須属性**」タブで、必須属性の値を入力します。この例では、**cn** フィールドに「**Monday**」と入力します。

注:

- a. 特定の属性に複数の値を追加する場合は、「**複数值**」をクリックします。次に属性の追加値を指定して、「**追加**」をクリックします。追加する各値に対してこれを繰り返します。値を除去する場合は、値を選択して「**除去**」をクリックします。複数の値を追加したら、「**OK**」をクリックします。これらの値は、属性の下に表示されるドロップダウン・メニューに追加されます。
 - b. サーバーで言語タグが使用可能な場合は、「**言語タグ値**」をクリックして言語タグ記述子の追加または除去を行うことができます。詳細については、530 ページの『言語タグ』を参照してください。
11. 「**メンバー**」フィールドに、少なくとも 1 つのメンバーの DN を追加します。例えば、cn=Bob Garcia,ou=austin,o=sample です。**注:** このメンバーは、既存の項目である必要はありません。メンバーは後で作成できます。
 - a. 「**複数值**」をクリックします。
 - b. 「**member**」フィールドに「cn=Ricardo Garcia,ou=austin,o=sample」と入力します。
 - c. 「**追加**」をクリックします。
 - d. 「**OK**」をクリックします。
 12. 「**オプションの属性**」をクリックします。

13. 「オプションの属性」タブで、他の属性の値を必要に応じて入力します。この例では、「説明」フィールドに、「月曜ランチ・グループ」と入力します。バイナリー値の追加の詳細については、528 ページの『属性のバイナリー・データ』を参照してください。
14. 「完了」をクリックすると、項目が作成されます。

タスクの結果

このグループに追加メンバーを追加する場合は、583 ページの『グループ項目のメンバーの管理』を参照してください。

動的グループ項目の作成

Web 管理ツールを使用して、動的グループ項目を作成できます。動的グループの利点は、ユーザー項目の追加など、サブツリー項目に変更を行うと、グループでも同様の変更が動的に行われる点です。

このタスクについて

このタスクでは、組織 `ou=Widget Division,ou=Austin,o=sample` の動的グループを作成します。

手順

1. ナビゲーション領域で「ディレクトリー管理」カテゴリを展開します。
2. 「項目の追加」をクリックします。
3. これが選択済みでなければ、メニューからフィルター・オブジェクト・クラス「すべて」を選択します。
4. 「再表示」をクリックします。
5. リスト・ボックスから**構造化オブジェクト・クラス**を 1 つ選択します。この例では、**container** を使用します。
6. 「次へ」をクリックします。
7. ドロップダウン・メニューから**グループ**のフィルター・オブジェクト・クラスを選択して、「再表示」をクリックします。
8. 「使用可能」ボックスから、使用する**補助オブジェクト・クラス**を選択します。この例では **ibm-dynamicGroup** を選択して、「追加」をクリックします。追加する補助オブジェクト・クラスごとにこのプロセスを繰り返します。補助オブジェクト・クラスを選択して、「除去」をクリックすることで、「選択済み」ボックスから補助オブジェクト・クラスを削除することもできます。
9. 「次へ」をクリックする。
10. 「**相対 DN**」フィールドに、追加する項目の相対識別名 (RDN) を入力します。例えば、`cn=Tuesday` などです。
11. 「**親 DN**」フィールドに、選択したツリー項目の識別名を入力します。例えば、`ou=Groups,o=sample` です。「参照」をクリックして、リストから親 DN を選択することもできます。選択を展開して、サブツリーの下位にある他の選択項目を表示することもできます。選択項目を指定して「**選択**」をクリックし、必要な親 DN を指定します。デフォルトでは、「**親 DN**」には、ツリー内で選択されている項目が設定されます。

注: このタスクを「項目の管理」パネルから開始した場合、このフィールドは事前に入力されています。「親 DN」を選択してから、「追加」をクリックして項目の追加プロセスを開始します。

12. 「必須属性」タブで、必要な属性の値を入力します。この例では、「cn」フィールドに Tuesday と入力します。

注:

- a. 特定の属性に複数の値を追加する場合は、「複数值」をクリックします。次に属性の追加値を指定して、「追加」をクリックします。追加する各値に対してこのステップを繰り返します。値を除去する場合は、値を選択して「除去」をクリックします。複数值の追加が完了したら、「OK」をクリックします。これらの値は、属性の下に表示されるドロップダウン・メニューに追加されます。
 - b. サーバーで言語タグが使用可能になっている場合は、「言語タグ値」をクリックすると、言語タグ記述子を追加または除去できます。詳細については、530 ページの『言語タグ』を参照してください。
13. 「オプションの属性」をクリックします。
 14. 「オプションの属性」タブで、他の属性の値を必要に応じて入力します。この例では、memberURL に ldap:///ou=Widget Division,ou=Austin,o=sample??sub? を入力します。
 15. 「完了」をクリックすると、項目が作成されます。

ネストされたグループ項目の作成

Web 管理ツールを使用して、動的グループ項目を作成できます。ネストされたグループは、親グループ項目内の属性によって参照される識別名 (DN) を持つ子グループ項目です。

このタスクについて

このタスクでは、他の 2 つのグループのコンテナーとなるネストされたグループを作成します。

手順

1. ナビゲーション領域で「ディレクトリー管理」カテゴリを展開します。
2. 「項目の追加」をクリックします。
3. これが選択済みでなければ、メニューからフィルター・オブジェクト・クラス「すべて」を選択します。
4. 「再表示」をクリックします。
5. リスト・ボックスから**構造化オブジェクト・クラス**を 1 つ選択します。この例では、**container** を使用します。
6. 「次へ」をクリックします。
7. ドロップダウン・メニューから**グループ**のフィルター・オブジェクト・クラスを選択して、「再表示」をクリックします。
8. 「使用可能」ボックスから、使用する**補助オブジェクト・クラス**を選択します。この例では **ibm-nestedGroup** を選択して、「追加」をクリックします。追加する補助オブジェクト・クラスごとにこのプロセスを繰り返します。補助オ

プロジェクト・クラスを選択して、「除去」をクリックすることで、「選択済み」ボックスから補助オブジェクト・クラスを削除することもできます。

9. 「次へ」をクリックする。
10. 「**相対 DN**」フィールドに、追加する項目の相対識別名 (RDN) を入力します。例えば、cn=Lunch bunch. です。
11. 「**親 DN**」フィールドに、選択したツリー項目の識別名を入力します。例えば、ou=Groups,o=sample です。「参照」をクリックして、リストから親 DN を選択することもできます。選択を展開して、サブツリーの下位にある他の選択項目を表示することもできます。選択項目を指定して「**選択**」をクリックし、必要な親 DN を指定します。デフォルトでは、「**親 DN**」には、ツリー内で選択されている項目が設定されます。

注: このタスクを「**項目の管理**」パネルから開始した場合、このフィールドは事前に入力されています。「**親 DN**」を選択してから、「**追加**」をクリックして項目の追加プロセスを開始します。

12. 「**必須属性**」タブで、必要な属性の値を入力します。この例では、「**cn**」フィールドに、Lunch bunch と入力します。

注:

- a. 特定の属性に複数の値を追加する場合は、「**複数値**」をクリックします。次に属性の追加値を指定して、「**追加**」をクリックします。追加する各値に対してこのステップを繰り返します。値を除去する場合は、値を選択して「**除去**」をクリックします。複数値の追加が完了したら、「**OK**」をクリックします。これらの値は、属性の下に表示されるドロップダウン・メニューに追加されます。
 - b. サーバーで言語タグが使用可能になっている場合は、「**言語タグ値**」をクリックすると、言語タグ記述子を追加または除去できます。詳細については、530 ページの『言語タグ』を参照してください。
13. 「**オプションの属性**」をクリックします。
 14. 「**オプションの属性**」タブで、他の属性の値を必要に応じて入力します。この例では、ibm-memberGroup に cn=Monday,ou=Groups,o=sample を入力します。
 - a. 「**複数値**」をクリックします。
 - b. 「**member**」フィールドに「cn=Tuesday,ou=Groups,o=sample」と入力します。
 - c. 「**追加**」をクリックします。
 - d. 「**OK**」をクリックします。
 15. 「**完了**」をクリックすると、項目が作成されます。

グループ・タスクの確認

以下の情報を使用して、前のタスクでグループを正しく作成したかどうかを検証します。

手順

1. ナビゲーション領域の「**ディレクトリー管理**」カテゴリがまだ展開されていない場合は展開します。

2. 「**項目の管理**」をクリックします。
3. `o=sample` を選択し、「**展開**」をクリックします。

注: 展開可能な項目は、その項目に子項目があることを示します。展開可能な項目の場合は、「**展開**」列の項目の隣にプラス記号「+」が付いています。項目の隣にある「+」記号をクリックすると、選択した項目の子項目を表示できます。

4. `ou=Groups` を選択し、「**展開**」をクリックします。
5. `cn=Lunch bunch` を選択します。
6. 「**アクションの選択**」メニューを展開して、「**メンバーの管理**」を選択し、「**実行**」をクリックします。

注: 「**ネストされたグループ**」タブには、`cn=monday,ou=group,o=sample` および `cn=tuesday,ou=group,o=sample` がリスト表示されます。

7. 「**有効なグループ・メンバー**」タブをクリックします。
8. グループごとの返すメンバーの最大数を指定します。「**返すメンバーの最大数**」をクリックした場合は、数字を入力してください。それ以外の場合は、「**無制限**」をクリックします。
9. テーブルにグループのメンバーを取り込むには、「**ロード**」をクリックするか、「**アクションの選択**」から「**ロード**」を選択して「**実行**」をクリックします。

グループ項目のメンバーの管理

以下の説明を参照して、メンバーをグループ項目に追加したり、グループ項目から除去したりすることができます。

グループ項目へのメンバーの追加

グループ項目にメンバーを追加する必要があります。グループ・メンバーには、さまざまな役割が割り当てられます。これらの役割は、グループ・メンバーにその実行が許可されているタスクを定義するものです。

手順

1. ナビゲーション領域から「**ディレクトリー管理**」トピックを展開します。
2. 「**項目の管理**」をクリックします。
3. 個々のサブツリーを展開して、作業するグループ項目を選択します。例えば、静的グループ項目の作成タスクで作成した `group`
`cn=Monday,ou=groups,o=sample` を選択します。
4. 「**アクションの選択**」ドロップダウン・メニューから、「**メンバーの管理**」を選択し、「**実行**」をクリックします。
5. グループごとの返すメンバーの最大数を指定します。「**返すメンバーの最大数**」をクリックした場合は、数字を入力してください。それ以外の場合は、「**無制限**」をクリックします。
6. 「**ロード**」をクリックして、既存のグループのメンバーを表示します。この例では、テーブルに `cn=Bob Garcia,ou=austin,o=sample` および `cn=Ricardo Garcia,ou=austin,o=sample` が表示されます。

注:

- a. 大きなグループの「ロード」をクリックしなくても、新規メンバーを追加できます。
 - b. 新規メンバーを追加する際に、追加する新規メンバーの 1 つが存在している場合は、「ロード」をクリックしても、その重複する新規メンバーは無視されます。
7. グループのメンバーとして追加する項目の名前を入力します。例えば、メンバー・フィールドに `cn=Kyle Nguyen,ou=austin,o=sample` と入力するか、「参照」機能を使用してこれを選択します (`o=sample` を展開 > `ou=Austin` を展開 > `cn=Kyle Nguyen,ou=austin,o=sample` を選択)。
 8. 「追加」をクリックします。
 9. テーブルには `cn=Kyle Nguyen,ou=austin,o=sample` が表示されます。変更を保存してメンバーの追加を続行する場合は「適用」をクリックします。変更を保存して「項目の管理」パネルに戻る場合は「OK」をクリックします。`cn=Bob Garcia,ou=austin,o=sample`、`cn=Ricardo Garcia,ou=austin,o=sample`、および `cn=Kyle Nguyen,ou=austin,o=sample` が新たに月曜グループのメンバーになります。
 10. 「有効グループ・メンバー」タブをクリックして「再表示」をクリックすると、`cn=Bob Garcia,ou=austin,o=sample`、`cn=Ricardo Garcia,ou=austin,o=sample`、および `cn=Kyle Nguyen,ou=austin,o=sample` がメンバーとして新たに表示されます。

グループのメンバー項目の編集

以下の説明を参照して、グループのメンバー項目を編集します。

手順

1. ナビゲーション領域から「ディレクトリー管理」を展開します。
2. 「項目の管理」をクリックします。
3. 個々のサブツリーを展開して、作業するグループ項目を選択します。
4. 「アクションの選択」メニューから、「メンバーの管理」を選択し、「実行」をクリックします。
5. 編集する項目の適切なグループのタブを選択します。このアクションでは、「静的グループ・メンバー」をクリックします。
6. テーブルにグループのメンバーを取り込むため、「ロード」をクリックします。「アクションの選択」メニューから「ロード」を選択して、「実行」をクリックすることもできます。
7. 既存のメンバーの項目の詳細を編集するには、`member` テーブルまたは `uniqueMember` テーブルから編集するメンバー項目を選択し、以下のいずれかのアクションを実行します。
 - 「編集」をクリックします。
 - 「アクションの選択」メニューから「編集」を選択し、「実行」をクリックします。

注: このアクションにより、選択したメンバー項目の「属性の編集」パネルが表示されます。このパネルで、該当するフィールドを変更できます。

グループ項目からのメンバーの除去

以下の情報により、グループ項目からメンバーを除去することができます。

手順

1. ナビゲーション領域から「**ディレクトリー管理**」トピックを展開します。
2. 「**項目の管理**」をクリックします。
3. 個々のサブツリーを展開して、作業するグループ項目を選択します。この例では、グループ項目の作成タスクで作成した、グループ `cn=lunch bunch,ou=groups,o=sample` を選択します。
4. 「**アクションの選択**」メニューから、「**メンバーの管理**」を選択し、「**実行**」をクリックします。
5. 除去する項目の適切なグループのタブを選択します。この例では、「**静的グループ・メンバー**」をクリックします。
6. グループごとの返すメンバーの最大数を指定します。「**返すメンバーの最大数**」をクリックした場合は、数字を入力してください。それ以外の場合は、「**無制限**」をクリックします。
7. テーブルにグループのメンバーを取り込むには、「**ロード**」をクリックするか、「**アクションの選択**」から「**ロード**」を選択して「**実行**」をクリックします。
8. 除去する項目を選択して、「**除去**」をクリックします。グループ項目からすべてのメンバーを除去する場合は、「**すべて除去**」をクリックします。
9. 除去の確認を求められます。「**OK**」をクリックして、メンバーを除去します。
10. 変更を保存して他のメンバーの除去を続行する場合は「**適用**」をクリックします。変更を保存して「**項目の管理**」パネルに戻る場合は「**OK**」をクリックします。

注: メンバーのフィールドにメンバー DN を入力して「**削除**」をクリックすれば、静的メンバー項目を削除することもできます。「**削除**」ボタンは、メンバーが「`member`」テーブルにロードされていない場合にのみ表示されます。

項目のメンバーシップの管理

以下の説明を参照して、項目に静的メンバーを追加したり、項目から静的メンバーを除去したりすることができます。

グループ・メンバーシップの追加

グループ・メンバーシップを追加して、アクセスを制御したり、メーリング・リストなどのアプリケーション固有の用途で使用したりすることができます。

手順

1. ナビゲーション領域から「**ディレクトリー管理**」を展開します。
2. 「**項目の管理**」をクリックします。
3. 個々のサブツリーを展開し、`cn=Bob Garcia,ou=austin,o=sample` などの項目を選択します。
4. 「**アクションの選択**」ドロップダウン・メニューから、「**メンバーシップの管理**」を選択し、「**実行**」をクリックします。

5. 「有効メンバーシップ」タブで、「ロード」をクリックして Bob Garcia のグループ・メンバーシップを表示します。

注: 選択したグループ項目が静的グループか動的グループのメンバーでない場合、有効なグループ・メンバーシップは表示できません。またグループ項目がネストされたグループだけのメンバーの場合も、メンバーシップは表示されません。

6. 「静的メンバーシップ」タブを選択します。
7. 「すべてのサフィックス」を選択します。表示するグループを制限する場合は、対応するサフィックスを選択します。この例では、**cn=ibmpolicies** を選択します。
8. 「グループのブラウズ」をクリックして、サフィックスの静的グループをすべて表示します。
9. 「**globalGroupName=GlobalAdminGroup,cn=ibmpolicies**」を選択します。
10. 「選択」をクリックします。

注: 「グループ DN」 フィールドに

globalGroupName=GlobalAdminGroup,cn=ibmpolicies と入力することもできます。また、「参照」をクリックしてディレクトリーからこれを選択し、「追加」をクリックすることも可能です。

11. 「ロード」をクリックして項目のメンバーシップを表示していない場合、または項目のメンバーシップが存在しない場合、次のメッセージが表示されます。「サーバーから項目をロードしていません。表には変更内容のみが表示されます。続行しますか?」 「OK」をクリックします。
12. 表には **globalGroupName=GlobalAdminGroup,cn=ibmpolicies** が表示されます。変更を保存してメンバーの追加を続行する場合は「適用」をクリックします。変更を保存して「項目の管理」パネルに戻る場合は「OK」をクリックします。**cn=Bob Garcia,ou=austin,o=sample** が新たにグローバル管理グループのメンバーになります。
13. 「有効グループ・メンバー」タブをクリックして「再表示」をクリックすると、項目 **cn=Bob Garcia,ou=austin,o=sample** のグループ・メンバーシップとして **globalGroupName=GlobalAdminGroup,cn=ibmpolicies** が新たに表示されます。

項目からのグループ・メンバーシップの除去

以下の情報により、項目からグループ・メンバーシップを除去できます。

手順

1. ナビゲーション領域から「ディレクトリー管理」トピックを展開します。
2. 「項目の管理」をクリックします。
3. 個々のサブツリーを展開し、**cn=Bob Garcia,ou=austin,o=sample** などの項目を選択します。
4. 「アクションの選択」メニューから、「メンバーシップの管理」を選択し、「実行」をクリックします。
5. 「静的メンバーシップ」タブで、「ロード」をクリックして Bob Garcia のグループ・メンバーシップを表示します。

6. 除去するグループ・メンバーシップを選択して、「**除去**」をクリックします。ユーザー項目からすべてのメンバーシップを除去する場合は、「**すべて除去**」をクリックします。
7. 除去を確認するプロンプトが出されたら、「**OK**」をクリックしてメンバーを除去します。
8. 変更を保存して他のメンバーの除去を続行する場合は「**適用**」をクリックします。変更を保存して「項目の管理」パネルに戻る場合は「**OK**」をクリックします。

動的グループの memberURL の編集

以下の説明を参照して、動的グループの memberURL を編集します。

手順

1. ナビゲーション領域から「**ディレクトリー管理**」トピックを展開します。
2. 「**項目の管理**」をクリックします。
3. 個々のサブツリーを展開して、作業するグループ項目を選択します。例えば、「**グループ項目の作成**」タスクで作成したグループ `cn=lunch bunch,ou=groups,o=sample` を選択します。

注: 選択するグループ項目は、動的グループである必要があります。

4. 「**アクションの選択**」メニューから、「**メンバーの管理**」を選択し、「**実行**」をクリックします。
5. 「動的グループ・フィルター」タブで、「**編集**」をクリックします。
6. 「**基本 DN**」を編集します。基本 DN は、検索の実行対象の DN です。必要な DN を検索するには、「**参照**」をクリックします。「**項目の参照**」パネルが表示されます。テーブルから必要な項目を選択して、「**選択**」をクリックします。
7. memberURL のスコープを選択します。オプションには、以下の項目があります。

オブジェクト

選択した (基本) 項目のみが検索範囲となります。

単一レベル

選択した (基本) 項目の直接の子項目のみが検索範囲となります。

注: この検索には、基本項目は含まれません。

サブツリー

基本項目を含め、選択した項目のすべての子孫を検索します。

8. 検索フィルター・ストリングを入力します。「**編集**」をクリックすると、検索フィルター・ストリングの作成に役立つパネルを開始できます。この新規パネルには以下のオプションがあります。
 - 簡易
 - 拡張
 - 手動

詳細については、542 ページの『検索フィルター』を参照してください。

役割

役割ベースの許可は、グループ・ベースの許可を補完する概念であり、いくつかの場面で役に立ちます。

役割のメンバーであるユーザーには、ジョブを完了するために役割で必要とされる作業を実行する権限があります。グループとは異なり、役割では、一連の暗黙的な許可が提供されます。グループのメンバーになることによって、得られる (または失われる) 許可についての前提条件はありません。

役割とグループは、ディレクトリー内でオブジェクトにより表現されるという点では同じです。役割には、さらに DN のグループも含まれています。アクセス制御で使用する役割は、オブジェクト・クラス `AccessRole` を持っている必要があります。Accessrole オブジェクト・クラスは、`GroupOfNames` オブジェクト・クラスのサブクラスです。

例えば、「sys admin」などの DN のコレクションがある場合、まず、それらの DN は「sys admin group」であると考えられます (グループとユーザーは、最もなじみのある特権属性タイプであるため)。しかしながら、「sys admin」のメンバーとして受け取ることを想定している一連の許可があるため、DN のコレクションは、「sys admin role」として、より正確に定義することができます。

検索制限グループ

IBM Security Directory Server では、ユーザーの検索要求によってリソースが過剰に消費されてサーバーのパフォーマンスが低下するのを防ぐために、サーバーに対するこれらの要求に検索制限を加えます。

管理者は、サーバーを構成する際に、検索のサイズや所要時間に対し、これらの検索制限を設定します。詳細については、122 ページの『検索設定』を参照してください。

これらの検索制限から除外されるのは、管理者、ローカル管理グループのメンバー、およびグローバル管理グループのメンバーのみで、その他のすべてのユーザーにはこれらの検索制限が適用されます。ただし、必要に応じて一般ユーザーより検索制限が柔軟な検索制限グループを作成できます。検索制限グループに含まれる個々のメンバーまたはグループには、検索制限グループで指定された検索制限が与えられます。

ユーザーが検索を開始すると、最初に検索要求の制限が検査されます。ユーザーが検索制限グループのメンバーである場合は、制限が比較されます。検索制限グループの制限値が検索要求の制限値より大きい場合は、検索要求の制限値が使用されます。検索要求の制限値が検索制限グループの制限値より大きい場合は、検索制限グループの制限値が使用されます。検索制限グループの項目が見つからなかった場合は、同じ比較がサーバー検索の制限値に対して実行されます。サーバーの検索制限が設定されていない場合は、デフォルトのサーバー設定値との比較が行われます。こうした比較で、常に最も低い設定値が、制限値として使用されます。

ユーザーが複数の検索制限グループに属している場合、このユーザーにはその中で最高レベルの検索機能が付与されます。例えば、ユーザーが検索グループ 1 と検索グループ 2 に属しているとします。検索グループ 1 では検索サイズ 2000 項目お

よび検索時間 4000 秒という検索制限が付与され、検索グループ 2 では検索サイズが無制限で検索時間が 3000 秒という検索制限が付与されます。この場合、このユーザーの検索制限は、検索サイズが無制限で検索時間が 4000 秒になります。

検索制限グループは、localhost と IBMpolicies のどちらに格納してもかまいません。IBMpolicies に格納される検索制限グループは複製されますが、localhost に格納されるグループは複製されません。同一の検索制限グループを localhost と IBMpolicies の両方に格納できます。これらの DN のいずれかの下に検索制限グループを格納しない場合、サーバーは、グループの検索制限パートを無視し、それを通常のグループとして扱います。

ユーザーが検索を開始すると、localhost に属する検索制限グループの項目が最初に検査されます。ユーザーの検索項目が検出されなかった場合は、IBMpolicies に属する検索制限グループの項目が検索されます。検索項目が localhost で検出された場合は、IBMpolicies に属する検索制限グループの項目は検査されません。localhost に属する検索制限グループの項目は、IBMpolicies に属するグループよりも優先されます。

検索制限グループの作成

この機能を使用すると、検索制限グループを作成できます。

検索制限グループを作成するには、Web 管理ツールまたはコマンド行を使用して、グループ項目を作成する必要があります。

Web 管理の使用

Web 管理ツールを使用して、以下の手順を実行すると、検索制限グループを作成できます。

このタスクについて

これを行うには、ナビゲーション領域で「ディレクトリー管理」カテゴリを展開します。

1. 「項目の追加」または「項目の管理」をクリックし、場所 `cn=ibmPolicies` または `cn=localhost` を選択して、「追加」をクリックします。
2. 「構造化オブジェクト・クラス」メニューからグループ・オブジェクト・クラスを 1 つ選択します。
 - accessGroup
 - accessRole
 - AIXaccessGroup
 - eNTGroup
 - groupofNames
 - groupofUniqueNames
 - groupofURLs
 - ibm-nestedGroup
 - ibm-proxyGroup
 - ibm-staticGroup

- `ibm-dynamicGroup`
3. 「次へ」をクリックします。
 4. 使用する `ibm-searchLimits` 補助オブジェクト・クラスを「使用可能」メニューから選択し、「追加」をクリックします。追加する補助オブジェクト・クラスごとにこの処理を繰り返します。「選択済み」メニューから補助オブジェクト・クラスを削除することもできます。削除対象を選択して「除去」をクリックします。
 5. 「次へ」をクリックする。
 6. 追加するグループの相対識別名 (RDN) を「相対 DN」フィールドに入力します (`cn=Search Group1` など)。
 7. 選択したツリー項目の識別名を「親 DN」フィールドに入力します (`cn=localhost` など)。「参照」をクリックして、リストから親 DN を選択することもできます。必要な「親 DN」を指定するには、選択項目を選択して、「選択」をクリックします。デフォルトでは、「親 DN」には、ツリー内で選択されている項目が設定されます。

注: このタスクを「項目の管理」パネルから開始した場合、このフィールドは事前に入力されます。「親 DN」を選択してから、「追加」をクリックして項目の追加プロセスを開始します。

8. 「必須属性」タブで、必要な値を入力します。必須属性は次のように定義されます。
 - `cn` は、指定した相対 DN です。
 - 「`ibm-searchSizeLimit`」フィールドで、検索のサイズを定義する項目数を指定します。この数の範囲は、0 から 2,147,483,647 までです。設定値 0 は、「無制限」と同じ意味を持ちます。
 - 「`ibm-searchTimeLimit`」フィールドで、検索の継続時間を定義する秒数を指定します。この数の範囲は、0 から 2,147,483,647 までです。設定値 0 は、「無制限」と同じ意味を持ちます。
 - 選択したオブジェクト・クラスに応じて、「Member」フィールドまたは「`uniqueMember`」フィールドが表示されます。これらは、作成するグループのメンバーです。項目は DN 形式となります。

例えば、`cn=Bob Garcia,ou=austin,o=sample` です。

注:

- a. 属性が複数值で、特定の属性に複数の値を追加する場合は、「複数值」をクリックします。528 ページの『属性の複数值の追加』を参照してください。
- b. 属性がバイナリー・データを必要とする場合は、「バイナリー・データ」をクリックします。528 ページの『属性のバイナリー・データ』を参照してください。
- c. サーバーで言語タグが使用可能な場合は、「言語タグ値」をクリックして言語タグ記述子を追加または除去します。詳細については、530 ページの『言語タグ』および 532 ページの『言語タグ値の追加』を参照してください。
- d. 属性に参照が含まれる場合は、「参照の管理」をクリックします。詳細については、301 ページの『参照』および 306 ページの『デフォルト参照の作成』を参照してください。

9. 「オプションの属性」タブをクリックして、該当する値を入力します。
10. 「完了」をクリックすると、項目が作成されます。

コマンド・ラインの使用

以下に示すコマンドを発行すると、`cn=localhost` というロケーションの `user1` と `user2` に 4000 秒、2000 項目の検索制限を設定できます。

このタスクについて

```
idsldapmodify -a -D <adminDN> -w <adminPW> -i <filename>
```

where *<filename>* contains:

```
Dn: cn=Search1, cn=localhost
Cn: Search1
member: cn=user1,o=sample
member: cn=user2,o=sample
ibm-searchTimeLimit: 4000
ibm-searchSizeLimit: 2000
objectclass: top
objectclass: ibm-searchLimits
objectclass: groupofNames
```

検索制限グループの変更

検索制限グループの変更には、Web 管理ツールとコマンド行のいずれも使用できません。

以下のアクションが実行可能です。

- 検索のサイズの変更
- 検索の時間制限の変更
- グループのメンバーの追加
- グループのメンバーの削除

Web 管理の使用

以下の情報により、検索制限グループの変更がサーバー管理で実行できます。

手順

1. 検索制限グループを変更します。 535 ページの『項目の変更』を参照してください。
2. オプション: 情報を表示して、検索制限グループが変更されていることを確認します。

コマンド・ラインの使用

`searchTimeLimit` の変更には、`idsldapmodify` コマンドが使用できます。

手順

1. `searchTimeLimit` を 3000 秒に変更し、`searchSizeLimit` を無制限に変更して、さらにメンバー (Bob Garcia) を追加するには、次のコマンドを入力します。

```
idsldapmodify -D adminDN -w adminPW -i filename
```

ここで、*filename* には、以下が含まれます。

```
dn: cn=Search1, cn=localhost
changetype: modify
replace: ibm-searchTimeLimit
ibm-searchTimeLimit: 3000
```

```
-
replace: ibm-searchSizeLimit
ibm-searchSizeLimit: 0
-
add: member
member: cn=Bob Garcia,ou=austin,o=sample
```

2. 情報を表示して、値が変更されていることを確認します。

検索制限グループの再作成

この機能を使用すると、検索制限グループをコピーできます。

同一の検索制限グループを `localhost` と `IBMpolicies` の両方に格納する場合は、検索制限グループのコピーが便利です。既存のグループと同様の情報を格納するが、若干の差がある新規のグループを作成する場合にも役立ちます。

サーバー管理の使用

サーバー管理の使用の詳細については、以下の説明とリンクを参照してください。

このタスクについて

検索制限グループをコピーするには、537 ページの『項目の再作成』を参照してください。

コマンド行の使用による検索制限グループのコピー

コマンド行を使用して、検索制限グループをコピーできます。同一の検索制限グループを `localhost` と `IBMpolicies` に適用する場合は、検索制限グループのコピーが便利です。

手順

1. `localhost` 内の検索グループを表示するには、以下のコマンドを実行します。

```
idsldapsearch -b cn=localhostobjectclass=ibm-searchLimits
```

2. コピーする検索制限グループを選択します。エディターを使用して該当する情報を変更し、`filename` に変更を保管します。以下のコマンドを実行します。

```
idsldapmodify -a -D adminDN -w adminPW -i
filename
```

ここで、`filename` には、以下の情報が含まれます。

```
Dn: cn=NewSearch1, cn=localhost
Cn: NewSearch1
member: cn=user1,o=sample
member: cn=user2,o=sample
ibm-searchTimeLimit: 4000
ibm-searchSizeLimit: 2000
objectclass: top
objectclass: ibm-searchLimits
objectclass: groupofNames
```

検索制限グループの除去

検索制限グループの除去には、Web 管理ツールとコマンド行のいずれも使用できません。

Web 管理の使用

以下の情報により、検索制限グループを除去できます。

手順

1. 検索制限グループを除去します。 534 ページの『項目の削除』を参照してください。
2. オプション: 情報を表示して、項目全体が削除されていることを確認します。

コマンド・ラインの使用

検索制限グループの除去には、**idsldapdelete** コマンドが使用できます。

手順

1. 次のコマンドを入力して、検索制限グループを除去します。

```
idsldapdelete -D adminDN -w adminPW -i filename
```

ここで、*filename* には、以下が含まれます。

```
#list additional DN's here, one per line  
cn=Search1, cn=localhost
```

2. 複数の検索制限グループを除去するには、DN を列挙します。各 DN は別々の行に記述する必要があります。

プロキシ許可グループ

プロキシ許可とは、ある特殊な形式の認証です。プロキシ許可という仕組みを利用すると、クライアント・アプリケーションは、それ独自の ID を持つディレクトリーとバインドできますが、別のユーザーの代わりに操作を実行して、ターゲット・ディレクトリーにアクセスできます。

複数のユーザーの代わりに、1 組の信頼できるアプリケーションまたはユーザーが IBM Security Directory Server にアクセスできます。

注: プロキシ許可は、プロキシ・サーバーとは異なります。

プロキシ許可グループのメンバーは、管理者、ローカル管理グループ・メンバー、またはグローバル管理グループ・メンバー以外の認証済み ID を持つことができます。またプロキシ許可グループのメンバーは、グループ許可制御を使用する権限も持ちます。

注: 管理者およびローカル管理グループのメンバーは、グローバル管理者グループのグループ許可制御を送信することで、グローバル管理グループ・メンバーの ID を前提とした権限を持ちます。

プロキシ許可グループは、localhost または IBMpolicies のいずれかに格納されません。

IBMpolicies の下のプロキシ許可グループは複製されます。localhost の下のプロキシ許可グループは複製されません。プロキシ許可グループは localhost と IBMpolicies の両方に格納できます。これらの DN のいずれかの下にプロキシ・グループを格納しない場合、サーバーは、グループのプロキシ・パートを無視し、それを通常のグループとして扱います。

例えば、クライアント・アプリケーションである client1 は、上位のアクセス許可を持つ IBM Security Directory Server にバインドできます。許可が制限されている

UserA が、このクライアント・アプリケーションに要求を送信します。クライアントがプロキシ許可グループのメンバーである場合は、client1 として IBM Security Directory Server に要求を渡すのではなく、より制限されたレベルの許可を使用して、UserA として要求を渡すことができます。つまりアプリケーション・サーバーは、client1 として要求を実行するのではなく、特定の情報にのみアクセスできるか、または UserA がアクセスしたり実行したりできるアクションのみを実行できるという意味です。アプリケーション・サーバーは、UserA の代わりに、つまり UserA のプロキシとして要求を実行します。

注: 属性メンバーは、その値を DN の形式で保持する必要があります。そうしないと、「DN 構文が無効です」というメッセージが戻されます。グループ DN をプロキシ許可グループのメンバーにすることは許可されていません。

管理者および管理グループのメンバーをプロキシ許可グループのメンバーにすることは許可されていません。すべての管理者には、そのグループのメンバーになっていなくても、プロキシ許可制御を使用する権限が付与されています。

監査ログには、バインド DN とプロキシ DN の両方が、プロキシ許可を使用して実行したアクションごとに記録されます。

プロキシ許可グループは Web 管理ツールによって管理できますが、プロキシ許可は、その他の Web 管理ツール機能には認識されていません。プロキシ許可機能を使用するには、プロキシ許可制御機能を LDAP 操作に組み込むか、または **-y** オプションを指定して LDAP コマンドを使用します。例:

```
idsldapsearch -D "cn=client1,ou=austin,o=sample" -w <client1password>
-y "cn=userA,o=sample" -b "o=sample" -s sub ou=austin
```

前述の idsldap 検索の指定に基づいて、client1 は、userA に読み取り許可が付与されているものはすべてターゲット・ディレクトリーから読み取ることができます。

プロキシ許可グループの作成

この機能を使用すると、プロキシ許可グループを作成できます。

プロキシ許可グループを作成するには、Web 管理ツールまたはコマンド行を使用してグループ項目を作成する必要があります。

Web 管理の使用

Web 管理ツールを使用して、以下の手順を実行すると、プロキシ許可グループを作成できます。

このタスクについて

ナビゲーション領域の「ディレクトリー管理」カテゴリがまだ展開されていない場合は、それを展開します。

手順

1. 以下のステップのいずれかを実行します。
 - 「項目の追加」をクリックします。
 - 「項目の管理」をクリックし、場所 (cn=ibmPolicies または cn=localhost) を選択して、「追加」をクリックします。

2. 「groupofNames」オブジェクト・クラスを「構造化オブジェクト・クラス」メニューから選択します。
 3. 「次へ」をクリックします。
 4. **ibm-proxyGroup** 補助オブジェクト・クラスを「使用可能」メニューから選択し、「追加」をクリックします。追加する補助オブジェクト・クラスごとにこの処理を繰り返します。「選択済み」メニューから補助オブジェクト・クラスを選択し、「除去」をクリックすれば、その補助オブジェクト・クラスを削除することもできます。
 5. 「次へ」をクリックします。
 6. 「相対 DN」フィールドで **cn=proxyGroup** を入力します。
 7. 選択したツリー項目の識別名を「親 DN」フィールドに入力します (cn=localhost など)。「参照」をクリックして、リストから親 DN を選択することもできます。必要な「親 DN」を指定するには、選択項目を選択して、「選択」をクリックします。デフォルトでは、「親 DN」には、ツリー内で選択されている項目が設定されます。**注:** このタスクを「項目の管理」パネルから開始した場合、このフィールドは事前に入力されています。「親 DN」を選択してから、「追加」をクリックして項目の追加プロセスを開始します。
 8. 「必須属性」タブで、必須属性の値を入力します。
 - a. 「cn」は proxyGroup です。
 - b. 「メンバー」は DN 形式となります (例: cn=Bob Garcia,ou=austin,o=sample)。
- 注:**
- 属性が複数值で、特定の属性に複数の値を追加する場合は、「複数值」をクリックします。cn 値に対して複数の値を作成しないでください。プロキシー許可グループには、既知の名前である proxyGroup を指定する必要があります。528 ページの『属性の複数值の追加』を参照してください。
 - 属性がバイナリー・データを必要とする場合は、「バイナリー・データ」をクリックします。528 ページの『属性のバイナリー・データ』を参照してください。
 - サーバーで言語タグが使用可能な場合は、「言語タグ値」をクリックして言語タグ記述子を追加または除去します。詳細については、530 ページの『言語タグ』および 532 ページの『言語タグ値の追加』を参照してください。
 - 属性に参照が含まれる場合は、「参照の管理」をクリックします。詳細については、301 ページの『参照』および 306 ページの『デフォルト参照の作成』を参照してください。
9. 「オプションの属性」をクリックします。
 10. 「オプションの属性」タブで、属性の値を必要に応じて入力します。
 11. 「完了」をクリックすると、項目が作成されます。

コマンド行の使用によるプロキシー許可グループの作成

コマンド行を使用して、プロキシー許可グループを作成できます。プロキシー許可という仕組みを利用すると、クライアント・アプリケーションは、独自の ID を持

つディレクトリーにバインドできます。その一方で、アプリケーションは、別のユーザーの代わりに操作を実行して、ターゲット・ディレクトリーにアクセスすることができます。

手順

1. `cn=localhost` が示す場所にある初期メンバーを使用してプロキシー許可グループを作成するには、以下のコマンドを実行します。

```
idsldapadd -D adminDN -w adminPW -i  
filename
```

ここで、`filename` には、以下の情報が含まれます。

```
dn: cn=proxyGroup,cn=localhost  
cn: proxyGroup  
member:cn=client1, ou=austin, o=sample  
objectclass: top  
objectclass: container  
objectclass: groupOfNames  
objectclass: ibm-proxyGroup
```

2. 別のメンバーを追加するには、以下のコマンドを実行します。

```
idsldapmodify -D adminDN -w adminPW -i  
filename
```

ここで、`filename` には、以下の情報が含まれます。

```
dn: cn=proxyGroup,cn=localhost  
cn: proxyGroup  
changetype: modify  
add: member  
member:cn=client2, ou=austin, o=sample
```

プロキシー許可機能を使用するには、LDAP 操作にプロキシー許可制御を組み込むか、LDAP コマンドに `-y` オプションを指定して使用します。例:

```
idsldapsearch -D "cn=client1,ou=austin,o=sample" -w <client1password>  
-y "cn=userA,o=sample" -b "o=sample" -s sub ou=austin
```

`client1` は、`idsldapsearch` の指定に基づいて、`userA` に読み取り許可があるものはすべてターゲット・ディレクトリーから読み取ることができます。

プロキシー許可グループの変更

プロキシー許可グループの変更は、サーバー管理とコマンド行を使用して実行できます。

サーバー管理の使用

以下の情報により、プロキシー許可グループの変更をサーバー管理で実行できます。

手順

1. グループのメンバーを追加または削除します。535 ページの『項目の変更』を参照してください。グループのメンバーの追加や削除は、プロキシー許可グループの変更に関するものです。
2. 情報を表示して、項目が変更されていることを確認します。

コマンド・ラインの使用

プロキシー許可グループの変更を、`idsldapmodify` コマンドを使用して実行します。

手順

1. `cn=IBMpolicies` にあるプロキシ許可グループを変更するには、次のコマンドを入力します。

注: このコマンドにより、`user1` が削除され、`user2` と `user3` が追加されます。

```
idsldapmodify -D adminDN -w adminPW -i filename
```

ここで、`filename` には、以下が含まれます。

```
dn: cn=proxyGroup,cn=IBMpolicies
changetype: modify
delete: member
member:cn=client1, ou=austin, o=sample
-
add: member
member: cn=client2, ou=austin, o=sample
-
add: member
member: cn=client3, ou=austin, o=sample
```

2. 情報を表示して、値が変更されていることを確認します。

プロキシ許可グループの再作成

この機能を使用すると、プロキシ許可グループをコピーできます。

Web 管理ツールの使用によるプロキシ許可グループのコピー

Web 管理ツールを使用して、プロキシ許可グループをコピーできます。同一のプロキシ許可グループを `localhost` と `IBMpolicies` の両方に格納する場合は、プロキシ許可グループのコピーが便利です。

このタスクについて

プロキシ許可グループをコピーするには、537 ページの『項目の再作成』を参照してください。

コマンド行の使用によるプロキシ許可グループのコピー

コマンド行を使用して、プロキシ許可グループをコピーできます。同一のプロキシ許可グループを `localhost` と `IBMpolicies` の両方に格納する場合は、プロキシ許可グループのコピーが便利です。

手順

1. `localhost` に含まれているプロキシ許可グループを表示するには、以下のコマンドを実行します。

```
idsldapsearch -D adminDN -w adminPW -b
cn=localhostobjectclass=ibm-proxyGroup
```

このコマンドを実行すると、以下の出力が生成されます。

```
Dn: cn=proxyGroup, cn=localhost
Cn: proxyGroup
objectclass: ibm-proxyGroup
objectclass: groupOfNames
member: cn=client1, ou=austin, o=sample
member: cn=client2, ou=austin, o=sample
member: cn=client3, ou=austin, o=sample
```

2. プロキシ許可グループを選択します。エディターを使用して `cn=localhost` を `cn=IBMpolicies` に変更し、`filename` という名前で保管します。
3. 次に、以下のコマンドを発行します。

```
idsldapmodify -a -D adminDN -w adminPW -i  
filename
```

ここで、*filename* には、以下の情報が含まれます。

```
Dn: cn=proxyGroup, cn=IBMpolicies  
Cn: proxyGroup  
objectclass: ibm-proxyGroup  
objectclass: groupOfNames  
member: cn=client1, ou=austin, o=sample  
member: cn=client2, ou=austin, o=sample  
member: cn=client3, ou=austin, o=sample
```

プロキシ許可グループの除去

プロキシ許可グループからメンバーを除去するには、以下のいずれかの方法を使用します。

Web 管理の使用

以下の情報により、プロキシ許可グループを除去することができます。

手順

1. プロキシ許可グループを除去します。 534 ページの『項目の削除』を参照してください。
2. オプション: 情報を表示して、項目全体が削除されていることを確認します。

コマンド・ラインの使用

プロキシ許可グループを除去するには、**idsldapdelete** コマンドが使用できます。

手順

1. 次のコマンドを入力して、プロキシ許可グループを除去します。

```
idsldapdelete -D adminDN -w adminPW -s "cn=ProxyGroup,cn=IBMpolicies"
```

2. オプション: コマンドを実行したら、情報を表示して、内容を確認します。

第 4 章 ユーザー関連のタスク

レルム、テンプレート、ユーザー、グループの詳細については、以下の情報を参照してください。

レルム、テンプレート、ユーザー、およびグループ

レルムは、ユーザーとグループが属する集合です。例えば、会社、ボウリング・チーム、クラブなどはすべてレルムになります。

レルムは、ユーザー命名コンテキスト内の任意の場所 (cn=localhost、cn=schema や cn=configuration の下ではなく) にオブジェクト・クラス `ibm-realm` の項目を作成することによって定義されます。 `ibm-realm` オブジェクトは、レルムの名前 (cn)、レルム管理者のグループ (`ibm-realmAdminGroup`)、レルム内のユーザーのオブジェクト・クラスと属性を指定するユーザー・テンプレート・オブジェクト (`ibm-realmUserTemplate`)、ユーザー項目とグループ項目が保管されるコンテナ項目の場所 (`ibm-realmUserContainer` と `ibm-realmGroupContainer`) を定義します。ディレクトリー管理者と管理グループのメンバーは、ユーザー・テンプレート、レルム、レルム管理者グループを管理する必要があります。レルムが作成されると、そのレルムの管理者グループのメンバー (レルム管理者) は、そのレルム内のユーザーとグループを管理する責任があります。

レルムの作成

Web 管理ツールを使用してレルムを作成するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「レルムとテンプレート」カテゴリを展開します。

手順

1. 「レルムの追加」をクリックします。
 - a. レルムの名前を入力します。例えば、**realm1** などです。
 - b. レルムの場所を識別する親 DN を入力します。この項目は、`o=sample` など、サフィックスの形式になります。また、「参照」をクリックして、使用するサブツリーの場所を選択することもできます。
2. 「次へ」をクリックして先に進みます。
3. 情報を確認します。この時点では、レルムは実際には作成されていないため、「ユーザー・テンプレート」および「ユーザー検索フィルター」は無視されません。
4. 「完了」をクリックしてレルムを作成します。

レルム管理者の作成

レルム管理者を作成するには、まずレルムの管理グループを作成する必要があります。

管理者は、レルム内の項目を管理するために作成されます。グループにメンバーを追加する方法については、583 ページの『グループ項目のメンバーの管理』を参照してください。

レルム管理グループの作成

Web 管理ツールを使用してレルムの管理グループを作成するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域の「ディレクトリー管理」カテゴリを展開します。

手順

1. 「項目の管理」をクリックします。
2. ツリーを展開して、作成したレルムの場所を識別する親の DN を探し出し、作成したレルム **cn=realm1,o=sample** を選択します。
3. 「アクションの選択」メニューを展開して、「ACL の編集」を選択し、「実行」をクリックします。
4. 「所有者」タブをクリックします。
5. 「所有者の伝搬」にチェック・マークが付いていることを確認します。
6. レルム **cn=realm1,o=sample** の対象 DN を入力します。
7. 対象タイプを**グループ**に変更します。
8. 「追加」をクリックします。
9. 「OK」をクリックして変更を保管し、「項目の管理」パネルに戻ります。

管理者項目の作成

Web 管理ツールを使用して管理者項目を作成するには、以下の手順を実行します。

このタスクについて

管理者のユーザー項目がまだない場合は、それを作成する必要があります。

Web 管理ツールのナビゲーション領域の「ディレクトリー管理」カテゴリを展開します。

1. 「項目の管理」をクリックします。
2. 管理者項目を常駐させたい場所のツリーを展開します。

注: 管理者項目はレルムの外側に配置すると、管理者は誤って自分自身を削除することがなくなります。この例では、場所は **o=sample** のように指定できます。

3. 「追加」をクリックします。
4. 構造化オブジェクト・クラス (**person** など) を選択します。
5. 「次へ」をクリックします。
6. 追加する補助オブジェクト・クラスを選択します。
7. 「次へ」をクリックします。

8. 項目の必須属性を入力します。以下に例を示します。

- 相対 DN cn=John Doe
- 親 DN o=sample (自動的に入力されます。)
- cn John Doe
- sn Doe

注:

- a. 属性が複数值で、特定の属性に複数の値を追加する場合は、「複数值」をクリックします。528 ページの『属性の複数值の追加』を参照してください。
 - b. 属性がバイナリー・データを必要とする場合は、「バイナリー・データ」をクリックします。528 ページの『属性のバイナリー・データ』を参照してください。
 - c. サーバーで言語タグが使用可能な場合は、「言語タグ値」をクリックして言語タグ記述子を追加または除去します。詳細については、530 ページの『言語タグ』および 532 ページの『言語タグ値の追加』を参照してください。
 - d. 属性に参照が含まれる場合は、「参照の管理」をクリックします。詳細については、301 ページの『参照』および 306 ページの『デフォルト参照の作成』を参照してください。
9. 「オプションの属性」タブで、ユーザー・パスワードを割り当て済みであることを確認します。
10. 完了したら、「完了」をクリックします。

管理グループへの管理者の追加

管理グループに管理者を追加するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域の「ディレクトリー管理」カテゴリを展開します。

手順

1. 「項目の管理」をクリックします。
2. ツリー (o=sample) を展開して、作成したレルム **cn=realm1,o=sample** を選択します。
3. 「アクションの選択」メニューを展開して、「メンバーの管理」を選択し、「実行」をクリックします。
4. 「静的グループ・メンバー」タブが強調表示されます。「ロード」をクリックして、グループのメンバーを表示します。この例では、メンバーをまだ追加していないため、テーブルに項目は表示されません。
5. グループのメンバーとして追加する項目の名前をメンバー・フィールドに入力します (この例では、前のタスクで作成した項目 **cn=John Doe,o=sample** を入力します)。または「ブラウズ」機能を使用してそれを選択します (この例では、o=sample を展開して **cn=John Doe,o=sample** を選択します)。
6. 「追加」をクリックします。

7. テーブルには **cn=John Doe,o=sample** が表示されます。変更を保管してメンバーの追加を続行する場合は「適用」をクリックします。終了する場合、「OK」をクリックして変更を保管して「項目の管理」パネルに戻ります。

テンプレートの作成

Web 管理ツールを使用してテンプレートを作成するには、以下の手順を実行します。

このタスクについて

レルムを作成した後、次のステップでは、ユーザー・テンプレートを作成します。テンプレートを使用すると、入力する情報を編成できます。Web 管理ツールのナビゲーション領域で「レルムとテンプレート」カテゴリを展開します。

手順

1. 「ユーザー・テンプレートの追加」をクリックします。
 - 既存のテンプレートがある場合は、テンプレートを選択して、その設定を作成中のテンプレートにコピーすることができます。ここでは最初のテンプレートを作成するので、この操作は行いません。
 - **template1** など、テンプレートの名前を入力します。
 - テンプレートを常駐させる場所を入力します。複製のために、このテンプレートを使用するレルムのサブツリー内にテンプレートを配置します。この例では、前の操作で作成したレルム **cn=realm1,o=sample** 用に、サブツリー **o=sample** 内にテンプレートを配置します。また、「参照」をクリックして、テンプレートの場所として別のサブツリーを選択することもできます。
2. 「次へ」をクリックします。「完了」をクリックすると、空のテンプレートが作成されます。後でテンプレートに情報を追加することができます。610 ページの『テンプレートの編集』を参照してください。
3. 「次へ」をクリックした場合は、**inetOrgPerson** など、テンプレートの構造化オブジェクト・クラスを選択します。必要に応じて補助オブジェクト・クラスを追加することもできます。
4. 「次へ」をクリックします。
5. 「命名属性」ドロップダウン・メニューから命名属性を選択します。この属性は、テンプレートを使用するレルムの各項目の RDN に使用されます。命名属性 (givenName など) には、このテンプレートを使用するレルムの各メンバーに固有な値が必要です。この値は、ユーザーおよびグループ・タスクに対するユーザー・リストのユーザー項目の表示名です。例えば、givenName が命名属性である場合に Bob Garcia を入力すると、項目は該当するユーザー・リストに Bob Garcia として表示されます。
6. テンプレートに「必須」タブが作成されました。このタブに含まれる情報を変更できます。
 - a. タブ・メニューの「必須」を選択して、「編集」をクリックします。「タブの編集」パネルが表示されます。タブ「必須」の名前と、オブジェクト・クラス **inetOrgPerson** で必要とされる選択された属性が表示されます。
 - *sn - 名字
 - *cn - 共通名

注: * は必須情報を示します。

- b. このタブに追加情報を追加する場合は、「属性」メニューから属性を選択します。例えば、**departmentNumber** を選択して、「追加」をクリックします。**employeeNumber** を選択して、「追加」をクリックします。**title** を選択して、「追加」をクリックします。「選択された属性」メニューには、以下のものが表示されます。
 - title
 - employeeNumber
 - departmentNumber
 - *sn
 - *cn
 - c. 選択した属性を強調表示して、「上へ移動」または「下へ移動」をクリックすることで、これらのフィールドがテンプレートにどのように表示されるかを再指定できます。これにより、属性の位置が 1 つずつ変更されます。属性が希望する順序で配列されるまで、この手順を繰り返します。例を以下に示します。
 - *sn
 - *cn
 - title
 - employeeNumber
 - departmentNumber
 - d. 選択された各属性を変更することもできます。
 - 1) 「選択された属性」ボックスの属性を強調表示して、「編集」をクリックします。
 - 2) テンプレートで使用されるフィールドの表示名を変更できます。例えば、**departmentNumber** を **Department number** として表示する場合は、「表示名」フィールドにそのように入力します。
 - 3) テンプレートの属性フィールドに事前に入力されるデフォルト値を指定することもできます。例えば、入力しようとするユーザーのほとんどが部門 789 のメンバーの場合、789 をデフォルト値として入力できます。テンプレートのフィールドに、事前に 789 が入力されます。実際のユーザー情報を追加するときに、値を変更できます。
 - 4) 「OK」をクリックします。
 - e. 「OK」をクリックします。
7. 追加情報用に別のタブ・カテゴリーを作成するには、「追加」をクリックします。
- 新しいタブの名前を入力します。例えば、「住所情報」などです。
 - このタブについて、「属性」メニューから属性を選択します。例えば、**homePostalAddress** を選択して、「追加」をクリックします。**postOfficeBox** を選択して、「追加」をクリックします。**telephoneNumber** を選択して、「追加」をクリックします。**homePhone** を選択して、「追加」をクリックします。**facsimileTelephoneNumber** を選択して、「追加」をクリックします。「選択された属性」メニューには、以下のものが表示されます。

- homePostalAddress
 - postOfficeBox
 - telephoneNumber
 - homePhone
 - facsimileTelephoneNumber
- 選択した属性を強調表示して、「上へ移動」または「下へ移動」をクリックすることで、これらのフィールドがテンプレートにどのように表示されるかを再指定できます。これにより、属性の位置が 1 つずつ変更されます。属性が希望する順序で配列されるまで、この手順を繰り返します。例を以下に示します。
 - homePostalAddress
 - postOfficeBox
 - telephoneNumber
 - facsimileTelephoneNumber
 - homePhone
 - 「OK」をクリックします。
8. 作成するタブの数だけこのプロセスを繰り返します。完了したら、「完了」をクリックすると、テンプレートが作成されます。

レルムへのテンプレートの追加

Web 管理ツールを使用してレルムにテンプレートを追加するには、以下の手順を実行します。

このタスクについて

レルムとテンプレートを作成した後に、レルムにテンプレートを追加する必要があります。Web 管理ツールのナビゲーション領域で「レルムとテンプレート」カテゴリを展開します。

手順

1. 「レルムの管理」をクリックします。
2. テンプレートを追加するレルム (この例では **cn=realm1,o=sample**) を選択して、「編集」をクリックします。
3. 「ユーザー・テンプレート」にスクロールして、ドロップダウン・メニューを展開します。
4. テンプレート (この例では **cn=template1,o=sample**) を選択します。
5. 「OK」をクリックします。
6. 「閉じる」をクリックします。

グループの作成

Web 管理ツールを使用してグループを作成するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」カテゴリを展開します。

1. 「グループの追加」をクリックします。
2. 作成するグループの名前を入力します。例えば、**group1** などです。
3. ユーザーを追加する対象となるレルムをドロップダウン・メニューから選択します。この場合は **realm1** です。
4. 「次へ」をクリックします。
5. 「完了」をクリックすると、グループが作成されます。レルムにすでにユーザーが存在する場合は、「次へ」をクリックして、ユーザーを **group1** に追加できます。「完了」をクリックします。

詳細については、570 ページの『グループ (Groups)』を参照してください。

レルムへのユーザーの追加

Web 管理ツールを使用してレルムにユーザーを追加するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」カテゴリを展開します。

手順

1. 「ユーザーの追加」をクリックします。
2. ユーザーを追加する対象となるレルムをドロップダウン・メニューから選択します。この場合は **realm1** です。
3. 「次へ」をクリックします。作成したテンプレート **template1** が表示されます。アスタリスク (*) で指示された必須フィールドと、タブのその他のフィールドに入力します。
4. レルム内にすでにグループが作成されている場合は、複数のグループにユーザーを追加することもできます。
 - a. 「ユーザー・グループ」タブを選択します。
 - b. 「追加」をクリックします。
 - c. グループの名前 (Group1) を「グループ名」フィールドに入力します。または「使用可能グループ」をクリックして、ユーザーを追加するグループをリストから 1 つ以上選択します。また、グループを選択して「表示」をクリックすると、そのグループの既存のメンバーを確認できます。グループのメンバーシップの詳細については、585 ページの『項目のメンバーシップの管理』を参照してください。
5. 完了したら、「完了」をクリックします。

レルムの管理

最初のレルムをセットアップしてデータを取り込んだら、他のレルムを追加したり、既存のレルムを変更したりすることができます。

ナビゲーション領域で「**レルムとテンプレート**」カテゴリを展開して、「**レルムの管理**」をクリックします。既存のレルムのリストが表示されます。このパネルで、レルムの追加、編集、削除を行うことができます。また、レルムのアクセス制御リスト (ACL) を編集することもできます。

レルムの追加

Web 管理ツールを使用してレルムを追加するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「**レルムとテンプレート**」カテゴリを展開します。

手順

1. 「**レルムの追加**」をクリックします。
 - レルムの名前を入力します。例えば、**realm2** などです。
 - 例えば **realm1** など、既存のレルムがある場合は、レルムを選択して、その設定を作成中のレルムにコピーすることができます。
 - レルムの場所を識別する親 DN を入力します。この項目は、**o=sample** など、サフィックスの形式になります。また、「**参照**」をクリックして、使用するサブツリーの場所を選択することもできます。
2. 続行する場合は「**次へ**」をクリックします。または「**完了**」をクリックします。
3. 「**次へ**」をクリックした場合は、情報を検討します。
4. ドロップダウン・メニューから「**ユーザー・テンプレート**」を選択します。既存のレルムから設定をコピーした場合、テンプレートのこのフィールドは事前に入力されています。
5. 「**ユーザー検索フィルター**」を入力します。
6. 「**完了**」をクリックしてレルムを作成します。

レルムの編集

Web 管理ツールを使用してレルムを編集するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「**レルムとテンプレート**」カテゴリを展開します。

- 「**レルムの管理**」をクリックします。
- 編集するレルムをレルムのリストから選択します。
- 「**編集**」をクリックします。
 - 「**ブラウズ**」ボタンを使用して、以下のものを変更できます。
 - 管理者グループ
 - グループ・コンテナ
 - ユーザー・コンテナ
 - ドロップダウン・メニューから別のテンプレートを選択できます。
 - 「**ユーザー検索フィルター**」を変更するには、「**編集**」をクリックします。

- 完了したら「OK」をクリックします。

レルムの除去

Web 管理ツールを使用してレルムを削除するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「レルムとテンプレート」カテゴリを展開します。

手順

1. 「レルムの管理」をクリックします。
2. 除去するレルムを選択します。
3. 「削除」をクリックします。
4. 削除を確認するプロンプトが出されたら、「OK」をクリックします。
5. レルムのリストからレルムが除去されます。

レルムの ACL の編集

レルム上で ACL を編集する場合は、以下の情報を参照してください。

このタスクについて

Web 管理ツール・ユーティリティーを使用して ACL プロパティを表示させたり ACL を処理したりするには、558 ページの『ACL の処理』を参照してください。

詳細については、546 ページの『アクセス制御リスト』を参照してください。

テンプレートの管理

最初のテンプレートを作成したら、他のテンプレートを追加したり、既存のテンプレートを変更したりすることができます。

ナビゲーション領域で「レルムとテンプレート」カテゴリを展開して、「ユーザー・テンプレートの管理」をクリックします。既存のテンプレートのリストが表示されます。このパネルで、テンプレートの追加、編集、削除を行うことができます。また、テンプレートのアクセス制御リスト (ACL) を編集することもできます。

ユーザー・テンプレートの追加

Web 管理ツールを使用してユーザー・テンプレートを追加するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「レルムとテンプレート」カテゴリを展開します。

手順

1. 「ユーザー・テンプレートの追加」をクリックするか、または「ユーザー・テンプレートの管理」をクリックして、「追加」をクリックします。

- a. 例えば **template1** など、既存のテンプレートがある場合は、テンプレートを
選択して、その設定を作成中のテンプレートにコピーすることができます。
 - b. 新しいテンプレートの名前を入力します。例えば、**template2** などです。
 - c. テンプレートの場所を識別する親 DN を入力します。この項目は、**o=sample**
など、DN の形式になります。また、「参照」をクリックして、使用するサ
ブツリーの場所を選択することもできます。
2. 「次へ」をクリックします。「完了」をクリックすると、空のテンプレートが
作成されます。後でテンプレートに情報を追加することができます。610 ページ
の『テンプレートの編集』を参照してください。
 3. 「次へ」をクリックした場合は、**inetOrgPerson** など、テンプレートの構造化オ
ブジェクト・クラスを選択します。必要に応じて補助オブジェクト・クラスを追
加することもできます。
 4. 「次へ」をクリックします。
 5. 「命名属性」ドロップダウン・メニューから、テンプレートを使用するレルム内
の各項目の RDN に使用する属性を選択します。この命名属性 (**employeeNumber**
など) には、このテンプレートを使用するレルム内の各メンバーに固有な値を指
定する必要があります。この命名属性の値は、ユーザー・タスクとグループ・タ
スクのユーザー・リストにおけるユーザー項目の表示名になります。例えば、
employeeNumber が命名属性であり **1234abc** を入力した場合、該当するユーザ
ー・リストには、項目が **1234abc** として表示されます。
 6. テンプレートに「必須」タブが作成されました。このタブに含まれる情報を変更
できます。
 - a. タブ・メニューの「必須」を選択して、「編集」をクリックします。タブ
「必須」の名前と、オブジェクト・クラス **inetOrgPerson** で必要とされる選
択された属性が表示されます。
 - *sn - 名字
 - *cn - 共通名
 注: 「*」が付いている項目は必須情報です。
 - b. このタブに追加情報を追加する場合は、「属性」メニューから属性を選択し
ます。例えば、**departmentNumber** を選択して、「追加」をクリックしま
す。**employeeNumber** を選択して、「追加」をクリックします。**title** を選択
して、「追加」をクリックします。「選択された属性」メニューには、以下
のものが表示されます。
 - title
 - employeeNumber
 - departmentNumber
 - *sn
 - *cn
 - c. 選択した属性を強調表示して、「上へ移動」または「下へ移動」をクリック
することで、これらのフィールドがテンプレートにどのように表示されるか
を再指定できます。これにより、属性の位置が 1 つずつ変更されます。属性
が希望する順序で配列されるまで、この手順を繰り返します。以下に例を示
します。
 - *sn

- *cn
 - title
 - employeeNumber
 - departmentNumber
- d. 選択された各属性を変更することもできます。
- 1) 「**選択された属性**」ボックスの属性を強調表示して、「**編集**」をクリックします。
 - 2) テンプレートで使用されるフィールドの表示名を変更できます。例えば、**departmentNumber** を **Department number** として表示する場合は、「**表示名**」フィールドにそのように入力します。
 - 3) テンプレートの属性フィールドに事前に入力されるデフォルト値を指定することもできます。例えば、入力しようとするユーザーのほとんどが部門 789 のメンバーの場合、789 をデフォルト値として入力できます。テンプレートのフィールドに、事前に 789 が入力されます。実際のユーザー情報を追加するときに、値を変更できます。
 - 4) 「**OK**」をクリックします。
- e. 「**OK**」をクリックします。
7. 追加用に別のタブ・カテゴリを作成するには、「**追加**」をクリックします。
- a. 新しいタブの名前を入力します。例えば、「住所情報」などです。
 - b. このタブについて、「**属性**」メニューから属性を選択します。例えば、**homePostalAddress** を選択して、「**追加**」をクリックします。**postOfficeBox** を選択して、「**追加**」をクリックします。**telephoneNumber** を選択して、「**追加**」をクリックします。**homePhone** を選択して、「**追加**」をクリックします。**facsimileTelephoneNumber** を選択して、「**追加**」をクリックします。「**選択された属性**」メニューには、以下のものが表示されます。
 - homePostalAddress
 - postOfficeBox
 - telephoneNumber
 - homePhone
 - facsimileTelephoneNumber
 - c. 選択した属性を強調表示して、「**上へ移動**」または「**下へ移動**」をクリックすることで、これらのフィールドがテンプレートにどのように表示されるかを再指定できます。これにより、属性の位置が 1 つずつ変更されます。属性が希望する順序で配列されるまで、この手順を繰り返します。以下に例を示します。
 - homePostalAddress
 - postOfficeBox
 - telephoneNumber
 - facsimileTelephoneNumber
 - homePhone
 - d. 「**OK**」をクリックします。
8. 作成するタブの数だけこのプロセスを繰り返します。完了したら、「**完了**」をクリックすると、テンプレートが作成されます。

テンプレートの編集

Web 管理ツールを使用してテンプレートを編集するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「レルムとテンプレート」カテゴリを展開します。

- 「**ユーザー・テンプレートの管理**」をクリックします。
- 編集するテンプレートをテンプレートのリストから選択します。
- 「**編集**」をクリックします。
- 例えば `template1` など、既存のテンプレートがある場合は、テンプレートを選択して、その設定を編集中のテンプレートにコピーすることができます。
- 「**次へ**」をクリックします。
 - ドロップダウン・メニューを使用して、テンプレートの構造化オブジェクト・クラスを変更できます。
 - 補助オブジェクト・クラスを追加または除去できます。
- 「**次へ**」をクリックします。
- テンプレートに含まれるタブと属性を変更できます。タブの変更の詳細については、[ステップ 6 \(608 ページ\)](#) を参照してください。
- 完了したら、「**完了**」をクリックします。

テンプレートの除去

Web 管理ツールを使用してテンプレートを削除するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「レルムとテンプレート」カテゴリを展開します。

手順

1. 「**ユーザー・テンプレートの管理**」をクリックします。
2. 除去するテンプレートを選択します。
3. 「**削除**」をクリックします。
4. 削除を確認するプロンプトが出されたら、「**OK**」をクリックします。
5. テンプレートのリストからテンプレートが除去されます。

テンプレートの ACL の編集

Web 管理ツールを使用してテンプレート上の ACL を編集するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「レルムとテンプレート」カテゴリを展開します。

1. 「**ユーザー・テンプレートの管理**」をクリックします。
2. ACL を編集する対象となるテンプレートを選択します。
3. 「**ACL の編集**」をクリックします。

Web 管理ツール・ユーティリティーを使用して ACL プロパティを表示させたり ACL を処理したりするには、558 ページの『ACL の処理』を参照してください。

詳細については、546 ページの『アクセス制御リスト』を参照してください。

ユーザー管理

レルムとテンプレートをセットアップしたら、そのレルムとテンプレートにユーザーのデータを取り込むことができます。

ユーザーの追加

Web 管理ツールを使用してユーザーを追加するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「**ユーザーとグループ**」カテゴリを展開します。

手順

1. 「**ユーザーの追加**」をクリックするか、または「**ユーザーの管理**」をクリックして、「**追加**」をクリックします。
2. ユーザーを追加する対象となるレルムをドロップダウン・メニューから選択します。
3. 「**次へ**」をクリックします。そのレルムに関連付けられたテンプレートが表示されます。アスタリスク (*) で指示された必須フィールドと、タブのその他のフィールドに入力します。レルム内にすでにグループが作成されている場合は、複数のグループにユーザーを追加することもできます。
4. 完了したら、「**完了**」をクリックします。

レルム内のユーザーの検索

Web 管理ツールを使用してレルム内のユーザーを検索するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「**ユーザーとグループ**」カテゴリを展開します。

1. 「**ユーザーの管理**」をクリックします。
2. 「**アクションの選択**」メニューを展開して、「**検索ツールバーの表示**」を選択し、「**実行**」をクリックします。
3. 「**レルムの選択**」フィールドから、検索するレルムを選択します。
4. 「**検索**」フィールドに検索ストリングを入力します。検索ユーティリティーの使用方法については、27 ページの『検索』を参照してください。
5. 選択されたユーザーについて、以下の操作を実行できます。

- **追加** - 611 ページの『ユーザーの追加』を参照してください。
- **編集** - 『ユーザー情報の編集』を参照してください。
- **コピー** - 『ユーザーのコピー』を参照してください。
- **削除** - 『ユーザーの除去』を参照してください。

6. 完了したら、「OK」をクリックします。

ユーザー情報の編集

Web 管理ツールを使用してユーザー情報を編集するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」カテゴリーを展開します。

手順

1. 「ユーザーの管理」をクリックします。
2. ドロップダウン・メニューからレلمムを選択します。「ユーザー」ボックスにユーザーがまだ表示されていない場合は、「ユーザーの表示」をクリックします。
3. 編集するユーザーを選択して、「編集」をクリックします。
4. タブの情報を変更して、グループ・メンバーシップを変更します。
5. 完了したら、「OK」をクリックします。

ユーザーのコピー

Web 管理ツールを使用してユーザーをコピーするには、以下の手順を実行します。

このタスクについて

ほとんど同じ情報を持つ多数のユーザーを作成する必要がある場合は、最初のユーザーをコピーして、その情報を変更することで、追加のユーザーを作成できます。

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」カテゴリーを展開します。

1. 「ユーザーの管理」をクリックします。
2. ドロップダウン・メニューからレلمムを選択します。「ユーザー」ボックスにユーザーがまだ表示されていない場合は、「ユーザーの表示」をクリックします。
3. コピーするユーザーを選択して、「コピー」をクリックします。
4. 特定のユーザー (sn または cn など) を識別する必須情報など、新しいユーザーの該当する情報を変更します。両方のユーザーに共通する情報を変更する必要はありません。
5. 完了したら、「OK」をクリックします。

ユーザーの除去

Web 管理ツールを使用してユーザーを削除するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」カテゴリを展開します。

手順

1. 「ユーザーの管理」をクリックします。
2. ドロップダウン・メニューからレルムを選択します。「ユーザー」ボックスにユーザーがまだ表示されていない場合は、「ユーザーの表示」をクリックします。
3. 除去するユーザーを選択して、「削除」をクリックします。
4. 削除を確認するプロンプトが出されたら、「OK」をクリックします。
5. ユーザーのリストからユーザーが除去されます。

グループ管理

レルムとテンプレートをセットアップしたら、グループを作成することができます。

グループの追加

Web 管理ツールを使用してグループを追加するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」カテゴリを展開します。

1. 「グループの追加」をクリックするか、または「グループの管理」をクリックして、「追加」をクリックします。
2. 作成するグループの名前を入力します。
3. グループを追加する対象となるレルムをドロップダウン・メニューから選択します。
4. 「完了」をクリックすると、グループが作成されます。レルムにすでにユーザーが存在する場合は、「次へ」をクリックして、ユーザーをグループに追加できます。「完了」をクリックします。

詳細については、570 ページの『グループ (Groups)』を参照してください。

レルム内のグループの検索

Web 管理ツールを使用してレルム内のグループを検索するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」カテゴリを展開します。

1. 「グループの管理」をクリックします。
2. 「アクションの選択」メニューを展開して、「検索ツールバーの表示」を選択し、「実行」をクリックします。
3. 「レルムの選択」フィールドから、検索するレルムを選択します。

4. 「検索」フィールドに検索ストリングを入力します。検索ユーティリティーの使用方法については、27 ページの『検索』を参照してください。
5. 選択されたグループについて、以下の操作を実行できます。
 - 追加 - 613 ページの『グループの追加』を参照してください。
 - 編集 - 『グループ情報の編集』を参照してください。
 - コピー - 『グループのコピー』を参照してください。
 - 削除 - 615 ページの『グループの除去』を参照してください。
6. 完了したら、「閉じる」をクリックします。

グループ情報の編集

Web 管理ツールを使用してグループの情報を編集するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」カテゴリーを展開します。

手順

1. 「グループの管理」をクリックします。
2. ドロップダウン・メニューからレلمムを選択します。「グループ」ボックスにグループがまだ表示されていない場合は、「グループの表示」をクリックします。
3. 編集するグループを選択して、「編集」をクリックします。
4. グループにユーザーを追加したり、グループからユーザーを除去することができます。
5. 完了したら、「OK」をクリックします。

グループのコピー

Web 管理ツールを使用してグループをコピーするには、以下の手順を実行します。

このタスクについて

ほとんど同じメンバーを持つ多数のグループを作成する必要がある場合は、最初のグループをコピーして、その情報を変更することで、追加のグループを作成できます。

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」カテゴリーを展開します。

1. 「グループの管理」をクリックします。
2. ドロップダウン・メニューからレلمムを選択します。「グループ」ボックスにユーザーがまだ表示されていない場合は、「グループの表示」をクリックします。
3. コピーするグループを選択して、「コピー」をクリックします。
4. 「グループ名」フィールドのグループ名を変更します。新しいグループのメンバーは、元のグループのメンバーと同じになります。

5. また、グループ・メンバーを選択して「**追加**」をクリックすると新規グループ・メンバーの追加を、「**削除**」をクリックするとグループ・メンバーの削除を、「**表示**」をクリックするとグループ・メンバー情報の表示を、それぞれ実行できます。
6. 完了したら、「**OK**」をクリックします。新しいグループが作成され、コピー中に行った追加または除去により、元のグループと同じメンバーが含まれます。

グループの除去

Web 管理ツールを使用してグループを削除するには、以下の手順を実行します。

このタスクについて

Web 管理ツールのナビゲーション領域で「**ユーザーとグループ**」カテゴリーを展開します。

手順

1. 「**グループの管理**」をクリックします。
2. ドロップダウン・メニューからレلمを選択します。「**グループ**」ボックスにグループがまだ表示されていない場合は、「**グループの表示**」をクリックします。
3. 除去するグループを選択して、「**削除**」をクリックします。
4. 削除を確認するプロンプトが出されたら、「**OK**」をクリックします。
5. グループのリストからグループが除去されます。

付録 A. エラー・コード

LDAP エラー・コードで可能な値を以下の表に示します。

表 40. 一般的な戻りコード

10 進 値	値	16 進 値	要旨	詳細記述
00	LDAP_SUCCESS	00	成功	要求は成功しました。
01	LDAP_OPERATIONS_ERROR	01	操作エラー	操作エラーが発生しました。
02	LDAP_PROTOCOL_ERROR	02	プロトコル・エラー	プロトコル違反が検出されました。
03	LDAP_TIMELIMIT_EXCEEDED	03	時間制限を超えました	LDAP 時間制限を超えました。
04	LDAP_SIZELIMIT_EXCEEDED	04	サイズ制限を超えました	LDAP サイズ制限を超えました。
05	LDAP_COMPARE_FALSE	05	比較 false	比較操作が false を戻しました。
06	LDAP_COMPARE_TRUE	06	比較 true	比較操作が true を戻しました。
07	LDAP_STRONG_AUTH_NOT_SUPPORTED	07	強力な認証はサポート されていません	LDAP サーバーは強力な 認証をサポートしていま せん。
08	LDAP_STRONG_AUTH_REQUIRED	08	強力な認証が必要です	操作には強力な認証が必 要です。
09	LDAP_PARTIAL_RESULTS	09	部分的結果と参照を受 信しました	部分的結果のみが戻され ました。
10	LDAP_REFERRAL	0A	参照が戻されました	参照が戻されました。
11	LDAP_ADMIN_LIMIT_EXCEEDED	0B	管理制限を超えました	管理制限を超えました。
12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION	0C	限界の拡張はサポート されていません	限界の拡張はサポートさ れていません。
13	LDAP_CONFIDENTIALITY_REQUIRED	0D	機密性が必要です	機密性が必要です。
14	LDAP_SASL_BIND_IN_PROGRESS	0E	SASL バインドが進行 中です	SASL バインドが進行中 です。
16	LDAP_NO_SUCH_ATTRIBUTE	10	そのような属性はあり ません	指定した属性タイプは項 目に存在しません。
17	LDAP_UNDEFINED_TYPE	11	属性タイプが未定義で す	指定した属性タイプは有 効ではありません。
18	LDAP_INAPPROPRIATE_MATCHING	12	不適切な突き合わせ	フィルター・タイプは、 指定した属性でサポート されていません。

表 40. 一般的な戻りコード (続き)

10 進値	値	16 進値	要旨	詳細記述
19	LDAP_CONSTRAINT_VIOLATION	13	制約違反	指定した属性値は、制約に違反しています (住所の行が多すぎる、1 行が長すぎるなど)。
20	LDAP_TYPE_OR_VALUE_EXISTS	14	タイプまたは値が存在します	指定した属性タイプまたは属性値は、項目にすでに存在します。
21	LDAP_INVALID_SYNTAX	15	構文が無効です	有効ではない属性値が指定されました。
32	LDAP_NO_SUCH_OBJECT	20	そのようなオブジェクトはありません	指定したオブジェクトはディレクトリーに存在しません。
33	LDAP_ALIAS_PROBLEM	21	別名の問題	ディレクトリー内の別名が存在しない項目を指しています。
34	LDAP_INVALID_DN_SYNTAX	22	DN 構文が無効です	構文が無効な DN が指定されました。
35	LDAP_IS_LEAF	23	オブジェクトはリーフです	指定したオブジェクトはリーフです。
36	LDAP_ALIAS_DEREF_PROBLEM	24	別名の参照解除の問題	別名を参照解除するときに問題が発生しました。
48	LDAP_INAPPROPRIATE_AUTH	30	不適切な認証	不適切な認証が指定されました (例えば、LDAP_AUTH_SIMPLE が指定され、項目に userPassword 属性がありません)。
49	LDAP_INVALID_CREDENTIALS	31	資格情報が無効です	無効な資格情報が示されました (例えばパスワードの間違いなど)。
50	LDAP_INSUFFICIENT_ACCESS	32	不十分なアクセス権	ユーザーが操作を実行するためのアクセス権が不十分です。
51	LDAP_BUSY	33	DSA は使用中です	DSA は使用中です
52	LDAP_UNAVAILABLE	34	DSA は使用不可です	DSA は使用不可です。
53	LDAP_UNWILLING_TO_PERFORM	35	DSA は実行を望んでいません	DSA は操作の実行を望んでいません。
54	LDAP_LOOP_DETECT	36	ループが検出されました	ループが検出されました。
64	LDAP_NAMING_VIOLATION	40	命名違反	命名違反が発生しました。

表 40. 一般的な戻りコード (続き)

10 進値	値	16 進値	要旨	詳細記述
65	LDAP_OBJECT_CLASS_VIOLATION	41	オブジェクト・クラス違反	オブジェクト・クラス違反が発生しました (例えば、"required" 属性が項目から抜けています)。
66	LDAP_NOT_ALLOWED_ON_NONLEAF	42	非リーフでの操作は許されません	非リーフ・オブジェクトでの操作は許されません。
67	LDAP_NOT_ALLOWED_ON_RDN	43	RDN での操作は許されません	RDN での操作は許されません。
68	LDAP_ALREADY_EXISTS	44	すでに存在しています	項目はすでに存在しています。
69	LDAP_NO_OBJECT_CLASS_MODS	45	オブジェクト・クラスを変更できません	オブジェクト・クラスの変更は許されません。
70	LDAP_RESULTS_TOO_LARGE	46	結果が大きすぎます	結果が大きすぎます。
71	LDAP_AFFECTS_MULTIPLE_DSAS	47	複数の DSA に影響を与えます	複数の DSA に影響を与えます。
80	LDAP_OTHER	50	不明なエラーです	不明のエラーが発生しました。
81	LDAP_SERVER_DOWN	51	LDAP サーバーに接続できません	LDAP ライブラリーは LDAP サーバーに接続できません。
82	LDAP_LOCAL_ERROR	52	ローカル・エラー	ローカル・エラーが発生しました。これは通常、メモリー割り振りの失敗です。
83	LDAP_ENCODING_ERROR	53	エンコード・エラー	LDAP サーバーに送信するパラメーターのエンコード中にエラーが発生しました。
84	LDAP_DECODING_ERROR	54	デコード・エラー	LDAP サーバーの結果のデコード中にエラーが発生しました。
85	LDAP_TIMEOUT	55	タイムアウト	結果の待機中に時間制限を超えました。
86	LDAP_AUTH_UNKNOWN	56	不明な認証方式	バインド操作で指定された認証方法が不明です。
87	LDAP_FILTER_ERROR	57	誤った検索フィルター	ldap_search に無効なフィルターが指定されました (例えば、括弧が対になっていないなど)。
88	LDAP_USER_CANCELLED	58	ユーザーが操作を取り消しました	ユーザーが操作を取り消しました。

表 40. 一般的な戻りコード (続き)

10 進値	値	16 進値	要旨	詳細記述
89	LDAP_PARAM_ERROR	59	LDAP ルーチンに対する誤ったパラメーター	誤ったパラメーターを使用して LDAP ルーチンが呼び出されました (例えばヌル LD ポインターなど)。
90	LDAP_NO_MEMORY	5A	メモリー不足	LDAP ライブラリー・ルーチンでメモリー割り振り (malloc など) 呼び出しが失敗しました。
91	LDAP_CONNECT_ERROR	5B	接続エラー	接続エラーです。
92	LDAP_NOT_SUPPORTED	5C	サポートされていません	サポートされていません。
93	LDAP_CONTROL_NOT_FOUND	5D	制御が見つかりません	制御が見つかりません。
94	LDAP_NO_RESULTS_RETURNED	5E	結果は戻されません	結果は戻されません。
95	LDAP_MORE_RESULTS_TO_RETURN	5F	さらに結果が戻されます	さらに結果が戻されます。
96	LDAP_URL_ERR_NOTLDAP	60	URL が ldap:// で始まっていません	URL が ldap:// で始まっていません。
97	LDAP_URL_ERR_NODN	61	URL に DN がありません (必須)	URL に DN がありません (必須)。
98	LDAP_URL_ERR_BADSCOPE	62	URL の有効範囲ストリングが無効です	URL の有効範囲ストリングが無効です。
99	LDAP_URL_ERR_MEM	63	メモリー・スペースの割り当てができません	メモリー・スペースの割り当てができません。
100	LDAP_CLIENT_LOOP	64	クライアント・ループ	クライアント・ループです。
101	LDAP_REFERRAL_LIMIT_EXCEEDED	65	参照制限を超えました	参照制限を超えました。
112	LDAP_SSL_ALREADY_INITIALIZED	70	ldap_ssl_client_init は、前にこのプロセスで正常に呼び出されました	ldap_ssl_client_init は、前にこのプロセスで正常に呼び出されました。
113	LDAP_SSL_INITIALIZE_FAILED	71	初期化呼び出しが失敗しました	SSL 初期化呼び出しが失敗しました。 注: GSKit がインストールされていて、GSKit ライブラリーが用意されている必要があります。
114	LDAP_SSL_CLIENT_INIT_NOT_CALLED	72	SSL 接続を使用する前に ldap_ssl_client_init を呼び出す必要があります	SSL 接続を使用する前に ldap_ssl_client_init を呼び出す必要があります。
115	LDAP_SSL_PARAM_ERROR	73	前に指定した SSL パラメーターが無効です	有効ではない SSL パラメーターが前に指定されました。

表 40. 一般的な戻りコード (続き)

10 進値	値	16 進値	要旨	詳細記述
116	LDAP_SSL_HANDSHAKE_FAILED	74	SSL サーバーへの接続に失敗しました	SSL サーバーへの接続に失敗しました。
117	LDAP_SSL_GET_CIPHER_FAILED	75	使用されていません	使用すべきではありません。
118	LDAP_SSL_NOT_AVAILABLE	76	SSL ライブラリーが見つかりません	GSKit がインストールされていることを確認してください。
	LDAP_SSL_KEYRING_NOT_FOUND	77		
	LDAP_SSL_PASSWORD_NOT_SPECIFIED	78		
128	LDAP_NO_EXPLICIT_OWNER	80	明示的な所有者が見つかりません	明示的な所有者が見つかりませんでした。
129	LDAP_NO_LOCK	81	ロックを取得できませんでした	クライアント・ライブラリーは、必要なリソースをロックできませんでした。

さらに、ldap.h ファイルでは以下の DNS 関連のエラー・コードが定義されています。

表 41. DNS 関連の戻りコード

10 進値	値	16 進値	詳細記述
133	LDAP_DNS_NO_SERVERS	85	LDAP サーバーが見つかりません
134	LDAP_DNS_TRUNCATED	86	警告: DNS 結果が切り捨てられました
135	LDAP_DNS_INVALID_DATA	87	DNS データが無効です
136	LDAP_DNS_RESOLVE_ERROR	88	システム・ドメインまたはネーム・サーバーを解決できません
137	LDAP_DNS_CONF_FILE_ERROR	89	DNS 構成ファイル・エラー

ldap.h ファイルでは、以下の UTF8 関連のエラー・コードが定義されています。

表 42. UTF8 関連の戻りコード

10 進値	値	16 進値	詳細記述
160	LDAP_XLATE_E2BIG	A0	出力バッファのオーバーフロー
161	LDAP_XLATE_EINVAL	A1	入力バッファが切り捨てられました
162	LDAP_XLATE_EILSEQ	A2	入力文字が使用不可能です
163	LDAP_XLATE_NO_ENTRY	A3	マップ先を指しているコード・セットがありません
176	LDAP_REG_FILE_NOT_FOUND	B0	ファイルが NT レジストリーにありません
177	LDAP_REG_CANNOT_OPEN	B1	NT レジストリーを開けません
178	LDAP_REG_ENTRY_NOT_FOUND	B2	項目が NT レジストリーにありません
192	LDAP_CONF_FILE_NOT_OPENED	C0	プラグイン構成ファイルが開きません

表 42. UTF8 関連の戻りコード (続き)

10 進 値	値	16 進 値	詳細記述
193	LDAP_PLUGIN_NOT_LOADED	C1	プラグイン・ライブラリーがロードされません
194	LDAP_PLUGIN_FUNCTION_ NOT_RESOLVED	C2	プラグイン関数が解決されません
195	LDAP_PLUGIN_NOT_INITIALIZED	C3	プラグイン・ライブラリーが初期化されません
196	LDAP_PLUGIN_COULD_NOT_BIND	C4	プラグイン関数にバインドできませんでした
208	LDAP_SASL_GSS_NO_SEC_CONTEXT	D0	gss_init_sec_context が失敗しました

付録 B. ルート DSE 内部のオブジェクト ID (OID) および属性

IBM Security Directory Server 6.3 では、以下のセクションに示す OID および属性が使用されます。

これらの OID および属性は、ルート DSE の内部にあります。ルート DSE 項目には、サーバー自体の情報が格納されています。

IBM Security Directory Server では、LDAP サーバーに関する情報をユーザーに示すために LDAP サーバーが提供するルート DSE 項目を定義します。例えば、LDAP がサポートしているバージョンを確認する場合などがこれに該当します。

ルート DSE 内部の OID や属性を表示するには、以下のコマンドを実行します。

```
idsldapsearch -D <AdminDN> -w <Adminpw> -s base  
-b "" objectclass=*
```

詳しくは、「*IBM Security Directory Server Version 6.3 Programming Reference*」を参照してください。

ルート DSE 内の属性

以下に示すのは、ルート DSE 内の属性のリストです。

namingcontexts

サーバー内に保持されている命名コンテキスト。

この属性の値は、このサーバーがマスターまたはシャドーを生成する命名コンテキストに対応します。サーバーがマスターもシャドーも生成しない (共通の X.500 ディレクトリーへの LDAP ゲートウェイであるなどの) 場合、この属性は存在しません。サーバーにディレクトリー全体が格納されていると想定される場合、属性の値は 1 つであり、この値は空ストリングです (ルートがヌル DN であることを示します)。この属性を使用すると、クライアントはサーバーと通信したときに、検索に適した基本オブジェクト (ユーザーが構成データに定義する一連の最上位サフィックス) を選択できます。

ibm-configurationnamingcontext

サーバーの構成項目が保管されるサフィックス。バージョン 6.0 以上では、cn=configuration となります。

subschemasubentry

この属性の値はサブスキーマ項目の名前です。この項目内では、スキーマを指定している属性をサーバーが有効にしています。この属性は cn=schema に設定されます。

セキュリティ

サーバーが listen するセキュア SSL ポート (例: 636)。

ポート サーバーが listen する非セキュア・ポート (例: 389)。これは、サーバーでセキュア・ポートが使用可能になっていない場合にのみ提供されます。

supportedSaslMechanisms

サポートされている一連の SASL セキュリティー機能。

この属性の値は、サーバーがサポートしている SASL メカニズムの名前です。サーバーがいずれのメカニズムもサポートしていない場合、この属性は存在しません。この属性には、サーバーに登録されている SASL メカニズムが含まれています。

supportedLdapVersion

現在のサーバーによってインプリメントされている LDAP バージョン。

この属性の値は、サーバーがインプリメントしている LDAP プロトコルのバージョンです。値は、2 および 3 です。

ibmDirectoryVersion

このサーバーにインストールされている IBM Security Directory Server のバージョン。現在のバージョンは 6.3 です。

ibm-enabledCapabilities

現在サーバーで使用可能になっているサーバー機能をリストします。値については、625 ページの『サポートされ、使用可能になっている機能の OID』を参照してください。

ibm-ldapserviceName

サーバーのホスト名を指定します。Kerberos レalmが定義されている場合、形式は `hostname@realmname` のようになります。

ibm-serverId

サーバーを最初に始動したときにサーバーに割り当てられる固有の ID。この ID は、サーバーの役割を判別するために複製トポロジーで使用されます。

vendorName

LDAP のこのバージョンのサプライヤー。IBM Security Directory Server では、この属性は International Business Machines (IBM) に設定されます。

vendorVersion

IBM Security Directory Server 6.3 では、ベンダーのバージョンは 6.3 に設定されます。

ibm-slapdSecurityProtocol

サーバーで構成されたセキュアな通信プロトコルを指定します。

ibm-tlsciphers

サーバーで構成された、サポートされている TLS 1.2 暗号を指定します。

ibm-slapdServerBackend

サーバーのロード対象がデータベースかプロキシ・バックエンドかを指定します。

ibm-slapdSizeLimit

管理者以外のユーザーが開始した検索で戻される項目の数を制限します。

ibm-slapdTimeLimit

管理者以外のユーザーが開始した検索要求の処理にサーバーが費やす時間の最大値 (秒) を指定します。

ibm-slapdSSLExtSigalg

サーバーで構成された TLS 1.2 署名およびハッシュ・アルゴリズムを指定します。

ibm-slapdSuiteBMode

サーバーで構成された Suite B 暗号セキュリティ・レベルを指定します。

ibm-slapdDerefAliases

参照解除を処理するためにサーバーをどのように構成するのかを記述します。

ibm-supportedAuditVersion

サポートされる監査のバージョン。例えば、バージョン 6.0 以上では、拡張操作の監査に対応する監査バージョン 3 をサーバーがサポートします。

ibm-supportedACIMechanisms

サーバーがサポートする ACL モデルをリストします。値については、636 ページの『ACI 機構の OID』を参照してください。

ibm-supportedcapabilities

現在サーバーでサポートされているサーバー機能をリストします。値については、『サポートされ、使用可能になっている機能の OID』を参照してください。

ibm-sasldigestrealmname

サーバーに関連付けられている SASL ダイジェスト・レルム名が表示されます。

ibm-slapdServerInstanceName

サーバーで実行中のディレクトリー・サーバー・インスタンスの名前。

ibm-slapdisconfigurationmode

サーバーが構成モードで実行中かどうかを識別します。TRUE の場合、サーバーは構成モードです。FALSE の場合、サーバーは構成モードではありません。

サポートされ、使用可能になっている機能の OID

以下の表に、サポートされ、使用可能になっている機能の OID を示します。これらの OID を使用すると、特定のサーバーがこれらの機能をサポートしているかどうかを確認できます。

表 43. サポートされ、使用可能になっている機能の OID

短縮名および OID	説明	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
			分割データなし	分割データあり
拡張複製モデル 1.3.18.0.2.32.1	サブツリーおよびカスケード複製などの複製モデルを示します。	はい	N/A	N/A

表 43. サポートされ、使用可能になっている機能の OID (続き)

短縮名および OID	説明	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
			分割データなし	分割データあり
項目のチェックサム 1.3.18.0.2.32.2	このサーバーが ibm-entrychecksum 機能および ibm-entrychecksumop 機能をサポートすることを示します。	はい	はい	はい
項目 UUID 1.3.18.0.2.32.3	この値は、ibm-entryuuid 属性をサポートしているサフィックスの ibm-capabilities サブエントリに表示されます。	はい	はい	はい
ACL のフィルター操作 1.3.18.0.2.32.4	このサーバーが IBM フィルター ACL モデルをサポートすることを示します。	はい	はい	はい
パスワード・ポリシー 1.3.18.0.2.32.5	このサーバーがパスワード・ポリシーをサポートすることを示します。	はい	はい	はい
DN を基準にしたソート 1.3.18.0.2.32.6	通常の属性に加えて DN でソートされる検索を使用可能にします。	はい	いいえ	いいえ
管理グループの委任 1.3.18.0.2.32.8	サーバーは、構成バックエンドに指定されている管理者グループに対するサーバー管理の委任をサポートしています。	はい	はい	はい
サービス妨害の防止 1.3.18.0.2.32.9	サーバーは、読み取り/書き込みタイムアウトなどのサービス妨害防止機能をサポートしています。	はい	はい	はい
別名の参照解除オプション 1.3.18.0.2.32.10	サーバーは、デフォルトでは別名の参照解除を実行しないオプションをサポートしています。 * プロキシの rootDSE は表示されません。 ** 区画をまたがった別名は逆参照されません。	はい	はい(*)	はい(**)
管理サーバーの監査ログ作成 1.3.18.0.2.32.11	サーバーは管理サーバーの監査機能をサポートしています。	はい	はい	はい

表 43. サポートされ、使用可能になっている機能の OID (続き)

短縮名および OID	説明	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
			分割データなし	分割データあり
128 文字のテーブル名 1.3.18.0.2.32.12	固有の属性名に 19 文字以上 (最大 128 文字) を使用できるようするサーバー機能。 * プロキシの rootDSE は表示されません。 ** 固有性は区画をまたがっては保証されません。	はい	はい(*)	はい(**)
検索フィルター解決用の属性キャッシュ 1.3.18.0.2.32.13	サーバーは、検索フィルター解決用の属性キャッシュをサポートしています。	はい	N/A	N/A
動的トレース 1.3.18.0.2.32.14	サーバーは、LDAP 拡張操作によるサーバーのアクティブ・トレースをサポートしています。	はい	はい	はい
項目とサブツリーの動的更新 1.3.18.0.2.32.15	サーバーは、項目とサブツリーの動的構成の更新をサポートしています。	はい	はい	はい
グローバルな固有属性 1.3.18.0.2.32.16	サーバーは、グローバルな固有属性値を適用する機能を備えています。	はい	いいえ	いいえ
グループ固有の検索制限 1.3.18.0.2.32.17	グループの拡張検索制限をサポートしています。 * プロキシの rootDSE は表示されません。 ** データが分割されている場合、グループ・ベースの検索制限の機能には一貫性がありません。	はい	はい(*)	はい(**)
IBMpolicies 複製サブツリー 1.3.18.0.2.32.18	サーバーは cn=IBMpolicies サブツリーの複製をサポートしています。	はい	はい	はい
最大存続期間の変更ログ項目 1.3.18.0.2.32.19	サーバーが変更ログ項目の保存期間を存続期間を基準にできることを指定します。	はい	N/A	N/A

表 43. サポートされ、使用可能になっている機能の OID (続き)

短縮名および OID	説明	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
			分割データなし	分割データあり
ロギング・カウントのモニター 1.3.18.0.2.32.20	サーバーは、サーバー、コマンド行インターフェース、および監査ログ・ファイルに追加されたメッセージのロギング・カウントのモニター機能を提供します。	はい	はい	はい
アクティブ・ワーカーのモニター情報 1.3.18.0.2.32.21	サーバーは、アクティブ・ワーカーのモニター情報 (cn=workers,cn=monitor) を提供します。	はい	はい	はい
接続タイプ・カウントのモニター 1.3.18.0.2.32.22	サーバーは、SSL 接続および TLS 接続の接続タイプ・カウントをモニターする機能を提供します。	はい	はい	はい
接続情報のモニター 1.3.18.0.2.32.23	サーバーは、接続 ID (cn=connections, cn=monitor) ではなく IP アドレス別に接続のモニター情報を提供します。	はい	はい	はい
操作カウントのモニター 1.3.18.0.2.32.24	サーバーは、開始操作タイプと完了操作タイプの操作カウントを新たにモニターする機能を提供します。 * 操作完了カウントは、プロキシー内で実際に完了した操作数を反映しません。代わりに、完了済みの操作数か、処理のためにバックエンド・サーバーに送信された操作数を表します。プロキシー固有のモニターは、Security Directory Server 6.1 以降のバージョンで使用する必要があります。	はい	はい(*)	はい(*)
トレース情報のモニター 1.3.18.0.2.32.25	サーバーは、現在使用中のトレース・オプションの情報をモニターする機能を提供します。	はい	はい	はい
ヌル・ベースのサブツリー検索 1.3.18.0.2.32.26	サーバーでは、サーバーで定義された DIT 全体を検索するヌル・ベースのサブツリー検索が可能です。	はい	いいえ	いいえ
プロキシー許可 1.3.18.0.2.32.27	サーバーは、ユーザー・グループのプロキシー許可をサポートしています。	はい	いいえ	いいえ

表 43. サポートされ、使用可能になっている機能の OID (続き)

短縮名および OID	説明	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
			分割データなし	分割データあり
TLS 機能 1.3.18.0.2.32.28	サーバーが実際に TLS を実行できることを指定します。	はい	はい	はい
非ブロッキング複製 1.3.18.0.2.32.29	サーバーは、コンシューマー (レプリカ) から受信したいくつかのエラーを無視する機能を備えています。このエラーは、通常、正常な結果コードを受信するまで更新情報が定期的に再送信されるというものです。	はい	N/A	N/A
Kerberos 機能 1.3.18.0.2.32.30	サーバーが Kerberos を使用できることを指定します。	はい	いいえ	いいえ
ibm-allMembers 運用属性および ibm-allGroups 運用属性 1.3.18.0.2.32.31	バックエンドが ibm-allGroups 運用属性および ibm-allMembers 運用属性に関する検索をサポートするかどうかを指定します。	はい	はい	はい
すべての運用属性 1.3.6.1.4.1.4203.1.5.1	すべての運用属性 * プロキシの rootDSE は表示されません。 ** 一部の運用属性は、分散していないデータに依存します。	はい	はい(*)	はい(**)
言語タグ 1.3.6.1.4.1.4203.1.5.4	サーバーが言語タグをサポートします。	はい	いいえ	いいえ
GSKit 用の FIPS モード 1.3.18.0.2.32.32	ICC FIPS 認証ライブラリーからの暗号化アルゴリズムをサーバーが使用できるようになります。	はい	はい	はい
DN の変更 (リーフの移動) 1.3.18.0.2.32.35	DN の変更操作がリーフ項目の新規上位をサポートするかどうかを示します。既存の DN 変更 (サブツリーの移動) 機能はこの機能を前提としている、ということに注意してください。アプリケーションは両方の機能をチェックする必要があります。 * DN の変更を使用できるのは、変更が複数の区画にまたがっていない場合に限られます。	はい	はい	はい(*)

表 43. サポートされ、使用可能になっている機能の OID (続き)

短縮名および OID	説明	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
			分割データなし	分割データあり
属性のサイズ変更の単純化 1.3.18.0.2.32.37	カスタマーは、スキーマ変更機能を介して属性の最大長を増加できます。	はい	N/A	N/A
グローバル管理グループ 1.3.18.0.2.32.38	サーバーは、RDBM バックエンドに指定されている管理者グループに対するサーバー管理の委任をサポートしています。グローバル管理者は、構成ファイルまたはログ・ファイルに対する権限を所有しません。	はい	はい	はい
AES 暗号化オプション 1.3.18.0.2.32.39	サーバーは AES パスワード暗号化をサポートしています。	はい	はい	はい
比較の監査機能 1.3.18.0.2.32.40	サーバーは比較操作の監査機能をサポートしています。	はい	はい	はい
ログの管理 1.3.18.0.2.32.41	このサーバーがログ管理をサポートすることを示します。	はい	はい	はい
マルチスレッド複製 1.3.18.0.2.32.42	複製合意で、マルチスレッドの使用、およびコンシューマーとの複数接続の使用を指定できます。	はい	N/A	N/A
サプライヤー複製構成 1.3.18.0.2.32.43	サプライヤーの複製用のサーバー構成。	はい	N/A	N/A
グローバル更新での CN=IBMPOLICIES の使用 1.3.18.0.2.32.44	サーバーは、cn=IBMPolicies サブツリーの複製トポロジーを使用した、グローバル更新の複製をサポートしています。	はい	N/A	N/A
マルチホーム構成のサポート 1.3.18.0.2.32.45	サーバーは、複数の IP アドレス (マルチホーム) の構成をサポートしています。	はい	はい	はい
複数の Directory Server インスタンス・アーキテクチャー 1.3.18.0.2.32.46	同一のマシンで複数のディレクトリー・サーバー・インスタンスを実行できるようにサーバーは設計されています。	はい	はい	はい
構成ツールの監査 1.3.18.0.2.32.47	サーバーは構成ツールの監査機能をサポートしています。	はい	はい	はい
監査統合の構成設定 1.3.18.0.2.32.48	監査ログ設定が構成ファイルにあることを示します。	はい	はい	はい

表 43. サポートされ、使用可能になっている機能の OID (続き)

短縮名および OID	説明	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
			分割データなし	分割データあり
プロキシ・サーバー 1.3.18.0.2.32.49	サーバーがプロキシ・サーバーまたは通常の RDBM サーバーとして動作できるかどうかを示します。 オプション情報。	はい	はい	はい
LDAP 属性キャッシュの自動調整 1.3.18.0.2.32.50	自動属性キャッシュがサポートされ、使用可能になっていることを示します。 注: IBM Security Directory Server 6.3 リリース以降、属性キャッシュは非推奨になりました。 今後は、属性キャッシュの使用を避けてください。	はい	N/A	N/A
複製競合解決の最大項目サイズ 1.3.18.0.2.32.51	サプライヤーは、この数値に基づいて、複製競合を解決するためにターゲット・サーバーに項目を再追加する必要があるかどうかを判断します。	はい	N/A	N/A
LostAndFound ログ・ファイル 1.3.18.0.2.32.52	複製競合解決の結果、置き換えられる項目をアーカイブする LostAndFound ファイルをサポートします。	はい	N/A	N/A
パスワード・ポリシーによるアカウントのロックアウト 1.3.18.0.2.32.53	サーバーがパスワード・ポリシーによるアカウントのロックアウト機能をサポートしていることを示します。	はい	はい	はい
管理者パスワード・ポリシー 1.3.18.0.2.32.54	サーバーが管理者パスワード・ポリシーをサポートしていることを示します。	はい	はい	はい
SSL FIPS 処理モード 1.3.18.0.2.32.55	サーバーは SSL FIPS モードの処理をサポートしています。	はい	はい	はい
IDS 6.0 ibm-entrychecksumop 1.3.18.0.2.32.56	バージョン 6.0 の ibm-entrychecksumop 計算がサーバーで使用されたことを示します。	はい	いいえ	いいえ
LDAP パスワードのグローバル開始時刻 1.3.18.0.2.32.57	サーバーが cn=pwdPolicy 項目の ibm-pwdPolicyStartTime 属性をサポートできることを示します。	はい	いいえ	いいえ

表 43. サポートされ、使用可能になっている機能の OID (続き)

短縮名および OID	説明	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
			分割データなし	分割データあり
監査構成設定の統合 1.3.18.0.2.32.58	監査構成設定が、現在、ibmslapd 構成ファイルにのみあることを示します。 * トランザクションがサポートされるのは、すべての更新情報が単一の区画を対象にしている場合に限られます。	はい	はい(*)	はい(*)
CBE ログの形式 1.3.18.0.2.32.59	Security Directory Server ログの管理およびイベント形式への変換がサポートされていることを示します。	はい	はい	はい
暗号化属性のサポート 1.3.18.0.2.32.60	サーバーは暗号化属性をサポートしています。	はい	はい	はい
プロキシ・モニター検索 1.3.18.0.2.32.61	サーバーは、プロキシ・サーバーを対象とする特殊なモニター検索をサポートしています。	はい	はい	はい
SSHA パスワード暗号化 1.3.18.0.2.32.63	サーバーは SSHA パスワード暗号化をサポートしています。	はい	はい	はい
MD5 パスワード暗号化 1.3.18.0.2.32.64	サーバーは MD5 パスワード暗号化をサポートしています。	はい	はい	はい
フィルター複製 1.3.18.0.2.32.65	必須項目とその属性のサブセットのみを複製するよう設計されているサーバー機能。	はい	N/A	N/A
グループ・メンバー・キャッシュ 1.3.18.0.2.32.66	サーバーはグループ・メンバーのキャッシングをサポートしています。	はい	N/A	N/A
PKCS11 サポート 1.3.18.0.2.32.67	サーバーは PKCS11 暗号化規格をサポートしています。	はい	はい	はい
サーバー管理の役割 1.3.18.0.2.32.68	サーバーはサーバー管理の役割をサポートしています。	はい	はい	はい
Digest MD5 サポート 1.3.18.0.2.32.69	サーバーが Digest MD5 バインドをサポートします。	はい	はい	はい
外部バインド・サポート 1.3.18.0.2.32.70	サーバーが外部バインドをサポートします。	はい	はい	はい

表 43. サポートされ、使用可能になっている機能の OID (続き)

短縮名および OID	説明	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
			分割データなし	分割データあり
永続検索 1.3.18.0.2.32.71	サーバーが永続検索をサポートします。	はい	いいえ	いいえ
管理サーバーのサービス妨害防止 1.3.18.0.2.32.72	管理サーバーはサービス妨害防止をサポートします。	はい	はい	はい
管理サーバーの拡張モニター・サポート 1.3.18.0.2.32.73	管理サーバーは、「cn=monitor」、「cn=connections,cn=monitor」、および「cn=workers,cn=monitor」検索をサポートしています。	はい	はい	はい
スキーマ検索用の管理サーバー・サポート 1.3.18.0.2.32.74	管理サーバーはスキーマに関する検索をサポートします。	はい	はい	はい
システム・モニター検索 1.3.18.0.2.32.76	サーバーは cn=system,cn=monitor 検索をサポートします。	はい	はい	はい
複数のパスワード・ポリシー 1.3.18.0.2.32.77	サーバーでは、複数のパスワード・ポリシーを定義して使用できます。	はい	はい	いいえ
パススルー認証 1.3.18.0.2.32.78	サーバーはパススルー認証機能をサポートしています。	はい	いいえ	いいえ
複製サプライヤー要求の動的更新 1.3.18.0.2.32.79	サーバーは複製サプライヤー情報の動的更新をサポートしています。	はい	N/A	N/A
パフォーマンスの監査 1.3.18.0.2.32.81	サーバーは操作についてのパフォーマンスの監査をサポートしています。	はい	はい	はい
無緊急スレッド・サポート 1.3.18.0.2.32.82	緊急スレッドはサーバーによってサポートされません。	はい	はい	はい
拡張複製グループ RI の処理 1.3.18.0.2.32.83	拡張複製グループ RI の処理	はい	N/A	N/A
DB2 パスワードの再読み取り 1.3.18.0.2.32.84	サーバーは DB2 パスワードを再度読み取って、構成情報に指定されている DB2 パスワードの変更点を確認します。	はい	N/A	N/A

表 43. サポートされ、使用可能になっている機能の OID (続き)

短縮名および OID	説明	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
			分割データなし	分割データあり
複製キューに基づくプロキシのフェイルバック 1.3.18.0.2.32.85	プロキシ・サーバーは、構成ファイルに指定されているしきい値を複製キューが下回る場合にのみフェイルバックを行います。	いいえ	はい	はい
プロキシのフロー制御 1.3.18.0.2.32.86	プロキシ・サーバーはフロー制御アルゴリズムをサポートしています。	いいえ	はい	はい
バックアップ/復元の構成機能 1.3.18.0.2.32.87	サーバーは自動バックアップおよび復元の構成をサポートしています。	はい	N/A	N/A
パスワード・ポリシーでの連続する反復文字の最大数 1.3.18.0.2.32.88	サーバーはパスワード・ポリシーでの連続する反復文字の最大数の制限をサポートしています。	はい	はい	はい
仮想リスト・ビューのサポート 1.3.18.0.2.32.89	サーバーは検索での仮想リスト・ビューの制御をサポートしています。	はい	いいえ	いいえ
プロキシでのページ検索 1.3.18.0.2.32.90	プロキシ・サーバーは検索でのページ制御をサポートしています。	いいえ	はい	はい
トゥームストーンのサポート 1.3.18.0.2.32.92	サーバーは削除された項目のトゥームストーン操作をサポートしています。	はい	いいえ	いいえ
プロキシによるヘルス・チェック未処理制限 1.3.18.0.2.32.93	プロキシは、構成されている未処理のヘルス・チェック要求に基づくハング・サーバーの確認をサポートしています。	いいえ	はい	はい
複製での高精度タイム・スタンプ 1.3.18.0.2.32.94	複製では、競合を解決するために高精度のタイム・スタンプを使用します。	はい	N/A	N/A
分散動的グループの使用可能化 1.3.18.0.2.32.96	プロキシ・サーバーでは、分散動的グループの使用可能化/使用不可化構成オプションをサポートしています。	いいえ	はい	はい
分散グループの使用可能化 1.3.18.0.2.32.97	プロキシ・サーバーでは、分散グループの使用可能化/使用不可化構成オプションをサポートしています。	いいえ	はい	はい

表 43. サポートされ、使用可能になっている機能の OID (続き)

短縮名および OID	説明	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
			分割データなし	分割データあり
SHA-2 1.3.18.0.2.32.99	このサーバーが SHA-2 アルゴリズム・ファミリー (SHA-224、SHA-256、SHA-384、SHA-512) をサポートすることを示します。また、このサーバーは、Salted パージョンの SHA-2 アルゴリズム・ファミリー (SSHA-224、SSHA-256、SSHA-384、SSHA-512) もサポートします。 * SHA-2 は、バックエンド・データベースを備えたサーバーにのみ適用できます。	はい	N/A(*)	N/A(*)
NIST SP800-131A Suite B 1.3.18.0.2.32.101	サーバーが Suite B モードをサポートしていることを示します。	はい	はい	はい
TLS 1.0 プロトコル 1.3.18.0.2.32.102	サーバーが TLS v1.0 プロトコルをサポートしていることを示します。	はい	はい	はい
TLS 1.1 プロトコル 1.3.18.0.2.32.103	サーバーが TLS v1.1 プロトコルをサポートしていることを示します。	はい	はい	はい
TLS 1.2 プロトコル 1.3.18.0.2.32.104	サーバーが TLS v1.2 プロトコルをサポートしていることを示します。	はい	はい	はい
セキュリティー属性の複製 1.3.18.0.2.32.105	読み取り専用レプリカが、パスワード・ポリシー運用属性の複製の更新を受け入れることを示します。読み取り専用レプリカは、ユーザーのパスワード・ポリシー運用属性に影響するバインド操作をマスター・サーバーに通知できます。マスター・サーバーが、ユーザーのパスワード・ポリシー運用属性に影響するバインド操作に関する通知を読み取り専用レプリカから受け取ることができることを示します。	はい	はい	はい

ACI 機構の OID

以下の表に、ACI 機構の OID を示します。

表 44. ACI 機構の OID

短縮名	説明	割り当てられている OID
IBM SecureWay V3.2 ACL モデル	LDAP サーバーが IBM SecureWay V3.2 ACL モデルをサポートすることを示します。	1.3.18.0.2.26.2
IBM フィルター・ベースの ACL 機構	LDAP サーバーが IBM Security Directory Server のフィルター・ベースの ACL をサポートしていることを示します。	1.3.18.0.2.26.3
System 属性と Restricted 属性の ACL サポート	サーバーは、system 属性と restricted 属性に関する ACL の指定および評価をサポートしています。	1.3.18.0.2.26.4

拡張操作の OID

以下の表に、拡張操作の OID を示します。

表 45. 拡張操作の OID

短縮名および OID	説明	管理サーバーによるサポートの対象	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
				分割データなし	分割データあり
アカウント・ステータス拡張操作 1.3.18.0.2.12.58	この拡張操作は、サーバーに、userPassword 属性を含む項目の DN を送信します。サーバーは、照会を受けたユーザー・アカウントのステータスを送り返します。 open locked expired	いいえ	はい	いいえ	いいえ
属性タイプの拡張操作 1.3.18.0.2.12.46	操作、言語タグ、属性キャッシュ、固有、または構成などのサポートされる機能により属性を検索します。	はい	はい	はい	はい
トランザクション開始の拡張操作 1.3.18.0.2.12.5	トランザクション・コンテキストを開始します。	いいえ	はい	はい	はい
カスケード複製操作の拡張操作 1.3.18.0.2.12.15	この操作では、要求されたアクションを発行先のサーバー上で実行し、この呼び出しを複製トポロジーでこの操作の下位に置かれているすべてのコンシューマーに継続的に転送します。	いいえ	はい	いいえ	いいえ
ログ消去の拡張操作 1.3.18.0.2.12.20	ログ・ファイルのクリアを要求します。	いいえ	はい	はい	はい
複製制御の拡張操作 1.3.18.0.2.12.16	この操作は、サブライヤーによる即時の複製、複製の中断、複製の再開のいずれかを適用するときに使用します。この操作は、複製の合意に対する更新をクライアントが許可されている場合にのみ許可されます。	いいえ	はい	いいえ	いいえ
キュー制御の拡張操作 1.3.18.0.2.12.17	この操作では、指定の合意の項目に「複製済み」とマークが付けられます。この操作は、複製の合意に対する更新をクライアントが許可されている場合にのみ許可されます。	いいえ	はい	いいえ	いいえ
DN 正規化の拡張操作 1.3.18.0.2.12.30	1 つの DN または一連の DN の正規化を要求します。	はい	はい	いいえ	いいえ

表 45. 拡張操作の OID (続き)

短縮名および OID	説明	管理サーバーによるサポートの対象	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
				分割データなし	分割データあり
動的サーバー・トレースの拡張操作 1.3.18.0.2.12.40	IBM Security Directory Server でのトレースを活動化または非活動化します。	いいえ	はい	はい	はい
動的更新要求の拡張操作 1.3.18.0.2.12.28	IBM Security Directory Server のサーバー構成の更新を要求します。	いいえ	はい	はい	はい
有効パスワード・ポリシー拡張操作 1.3.18.0.2.12.75	ユーザーまたはグループの有効なパスワード・ポリシーを照会する場合に使用します。	いいえ	はい	いいえ	いいえ
トランザクション終了の拡張操作 1.3.18.0.2.12.6	トランザクション・コンテキストを終了させます (コミット/ロールバック)。	いいえ	はい	はい	はい
イベント通知の登録要求の拡張操作 1.3.18.0.2.12.1	イベント通知の登録を要求します。	いいえ	はい	いいえ	いいえ
イベント通知の登録抹消要求の拡張操作 1.3.18.0.2.12.3	イベント登録要求を使用して登録したイベントの登録を抹消します。	いいえ	はい	いいえ	いいえ
ファイル取得拡張操作 1.3.18.0.2.12.73	サーバー上の特定のファイルのコンテンツを返します。	いいえ	はい	はい	はい
行取得の拡張操作 1.3.18.0.2.12.22	ログ・ファイルからの行の取り込みを要求します。	はい	はい	はい	はい
行数取得の拡張操作 1.3.18.0.2.12.24	ログ・ファイル行数を要求します。	はい	はい	はい	はい
グループ評価拡張操作 1.3.18.0.2.12.50	所定のユーザーが属するすべてのグループを要求します。	いいえ	はい	いいえ	いいえ
接続強制終了の拡張操作 1.3.18.0.2.12.35	サーバーの接続の強制終了を要求します。この要求は、すべての接続を強制終了するものでも、バインド済み DN、IP、特定の IP からバインドされた DN のいずれかによる接続を強制終了するものでもかまいません。	いいえ	はい	はい	はい
LDAP トレース機能の拡張操作 1.3.18.0.2.12.41	この拡張操作を使用すると、リモート側で管理サーバーを使用して LDAP トレース機能を制御できます。	はい	はい	はい	はい
項目検出拡張操作 1.3.18.0.2.12.71	この拡張操作は、特定の組の項目 DN についてバックエンド・サーバーの詳細を抽出し、それをクライアントに出力する場合に使用します。	いいえ	いいえ	はい	はい
LogMgmtControl 拡張操作 1.3.18.0.2.12.70	LogMgmtControl 拡張操作は、サーバー上で動作している IBM Security Directory Server インスタンスのログ管理の開始、停止、およびステータスの照会を行う場合に使用します。	はい	はい	はい	はい
オンライン・バックアップ拡張操作 1.3.18.0.2.12.74	ディレクトリー・サーバー・インスタンスの DB2 データベースのオンライン・バックアップを実行します。	いいえ	はい	いいえ	いいえ
パスワード・ポリシー・バインド初期化および検証拡張操作 1.3.18.0.2.12.79	パスワード・ポリシー・バインド初期化および検証拡張操作では、指定したユーザーについてパスワード・ポリシーのバインドの初期化および検証を実行します。	いいえ	はい	いいえ	いいえ
パスワード・ポリシー・バインド・ファイナライズおよび検証拡張操作 1.3.18.0.2.12.80	パスワード・ポリシー・バインド・ファイナライズおよび検証拡張操作では、指定したユーザーについてパスワード・ポリシーのバインド後の処理を実行します。	いいえ	はい	いいえ	いいえ
トランザクション準備拡張操作 1.3.18.0.2.12.64	トランザクション準備拡張操作を使用すると、クライアントは、トランザクションで送信した操作の処理を開始するようサーバーに要求します。	いいえ	はい	はい	はい

表 45. 拡張操作の OID (続き)

短縮名および OID	説明	管理サーバーによるサポートの対象	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
				分割データなし	分割データあり
プロキシ・バックエンド・サーバー役割再開拡張操作 1.3.18.0.2.12.65	この拡張操作を使用すると、プロキシ・サーバーがバックエンド・サーバーの構成済みの役割を分散ディレクトリー環境で再開できます。	いいえ	いいえ	はい	はい
複製コンテキストの静止または静止解除の拡張操作 1.3.18.0.2.12.19	この操作では、クライアントの更新を受け入れない (またはこの状態を終了する) 状態にサブツリーが書き込まれます。ただし、サーバー管理制御が存在する、ディレクトリー管理者として認証されたクライアントからの更新は除きます。	いいえ	はい	いいえ	いいえ
複製エラー・ログの拡張操作 1.3.18.0.2.12.56	複製エラー・ログの保守。	いいえ	はい	いいえ	いいえ
複製トポロジーの拡張操作 1.3.18.0.2.12.54	所定の複製コンテキストの下の、複製トポロジー関連の項目の複製をトリガーします。	いいえ	はい	いいえ	いいえ
ServerBackupRestore 拡張操作 1.3.18.0.2.12.81	ディレクトリー・サーバーのデータおよび構成ファイルをバックアップするか、ディレクトリー・サーバーのデータおよび構成を既存のバックアップから復元するために、管理サーバーに要求を出します。	はい	はい	いいえ	いいえ
サーバーの始動、停止の拡張操作 1.3.18.0.2.12.26	LDAP サーバーの始動、停止、または再始動を要求します。	はい	はい	はい	はい
TLS 始動の拡張操作 1.3.6.1.4.1.1466.20037	Transport Layer Security の始動を要求します。	はい	はい	はい	はい
固有属性の拡張操作 1.3.18.0.2.12.44	固有属性拡張操作を実行すると、特定の属性に関するすべての非固有 (重複) 値のリストが表示されます。	いいえ	はい	いいえ	いいえ
構成更新の拡張操作 1.3.18.0.2.12.28	IBM Security Directory Server および Security Directory Proxy Server のサーバー構成の更新を要求します。	はい	はい	はい	はい
ユーザー・タイプの拡張操作 1.3.18.0.2.12.37	バインドされているユーザーのユーザー・タイプの取得を要求します。	はい	はい	はい	はい

コントロールの OID

以下の表に、コントロールの OID を示します。

表 46. コントロールの OID

短縮名および OID	説明	管理サーバーによるサポートの対象	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
				分割データなし	分割データあり
AES バインドのコントロール 1.3.18.0.2.10.28	このコントロールにより、IBM Security Directory Server は、AES で暗号化したパスワードを使用してコンシューマー・サーバーに更新を送信できます。	いいえ	はい	いいえ	いいえ
監査のコントロール 1.3.18.0.2.10.22	コントロールは、一連の uniqueid ストリングおよびソース ip ストリングをサーバーに送信します。サーバーはこのコントロールを受け取ると、この操作の監査レコードにある uniqueid および sourceip のリストを監査します。	はい	はい	はい	はい
複製不可のコントロール 1.3.18.0.2.10.23	このコントロールは更新操作 (追加、削除、変更、modDn、modRdn) で指定できます。	いいえ	はい	いいえ	いいえ
グループ許可のコントロール 1.3.18.0.2.10.21	このコントロールは、ユーザーが属するグループのリストを送信します。	いいえ	はい	いいえ	いいえ

表 46. コントロールの OID (続き)

短縮名および OID	説明	管理サーバーによるサポートの対象	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
				分割データなし	分割データあり
LDAP 削除操作のタイム・スタンプ・コントロール 1.3.18.0.2.10.32	このコントロールは、変更済みのタイム・スタンプ値を削除操作時にレプリカに送る場合に使用します。	いいえ	はい	いいえ	いいえ
属性値制御の制限数 1.3.18.0.2.10.30	このコントロールを使用すると、検索操作時に 1 つの項目に返される属性値の数が制限されます。	いいえ	はい	はい	はい
DSAIT 管理のコントロール 2.16.840.1.113730.3.4.2	「ref」属性を持つ項目が通常の項目として処理され、クライアントはこれらの項目を読み取ったり変更したりできるようになります。 * IBM Security Directory Proxy Server (分割データなし) では、このコントロールが要求に含まれていない場合でも、プロキシ・サーバーは「DSAIT 制御の管理」コントロールを必ずバックエンド・サーバーに送信します。	いいえ	はい	はい (*)	いいえ
グループ変更限定のコントロール 1.3.18.0.2.10.25	このコントロールを DN 削除要求または DN 変更要求に付加すると、サーバーは、削除または名前変更要求でグループ参照整合性処理しか行わず、項目自体は実際に削除または名前変更されません。DN 削除要求または DN 変更要求で指定されている項目がサーバーに存在する必要はありません。	いいえ	はい	いいえ	いいえ
複製競合の無解決のコントロール 1.3.18.0.2.10.27	このコントロールが存在すると、レプリカ・サーバーは、項目の複製競合の解決を試行せずにその複製項目を受け入れます。	いいえ	はい	いいえ	いいえ
グループの参照整合性省略のコントロール 1.3.18.0.2.10.26	削除要求または modrdn 要求で、グループの参照整合性処理を省略します。削除操作または名前変更操作時に項目が存在する場合は、その項目がディレクトリーから削除されるかディレクトリー内で名前変更されますが、項目がメンバーになっているグループ内では、項目のメンバーシップが削除されたり名前変更されたりすることはありません。	いいえ	はい	いいえ	いいえ
検索結果のページングのコントロール 1.2.840.1.113556.1.4.319	このコントロールを使用すると、検索要求から戻されるデータの量を管理できます。	いいえ	はい	はい	はい
パスワード・ポリシー要求のコントロール 1.3.6.1.4.1.42.2.27.8.5.1	パスワード・ポリシー要求または応答	はい	はい	はい	はい
永続検索のコントロール 2.16.840.1.113730.3.4.3	このコントロールは、LDAP サーバーでの変更の通知を受信する手段をクライアントに提供します。	いいえ	はい	いいえ	いいえ
プロキシ許可のコントロール 2.16.840.1.113730.3.4.18	プロキシ許可制御により、バインド済みユーザーには、別のユーザーの ID に対するアサーションが可能になります。サーバーは、このアサーションされた ID を使用して、操作の ACL を評価します。	いいえ	はい	いいえ	いいえ
項目のリフレッシュのコントロール 1.3.18.0.2.10.24	ターゲット・サーバーは、複製された変更操作中に競合を検出すると、このコントロールを返します。	いいえ	はい	いいえ	いいえ
複製サブライヤーのバインドのコントロール 1.3.18.0.2.10.18	サブライヤーがゲートウェイ・サーバーの場合、このコントロールはサブライヤーによって追加されます。	いいえ	はい	いいえ	いいえ
削除済みオブジェクトの返却コントロール 1.3.18.0.2.10.33	このコントロールをヌル・ベースの検索要求に組み込むと、属性 isDeleted が TRUE に設定されている項目を含む、データベース内のすべての項目が返されます。	いいえ	はい	いいえ	いいえ

表 46. コントロールの OID (続き)

短縮名および OID	説明	管理サーバーによるサポートの対象	IBM Security Directory Base Server v6.3 によるサポートの対象	IBM Security Directory Proxy Server v6.3 によるサポートの対象	
				分割データなし	分割データあり
サーバー管理のコントロール 1.3.18.0.2.10.15	通常は操作が拒否される条件下 (サーバーが静止状態、読み取り専用レプリカなど) で、管理者による更新操作を許可します。 * IBM Security Directory Proxy Server では、このコントロールがサポートされるのはバインド操作の場合に限られます。	はい	はい	はい (*)	はい (*)
検索結果のソートのコントロール 1.2.840.1.113556.1.4.473	このコントロールを使用すると、クライアントは、一連の基準でソートした検索結果を受け取ることができます。この場合、各基準はソート・キーを表しています。	いいえ	はい	いいえ	いいえ
サブツリー削除のコントロール 1.2.840.1.113556.1.4.805	このコントロールは削除要求に接続して、指定の項目およびすべての下位項目を削除することを示します。	いいえ	はい	いいえ	いいえ
トランザクションのコントロール 1.3.18.0.2.10.5	トランザクション・コンテキストの一部として操作をマークします。 * IBM Security Directory Proxy Server では、トランザクションがサポートされるのは、すべての更新が単一区画をターゲットにしている場合に限られます。	いいえ	はい	はい (*)	はい (*)
仮想リスト・ビューのコントロール 2.16.840.1.113730.3.4.9	このコントロールでは、通常の LDAP 検索操作が拡張されます。また、このコントロールにはサーバー・サイドのソート・コントロールが組み込まれています。	いいえ	はい	いいえ	いいえ

付録 C. LDAP データ交換フォーマット (LDIF)

ここに示す情報により、`idsldapmodify`、`idsldapsearch`、および `idsldapadd` の各ユーティリティーで使用される LDAP データ交換フォーマット (LDIF) について説明します。

ここで記述する LDIF は、IBM Security Directory Server で提供されるサーバー・ユーティリティーにおいてもサポートされます。

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。LDIF 項目の基本フォームは以下のとおりです。

```
dn: <distinguished name>
<attrtype> : <attrvalue>
<attrtype> : <attrvalue>
...
```

行を続けるには、次の行を単一のスペースまたはタブ文字で始めます。例を以下に示します。

```
dn: cn=John E Doe, o=University of Higher Learning, c=US
```

複数の属性値は、別々の行に指定します。例を以下に示します。

```
cn: John E Doe
cn: John Doe
```

<attrvalue> が非 US-ASCII 文字を含んでいるか、スペースあるいはコロン「:」で始まる場合、<attrtype> には二重コロンが続き、値は base-64 表記でエンコードされます。例えば、スペースで始まる値は、以下のようにエンコードされます。

```
cn:: IGJlZ21lucyB3aXRoIGEgc3BhY2U=
```

同じ LDIF ファイル内に複数の項目がある場合は、ブランク行で区切ります。ブランク行を複数指定すると、論理的なファイルの終わりから見なされます。

LDIF の例

ここでは、3 つの項目を含む LDIF ファイルの例を示します。

```
dn: cn=John E Doe, o=University of Higher Learning, c=US
cn: John E Doe
cn: John Doe
objectclass: person
sn: Doe

dn: cn=Bjorn L Doe, o=University of Higher Learning, c=US
cn: Bjorn L Doe
cn: Bjorn Doe
objectclass: person
sn: Doe

dn: cn=Jennifer K. Doe, o=University of Higher Learning, c=US
cn: Jennifer K. Doe
cn: Jennifer Doe
objectclass: person
sn: Doe
jpegPhoto:: /9j/4AAQSkZJRgABAAAAQABAAD/2wBDABALD
A4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQ
ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2ZP/2wBDARESEhgVG
...
```

Jennifer Doe の項目の `jpegPhoto` は、base-64 を使用してエンコードされます。base-64 フォーマットでは、テキスト属性値も指定できます。ただし、その場合は、

プロトコルのワイヤー・フォーマットのコード・ページの範囲内で base-64 エンコードを行う必要があります (つまり、LDAP V2 の場合は IA5 文字セット、LDAP V3 の場合は UTF-8 エンコードになります)。

バージョン 1 LDIF サポート

ここに示す情報およびリンクにより、バージョン 1 LDIF サポートの詳細を知ることができます。

クライアント・ユーティリティーの `idsldapmodify` と `idsldapadd` が、最新バージョンの LDIF を認識するように拡張されました (最新バージョンの LDIF は、ファイルの先頭に "version: 1" タグが付いています)。非常に制限された US-ASCII しかサポートされない最初のバージョンの LDIF とは異なり、新しいバージョンの LDIF では、UTF-8 表記の属性値がサポートされます。

ただし、UTF-8 の値を含む LDIF ファイルを手作業で作成するのは困難です。この作業を簡素化するために、LDIF 形式を拡張した `charset` がサポートされています。この拡張機能では、IANA 文字セット名を LDIF ファイルのヘッダーに (バージョン番号とともに) 指定することができます。一連の IANA 文字セットは、制限付きでサポートされます。各オペレーティング・システム・プラットフォームでサポートされる特定の `charset` の値については、643 ページの『プラットフォームでサポートされている IANA 文字セット』を参照してください。

バージョン 1 LDIF 形式では、ファイル URL もサポートされます。これにより、ファイル指定をより柔軟に定義できます。ファイル URL は、以下の形式で指定します。

```
attribute:< file:///path(where path syntax depends on platform)
```

有効なファイル Web アドレスの例を以下に示します。

```
jpegphoto:< file:///d:\temp\photos\myphoto.jpg(DOS/Windows style paths)
jpegphoto:< file:///etc/temp/photos/myphoto.jpg
              (UNIX または Linux スタイルのパス)
```

注: IBM Security Directory Server ユーティリティーでは、バージョンの指定にかかわらず、新しいファイル URL 指定と古いスタイル ("`jpegphoto: /etc/temp/myphoto`" など) の両方がサポートされます。つまり、LDIF ファイルにバージョン・タグを追加しなくても、新しいファイル URL フォーマットを使用できます。

バージョン 1 LDIF の例

以下の例に示すように、オプションの `charset` タグを使用すると、ユーティリティーによって、指定された文字セットから UTF-8 に自動的に変換されます。

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, o=University of New Mexico, c=US
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcVhZGVyIH1vd
title: Associate Dean
title: [title in Spanish]
jpegPhoto:< file:///usr/local/photos/jgriego.jpg
```

この例では、属性名と単一コロンの続く値はすべて、ISO-8859-1 文字セットから UTF-8 に変換されます。属性名と二重コロンの後に続く値 (`description::`

V2hhdCBhIGNhcm... など) は、base-64 でエンコードされている必要があります。この値は、バイナリーまたは UTF-8 文字ストリングに変換されます。ファイルから読み取られる値 (例えば、上記の例の Web アドレスで指定された jpegPhoto 属性) も、バイナリーか UTF-8 に変換されます。これらの値に関しては、指定された charset から UTF-8 への変換は行われません。

以下に示す、charset タグを持たない LDIF ファイルの例では、内容は、UTF-8、base-64 エンコード UTF-8、または base-64 エンコード・バイナリー・データの形式に変換されます。

```
# 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=Linda Carlesberg, ou=Austin, o=sample
```

以前のリリースの IBM Security Directory Server の場合のように、「version: 1」ヘッダー情報を付けずに、これと同じファイルを使用することもできます。

```
# 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
```

注: base-64 フォーマットでは、テキスト属性値を指定できます。

プラットフォームでサポートされている IANA 文字セット

以下の表では、バージョン 1 LDIF ファイルの charset タグに指定可能な一連の IANA 定義文字セットを、プラットフォーム別に示しています。

一番左の列の値は、charset タグに指定可能なテキスト・ストリングを示しています。「X」は、指定した charset から UTF-8 への変換が該当するプラットフォームでサポートされ、LDIF ファイルのストリングの内容がすべてその charset で表現されることを示します。「N/A」は、そのプラットフォームで変換がサポートされないことを示します。

ストリングの内容は、属性名と単一コロンの続くものはすべて属性値であるものとして定義されます。

IANA に登録された文字セットの詳細については、『IANA 文字セット』を参照してください。以下に掲載されています。

<http://www.iana.org/assignments/character-sets>

表 47. IANA 定義の文字セット

文字	ロケール					DB2 コード・ページ	
	HP-UX	Linux、 Linux_390	NT	AIX	Solaris	UNIX	NT
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
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)						

* Solaris 7 ではサポートされています。

注:

1. 新しい中国語の文字セット規格 (GB18030) は、www.sun.com および www.microsoft.com で入手できる該当のパッチを使用することによってサポートされます。
2. Windows 2000 オペレーティング・システムでは、環境変数 `zhCNGB18030=TRUE` を設定する必要があります。

付録 D. 33 番から 126 番までの ASCII 文字

33 番から 126 番の ASCII 文字を次の表に示します。これらの文字は、暗号化シード・ストリングで使用できます。

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	& アンパーサンド
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
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				

付録 E. IPv6 サポート

ここに示す情報により、IPv6 サポートの詳細を知ることができます。

インターネット・プロトコル・バージョン 6 (IPv6) は、現行バージョンのインターネット・プロトコルである IP バージョン 4 (IPv4) を置き換えるために IETF によって設計されたプロトコルです。IPv6 では、使用可能な IPv4 アドレスの数が限られているなど、IPv4 に存在する多くの問題を解決しました。IPv6 では、IPv4 と比較してアドレスの桁数が多い (128 ビット対 32 ビット) ため、TCP アプリケーション・レベルで影響があります。ルーティングやネットワークの自動構成の領域にも改良点があります。IPv4 は IPv6 によって徐々に置き換えていくものと予想されています。

IBM Security Directory Server 6.0 以降のバージョンをサポートしているすべてのサーバーおよびクライアントは、IPv4 ノードだけでなく IPv6 ノードのサポートにも対応しています。以下に、IPv4 および IPv6 の LDAP URL のフォーマットの例を示します。

注: URL で *:portnumber* を指定しないと、デフォルトのポート (非 SSL の場合 389、SSL の場合 636) が使用されます。

- URL にリテラル IPv4 アドレスを使用する場合、フォーマットは *x.x.x.x:port* となります。以下の例は、ポート 80 を listen する、非 SSL 通信を行う LDAP サーバーの URL 形式の名前です。

– ldap://9.53.90.21:80

以下の例は、デフォルト・ポート 636 を listen する、SSL 通信を行う LDAP サーバーの URL 形式の名前です。

– ldaps://9.53.90.21

- RFC 2732 に準拠するには、URL でのリテラル IPv6 アドレスを [および] という記号で囲む必要があります。以下の例は非 SSL 通信を行う LDAP サーバーの URL 形式の名前で、それぞれポート 80 とデフォルトのポート 389 を listen します。

– ldap://[107:0:0:0:200:7051]:80

– ldap://[::ffff:9.53.96.21]

以下の例は SSL 通信を行う LDAP サーバーの URL 形式の名前で、それぞれポート 80 とデフォルトのポート 636 を listen します。

– ldaps://[107:0:0:0:200:7051]:80

– ldaps://[::ffff:9.53.96.21]

注:

1. IPv6 非対応のディレクトリー・サーバーを併用している環境で IPv6 URL フォーマットを使用すると、IPv6 URL フォーマットは、IPv6 非対応のクライアントおよびサーバーには認識されません。例:
 - IPv6 非対応のクライアントが IPv6 フォーマットの URL アドレスを受け取っても、URL アドレスが示す先を参照できません。

- IPv6 非対応のコンシューマー・サーバーが、サプライヤーの URL 情報を IPv6 フォーマットで受け取っても、複製は機能しません。
2. Linux システムには、リンク・ローカル IP アドレスを解決するためのインターフェース ID が必要です。getaddrinfo または他のインターフェース変換ルーチンが機能しますが、解決済みの IP アドレスは connect() 関数では処理できません。以下のフォーマットを使用して、IP アドレスとインターフェース ID を指定してください。

```
ldap://[xxxx:xxxx:xxxx:xxxx:xxxx%InterfaceID]
```

scope:local を使用したリンク・ローカル IPv6 アドレスは、Linux システムでは処理できません。Linux システムの IPv6 アドレスで、IBM Security Directory Server バージョン 6.0 以降がサポートしているのは scope:global のみです。

付録 F. Simple Network Management Protocol エージェント

ここに示す情報により、Simple Network Management Protocol エージェントの詳細を知ることができます。

Simple Network Management Protocol (SNMP) エージェントは、ディレクトリー・サーバーの状態をモニターするための要求に対応して、ネットワーク管理ステーションに対してトラップを送信します。IBM Security Directory Integrator アセンブリー・ラインを SNMP エージェントとともに使用することで、ディレクトリー・サーバーのパフォーマンス情報および正常性情報をレポートしたりモニターしたりできます。Security Directory Integrator アセンブリー・ラインは、モニター検索、ルート DSE 検索、およびモニター対象のディレクトリー・サーバーのシステム情報といった、パフォーマンス情報および正常性情報を収集してレポートします。ディレクトリー・サーバーのパフォーマンス情報は定期的にログに記録され、Common Base Event (CBE) に合わせて定義されている Extensible Markup Language (XML) 形式で利用できるようになります。

注:

- SNMP エージェントを使用するには、IBM Security Directory Integrator 7.1 をインストールしておく必要があります。

また、ディレクトリー・ユーザーを追加し、DIT (Data Information Tree) データに対するこのユーザーのアクセス権を否認するための ACL をディレクトリーのサブツックスに配置する必要があります。このユーザーは、モニター検索のみを実行するために作成され、モニター対象のすべてのインスタンスに存在する必要があります。

IBM Security Directory Server をモニターするには、Simple Network Management Protocol (SNMP) エージェントのプロパティー・ファイルおよび構成ファイルを変更する必要があります。

各ディレクトリー・サーバー・インスタンスは、`idssnmp.properties` ファイルに個別の項目があります。構成の詳細は、`idssnmp` ツールによってモニターされるディレクトリー・サーバー・インスタンスごとに固有になります。このため、`idssnmp` ツールで複数のディレクトリー・サーバー・インスタンスをモニターできます。`idssnmp` ツールのインスタンスを 1 つ起動することで、`idssnmp.properties` ファイルに記述されているすべてのディレクトリー・サーバー・インスタンスをモニターできます。

`idssnmp.properties` ファイルは、いったん `idssnmp` エージェントを始動させると、デフォルトでは暗号化されます。このファイルは、`<TDSinstall_directory>%idstools%snmp` ディレクトリーに配置されています。`idssnmp.properties` ファイルには、以下の設定が含まれています。

```
server: <IP_address>
port: <port_number>
isSSL: True/False
ldapbindDN: <bind_DN>
bindDNpwd: <bind_pwd>
systemuser: <user_ID>
systemuserpwd: <user_pwd>
```

```
filterCacheActive: True/False
filterCacheThreshold: <Threshold Value in percentage>
pendingRequestsActive: True/False
pendingRequestsThreshold: <Threshold Value>
pendingRequestsSinceLastIntervalActive: True/False
pendingRequestsSinceLastIntervalThreshold: <Threshold Value>
activeConnectionActive: True/False
activeConnectionThreshold: <Threshold Value>
memoryUtilizationActive: True/False
memoryUtilizationThreshold: <Threshold Value in kilobytes>
cpuUtilizationActive: True/False
cpuUtilizationThreshold: <Threshold Value in percentage>
diskSpaceUtilizationActive: True/False
diskSpaceUtilizationThreshold: <Threshold Value in kilobytes>
replicationPendingChangeCountActive: True/False
replicationPendingChangeCountThreshold: <Threshold Value>
replicationStatusActive: True/False
trapForMessageId-<log_type>: <GLP...>
```

説明:

サーバー

モニターされる LDAP サーバーの IP アドレスを表します。

ポート モニターされる LDAP サーバーの実行先ポートを表します。

isSSL LDAP インスタンスと SNMP エージェント間の通信を SSL で暗号化するかどうかを指定します。

ldapbindDN

バインド DN を表します。

bindDNpwd

バインド・パスワードを表します。

systemuser

システム・ユーザー ID を表します。

systemuserpwd

システム・ユーザー・パスワードを表します。

filterCacheActive

TRUE に設定した場合、検索フィルター・キャッシュの使用率 (パーセント) がしきい値の制限を超えると、トラップ・アラートが生成されます。

filterCacheThreshold

しきい値をパーセント値で指定します。

pendingRequestsActive

TRUE に設定した場合、要求された操作数と完了した操作数との差 (未処理要求) がしきい値の制限を超えると、トラップ・アラートが生成されます。

pendingRequestsThreshold

しきい値を指定します。

pendingRequestsSinceLastIntervalActive

TRUE に設定した場合、最後の間隔以降の未処理要求の数がしきい値の制限を超えると、トラップ・アラートが生成されます。

pendingRequestsSinceLastIntervalThreshold

しきい値を指定します。

activeConnectionActive

TRUE に設定した場合、アクティブな接続の数がしきい値の制限を超えると、トラップ・アラートが生成されます。

activeConnectionThreshold

しきい値を指定します。

memoryUtilizationActive

TRUE に設定した場合、システム・メモリー使用率の最大値がしきい値の制限を超えると、トラップ・アラートが生成されます。

memoryUtilizationThreshold

しきい値をキロバイト単位で指定します。

cpuUtilizationActive

TRUE に設定した場合、CPU 使用率の最大値がしきい値の制限を超えると、トラップ・アラートが生成されます。これを適用できるのは、Windows 以外のオペレーティング・システムの場合に限られます。

cpuUtilizationThreshold

しきい値をパーセント値で指定します。

diskSpaceUtilizationActive

TRUE に設定した場合、DB2 データベースが格納されているディレクトリによるディスク・スペースの使用率がしきい値の制限を超えると、トラップ・アラートが生成されます。

diskSpaceUtilizationThreshold

しきい値をキロバイト単位で指定します。

replicationPendingChangeCountActive

TRUE に設定した場合、複製キューが事前定義のしきい値に到達する (例えば、キューの項目数が 10000 を超える) と、トラップ・アラートが生成されます。

replicationPendingChangeCountThreshold

しきい値を指定します。

replicationStatusActive

TRUE に設定した場合、複製の現在の状態が非互換、サーバーがダウンしている、認証に失敗した、またはダウン・レベルのサーバーはサポートされていない、のいずれかになると、トラップ・アラートが生成されます。

trapForMessageId

メッセージ ID のリストを表します。このリストは、メッセージ ID が「,」で区切られたリストになります。LDAP 拡張操作で要求されたサーバー・ログ内に、一致するメッセージ ID があると、SNMP トラップが生成されます。ログ・タイプは、LDAP 拡張操作で要求されたログのタイプを記述したものです。各ログ・タイプは個別に記述する必要があります。以下に例を示します。

- trapForMessageId-slapd:
- trapForMessageId-audit:
- trapForMessageId-ibmdiradm:

ログ・ファイルで生成されたすべてのメッセージに対してトラップを送信する場合は、以下のいずれかのオプションを指定できます。

- TRAP_MAX – ログ・ファイルに出現するすべてのメッセージ (情報、警告、およびエラー) に対してトラップが送信されます。

- TRAP_MID – ログ・ファイルに出現するすべての警告メッセージおよびエラー・メッセージに対してのみトラップが送信されます。
- TRAP_MIN – ログ・ファイルに出現するすべてのエラー・メッセージに対してのみトラップが送信されます。

slapd、audit、および ibmdiradm の各ログ・ファイルに対して設定できるトラップの例を以下に示します。

```
trapForMessageId-slapd: TRAP_MID
trapForMessageId-audit: TRAP_MAX
trapForMessageId-ibmdiradm: TRAP_MID
```

注:

- TRAP_MIN および TRAP_MID は、trapForMessageId-audit に対しては有効な値ではありません。監査ログの内容は情報メッセージのみであることがその理由です。
- idssnmp ツールによって送信されるトラップには、OID 1.3.6.1.4.1.2.6.199.1.1.7 が含まれます。この OID には、イベントに対応するインスタンスの名前が保持されます。

構成ファイル idssnmp.conf は、標準 SNMP フォーマットです。つまり、特定のキーワードをスペースで区切って記載します。この構成ファイルには、SNMP エージェントを実行するポート番号、少なくとも 1 つの IP アドレスまたはホスト名、接続側がトラップを送るネットワーク管理システム (NMS) の IP アドレス、および SNMP エージェントが応答するコミュニティーを記載します。このファイルは、`<TDSinstall_directory>%idstools%snmp` ディレクトリーに配置されています。

1. IBM Security Directory Server SNMP エージェントの構成ファイルのポート番号を編集します。SNMP エージェントは、IBM Security Directory Server をモニターします。ディレクトリー・サーバー以外のものをモニターする場合は、IBM Security Directory Server の SNMP エージェントを、標準ポート以外のポートで実行する必要があります。この非標準ポートは、他のアプリケーションのエージェントが使用するポートと競合しないものを選択する必要があります。

Port 161

SNMP エージェントをポート 161 で実行する場合は、上記のように指定します。複数のポートを指定しても、最初の行のポートだけが読み取られ、他は無視されます。

2. トラップを適切に受信するためには、トラップを受信する NMS の IP アドレス (デフォルト値は 127.0.0.1)、NMS のポート番号、および NMS がエージェントからの受信に使用するコミュニティー・ストリングを追加し、SNMP 構成ファイルのキーワード Trap を含む行を編集します。トラップを受信するマシンを複数指定する場合は、この行を複数指定します。例:

```
Trap 5.4.3.2 162 public
```

この例では、生成されたトラップは、IP アドレス 5.4.3.2 のマシンの、コミュニティー・ストリング public を使用して、ポート 162 に送信されます。

3. ポーリング間隔を秒単位で指定します。指定した秒数が経過すると、エージェントはサーバーをポーリングし、それらのステータスを検出します。

Poll 600

この例では、600 秒間隔、つまり 10 分間隔でエージェントはサーバーをチェックします。

4. エージェントへのアクセスを制限する場合は、オプションのコミュニティ・ストリングを指定します。コミュニティを指定する場合、ストリングを提供する必要があります。例えば、

```
Community dirServer
```

コミュニティ・ストリング `dirServer` を提供するマシンは、データにアクセスできます。コミュニティ・ストリングを指定しないと、アクセス権限は制限されません。さらにアクセスを制限する場合は、コミュニティ・ストリング行に IP アドレスなど他のトークンを指定します。要求を発信するマシンは、このトークンを所有している必要があります。

```
Community dirServer 1.2.3.4
```

IP アドレスを指定しない場合、コミュニティ・ストリングを提供するマシンであればどのようなマシンでもデータにアクセスできます。追加のアクセス制限が必要な場合は、サポートされている読み取り専用アクセス権 (`readOnly`) をコミュニティの要素および、最終的には、サブツリーのビューに追加します。データは暗黙的に読み取り専用になる点、および SNMP 構成ファイル標準に準拠するためには、読み取り専用権限を使用する必要があるという点に注意してください。コミュニティを指定する場合は、ストリングが必要です。IP アドレス、アクセス権、およびビューはオプションですが、これらの制限は、基本的にはこの順番で指定する必要があります。オプションとして IP アドレス、または IP アドレスとアクセス権は指定できますが、アクセス権とビューを指定して IP アドレスは指定しないということはありません。

以下は、最も制限の厳しい例です。また、トークンを正しい順番で指定していません。

```
Community dirServer 1.2.3.4 readOnly 1.5.4.3.2.1
```

この例の場合、要求を送信する NMS は、コミュニティ・ストリングとして "`dirServer`" を提供する必要があります。また、要求を発信するマシンの IP アドレスは `1.2.3.4` でなければなりません。さらにはコミュニティ内のすべての要素は読み取り専用で、ビューは `1.5.4.3.2.1` です。

注: 権限が制限されている状態で、複数のマシンが許可された NMS を実行して Directory SNMP エージェントの取得操作を実行する場合、コミュニティ行を複写する必要があります。

5. SNMP OID ツリーを分割する必要がある場合は、サブツリーのビューを指定します。

```
View 1.5.4.3.2.1
```

この例の場合、エージェントは、OID `1.5.4.3.2.1` の下のすべてのサブツリーを処理します。

注:

- 以下の MIB を NMS にロードします。

```
<TDSinstall_directory>%idstools%snmp%IBM-DIRECTORYSERVER-MIB
<TDSinstall_directory>%idstools%snmp%INET-ADDRESS-MIB
```

SNMP エージェントは、<TDSinstall_directory>%sbin ディレクトリーにある idssnmp スクリプトを実行することで始動できます。

IBM Security Directory Integrator のインストール方法および SSL のセットアップ方法について詳しくは、IBM Security Directory Integrator の資料の『構成』セクションを参照してください。

SNMP ロギング

以下に示すステップおよび追加情報を使用して、SNMP にログインできます。

デフォルトでは、idssnmp アプリケーションは、UNIX プラットフォームの場合はデータをファイル /var/idsldap/V6.2/idssnmp.log に、Windows プラットフォームの場合はデータをファイル <TDSinstall_directory>%var%idssnmp.log に記録します。

ツールのメインのログ・ファイル idssnmp.log に加えて、Security Directory Integrator が作成する 2 つのログ・ファイルがあります。

- ibmdi.log
- idssnmpinit.log

Security Directory Integrator アプリケーションは静的ロケーションにログを書き込むため、これらのファイルが作成されます。idssnmp ツールが初期化されたら、ログ・ステートメントのほとんどは idssnmp.log に書き込まれます。ibmdi.log ファイルおよび idssnmpinit.log ファイルは、以下のディレクトリーに書き込まれます。

- <TDSinstall_directory>/idstools/snmp/logs (UNIX)
- <TDSinstall_directory>%idstools%snmp%logs (Windows)

これらのディレクトリーが作成されていない場合、ログは現行作業ディレクトリーに格納されます。ibmdi.log および idssnmpinit.log は、ファイル・サイズを小さく保つために、idssnmp ツールが実行されるたびに上書きされます。

以下のコマンド行オプション:

```
-D DEBUG
```

を使用すると、idssnmp をデバッグできます。この場合のログには、エージェントの実行に関する、より詳細な情報が記録されます。

注: Security Directory Integrator アセンブリー・ラインは、ディレクトリー・サーバーのパフォーマンス情報を、Common Base Event (CBE) に合わせて定義されている XML 形式で定期的にログに記録します。

コマンド行の使用 – idssnmp

idssnmp には、以下のコマンド行オプションがあります。

- q このオプションを指定すると、ログ・メッセージが画面に表示されなくなります。これはオプション・パラメーターです。
- v idssnmp ツールのバージョン番号を表示します。これはオプション・パラメーターです。
- ? 使用方法を表示します。これはオプション・パラメーターです。

IBM Security Directory Integrator が失敗した場合は、以下のいずれかの終了コードが戻されます。

- 0** ユーザーが **-v** パラメーター (情報を表示して終了) を指定して IBM Security Directory Integrator を始動していたことを示します。
- 1**
 - ログ・ファイル (**-l** parameter) を開くことができません
 - 構成ファイルを開くことができません
 - 管理要求により停止しました
- 2** 自動実行の後、終了したことを示します。**-w** オプションを指定して IBM Security Directory Integrator を始動すると、IBM Security Directory Integrator は **-r** パラメーターで指定されている AssemblyLine を実行してから終了します。
- 9** ライセンスが有効期限切れ、または無効であることを示します。

付録 G. Active Directory との同期

注: IBM Security Directory Server バージョン 6.3.1 からは、Active Directory との同期ソリューションは推奨されません。

Active Directory との同期は、LDAPSync ソリューションによって置き換えられます。

Active Directory との同期は、Microsoft Active Directory と IBM Security Directory Server インスタンスとの間でユーザーおよびグループを同期させるためのツールです。同期は、Active Directory から IBM Security Directory Server への片方向のみです。ここに示す情報により、その詳細を知ることができます。

注: Active Directory と IBM Security Directory Server インスタンス間で IBM Security Directory Proxy サーバーを介してユーザーとグループを同期させる操作はサポートされません。

Active Directory との同期では、IBM Security Directory Integrator を使用してディレクトリーを同期します。IBM Security Directory Integrator をインストールしないと、Active Directory との同期は実行できません。IBM Security Integrator は、構成を実行する目的で使用し、IBM Security Directory Integrator 管理およびモニター・コンソールは、実行の開始、停止、再開、およびモニターを行う目的で使用します。IBM Security Directory Integrator をインストールしないと、Active Directory との同期は実行できません。

注:

1. Active Directory との同期機能および IBM Security Directory Integrator は、関連のディレクトリー・サーバー・インスタンスと同じコンピューターに導入する必要があります。
2. Active Directory との同期では、ユーザーとグループのみが同期されます。ディレクトリー内の他のオブジェクトは同期されません。
3. 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。
4. Active Directory からの複数の属性を IBM Security Directory Server の単一属性にマップすることはできません。
5. userPassword 属性をマッピングすることはできません。(ユーザー・パスワードのデータは、このソリューションとは同期しません)。
6. Active Directory との同期では、Active Directory の 1 つ以上のユーザー・コンテナからのユーザーおよびグループを Security Directory Server の単一 OU と同期させることができます。ただし、Active Directory の複数のユーザー・コンテナおよびグループ・コンテナを Security Directory Server の複数の OU に同期させることはありません。
7. 複数のユーザー・コンテナを指定して、これを Security Directory Server の単一の組織単位 (OU) と同期させることができます。

注: 複数のユーザー・コンテナが Security Directory Server の単一の組織単位 (OU) と同期するように指定するには、分離文字としてセミコロン (;) を使用します。(それ以外の文字は分離文字として使用できません。) セミコロン (;) 分離文字を使用する場合は、引数を引用符 (") で囲んでください。以下に例を示します。 "ou=SWUGroups,dc=adsync,dc=com;ou=STGGroups,dc=adsync,dc=com"

Active Directory の sAMAccountName 属性は、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・コンテナを単一の Security Directory Server OU に同期させても競合は発生しません。

8. このソリューションは、現時点では Active Directory への SSL 接続をサポートしていますが、IBM Security Directory Server への SSL 接続はサポートしていません。
9. 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、またはこれら両方を構成または変更した場合は、必ず Active Directory との同期を再構成してください。
10. Active Directory からのユーザー・コンテナ名またはグループ・コンテナ名を (Active Directory との同期の実行中に) 動的に変更した場合は、必ず Active Directory との同期を新しい名前でも再構成してください。再構成しないと、Active Directory との同期が実行されなくなります。
11. IBM Security Directory Server のユーザーとグループを Active Directory との同期以外の方法で変更すると、Active Directory との同期が正常に機能しないことがあります。
12. 同期は、Active Directory から IBM Security Directory Server への片方向のみです。
13. ユーザー項目属性のみが同期します。
14. ユーザーが Security Directory Server インスタンスのユーザーまたはグループを外部的に、つまり同期ソリューションの外部から変更した場合は、Active Directory から Security Directory Server への同期は保証できません。

Active Directory との同期を使用する場合の手順

IBM Security Directory Server および IBM Security Directory Integrator をインストールし、ディレクトリー・サーバー・インスタンスを作成して構成したら、以下の手順に従って Active Directory との同期を構成して使用します。

このタスクについて

手順

1. デフォルト・パス (UNIX ベースのシステムでは /opt/IBM/TDI/V7.1、Windows システムでは C:\Program Files\IBM\TDI\V7.1) にインストールしなかった IBM Security Directory Integrator のコピーを使用する場合は、IDS_LDAP_TDI_HOME 環境変数を IBM Security Directory Integrator V7.1 をインストールしたディレクトリーに設定する必要があります。注: (Windows システムでは、このパスにスペースが含まれていると、Active Directory との同期が正常に動作しません。この環境変数にはスペースも引用符も含まないパスを設定するか、あるいはパスを指定するときは短縮名を使用するようにしてください。

2. オプションで、サンプルの `users.ldif` ファイルおよび `groups.ldif` ファイルを Active Directory Server にロードします。Active Directory Server の資料を参照してください。
3. IBM Security Directory Server 構成ツールまたは `idsadscfg` コマンドを使用して、Active Directory との同期を構成します。この結果、`adsync_private.prop` ファイルおよび `adsync_public.prop` ファイルが生成されます。詳しくは、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。
4. 必要に応じて `adsync_public.prop` ファイルを変更し、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。詳しくは、『Active Directory との同期で使用されるファイル』を参照してください。SSL を使用している場合の詳細については、665 ページの『Active Directory への SSL 接続を使用するための Active Directory との同期の構成』を参照してください。
5. `idsadsrun` コマンドを使用して、Active Directory との同期を開始します。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、あるいはリアルタイム同期のみ開始するかを尋ねられます。詳しくは、665 ページの『Active Directory との同期の実行』を参照してください。
Active Directory 項目に対する変更は、変更を識別する Active Directory 同期ツールによって読み取られます。
Active Directory との同期では、IBM Security Directory Server に対するすべての変更が同期化されます。IBM Security Directory Integrator 管理およびモニター・コンソールを使用すると、より詳細な管理およびモニターができます。

タスクの結果

注:

- Active Directory との同期を構成するには、構成ツールまたは `idsadscfg` コマンドを使用します。
- 構成ツールによる Active Directory との同期機能の構成については、IBM Security Directory Server の資料の『インストールと構成』セクションを参照してください。
- `idsadscfg` コマンドによる Active Directory との同期機能の構成については、IBM Security Directory Server の資料の『コマンド解説書』セクションを参照してください。

Active Directory との同期で使用されるファイル

Active Directory との同期で使用されるファイルのリストは、以下で確認できます。

`adsync.xml`

`adsync.xml` ファイルは構成ファイルです。このファイルには、IBM Security Directory Server と Active Directory の同期を実行するために必要な、事前構成済みのアセンブリー・ラインおよびコネクターが記述されています。このファイルの最初の作成時には、IBM Security Directory Integrator 構成エディター・ユーティリティーが使用されています。`adsync.xml` ファイルは、1 台のコンピューターに 1 つのみ存在します。このファイルは変更できません。カスタマイズを行う場合は、それぞれの IBM Security Directory Server インスタンスを構成して、特定のディレクトリー・サーバー・インスタンス

に対して Active Directory との同期機能がどのように動作するかを定義するプロパティ・ファイルを作成します。

プロパティ・ファイル

2 つのプロパティ・ファイル (adsync_private.prop および adsync_public.prop) は、ディレクトリー・サーバー・インスタンスを Active Directory との同期機能に対応するように構成すると更新されます。adsync.xml ファイルには、これらの外部プロパティ・ファイルへの参照が含まれています。

•

adsync_private.prop プロパティ・ファイルは暗号化されており、このファイルのプロパティ値を変更するには、構成ツールまたは **idsadscfg** コマンドを使用する必要があります。

Active Directory との同期では、IBM Security Directory Server のユーザー項目を同期化するために、以下の属性を必須属性として使用します。

- \$dn 属性 (sAMAccountName を基に作成)
- cn
- sn
- uid
- objectClass

以下の例は、adsync_private.prop ファイルを示しています。

```
Adhost1.AdGroupContainer:ou=SWUGroups,dc=adsyncctest,dc=com
Adhost1.AdLdapLoginName:cn=administrator,cn=users,dc=adsyncctest,dc=com
Adhost1.AdLdapPwd:dd06proxy
Adhost1.AdLdapSrchBase:dc=adsyncctest,dc=com
Adhost1.AdLdapUrl:ldap://localhost:389
Adhost1.AdLdapUserContainer:ou=sales,dc=adsyncctest,dc=com
Adhost1.IbmlDapGroupContainer:ou=groups,o=sample
Adhost1.IbmlDapUserContainer:ou=Austin,o=sample
IbmlDapLoginName:cn=root
IbmlDapPwd:sec001ret
IbmlDapSrchBase:ou=austin,o=sample
IbmlDapSuffix:o=sample
IbmlDapUrl:ldap://localhost:2389
```

残りの属性はオプションであり、これらの属性 (およびマッピング) は `<TDSinstance_home>/idsslapd-<instance>/etc/tdisoldir/adsync_public.prop` ファイルで変更できます。

•

adsync_public.prop ファイルは ASCII テキスト・ファイルです。このファイルには以下のプロパティが含まれており、変更できます。

表 48. theadsync_public.prop ファイル内のプロパティ

プロパティ	説明	例
AdDc1.AdSSL	<p>値が true の場合は、SSL が構成済みであることと、Active Directory との接続に SSL が使用されることを示します。</p> <p>値が false の場合は、接続が SSL セッションを介して行われなことを示します。</p> <p>値を true に設定した場合は、665 ページの『Active Directory への SSL 接続を使用するための Active Directory との同期の構成』の手順に従って、IBM Security Directory Integrator サーバーで鍵ファイルを構成してから構成を実行する必要があります。</p>	true
TdsOptionalAttributes	<p>セミコロン (;) 文字で区切られた、オプションの構文 [属性:(コロン)属性] を持つ属性のリスト。</p> <p>これらの属性は、Active Directory からの属性名を IBM Security Directory Integrator (初期作業項目) にそれぞれ別の名前で保管できることを意味しています。この名前は、属性を IBM Security Directory Server の別の属性にマップするときに使用することもできます。</p> <p>属性では大文字と小文字が区別されます。</p> <p>1 つの IBM Security Directory Server 属性に複数の属性をマップすることはできません。</p> <p>userPassword 属性はマップできません。</p>	otherTelephone:telephoneNumber とは、Active Directory の属性 otherTelephone が、IBM Security Directory Server 項目の対応する属性 telephoneNumber にマップされることを表しています。
LogLevel	<p>Active Directory ソリューションでは、adsync の構成および実行の詳細を記録するときに LogLevel パラメーターを使用します。以下のログ・レベルを指定できます。</p> <ul style="list-style-type: none"> • DEBUG • INFO • WARN • ERROR • FATAL 	

以下の例は、adsync_public.prop ファイルを示しています。

```
Adhost1.OptionalAttributes:mail;displayName:cn;l:city;postalCode;initials:initials;givenName:givenName;streetAddress:street;st:st;department:departmentNumber;telephoneNumber:telephoneNumber;title:title;physicalDeliveryOfficeName:roomNumber;otherTelephone:telephoneNumber;description:description;ibmLdapHost1.OptionalAttributes:mail; cn; city:l; postalCode; initials; givenName; street; st; departmentNumber; telephoneNumber; title; roomNumber; descriptionAdhost1.AdLdapSSL: false
```

adsync_cfg.xml

このファイルは、構成ツールまたは **idsadscfg** コマンドにより、構成時に使用されます。このファイルには、構成済みのパラメーターを使用して adsync_private.prop および adsync_public.prop プロパティ・ファイルを作成する AssemblyLine が含まれています。

groups.ldif (サンプル・ファイル)

このファイルには、Active Directory のセットアップに追加するサンプルのグループが入っています。これは、Active Directory と IBM Security Directory Server とを同期化するために使用されるサンプル・データです。このファイルはそのままの状態では使用しないでください。このファイルは、指定するユーザーとグループのコンテナ、およびドメイン情報により、構成時に変更されます。

groups.ldif ファイルの例を以下に示します。

```
CN=SWUGroup1,OU=SWUGroups,dc=adsynctest,dc=com
objectClass=top
objectClass=group
cn=SWUGroup1
member=CN=lwood,ou=sales,dc=adsynctest,dc=com
member=CN=jdixon,ou=sales,dc=adsynctest,dc=com
member=CN=jcarroll,ou=sales,dc=adsynctest,dc=com
member=CN=twatson,ou=sales,dc=adsynctest,dc=com
member=CN=jsanchez,ou=sales,dc=adsynctest,dc=com
sAMAccountName=SWUGroup1
groupType=-2147483646

CN=SWUGroup2,OU=SWUGroups,dc=adsynctest,dc=com
objectClass=top
objectClass=group
cn=SWUGroup2
member=CN=amason,ou=sales,dc=adsynctest,dc=com
member=CN=swilson,ou=sales,dc=adsynctest,dc=com
member=CN=Elizabeth Brown,ou=sales,dc=adsynctest,dc=com
sAMAccountName=SWUGroup2
groupType=-2147483646
```

users.ldif (サンプル・ファイル)

このファイルには、Active Directory のセットアップに追加するサンプルのユーザーが入っています。これは、Active Directory と IBM Security Directory Server とを同期化するために使用されるサンプル・データです。このファイルはそのままの状態では使用しないでください。このファイルは、指定するユーザーとグループのコンテナ、およびドメイン情報により、構成時に変更されます。

users.ldif ファイルの例を以下に示します。

```
CN=lwood,ou=sales,dc=adsynctest,dc=com
cn=lwood
displayName=LORI H. WOOD
givenName=LORI
initials=H
objectClass=top
objectClass=person
objectClass=organizationalPerson
objectClass=user
physicalDeliveryOfficeName=88001
name=lwood
sAMAccountName=lwood
sn=WOOD
userAccountControl=544
userPrincipalName=lwood@xyz.com

CN=pburns,ou=sales,dc=adsynctest,dc=com
cn=pburns
displayName=PATRICK BURNS
givenName=PATRICK
objectClass=top
```

```
objectClass=person
objectClass=organizationalPerson
objectClass=user
name=pburns
sAMAccountName=pburns
sn=BURNS
userAccountControl=544
userPrincipalName=pburns@xyz.com
```

adsync.log

同期の詳細 (idsadsrun の実行) ログは、<TDS instance_home>/idsslapd-<instance>/etc/tdisoldir/logs フォルダにある adsync.log ファイルに記録されます。

ログの詳細を構成するには、<TDS instance_home>/idsslapd-<instance>/etc/tdisoldir/adsync_public.prop ファイルの LogLevel パラメーターを使用します。LogLevel パラメーターのデフォルト値は INFO ですが、DEBUG に変更すればデバッグのログを取得できます。詳しくは、「Security Directory Integrator Logging」を参照してください。

Active Directory との同期の実行

Active Directory との同期を構成後に実行するには、idsadsrun コマンドを使用する必要があります。

このタスクについて

idsadsrun コマンドによる Active Directory との同期機能の実行については、IBM Security Directory Server の資料の『コマンド解説書』セクションを参照してください。

注: Active Directory に指定されたパラメーターにエラーがあった場合、それらのエラーは構成時ではなく、実行時に生成されます。Active Directory パラメーターのエラーが実行時に報告された場合は、構成ツール (「Active Directory との同期: Active Directory の詳細」ウィンドウ内) または idsadscfg コマンドを使用して Active Directory パラメーターを再構成する必要があります。

Active Directory への SSL 接続を使用するための Active Directory との同期の構成

Active Directory Server に対しては、SSL 接続を使用できます。(ただし、IBM Security Directory Server に対して SSL 接続を使用することはできません)。Active Directory との同期機能をセットアップして Active Directory への SSL 接続を処理するには、ここに示す手順を使用できます。

このタスクについて

手順

1. 適切なポート番号を使用するように Active Directory との同期を構成します。Active Directory との同期の構成に使用するツールに応じて、以下の点を考慮してください。
 - 構成ツールを使用して構成する場合は、「Active Directory との同期: インスタンスの詳細」ウィンドウで「Active Directory に SSL 接続を使用」チェック

ク・ボックスを選択して、「Active Directory との同期: Active Directory の詳細」ウィンドウの「ホスト・ポート」フィールドに正しいポート番号を入力するようにしてください。

- **idsadsCfg** コマンドを使用して構成する場合は、必ず **-Z** フラグを使用してください。
2. 以下の手順に従って、自己証明書を使用して Active Directory を SSL に構成します。
 - a. Internet Information Services (IIS) を Windows 2003 Server にインストールします。
 - b. 証明書サービスを Windows 2003 Server にインストールし、エンタープライズ証明機関を Active Directory ドメインにインストールします。エンタープライズ証明機関を必ずインストールしてください。
 - c. 証明書サーバー・サービスを始動します。これにより、証明書を配布できるようにするための仮想ディレクトリーが Internet Information Service (IIS) に作成されます。
 - d. セキュリティー (グループ) ポリシーを作成し、ドメイン・コントローラーに指示して、証明機関 (CA) から SSL 証明書を取得します。
 - e. 「Active Directory ユーザーとコンピュータ」管理ツールを開きます。
 - f. ドメインの下で、「ドメイン コントローラ」を右クリックします。「プロパティ」を選択します。
 - g. 「グループ ポリシー」タブで、「既定のドメイン コントローラのポリシー」をクリックしてポリシーを編集します。
 - h. 「コンピュータの構成」->「Windows の設定」->「セキュリティの設定」->「公開キーのポリシー」の順に進みます。
 - i. 「自動証明書要求の設定」を右クリックします。
 - j. 「新規作成」を選択します。
 - k. 「自動証明書要求」を選択します。
 - l. ウィザードを実行します。ドメイン・コントローラーの証明書テンプレートを選択します。
 - m. エンタープライズ証明機関を CA として選択します。サード・パーティーの CA を選択した場合も同様に機能します。
 - n. ウィザードを完了します。これで、すべてのドメイン・コントローラーが自動的に CA から証明書を要求するようになり、ポート 636 で SSL を使用する LDAP をサポートするようになりました。
 - o. Active Directory との同期機能をインストールしたコンピューターへの認証局証明書を検索します。
 - p. Active Directory との同期機能をインストールしたコンピューターで Web ブラウザーを開きます。
 - q. `http://<server_name>/certsrv/` (<server_name> は Windows 2003 サーバーの名前) に移動します。ログインすることを求められます。
 - r. 「CA 証明書または証明書失効リストの検索 (Retrieve the CA certificate or certificate revocation list)」というタスクを選択して、「次へ」をクリックします。

- s. 次のページでは、CA 証明書が自動的に強調表示されます。「CA 証明書のダウンロード (Download CA certificate)」をクリックします。
 - t. 新しいダウンロード・ウィンドウが開きます。ファイルをハード・ディスクに保存します。
3. jks ファイルを生成し、Active Directory との同期で構成します。
 - a. **keytool** を使用して証明書ストアを作成します。keytool.exe ファイルを使用して証明書ストアを作成し、この証明書ストアに CA 証明書をインポートします。

注: keytool.exe ファイルは、¥_jvm¥bin ディレクトリーの IBM Security Directory Integrator ディレクトリーにあります。
以下のコマンドを使用します。

```
_jvm¥bin¥keytool -import -file certnew.cer -keystore <keystore_name>.jks
-storepass <password> -alias <keyalias_name>
```

例えば、以下の値を想定します。

- Keystorename = idi.jks
- Password = secret Keyalias
- name = AD_CA

これらの値を使用した場合のコマンドは、以下のようになります。(現在のディレクトリーは C:¥Program Files¥IBM¥SecurityDirectoryIntegrator であるという前提です)。

```
_jvm¥bin¥keytool -import -file certnew.cer -keystore idi.jks
-storepass secret -alias AD_CA
```

- b. 鍵ストアの内容を確認するため、以下のコマンドを入力します。

```
_jvm¥bin¥keytool -list -keystore idi.jks -storepass secret
```

コマンドが以下の出力を返します。

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry:
ad_ca, Mon Nov 04 22:11:46 MST 2002, trustedCertEntry,
Certificate fingerprint (MD5): A0:2D:0E:4A:68:34:7F:A0:21:36:78:65:A7:1B:25:55
```

4. Active Directory との同期を構成し、ステップ 3 で作成した鍵ストアを使用します。 <TDS_instance_home>¥idsldapd-<instance>¥etc¥tdisoldir¥solution.properties ファイルを編集して、鍵ストア・ファイルの場所、鍵ストア・ファイルのパスワード、および鍵ストア・ファイルの種類を設定します (現行リリースでは、jks タイプのみがサポートされています)。

```
#server authentication
#example
javax.net.ssl.trustStore=c:¥test¥idi.jks
javax.net.ssl.trustStorePassword=secret
javax.net.ssl.trustStoreType=jks
#client authentication
#example
javax.net.ssl.keyStore=c:¥test¥idi.jks
javax.net.ssl.keyStorePassword=secret
javax.net.ssl.keyStoreType=jks
```

5. **idsadsrun** コマンドを使用して、Active Directory との同期を開始します。このリレーションにより、SSL を介して Active Directory に接続します。

付録 H. パスワード・ポリシーに関する追加情報

ここに示す情報により、パスワード・ポリシーに関する追加情報を知ることができます。

パスワード・ポリシー運用属性

以下は、パスワード・ポリシー機能が提供している運用属性です。

属性名	構文	説明
pwdChangedTime	GeneralizedTime	パスワードの最終変更時刻か、パスワード・ポリシーの開始時刻のうち後の方の時刻が格納されます。
pwdAccountLockedTime	GeneralizedTime	アカウントがロックされた時刻が格納されます。アカウントがロックされていない場合、この属性は提供されません。
pwdExpirationWarned	GeneralizedTime	パスワードの有効期限の警告をクライアントに最初に送信した時の時刻が格納されます。
pwdFailureTime	GeneralizedTime	複数値属性。前回の連続ログインに失敗した時刻が格納されます。最後のログインが成功した場合、この属性は提供されません。
pwdGraceUseTime	GeneralizedTime	複数値属性。前回の猶予ログイン時刻が格納されます。
pwdHistory	ディレクトリー・ストリング	以前に使用されたパスワードの履歴が格納されます。この属性のパスワード部分は、userPassword が格納されたのと同じ暗号化方式を使用して格納されます。この属性に格納されるパスワードは、ユーザーが入力した新規の userPassword と比較されます。
pwdReset	Boolean	パスワードがリセットされて、ユーザーが変更する必要がある場合は、値 TRUE が格納されます。それ以外の場合、値は FALSE または非表示になります。
ibm-pwdAccountLocked	Boolean	アカウントが管理上の理由でロックされたことを示します。
ibm-pwdIndividualPolicyDn	GeneralizedTime	ユーザー項目と関連付けることができるパスワード・ポリシー項目の DN。
ibm-pwdGroupPolicyDn	GeneralizedTime	グループ項目と関連付けることができるパスワード・ポリシー項目の DN。

パスワード・ポリシーの応答制御の相互運用性サポート

以下に示すコマンドを実行すると、パスワード・ポリシーの応答制御の相互運用性サポートを実行できます。

相互運用性のために、RFC 準拠のパスワード・ポリシーの応答制御に戻すには、環境変数 `USE_OPENLDAP_PWDPOLICY_CONTROL` に `YES` を設定する必要があります。これを行うには、`idsldapmodify` コマンドを以下の形式で発行します。

```
idsldapmodify -p port -D <adminDN> -w <adminPW>
dn: cn=Front End, cn=configuration
changetype: modify
add: ibm-slapdSetEnv
ibm-slapdSetEnv: USE_OPENLDAP_PWDPOLICY_CONTROL=YES
```

環境変数を設定したら、サーバーを再起動して変更を有効にします。

パスワード・ポリシー照会

以下に示すコマンドを実行すると、パスワード・ポリシー照会を解決できます。

パスワード・ポリシー運用属性を使用すると、ディレクトリー項目のステータスを表示したり、指定した基準に一致する項目を照会したりできます。検索要求に対し運用属性が返されるのは、クライアントからの明示的な要求があった場合のみです。検索操作でこれらの属性を使用するには、重要属性へのアクセス権を所有しているか、使用する特定の属性へのアクセス権を所有している必要があります。

所定の項目のパスワード・ポリシー属性をすべて表示するには、以下のコマンドを使用します。

```
ldapsearch -s base -D <adminDN> -w <adminPW> -b "uid=user1,cn=users,o=sample"
"objectclass=*" +ibmpwdpolicy
```

`pwdChangedTime` 属性値は、パスワードの有効期限を決定するのに使用できます。有効期限は、パスワード・ポリシーの開始時刻とユーザー項目の作成タイム・スタンプに基づいて計算されます。これらの従属値のいずれかが存在しない場合、`pwdChangedTime` 属性が存在しない可能性があります。このため、検索フィルター内の `pwdChangedTime` 属性が、パスワードの期限切れが近いユーザー項目の一部を返さない場合があります。ユーザー・パスワードの期限切れが近いかどうかを判別するには、以下のコマンドを実行します。

```
idsldapsearch -p port -D adminDN -w adminPWD -b base -s sub ¥
'(&(! (pwdChangedTime=*)) (userPassword=*))' pwdChangedTime
```

注: サーバーに多数の項目が含まれている場合、検索に要する時間がかなり長くなることがあります。このため、検索を実行するタイミングを計画する必要があります。

パスワードの期限切れが近いユーザー項目をすべて検出するには、以下のコマンドを実行します。

```
idsldapsearch -p port -D adminDN -w adminPWD -b base
-s sub '(userPassword=*)' pwdChangedTime
```

ロックされたアカウントを照会するには、`pwdAccountLockedTime` を使用します。

```
idsldapsearch -b "cn=users,o=sample" -s sub "(pwdAccountLockedTime=*)" dn
```

リセットされて変更の必要があるパスワードのアカウントを照会するには、`pwdReset` 属性を使用します。

```
idsldapsearch -b "cn=users,o=sample" -s sub "(pwdReset=TRUE)" dn
```

パスワード・ポリシーのオーバーライドおよびアカウントのアンロック

以下に示すコマンドを実行すると、パスワード・ポリシーのオーバーライドおよびアカウントのアンロックが可能になります。

ディレクトリー管理者は、パスワード・ポリシー運用属性を変更し、サーバー管理コントロール (LDAP コマンド行ユーティリティの **-k** オプション) を使用することで、特定項目の通常のパスワード・ポリシーの動作をオーバーライドできます。

`userPassword` 属性を設定する際、`pwdChangedTime` 属性に遠い将来の日付を設定しておくことで、特定アカウントのパスワードが有効期限切れになるのを防ぐことができます。以下の例では、時間を 2200 年 1 月 1 日 午前零時に設定しています。

```
idsldapmodify -D cn=root -w ? -k
dn: uid=wasadmin,cn=users,o=sample
changetype: modify
replace: pwdChangedTime
pwdChangedTime: 22000101000000Z
```

`pwdAccountLockedTime` 属性および `pwdFailureTime` 属性を除去すれば、過度のログイン失敗が原因でロックされたアカウントをアンロックできます。

```
idsldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=sample
changetype: modify
delete: pwdAccountLockedTime
-
delete: pwdFailureTime
```

`pwdChangedTime` 属性を変更して、`pwdExpirationWarned` 属性および `pwdGraceUseTime` 属性を消去すれば、有効期限が切れたアカウントをアンロックできます。

```
idsldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=sample
changetype: modify
replace: pwdChangedTime
pwdChangedTime: yyymddhhss.Z
-
delete: pwdExpirationWarned
-
delete: pwdGraceUseTime
```

`pwdReset` 属性を削除して追加すれば、「パスワードを変更する必要がある」というステータスをクリアしてリセットできます。

```
idsldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=sample
changetype: modify
delete: pwdReset
```

```
idsldapmodify -D cn=root -w ? -k
dn: uid=user2,cn=users,o=sample
changetype: modify
replace: pwdReset
pwdReset: TRUE
```

アカウントを管理上の理由でロックするには、`ibm-pwdAccountLocked` 運用属性を `TRUE` に設定します。アカウントをアンロックするには、この属性を `FALSE` に設定します。この方法でアカウントをアンロックしても、過度のパスワード認証失敗やパスワードの有効期限切れが原因でロックされるアカウントのステータスには影響しません。

この属性を設定するユーザーは、ibm-pwdAccountLocked 属性への書き込み権限を所有している必要があります。この権限は CRITICAL アクセス・クラスで定義されています。

```
idsldapmodify -D uid=useradmin,cn=users,o=sample -w ?
dn: uid=user1,cn=users,o=sample
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: TRUE
```

アカウントをアンロックするには、以下のようにします。

```
idsldapmodify -D uid=useradmin,cn=users,o=sample -w ?
dn: uid=user1,cn=users,o=sample
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: FALSE
```

属性 `ibm-pwdAccountLocked` に `TRUE` が設定されていてアカウントがロックされている場合、管理者がこの属性をクリアして (`FALSE` を設定する)、管理コントロール (`-k` オプション) を使用すれば、アカウントは完全にアンロックされます。また、`pwdAccountLockedTime` 属性および `pwdFailureTime` 属性もクリアしてリセットします。

複数のパスワード・ポリシー属性の複製

ここに示す情報により、複数のパスワード・ポリシー属性の複製について知ることができます。

複数のパスワード・ポリシー属性を複製するには、複製に参加しているサーバーが `ibm-supportedcapabilities` 属性と `ibm-enabledcapabilities` 属性の `OID`、`LDAP_MULTIPLE_PASSWORD_POLICIES_OID` を持つ必要があります。この機能の `OID` 番号は、`1.3.18.0.2.32.77` です。この `OID` がサーバーのルート `DSE` に存在する場合は、サーバーが複数のパスワード・ポリシーとより詳細なパスワード・ポリシー・エラー・メッセージをサポートできます。

パスワード・ポリシー運用属性の複製

以下に示すのは、パスワード・ポリシー運用属性の複製のリストです。

複製環境では、パスワード・ポリシー実装の一貫性を保つために、特定のパスワード・ポリシー属性を複製トポロジー内のサーバーに複製する必要があります。そのためには、`cn=ibmpolicies` サブツリーのすべてのコンシューマーにグローバル・パスワード・ポリシー項目 `“cn=pwdpolicy,cn=ibmpolicies”` を複製する必要があります。すべてのサーバーのパスワード・ポリシー項目を同一にするには、パスワード・ポリシー項目を `cn=ibmpolicies` 項目の下で定義してコンシューマーに複製する必要があります。

パスワード・ポリシーのユーザー関連の要素は、項目の運用属性に保管されます。これらの属性は、読み取り専用のレプリカの属性であったとしても、変更の対象になります。したがって、これらの属性を複製する場合は慎重な考慮が必要になります。

pwdChangedTime

`pwdChangedTime` 属性は、すべてのレプリカに複製する必要があります。これは、パスワードの有効期限を使用可能にするためです。

pwdReset

pwdReset 属性は、すべてのレプリカに複製する必要があります。これは、パスワードのバインドおよび変更以外の操作へのアクセスを拒否するためです。

pwdHistory

pwdHistory 属性は、書き込み可能なレプリカに複製する必要があります。この属性は、読み取り専用のレプリカには複製する必要ありません。レプリカではパスワードは直接変更されないからです。

pwdAccountLockedTime、pwdExpirationWarned、pwdFailureTime、pwdGraceUseTime

pwdAccountLockedTime 属性、pwdExpirationWarned 属性、pwdFailureTime 属性、および pwdGraceUseTime 属性は、書き込み可能なレプリカに複製する必要があります。これは、パスワード・ポリシーをすべてのサーバーに適用するためです。ただし、ユーザー項目を読み取り専用のレプリカに複製する場合、これらの属性は複製しないでください。これは、失敗の回数、猶予ログインの回数が各複製サーバーに記録され、ロックが各複製サーバーで発生してしまうからです。

ユーザーに設定されているパスワード失敗の有効なカウントが M (pwdMaxFailure 属性の値) である場合、マスター・レプリカ・トポロジー上のユーザーは $N * M$ 回試行することができます。N はサーバーの数で、M は pwdMaxFailure 属性の値です。サーバーの数が N を超えている場合、書き込みレプリカではカウントは 1 であると見なされます。ピア・サーバーでユーザー項目のパスワード・ポリシー運用属性が更新された場合、すべての書き込みレプリカに対してこれらの更新が複製されます。残りの N-1 のサーバーは、読み取り専用レプリカのカウントです。各読み取り専用レプリカでは、ユーザー項目のパスワード・ポリシー運用属性に対する更新が独自のデータベースに格納されます。

これらの属性を読み取り専用レプリカに複製すると、失敗試行の許可回数は全体的には削減できますが、パスワード・ポリシーの適用が不安定になる場合があります。

pwdAccountLockedTime、pwdExpirationWarned、pwdFailureTime、および pwdGraceUseTime は、各種の局面で複製されます。ユーザーのパスワードがリセットされ、その結果一部の属性がクリアされた場合、その操作は読み取り専用レプリカにも複製されます。また、マスター・サーバーの管理者が管理コントロールを使用してマスター・サーバーのこれらの運用属性の値を上書きした場合、これらの属性の強制書き込みされた値は、読み取り/書き込みレプリカおよび読み取り専用レプリカに複製されます。

ibm-pwdAccountLocked

ibm-pwdAccountLocked 属性がマスター・サーバーで設定またはクリアされた場合、この属性はレプリカにも複製されます。管理コントロールを使用して操作を行っている間にこの属性がクリアされると、

pwdAccountLockedTime 属性もクリアされ、さらにこの属性に FALSE が設定されると、アカウントは完全にアンロックされます。ただし、

ibm-pwdAccountLocked 属性をコンシューマー・サーバーに複製する前に、サポートされる機能の

LDAP_PASSWORD_POLICY_ACCOUNT_LOCKED_OID がサーバー上に存

在している必要があります。

LDAP_PASSWORD_POLICY_ACCOUNT_LOCKED_OID がコンシューマー・サーバー上に存在しない場合は、複製で属性 `ibm-pwdAccountLocked` を削除してから更新をサーバーに送信する必要があります。

項目に対する強制追加または強制更新

ここに示す情報により、項目に追加または更新を強制する手順の詳細を知ることができます。

管理ユーザーが項目を更新または追加する際、変更あるいは新規に追加する属性の 1 つとしてパスワード・ポリシー運用属性を指定する場合、その管理ユーザーは 1 つ以上の運用属性の値を指定してから、項目に対して強制追加/強制更新を実行することになります。

項目に対する強制追加/強制更新は、通常のパスワード・ポリシー処理がその項目に対して実行されない場合に使用します。この操作では、指定したパスワード・ポリシー運用属性のみが指示通りに変更されます。

通常、強制追加/強制更新は、パスワード・ポリシー属性を指定すると同時に、操作で管理コントロールを使用することで指定します。

`ibm-pwdAccountLocked` 属性を更新する場合、管理コントロールは送信する必要ありません。

管理者は、項目に対して強制追加/強制更新を実行する場合、必要に応じてすべてのパスワード・ポリシー属性を設定します。

通常のパスワード・ポリシー運用属性 (`pwdReset` や `pwdChangedTime` など) のすべてに正しい値が設定されているのでなければ、強制追加は実行しないでください。`pwdChangedTime` に強制追加で値が設定されない場合、ユーザーの方からサーバーへのバインドを試行するか、別の強制更新によってこの属性の値 (回数) が設定されるまで、この属性は設定できません。

パスワード・ポリシー属性を追加操作で明示的に設定する必要がある場合、最初に新規の項目を作成してから、別の変更操作を使用して他のパスワード・ポリシー属性を設定する必要があります。

変更操作でユーザー・パスワード属性を変更する場合、強制更新する必要があるパスワード・ポリシー属性は、`userpassword` 変更操作とは別の操作で更新する必要があります。これにより、パスワード・ポリシーの変更は、追加または変更操作で、すべて適切に実行されます。

付録 I. IBM Security Directory Server の必須属性定義

ここに示す例により、IBM Security Directory Server の必須属性定義の詳細について説明します。

```
attributetypes=( 1.3.18.0.2.4.285
NAME 'aclEntry'
DESC 'Holds the access controls for entries in an IBM eNetwork LDAP
directory'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.285
DBNAME( 'aclEntry' 'aclEntry' )
ACCESS-CLASS restricted
LENGTH 32700 )
```

```
attributetypes=( 1.3.18.0.2.4.286
NAME 'aclPropagate'
DESC 'Indicates whether the ACL applies on entry or subtree.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.286
DBNAME( 'aclPropagate' 'aclPropagate' )
ACCESS-CLASS restricted
LENGTH 5 )
```

```
attributetypes=( 1.3.18.0.2.4.287
NAME 'aclSource'
DESC 'Indicates whether the ACL applies on entry or subtree.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.287
DBNAME( 'aclSource' 'aclSource' )
ACCESS-CLASS system
LENGTH 1000 )
```

```
attributetypes=( 2.5.4.1
NAME ( 'aliasedObjectName' 'aliasedentryname' )
DESC 'Represents the pointed to entry that is specified within an
alias entry.'
EQUALITY 2.5.13.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 2.5.4.1
DBNAME( 'aliasedObject' 'aliasedObject' )
ACCESS-CLASS normal
LENGTH 1000
EQUALITY )
```

```
attributetypes=( 1.3.6.1.4.1.1466.101.120.6
NAME 'altServer'
DESC 'The values of this attribute are URLs of other servers which
may be contacted when this server becomes unavailable.'
EQUALITY 1.3.6.1.4.1.1466.109.114.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
USAGE dSAOperation )
IBMAttributetypes=( 1.3.6.1.4.1.1466.101.120.6
DBNAME( 'altServer' 'altServer' )
ACCESS-CLASS normal
LENGTH 2048 )
```

```
attributetypes=( 2.5.21.5
NAME 'attributeTypes'
DESC 'This attribute is typically located in the subschema entry
and is used to store all attributes known to the server and
objectClasses.'
EQUALITY 2.5.13.30
SYNTAX 1.3.6.1.4.1.1466.115.121.1.3
USAGE directoryOperation )
IBMAttributetypes=( 2.5.21.5
DBNAME( 'attributeTypes' 'attributeTypes' )
ACCESS-CLASS system
LENGTH 30
EQUALITY )
```

```
attributetypes=( 2.5.4.15
NAME 'businessCategory'
DESC 'This attribute describes the kind of business performed by an
organization.'
EQUALITY 2.5.13.2
SUBSTR 2.5.13.4
```

```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE userApplications )
IBMAttributetypes=( 2.5.4.15
DBNAME( 'businessCategory' 'businessCategory' )
ACCESS-CLASS normal
LENGTH 128
EQUALITY
SUBSTR)

attributetypes=( 2.16.840.1.113730.3.1.5
NAME 'changeNumber'
DESC 'Contains the change number of the entry as assigned by the
supplier server.'
EQUALITY 2.5.13.14
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE userApplications )
IBMAttributetypes=( 2.16.840.1.113730.3.1.5
DBNAME( 'changeNumber' 'changeNumber' )
ACCESS-CLASS normal
LENGTH 11
EQUALITY APPROX )

attributetypes=( 2.16.840.1.113730.3.1.8
NAME 'changes'
DESC 'Defines changes made to a directory server. These changes are
in LDIF format.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE userApplications )
IBMAttributetypes=( 2.16.840.1.113730.3.1.8
DBNAME( 'changes' 'changes' )
ACCESS-CLASS sensitive )

attributetypes=( 2.16.840.1.113730.3.1.77
NAME 'changeTime'
DESC 'Time last changed.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE userApplications )
IBMAttributetypes=( 2.16.840.1.113730.3.1.77
DBNAME( 'changeTime' 'changeTime' )
ACCESS-CLASS normal
LENGTH 30 )

attributetypes=( 2.16.840.1.113730.3.1.7
NAME 'changeType'
DESC 'Describes the type of change performed on an entry. Accepted
values include: add, delete, modify, modrdn.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE userApplications )
IBMAttributetypes=( 2.16.840.1.113730.3.1.7
DBNAME( 'changeType' 'changeType' )
ACCESS-CLASS normal
LENGTH 250
EQUALITY )

attributetypes=( 2.5.4.3
NAME ( 'cn' 'commonName' )
DESC 'This is the X.500 commonName attribute, which contains a name of an object.
If the object corresponds to a person, it is typically the persons
full name.'
SUP 2.5.4.41
EQUALITY 2.5.13.2
ORDERING 2.5.13.3
SUBSTR 2.5.13.4
USAGE userApplications )
IBMAttributetypes=( 2.5.4.3
DBNAME( 'cn' 'cn' )
ACCESS-CLASS normal
LENGTH 256
EQUALITY
ORDERING
SUBSTR
APPROX )

attributetypes=( 2.5.18.1
NAME 'createTimestamp'
DESC 'Contains the time that the directory entry was created.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 2.5.18.1
DBNAME( 'ldap_entry' 'create_Timestamp' )

```

```

ACCESS-CLASS system
LENGTH 26 )

attributetypes=( 2.5.18.3
NAME 'creatorsName'
DESC 'Contains the creator of a directory entry.'
EQUALITY 2.5.13.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 2.5.18.3
DBNAME( 'ldap_entry'creator' )
ACCESS-CLASS system
LENGTH 1000
EQUALITY )

attributetypes=( 2.16.840.1.113730.3.1.10
NAME 'deleteOldRdn'
DESC 'a flag which indicates if the old RDN should be retained as
an attribute of the entry'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE userApplications )
IBMAttributetypes=( 2.16.840.1.113730.3.1.10
DBNAME( 'deleteOldRdn'deleteOldRdn' )
ACCESS-CLASS normal
LENGTH 5 )

attributetypes=( 2.5.4.13
NAME 'description'
DESC 'Attribute common
to CIM and LDAP schema to provide lengthy description of a
directory object entry.'
EQUALITY 2.5.13.2
SUBSTR 2.5.13.4
SYNTAX
1.3.6.1.4.1.1466.115.121.1.15
USAGE userApplications )
IBMAttributetypes=( 2.5.4.13
DBNAME( 'description'description' )
ACCESS-CLASS normal
LENGTH 1024
EQUALITY
SUBSTR )

attributetypes=( 2.5.21.2
NAME 'ditContentRules'
DESC 'Refer to RFC 2252.'
EQUALITY 2.5.13.30
SYNTAX 1.3.6.1.4.1.1466.115.121.1.16
USAGE directoryOperation )
IBMAttributetypes=( 2.5.21.2
DBNAME( 'ditContentRules'ditContentRules' )
ACCESS-CLASS system
LENGTH 256
EQUALITY )

attributetypes=( 2.5.21.1
NAME 'ditStructureRules'
DESC 'Refer to RFC 2252.'
EQUALITY 2.5.13.29
SYNTAX 1.3.6.1.4.1.1466.115.121.1.17
USAGE directoryOperation )
IBMAttributetypes=( 2.5.21.1
DBNAME( 'ditStructureRules'ditStructureRules' )
ACCESS-CLASS system
LENGTH 256
EQUALITY )

attributetypes=( 2.5.4.49
NAME ( 'dn'distinguishedName')
DESC 'This attribute type is not used as the name of the object itself,
but it is instead a base type from which attributes with DN syntax
inherit.It is unlikely that values of this type itself will occur
in an entry.'
EQUALITY 2.5.13.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
USAGE userApplications )
IBMAttributetypes=( 2.5.4.49
DBNAME( 'dn'dn' )
ACCESS-CLASS normal
LENGTH 1000
EQUALITY )

attributetypes=( 1.3.18.0.2.4.288
NAME 'entryOwner'
DESC 'Indicates the distinguished name noted as the owner of the
entry'
EQUALITY 2.5.13.2

```

```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.288
DBNAME( 'entryOwner' 'entryOwner' )
ACCESS-CLASS restricted
LENGTH 1000 )

attributetypes=( 2.5.18.9
NAME 'hasSubordinates'
DESC 'Indicates whether any subordinate entries exist below the
entry holding this attribute.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 2.5.18.9
DBNAME( 'hasSubordinates' 'hasSubordinates' )
ACCESS-CLASS system
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.2244
NAME 'ibm-allGroups'
DESC 'All groups to which an entry belongs. An entry may be a member
directly via member, uniqueMember or memberURL attributes, or
indirectly via ibm-memberGroup attributes. Read-only operational
attribute (not allowed in filter).'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2244
DBNAME( 'allGroups' 'allGroups' )
ACCESS-CLASS normal
LENGTH 1000 )

attributetypes=( 1.3.18.0.2.4.2243
NAME 'ibm-allMembers'
DESC 'All members of a group. An entry may be a member directly via
member, uniqueMember or memberURL attributes, or indirectly via
ibm-memberGroup attributes. Read-only operational attribute (not
allowed in filter).'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2243
DBNAME( 'ibmAllMembers' 'ibmAllMembers' )
ACCESS-CLASS normal
LENGTH 1000 )

attributetypes=( 1.3.18.0.2.4.1077
NAME 'ibm-audit'
DESC 'TRUE or FALSE. Enable or disable the audit service. デフォルト
is FALSE.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.1077
DBNAME( 'audit' 'audit' )
ACCESS-CLASS critical
LENGTH 16 )

attributetypes=( 1.3.18.0.2.4.1073
NAME 'ibm-auditAdd'
DESC 'TRUE or FALSE. Indicate whether to log the Add operation.
Default is FALSE.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.1073
DBNAME( 'auditAdd' 'auditAdd' )
ACCESS-CLASS critical
LENGTH 16 )

attributetypes=( 1.3.18.0.2.4.1070
NAME 'ibm-auditBind'
DESC 'TRUE or FALSE. Indicate whether to log the Bind operation.
Default is FALSE.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.1070
DBNAME( 'auditBind' 'auditBind' )
ACCESS-CLASS critical
LENGTH 16 )

attributetypes=( 1.3.18.0.2.4.1071
NAME 'ibm-auditDelete'
DESC 'TRUE or FALSE. Indicate whether to log the Delete operation.
Default is FALSE.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )

```

```

IBMAttributetypes=( 1.3.18.0.2.4.1071
DBNAME( 'auditDelete''auditDelete' )
ACCESS-CLASS critical
LENGTH 16 )

attributetypes=( 1.3.18.0.2.4.1069
NAME 'ibm-auditExtOpEvent'
DESC 'TRUE or FALSE. Indicate whether to log LDAP v3 Event
Notification extended operations. Default is FALSE.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.1069
DBNAME( 'auditExtOpEvent''auditExtOpEvent' )
ACCESS-CLASS critical
LENGTH 16 )

attributetypes=( 1.3.18.0.2.4.1078
NAME 'ibm-auditFailedOpOnly'
DESC 'TRUE or FALSE. Indicate whether to only log failed operations.
Default is FALSE.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.1078
DBNAME( 'auditFailedOpOnly''auditFailedOpOnly' )
ACCESS-CLASS
critical LENGTH 16 )

attributetypes=( 1.3.18.0.2.4.1079
NAME 'ibm-auditLog'
DESC 'Specifies the pathname for the audit log.'
EQUALITY 2.5.13.5 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.1079
DBNAME( 'auditLog''auditLog' )
ACCESS-CLASS critical
LENGTH 1024 )

attributetypes=( 1.3.18.0.2.4.1072
NAME 'ibm-auditModify'
DESC 'TRUE or FALSE. Indicate whether to log the Modify operation.
Default is FALSE.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.1072
DBNAME( 'auditModify''auditModify' )
ACCESS-CLASS critical
LENGTH 16 )

attributetypes=( 1.3.18.0.2.4.1075
NAME 'ibm-auditModifyDN'
DESC 'TRUE or FALSE. Indicate whether to log the ModifyRDN
operation. Default is FALSE.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.1075
DBNAME( 'auditModifyDN''auditModifyDN' )
ACCESS-CLASS critical
LENGTH 16 )

attributetypes=( 1.3.18.0.2.4.1074
NAME 'ibm-auditSearch'
DESC 'TRUE or FALSE. Indicate whether to log the Search operation.
Default is FALSE.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.1074
DBNAME( 'auditSearch''auditSearch' )
ACCESS-CLASS critical
LENGTH 16 )

attributetypes=( 1.3.18.0.2.4.1076
NAME 'ibm-auditUnbind'
DESC 'TRUE or FALSE. Indicate whether to log the Unbind operation.
Default is FALSE.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.1076
DBNAME( 'auditUnbind''auditUnbind' )
ACCESS-CLASS critical
LENGTH 16 )

attributetypes=( 1.3.18.0.2.4.2483
NAME 'ibm-capabilitiessubentry'
DESC 'Names the ibm-capabilitiessubentry object listing the

```

```

capabilities of the naming context containing this object.'
EQUALITY 2.5.13.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
NO-USER-MODIFICATION
USAGE dSAOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2483
DBNAME( 'ibmcapsubentry' 'ibmcapsubentry' )
ACCESS-CLASS system
LENGTH 1000 )

attributetypes=( 1.3.18.0.2.4.2444
NAME 'ibm-effectiveAcl'
DESC 'An operational attribute that contains the accumulated filter
based effective access for entries in an IBM LDAP directory.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2444
DBNAME( 'effectiveAcl' 'effectiveAcl' )
ACCESS-CLASS restricted
LENGTH 32700 )

attributetypes=( 1.3.18.0.2.4.2331
NAME 'ibm-effectiveReplicationModel'
DESC 'Advertises in the Root DSE the OID of the replication model in
use by the server'
EQUALITY 1.3.6.1.4.1.1466.109.114.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
SINGLE-VALUE NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2331
DBNAME( 'effectiveReplicat' 'effectiveReplicat' )
ACCESS-CLASS system
LENGTH 240 )

attributetypes=( 1.3.18.0.2.4.2482
NAME 'ibm-enabledCapabilities'
DESC 'Lists capabilities that are enabled for use on this server.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
NO-USER-MODIFICATION
USAGE dSAOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2482
DBNAME( 'ibmenabledcap' 'ibmenabledcap' )
ACCESS-CLASS system
LENGTH 100 )

attributetypes=( 1.3.18.0.2.4.2325
NAME 'ibm-entryChecksum'
DESC 'A checksum of the user attributes for the entry containing
this attribute.'
EQUALITY 1.3.6.1.4.1.1466.109.114.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2325
DBNAME( 'entryChecksum' 'entryChecksum' )
ACCESS-CLASS system
LENGTH 100 )

attributetypes=( 1.3.18.0.2.4.2326
NAME 'ibm-entryChecksumOp'
DESC 'A checksum of the replicated operational attributes for the
entry containing this attribute.'
EQUALITY 1.3.6.1.4.1.1466.109.114.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
SINGLE-VALUE NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2326
DBNAME( 'entryChecksumOp' 'entryChecksumOp' )
ACCESS-CLASS system
LENGTH 100 )

attributetypes=( 1.3.18.0.2.4.1780
NAME 'ibm-entryUuid'
DESC 'Uniquely identifies a directory entry throughout its life.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.1780
DBNAME( 'ibmEntryUuid' 'ibmEntryUuid' )
ACCESS-CLASS system
LENGTH 36
EQUALITY )

attributetypes=( 1.3.18.0.2.4.2443
NAME 'ibm-filterAclEntry'
DESC 'Contains filter based access controls for entries in an IBM

```

```

LDAP directory.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2443
DBNAME( 'filterAcEntry' 'filterAcEntry' )
ACCESS-CLASS restricted
LENGTH 32700 )

attributetypes=( 1.3.18.0.2.4.2445
NAME 'ibm-filterAcInherit'
DESC 'Indicates whether filter based ACLs should accumulate up the
ancestor tree.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2445
DBNAME( 'filterAcInherit' 'filterAcInherit' )
ACCESS-CLASS restricted
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.3238
NAME 'ibm-pwdPolicyStartTime'
DESC 'Specifies the time Password Policy was last turned on.'
ORDERING 2.5.13.28
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.3238
DBNAME( 'pwdPolicyStartTim' 'pwdPolicyStartTim' )
ACCESS-CLASS normal
LENGTH 30 )

attributetypes=( 1.3.18.0.2.4.2330
NAME 'ibm-replicationChangeLDIF'
DESC 'Provides LDIF representation of the last failing operation'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2330
DBNAME( 'replicationChange' 'replicationChange' )
ACCESS-CLASS system )

attributetypes=( 1.3.18.0.2.4.2498
NAME 'ibm-replicationIsQuiesced'
DESC 'Indicates whether the replicated subtree containing this
attribute is quiesced on this server.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 S
INGLE-VALUE
NO-USER-MODIFICATION
USAGE dSAOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2498
DBNAME( 'replIsQuiesced' 'replIsQuiesced' )
ACCESS-CLASS system
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.2338
NAME 'ibm-replicationLastActivationTime'
DESC 'Indicates the last time the replication thread was activated'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2338
DBNAME( 'replicationLastAc' 'replicationLastAc' )
ACCESS-CLASS system
LENGTH 32 )

attributetypes=( 1.3.18.0.2.4.2334
NAME 'ibm-replicationLastChangeId'
DESC 'Indicates last change ID successfully replicated for a
replication agreement'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2334
DBNAME( 'replicationLastCh' 'replicationLastCh' )
ACCESS-CLASS system
LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2335
NAME 'ibm-replicationLastFinishTime'
DESC 'Indicates the last time the replication thread completed
sending all of the pending entries.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2335

```

```

DBNAME( 'replicationLastFi''replicationLastFi' )
ACCESS-CLASS system
LENGTH 30 )

attributetypes=( 1.3.18.0.2.4.2448
NAME 'ibm-replicationLastGlobalChangeId'
DESC 'Indicates the ID of the last global (applies to the entire
DIT, such as schema) change successfully replicated.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2448
DBNAME( 'replicationLastGI''replicationLastGI' )
ACCESS-CLASS normal
LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2340
NAME 'ibm-replicationLastResult'
DESC 'Result of last attempted replication in the form:
<time><change ID><resultcode> <entry-dn> '
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2340
DBNAME( 'replicationLastRe''replicationLastRe' )
ACCESS-CLASS system
LENGTH 2048 )

attributetypes=( 1.3.18.0.2.4.2332
NAME 'ibm-replicationLastResultAdditional'
DESC 'Provides any additional error information returned by the
consuming server in the message component of the LDAP result'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2332
BNAME( 'replicationLastAd''replicationLastAd' )
ACCESS-CLASS system
LENGTH 1024 )

attributetypes=( 1.3.18.0.2.4.2339
NAME 'ibm-replicationNextTime'
DESC 'Indicates next scheduled time for replication'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2339
DBNAME( 'replicationNextTi''replicationNextTi' )
ACCESS-CLASS system
LENGTH 30 )

attributetypes=( 1.3.18.0.2.4.2333
NAME 'ibm-replicationPendingChangeCount'
DESC 'Indicates the total number of pending unreplicated changes for
this replication agreement'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2333
DBNAME( 'replicationPendig''replicationPendig' )
ACCESS-CLASS system
LENGTH 12 )

attributetypes=( 1.3.18.0.2.4.2337
NAME 'ibm-replicationPendingChanges'
DESC 'Unreplicated change in the form
<change ID><operation> <dn>
where operation is ADD, DELETE, MODIFY, MODIFYDN'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2337
DBNAME( 'replicationPendch''replicationPendch' )
ACCESS-CLASS system
LENGTH 1100 )

attributetypes=( 1.3.18.0.2.4.2336
NAME 'ibm-replicationState'
DESC 'Indicates the state of the replication thread:
active,ready,waiting,suspended, or full; if full, the value will
indicate the amount of progress'
EQUALITY 1.3.6.1.4.1.1466.109.114.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )

```

```

IBMAttributetypes=( 1.3.18.0.2.4.2336
DBNAME( 'replicationState' 'replicationState' )
ACCESS-CLASS system
LENGTH 240 )

attributetypes=( 1.3.18.0.2.4.2495
NAME 'ibm-replicationThisServerIsMaster'
DESC 'Indicates whether the server returning this attribute is a
master server for the subtree containing this entry.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE NO-USER-MODIFICATION
USAGE dSAOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2495
DBNAME( 'replThisSvrMast' 'replThisSvrMast' )
ACCESS-CLASS system
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.2328
NAME 'ibm-serverId'
DESC 'Advertises in the Root DSE the ibm-slapdServerId configuration
setting'
EQUALITY 1.3.6.1.4.1.1466.109.114.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE dSAOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2328
DBNAME( 'serverId' 'serverId' )
ACCESS-CLASS system
LENGTH 240 )

attributetypes=( 1.3.18.0.2.4.2374
NAME 'ibm-slapdACLCache'
DESC 'Controls whether or not the server caches ACL information'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2374
DBNAME( 'ACLCache' 'ACLCache' )
ACCESS-CLASS normal
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.2373
NAME 'ibm-slapdACLCacheSize'
DESC 'Maximum number of entries to keep in the ACL Cache'
EQUALITY 2.5.13.14
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 S
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2373
DBNAME( 'slapdACLCacheSize' 'slapdACLCacheSize' )
ACCESS-CLASS normal
LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2428
NAME 'ibm-slapdAdminDN'
DESC 'Bind DN for ibmslapd administrator, e.g.: cn=root'
EQUALITY 2.5.13.1
ORDERING 1.3.18.0.2.4.405
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2428
DBNAME( 'slapdAdminDN' 'slapdAdminDN' )
ACCESS-CLASS critical
LENGTH 1000
EQUALITY ORDERING )

attributetypes=( 1.3.18.0.2.4.2425
NAME 'ibm-slapdAdminPW'
DESC 'Bind password for ibmslapd administrator.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE
SAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2425
DBNAME( 'slapdAdminPW' 'slapdAdminPW' )
ACCESS-CLASS critical )

attributetypes=( 1.3.18.0.2.4.2366
NAME 'ibm-slapdAuthIntegration'
DESC 'Specifies integration of LDAP administrator access with local
OS users. Legal values are : 0 - do not map local OS users to LDAP
administrator, 1 - map local OS users with proper authority to LDAP
administrator. This is supported only on i5/OS.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2366
DBNAME( 'slapdAuthIntegrat' 'slapdAuthIntegrat' )
ACCESS-CLASS system

```

```

LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2432
NAME 'ibm-slapdCLIErrors'
DESC 'File path or device on ibmslapd host machine to which DB2 CLI
error messages will be written.On Windows, forward slashes are
allowed, and a leading slash not preceded by a drive letter is
assumed to be rooted at the install directory (i.e.: /tmp/cli.errors
= D:\Program Files\IBM\ldap\tmp\cli.errors).'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2432
DBNAME( 'slapdCLIErrors' 'slapdCLIErrors' )
ACCESS-CLASS normal
LENGTH 1024 )
attributetypes=( 1.3.18.0.2.4.3147
NAME 'ibm-slapdCachedAttributeAutoAdjust'
DESC 'Specifies if autonomic attribute caching is to be enabled.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=(1.3.18.0.2.4.3147
DBNAME('slapdCachAttrAA' 'slapdCachAttrAA' )
ACCESS-CLASS normal
LENGTH 5)

attributetypes=( 1.3.18.0.2.4.3149
NAME 'ibm-slapdCachedAttributeAutoAdjustTime'
DESC 'Time to start autonomic attribute cache processing.
Values are in the form of Thhmss where hh is hours, mm is minutes
and ss is seconds, using a 24 hour clock.'
EQUALITY 1.3.6.1.4.1.1466.109.114.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=(1.3.18.0.2.4.3149
DBNAME('slapdCachAttrAAT' 'slapdCachAttrAAT' )
ACCESS-CLASS normal
LENGTH 7)

attributetypes=( 1.3.18.0.2.4.3148
NAME 'ibm-slapdCachedAttributeAutoAdjustTimeInterval'
DESC 'Specifies the time interval, in hours,
for autonomic attribute cache processing.'
EQUALITY 2.5.13.14
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=(1.3.18.0.2.4.3148
DBNAME('slapdCachAttrAAI' 'slapdCachAttrAAI' )
ACCESS-CLASS normal
LENGTH 11)

attributetypes=( 1.3.18.0.2.4.3116
NAME 'ibm-slapdCryptoSync'
DESC 'A key stash file consistency marker string.
It is queried by the server atstart up as part of
a verification process to ensure that the key stash
files match any data that has been two-way encrypted.'
EQUALITY 2.5.13.17
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.3116
DBNAME('CryptoSync' 'CryptoSync' )
ACCESS-CLASS system )

attributetypes=( 1.3.18.0.2.4.2369
NAME 'ibm-slapdDB2CP'
DESC 'Specifies the Code Page of the directory database.1208 is
the code page for UTF-8 databases.'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2369
DBNAME( 'slapdDB2CP' 'slapdDB2CP' )
ACCESS-CLASS normal
LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2431
NAME 'ibm-slapdDBAlias'
DESC 'The DB2 database alias.'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 S
INGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2431

```

```

DBNAME( 'slapdDBAlias' 'slapdDBAlias' )
ACCESS-CLASS normal L
LENGTH 8 )
attributetypes=( 1.3.18.0.2.4.2417
NAME 'ibm-slapdDbConnections'
DESC 'The number of DB2 connections the server will dedicate to the DB2
backend. The value must be 5 or greater. Additional connections may
be created for replication and change log.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2417
DBNAME( 'DbConnections' 'DbConnections' )
ACCESS-CLASS critical
LENGTH 2 )

ttributetypes=( 1.3.18.0.2.4.2418
NAME 'ibm-slapdDbInstance'
DESC 'The DB2 database instance for this backend.'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2418
DBNAME( 'slapdDbInstance' 'slapdDbInstance' )
ACCESS-CLASS critical
LENGTH 8 )

attributetypes=( 1.3.18.0.2.4.2382
NAME 'ibm-slapdDbLocation'
DESC 'The file system path where the backend database is located. オン
UNIX or Linux this is usually the home directory of the DB2INSTANCE owner
(e.g.: /home/ldapdb2). On windows its just a drive specifier (e.g.: D:)'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2382
DBNAME( 'slapdDbLocation' 'slapdDbLocation' )
ACCESS-CLASS critical
LENGTH 1024 )

attributetypes=( 1.3.18.0.2.4.2426
NAME 'ibm-slapdDbName'
DESC 'The DB2 database name for this backend.'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2426
DBNAME( 'slapdDbName' 'slapdDbName' )
ACCESS-CLASS critical
LENGTH 8 )

attributetypes=( 1.3.18.0.2.4.2422
NAME 'ibm-slapdDbUserID'
DESC 'The user name with which to connect to the DB2 database for
this backend.'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2422
DBNAME( 'slapdDbUserID' 'slapdDbUserID' )
ACCESS-CLASS critical
LENGTH 8 )

attributetypes=( 1.3.18.0.2.4.2423
NAME 'ibm-slapdDbUserPW'
DESC 'The userpassword with which to connect to the DB2 database
for this backend.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2423
DBNAME( 'slapdDbUserPW' 'slapdDbUserPW' )
ACCESS-CLASS critical )

attributetypes=( OID TBD
NAME 'ibm-slapdDerefAliases'
DESC 'Maximum alias dereferencing level on search requests, regardless of
any derefAliases that may have been specified on the client requests. 許可
values are "never", "find", "search" and "always".'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.3054
DBNAME( 'DerefAliases' 'DerefAliases' )
ACCESS-CLASS critical
LENGTH 6)

attributetypes=( 1.3.18.0.2.4.2449

```

```

NAME 'ibm-slapdDN' DESC 'This attribute is used to sort search
results by the entry DN (LDAP_ENTRY.DN column in the LDAPDB2
database).'
EQUALITY 2.5.13.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE NO-USER-MODIFICATION
USAGE dSAOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2449
DBNAME( 'LDAP_ENTRY''DN' )
ACCESS-CLASS system
LENGTH 1000 )

attributetypes=( 1.3.18.0.2.4.3287NAME 'ibm-slapdGroupMembersCacheBypassLimit'
DESC 'Maximum number of members
that can be in a group in order for the group and its members to be cached
in the group members cache.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.3287
DBNAME( 'slapdGMCacheBy''slapdGMCacheBy' )
ACCESS-CLASS normal
LENGTH 11)

attributetypes=( 1.3.18.0.2.4.3297
NAME NAME 'ibm-slapdGroupMembersCacheSize' DESC 'Maximum number of group
entries whose members should be cached.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.3297
DBNAME('slapdGMCacheSiz''slapdGMCacheSiz')
ACCESS-CLASS normal
LENGTH 11)

attributetypes=( 1.3.18.0.2.4.3399
NAME NAME 'ibm-slapdProxyMaxPendingOpsPerClient' DESC 'The maximum number of
operations that could be pending for a single backend server from a single
client connection. If not specified, defaults to 5'
EQUALITY 2.5.13.14
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.3399
DBNAME( 'ProxyMaxPendOps''ProxyMaxPendOps' )
ACCESS-CLASS critical
LENGTH 11)

attributetypes=( 1.3.18.0.2.4.2481
NAME 'ibm-supportedCapabilities'
DESC 'Lists capabilities supported, but necessarily enabled, by this
server.'
QUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
NO-USER-MODIFICATION
USAGE dSAOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2481
DBNAME( 'ibmsupportedCap''ibmsupportedCap' )
ACCESS-CLASS system
LENGTH 100 )

attributetypes=( 1.3.18.0.2.4.2421
NAME 'ibm-slapdEnableEventNotification'
DESC 'If set to FALSE, the server will reject all extended
operation requests to register for event notification withthe
extended result LDAP_UNWILLING_TO_PERFORM.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2421
DBNAME( 'enableEvtNotify''enableEvtNotify' )
ACCESS-CLASS critical
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.xxxx
NAME 'ibm-slapdEnablePersistentSearch'
DESC 'If set to FALSE, the server will ignore non-critical
persistent search control sent with a search request and
will return LDAP_UNWILLING_TO_PERFORM for critical persistent
search control sent with a search request'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.xxxx
DBNAME( 'enablePersistentSearch' )
ACCESS-CLASS critical
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.2372
NAME 'ibm-slapdEntryCacheSize'
DESC 'Maximum number of entries to keep in the entry cache'

```

```

EQUALITY 2.5.13.14
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=(1.3.18.0.2.4.2372
DBNAME( 'slapdRDBMCacheSiz' 'slapdRDBMCacheSiz' )
ACCESS-CLASS normal
LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2424
NAME 'ibm-slapdErrorLog'
DESC 'File path or device on the ibmslapd host machine
to which error messages will be written. On Windows, forward
slashes are allowed, and a leading slash not preceded by a drive
letter is assumed to be rooted at the install directory (i.e.:
/tmp/slapd.errors = D:\Program Files\IBM\1dap\tmp\slapd.errors).'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2424
DBNAME( 'slapdErrorLog' 'slapdErrorLog' )
ACCESS-CLASS critical
LENGTH 1024 )

attributetypes=( 1.3.18.0.2.4.2371
NAME 'ibm-slapdFilterCacheBypassLimit'
DESC 'Search filters that match more than this number of entries
will not be added to the Search Filter cache. Because the list of
entry ids that matched the filter are included in this cache, this
setting helps to limit memory use. A value of 0 indicates no
limit.'
EQUALITY 2.5.13.14
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=(1.3.18.0.2.4.2371
DBNAME( 'slapdRDBMCacheByP' 'slapdRDBMCacheByP' )
ACCESS-CLASS normal
LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2370
NAME 'ibm-slapdFilterCacheSize'
DESC 'Specifies the maximum number of entries to keep in the Search
Filter Cache.'
EQUALITY 2.5.13.14
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2370
DBNAME( 'slapdFilterCacheS' 'slapdFilterCacheS' )
ACCESS-CLASS normal
LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2378
NAME 'ibm-slapdIdleTimeout'
DESC 'Reserved for future use.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2378
DBNAME( 'SlapdIdleTimeout' 'SlapdIdleTimeout' )
ACCESS-CLASS critical
LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2364
NAME 'ibm-slapdIncludeSchema'
DESC 'File path on the ibmslapd host machine containing schema
definitions used by the LDCF backend. Standard values are:
/etc/V3.system.at /etc/V3.system.oc
/etc/V3.ibm.at/etc/V3.ibm.oc /etc/V3.user.at /etc/V3.user.oc
/etc/V3.ldapsyntaxes /etc/V3.matchingrules/etc/V3.modifiedschema
On Windows, forward slashes are allowed, and a leading slash not
preceded by a drive letter is assumed to be rooted at the install
directory (i.e.: /etc/V3.system.at =
D:\Program Files\IBM\1dap\etc\V3.system.at).'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE directoryOperation )
IBMAttributeTypes=(1.3.18.0.2.4.2364
DBNAME( 'slapdIncludeSchema' 'slapdIncludeSchema' )
ACCESS-CLASS critical
LENGTH 1024 )

attributetypes=( 1.3.18.0.2.4.2365
NAME 'ibm-slapdIpAddress'
DESC 'Specifies IP addresses the server will listen on. These can
be IPv4 or IPv6 addresses. If the attribute is not specified, the
server uses all IP addresses assigned to the host machine. This is
supported on i5/OS only.'
EQUALITY 1.3.6.1.4.1.1466.109.114.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26

```

```

USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2365
DBNAME('slapdIpAddress' 'slapdIpAddress' )
ACCESS-CLASS system
LENGTH 32 )

attributetypes=(1.3.18.0.2.4.2420
NAME 'ibm-slapdKrbAdminDN'
DESC 'Specifies the kerberos ID of the LDAP administrator (e.g.
ibm-kn=name@realm). Used when kerberos authentication is used to
authenticate the administrator when logged onto the Web Admin
interface. This is specified instead of adminDN and adminPW.'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2420
DBNAME( 'slapdKrbAdminDN' 'slapdKrbAdminDN' )
ACCESS-CLASS critical
LENGTH 512 )

attributetypes=( 1.3.18.0.2.4.2394
NAME 'ibm-slapdKrbEnable'
DESC 'Must be one of { TRUE | FALSE }. Specifies whether the
server supports kerberos authentication.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2394
DBNAME( 'slapdKrbEnable' 'slapdKrbEnable' )
ACCESS-CLASS critical
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.2419
NAME 'ibm-slapdKrbIdentityMap'
DESC 'If set to TRUE, when a client is authenticated with a
kerberos ID, the server will search for a local user with matching
kerberos credentials, and add that userDN to the connections
bind credentials. This allows ACLs based on LDAP user DNs to still
be usable with kerberos authentication.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2419
DBNAME('KrbIdentityMap' 'KrbIdentityMap' )
ACCESS-CLASS critical
LENGTH 5 )

attributetypes=(1.3.18.0.2.4.2416
NAME 'ibm-slapdKrbKeyTab'
DESC 'Specifies the LDAP servers keytab file. This file contains the
LDAP servers private key, as associated with its kerberos account.
This file should be protected (like the servers SSL key database
file).
On Windows, forward slashes are allowed, and a leading slash not
preceded by a drive letter (D:) is assumed to be rooted at the
install directory (i.e.: /tmp/slapd.errors =
D:\Program Files\IBM\ltdap\tmp\slapd.errors).'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2416
DBNAME( 'slapdKrbKeyTab' 'slapdKrbKeyTab' )
ACCESS-CLASS critical
LENGTH 1024 )

attributetypes=( 1.3.18.0.2.4.2400
NAME 'ibm-slapdKrbRealm'
DESC 'Specifies the LDAP servers kerberos realm. Used to publish
the ldapServiceName attribute in the root DSE. Note that an LDAP
server can serve as the repository of account information for
multiple KDCs (and realms), but the LDAP server, as a kerberos
server, can only be a member of a single realm.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2400
DBNAME( 'slapdKrbRealm' 'slapdKrbRealm' )
ACCESS-CLASS critical
LENGTH 256 )

attributetypes=( 1.3.18.0.2.4.2415
NAME 'ibm-slapdLdapCrHost'
DESC 'Specify the hostname of the LDAP server that contains the
Certificate Revocation Lists (CRLs) for validating client x.509v3
certificates. This parameter is needed when
ibm-slapdSslAuth=serverclientauth AND the client certificates
have been issued for CRL validation'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE

```

```

USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2415
DBNAME( 'LdapCrIHost' 'LdapCrIHost' )
ACCESS-CLASS critical
LENGTH 256 )

attributetypes=( 1.3.18.0.2.4.2407
NAME 'ibm-slapdLdapCrIPassword'
DESC 'Specify the password that server-side SSL will use to bind to
the LDAP server that contains the CertificateRevocation Lists
(CRLs) for validating client x.509v3certificates.This parameter
may be needed when ibm-slapdSslAuth=serverclientauth AND the client
certificateshave been issued for CRL validation.Note:If the
LDAPserver holding the CRLs permits unauthenticated
access tothe CRLs (i.e. anonymous access), then
ibm-slapdLdapCrIPassword is not required.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2407
DBNAME( 'CrIPassword' 'CrIPassword' )
ACCESS-CLASS critical )

attributetypes=( 1.3.18.0.2.4.2404
NAME 'ibm-slapdLdapCrIPort'
DESC 'Specify the LDAP ibm-slapdPort used by the LDAP serverthat
contains the Certificate Revocation Lists (CRLs) for validating
client x.509v3 certificates. This parameter is needed when
ibm-slapdSslAuth=serverclientauth AND the client certificateshave
been issued for CRL validation. (IP ports are unsigned, 16-bit
integers in the range 1 - 65535)'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
BMAttributetypes=( 1.3.18.0.2.4.2404
DBNAME( 'LdapCrIPort''LdapCrIPort' )
ACCESS-CLASS critical
LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2403
NAME 'ibm-slapdLdapCrIUser'
DESC 'Specify the bindDN that server-side SSL will use to bindto
the LDAP server that contains the Certificate Revocation Lists
(CRLs)for validating client x.509v3 certificates.This parameter
may be neededwhen ibm-slapdSslAuth=serverclientauth AND the client
certificates havebeen issued for CRL validation.
Note:
If the LDAP server holding theCRLs permits unauthenticated access
to the CRLs (i.e. anonymous access), then ibm-slapdLdapCrIUser is
not required.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2403
DBNAME( 'LdapCrIUser''LdapCrIUser' )
ACCESS-CLASS critical
LENGTH 1000)

attributetypes=( 1.3.18.0.2.4.2409
NAME 'ibm-slapdMasterDN'
DESC 'Bind DN used by a replication supplier server. The value has
to matchthe replicaBindDN in the credentials object associated
with the replication agreement defined between the servers.
When kerberos is used to authenticate to the replica,
ibm-slapdMasterDNmust specify the DN representation of the
kerberos ID(e.g. ibm-kn=freddy@realml).When kerberos is used,
MasterServerPW is ignored.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2409
DBNAME( 'MasterDN''MasterDN' )
ACCESS-CLASS critical
LENGTH 1000 )

attributetypes=(1.3.18.0.2.4.2411
NAME 'ibm-slapdMasterPW'
DESC 'Bind password used by a replication supplier. The value has to
match the replicaBindPW in the credentials object associated with
the replication agreement defined between the servers. When kerberos
is used, MasterServerPWis ignored.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE
USAGE directoryOperation)
IBMAttributetypes=( 1.3.18.0.2.4.2411
DBNAME( 'MasterPW''MasterPW' )
ACCESS-CLASS critical )

attributetypes=( 1.3.18.0.2.4.2401
NAME 'ibm-slapdMasterReferral'
DESC 'URL of a master replica server (e.g.:

```

```

1daps://master.us.ibm.com:636)'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUEUSAGE directoryOperation)
IBMAttributetypes=( 1.3.18.0.2.4.2401
DBNAME( 'MasterReferral' 'MasterReferral' )
ACCESS-CLASS critical
LENGTH 256 )

attributetypes=( 1.3.18.0.2.4.2412
NAME 'ibm-slapdMaxEventsPerConnection'
DESC 'Maximum number of event notifications which can be registered
per connection. Minimum = 0 (unlimited) Maximum = 2,147,483,647'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE
directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2412
DBNAME( 'EventsPerCon' 'EventsPerCon' )
ACCESS-CLASS critical
LENGTH 11)

attributetypes=( 1.3.18.0.2.4.2405
NAME 'ibm-slapdMaxEventsTotal'
DESC 'Maximum total number of event notifications which can be
registered for all connections. Minimum = 0 (unlimited)Maximum =
2,147,483,647'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2405
DBNAME( 'MaxEventsTotal' 'MaxEventsTotal' )
ACCESS-CLASS critical
LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2439
NAME 'ibm-slapdMaxNumOfTransactions'
DESC 'Maximum number of transactions active at one time, 0 = unlimited.'
EQUALITY 2.5.13.29
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2439
DBNAME( 'MaxNumOfTrans' 'MaxNumOfTrans' )
ACCESS-CLASS critical
LENGTH 11
EQUALITY ORDERING SUBSTR APPROX )
attributetypes=( 1.3.18.0.2.4.2385
NAME 'ibm-slapdMaxOpPerTransaction'
DESC 'Maximum number of operations per transaction. Minimum = 1 Maximum = 500'
EQUALITY 2.5.13.29
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2385
DBNAME( 'MaxOpPerTrans' 'MaxOpPerTrans' )
ACCESS-CLASS critical
LENGTH 11
EQUALITY ORDERING APPROX )

attributetypes=( 1.3.18.0.2.4.2386
NAME 'ibm-slapdMaxTimeLimitOfTransactions'
DESC 'The maximum timeout value of a pending transaction in
seconds. 0 = unlimited'
EQUALITY 2.5.13.29
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2386
DBNAME( 'MaxTimeOfTrans' 'MaxTimeOfTrans' )
ACCESS-CLASS critical
LENGTH 11
EQUALITYORDERINGAPPROX )

attributetypes=( 1.3.18.0.2.4.2500
NAME 'ibm-slapdMigrationInfo'
DESC 'Information used to control migration of a component.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE directoryOperation )
IBMAttributetypes=(1.3.18.0.2.4.2500
DBNAME( 'slapdMigrationInf' 'slapdMigrationInf' )
ACCESS-CLASS critical
LENGTH 2048 )

attributetypes=( 1.3.18.0.2.4.2376
NAME 'ibm-slapdPagedResAllowNonAdmin'
DESC 'Whether or not the server should allow non-Administrator
bind for paged results requests on a search request.If thevalue
read from the ibmslapd.conf file is TRUE, the server willprocess
any client request,including those submitted by a userbinding
anonymously.If the value read from the ibmslapd.conf file is

```

```

FALSE, the server will process only those client requests submitted
by a user with Administrator authority. If a client requests paged
results with a criticality of TRUE or FALSE for a search operation,
does not have Administrator authority, and the value read from the
ibmslapd.conf file for this attribute is FALSE, the server will
return to the client with return code insufficientAccessRights - no
searching or paging will be performed.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2376
DBNAME( 'SlapdPagedNonAdmn' 'SlapdPagedNonAdmn' )
ACCESS-CLASS critical
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.2380
NAME 'ibm-slapdPagedResLmt'
DESC 'Maximum number of outstanding paged results search requests
allowed active simultaneously. Range = 0... If a client requests
a paged results operation, and a maximum number of outstanding paged
results are currently active, then the server will return to the
client with return code of busy - no searching or paging will be
performed.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2380
DBNAME( 'SlapdPagedResLmt' 'SlapdPagedResLmt' )
ACCESS-CLASS critical
LENGTH 11 )
attributetypes=( 1.3.18.0.2.4.2406
NAME 'ibm-slapdPlugin'
DESC 'A plug-in is a dynamically loaded library which extends the
capabilities of the server. An ibm-slapdPlugin attribute specifies
to the server how to load and initialize a plug-in library. The
syntax is: keyword filename init_function [args...]. The syntax
will be slightly different for each platform due to library
naming conventions.'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2406
DBNAME( 'slapdPlugin' 'slapdPlugin' )
ACCESS-CLASS critical
LENGTH 2000 )

attributetypes=( 1.3.18.0.2.4.2408
NAME 'ibm-slapdPort'
DESC 'TCP/IP ibm-slapdPort used for non-SSL connections.
Can not have the same value as ibm-slapdSecurePort. (IP ports are
unsigned, 16-bit integers in the range 1 - 65535)'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2408
DBNAME( 'slapdPort' 'slapdPort' )
ACCESS-CLASS critical
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.2402
NAME 'ibm-slapdPwEncryption'
DESC 'Must be one of { none | AES128 | AES192 | AES256 | crypt | sha | ssha | md5
| sha224 | sha256 | sha384 | sha512 | ssha224 | ssha256 | ssha384 | ssha512 }.
Specify the encoding mechanism for the user passwords before they are
stored in the directory. Defaults to none if unspecified. If the
value is set other than none, SASL digest-md5 bind will fail.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2402
DBNAME( 'PwEncryption' 'PwEncryption' )
ACCESS-CLASS critical
LENGTH 6 )

attributetypes=( 1.3.18.0.2.4.2413
NAME 'ibm-slapdReadOnly'
DESC 'Must be one of { TRUE | FALSE }. Specifies whether
the backend can be written to. Defaults to FALSE if unspecified. If
set to TRUE, the server will return LDAP_UNWILLING_TO_PERFORM (0x35)
in response to any client request which would change data in the
readOnly database.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2413
DBNAME( 'ReadOnly' 'ReadOnly' )
ACCESS-CLASS critical
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.2487

```

```

NAME 'ibm-slapdReferral'
DESC 'Specify the referral LDAP URL to pass back when the local
suffixes do not match the request. Used for superior referral
(i.e. ibm-slapdSuffix is not within the servers naming context).'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2487
DBNAME( 'Referral' 'Referral' )
ACCESS-CLASS critical
LENGTH 32700)
attributeTypes=( 1.3.18.0.2.4.3641
NAME 'ibm-slapdReplicateSecurityAttributes'
DESC 'Attribute to enable replication of security attributes
between master and read-only replica so that password policy
for account lockout can be strongly enforced in replication
topologies'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
attributeTypes=( 1.3.18.0.2.4.2437
NAME 'ibm-slapdSchemaAdditions'
DESC 'File path on the ibmslapd host machine containing additional
schema definitions used by the LDCF backend. Standard values are:
/etc/V3.modifiedSchemaOn Windows, forward slashes are allowed,
and a leading slash not preceded by a drive letter is assumed to be
rooted at the install directory (i.e.: /etc/V3.system.at=
D:\Program Files\IBM\ldap\etc\V3.system.at).'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2437
DBNAME( 'slapdSchemaAdditi' 'slapdSchemaAdditi' )
ACCESS-CLASS normal
LENGTH 1024)

attributeTypes=( 1.3.18.0.2.4.2363
NAME 'ibm-slapdSchemaCheck'
DESC 'Must be one of { V2 | V3 | V3_lenient }. Specifies schema
checking mechanism for add/modify operation. V2 = perform LDAP v2
checking. V3 = perform LDAP v3 checking. V3_lenient = not ALL
parent object classes are required. Only the immediate object class
is needed when adding entries.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2363
DBNAME( 'SchemaCheck' 'SchemaCheck' )
ACCESS-CLASS critical
LENGTH 10)

attributeTypes=( 1.3.18.0.2.4.2398
NAME 'ibm-slapdSecurePort'
DESC 'TCP/IP port used for SSL connections. Can not have the same
value as ibm-slapdPort. (IP ports are unsigned, 16-bit integers in
the range 1 - 65535)'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2398
DBNAME( 'SecurePort' 'SecurePort' )
ACCESS-CLASS critical
LENGTH 5)

attributeTypes=( 1.3.18.0.2.4.3637
NAME ( 'ibm-slapdSecurityProtocol' 'slapdSecurityProt' )
DESC 'Attribute used to set the protocol for secure communication.
The supported protocols are SSLV3, TLS10, TLS11 and TLS12.'
EQUALITY 1.3.6.1.4.1.1466.109.114.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
USAGE directoryOperation )
attributeTypes=( 1.3.18.0.2.4.2399
NAME 'ibm-slapdSecurity'
DESC 'Must be one of { none | SSL | SSLOnly }. Specifies types of
connections accepted by the server. none - server listens on
non-ssl port only. ssl - server listens on both ssl and non-ssl
ports. sslonly - server listens on ssl port only.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2399
DBNAME( 'Security' 'Security' )
ACCESS-CLASS critical
LENGTH 7)

attributeTypes=( 1.3.18.0.2.4.2397
NAME 'ibm-slapdSetenv'
DESC 'Server executes putenv() for all values of ibm-slapdSetenv
at startupto modify its own runtime environment. Shell variables

```

```

(%PATH% or ¥24LANG) will not be expanded. The only current use for
this attribute is to setDB2CODEPAGE=1208, which is required if
using UCS-2 (Unicode) databases.'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE directoryOperation)
IBMAttributeTypes=( 1.3.18.0.2.4.2397
DBNAME( 'slapSetenv','slapSetenv')
ACCESS-CLASS critical
LENGTH 2000)

attributetypes=( 1.3.18.0.2.4.2396
NAME 'ibm-slapdSizeLimit'
DESC 'Maximum number of entries to return from search, regardless of
any sizelimit that may have been specified on the client search
request.Range = 0... If a client has passed a limit, then the
smaller value ofthe client value and the value read from
ibmslapd.conf will be used. If aclient has not passed a limit and
has bound as admin DN, then the limitwill be considered unlimited.
If the client has not passed a limit and has not bound as admin DN,
then the limit will be that which was readfrom ibmslapd.conf file.
0 = unlimited.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUEUSAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2396
DBNAME( 'SizeLimit','SizeLimit' )
ACCESS-CLASS critical
LENGTH 11)

attributetypes=(1.3.18.0.2.4.2381
NAME 'ibm-slapdSortKeyLimit'
DESC 'Maximum number of sort conditions (keys) that can be specified
on a single search request.Range = 0... If a client has passed a
search request with more sort keys than the limit allows, and the
sorted search control criticality is FALSE, then the server will
honor the value read fromibmslapd.conf and ignore any sort keys
encountered after the limit hasbeen reached - searching and
sorting will be performed. If a client haspassed a search request
with more keys than the limit allows, and thesorted search control
criticality is TRUE, then the server will return tothe client with
return code of adminLimitExceeded - no searching or sorting
will be performed.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2381
DBNAME( 'SlapdSortKeyLimit' 'SlapdSortKeyLimit' )
ACCESS-CLASS critical
LENGTH 11)

attributetypes=(1.3.18.0.2.4.2377
NAME 'ibm-slapdSortSrchAllowNonAdmin'
DESC 'Whether or not the server should allow non-Administrator bind
for sort on a search request. If the value read from the
ibmslapd.conf file is TRUE, the server will process any client
request, including those submitted by a user binding anonymously.
If the value read from theibmslapd.conf file is FALSE, the server
will process only those clientrequests submitted by a user with
Administrator authority.If a clientrequests sort with a
criticality of TRUE for a search operation, does nothave
Administrator authority, and the value read from the ibmslapd.conf
file for this attribute is FALSE, the server will return to the
client with returncode insufficientAccessRights - no searching or
sorting will be performed.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation)
IBMAttributeTypes=( 1.3.18.0.2.4.2377
DBNAME( 'SlapdSortNonAdmin' 'SlapdSortNonAdmin' )
ACCESS-CLASS critical
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.2395
NAME 'ibm-slapdSslAuth'
DESC 'Must be one of { serverauth | serverclientauth}.Specify
authenticationtype for ssl connection.serverauth - supports
server authentication at theclient.serverclientauth - supports
both server and client authentication.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation)
IBMAttributeTypes=( 1.3.18.0.2.4.2395
DBNAME( 'slapdSslAuth','slapdSslAuth')
ACCESS-CLASS critical
LENGTH 16)

attributetypes=( 1.3.18.0.2.4.2389
NAME 'ibm-slapdSslCertificate'
DESC 'Specify the label that identifies the servers Personal
Certificatein the key database file.This label is specified

```

```

when the servers privatekey and certificate are created with the
ikmgui application. Ifibm-slapdSslCertificate is not defined, the
default private key, as defined in the key database file, is used by
the LDAP server for SSL connections.'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2389
DBNAME( 'SslCertificate' 'SslCertificate' )
ACCESS-CLASS critical
LENGTH 128 )

attributetypes=(1.3.18.0.2.4.2429
NAME 'ibm-slapdSslCipherSpec'
ESC 'SSL Cipher Spec Value must be set to DES-56, RC2-40-MD5,
RC4-128-MD5,RC4-128-SHA, RC4-40-MD5,TripleDES-168, or AES.It
identifies the allowable encryption/decryption methods for
establishing a SSL connection between LDAP clients and the server.'
EQUALITY 1.3.6.1.4.1.1466.109.114.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
USAGE directoryOperation )
IBMAttributeTypes=(1.3.18.0.2.4.2429
DBNAME( 'slapdSslCipherSpe','slapdSslCipherSpe' )
ACCESS-CLASS normal
LENGTH 30)

attributetypes=( 1.3.18.0.2.4.2362
NAME 'ibm-slapdSslCipherSpecs'
DESC 'This attribute is deprecated in favor of
ibm-slapdSslCipherSpec. Specifies a decimal number which identifies
the allowable encryption/decryption methods for establishing a SSL
connectionbetween LDAP client(s) and the server.This number
represents the availabilityof the encryption/decryption methods
supported by the LDAP server.The pre-defined Cipher values and
their descriptions are: SLAPD_SSL_TRIPLE_DES_SHA_US0x0A Triple DES
encryption with a 168-bit key and a SHA-1 MAC LAPD_SSL_DES_SHA_US
0x09DES encryption with a 56-bit key and a SHA-1 MAC
SLAPD_SSL_RC4_SHA_US 0x05 RC4 encryption with a 128-bit key and a
SHA-1 MAC SLAPD_SSL_RC4_MD5_US0x04 RC4 encryption with a 128-bit
key and a MD5 MAC SLAPD_SSL_RC4_MD5_EXPORT 0x03 RC4 encryption
with a 40-bit key and a MD5 MAC SLAPD_SSL_RC2_MD5_EXPORT 0x06 RC2
encryption with a 40-bit key and a MD5 MAC'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2362
DBNAME( 'SslCipherSpecs','SslCipherSpecs' )
ACCESS-CLASS critical
LENGTH 11 )

attributetypes=( 1.3.18.0.2.4.2375
NAME 'ibm-slapdSSLKeyDatabase'
DESC 'File path to the LDAP servers SSL key database file. This key
databasefile is used for handling SSL connections from LDAP
clients, as well as forcreating secure SSL connections to replica
LDAP servers. On Windows, forwardslashes are allowed, and a
leading slash not preceded by a drivespecifier (D:) is assumed to
be rooted at the install directory (i.e.: /etc/key.kdb = D:\Program
Files\IBM\ldap\etc\key.kdb).'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2375
DBNAME( 'slapdSSLKeyDataba' 'slapdSSLKeyDataba' )
ACCESS-CLASS critical
LENGTH 1024)

attributetypes=(1.3.18.0.2.4.2438
NAME 'ibm-slapdSSLKeyDatabasePW'
DESC 'Specify the password associated with the LDAP servers SSL key
database file,as specified on the ibm-slapdSslKeyDatabase
parameter.If the LDAP servers keydatabase file has an associated
password stash file, then the ibm-slapdSslKeyDatabasePW parameter
can be omitted, or set toibm-slapdSslKeyDatabasePW = none.
Note:
The password stash file mustbe located in the same
directory as the key database file and it must havethe same file
name as the key database file, but with an extension of .sth,
instead of .kdb'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUEUSAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2438
DBNAME( 'slapdSSLKeyDPW','slapdSSLKeyDPW' )
ACCESS-CLASS normal )

attributetypes=(1.3.18.0.2.4.2392
NAME 'ibm-slapdSslKeyRingFile'
DESC 'file path to the LDAP servers SSL key database file. This key
databasefile is used for handling SSL connections from LDAP
clients, as well as forcreating secure SSL connections to replica

```

LDAP servers. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive specifier (D:) is assumed to be rooted at the install directory (i.e.:/etc/key.kdb = D:\Program Files\IBM\lpad\etc\key.kdb).'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation)
IBMAttributeTypes=(1.3.18.0.2.4.2392
 DBNAME('SslKeyRingFile' 'SslKeyRingFile')
 ACCESS-CLASS critical
 LENGTH 1024)

attributetypes=(1.3.18.0.2.4.2390
NAME 'ibm-slappSslKeyRingFilePW'
DESC 'Specify the password associated with the LDAP servers SSL key database file, as specified on the ibm-slappSslKeyRingFile parameter. If the LDAP servers key database file has an associated password stash file, then the ibm-slappSslKeyRingFilePW parameter can be omitted, or set to ibm-slappSslKeyRingFilePW = none.
Note:
The password stash file must be located in the same directory as the key database file and it must have the same file name as the key database file, but with an extension of .sth, instead of .kdb.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE
USAGE directoryOperation)
IBMAttributeTypes=(1.3.18.0.2.4.2390
 DBNAME('SslKeyRingFilePW' 'SslKeyRingFilePW')
 ACCESS-CLASS critical)

attributetypes=(1.3.18.0.2.4.2388
NAME 'ibm-slappSuffix'
DESC 'Specifies a naming context to be stored in this backend.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
USAGE directoryOperation)
IBMAttributeTypes=(1.3.18.0.2.4.2388
 DBNAME('slappSuffix' 'slappSuffix')
 ACCESS-CLASS critical
 LENGTH 1000)
attributeTypes=(1.3.18.0.2.4.3639
NAME 'ibm-slappSuiteBMode'
DESC 'Attribute used to set the restrictive subset of the NIST SP 800-131A specification.
The supported Suite B modes are 128 and 192'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE USAGE directoryOperation)
attributetypes=(1.3.18.0.2.4.2480
NAME 'ibm-slappSupportedWebAdmVersion'
DESC 'This attribute defines the earliest version of the web administration console that supports configuration of this server.'
EQUALITY 2.5.13.2
ORDERING 2.5.13.3
SUBSTR 2.5.13.4
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation)
IBMAttributeTypes=(1.3.18.0.2.4.2480
 DBNAME('slappSupWebAdmVer' 'slappSupWebAdmVer')
 ACCESS-CLASS normal
 LENGTH 256)

attributetypes=(1.3.18.0.2.4.2393
NAME 'ibm-slappSysLogLevel'
DESC 'Must be one of { l | m | h }. Level at which debugging and operation statistics are logged in ibm-slapp.log file. h - high (verbose), m - medium, l - low (terse).'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation)
IBMAttributeTypes=(1.3.18.0.2.4.2393
 DBNAME('SysLogLevel' 'SysLogLevel')
 ACCESS-CLASS critical
 LENGTH 1)

attributetypes=(1.3.18.0.2.4.3412
NAME 'ibm-slappTombstoneEnabled'
DESC 'Enable or Disable tombstones to record deleted entries.
The default value is FALSE'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation)
IBMAttributeTypes=(1.3.18.0.2.4.3412
 DBNAME('slappTSEnabled' 'slappTSEnabled')
 ACCESS-CLASS normal
 LENGTH 5)

attributetypes=(1.3.18.0.2.4.3413
NAME 'ibm-slappTombstoneLifetime'

```

DESC 'Specifies the time in hours that tombstones may live.
When the time limit is reached the tombstones will be deleted
from the database.'
EQUALITY 2.5.13.14
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.3413
DBNAME( 'slapdTLifetime' 'slapdTLifetime' )
ACCESS-CLASS normal
LENGTH 11 )

attributeTypes=( 1.3.18.0.2.4.2391
NAME 'ibm-slapdTimeLimit'
DESC 'Maximum number of number of seconds to spend on search
request, regardless of any timelimit that may have been specified
on the client request. Range = 0.... If a client has passed a
limit, then the smaller value of the client value and the value
read from ibmslapd.conf will be used. If a client has not passed a
limit and has bound as admin DN, then the limit will be considered
unlimited. If the client has not passed a limit and has not bound as
admin DN, then the limit will be that which was read from
ibmslapd.conf file. 0 = unlimited.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2391
DBNAME( 'TimeLimit' 'TimeLimit' )
ACCESS-CLASS critical
LENGTH 11 )

attributeTypes=( ibm-slapdStartupTraceEnabled-oid
NAME 'ibm-slapdTraceEnabled'
DESC 'Must be one of { TRUE | FALSE }. Specifies whether trace information is to be
collected at server startup'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( ibm-slapdStartupTraceEnabled-oid
ACCESS-CLASS normal
LENGTH 5 )

attributeTypes=( ibm-slapdTraceMessageLevel-oid
NAME 'ibm-slapdTraceMessageLevel'
DESC 'any value that would be acceptable after the command line -h option, sets
Debug message level'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( ibm-slapdTraceMessageLevel-oid
ACCESS-CLASS normal
LENGTH 16 )

attributeTypes=( ibm-slapdTraceMessageLog-oid
NAME 'ibm-slapdTraceMessageLog'
DESC 'File path or device on ibmslapd host machine to which
LDAP C API and Debug macro messages will be written.
On Windows, forward slashes are allowed, and a leading
slash not preceded by a drive letter is assumed to be rooted at
the install directory
(i.e., /tmp/tracemsg.log = C:\Program Files\IBM\ldap\tmp\tracemsg.log).'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( ibm-slapdTraceMessageLog-oid
ACCESS-CLASS normal
LENGTH 1024 )

attributeTypes=( 1.3.18.0.2.4.2384
NAME 'ibm-slapdTransactionEnable'
DESC 'If FALSE, globally disables transaction support; the server
will reject all StartTransaction requests with the response
LDAP_UNWILLING_TO_PERFORM.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributeTypes=( 1.3.18.0.2.4.2384
DBNAME( 'TransactionEnable' 'TransactionEnable' )
ACCESS-CLASS critical
LENGTH 5 )
attributeTypes=( 1.3.18.0.2.4.3638 NAME 'ibm-slapdUniqueAttrForBindWithValue' DESC
'Configuration attribute used for enabling binds using value of a unique attribute.
For example, mail, employeeNumber etc.' EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE USAGE directoryOperation )
attributeTypes=( 1.3.18.0.2.4.3646 NAME 'ibm-slapdBindWithUniqueAttrsEnabled' DESC
'Configuration attribute used for enabling binds using combination of a unique attribute and
value. For example, mail=xyz@ibm.com, employeeNumber=123456 etc.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 {5}
SINGLE-VALUE
USAGE directoryOperation

```

```

)
attributetypes=( 1.3.18.0.2.4.2499
NAME 'ibm-slapdUseProcessIdPW'
DESC 'If set to true the server will use the user login ID
associated with the ibmslapd process to connect to the database.If
set to false the server will use the ibm-slapddbUserID and
ibm-slapddbUserPW values to connect to the database.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2499
DBNAME( 'useprocidpw''useprocidpw' )
ACCESS-CLASS normal
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.2436
NAME 'ibm-slapdVersion'
DESC 'IBM Slapd version Number'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2436
DBNAME( 'slapdVersion''slapdVersion' )
ACCESS-CLASS normal
LENGTH 1024 )

attributetypes=( 1.3.18.0.2.4.2327
NAME 'ibm-supportedReplicationModels'
DESC 'Advertises in the Root DSE the OIDs of replication models
supported by the server'
EQUALITY 1.3.6.1.4.1.1466.109.114.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
NO-USER-MODIFICATION
USAGE dSAOperation )
IBMAttributetypes=( 1.3.18.0.2.4.2327
DBNAME( 'supportedReplicat''supportedReplicat' )
ACCESS-CLASS system
LENGTH 240 )

attributetypes=( 1.3.18.0.2.4.470
NAME 'IBMAttributeTypes'
DESC ''
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.470
DBNAME( 'IBMAttributeTypes''IBMAttributeTypes' )
ACCESS-CLASS normal
LENGTH 256 )

attributetypes=( 1.3.6.1.4.1.1466.101.120.16
NAME 'ldapSyntaxes'
DESC 'Servers MAY use this attribute to list the syntaxes which are
implemented. Each value corresponds to one syntax.'
EQUALITY 2.5.13.30
SYNTAX 1.3.6.1.4.1.1466.115.121.1.54
USAGE directoryOperation )
IBMAttributetypes=( 1.3.6.1.4.1.1466.101.120.16
DBNAME( 'ldapSyntaxes''ldapSyntaxes' )
ACCESS-CLASS system
LENGTH 256 EQUALITY )

attributetypes=( 2.5.21.4
NAME 'matchingRules'
DESC 'This attribute is typically located in the subschema entry.'
EQUALITY 2.5.13.30
SYNTAX 1.3.6.1.4.1.1466.115.121.1.30
USAGE directoryOperation )
IBMAttributetypes=( 2.5.21.4
DBNAME( 'matchingRules''matchingRules' )
ACCESS-CLASS system
LENGTH 256
EQUALITY )

attributetypes=( 2.5.21.8
NAME 'matchingRuleUse'
DESC 'This attribute is typically located in the subschema entry.'
EQUALITY 2.5.13.30
SYNTAX 1.3.6.1.4.1.1466.115.121.1.31
USAGE directoryOperation )
IBMAttributetypes=( 2.5.21.8
DBNAME( 'matchingRuleUse''matchingRuleUse' )
ACCESS-CLASS system
LENGTH 256
EQUALITY )

attributetypes=( 2.5.4.31
NAME 'member'
DESC 'Identifies the distinguished names for each member of the group.'
SUP 2.5.4.49

```

```

EQUALITY 2.5.13.1
USAGE userApplications )
IBMAttributetypes=( 2.5.4.31
DBNAME( 'member' 'member' )
ACCESS-CLASS normal
LENGTH 1000
EQUALITY )

attributetypes=( 2.5.18.4
NAME 'modifiersName'
DESC 'Contains the last modifier of a directory entry.'
EQUALITY 2.5.13.1 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 2.5.18.4
DBNAME( 'ldap_entry' 'modifier' )
ACCESS-CLASS system
LENGTH 1000
EQUALITY )

attributetypes=( 2.5.18.2
NAME 'modifyTimestamp'
DESC 'Contains the time of the last modification of the directory
entry.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 2.5.18.2
DBNAME( 'ldap_entry' 'modify_Timestamp' )
ACCESS-CLASS system
LENGTH 26 )

attributetypes=( 2.5.4.41
NAME 'name' DESC 'The name attribute type
is the attribute supertype from which string attribute types
typically used for naming may be formed. It is unlikely that values
of this type itself will occur in an entry.'
EQUALITY 1.3.6.1.4.1.1466.109.114.2
SUBSTR 2.5.13.4
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE userApplications )
IBMAttributetypes=( 2.5.4.41
DBNAME( 'name' 'name' )
ACCESS-CLASS normal
LENGTH 32700
EQUALITY
SUBSTR )

attributetypes=( 2.5.21.7
NAME 'nameForms'
DESC 'This attribute is typically located in the subschema entry.'
EQUALITY 2.5.13.30
SYNTAX 1.3.6.1.4.1.1466.115.121.1.35
USAGE directoryOperation )
IBMAttributetypes=( 2.5.21.7
DBNAME( 'nameForms' 'nameForms' )
ACCESS-CLASS normal
LENGTH 256
EQUALITY )

attributetypes=( 1.3.6.1.4.1.1466.101.120.5
NAME 'namingContexts'
DESC 'The values of this attribute correspond to naming contexts
which this server masters or shadows.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
USAGE dSAOperation )
IBMAttributetypes=( 1.3.6.1.4.1.1466.101.120.5
DBNAME( 'namingContexts' 'namingContexts' )
ACCESS-CLASS normal
LENGTH 1000 )

attributetypes=( 2.16.840.1.113730.3.1.11
NAME 'newSuperior'
DESC 'Specifies the name of the entry that will become the
immediate superior of the existing entry, when processing a modDN
operation.'
EQUALITY 2.5.13.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE userApplications )
IBMAttributetypes=( 2.16.840.1.113730.3.1.11
DBNAME( 'newSuperior' 'newSuperior' )
ACCESS-CLASS normal
LENGTH 1000
EQUALITY APPROX )

attributetypes=( 1.3.1.1.4.1.453.16.2.103
NAME 'numSubordinates'

```

```

DESC 'Counts the number of children of this entry.'
EQUALITY 2.5.13.14
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.1.1.4.1.453.16.2.103
DBNAME( 'numSubordinates' 'numSubordinates' )
ACCESS-CLASS system
LENGTH 11

attributetypes=( 2.5.4.10
NAME ( 'o' 'organizationName' 'organization' )
DESC 'This attribute contains the name of an organization (organizationName).'
SUP 2.5.4.41
EQUALITY 1.3.6.1.4.1.1466.109.114.2
SUBSTR 2.5.13.4
USAGE userApplications )
IBMAttributetypes=( 2.5.4.10
DBNAME( 'o' 'o' )
ACCESS-CLASS normal
LENGTH 128 )

attributetypes=( 2.5.4.0
NAME 'objectClass'
DESC 'The values of the objectClass attribute describe the kind of
object which an entry represents.'
EQUALITY 2.5.13.0
SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
USAGE userApplications )
IBMAttributetypes=( 2.5.4.0
DBNAME( 'objectClass' 'objectClass' )
ACCESS-CLASS normal
LENGTH 128
EQUALITY )

attributetypes=( 2.5.21.6
NAME 'objectClasses'
DESC 'This attribute is typically located in the subschema entry.'
EQUALITY 2.5.13.30
SYNTAX 1.3.6.1.4.1.1466.115.121.1.37
USAGE directoryOperation )
IBMAttributetypes=( 2.5.21.6
DBNAME( 'objectClasses' 'objectClasses' )
ACCESS-CLASS system
LENGTH 256
EQUALITY )

attributetypes=( 1.3.18.0.2.4.289
NAME 'ownerPropagate'
DESC 'Indicates whether the entryOwner applies on entry or subtree.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.289
DBNAME( 'ownerPropagate' 'ownerPropagate' )
ACCESS-CLASS restricted
LENGTH 5 )

attributetypes=( 2.5.4.11
NAME ( 'ou' 'organizationalUnit' 'organizationalUnitName' )
DESC 'This attribute contains the name of an organization (organizationName).'
SUP 2.5.4.41
EQUALITY 1.3.6.1.4.1.1466.109.114.2
SUBSTR 2.5.13.4
USAGE userApplications )
IBMAttributetypes=( 2.5.4.11
DBNAME( 'ou' 'ou' )
ACCESS-CLASS normal
LENGTH 128 )

attributetypes=( 2.5.4.32
NAME 'owner'
DESC 'Identifies the distinguished name (DN) of the person responsible
for the entry.'
SUP 2.5.4.49
EQUALITY 2.5.13.1
USAGE userApplications )
IBMAttributetypes=( 2.5.4.32
DBNAME( 'owner' 'owner' )
ACCESS-CLASS normal
LENGTH 1000 )

attributetypes=( 1.3.18.0.2.4.290
NAME 'ownerSource'
DESC 'Indicates the distinguished name of the entry whose entryOwner
value is being applied to the entry.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.290
DBNAME( 'ownerSource' 'ownerSource' )

```

```

ACCESS-CLASS system
LENGTH 1000 )

attributetypes=( 1.3.6.1.4.1.42.2.27.8.1.17
NAME 'pwdAccountLockedTime'
DESC 'Specifies the time that the users account was locked'
EQUALITY 2.5.13.27
ORDERING 2.5.13.28
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.6.1.4.1.42.2.27.8.1.17
DBNAME( 'pwdAccLockTime' 'pwdAccLockTime' )
ACCESS-CLASS critical
LENGTH 30 )

attributetypes=( 1.3.6.1.4.1.42.2.27.8.1.16
NAME 'pwdChangedTime'
DESC 'Specifies the last time the entries password was changed'
EQUALITY 2.5.13.27
ORDERING 2.5.13.28
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.6.1.4.1.42.2.27.8.1.16
DBNAME( 'pwdChangedTime' 'pwdChangedTime' )
ACCESS-CLASS critical
LENGTH 30 )

attributetypes=( 1.3.6.1.4.1.42.2.27.8.1.18
NAME 'pwdExpirationWarned'
DESC 'The time the user was first warned about the coming expiration
of the password'
EQUALITY 2.5.13.27
ORDERING 2.5.13.28
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.6.1.4.1.42.2.27.8.1.18
DBNAME( 'pwdExpireWarned' 'pwdExpireWarned' )
ACCESS-CLASS critical
LENGTH 30)

attributetypes=( 1.3.6.1.4.1.42.2.27.8.1.19
NAME 'pwdFailureTime'
DESC 'The timestamps of the last consecutive authentication
failures'
EQUALITY 2.5.13.27
ORDERING 2.5.13.28
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
USAGE directoryOperation )
IBMAttributetypes=( 1.3.6.1.4.1.42.2.27.8.1.19
DBNAME( 'pwdFailureTime' 'pwdFailureTime' )
ACCESS-CLASS critical
LENGTH 30 )

attributetypes=( 1.3.6.1.4.1.42.2.27.8.1.21
NAME 'pwdGraceUseTime'
DESC 'The timestamps of the grace login once the password has
expired'
EQUALITY 2.5.13.27
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
USAGE directoryOperation )
IBMAttributetypes=( 1.3.6.1.4.1.42.2.27.8.1.21
DBNAME( 'pwdGraceUseTime' 'pwdGraceUseTime' )
ACCESS-CLASS critical
LENGTH 30)

attributetypes=( 1.3.6.1.4.1.42.2.27.8.1.20
NAME 'pwdHistory'
DESC 'The history of users passwords'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE directoryOperation )
IBMAttributetypes=( 1.3.6.1.4.1.42.2.27.8.1.20
DBNAME( 'pwdHistory' 'pwdHistory' )
ACCESS-CLASS critical
LENGTH 1024 )

attributetypes=( 1.3.6.1.4.1.42.2.27.8.1.22
NAME 'pwdReset'
DESC 'Indicates that the password has been reset.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.6.1.4.1.42.2.27.8.1.22
DBNAME( 'pwdReset' 'pwdReset' )
ACCESS-CLASS critical
LENGTH 5 )

attributetypes=( 1.3.18.0.2.4.299

```

```

NAME 'replicaBindDN'
DESC 'Distinguished name to use on LDAP bind to the remote replica'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.299
DBNAME( 'replicaBindDN''replicaBindDN' )
ACCESS-CLASS critical
LENGTH 1000 )

attributetypes=( 1.3.18.0.2.4.302
NAME 'replicaBindMethod'
DESC 'LDAP bind type to use on LDAP bind to replica.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.302
DBNAME( 'replicaBindMethod''replicaBindMethod' )
ACCESS-CLASS normal
LENGTH 100 )

attributetypes=( 1.3.18.0.2.4.300
NAME ( 'replicaCredentials''replicaBindCredentials')
DESC 'Credentials to use on LDAP bind to the remote replica'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.300
DBNAME( 'replicaCred''replicaCred' )
ACCESS-CLASS critical )

attributetypes=( 1.3.18.0.2.4.298
NAME 'replicaHost'
DESC 'Hostname of the remote replica'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.298
DBNAME( 'replicaHost''replicaHost' )
ACCESS-CLASS normal
LENGTH 100 )

attributetypes=( 1.3.18.0.2.4.301
NAME 'replicaPort'
DESC 'TCP/IP port that the replica server is listening on.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.301
DBNAME( 'replicaPort''replicaPort' )
ACCESS-CLASS normal
LENGTH 10 )

attributetypes=( 1.3.18.0.2.4.304
NAME 'replicaUpdateTimeInterval'
DESC 'Specifies the time between replica update transmissions from
master to slave replica.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.304
DBNAME( 'replicaUpdateInt''replicaUpdateInt' )
ACCESS-CLASS normal
LENGTH 20 )

attributetypes=( 1.3.18.0.2.4.303
NAME 'replicaUseSSL'
DESC 'Signifies whether replication flows should be protected using
SSL communications.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.303
DBNAME( 'replicaUseSSL''replicaUseSSL' )
ACCESS-CLASS normal
LENGTH 10 )

attributetypes=( 2.16.840.1.113730.3.1.34
NAME 'ref'
DESC 'standard Attribute'
EQUALITY 2.5.13.5
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
USAGE userApplications )
IBMAttributetypes=( 2.16.840.1.113730.3.1.34
DBNAME( 'ref''ref' )
ACCESS-CLASS normal
LENGTH 100 )

```

```

attributetypes=( 2.5.4.34
NAME 'seeAlso'
DESC 'Identifies anotherdirectory server entry that may contain information
related to this entry.'
SUP 2.5.4.49
EQUALITY 2.5.13.1
USAGE userApplications )
IBMAttributetypes=( 2.5.4.34
DBNAME( 'seeAlso' 'seeAlso' )
ACCESS-CLASS normal
LENGTH 1000 )

attributetypes=( 2.5.18.10
NAME 'subschemaSubentry'
DESC 'The value of this attribute is the name of a subschema entry
in which the server makes available attributes specifying the
schema.'
EQUALITY 2.5.13.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 2.5.18.10
DBNAME( 'subschemaSubent' 'subschemaSubent' )
ACCESS-CLASS system
LENGTH 1000
EQUALITY )

attributetypes=( 1.3.18.0.2.4.819
NAME 'subtreeSpecification'
DESC 'Identifies a collection of entries that are located at the
vertices of a single subtree.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE directoryOperation )
IBMAttributetypes=( 1.3.18.0.2.4.819
DBNAME( 'subtreeSpec' 'subtreeSpec' )
ACCESS-CLASS system
LENGTH 2024 )

attributetypes=( 1.3.6.1.4.1.1466.101.120.7
NAME 'supportedExtension'
DESC 'The values of this attribute are OBJECT IDENTIFIERS
identifying the supported extended operations which the server
supports.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
USAGE dSAOperation )
IBMAttributetypes=( 1.3.6.1.4.1.1466.101.120.7
DBNAME( 'supportedExtensio' 'supportedExtensio' )
ACCESS-CLASS normal
LENGTH 256 )

attributetypes=( 1.3.6.1.4.1.1466.101.120.15
NAME 'supportedLDAPVersion'
DESC 'The values of this attribute are the versions of the LDAP
protocol which the server implements.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
USAGE dSAOperation )
IBMAttributetypes=( 1.3.6.1.4.1.1466.101.120.15
DBNAME( 'supportedLDAPVers' 'supportedLDAPVers' )
ACCESS-CLASS normal
LENGTH 11 )

attributetypes=( 1.3.6.1.4.1.1466.101.120.14
NAME 'supportedSASLMechanisms'
DESC 'The values of this attribute are the names of supported SASL
mechanisms which the server supports.'
EQUALITY 2.5.13.2
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE dSAOperation )
IBMAttributetypes=( 1.3.6.1.4.1.1466.101.120.14
DBNAME( 'supportedSASLMech' 'supportedSASLMech' )
ACCESS-CLASS normal LENGTH 2048)

attributetypes=( 2.16.840.1.113730.3.1.6
NAME 'targetDN'
DESC 'Defines the distinguished name of an entry that was added,
modified, or deleted on a supplier server. In the case of a modrdn
operation, the targetDn contains the distinguished name of the
entry before it was modified.'
EQUALITY 2.5.13.1
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE
NO-USER-MODIFICATION
USAGE userApplications )
IBMAttributetypes=( 2.16.840.1.113730.3.1.6
DBNAME( 'targetDN' 'targetDN' )
ACCESS-CLASS normal
LENGTH 1000
EQUALITY APPROX)

```

付録 J. サーバー・インスタンス間の両方向の暗号化の同期

以下に示す手順を使用して、サーバー・インスタンス間の両方向の暗号化を同期できます。

このタスクについて

複製を使用する場合、分散ディレクトリーを使用する場合、またはサーバー・インスタンス間で LDIF データをインポートおよびエクスポートする場合、最高のパフォーマンスを得るため、サーバー・インスタンスの暗号化を同期させる必要があります。

サーバー・インスタンスが既に存在し、その 1 番目のサーバー・インスタンスと暗号化を同期させる 2 番目のサーバー・インスタンスがある場合は、次のような処理を行う **前に**、その後に説明する手順を実施してください。

- 2 番目のサーバー・インスタンスの始動
- 2 番目のサーバー・インスタンスからの、**idsbulkload** コマンドの実行
- 2 番目のサーバー・インスタンスからの、**idsldif2db** コマンドの実行

2 つのサーバー・インスタンスの暗号化を同期させるには、次の手順で行います。ここでは、1 番目のサーバー・インスタンスはすでに作成されているものと想定しています。

手順

1. 2 番目のサーバー・インスタンスを作成します。ただし、このサーバー・インスタンスは始動させません。次に、作成した 2 番目のサーバー・インスタンスで **idsbulkload** コマンド、または **idsldif2db** コマンドを実行します。
2. 2 番目のサーバー・インスタンスで **idsgendirksf** ユーティリティを使用して、最初のサーバー・インスタンスから **ibmslapddir.ksf** ファイル (鍵 **stash** ファイル) を再作成します。このファイルは、2 番目のサーバー・インスタンスのオリジナルの **ibmslapddir.ksf** ファイルを置換するために使用します。**idsgendirksf** ユーティリティに関する詳細については、「*IBM Security Directory Server Version 6.3 Command Reference*」の **idsgendirksf** コマンド情報を参照してください。このファイルは、Windows システムの場合は **idsslapd-instance_name\etc** ディレクトリー、AIX、Linux、および Solaris システムの場合は **idsslapd-instance_name/etc** ディレクトリーに入っています。(**instance_name** は、サーバー・インスタンスの名前です)。
3. 2 番目のサーバー・インスタンスを始動し、この 2 番目のサーバー・インスタンス上で **idsbulkload** コマンド、または **idsldif2db** コマンドを実行します。

タスクの結果

これでサーバー・インスタンスが暗号的に同期し、AES 暗号化データが正常にロードされるようになります。この手順でのサーバー・インスタンスは 2 つですが、サーバー・インスタンスのグループで暗号化を同期させることが必要な場合があります。注: LDIF データをインポートする場合、LDIF インポート・ファイルが LDIF

データをインポートするサーバー・インスタンスと暗号同期化していないと、LDIF インポート・ファイルの AES 暗号化された項目はインポートされません。新規ディレクトリー・サーバー・インスタンスを作成し、その新規ディレクトリー・サーバー・インスタンスと他のディレクトリー・サーバー・インスタンスとで暗号化を同期させる場合は、以下の手順を実行します。

1. 元のサーバーで次の検索を実行し、暗号化ソルト値を入手します。

```
ldapsearch -D adminDN -w adminPw -b "cn=crypto,cn=localhost" objectclass=* ibm-slapdCryptoSalt
```
2. 次のような値が返されます。ibm-slapdCryptoSalt=d?TRm\$'ucc5m。等号 (=) の後のストリングの部分が、暗号化ソルト値です。この例では、暗号化ソルトの値は d?TRm\$'ucc5m です。
3. 元のサーバーの作成時に指定された暗号化シード値を見つけます。
4. 以下のいずれかの方法で新規サーバーを作成します。
 - インスタンス管理ツールを使用し、「暗号化シード・ストリング」フィールドに元のサーバーの暗号化シードの値を入力して、「暗号化ソルト・ストリング」フィールドに元のサーバーの暗号化ソルトの値を入力します。
 - **idsicrt** コマンドを使用し、**-e encryptionseed** と **-g encryptsalt** オプションを指定します。

付録 K. フィルターに掛けられた ACL およびフィルターに掛けられていない ACL – サンプル LDIF ファイル

ここに示す情報を使用して実際に操作してみることで、管理者は ACL モデルを完全に理解できます。ディレクトリーのサンプル ACL を使用してサンプル・データを作成し、各項目の ACL の有効性をチェックし、ACL スキーマが適切に必要なアクセスを制御するか確認します。

フィルター ACL と非フィルター ACL との組み合わせを含むサンプル LDIF ファイルが付属されています。このサンプル LDIF ファイルは、ディレクトリー・サーバーにロードできます。

このサンプル LDIF ファイルには、5 レベルのディレクトリー・ツリー上にサフィックス項目、2 つのユーザー項目、17 の追加エントリーが広がっています。各項目には 2 桁の指定があります。最初の桁は、ディレクトリー・ツリー内での項目のレベルを示します。また、項目にはレベルごとに左から右に向かって順番に番号が付けられます。この番号付け形式は 2 桁目に反映されています。

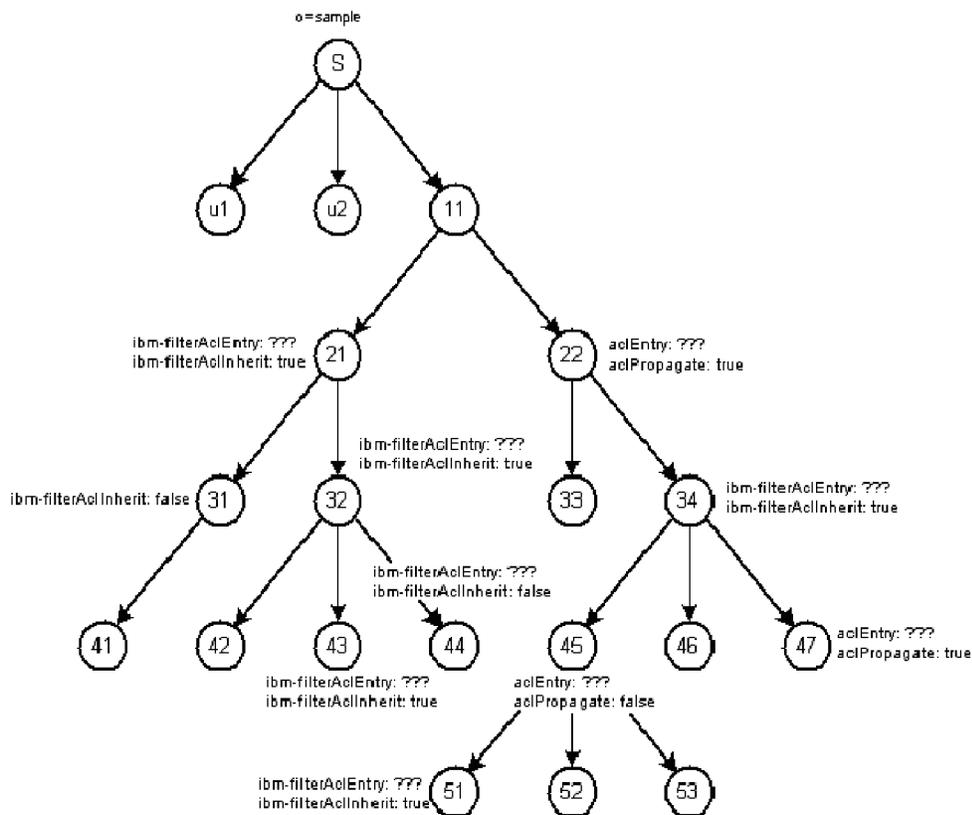


図 21. フィルターに掛けられた ACL およびフィルターに掛けられていない ACL

LDIF File:
version: 1

```

dn: o=sample
objectclass: organization
objectclass: top
o: sample

dn: cn=User1, o=sample
cn: User1
sn: User
objectclass: person
objectclass: top
userPassword: User1

dn: o=Level11, o=sample
o: Level11
objectclass: organization
objectclass: top

dn: o=Level21, o=Level11, o=sample
o: Level21
objectclass: organization
objectclass: top
ibm-filterAclEntry: access-id:CN=USER1,o=sample:(o=Level32):normal:rwc:
sensitive:rsc:critical:rsc

dn: o=Level31, o=Level21, o=Level11, o=sample
o: Level31
objectclass: organization
objectclass: top
ibm-filterAclInherit: FALSE

dn: o=Level41, o=Level31, o=Level21, o=Level11, o=sample
o: Level41
objectclass: organization
objectclass: top

dn: o=Level32, o=Level21, o=Level11, o=sample
o: Level32
objectclass: organization
objectclass: top
ibm-filterAclEntry: access-id:CN=USER1,o=sample:(o=Level42):normal:rwc:
sensitive:rsc:critical:rsc
ibm-filterAclEntry: access-id:CN=USER1,o=sample:(o=Level43):normal:rwc:
sensitive:rwc:critical:rsc
ibm-filterAclEntry: access-id:CN=USER2,o=sample:(o=Level44):normal:rwc:
sensitive:rsc:critical:rsc

dn: o=Level42, o=Level32, o=Level21, o=Level11, o=sample
o: Level42
objectclass: organization
objectclass: top

dn: o=Level43, o=Level32, o=Level21, o=Level11, o=sample
o: Level43
objectclass: organization
objectclass: top
ibm-filterAclEntry: access-id:CN=USER1,o=sample:(o=Level43):normal:rwc:
sensitive:rsc:critical:rwc

dn: o=Level44, o=Level32, o=Level21, o=Level11, o=sample
o: Level44
objectclass: organization
objectclass: top
ibm-filterAclEntry: access-id:CN=USER1,o=sample:(o=Level44):normal:rwc:
sensitive:rsc:critical:rsc
ibm-filterAclInherit: FALSE

dn: cn=User2, o=sample
cn: User2
sn: User
objectclass: person
objectclass: top
userPassword: User2

dn: o=Level22, o=Level11, o=sample
o: Level22
objectclass: organization
objectclass: top
aclentry: access-id:CN=USER2,o=sample:normal:rsc:at.sn:deny:c:sensitive:
c:critical:c

dn: o=Level33, o=Level22, o=Level11, o=sample
o: Level33
objectclass: organization
objectclass: top

dn: o=Level34, o=Level22, o=Level11, o=sample
o: Level34
objectclass: organization
objectclass: top
ibm-filterAclEntry: access-id:CN=USER2,o=sample:(o=Level34):normal:rwc:
sensitive:rsc:critical:rsc

```

```

ibm-filterAclEntry: access-id:CN=USER2,o=sample:(o=Level151):normal:rwc:
sensitive:rwc:critical:rsc
ibm-filterAclEntry: access-id:CN=USER1,o=sample:(o=Level153):normal:rwc:
sensitive:rsc:critical:rsc
ibm-filterAclEntry: access-id:CN=USER2,o=sample:(o=Level146):normal:rwc:
sensitive:rsc:critical:rsc

dn: o=Level145, o=Level134, o=Level122, o=Level111, o=sample
o: Level145
objectclass: organization
objectclass: top
aclentry: access-id:CN=USER2,o=sample:normal:rwc:sensitive:rsc:critical
:rsc
aclpropagate: FALSE

dn: o=Level151, o=Level145, o=Level134, o=Level122, o=Level111, o=sample
o: Level151
objectclass: organization
objectclass: top
ibm-filterAclEntry: access-id:CN=USER2,o=sample:(o=Level151):normal:rwc:
sensitive:rsc:critical:rsc

dn: o=Level152, o=Level145, o=Level134, o=Level122, o=Level111, o=sample
o: Level152
objectclass: organization
objectclass: top

dn: o=Level153, o=Level145, o=Level134, o=Level122, o=Level111, o=sample
o: Level153
objectclass: organization
objectclass: top

dn: o=Level146, o=Level134, o=Level122, o=Level111, o=sample
o: Level146
objectclass: organization
objectclass: top

dn: o=Level147, o=Level134, o=Level122, o=Level111, o=sample
o: Level147
objectclass: organization
objectclass: top
aclentry: access-id:CN=USER2,o=sample:normal:rwc:sensitive:rsc:critical
:rsc

```

以下の出力は、検索出力のサンプルと、各項目で ACL がどのように計算されたかを説明したコメントです。

```

>idsldapsearch -D <admin DN> -w <admin PW> -b o=sample objectclass=*
ibm-effectiveACL ibm-filterAclEntry
ibm-filterACLInherit aclEntry aclPropagate

o=sample
aclPropagate=TRUE
aclEntry=group:CN=ANYBODY:system:rsc:normal:rsc:restricted:rsc
ibm-effectiveACL=group:CN=ANYBODY:restricted:rsc:normal:rsc:system:rsc

```

以下の条件が真であるため、この項目の有効な ACL はデフォルト ACL です。

- この項目には、フィルターに掛けられていない ACL が明示的に定義されていません。
- ディレクトリー・ツリーのこの項目の上位では、伝搬する、フィルターに掛けられていない ACL が定義されていません。
- 定義されている、フィルターに掛けられた ACL はどれもこの項目には適用されません。

```

cn=User1,o=sample
aclPropagate=TRUE
aclEntry=group:CN=ANYBODY:system:rsc:normal:rsc:restricted:rsc
ibm-effectiveACL=group:CN=ANYBODY:restricted:rsc:normal:rsc:system:rsc

```

以下の条件が真であるため、この項目の有効な ACL はデフォルト ACL です。

- この項目には、フィルターに掛けられていない ACL が明示的に定義されていません。
- ディレクトリー・ツリーのこの項目の上位では、伝搬する、フィルターに掛けられていない ACL が定義されていません。

- 定義されている、フィルターに掛けられた ACL はどれもこの項目には適用されません。

```
o=Level11,o=sample
aclPropagate=TRUE
aclEntry=group:CN=ANYBODY:system:rsc:normal:rsc:restricted:rsc
ibm-effectiveACL=group:CN=ANYBODY:restricted:rsc:normal:rsc:system:rsc
```

以下の条件が真であるため、この項目の有効な ACL はデフォルト ACL です。

- この項目には、フィルターに掛けられていない ACL が明示的に定義されていません。
- ディレクトリー・ツリーのこの項目の上位では、伝搬する、フィルターに掛けられていない ACL が定義されていません。
- 定義されている、フィルターに掛けられた ACL はどれもこの項目には適用されません。

```
o=Level21,o=Level11,o=sample
ibm-filterACLInherit=TRUE
ibm-filterACLEntry=access-id:CN=USER1,o=sample:(o=Level32):normal:rwc:
sensitive:rsc:critical:rsc
ibm-effectiveACL=group:CN=ANYBODY:restricted:rsc:system:rsc:normal:rsc
```

この項目には、この項目に適用されないフィルター ACL が定義されています。フィルター ACL でこの項目に定義されているものは、o=Level32 を持つ項目にのみ適用されます。以下の条件が真であるため、この項目に対して有効な ACL はデフォルト ACL です。

- この項目には、フィルターに掛けられていない ACL が明示的に定義されていません。
- ディレクトリー・ツリーのこの項目の上位では、伝搬する、フィルターに掛けられていない ACL が定義されていません。
- 定義されている、フィルターに掛けられた ACL はどれもこの項目には適用されません。

```
o=Level31,o=Level21,o=Level11,o=sample
ibm-filterACLInherit=FALSE
ibm-effectiveACL=group:CN=ANYBODY:restricted:rsc:system:rsc:normal:rsc
```

この項目には `ibm-filterACLInherit=FALSE` が定義されています。この属性は上限として機能し、フィルター ACL の累積を停止します。この場合、フィルター ACL でこの項目より下に定義されているものはありません。以下の条件が真であるため、この項目の有効な ACL はデフォルト ACL です。

- `ibm-filterACLInherit` 定義により、この項目はフィルター ACL モードになり、フィルターに掛けられていない ACL 定義は除外されます。
- 定義されている、フィルターに掛けられた ACL はどれもこの項目には適用されません。

```
o=Level41,o=Level31,o=Level21,o=Level11,o=sample
ibm-effectiveACL=group:CN=ANYBODY:restricted:rsc:system:rsc:normal:rsc
```

以下の条件が真であるため、この項目の有効な ACL はデフォルト ACL です。

- この項目には、フィルターに掛けられていない ACL が明示的に定義されていません。
- ディレクトリー・ツリーのこの項目の上位では、伝搬する、フィルターに掛けられていない ACL が定義されていません。
- 定義されている、フィルターに掛けられた ACL はどれもこの項目には適用されません。

```

o=Level32,o=Level21,o=Level11,o=sample
ibm-filterACLInherit=TRUE
ibm-filterAclEntry=access-id:CN=USER2,o=sample:(o=Level44):normal:rws:
sensitive:rsc:critical:rsc
ibm-filterAclEntry=access-id:CN=USER1,o=sample:(o=Level43):normal:rws:
sensitive:rws:critical:rsc
ibm-filterAclEntry=access-id:CN=USER1,o=sample:(o=Level42):normal:rws:
sensitive:rsc:critical:rsc
ibm-effectiveACL=access-id:CN=USER1,o=sample:normal:rws:sensitive:rsc:
critical:rsc

```

属性 `ibm-filterACLInherit=TRUE` により、この項目は、フィルターに掛けられた ACL の上限としては機能しません。

この 3 つの `ibm-filterAclEntry` 属性は、フィルターに掛けられた ACL を 1 つの項目に定義して別の項目に適用する方法のサンプルとして使用できます。このケースでは、フィルターに掛けられた 3 つの ACL は、この項目の 3 つの子項目に適用されますが、この項目自体には適用されません。有効な ACL は、すべてのフィルター ACL の累算で計算され、この項目に適用されます。

`o=Level21,o=Level11,o=sample` 項目に定義されているフィルターに ACL が、この項目に適用される唯一のフィルター ACL です。他のフィルターに掛けられた ACL はこの項目には適用されません。したがって、有効な ACL は、`o=Level21,o=Level11,o=sample` 項目に定義されている、フィルターに掛けられた ACL から直接取得されます。

```

o=Level42,o=Level32,o=Level21,o=Level11,o=sample
ibm-effectiveACL=access-id:CN=USER1,o=sample:normal:rws:sensitive:rsc:
critical:rsc

```

`o=Level32,o=Level21,o=Level11,o=sample` 項目に定義されている、フィルターに掛けられた ACL が、この項目の有効な ACL の計算に使用されます。

```

o=Level43,o=Level32,o=Level21,o=Level11,o=sample
ibm-filterACLInherit=TRUE
ibm-filterAclEntry=access-id:CN=USER1,o=sample:(o=Level43):normal:rws:
sensitive:rsc:critical:rws
ibm-effectiveACL=access-id:CN=USER1,o=sample:normal:rws:sensitive:rws:
critical:rws

```

この項目は、フィルター ACL の累算方法の単純な例です。

`o=Level32,o=Level21,o=Level11,o=sample` 項目に定義されているフィルター ACL と、`o=Level43,o=Level32,o=Level21,o=Level11,o=sample` 項目に定義されているフィルター ACL とを結合することで、user 1 の 3 つすべての属性クラスに対して読み取り、書き込み、検索、および比較のアクセス権を設定できます。

```

o=Level44,o=Level32,o=Level21,o=Level11,o=sample
ibm-filterACLInherit=FALSE
ibm-filterAclEntry=access-id:CN=USER1,o=sample:(o=Level44):normal:rws:
sensitive:rsc:critical:rsc
ibm-effectiveACL=access-id:CN=USER1,o=sample:normal:rws:sensitive:rsc:
critical:rsc

```

この項目は、`ibm-filterACLInherit` 属性を使用して、フィルターに掛けられた ACL の累算を停止させる方法を理解するためのサンプルです。

`o=Level32,o=Level21,o=Level11,o=sample` 項目に定義されているフィルターに掛けられた ACL は、`ibm-filterACLInherit=FALSE` が定義されているため、この項目には適用されません。`o=Level44,o=Level32,o=Level21,o=Level11,o=sample` 項目に定義されているフィルター ACL のみ、user 1 へのアクセス権の付与に適用されます。`ibm-filterACLInherit` の値を `TRUE` に変更した場合、有効な ACL により user 2 と user 1 の両方にアクセス権が付与されます。以下の例のようになります。

```

ibm-effectiveACL=access-id:CN=USER2,o=sample:normal:rws:sensitive:rsc:
critical:rsc
ibm-effectiveACL=access-id:CN=USER1,o=sample:normal:rws:sensitive:rsc:
critical:rsc

```

```
cn=User2,o=sample
aclPropagate=TRUE
aclEntry=group:CN=ANYBODY:system:rsc:normal:rsc:restricted:rsc
ibm-effectiveACL=group:CN=ANYBODY:restricted:rsc:normal:rsc:system:rsc
```

以下の条件が真であるため、この項目の有効な ACL はデフォルト ACL です。

- この項目には、フィルターに掛けられていない ACL が明示的に定義されていません。
- ディレクトリー・ツリーのこの項目の上位では、伝搬する、フィルターに掛けられていない ACL が定義されていません。
- 定義されている、フィルターに掛けられた ACL はどれもこの項目には適用されません。

```
o=Level22,o=Level11,o=sample
aclPropagate=TRUE
aclEntry=access-id:CN=USER2,o=sample:sensitive:c:at.sn:deny:c:normal:
rsc:critical:c
ibm-effectiveACL=access-id:CN=USER2,o=sample:critical:c:normal:rsc:
at.sn:deny:c:sensitive:c
```

これは、非フィルター ACL の例です。この項目の有効な ACL は、項目に定義された ACL です。

注: 有効な ACL から戻される値は、サーバーの正規化された値です。

```
o=Level133,o=Level122,o=Level11,o=sample
aclPropagate=TRUE
aclEntry=access-id:CN=USER2,o=sample:sensitive:c:at.sn:deny:c:normal:
rsc:critical:c
ibm-effectiveACL=access-id:CN=USER2,o=sample:critical:c:normal:rsc:
at.sn:deny:c:sensitive:c
```

この例では、`o=Level122,o=Level11,o=sample` 項目に定義されているフィルターに掛けられていない ACL が、`o=Level133,o=Level122,o=Level11,o=sample` 項目に伝搬します。この伝搬が発生するのは、`o=Level122,o=Level11,o=sample` 項目の `aclPropagate` 属性に `TRUE` が設定されているからです。

```
o=Level134,o=Level122,o=Level11,o=sample
ibm-filterACLInherit=TRUE
ibm-filterAclEntry=access-id:CN=USER2,o=sample:(o=Level146):normal:rwc:
sensitive:rsc:critical:rsc
ibm-filterAclEntry=access-id:CN=USER1,o=sample:(o=Level153):normal:rwc:
sensitive:rsc:critical:rsc
ibm-filterAclEntry=access-id:CN=USER2,o=sample:(o=Level151):normal:rwc:
sensitive:rwc:critical:rsc
ibm-filterAclEntry=access-id:CN=USER2,o=sample:(o=Level134):normal:rwc:
sensitive:rsc:critical:rsc
ibm-effectiveACL=access-id:CN=USER2,o=sample:normal:rwc:sensitive:rsc:
critical:rsc
```

この項目には、フィルターに掛けられた 4 つの ACL が定義されています。フィルターに掛けられた ACL の 1 つが、この項目には適用されます。有効な ACL は、このフィルターに掛けられた ACL の結果です。

注: `o=Level122,o=Level11,o=sample` 項目に定義されている非フィルター ACL は、この項目には伝搬しません。当の非フィルター ACL がこの項目に伝搬しないのは、この項目に対し、フィルター ACL が定義されているからです。所定の項目に存在できる ACL は 1 種類のみです。

```
o=Level145,o=Level134,o=Level122,o=Level11,o=sample
aclPropagate=FALSE
aclEntry=access-id:CN=USER2,o=sample:sensitive:rsc:normal:rwc:critical:
rsc
ibm-effectiveACL=access-id:CN=USER2,o=sample:critical:rsc:normal:rwc:
sensitive:rsc
```

この項目には、非フィルター ACL が明示的に定義されています。有効な ACL は、この明示的に定義された ACL から取得されます。aclPropagate が FALSE であるため、ここで定義されている非フィルター ACL は、下位ツリーに伝搬されません。

```
o=Level151,o=Level145,o=Level134,o=Level122,o=Level111,o=sample
ibm-filterACLInherit=TRUE
ibm-filterAclEntry=access-id:CN=USER2,o=sample:(o=Level151):normal:rws:
sensitive:rsc:critical:rsc
ibm-effectiveACL=access-id:CN=USER2,o=sample:normal:rws:sensitive:rws:
critical:rsc
```

この項目は、フィルター ACL が非フィルター ACL 項目をも累算する方法の例です。項目で有効な ACL は、o=Level134,o=Level122,o=Level111,o=sample 項目に定義されているフィルター ACL と、

o=Level151,o=Level145,o=Level134,o=Level122,o=Level111,o=sample 項目に定義されているフィルター ACL との組み合わせです。

```
o=Level152,o=Level145,o=Level134,o=Level122,o=Level111,o=sample
ibm-effectiveACL=group:CN=ANYBODY:restricted:rsc:system:rsc:normal:rsc
```

この項目の有効な ACL は、デフォルト ACL です。この項目には、モードをフィルターか非フィルターのいずれかに設定するための明示的な ACL 属性がないので、ディレクトリー・ツリーをたどって ACL ソースを確認する必要があります。Level145 項目には非フィルター ACL がありますが、aclPropagate が FALSE に設定されているため、ACL ソースではありません。次に、ディレクトリー・ツリー内の次の上位項目である Level 34 に移動します。Level 34 項目は、フィルター ACL タイプです。Level 34 項目は、この項目の ACL ソースです。ツリーには、この項目に適用されるフィルター ACL が存在しないので、デフォルト ACL が適用されます。

```
o=Level153,o=Level145,o=Level134,o=Level122,o=Level111,o=sample
ibm-effectiveACL=access-id:CN=USER1,o=sample:normal:rws:sensitive:rsc:
critical:rsc
```

この項目の有効な ACL は、o=Level134,o=Level122,o=Level111,o=sample 項目に定義されているフィルターに掛けられた ACL です。

```
o=Level146,o=Level134,o=Level122,o=Level111,o=sample
ibm-effectiveACL=access-id:CN=USER2,o=sample:normal:rws:sensitive:rsc:
critical:rsc
```

この項目の有効な ACL は、o=Level134,o=Level122,o=Level111,o=sample 項目に定義されているフィルターに掛けられていない ACL です。この ACL が伝搬します。

```
o=Level147,o=Level134,o=Level122,o=Level111,o=sample
aclPropagate=TRUE
aclEntry=access-id:CN=USER2,o=sample:sensitive:rsc:normal:rws:critical:
rsc
ibm-effectiveACL=access-id:CN=USER2,o=sample:critical:rsc:normal:rws:
sensitive:rsc
```

この項目には、フィルターに掛けられていない ACL が明示的に定義されています。したがって、有効な ACL は、この明示的に定義された ACL から取得されます。

付録 L. 動的に変更される属性

以下に、動的に変更できる属性のリストを示します。

これらの変更を有効にするために、サーバーを再始動する必要はありません。コマンド行を使用して値を更新する場合は、`ldapexop -op readconfig` オプションを要求する必要があります。詳しくは、「*IBM Security Directory Server Version 6.3 Command Reference*」の **idsldapexop** コマンド情報を参照してください。

cn=Configuration

- `ibm-slapdadmindn`
- `ibm-slapdAdminGroupEnabled`
- `ibm-slapdadminpw`
- `ibm-slapdDerefAliases`
- `ibm-slapdpwencryption`
- `ibm-slapdsizelimit`
- `ibm-slapdtimelimit`
- `ibm-slapdAdminRole`
- `ibm-slapdPtaEnabled`

cn=Log Management, cn=Configuration

動的に変更される属性は、次のサブ項目に適用されます。

- `cn=Default, cn=Log Management, cn=Configuration`
- `cn=ibmslapd, cn=Log Management, cn=Configuration`
- `cn=Audit, cn=Log Management, cn=Configuration`
- `cn=Bulkload, cn=Log Management, cn=Configuration`
- `cn=DB2CLI, cn=Log Management, cn=Configuration`
- `cn=Tools, cn=Log Management, cn=Configuration`
- `cn=Replication, cn=Log Management, cn=Configuration`
- `cn=Admin, cn=Log Management, cn=Configuration`
- `cn=Admin Audit, cn=Log Management, cn=Configuration`

以下は、これらのサブ項目に関し、動的に変更される属性です。

- `ibm-slapdLog` (`cn=Default` には適用されません)
- `ibm-slapdLogArchivePath`
- `ibm-slapdLogMaxArchives`
- `ibm-slapdLogOptions` (`cn=Default` には適用されません)
- `ibm-slapdLogSizeThreshold`

cn=AdminGroup, cn=Configuration

以下は、この項目の下のサブツリーで動的に変更される属性です。

- `ibm-slapdAdminDN`
- `ibm-slapdAdminPW`

- ibm-slapdDigestAdminUser
- ibm-slapdKrbAdminDN

cn=Front End, cn=Configuration

- ibm-slapdaclcache
- ibm-slapdaclcachesize
-
- ibm-slapdfiltercachebypasslimit
- ibm-slapdfiltercachesize
- ibm-slapdidletimeout

cn=Connection Management, cn=Front End, cn=Configuration

- ibm-slapdAllowAnon
- ibm-slapdAllReapingThreshold
- ibm-slapdAnonReapingThreshold
- ibm-slapdBoundReapingThreshold
- ibm-slapdESizeThreshold
- ibm-slapdEThreadActivate
- ibm-slapdEThreadEnable
- ibm-slapdETimeThreshold
- ibm-slapdIdleTimeOut
- ibm-slapdWriteTimeout

cn=Event Notification, cn=Configuration

- ibm-slapdmaxeventsperconnection
- ibm-slapdmaxeventstotal

cn=Transaction, cn=Configuration

- ibm-slapdmaxnumoftransactions
- ibm-slapdmaxoppertransaction
- ibm-slapdmaxtimelimitoftransactions
- ibm-slapdMaxTimeBetweenPrepareAndCommit

cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

- ibm-slapdreadonly

cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeSize
- ibm-slapdLanguageTagsEnabled
- ibm-slapdpagedresallownonadmin
- ibm-slapdpagedreslmt
- ibm-slapdreadonly

- ibm-slapsortkeylimit
- ibm-slapsortsrchallownonadmin
- ibm-slapsuffix
- ibm-slapdCachedAttributeAutoAdjust
- ibm-slapdCachedAttributeAutoAdjustTime
- ibm-slapdCachedAttributeAutoAdjustTimeInterval
- ibm-slapdNumRetry
- ibm-slapdGroupMembersCacheSize
- ibm-slapdGroupMembersCacheBypassLimit
- ibm-slapdDbUserPW
- ibm-slapdTombstoneEnabled
- ibm-slapdTombstoneLifetime

cn=change log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeSize
- ibm-slapdCachedAttributeAutoAdjust
- ibm-slapdCachedAttributeAutoAdjustTime
- ibm-slapdCachedAttributeAutoAdjustTimeInterval

cn=Digest, cn=configuration

- ibm-slapdDigestAdminUser
- ibm-slapdDigestRealm
- ibm-slapdDigestAttr

cn=pwdPolicy Admin, cn=Configuration

- ibm-slapdConfigPwdPolicyOn
- pwdMinLength
- pwdLockout
- pwdLockoutDuration
- pwdMaxFailure
- pwdFailureCountInterval
- passwordMinAlphaChars
- passwordMinOtherChars
- passwordMaxRepeatedChars
- passwordMaxConsecutiveRepeatedChars
- passwordMinDiffChars

cn=Replication, cn=configuration

- ibm-slapdReplConflictMaxEntrySize
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdReplMaxErrors

- ibm-slapdReplContextCacheSize
- ibm-slapdReplRestrictedAccess
- ibm-slapdEnableConflictResolutionForGroups

cn=VirtualListView, cn=Configuration

- ibm-slapdVLVEnabled
- ibm-slapdMaxVLVBeforeCount

cn=Persistent Search, cn=Configuration

- ibm-slapdMaxPersistentSearches
- ibm-slapdEnablePersistentSearch

cn=RDBM Backup, cn=Configuration

- ibm-slapdBackupLocation
- ibm-slapdBackupAt
- ibm-slapdBackupEvery
- ibm-slapdBackupOnline
- ibm-slapdBackupEnabled
- ibm-slapdBackupChangelog

cn=Master Server, cn=Configuration

- ibm-slapdMasterDN
- ibm-slapdMasterPW

付録 M. IBM Security Directory Server のバックアップおよび復元

ここに示す情報により、IBM Security Directory Server のバックアップおよび復元の詳細を知ることができます。

Security Directory Server には、ディレクトリー・サーバー・インスタンス情報のバックアップ/復元方式が複数あります。ディレクトリー・サーバー・インスタンスの情報全体をバックアップする方式と、データベースのデータのみをバックアップする方式があります。この付録では、データベース内のデータのみをバックアップする方法について説明します。これには、DB2 データのバックアップおよび復元を行うための DB2 バックアップ・コマンドおよび復元コマンドが含まれます。ディレクトリー・サーバー・インスタンス情報のバックアップ方法および復元方法について詳しくは、466 ページの『ディレクトリー・サーバーをバックアップおよびリストアする』を参照してください。

IBM Security Directory Server は、IBM DB2 リレーショナル・データベースを使用してディレクトリー情報を保管します。ディレクトリー情報の可用性を確保して、紛失や破損から重要なデータを回復できるようにするには、Security Directory Server のディレクトリー管理者が、Security Directory Server の使用環境に合わせてバックアップと復元の方法を計画する必要があります。

DB2 は、オンライン・バックアップ機能を備えています。そのため、Security Directory Server などの他のアプリケーションがデータベースにアクセスしている間に、データベースのバックアップを作成することが可能です。オンライン・バックアップを含むバックアップと復元の方法を検討する前に、オンライン・バックアップを実行すると相当量の DB2 リソースが消費されることを認識しておいてください。

この付録では、Security Directory Server データベースとテーブル・スペースの定義についての説明から始めます。個々のセクションでは、DB2 のオフライン・バックアップおよびオンライン・バックアップ、DB2 のオフライン復元、およびリダイレクトされた復元を含む、Security Directory Server のバックアップと復元の手順の代替手段について説明します。

Security Directory Server のディレクトリー・スキーマおよびデータベース定義

ここに示す情報により、Security Directory Server ディレクトリー・スキーマおよびデータベース定義の詳細を知ることができます。

Security Directory Server では、ディレクトリー・スキーマ・ファイルを使用して、基盤となる DB2 ディレクトリー・データベースを定義します (このデータベースは、データの保管用に使用されます)。Security Directory Server に保管されている

ータを復旧するには、Security Directory Server のディレクトリー構成およびディレクトリー・スキーマが格納されているファイルと DB2 データベースをバックアップする必要があります。

Security Directory Server のディレクトリー・スキーマ

ここに示す情報により、Security Directory Server ディレクトリー・スキーマの詳細を知ることができます。

デフォルトでは、Security Directory Server 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・ディレクトリー下の etc ディレクトリーでスキーマ・ファイルを維持します。例えば、**ldapdb2** というインスタンス所有者の場合、スキーマ・ファイルの場所は次のようになります。

```
/home/ldapdb2/idsslapd-ldapdb2/etc
```

注: インスタンス作成時に、スキーマ・ファイルに別の場所を指定することもできます。ただし、インスタンス所有者がディレクトリー上での書き込み権限を保有していることが前提です。

サーバーを始動すると、サーバーはそのたびにスキーマ・ファイルを検査し、基となる DB2 データベースと照合して、このデータベースがスキーマをサポートできるように正しく構成されていることを確認します。

スキーマが同じになるように新規インスタンスを構成するには、スキーマ・ファイルを新規のサーバー・インスタンス所有者の `<inst_owner_home>/idsslapd-<inst_name>/etc` ディレクトリーにコピーします。例えば、AIX 上のスキーマ・ファイルをバックアップするには、使用する Security Directory Server インスタンスが `ldapdb2` であり、スキーマ・ファイルの保存先の場所が `/safeplace/etc` ディレクトリーである場合、次のコマンドを実行します。

```
cp /home/ldapdb2/idsslapd-ldapdb2/etc/* /safeplace/etc
```

スキーマが同じ新規インスタンスをセットアップするには、次のコマンドを実行します。

```
cp /safeplace/etc/* /home/<newuser>/idsslapd-<new_user>/etc
```

Security Directory Server ディレクトリー・データベースおよびテーブル・スペース

ここに示す情報により、Security Directory Server ディレクトリー・データベースおよびテーブル・スペースの詳細を知ることができます。

テーブル・スペースとは、データベース・オブジェクトの基礎となる実際のデータを保管できるストレージ構造のことです。DB2 では、以下の 2 種類のテーブル・スペースがサポートされています。

- **システム管理スペース (SMS)** - SMS では、オペレーティング・システムのファイル・システム・マネージャーがテーブルを保管するスペースを割り振って管理します。テーブル・スペースが急速に増大および縮小する場合には、このタイプが適しています。
- **データベース管理スペース (DMS)** - DMS では、データベース・マネージャーがストレージ・スペースを制御します。

データベース構成時には、DMS テーブル・スペースのデータベースがデフォルトで作成されます。テーブル・スペースの場所は、管理者により明示的に指定されます。指定した場所がファイル・システムの場合は、DMS クックド・テーブル・スペースが作成されます。指定された場所がロー・デバイスまたはブロック・デバイスである場合は、DMS ロー・テーブル・スペースが作成されます。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。SMS テーブル・スペースまたは DMS テーブル・スペースを使用するデータベースの作成方法と、各種のパラメーターのデフォルト値については、「*IBM Security Directory Server Version 6.3 Command Reference*」の **idscfgdb** コマンド情報を参照してください。

注:

- DB2 では、デフォルトで USERSPACE1、SYSCATSPACE、および TEMPSPACE1 という 3 つのテーブル・スペースが作成されます。Security Directory Server では、LDAPSPACE と呼ばれる追加のテーブル・スペースが作成されます。
- USERSPACE1 および LDAPSPACE テーブル・スペースには、Security Directory Server データが保管されます。
- 管理者は、USERSPACE1 および LDAPSPACE に対して DMS または SMS タイプのテーブル・スペースを作成することを選択できます。

DB2 のバックアップと復元は、データベース・レベル、テーブル・スペース・レベル、またはその両方のレベルで実行できるため、さまざまな Security Directory Server 環境で最適なバックアップと復元の方法を判別するには、基礎となる構造を理解することが重要です。通常は、上記の理由により、テーブル・スペース・レベルでは DB2 バックアップおよび復元を使用しないことをお勧めします。

以下の例では、データベース名として `ldapdb2` が使用されています。***db2 list database directory*** コマンドおよび ***db2 list tablespace show detail*** コマンドを使用すると、ご使用の環境でのデータベースとテーブル・スペースの情報を検索できます。

テーブル・スペースを表示するには、DB2 インスタンス所有者のコンテキストで実行される以下の DB2 コマンドを使用します。この例では、`ldapdb2` を使用します。

```
db2 connect to <databasename>
db2 list tablespaces
```

以下の例では、AIX、Linux、または Solaris システムでの Security Directory Server ディレクトリー・データベースのテーブル・スペース出力を示します。

```
Tablespaces for Current Database

Tablespace ID= 0
Name= SYSCATSPACE
Type= System managed space
Contents= All permanent data. Regular table space.
State= 0x0000
Detailed explanation:
Normal (通常)

Tablespace ID= 1
Name= TEMPSPACE1
Type= System managed space
Contents= System Temporary data
State= 0x0000
Detailed explanation:
Normal (通常)

Tablespace ID= 2
```

```
Name= USERSPACE1
Type= Database managed space
Contents= All permanent data. Large table space.
State= 0x0000
Detailed explanation:
Normal (通常)
```

```
Tablespace ID= 3
Name= LDAPSPACE
Type= Database managed space
Contents= All permanent data. Large table space.
State= 0x0000
Detailed explanation:
Normal (通常)
```

Security Directory Server のデータは、USERSPACE1 および LDAPSPACE という 2 つの独立したテーブル・スペースに保管されます。デフォルトでは、テーブル・スペースごとにコンテナまたはディレクトリーが 1 つのみ存在します。

USERSPACE1 テーブル・スペースの詳細を表示するには、次の DB2 コマンドを実行します。

```
db2 list tablespace containers for 2
```

以下の例は、Security Directory Server インスタンス ldapdb2 の出力です。

DMS クックド・テーブル・スペースの場合のテーブル・スペース・コンテナ 2 の出力:

Windows 以外の場合:

```
Container ID = 0
Name = /home/ldapdb2/1dapdb2/NODE0000/SQL00001/USPACE
Type = File
```

Windows の場合:

```
Container ID = 0
Name = C:\1dapdb2\N0DE0000\SQL00001\USPACE
Type = File
```

DMS ロー・テーブル・スペースの場合のテーブル・スペース・コンテナ 2 の出力:

Linux の場合:

```
Container ID = 0
Name = /dev/raw/raw1
Type = disk
```

Windows の場合:

```
Container ID = 0
Name = %%H
Type = disk
```

SMS テーブル・スペースの場合のテーブル・スペース・コンテナ 2 の出力:

Windows 以外の場合:

```
Container ID = 0
Name = /home/ldapdb2/1dapdb2/NODE0000/SQL00001/SQLT0002.0
Type = path
```

Windows の場合:

```
Container ID = 0
Name = C:\1dapdb2\N0DE0000\SQL00001\SQLT0002.0
Type = path
```

DB2 がテーブル・スペース 2 (USERSPACE1) に対して使用するデフォルトのコンテナまたはディレクトリーは、/home/ldapdb2/ldapdb2/NODE0000/SQL00001/USPACE です。ここには ldapdb2 データベース表がすべて格納されており、その中の行は 4K のページ・サイズに収まります。このデータベース表には、DB2 の高速検索に使用される属性テーブルが含まれます。テーブル・スペース 3 (LDAPSPACE) には、データベース表の残りが格納されており、32K のページ・サイズを必要とします。これには、Security Directory Server ディレクトリー・データ

や複製テーブルの大部分を収容する ldap_entry テーブルが含まれます。
LDAPSPACE テーブル・スペースのテーブル・スペース・コンテナー情報を表示するには、次の DB2 コマンドを実行します。

```
db2 list tablespace containers for 3
```

以下の例は、Security Directory Server インスタンス ldapdb2 の出力です。

DMS クックド・テーブル・スペースの場合のテーブル・スペース・コンテナー 3 の出力:

Windows 以外の場合:

```
Container ID = 0  
Name = /home/ldapdb2/1dap32kcont_ldapdb2/1dapspace  
Type = File
```

Windows の場合:

```
Container ID = 0  
Name = C:\1dapdb2\1dap32kcont_ldapdb2\1dapspace  
Type = File
```

DMS ロー・テーブル・スペースの場合のテーブル・スペース・コンテナー 3 の出力:

Linux の場合:

```
Container ID = 0  
Name = /dev/raw/raw2  
Type = disk
```

Windows の場合:

```
Container ID = 0  
Name = %K  
Type = disk
```

SMS テーブル・スペースの場合のテーブル・スペース・コンテナー 3 の出力:

Windows 以外の場合:

```
Container ID = 0  
Name = /home/ldapdb2/1dap32kcont_ldapdb2  
Type = path
```

Windows の場合:

```
Container ID = 0  
Name = C:\1dapdb2\1dap32kcont_ldapdb2  
Type = path
```

Security Directory Server のデータはテーブル・スペース 2 とテーブル・スペース 3 に広がっており、1 回の Security Directory Server 操作の大半では、両方のテーブル・スペースへのアクセスが必要であることに注意してください。検索操作の場合、テーブル・スペース 2 の属性テーブルは、所与の基準に一致する項目の検索に使用されますが、項目情報はテーブル・スペース 3 の ldap_entry テーブルから返されます。更新操作の場合、テーブル・スペース 2 の属性テーブルおよびテーブル・スペース 3 の ldap_entry テーブル (および場合によっては複製テーブル) が更新されることとなります。このため、ユーザーはバックアップおよび復元をデータベース・レベルでのみ実行して、関連するデータ・セットをまとめておく必要があります。関連するデータ・セットがまとめられていない場合、すべてのデータに一貫性がある時点にまでリカバリーしてもうまくいきません。

Security Directory Server の変更ログ・データベースおよびテーブル・スペース

ここに示す情報により、Security Directory Server の変更ログ・データベースおよびテーブル・スペースの詳細を知ることができます。

Tivoli Directory Server 6.0 以降のバージョンでは、変更ログ機能により、独立した変更ログ DB2 データベース内のディレクトリーにすべての更新情報が記録されます。このデータベースは、Security Directory Server のディレクトリー情報ツリー (DIT) を保持するデータベースとは異なります。変更ログ・データベースは、他のアプリケーションが LDAP 更新情報を照会して追跡するために使用することができます。デフォルトでは、変更ログ機能は使用不可になっています。変更ログ機能を使用すると、ロギング・オーバーヘッドが増加して更新の効率が低下するため、必要な場合にのみ構成するようにしてください。変更ログ機能が使用可能になっているかどうかを確認するには、サフィックス CN=CHANGELOG を検索します。これが存在する場合は、変更ログ機能が使用可能になっています。

Security Directory Server では、変更ログを使用するようにデータベースを作成する場合、`db2 create database` コマンドを使用して `ldapclog` というデータベースを作成します。IBM Security Directory Server がこのデータベースを作成するときは、`ldapdb2` データベースと同一である 4 つの SMS テーブル・スペースが使用されます。

テーブル・スペースを表示するには、DB2 インスタンス所有者のコンテキストで実行される以下の DB2 コマンドを使用します。この例では、`ldapdb2` を使用します。

```
db2 connect to ldapclog
db2 list tablespaces
```

Security Directory Server のディレクトリー情報は、変更ログ・データベース (`ldapclog`) とは異なるデータベース (`ldapdb2`) に保管される、ということに注意することは重要です。関連するデータ・セットをまとめておくには、それらが一貫した方法でバックアップおよび復元されるようにするよう注意する必要があります。

LDAP のバックアップと復元の手順の概要

Security Directory Server 環境では、データベースのバックアップおよび復元を行うために、DB2 コマンド、Security Directory Server バックアップおよび復元コマンド、および Security Directory Server ツールを使用できます。これらのオプションには、それぞれに利点と欠点があります。

DB2 の `backup` と `restore` は、データベースのバックアップと復元を行うために DB2 で使用可能な組み込みコマンドです。`db2 backup` コマンドおよび `db2 restore` コマンドまたは `dbback` コマンドおよび `dbrestore` コマンドを使用する利点は、DB2 構成パラメーターおよびデータベース最適化パラメーターがバックアップ・データベース用に保存されることです。さらに、復元したデータベースとバックアップしたデータベースのパフォーマンス・チューニングの指定が同じです。`db2 backup` および `db2 restore` を使用した場合の欠点の 1 つは、あるハードウェア・プラットフォームでバックアップしたデータベースを別のプラットフォームでは復元できないことです。例えば、AIX システムでバックアップしたデータベースを Solaris システムで復元することはできません。さらに、Security Directory Server のあるバージョンでバックアップしたデータベースは、別のバージョンの Security Directory Server では復元できません。`db2 backup` と `db2 restore` の両方の操作に対して同じバージョンの DB2 を使用することも必要です。DB2 のバックアップと復元の手順について詳しくは、「DB2 管理ガイド」を参照してください。DB2 コマンドについて詳しくは、「DB2 コマンド解説書」を参照してください。「DB2 管理ガイド」お

および「コマンド解説書」は、DB2 および Security Directory Server と共にインストールされるオンライン・ライブラリーの一部です。

データベースのバックアップおよび復元のための Security Directory Server コマンドである `idsdbback` および `idsdbrestore` では、DB2 のバックアップおよび復元コマンドが使用されます。DB2 のバックアップおよび復元コマンドによって提供される機能の他に、`idsdbback` および `idsdbrestore` は、Security Directory Server の構成ファイルおよびスキーマ・ファイルのバックアップと復元も行います。ただし `idsdbback` は、Security Directory Server V6.0 では DB2 オンライン・バックアップをサポートしていないので注意してください。`idsdbback` コマンドを使用できるのは、Security Directory Server を実行していない場合に限られます。これらのコマンドの使用法については、「*IBM Security Directory Server Version 6.3 Command Reference*」の『Server utilities』のセクションを参照してください。

DB2 および Security Directory Server のバックアップおよび復元コマンドの代替機能には、LDAP データ交換フォーマット (LDIF) のエクスポートおよびインポート・コマンドである `db2ldif` や `ldif2db` などの Security Directory Server ツールがあります。これらのツールは異種のハードウェア・プラットフォームにまたがって使用できますが、処理速度は低下します。これらのツールでは、DB2 構成パラメーターやデータベース最適化パラメーターは保存されません。これらのコマンドの使用法については、「*IBM Security Directory Server Version 6.3 Command Reference*」の『Server utilities』のセクションを参照してください。

注: 既存のデータベース上で復元を実行すると、その既存データベース上のパフォーマンス・チューニング・タスクは失われます。復元の実行後は、すべての DB2 構成パラメーターを確認する必要があります。また、データベースのバックアップ前に `db2 reorgchk` を実行してあるかどうか不明な場合は、復元後に `db2 reorgchk` を実行してください。

ディレクトリー・データベースのオフライン・バックアップおよびリストアの手順の例

ディレクトリー・データベースのオフライン・バックアップおよび復元には、以下に示す手順の例を使用できます。

ディレクトリー・データベース (`ldapdb2`) のオフライン・バックアップ操作および復元操作を実行するための DB2 コマンドは、次のとおりです。

```
su - ldapdb2
db2start
db2 force applications all
db2 backup db ldapdb2 to <directory_or_device>
db2 restore db ldapdb2 from <directory_or_device> replace existing
```

ここで `directory_or_device` は、バックアップが保管されるディレクトリーまたはデバイスの名前です。

変更ログ・データベースのオフライン・バックアップ操作および復元操作を実行するための DB2 コマンドは、次のとおりです。

```
su - ldapdb2
db2start
db2 force applications all
db2 backup db ldapclog to <directory_or_device>
db2 restore db ldapclog from <directory_or_device> replace existing
```

復元時に発生する最も一般的なエラーは、ファイルのアクセス権エラーです。このエラーが発生するのは、以下の原因が考えられます。

- DB2 インスタンス所有者が、指定のディレクトリーおよびファイルにアクセスするための権限を保持していない。これを解決するための 1 つの方法は、ディレクトリーおよびファイルの所有権を DB2 インスタンス所有者に変更することです。例えば、以下のコマンドを入力します。

```
chown ldapdb2 <fil_or_dev>
```

- バックアップされたデータベースは複数のディレクトリーにまたがって分散しており、該当するディレクトリーが復元のターゲット・システムに存在しない。複数のディレクトリーにまたがったデータベースの分散を実現するには、リダイレクトされた復元を使用します。この問題を解決するには、ターゲット・システム上に同じディレクトリーを作成するか、リダイレクトされた復元を実行して、新しいシステム上で正しいディレクトリーを指定します。同じディレクトリーを作成する場合は、ディレクトリーの所有者が DB2 インスタンス所有者であることを確認してください。

複製に関する考慮事項

ここに示す、複製に関する考慮事項に注意してください。

バックアップ操作および復元操作は、コンシューマーとサプライヤーを初めて同期化する場合に使用できます。また、サプライヤーとコンシューマーとの同期が外れた場合はそのつど使用できます。コンシューマーは、サプライヤーに対して定義されなかった場合や、サプライヤーから到達できない場合に、同期が外れることがあります。この場合、サプライヤーはコンシューマーを認識しないため、このコンシューマーの伝搬キューの更新情報がサプライヤー側で保存されません。

Security Directory Server のオンライン・バックアップと復元の手順の概要

ここに示す情報により、Security Directory Server のオンライン・バックアップと復元の手順の概要について知ることができます。

Security Directory Server データベースを作成したときに、使用可能になるのは循環ログのみです。つまり、ログ・ファイルは循環的に再使用され、保存またはアーカイブされることはありません。循環ログでは、ロールフォワード・リカバリーはできませんが、クラッシュ・リカバリーは可能です。バックアップを取るときは、ディレクトリー・サーバーを停止する必要があるため、オフラインにすることが求められます。管理者は、オンライン・バックアップを実行する前に、オンライン・バックアップから復元を実行する場合に必要な DB2 ログ・ファイルの管理方法を計画する必要があります。

ログの管理

ここに示す情報により、ログの管理について知ることができます。

データベースに対してログ・アーカイブを構成すると、ロールフォワード・リカバリーが可能になります。この理由は以下のとおりです。

- バックアップの実行中および実行後、ログにはデータベースに対する変更内容が記録されます。
- ログ・ファイルは、「非アクティブ」ログと呼ばれる、コミット済みで外部化済みのデータが保管された後でも保存されます。

ログのアーカイブを構成するには、目的のアーカイブ・モードを選択することにより、**logarchmeth1** データベース・パラメーターを OFF から必要な値に変更します。適用可能なモードの値は以下のとおりです。

LOGRETAIN

このモードでは、非アクティブ・ログ・ファイルは上書きされません。つまり、1 次ログのディスク・スペースを使い果たすことがないように、非アクティブ・ログはアーカイブ・ロケーションに移動する必要があります。データベース構成により、アクティブな 1 次ログ・ファイルとアクティブな 2 次ログ・ファイルの作成可能な数が指定されます。**LOGRETAIN** を設定すると、まず DB2 によって 1 次ログが書き込まれ、次に、1 次ログがまだアクティブである場合、DB2 によって 2 次ログが作成されます。作成されて書き込まれた 1 次ログおよび 2 次ログの数が、最初の 1 次ログが非アクティブになる前に最大限度に到達した場合は、「ログ満杯」の状態になります。1 次ログが非アクティブになると、必要に応じて、DB2 によって追加の 1 次ログが作成されます。ディスクがいっぱいになると、その状態が解消されるまでディレクトリーの更新は不可能であるため、**LOGRETAIN** モードでは、ログ・ファイルに使用できるディスク・スペースをモニターすることが重要です。

USEREXIT

このモードでは、ログのアーカイブと取り出しは、ユーザー提供のユーザー出口プログラム **db2uext2** で実行します。ログ・ファイルがいっぱいになるとすぐに、そのログ・ファイルをアーカイブ・ロケーションにコピーするために、ユーザー出口プログラムが呼び出されます。これにより、ファイルが非アクティブになると、DB2 はファイルの名前変更および再利用を行えます。リカバリー操作中、データベースをバックアップから復元した後になって非アクティブ・ログ・ファイルを必要とする場合、DB2 はユーザー出口プログラムを呼び出して、アーカイブ・ロケーションから必要なログを取り出します。

DISK:ディレクトリー

この設定では、**USEREXIT** モードと同様のアルゴリズムを使用してログの管理が実行されます。**USEREXIT** と **DISK:**ディレクトリー の 2 つのモードの違いは、ユーザー出口プログラムを呼び出す代わりに、DB2 がアーカイブ・ログ・ディレクトリーから指定のディレクトリーへログを自動的にアーカイブする点です。DB2 は、リカバリー中にこれらのログを該当の場所から取り出します。

TSM:[管理クラス名]

このモードは **USEREXIT** モードに似ていますが、ログが Security Storage Manager のローカル・サーバーに自動的にアーカイブされる点が異なります。管理クラス名パラメーターはオプションです。指定しなかった場合は、デフォルト管理クラスが使用されます。

VENDOR: ライブラリー

このモードでは、ロギングは USEREXIT と同様に動作しますが、指定したベンダー・ライブラリーを呼び出してログのアーカイブまたは取り出しを行う点が異なります。

このパラメーターを構成すると、データベースがロールフォワード・リカバリー対応になります。logarchmeth1 をログのアーカイブに合わせて設定したら、「バックアップ保留状態」の条件を満たすようにデータベースの完全なオフライン・バックアップを実行して、データベースを使用できるようにする必要があります。データベースが「バックアップ保留状態」であるかどうかを確認するには、次の DB2 コマンドを実行すると返される「Backup pending」の値（「YES」または「NO」）を参照します。

```
db2 get db config for ldapdb2
```

データベースがリカバリー可能な場合は、データベースのバックアップをすべてオンラインで実行できます。ロールフォワード・リカバリーにより、ログに記録されている完了済みの作業単位が、復元されたデータベースまたはテーブル・スペース（複数を含む）に再度適用されます。ロールフォワード・リカバリーは、ログの終了時と特定の時点のいずれかに指定しても構いません。

データベースごとにリカバリー・ヒストリー・ファイルが作成されます。このファイルは、データベースまたはテーブル・スペース全体のバックアップまたは復元を実行すると、そのたびに集計情報によって自動的に更新されます。リカバリー・ヒストリー・ファイルは、データベース内部での復元作業に関する有用な追跡手段です。このファイルはデータベース構成ファイルと同じディレクトリーに作成されます。このファイルは、以下のいずれかの作業が行われる場合は、必ず自動的に更新されます。

- データベースおよびテーブル・スペースのバックアップ
- データベースおよびテーブル・スペースの復元
- データベースおよびテーブル・スペースのロールフォワード
- テーブル・スペースの変更
- テーブル・スペースの静止
- テーブル・スペースの名前変更
- テーブルのロード
- テーブルの除去
- テーブルの再編成
- テーブル統計情報の更新

既存のバックアップ済みデータベースについては、次の DB2 コマンドを入力します。

```
db2 list history backup all for db ldapdb2
```

データベース構成ファイルには、logarchmeth1 パラメーターと、ロールフォワード・リカバリーに関連するその他のパラメーターが記述されています。場合によっては、デフォルトのパラメーター設定では正常に機能しないため、セットアップについてこれらのデフォルト設定の一部を変更する必要があります。DB2 でのこれらのパラメーターの構成について詳しくは、「DB2 管理ガイド」を参照してください。

1 次ログ (logprimary)

このパラメーターでは、特定の時刻にアクティブになることができる 1 次ログの数を指定します。

2 次ログ (logsecond)

このパラメーターでは、アクティブな 1 次ログがすべていっぱいになった場合に作成できる 2 次ログ・ファイルの数を指定します。

ログ・サイズ (logfilsiz)

このパラメーターでは、各構成済みログのページ数を指定します。1 ページのサイズは 4 KB です。

ログ・バッファ (logbufsz)

このパラメーターでは、ログ・レコードをディスクに書き込む前にそのバッファとして使用するデータベース共用メモリのサイズを指定できます。

グループに対するコミットの数 (mincommit)

このパラメーターを使用すると、最低限のコミット数が実行されるまでログ・レコードをディスクに書き込むのを遅らせることができます。

新規のログ・パス (newlogpath)

アクティブなログや将来のアーカイブ・ログを置く場所を変更するには、この構成パラメーターの値を変更して、別のディレクトリまたはデバイスを指すようにします。

1 次ログ・アーカイブ方式 (logarchmeth1)

このパラメーターでは、アーカイブ済みログの 1 次宛先のメディア・タイプを指定します。選択可能なオプションについては、「ログの管理」セクションを参照してください。

2 次ログ・アーカイブ方式 (logarchmeth2)

このパラメーターでは、アーカイブ済みログの 2 次宛先のメディア・タイプを指定します。このパラメーターを指定すると、ログ・ファイルは、この方法と logarchmeth1 で指定した方法との両方を使用してアーカイブされます。

変更されたページの追跡 (trackmod)

このパラメーターを「Yes」に設定すると、データベース・マネージャーによってデータベースの変更が追跡されるため、バックアップ・ユーティリティーは、増分バックアップによって検査する必要があるデータベース・ページのサブセット、およびバックアップ・イメージに組み込まれる可能性があるデータベース・ページのサブセットを検出できます。このパラメーターを「Yes」に設定したら、増分バックアップを取るためのベースラインを把握するため、データベース全体のバックアップを取る必要があります。

DB2 のバックアップおよび復元の使用

データベースのオフライン・バックアップとオンライン・バックアップの基本的な例を、以下のセクションで説明します。

ここに示す例は AIX オペレーティング・システムの場合であるため、他のオペレーティング・システムの場合には変更が必要なことがあります。これらの例では、バックアップ・ロケーションの命名に曜日の略語も組み込まれています。

DB2 のバックアップおよびリストアを使用した Security Directory Server データベースのオフライン・バックアップおよびオフライン・リストアの手順

ここに示す情報により、DB2 のバックアップおよび復元を使用して Security Directory Server データベースのオフライン・バックアップおよびオフライン復元を行う手順の詳細を知ることができます。

このタスクについて

ディレクトリー・データベースのバックアップ:

1. バックアップおよびリカバリーに使用するファイルを保管するための安全な場所 (バックアップ・マシンや単独のメディアなど) を決めます。リストになっている例では、ファイルの保管場所として /safeplace ディレクトリーを使用しています。DB2 インスタンス所有者には、/safeplace ディレクトリーの書き込み権限が必要です。
2. Security Directory Server の構成ファイルおよびスキーマ・ファイルを安全な場所に保存します。これらのファイルを更新する必要があるのは、トポロジー、構成パラメーター、またはスキーマを変更した場合に限られます。以下の例では、Security Directory Server インスタンスおよびデータベースの名前を ldapdb2 にしています。

```
cp /home/ldapdb2/idsslapd-ldapdb2/etc/* /safeplace/etc
```

3. ibmslapd が実行中でないことを確認してください。

```
ibmslapd -I ldapdb2 -k
```

4. データベースの完全オフライン・バックアップを作成します。すべての DB2 コマンドを DB2 インスタンス所有者として実行する必要があります。

```
db2 force applications all  
db2 backup db ldapdb2 to /safeplace/sun-full-ldapdb2
```

別のマシンでのディレクトリー・データベースの復元:

1. 必要に応じて、Security Directory Server をインストールします。
2. バックアップ・マシンに指定したものと同一情報を使用してデータベースを構成します。
3. 構成ファイル、スキーマ・ファイル、およびバックアップ・イメージ・ファイルをバックアップ・マシンからこのマシンの /safeplace ディレクトリーへコピーするか、FTP で転送します。
4. バックアップ済みの構成ファイルおよびスキーマ・ファイルをこのマシンへコピーします。

```
cp /safeplace/etc/* /home/ldapdb2/idsslapd-ldapdb2/etc
```

5. ディレクトリー・データベースを復元します。

```
db2 restore db ldapdb2 from /safeplace/sun-full-ldapdb2 replace existing
```

注: バージョンによっては、DB2 でクロスプラットフォーム・バックアップ/復元操作および混合バージョンのバックアップ/復元操作がサポートされます。Security Directory Server の観点からは、Security Directory Server のあるバージョンでデータベースをバックアップしてから、そのデータベースを Security Directory Server の別のバージョンで復元することはできません。DB2 操作には同じバージョンの db2 バックアップおよび db2 復元操作を使用することをお勧めします。

Security Directory Server での DB2 オンライン・バックアップおよびオフライン復元の手順

ここに示す情報により、オンライン・バックアップおよびオフライン復元の手順について知ることができます。

このタスクについて

ディレクトリー・データベースのオンライン・バックアップの設定 (変更ログなし)

1. バックアップおよびリカバリーに使用するファイルを保管するための安全な場所 (バックアップ・マシンや単独のメディアなど) を使用します。リストになっている例では、ファイルの保管場所として /safeflace ディレクトリーを使用しています。DB2 インスタンス所有者には、/safeflace ディレクトリーの書き込み権限が必要です。以下の例では、Security Directory Server インスタンスおよびデータベースの名前を ldapdb2 にしています。
2. Security Directory Server の構成ファイルおよびスキーマ・ファイルを安全な場所に保存します。これらのファイルを更新する必要があるのは、トポロジー、構成パラメーター、またはスキーマを変更した場合に限られます。

```
cp /home/ldapdb2/idsslapd-ldapdb2/etc/* /safeflace/etc
```

3. ibmslapd が実行中でないことを確認してください。

```
ibmslapd -I ldapdb2 -k
```

4. リカバリーに備えて、ログ・ファイルはデータベースとは物理的に異なるドライブに保存してください。この例では、/safeflace/db2logs-ldapdb2 ディレクトリーが安全な場所として使用されます。すべての DB2 コマンドを DB2 インスタンス所有者として実行する必要があります。

```
db2 update db config for ldapdb2 using newlogpath /safeflace/db2logs-ldapdb2
```

5. ログのアーカイブ処理をオンにしてオンライン・バックアップをサポートするため、ディレクトリー・サーバー・データベースを更新します。

```
db2 update db config for ldapdb2 using logarchmeth1 logretain
db2 force applications all
db2stop
db2start
```

6. アーカイブ・ロギングを設定したら、完全オフライン・バックアップを作成する必要があります。データベースの完全オフライン・バックアップを作成します。

```
db2 backup db ldapdb2 to /safeflace/sun-full-ldapdb2
```

7. ディレクトリー・サーバー・インスタンスを始動します。

```
ibmslapd -I ldapdb2
```

ディレクトリー・データベースの完全オンライン・バックアップの作成

1. 完全バックアップを毎晩作成し、ログ・ファイルをログ・ファイルのパスからコピーします (バックアップの作成頻度は必要に応じて高めます)。

注: オンライン・バックアップ・イメージをリカバリーに使用できるのは、バックアップ操作が実行された時間のログがある場合に限られます。

```
db2 backup db ldapdb2 online to /safeflace/mon-ldapdb2
```

2. ログのパスを確認します。DB2 により、指定したパスにノードが付加されます。

```
db2 get db config for 1dapdb2 | grep -i "Path to log files"
```

返される情報の例を以下に示します。

```
Path to log files= /safeplace/db2logs-1dapdb2/NODE0000/
```

ディレクトリー・データベースの復元

水曜日の朝に、使用しているマシンのディスク駆動装置が故障したとします。ファイルおよびログのバックアップに使用している /safeplace ディレクトリーは影響を受けなかったため、これを復元に使用できます。

データベースを復元するために別のマシンを使用する場合は、バックアップ済みマシンの /safeplace ディレクトリーを新しいマシンのローカル /safeplace ディレクトリーにセットアップする必要があります。このディレクトリーには、/safeplace/db2log-1dapdb2/NODE0000 ディレクトリーにあるログ・ファイルのほか、使用されるすべてのバックアップ・ディレクトリーを組み込む必要があります。

1. 必要に応じて、Security Directory Server をインストールします。
2. バックアップ・マシンに指定したものと同一情報を使用してデータベースを構成します。
3. 以前にバックアップした構成ファイルおよびスキーマ・ファイルをコピーするか、tar ファイルを作成します。

```
cp /safeplace/etc/* /home/1dapdb2/idssl1apd-1dapdb2/etc
```

4. 火曜日のバックアップからディレクトリー・データベースを復元します。

```
db2 restore db 1dapdb2 from /safeplace/tues-1dapdb2 taken  
at <timestamp_of_backup>
```

注: <timestamp_of_backup> オプションが必要なのは、指定したディレクトリー・パスに複数のバックアップ・イメージがある場合だけです。

新しいマシン上で復元している場合は、次の警告メッセージが表示されます。

```
SQL2523Warning!Restoring to an existing database that  
is different from the database on the backup image, but  
have matching names. The target database will be  
overwritten by the backup version. The Roll-forward  
recovery logs associated with the target database will be deleted.  
続行しますか?(y/n) y  
DB20000IThe RESTORE DATABASE command completed successfully.
```

5. 新しいデータベースのログのパスを、ログ・ファイルに使用していたのと同じパスに設定します。新しいシステム上で復元している場合は、旧システムから新システムへログ・ファイルをコピーする必要があります。

```
db2 update db config for 1dapdb2 using  
newlogpath /safeplace/db2logs-1dapdb2
```

6. ログ・ディレクトリーに置かれているすべてのログをロールフォワードします。ここでは、火曜日の晩のバックアップ以降の変更内容が記録されています。

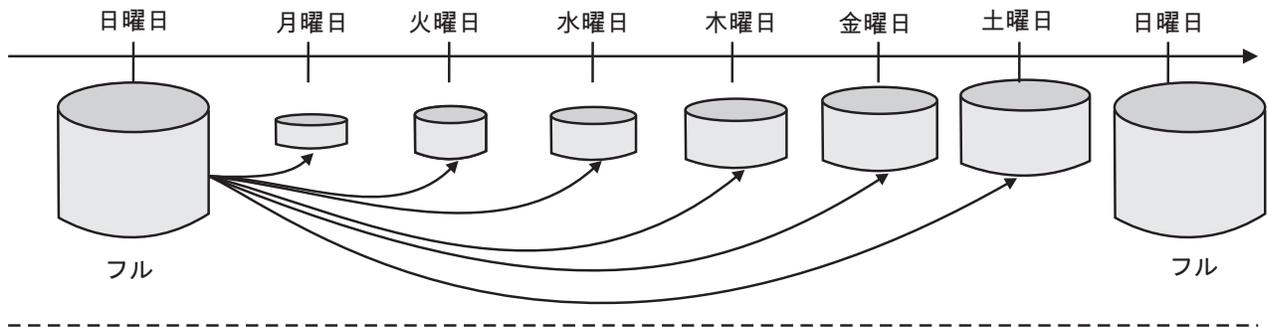
```
db2 rollforward db 1dapdb2 to end of logs and stop
```

注: この場合、リカバリーに必要なのは、最後の完全バックアップ・イメージと、バックアップ実行以降の時間にわたるログのみです。

リカバリーに使用するディレクトリー・データベースおよび変更ログ・データベースの両方を対象とする増分オンライン・バックアップの設定

このセクションおよび後続のセクションで基本になっているのは、日曜日に完全バックアップを実行し、その週の間は増分バックアップを使用するという週単位のスケジュールを採用したバックアップ方式です。

増分累積バックアップ



差分バックアップ

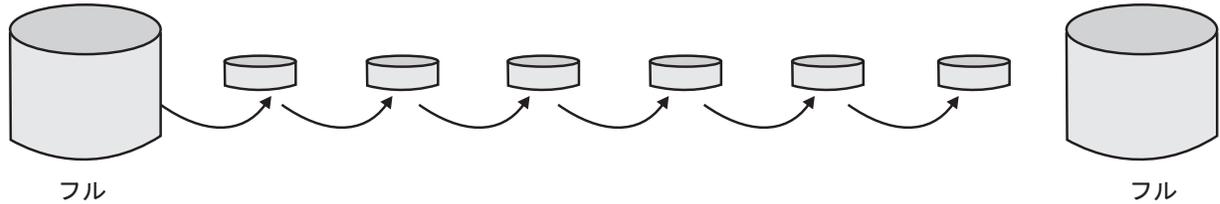


図 22. 増分累積バックアップおよび差分バックアップ

1. バックアップおよびリカバリーに使用するファイルを保管するための安全な場所 (バックアップ・マシンや単独のメディアなど) を使用します。リストになっている例では、ファイルの保管場所として `/safeplace` ディレクトリーを使用しています。変更ログを構成していない場合は、`ldapclog` を含むすべてのコマンドは無視されることがあります。
2. Security Directory Server の構成ファイルおよびスキーマ・ファイルを安全な場所に保存します。これらのファイルを更新する必要があるのは、トポロジー、構成パラメーター、またはスキーマを変更した場合に限られます。以下の例では、Security Directory Server のインスタンス名およびデータベース・インスタンス名として `ldapdb2` を使用しています。

```
cp /home/ldapdb2/idsslapd-ldapdb2/etc/*/safeplace/etc
```

3. `ibmslapd` が実行中でないことを確認してください。

```
ibmslapd -I ldapdb2 -k
```

注: この例では、ログ・ファイルのパスをデフォルトの場所から変更していません。ここでは、ディレクトリー・データベースと変更ログ・データベースの両方に対してデフォルトのログ・パスが使用されます。リカバリーに備えて、ログ・ファイルはデータベースとは物理的に異なるドライブに保存してください。

4. アーカイブ・ロギングをオンにしたオンライン・バックアップのサポートと、`trackmod` をオンにした増分バックアップのため、ディレクトリー・サーバー・データベースおよび変更ログ・データベースを更新します。

注: 増分バックアップをサポートするために `trackmod` をオンに設定すると、データベースの更新操作または挿入操作の実行時パフォーマンスに影響を及ぼすことがあります。

```
db2 update db cfg for ldapdb2 using logarchmeth1 logretain trackmod on
db2 update db config for ldapclog using logarchmeth1 logretain trackmod on
db2 force applications all
db2stop
db2start
```

ディレクトリー・データベースおよび変更ログ・データベースの両方を対象とする完全オフライン・バックアップの作成

1. ディレクトリー・データベースと変更ログ・データベースの両方を対象に、日曜日にデータベースの完全オフライン・バックアップを作成します。

```
db2 backup db ldapdb2 to /safep/ace/sun-full-ldapdb2
db2 backup db ldapclog to /safep/ace/sun-full-ldapclog
```

2. ディレクトリー・サーバー・インスタンスを始動します。

```
ibmslapd -i ldapdb2
```

ディレクトリー・データベースおよび変更ログ・データベースの両方を対象とする増分オンライン・バックアップの作成

1. 増分バックアップを毎日作成します。必要と判断した場合は、作成頻度を高くします。

注: オンライン・バックアップ・イメージをリカバリーに使用できるのは、バックアップ操作が実行された時間のログがある場合にに限られます。ディレクトリー・データベースのログと変更ログ・データベースのログは異なるパスに同一名で保存されます(例: S0000000.LOG および S0000001.LOG)。このため、変更ログを構成する場合には、これらのログ・ファイルを異なるディレクトリーに保存する必要があります。

```
db2 backup db ldapdb2 online incremental to /safep/ace/mon-ldapdb2
```

2. ディレクトリー・データベースのログ・ファイルへのパスを確認します。

```
db2 get db config for ldapdb2 | grep -i "Path to log files"
```

表示される出力の例を以下に示します。

```
Path to log files = /home/ldapdb2/ldapdb2/NODE0000/SQL00001/SQLLOGDIR/
cp /home/ldapdb2/ldapdb2/NODE0000/SQL00001/SQLLOGDIR/*
/safep/ace/db2logs-ldapdb2
db2 backup db ldapclog online incremental to /safep/ace/mon-ldapclog
```

3. 変更ログ・データベースのログ・ファイルへのパスを確認します。

```
db2 get db config for ldapclog | grep "Path to log files"
```

表示される出力の例を以下に示します。

```
Path to log files= /home/ldapdb2/ldapdb2/NODE0000/SQL00002/SQLLOGDIR/
cp /home/ldapdb2/ldapdb2/NODE0000/SQL00002/SQLLOGDIR/*
/safep/ace/db2logs-ldapclog
```

ディレクトリー・データベースおよび変更ログ・データベースの復元

水曜日の朝に、使用しているマシンのディスク駆動装置が故障したとします。ファイルのバックアップに使用している /safeplace ディレクトリーは影響を受けなかったため、これを復元に使用できます。

データベースを復元するために別のシステムを使用する場合は、バックアップ済みシステムの /safeplace ディレクトリーを新しいシステムのローカル /safeplace ディレクトリーにセットアップする必要があります。このディレクトリーには、/safeplace/db2log-ldapdb2/NODE0000 ディレクトリーおよび /safeplace/db2log-ldaplog/NODE0000 ディレクトリーにあるログ・ファイルのほか、使用されるすべてのバックアップ・ディレクトリーを組み込む必要があります。

1. 必要に応じて、Security Directory Server をインストールします。以前に指定したものと同一情報を使用して新しいデータベースを構成します。以前にバックアップした構成ファイルおよびスキーマ・ファイルをコピーします。

```
cp/safeplace/etc/*/*home/1dapdb2/idsslapd-1dapdb2/etc
```

2. ibmslapd が実行中でないことを確認してください。

```
ibmslapd -l 1dapdb2 -k
```

3. ディレクトリー・データベースを復元します。復元する最後のバックアップ・イメージは、ターゲット・イメージと呼ばれます。ターゲット・イメージは、復元手順の最初と最後の 2 回復元する必要があります。火曜日の増分バックアップを復元するには、以下のコマンドを実行します。

```
db2 restore db 1dapdb2 incremental from /safeplace/tues-1dapdb2
db2 restore db 1dapdb2 incremental from /safeplace/sun-full-1dapdb2
db2 restore db 1dapdb2 incremental from /safeplace/tues-1dapdb2
```

4. 以前にバックアップしたログ・ファイルをデフォルトのログ・パスの場所へコピーします。

```
cp /safeplace/db2logs-1dapdb2/*
/home/1dapdb2/1dapdb2/NODE0000/SQL00001/SQLLOGDIR
```

```
db2 rollforward db 1dapdb2 to end of logs and stop
```

5. 変更ログ・データベースを復元します。

```
db2 restore db 1daplog incremental from /safeplace/tues-1daplog
db2 restore db 1daplog incremental from /safeplace/sun-full-1daplog
db2 restore db 1daplog incremental from /safeplace/tues-1daplog
```

6. 以前にバックアップしたログ・ファイルをデフォルトのログ・パスの場所へコピーします。

```
cp /safeplace/db2logs-1daplog/*
/home/1dapdb2/1dapdb2/NODE0000/SQL00002/SQLLOGDIR
```

```
db2 rollforward db 1daplog to end of logs and stop
```

注: この場合、リカバリーに必要なのは、完全バックアップ・イメージと最後の増分バックアップです。火曜日までのバックアップを復元するのに月曜日の増分バックアップは必要ありません。

増分差分バックアップの使用

増分バックアップを使用する例では、次の完全バックアップが実行されるまで、増分バックアップによりサイズが増大します。これは、バックアップには長期間にわたり累積している変更が含まれるためです。したがって、月曜日に保存された変更より土曜日に保存された変更の方が多くなります。DB2 では、あらゆる種類の最終バックアップ以降の変更のみが保存される「差

分」バックアップも許可されます。このような差分バックアップは、サイズがかなり小さく、より短時間で実行できます。復元時には、前回の完全バックアップまたは増分バックアップ以降のすべての差分が必要です。

ldapdb2 データベースのオンライン差分バックアップを毎日実行するコマンドを以下に示します。

```
db2 backup db ldapdb2 online incremental delta to /safeplace/mon-delta-ldapdb2
db2 backup db ldapdb2 online incremental delta to /safeplace/tues-delta-ldapdb2
db2 backup db ldapdb2 online incremental delta to /safeplace/wed-delta-ldapdb2
db2 backup db ldapdb2 online incremental delta to /safeplace/thurs-delta-ldapdb2
db2 backup db ldapdb2 online incremental delta to /safeplace/fri-delta-ldapdb2
db2 backup db ldapdb2 online incremental delta to /safeplace/sat-delta-ldapdb2
```

差分バックアップを使用する場合は、データベース用のログ・ファイルを安全な場所に保存する必要があります。デフォルトのログ・パスを使用する場合は、パスを `/safeplace/db2logs-ldapdb2` ディレクトリーにコピーするか、データベース構成を変更して、パスを `/safeplace/db2logs-ldapdb2` ディレクトリーに直接保存します。

増分差分バックアップからの復元

例では、バックアップ・マシンのデータベース用のログ・ファイルが、差分バックアップの復元に使用するマシンで取得できるようになっています。デフォルトのログ・パスを使用する場合は、バックアップ・マシン上の `/safeplace/db2logs-ldapdb2/NODE0000` ディレクトリーにあるログ・ファイルを復元先マシン上のデフォルトのログ・パスにコピーするか、新規マシン上でデータベース構成の `newlogpath` を変更して `/safeplace/db2logs-ldapdb2/NODE0000` ディレクトリーに直接コピーする必要があります。差分バックアップから復元する場合には、前回の完全バックアップまたは増分バックアップ以降のすべての差分が必要です。

ldapdb2 データベースのオンライン差分バックアップを復元するコマンドを以下に示します。

```
db2 restore db ldapdb2 incremental from /safeplace/sat-delta-ldapdb2
db2 restore db ldapdb2 incremental from /safeplace/sun-full-ldapdb2
db2 restore db ldapdb2 incremental from /safeplace/mon-delta-ldapdb2
db2 restore db ldapdb2 incremental from /safeplace/tues-delta-ldapdb2
db2 restore db ldapdb2 incremental from /safeplace/wed-delta-ldapdb2
db2 restore db ldapdb2 incremental from /safeplace/thurs-delta-ldapdb2
db2 restore db ldapdb2 incremental from /safeplace/fri-delta-ldapdb2
db2 restore db ldapdb2 incremental from /safeplace/sat-delta-ldapdb2
```

注: ターゲット・イメージは、最初と最後の 2 回復元する必要があります。

ログをコピーしてロールフォワードを実行します。

```
cp /safeplace/db2logs-ldapdb2/*
/home/ldapdb2/ldapdb2/NODE0000/SQL0001/SQLLOGDIR/
db2 rollforward db ldapdb2 to end of logs and stop
```

各種のバックアップと復元方法の長所と欠点

ここに示す情報により、各種のバックアップと復元方法の長所と欠点について知ることができます。

データベースが書き込み頻度の高い作業に使用される場合は、オンラインの完全バックアップが効率的である場合があります。データベースの更新を追跡すると、その頻度を最小限にとどめた場合でも、データを更新または挿入するトランザクションの実行時パフォーマンスに影響を及ぼす可能性があります。

大半の作業が読み取り専用で、書き込み作業は一部に過ぎないデータベースを保護する 1 つの方法として、増分バックアップを使用できます。このことは、データベースをリカバリー可能にする上で重要になります。増分バックアップ・イメージは、最後の正常な完全バックアップ操作以降に変更されたすべてのデータベース・データのコピーです。これは累積バックアップ・イメージとも呼ばれます。増分バックアップ・イメージの先行イメージは、必ず同じオブジェクトの正常な最後の完全バックアップになります。この方法では、最後の完全バックアップと最後の累積増分バックアップを保存する必要があります。データベースを復元するためには両方のバックアップを使用するためです。

増分差分バックアップ・イメージは、正常な最後のバックアップ (完全バックアップ、増分バックアップ、または増分差分バックアップ) 以降に変更されたすべてのデータベース・データのコピーです。差分バックアップ・イメージまたは非累積的バックアップ・イメージという別名もあります。差分バックアップは小サイズですが、データベースを復元するには、最後の完全バックアップ以降または累積増分バックアップ以降のすべての差分が必要です。

アーカイブ・ログの管理

ここに示す情報により、アーカイブ・ログの管理について、いくつかの例と併せて知ることができます。

オンライン・バックアップを使用する場合は、データベースを復元するためにアーカイブ・ログが必要になる可能性がある限り、アーカイブ・ログを保存しておく必要があります。アーカイブ・ログが必要になるかどうかは、バックアップの方法および目的により異なります。この原則は、ログのアーカイブ処理を「自動化」するいずれかのログ・アーカイブ・オプションを構成した場合でも適用されます。アーカイブ・スペースがいっぱいにならないように、古いログ・ファイルが消費可能になったらそのファイルを削除する計画を立てる必要があります。判断が必要な重要事項の 1 つは、最新のバックアップまでのデータを回復するか、システム障害直前までのデータを回復するかです。ディスクが故障し、データベースをバックアップから復元する必要がある場合は、バックアップ時に作成したログ・ファイルが必要です。復元作業後、データベースの状態を、最後のバックアップ後に存在した整合状態にするため、ログ・ファイルはロールフォワードされます。最後のバックアップ以降に生成されたすべてのログ・ファイルを保存していた場合は、クラッシュ直前の時点までログを再生できます。こうすると、ディレクトリーの更新情報の損失を大幅に低減するのに役立ちます。次に重要な項目は、バックアップの方法とスケジュールです。以下の例について考えます。

1. 完全なオンライン・バックアップを毎日実行する場合は、少なくとも最後のバックアップ操作時にアクティブだったログ・ファイルを保存しておく必要があります。最後のバックアップの開始時以降に生成されたすべてのログを保存してある場合は、ディスクの障害やシステム障害などの事態が発生する直前の時点までデータベースを復元するために必要なすべてのデータが揃っています。最後のバックアップより前にアーカイブしたログ・ファイルは、ディスク・スペースを空けるためにすべて削除できます。
2. 完全なオンライン・バックアップを週 1 回実行し、それ以降次の週までの間は増分バックアップを毎日実行する場合は、少なくとも最後の (完全または増分) バックアップ時にアクティブだったログを保存する必要があります。また、この

方法では、最後の完全バックアップより前のすべてのアーカイブ・ログは必要でなくなっているため、削除して構いません。

3. 完全なオンライン・バックアップを週 1 回実行し、それ以降の週までの間は増分差分バックアップを毎日実行する場合は、最後の (完全または差分) バックアップ時にアクティブだったログを保存する必要があります。データを損失した時点までのデータを復元するには、最後のバックアップ操作以降のすべてのログを保存する必要があります。最後の完全バックアップより前にアーカイブしたログ・ファイルは、すべて削除できます。

DB2 バックアップ、復元、およびロールフォワード・コマンド・オプションのその他の例

DB2 バックアップ、復元、およびロールフォワード・コマンド・オプションの以下に示す例を使用できます。

データベースを特定の時点の状態に復元し、その時点より後の変更はロールフォワードしない場合は、「without rolling forward」オプションを指定すると、ロールフォワード保留状態の復元済みデータベースを DB2 が変更しないようにすることができます。

```
db2 restore db ldapdb2 from /safepplace taken at 20040405154705 without rolling forward
```

バックアップ・データベース・イメージが 1 つだけ保管されているパスの入力を要求せずにデータベースを復元するには、次のコマンドを使用します。

```
db2 restore db ldapclog from /safepplace/full-backup-ldapclog without rolling forward without prompting
```

データベースをある時点までオフライン・ロールフォワードするためのコマンドは、次のとおりです。

```
db2 rollforward database ldapdb2 to 2004-04-22-14.54.21.253422 and stop
```

このコマンドを実行すると、データベース構成ファイルに指定されているログ・フォルダーに置かれているすべてのログが、例に記載されている時点までロールフォワードされます。「and stop」というキー・フレーズが指定されているため、未完了のトランザクションをロールバックし、データベースのロールフォワード保留状態を解除することにより、ロールフォワード・リカバリー処理が実行されます。

DB2 バックアップ、復元、またはロールフォワード時に発生することのある共通の問題

以下に示すシナリオでは、データベース名 ldapdb2 を使用します。変更ログの場合は、変更ログデータベース ldapclog を使用できます。

シナリオ 1

ibmslapd の実行中にオンライン・バックアップ・パラメーターのデータベース構成を更新しようとする場合は、次のコマンドを実行します。

```
db2 update db cfg for ldapdb2 using logarchmeth1 logretain trackmod on
```

```
DB20000IThe UPDATE DATABASE CONFIGURATION command completed successfully.
```

```
SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, all applications must disconnect from this database before the changes become effective.
```

このメッセージが表示された場合は、ibmslapd を停止してから再始動して変更内容を有効にする必要があります。以下のコマンドを使用します。

```
ibmslapd -I ldapdb2 -k
ibmslapd -I ldapdb2
```

シナリオ 2

logretain を設定せずにオンライン・バックアップを実行しようとする場合は、次のコマンドを実行します。

```
db2 backup database ldapdb2 online to /safeplace
```

```
SQL2413N Online backup is not allowed because either logretain or userexit
for roll-forward is not activated, or a backup pending condition is in
effect for the database.
```

アーカイブ・ロギング・パラメーターを設定して、データベース ldapdb2 のロールフォワード・リカバリーを使用可能にするには、次の DB2 コマンドを実行する必要があります。

```
db2 update db config for ldapdb2 using logarchmeth1 logretain
```

アーカイブ・ロギングを構成したら、ユーザーはデータベースの完全バックアップを作成する必要があります。この状態は、backup_pending フラグ・パラメーターにより表示されます。完全バックアップを作成していなかった場合は、ユーザーがデータベースに接続すると、以下のメッセージが表示されます。

```
db2 connect to ldapdb2
SQL1116N A connection to or activation of database <ldapdb2>
cannot be made because of a BACKUP PENDING.
```

データベースは、オフライン・バックアップが実行されるまでバックアップ保留状態になります。このため、サーバーがデータベースに接続するとサーバーに障害が発生し、構成モード限定で始動します。

シナリオ 3

次のコマンドを実行して、完全バックアップを作成します。

```
db2 backup database ldapdb2 to /safeplace
```

バックアップが成功すると、次のメッセージが表示されます。

```
Backup successful.The timestamp for this backup image is : 20040308170601
```

シナリオ 4

ibmslapd を実行中にデータベースを復元しようとする、次のメッセージが表示されます。

```
db2 restore db ldapdb2 from /safeplace
SQL1035N The database is currently in use.
```

シナリオ 5

復元してからロールフォワードを実行することが必要になった場合は、以下のコマンドを実行します。

```
db2 connect to ldapdb2
SQL1117N A connection to or activation of database "LDAPDB2" cannot be made
because of ROLL-FORWARD PENDING.SQLSTATE=57019
```

データベースは、ロールフォワード・コマンドが実行されるまでロールフォワード保留状態になります。このため、サーバーがデータベースに接続するとサーバーに障害が発生し、構成モード限定で始動します。

付録 N. SSL セキュリティーのセットアップ – SSL シナリオ

SSL セキュリティーのセットアップ – SSL シナリオで想定される条件を使用できません。

この付録で提供するシナリオは、IBM Security Directory Server システムの各種コンポーネント間でセキュア接続を作成するためのものです。

以下の条件が想定されます。

- IBM Security Directory Server 6.3 がマシンにインストールされています。
- IBM Security Directory Server インスタンスが作成されています。
- IBM Security Directory Server データベースが作成されています。
- 作成された鍵データベース (.kdb) ファイルまたは鍵ストア (.jks) ファイルがありません。

組み込み WebSphere Application Server バージョン 7.x での HTTPS の使用

組み込みバージョンの WebSphere Application Server バージョン 7.x は、デフォルトではポート 12101 で HTTPS を実行するように設定されています。以下に示す Web アドレスは、別のシチュエーションで使用することもできます。

HTTPS を使用するには、ログイン Web アドレスを以下のアドレスに変更する必要があります。

```
https://<hostname>:12101/IDSWebApp/IDSjsp/Login.jsp
```

非 HTTPS 接続の場合、以下の Web アドレスを使用します。

```
http://<hostname>:12100/IDSWebApp/IDSjsp/Login.jsp
```

さらに、アプリケーション・サーバーの SSL 証明書を変更する場合は、WebSphere Application Server が使用する新規の鍵ファイルとトラスト・ストア・データベース・ファイルを作成します。デフォルトでは、鍵とトラストの 2 つのストア・データベース・ファイルは独立しており、<WAS_HOME>/profiles/TDSWebAdminProfile/etc/ ディレクトリーに置かれています。これらのファイルには、それぞれ DummyServerKeyFile.jks および DummyServerTrustFile.jks という名前が付けられます。

新しい jks ファイルを作成すると、<WAS_HOME>/profiles/TDSWebAdminProfile/config/cells/DefaultNode/security.xml ファイル内の次の項目 (太字で強調表示されている箇所) を追加または変更することにより、IBM WebSphere Application Server が使用している鍵とトラストのストア・データベース・ファイルを変更して、新しいファイル名、パスワード、およびファイル形式を使用できるようになります。

```
<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"/>
```

IBM Security Directory Server および IBM Security Directory Server Web 管理ツール間でのセキュア接続の作成

以下に示す手順を使用して、IBM Security Directory Server と IBM Security Directory Server Web 管理ツールとの間のセキュア接続を作成できます。

このタスクについて

鍵ペアと、自己署名鍵ストア・ファイル (.jks) および鍵データベース・ファイル (.kdb) に対する認証要求を作成します。

注:

1. IBM Security Directory Server の資料の『インストールと構成』セクションの付録『CMS 鍵データベースをサポートするための GSKit のセットアップ』を参照してください。
2. 鍵ペアの作成の指示、および自己署名鍵ストア・ファイル (.jks) と鍵データベース・ファイル (.kdb) に対する認証要求の作成の指示は、鍵データベースまたは鍵ストア・ファイルが作成されていないという前提で記述されています。使用する鍵データベースまたは鍵ストア・ファイルをすでに作成している場合は、ステップ 5 (744 ページ) までスキップしてかまいません。鍵データベースは、1 つ以上の鍵ペアと証明書を保管するためにクライアントやサーバーが使用するファイルです。

唯一の必要要件は、鍵ストア・ファイルおよび鍵データベース・ファイルを、GSKit および Java がインストールされているマシンで作成することです。

注: 1 つの Web アプリケーション・サーバーで作成できる鍵ストア・ファイル (.jks) は 1 つのみです。

ユーザーは、以下の証明書のいずれかを要求できます。

- VeriSign から発行される低保証証明書。これは、機密保護機能のある環境のベータ・テストなど、非商用目的に最適です。
- インターネット上で商用ビジネスを行うためのサーバー証明書。VeriSign やその他の CA から入手できます。
- 自己署名サーバー証明書 (プライベートな Web ネットワークにおいて、自分自身の CA として機能する場合)。

VeriSign などの CA を利用してサーバー証明書に署名する方法については、168 ページの『鍵ペアの作成と認証局からの証明書の要求』を参照してください。

手順

1. 以下のアクションを実行して、Security Directory Server がインストールされたシステムで鍵データベース (.kdb) ファイルを作成します。
 - a. ikeyman と入力して、Java ユーティリティを開始します。
 - b. 「鍵データベース・ファイル」を選択します。
 - c. 「新規」を選択します (鍵データベースがすでに存在する場合は、「開く」を選択します)。
 - d. 「鍵データベース・タイプ」リストから「CMS」を選択します。
 - e. 鍵データベース・ファイルの名前と場所を指定します。「OK」をクリックします。
 - f. 指示に従って、鍵データベース・ファイルのパスワードを入力します。「OK」をクリックします。
 - g. 「作成」->「新しい自己署名証明書 (New Self-Signed Certificate)」に移動します。
 - h. 以下の値を入力します。
 - 鍵ペアのユーザー割り当てラベル。鍵データベース・ファイル内の鍵ペアと証明書は、このラベルで識別されます。

注: このラベルは控えておいてください。
 - 必要な証明書のバージョン。
 - 必要な鍵のサイズ。
 - サーバーの X.500 共通名。通常は、www.ibm.com のような TCP/IP 完全修飾ホスト名として入力します。
 - 組織名。これは、組織の名前です。
 - 組織の単位名。このフィールドは、必要に応じて入力します。
 - サーバーが設置されている地域。このフィールドは、必要に応じて入力します。
 - サーバーが設置されている都道府県の省略形 (3 文字)。これはオプション・フィールドです。
 - サーバーが設置されている場所に該当する郵便番号。このフィールドは、必要に応じて入力します。
 - サーバーの設置場所の国別コード (2 文字)。
 - 証明書の有効期間。
 - i. 「OK」をクリックします。
2. 以下のアクションを実行して、Web 管理ツールがインストールされたシステム上で、自己署名鍵ストア・ファイル (.jks) を作成します。
 - a. ikeyman と入力して、Java ユーティリティを開始します。
 - b. 「鍵データベース・ファイル」を選択します。
 - c. 「新規」を選択します (鍵データベースがすでに存在する場合は、「開く」を選択します)。
 - d. 「鍵データベース・タイプ」リストから「JKS」を選択します。
 - e. 鍵ストア・ファイルの名前と場所を指定します。「OK」をクリックします。

- f. 指示に従って、鍵ストア・ファイルのパスワードを入力します。「OK」をクリックします。
 - g. 「作成」->「新しい自己署名証明書 (New Self-Signed Certificate)」に移動します。
 - h. 以下の値を入力します。
 - 鍵ペアのユーザー割り当てラベル。鍵データベース・ファイル内の鍵ペアと証明書は、このラベルで識別されます。

注: ステップ 1g で使用したのと同じラベルは使用しないようにしてください。

 - 必要な証明書のバージョン。
 - 必要な鍵のサイズ。
 - サーバーの X.500 共通名。通常は、www.ibm.com のような TCP/IP 完全修飾ホスト名として入力します。
 - 組織名。これは、組織の名前です。
 - 組織の単位名。このフィールドは、必要に応じて入力します。
 - サーバーが設置されている地域。このフィールドは、必要に応じて入力します。
 - サーバーが設置されている都道府県の省略形 (3 文字)。これはオプション・フィールドです。
 - サーバーが設置されている場所に該当する郵便番号。このフィールドは、必要に応じて入力します。
 - サーバーの設置場所の国別コード (2 文字)。
 - 証明書の有効期間。
 - i. 「OK」をクリックします。
3. 証明書を .kdb ファイルから .jks ファイルへ抽出します。
 - a. 「鍵データベース・ファイル」を選択します。
 - b. 「開く」を選択します。
 - c. 鍵データベース・タイプ、鍵データベース (.kdb) のファイル名と場所を選択します。ここでは先に作成した鍵データベース・ファイルを選択します。
 - d. 指示に従って、パスワードを指定します。
 - e. 「OK」をクリックします。
 - f. 「個人用証明書」を選択します。
 - g. 「証明書の抽出 (Extract Certificate)」をクリックします。
 - h. 「データ・タイプ」を選択します。このシナリオでは、「バイナリー DER データ」を選択します。「データ・タイプ」では、.arm ファイルを作成する「Base-64 エンコード ASCII データ」を選択することもできます。
 - i. ファイル名と場所を指定します。このファイル名と場所は覚えておいてください。
 - j. 必要な場合は、サーバー・システムから抽出したサーバー証明書をクライアント・システムに転送します。
 - k. 「鍵データベース・ファイル」を選択します。

- l. 「開く」を選択します。
 - m. 鍵データベース・タイプ、鍵ストア (.jks) のファイル名と場所を選択します。ここでは先に作成した鍵ストア・ファイルを選択します。
 - n. 指示に従って、パスワードを指定します。
 - o. 「OK」をクリックします。
 - p. 「署名者証明書 (Signer Certificates)」に移動します。
 - q. 「追加」をクリックします。
 - r. 鍵データベース (.kdb) ファイル用に以前作成した「バイナリー DER データ」(.der) ファイルを選択します。
 - s. 「OK」をクリックします。
 - t. 証明書のラベルを入力します。
 - u. 「OK」をクリックします。
4. 証明書を .jks ファイルから .kdb ファイルへ抽出します。
 - a. 「鍵データベース・ファイル」を選択します。
 - b. 「開く」を選択します。
 - c. 鍵データベース・タイプ、鍵ストア (.jks) のファイル名と場所を選択します。ここでは先に作成した鍵ストア・ファイルを選択します。
 - d. 指示に従って、パスワードを指定します。
 - e. 「OK」をクリックします。
 - f. 「個人証明書」に移動します。
 - g. 「証明書の抽出 (Extract Certificate)」をクリックします。
 - h. 「データ・タイプ」を選択します。このシナリオでは、「バイナリー DER データ」を選択します。
 - i. ファイル名と場所を指定します。このファイル名と場所は覚えておいてください。必要な場合は、クライアント・システムから抽出したクライアント証明書をサーバー・システムに転送します。
 - j. 「鍵データベース・ファイル」を選択します。
 - k. 「開く」を選択します。
 - l. 鍵データベース・タイプ、鍵データベース (.kdb) のファイル名と場所を選択します。ここでは先に作成した鍵データベース・ファイルを選択します。
 - m. 指示に従って、パスワードを指定します。
 - n. 「OK」をクリックします。
 - o. 「署名者証明書 (Signer Certificates)」に移動します。
 - p. 「追加」をクリックします。
 - q. 鍵ストア (.jks) ファイル用に以前作成した「バイナリー DER データ」(.der) ファイルを選択します。
 - r. 「OK」をクリックします。
 - s. 証明書のラベルを入力します。
 - t. 追加する証明書を選択して、「表示/編集」をクリックします。「証明書をトラステッド・ルートとして設定」チェック・ボックスが選択されていることを確認します。

- u. 「OK」をクリックします。
- 5. ディレクトリー・サーバー・インスタンスがまだ始動していない場合は、始動します。IBM Security Directory Server の資料の『インストールと構成』セクションの『ディレクトリー・サーバー・インスタンスの始動』を参照してください。
- 6. Web アプリケーション・サーバーを始動します。IBM Security Directory Server の資料の『インストールと構成』セクションの『Web 管理ツールを使用するための Web アプリケーション・サーバーの始動』を参照してください。
- 7. Web 管理ツールにログオンして、SSL が使用不可なサーバーを追加します。Web 管理ツールを起動します。
 - a. アプリケーション・サーバーを始動したら、Web ブラウザーから次のアドレスを入力します: <http://localhost:12100/IDSWebApp/IDSjsp/Login.jsp>

注: Web 管理ツールがインストールされているコンピューターでブラウザーを実行している場合に限り、このアドレスが使用できます。Web 管理ツールが別のコンピューターにインストールされている場合は、**localhost** を、Web 管理ツール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。

- b. コンソールにコンソール管理者としてログインします。
- c. 以下の指示に従い、SSL が使用不可なサーバーをコンソールに追加します。
 - 1) ナビゲーション領域で「**コンソール管理**」を展開します。
 - 2) 「**コンソール・サーバーの管理**」をクリックします。サーバー・ホスト名およびポート番号の表が表示されます。
 - 3) 「**追加**」をクリックします。
 - 4) 指定されたホスト名または IP アドレスおよびサーバー・ポートで実行されている登録済みの IBM Security Directory Server インスタンスを識別する、固有の名前を指定します。「directory server ログイン」パネルの「LDAP ホスト名」リストにサーバー名が表示されます。「サーバー名」フィールドに名前が指定されていない場合、「directory server ログイン」パネルの「LDAP ホスト名」リストに、サーバー・インスタンスの hostname:port の組み合わせが表示されます。
 - 5) 「**ホスト名**」フィールドに、サーバーのホスト名または IP アドレス (例えば、myserver.mycity.mycompany.com) を入力します。
 - 6) 「**ポート**」フィールドにサーバー・ポート番号を指定します。
 - 7) 「**サポートされる管理サーバー**」チェック・ボックスを選択して、管理ポートの制御を使用可能にします。
 - 8) 「**管理ポート**」フィールドに管理サーバー・ポート番号を指定します。
 - 9) 「**SSL 暗号化を使用可能にする**」チェック・ボックスがチェックされていないことを確認します。
 - 10) 「**OK**」をクリックし、確認パネルでもう一度「**OK**」をクリックします。
- d. ナビゲーション領域で「**ログアウト**」をクリックします。
- 8. ディレクトリー・サーバー・インスタンスの管理者としてログインします。

- a. IBM Security Directory Server Web 管理ツールのログイン・ページで、「LDAP ホスト名」フィールドのドロップダウン・メニューから、コンピューターの LDAP ホスト名または IP アドレスを選択します。
 - b. ディレクトリー・サーバー・インスタンスの管理者 DN およびパスワードを入力します。インスタンスの作成中に、これらのフィールドを指定しました。
 - c. 「ログイン」をクリックします。
9. Web 管理コンソールのセキュリティー設定を構成します。
- a. Web 管理コンソールに移動します。
 - b. 「サーバー管理」をクリックします。
 - c. 「セキュリティー・プロパティーの管理」をクリックします。
 - d. 「設定」をクリックします。
 - e. SSL 接続を使用可能にするには、「SSL」ラジオ・ボタンを選択します。ここで IBM Security Directory Server に設定したセキュリティー設定は、ディレクトリー管理サーバーにも適用されます。
 - f. 「サーバーおよびクライアントの認証」ラジオ・ボタンを選択します。

注: クライアントにサーバー証明書を配布する必要があります。サーバーおよびクライアント認証の場合は、クライアント証明書をサーバーの鍵データベースに追加する必要があります。

- g. 「鍵データベース」タブを選択します。
 - 1) 「鍵データベースのパスおよびファイル名」を指定します。これは、鍵データベース・ファイルの完全修飾ファイル仕様です。パスワード stash ファイルが定義されている場合、そのファイルの拡張子は **.sth** で、同じファイル仕様を持つものと見なされます。
 - 2) 「鍵パスワード」を指定します。パスワード stash ファイルが使用されていない場合は、鍵データベース・ファイルのパスワードをここで指定する必要があります。「パスワードの確認」フィールドにパスワードを再度入力します。
 - 3) 「鍵ラベル」を指定します。この管理者定義鍵ラベルは、鍵データベースのどの部分を使用するかを示します。

注: このファイルをサーバーで使用するには、ユーザー ID **idsldap** でこのファイルを読み取れるように設定する必要があります。ファイルのアクセス権について詳しくは、IBM Security Directory Server の資料の『トラブルシューティングとサポート』セクションを参照してください。

- h. 終了したら、次のいずれかの操作を実行します。
 - 「適用」をクリックして、変更を保存します (パネルは終了しません)。
 - 「OK」をクリックして変更を適用し、パネルを終了します。
 - 「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。
 - i. 変更内容を有効にするには、IBM Security Directory Server と管理サーバーの両方を停止して再始動する必要があります。
10. Web 管理コンソールのコンソール・プロパティー設定を構成します。

- a. アプリケーション・サーバーを再始動後、コンソールにコンソール管理者としてログインします。
- b. ナビゲーション領域で「**コンソール管理**」を展開します。
- c. 「**コンソール・プロパティの管理**」をクリックします。
- d. 「**コンポーネント管理**」をクリックし、コンソール内のすべてのサーバーで使用可能にするコンポーネントを指定します。デフォルトでは、すべてのコンポーネントが使用可能です。

注: ユーザーが適切なサーバー権限を持っていなかったり、必要な機能がサーバーに備わっていない場合、管理コンポーネントやそのタスクの一部は、たとえ使用可能であっても表示されません。

- e. 「**セッション・プロパティ**」をクリックし、コンソール・セッションのタイムアウト制限を設定します。デフォルトの設定は 60 分です。

注: セッションは、設定した時間が経過してから 3 分から 5 分間有効である場合があります。これは、タイマー間隔に作用するアプリケーション・サーバーのバックグラウンド・スレッドによってセッションの無効化が実行されるためです。このタイマー間隔によってセッションのタイムアウト期間が延長されます。

- f. 「**SSL 鍵データベース**」をクリックし、必要に応じて、Secure Sockets Layer (SSL) 経由で他の LDAP サーバーと通信できるようにコンソールをセットアップします。鍵データベースのパスとファイル名、鍵パスワード、トラステッド・データベースのパスとファイル名、トラステッド・パスワードを、該当するフィールドに設定します。サポートされるファイル・タイプは jks です。先に作成した .jks ファイルを使用してください。

注:

鍵データベースと SSL の詳細については、167 ページの『iKeyman ツール』および 154 ページの『Secure Sockets Layer』を参照してください。

- g. 「**OK**」をクリックします。

11. SSL が使用可能なサーバーをコンソールに追加します。

- a. ナビゲーション領域で「**コンソール管理**」を展開します。
- b. 「**コンソール・サーバーの管理**」をクリックします。
- c. 「**追加**」をクリックします。
- d. 指定されたホスト名または IP アドレスおよびサーバー・ポートで実行されている登録済みの IBM Security Directory Server インスタンスを識別する、固有の名前を指定します。「directory server ログイン」パネルの「LDAP ホスト名」リストにサーバー名が表示されます。「サーバー名」フィールドに名前が指定されていない場合、「directory server ログイン」パネルの「LDAP ホスト名」リストに、サーバー・インスタンスの hostname:port の組み合わせが表示されます。
- e. 「**ホスト名**」フィールドに、サーバーのホスト名または IP アドレス (例えば、myserver.mycity.mycompany.com) を入力します。
- f. 「**ポート**」フィールドにサーバー・セキュア・ポート番号を指定します。
- g. 「**サポートされる管理サーバー**」チェック・ボックスを選択して、管理ポートの制御を使用可能にします。

- h. 「管理ポート」フィールドに管理サーバー・セキュア・ポート番号を指定します。ポート番号と管理ポート番号は、SSL が使用可能なサーバーでは異なります。詳細については、「ヘルプ」を参照してください。
 - i. 「SSL 暗号化を使用可能にする」チェック・ボックスを選択します。
 - j. 「OK」をクリックし、確認パネルでもう一度「OK」をクリックします。
 - k. ナビゲーション領域で「ログアウト」をクリックします。
 - l. IBM WebSphere Application Server を再始動します。
12. Directory Server インスタンス管理者としてログインし、SSL が使用可能なサーバーが正しく追加されているか検証します。
- a. IBM Security Directory Server Web 管理ツールのログイン・ページで、「LDAP ホスト名」フィールドのドロップダウン・メニューから、コンピューターの LDAP ホスト名または IP アドレスを選択します。
 - b. ディレクトリー・サーバー・インスタンスの管理者 DN およびパスワードを入力します。インスタンスの作成中に、これらのフィールドを指定しました。
 - c. 「ログイン」をクリックします。
13. SSL が使用可能なローカル・ホストを、SSL のみ使用可能に構成します。
- a. Web 管理コンソールに移動します。
 - b. 「サーバー管理」をクリックします。
 - c. 「セキュリティー・プロパティーの管理」をクリックします。
 - d. 「設定」をクリックします。
 - e. SSL 接続を使用可能にするには、「SSL のみ」ラジオ・ボタンを選択します。
 - f. 「サーバーおよびクライアントの認証」ラジオ・ボタンを選択します。各クライアントにサーバー証明書を配布する必要があります。サーバーおよびクライアント認証の場合は、各クライアント証明書をサーバーの鍵データベースに追加する必要があります。
 - g. 終了したら、「適用」をクリックして変更を保存します。画面は終了しません。「OK」をクリックして、変更を適用し終了します。「キャンセル」をクリックし、変更を行わずにこのパネルを終了します。
 - h. 変更内容を有効にするには、IBM Security Directory Server と管理サーバーの両方を停止して再始動する必要があります。
14. 以下のコマンドを発行して、サーバーが SSL サーバーとして機能するか検証します。

```
idsldapsearch -D <admin_dn> -w <admin_pw> -Z-K <server_kdb_file>
-P <keyfile_password> -b "cn=localhost"
-p <server_secure_port> objectclass=*
```

IBM Security Directory Server C ベース・クライアントと IBM Security Directory Server 間の SSL 接続のセットアップ

以下に示す手順を使用して、IBM Security Directory Server C ベース・クライアントと IBM Security Directory Server との間の接続をセットアップできます。

手順

1. 以下のアクションを実行して、ikeyman ユーティリティを使用して、サーバー上に鍵データベース (.kdb) ファイルと自己署名証明書を作成します。
 - a. ikeyman と入力して、Java ユーティリティを開始します。
 - b. 「**鍵データベース・ファイル**」を選択します。
 - c. 「**新規**」を選択します (鍵データベースがすでに存在する場合は、「**開く**」を選択します)。
 - d. 鍵データベース・タイプ、鍵データベースのファイル名 (例えば、`<server_file> .kdb`) とロケーションを指定します。「**OK**」をクリックします。
 - e. 指示に従って、鍵データベース・ファイルのパスワードを入力します。
 - f. 「**ファイルにパスワードを隠しますか (Stash a password to a file)**」ボックスにチェック・マークが付いていることを確認します。
 - g. 「**OK**」をクリックします。
 - h. 「**作成**」->「**新しい自己署名証明書 (New Self-Signed Certificate)**」に移動します。
 - i. 以下のフィールドに値を入力します。
 - 鍵ペアのユーザー割り当てラベル。鍵データベース・ファイル内の鍵ペアと証明書は、このラベルで識別されます。

注: このラベルは控えておいてください。
 - 必要な証明書のバージョン。
 - 必要な鍵のサイズ。
 - サーバーの X.500 共通名。通常は、www.ibm.com のような TCP/IP 完全修飾ホスト名として入力します。
 - 組織名。これは、組織の名前です。
 - 組織の単位名。このフィールドは、必要に応じて入力します。
 - サーバーが設置されている地域。このフィールドは、必要に応じて入力します。
 - サーバーが設置されている都道府県の省略形 (3 文字)。これはオプション・フィールドです。
 - サーバーが設置されている場所に該当する郵便番号。このフィールドは、必要に応じて入力します。
 - サーバーの設置場所の国別コード (2 文字)。
 - 証明書の有効期間。
2. 以下のアクションを実行して、クライアント・マシンに新規の .kdb ファイルを作成します。
 - a. ikeyman と入力して、Java ユーティリティを開始します。
 - b. 「**鍵データベース・ファイル**」を選択します。
 - c. 「**新規**」を選択します (鍵データベースがすでに存在する場合は、「**開く**」を選択します)。

- d. 鍵データベース・タイプ、鍵データベース・ファイルの名前 (例えば、`<client_file> .kdb`)、およびロケーションを指定します。「OK」をクリックします。
 - e. 指示に従って、鍵データベース・ファイルのパスワードを入力します。
 - f. 「ファイルにパスワードを隠しますか (Stash a password to a file)」ボックスにチェック・マークが付いていることを確認します。
 - g. 「OK」をクリックします。
3. サーバー・マシンで以下のアクションを実行します。
 - a. `<server_file> .kdb` ファイルを開きます。
 - b. 「個人証明書」に移動します。
 - c. 「証明書の抽出 (Extract Certificate)」をクリックします。
 - d. ファイル名と場所を指定します。このファイル名と場所は、後で参照できるように、覚えておいてください。
 4. サーバー・マシンから抽出したサーバーの自己署名証明書をクライアント・マシンに転送します。
 5. クライアント・マシンで以下のアクションを実行します。
 - a. `<client_file> .kdb` ファイルを開きます。
 - b. 「署名者証明書 (Signer Certificates)」に移動します。
 - c. 「追加」をクリックします。
 - d. 「ブラウズ」をクリックして、クライアント・マシンに転送したサーバーの自己署名証明書を探します。
 - e. ファイルを開きます。
 - f. 「OK」をクリックします。
 - g. この証明書のラベルを入力します。

注: このラベルは、ステップ 1-i で定義したラベルと一致している必要があります。

- h. 証明書を選択して、「表示/編集」をクリックします。「証明書をトラステッド・ルートとして設定」ボックスが選択されていることを確認します。
- i. 「作成」->「新しい自己署名証明書 (New Self-Signed Certificate)」に移動します。
- j. 以下のフィールドに値を入力します。

- 鍵ペアのユーザー割り当てラベル。鍵データベース・ファイル内の鍵ペアと証明書は、このラベルで識別されます。

注: このラベルは控えておいてください。

- 必要な証明書のバージョン。
- 必要な鍵のサイズ。
- サーバーの X.500 共通名。通常は、`www.ibm.com` のような TCP/IP 完全修飾ホスト名として入力します。
- 組織名。これは、組織の名前です。
- 組織の単位名。このフィールドは、必要に応じて入力します。

- サーバーが設置されている地域。このフィールドは、必要に応じて入力します。
 - サーバーが設置されている都道府県の省略形 (3 文字)。これはオプション・フィールドです。
 - サーバーが設置されている場所に該当する郵便番号。このフィールドは、必要に応じて入力します。
 - サーバーの設置場所の国別コード (2 文字)。
 - 証明書の有効期間。
- k. 「**OK**」をクリックします。
 - l. 「**証明書の抽出 (Extract Certificate)**」をクリックします。
 - m. ファイル名と場所を指定します。このファイル名と場所は、後で参照できるよう、覚えておいてください。
 - n. 「**OK**」をクリックします。
6. クライアント・マシンから抽出したクライアントの自己署名証明書をサーバー・マシンに転送します。
 7. サーバー・マシンで以下のアクションを実行します。
 - a. `<server_file> .kdb` ファイルを開きます。
 - b. 「**署名者証明書 (Signer Certificates)**」に移動します。
 - c. 「**追加**」をクリックします。
 - d. 「**ブラウズ**」をクリックして、サーバー・マシンに転送したクライアントの自己署名証明書を探します。
 - e. ファイルを開きます。
 - f. 「**OK**」をクリックします。
 - g. 証明書のラベルを入力します。

注: このラベルは、ステップ 1-i で定義したラベルと一致している必要があります。

- h. 証明書を選択して、「**表示/編集**」をクリックします。「**証明書をトラステッド・ルートとして設定**」ボックスが選択されていることを確認します。
8. サーバー・マシン上で以下のコマンドを発行して、`ibmslapd.conf` ファイルの `cn=SSL,cn=Configuration` 項目を変更します。

```
idsldapmodify -p <port> -D <admin_dn> -w <admin_pw> -i <filename>
```

`<filename>` には、以下の項目が含まれています。

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSslAuth
ibm-slapdSslAuth: serverClientAuth
-
replace: ibm-slapdSecurity
ibm-slapdSecurity: SSLOnly
-
replace: ibm-slapdSSLKeyDatabase
ibm-slapdSSLKeyDatabase: <server_keyfile>
-
replace: ibm-slapdSSLKeyDatabasePW
ibm-slapdSSLKeyDatabasePW: <server_keyfile_password>
-
replace: ibm-slapdSslKeyRingFilePW
ibm-slapdSslKeyRingFilePW: <server_keyfile_password>
```

9. 変更した内容を有効にするには、ディレクトリー・サーバーおよび管理サーバーを再始動します。

10. クライアントから以下のコマンドを発行し、サーバーが SSL サーバーとして機能しているか検証します。

```
idsldapsearch -h <hostname> -p <server_secure_port> -D <admin_dn> -w <admin_pw>  
-K <keyfile> -b "cn=localhost" objectclass=*
```

注: 鍵ファイルのパスワードを `stash` ファイル内で指定する場合は、**-P** オプションを指定する必要はありません。

付録 O. 高可用性のシナリオ

ここに示す情報により、高可用性のシナリオの詳細を知ることができます。

IBM Security Directory Server は、高可用性 (HA) 構成で幅広くデプロイされます。標準の HA 構成では、ロード・バランサーがいくつかのピア・マスターよりも前に構成されます。ロード・バランシング機能 (仮想 IP サポートまたはレイヤー 4 ルーティングとも呼ばれる) は通常、ネットワーク・スイッチを使用して実装されます。Cisco、F5、Nortel などのスイッチ・ベンダーから販売されている多くのネットワーク・スイッチは、この機能を備えています。

HA 構成の場合、ロード・バランサーが構成される目的は、フェイルオーバー対応のみです。1 次マスターがダウンすると、このマスターに送られるすべてのトラフィックは、ピア・マスターのうちいずれかに転送されます。通常、元のピアへのフェイルバックは自動的に行われません。しかし、フェイルバックが必要なのは、新たに再始動したピアへの複製キューが空になった場合のみであるため、これは適切です。ロード・バランサーは、正常性検査メッセージを LDAP サーバーへ頻繁に送信します。大半のロード・バランサーでは、デフォルトの正常性検査メッセージは、TCP SYN パケットのように非常に基本的です。ターゲット・サーバーが ACK で応答した場合、ターゲット・サーバーは稼働中とみなされます。ただし、SYN パケットは、可用性の尺度としてはあまり正確ではありません。ACK はターゲット・サーバーがハング状態の場合にも返されるためです。

比較的大規模な構成の場合は、ロード・バランシングとフェイルオーバーの両方が必要な場合があります。通常、書き込みトラフィックのロード・バランシングは更新の競合を招く可能性があるため、得策ではありません。このため、一般的な手法の 1 つとして、フェイルオーバーを対象に構成されている仮想 IP アドレスをロード・バランサー内で使用するよう読み取り/書き込みアプリケーションを構成し、さらに、ロード・バランシングを対象に構成されている別の仮想 IP アドレスを読み取り専用アプリケーションが指すようにする方法があります。書き込みアクセスの場合、ロード・バランサーはピア・マスター間でフェイルオーバーを行うように構成されます。読み取りアクセスの場合は、読み取り専用レプリカ間またはピア・マスターと読み取り専用レプリカの組み合わせ間でフェイルオーバーまたはロード・バランシングが行われることがあります。

Security Directory Server のライセンス版には、プロキシ・サーバーも組み込まれています。プロキシ・サーバーには LDAP の読み取りと書き込みを区別する機能があるため、プロキシ・サーバーでは、書き込みのフェイルオーバーと読み取りのロード・バランシングが可能です。ただし、Single Point of Failure が存在しないように、いくつかのプロキシを保持することをお勧めします。プロキシは、通常、1 つまたはいくつかのロード・バランサーを介して動作します。

多くの LDAP アプリケーションでは、持続セッションが使用されます。持続セッションが使用される場合、フェイルオーバー・プロセスは高速にならない可能性があります。新しいセッションはバックアップ・サーバーにリダイレクトされる一方で、既存のセッションはタイムアウトになるまでに数分かかることがあるため、その間はサービスが提供されなくなります。この問題を解決するには、Security

Directory Server V6.1 以上のプロキシ・サーバーを使用します。これにより、既存のセッションを停止することなくフェイルオーバーできます。一部のロード・バランサー、例えば IBM WebSphere Application Server Network Deployment に組み込まれているソフトウェア・ロード・バランサーなどを構成すると、リセット (RST) パケットを任意の持続セッションに送信できるため、セッションをフェイルオーバー・サーバー上で素早く再確立できます。

HA 構成には、その他にもいくつかの特性があります。例えば、HA 構成のシナリオでは、1 つのシステムがダウンした場合、残りのシステムは負荷に耐えることができる必要があります。また、ネットワーク構成の冗長性を高めることにより、ある 1 つの LAN セグメントまたはスイッチがダウンした場合にも、引き続き LDAP クライアントから LDAP サーバーへトラフィックが流れることができるようにすることも推奨されます。HA 構成では、LDAP データを RAID アレイに保管して、物理的なディスクの故障ではサーバーが停止しないようにすることが賢明です。システム・モニター・ツールを使用してサーバーの可用性をポーリングし、いずれかのサーバーがダウンした場合にはリカバリー手順を開始できるようにすることもお勧めします。シナリオによっては、サイト全体が失われた場合に別のサイトが引き継ぐことができるように、複数の冗長サイトを組み込んだ HA サポートが使用されることもあります。

HA 構成のその他の重要な特性として、システムのダウン時間なしで保守を遂行できる機能があります。IBM Security Directory Server では、サーバー・トポロジーの増分アップグレードがサポートされているため、ディレクトリー・サービスのダウン時間を発生させずに、一度に 1 つのサーバーに対してサービスを適用できます。ダウンしているサーバーへの更新情報はキューに格納されるため、サーバーは再始動すると完全な同期状態に復帰します。Security Directory Server では、DB2 の機能または RAID 装置を使用することにより、既存のサーバーのオンライン・バックアップもサポートしています。これにより、トポロジー内で新しいサーバーを追加することや既存のサーバーを置き換えることが、ダウン時間なしで可能になります。

付録 P. 参照整合性プラグイン

ここに示す情報により、参照整合性プラグインおよび使用できるコマンドについての詳細を知ることができます。

Security Directory Server は、LDAP 削除操作の参照整合性制約を有効にする操作前プラグインである `libdelref` というプラグインを備えています。 `<TDS_HOME>/lib` または `lib64` にはライブラリーがあり、ライブラリー名は `libdelref.dll` (Windows)、`libdelref.a` (AIX)、`libdelref.so` (Solaris および Linux) のように、プラットフォームに応じて異なります。また、サンプル構成ファイル `tdsdelref.conf` が、Security Directory Server をインストールした場所の `/etc` ディレクトリーにあります。インスタンスを作成すると、`tdsdelref.conf` ファイルはインスタンスの場所の `etc` ディレクトリーで使用可能になります。

`libdelref` プラグインは、`ibmslapd.conf` ファイルに定義されている属性 `ibm-slapdReferentialIntegrityPlugin` を使用すれば使用可能にすることができます。デフォルトでは、この属性の値は `false` です。`libdelref` プラグインを使用可能にするには、属性値を `true` に変更して、サーバーを再始動する必要があります。

`libdelref` プラグインは、`ibmslapd.conf` ファイルの以下の行で定義します。

```
dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
ibm-slapdPlugin: preoperation libdelref.so DeleteReferenceInit
file=/home/nuser/idslapd-nuser/etc/tdsdelref.conf dn=o=sample
ibm-slapdReferentialIntegrityPlugin: FALSE
```

注: デフォルトでは、プラグイン入力関数は「DeleteReferenceInit」です。ただし、デバッグを目的とする場合は、`ibmslapd.conf` ファイルの `<init-function>` 指定で関数「DeleteReferenceInitDebug」に置き換えて、より詳細なログを `ibmslapd.log` に生成できます。

ここでは、プラグインは操作前プラグインで、そのライブラリーは `libdelref.so` であることが `ibm-slapdPlugin` 属性によって定義されています。`file` パラメーターでは、`etc` ディレクトリー内にある `tdsdelref.conf` というサンプル・ファイルの完全なパスをデフォルト値に設定しており、`dn` パラメーターでは、項目の検索対象にする `dn` のデフォルト値を `o=sample` に設定しています。

プラグインを使用可能にするには、以下のコマンドを使用します。

```
idsldapmodify -D <bindDN> -w <password>
```

```
dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
ibm-slapdReferentialIntegrityPlugin: True
```

プラグインは、ファイルおよび `dn` から参照整合性制約の情報を読み取ることで初期化されます。ファイルは `file` パラメーターで指定し、`dn` は `tdsdelref.conf` ファイル内の `dn` パラメーターで指定します。`tdsdelref.conf` ファイルを指定するのは参照のためです。ファイルが次のフォーマットに合致している限り、任意のファイルを使用できます。

```
file=<absolutePathToFile>
dn=<searchDN>
```

または

```
oc=<deleteObjectClass:referenceObjectClass:referenceAttribute>
```

dn=<searchDN>

説明:

absolutePathToFile は、oc パラメーターおよび dn パラメーターを格納しているファイルへの絶対パスです。

deleteObjectClass: is the objectclass name of the deleted object for which the referential integrity is to be maintained

referenceObjectClass: is the objectclass name of the reference object which might contain reference to the deleted object

referenceAttribute: is the attribute name in the referenceObjectClass whose value is the reference to the object being deleted

searchDN: is the base DN, where objects need to be searched (for references to the object being deleted)

ファイルには、複数の属性と検索ベース DN の指定項目が任意の順序で入っていることがあります。各指定項目は文字どおり処理されるため、指定項目の前後に空白文字を使用することはできません。使用すると、望ましくない結果を招くことになります。

注: 「oc」 および 「dn」 の複数の事例がスペースで区切られて存在することがあります。

削除操作に対して参照整合性がどのように機能するかの例について考えます。
tdsdelref.conf 内の項目が次のとおりである例を考えます。

```
oc=inetOrgPerson:inetOrgPerson:manager
```

DIT に cn=testmanager と cn=testuser という 2 人のユーザーがいるとします。また、cn=testuser の管理者が cn=testmanager であるとします。以下に例を示します。

```
dn: cn=testmanager,o=sample
objectclass: inetOrgPerson
sn: manager
```

```
dn: cn=testuser,o=sample
objectclass: inetOrgPerson
sn: testuser
manager: cn=testmanager,o=sample
```

ここで参照整合性プラグインを有効にして、cn=testmanager を削除すると、cn=testuser の manager 属性について cn=testmanager への参照もすべて削除されます。

付録 Q. IBM Security Directory Server と z/OS IBM Security Directory Server との間の相互運用性のガイドライン

ここに示す情報は、Linux、UNIX、または Windows プラットフォーム上の Security Directory Server と z/OS IBM Security Directory Server との間で LDAP ディレクトリーを複製する混合プラットフォーム環境をセットアップする場合の考慮事項として使用できます。

この説明内容は、これらの異種プラットフォーム間でのスキーマ項目およびディレクトリー項目の移行にも適用されます。

注: z/OS LDAP サーバーから分散プラットフォーム上の分散 LDAP サーバーへの複製は、以下の条件により異なります。

- z/OSサーバー上で保管または変更が行われるデータ、およびこれらのデータを更新するときに使用される操作は、両方のディレクトリー・サーバー上でサポートされているサブセットに制限されます。
- スキーマ定義は 2 つのサーバー間で同等です。

分散プラットフォームには、AIX、Windows、Solaris、Linux、および HP-UX が含まれます。最適なパフォーマンスを得るためには、分散プラットフォーム上の分散 LDAP サーバー間でのみ複製を使用する方が適切です。

スキーマに関する考慮事項

ここに示す、スキーマに関する考慮事項に注意してください。

1. 構文規則および突き合わせ規則:

Security Directory Server では、z/OS IBM Security Directory Server より多くの構文規則および突き合わせ規則がサポートされています。

Security Directory Server スキーマを z/OS IBM Security Directory Server で使用するには、その前に z/OS IBM Security Directory Server で対応していない構文規則および突き合わせ規則を、このスキーマから除去しておく必要があります。これらの構文規則または突き合わせ規則を使用する属性は、スキーマから削除するか、z/OS IBM Security Directory Server でサポートされる構文規則および突き合わせ規則を使用するよう変更する必要があります。ある項目内で該当の属性を使用中の場合は、その項目から属性値を除去する（属性をスキーマから削除する予定の場合）か、属性値をスキーマ内の変更済み属性定義に適合させるようにしてください。

2. スキーマの LDIF フォーマット:

(`ldapsearch -L` を使用し) スキーマを公開することによって Security Directory Server または z/OS IBM Security Directory Server から取得したスキーマ LDIF のフォーマットは、スキーマ変更コードの入力として受け入れられない場合があります。

- a. Security Directory Server スキーマを変更する場合は、スキーマ・ファイル内の **attributetypes** および **objectclasses** を別々のスキーマ変更コードに分割し、各コードに **attributetypes** 値または **objectclasses** 値が 1 つずつ含まれるようにします。また、関連する **attributetypes** 値の変更コードに **ibmattributetypes** 値 (ある場合) が含まれるようにします。スキーマ内に属性またはオブジェクト・クラスが既に存在する場合は、スキーマ変更コードを **modify-replace** にします。属性またはオブジェクト・クラスが存在しない場合は、スキーマ変更コードを **modify-add** にします。

z/OS IBM Security Directory Server スキーマを変更する場合は、スキーマ内に属性またはオブジェクト・クラスが既に存在するかどうかに関係なく、LDIF 全体を 1 回の **modify-replace** 操作で処理できます。

例えば、属性 **attr1** およびオブジェクト・クラス **objclass1** がスキーマ内に既に存在するとします。z/OS IBM Security Directory Server の場合は、以下に示すスキーマ変更コードによって該当のスキーマ・エレメントが置き換えられ、属性 **attr2** およびオブジェクト・クラス **objclass2** が新規に追加されます。

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: (
1.3.18.0.2.4.11111
NAME 'attr1'
DESC 'Description for attribute attr1'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE userApplications
)
IBMAttributetypes: (
1.3.18.0.2.4.11111
ACCESS-CLASS normal
)
attributetypes: (
1.3.18.0.2.4.22222
NAME 'attr2'
DESC 'Description for attribute attr2'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE userApplications
)
IBMAttributetypes: (
1.3.18.0.2.4.22222
ACCESS-CLASS normal
)
-
replace: objectclasses
objectclasses: (
1.3.18.0.2.6.33333
NAME 'objclass1'
DESC 'Description for object class objclass1'
SUP top
STRUCTURAL
MUST ( cn )
MAY ( attr1 )
)
objectclasses: (
1.3.18.0.2.6.44444
NAME 'objclass2'
DESC 'Description for object class objclass2'
SUP top
STRUCTURAL
MUST ( cn )
MAY ( attr1 $ attr2 )
)
```

Security Directory Server の場合は、以下に示すように、このスキーマ変更コードを別々のスキーマ変更コードに再フォーマットし、新規のスキーマ・エレメントの場合は **modify-replace** の代わりに **modify-add** を使用する必要があります。

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: (
1.3.18.0.2.4.11111
NAME 'attr1'
DESC 'Description for attribute attr1'
```

```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE userApplications
)
IBMAttributetypes: (
1.3.18.0.2.4.11111
ACCESS-CLASS normal
)

dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: (
1.3.18.0.2.4.22222
NAME 'attr2'
DESC 'Description for attribute attr2'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE userApplications
)
IBMAttributetypes: (
1.3.18.0.2.4.22222
ACCESS-CLASS normal
)

dn: cn=schema
changetype: modify
replace: objectclasses
objectclasses: (
1.3.18.0.2.6.33333
NAME 'objclass1'
DESC 'Description for object class objclass1'
SUP top
STRUCTURAL
MUST ( cn )
MAY ( attr1 )
)

dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: (
1.3.18.0.2.6.44444
NAME 'objclass2'
DESC 'Description for object class objclass2'
SUP top
STRUCTURAL
MUST ( cn )
MAY ( attr1 $ attr2 )
)

```

- b. オブジェクト・クラスは、その参照先属性より前に指定しないように注意してください。

ディレクトリー項目のインポートまたはエクスポート

ここに示す手順を使用して、ディレクトリー項目をインポートまたはエクスポートできます。

手順

1. Security Directory Server から z/OS IBM Security Directory Server へのデータのエクスポート:

Security Directory Server には、cn=configuration、cn=ibmPolicies、cn=localhost などの特定のサフィックスが含まれます。これらのサフィックスには、LDAP 構成、ポリシー、および複製を管理するために使用する特別な項目が含まれます。z/OS IBM Security Directory Server は、これらの特別な項目の一部のみをサポートします。

- a. ユーザーは、他の特別な項目を LDIF から削除するか、または **db2ldif-s <subtreeDN> -x** を使用して、これらのサフィックスがアンロードされないようにする必要があります。cn=configuration サフィックスには、拡張複製サポートを構成するために使用する項目が含まれます。サーバーを最初に始動すると、cn=configuration サフィックスの下に以下の拡張複製構成項目が自動的に作成されます。

- cn=configuration
- cn=Replication,cn=configuration

- cn=Log Management,cn=Configuration
- cn=Replication,cn=Log Management,cn=Configuration

z/OS IBM Security Directory Server の特殊な項目について詳しくは、IBM Security Directory Server の資料の『z/OS IBM Security Directory Server の管理および使用』セクションの『拡張複製』にある『拡張複製の使用可能化』を参照してください。

- ユーザー・パスワードは、平文、SHA、または CRYPT にする必要があります。これ以外の形式は、z/OS IBM Security Directory Server との互換性はありません。CRYPT を使用する場合は、z/OS IBM Security Directory Server の構成ファイルに **pwCryptCompat off** が指定されているようにしてください。
 - z/OS IBM Security Directory Server は、**aclEntry** 属性値 (**ibm-filterAclEntry** 属性) での、フィルター ACL の使用をサポートしていません。この ACL は、z/OS IBM Security Directory Server にインポートする前に削除する必要があります。
- z/OS IBM Security Directory Server から Security Directory Server へのデータのエクスポート:**
 - Security Directory Server では、**aclEntry** 属性値と **entryOwner** 属性値は "access-id:|group:|role:" という形式で始まる必要があります。これは z/OS IBM Security Directory Server では必須ではないため、Security Directory Server にインポートする前に、この形式をこれらの属性値に追加することが必要になる場合があります。この問題を回避するため、z/OS IBM Security Directory Server では、これらを必ず指定してください。
 - ユーザー・パスワードは、平文、SHA、または CRYPT にする必要があります。これ以外の形式は、Security Directory Server との互換性はありません。CRYPT を使用する場合は、z/OS IBM Security Directory Server の構成ファイルに **pwCryptCompat off** が指定されているようにしてください。Security Directory Server で使用されているタグ付き形式のパスワードをアンロードするには、**ds2ldif -t** を使用します。

機能に関する考慮事項

ここに示す、機能に関する考慮事項に注意してください。

- Security Directory Server では、ユーザー項目を削除すると、グループおよび ACL から項目の DN を削除する結果になります。これは、z/OS IBM Security Directory Server では行われません。代わりに、アプリケーション自体にこの動作を実行させる必要があります。
- 同様に、Security Directory Server ではサブツリー内のすべての項目について、削除を許可するコントロールがサポートされません。z/OS IBM Security Directory Server では、このコントロールはサポートされていません。したがって、アプリケーション自体でこの処理を行う必要があります。
- Security Directory Server のみ、または z/OS IBM Security Directory Server のみがサポートする機能がいくつかあります。操作の複製や項目の移行を円滑にするため、この 2 つのプラットフォームでサポートされている機能に使用を制限してください。

付録 R. LDAPSync

LDAPSync ソリューションは、Sun Directory Server や Active Directory などの 1 つ以上のソース・システムからターゲット LDAP ディレクトリー・サーバーへの、マイグレーション・サービスと同期サービスを提供します。このソリューションは、ターゲットとして IBM Security Directory Server を使用して作成されています。

LDAPSync ソリューションは、非推奨となった Active Directory との同期にとって代わるものです。

LDAPSync は、ユーザー項目およびグループ項目のマイグレーションと同期を行うために設計されています。また、organizationalUnit や dcObject などのコンテナークラスの処理も行います。ソース・ディレクトリー内のサブツリーはターゲット内にミラーリングされます。階層のミラーリングのためのプロパティ設定を指定する必要があります。

パスワードの処理を行うには、IBM Security Directory Server のパススルー認証機能を使用できます。この機能は、ユーザーが認証されたときにパスワードをマイグレーションするように構成することができます。この機能は、ソース・システムが存在し続ける限り使用できます (Active Directory のようなネットワーク・オペレーティング・システム (NOS) ディレクトリーなど)。LDAPSync ソリューションではパスワードは処理されません。詳しくは、『パススルー認証』を参照してください。

LDAPSync の概念

LDAPSync ソリューションの主要な概念とコンポーネントについて説明します。

ターゲット・ディレクトリー

IBM Security Directory Server は、LDAPSync の一元化されたターゲット・ディレクトリーです。

ソース・エンドポイント

フローの入力データを提供できる構成済みのソース・システム。

LDAPSync によってサポートされるソース・エンドポイントのタイプは、IBM Security Directory Server、Sun Directory Server、OpenLDAP など、変更ログをサポートする LDAP ディレクトリーです。

LDAPSync では Active Directory もサポートされます。Active Directory では変更履歴は提供されませんが、Active Directory 内の各項目は、オブジェクトがいつ作成または変更されたかを示す特殊な更新シーケンス番号 (USN) を保持しています。

フロー ソース・エンドポイントとターゲット IBM Security Directory Server との関係性を定義する構成。

属性マップ

ソース・スキーマの属性をターゲット・スキーマの対応する属性に変換するマップ。

LDAPSync のインストール

LDAPSync ソリューションを構成する前に、それを IBM Security Directory Integrator がアクセスできる場所にインストールする必要があります。

始める前に

LDAPSync ソリューションに必要な IBM Security Directory Integrator の最小サポート・バージョンは、バージョン 7.1.0.8 です。

手順

圧縮ファイル `sds_install_dir\midstools\LDAPSync.zip` の内容を `sdi_solution_dir` に解凍します。

注: `sdi_solution_dir` は、IBM Security Directory Integrator ソリューションのディレクトリーです。これは、IBM Security Directory Integrator のインストール時に指定します。ソリューション・ディレクトリーは、IBM Security Directory Integrator のインストール・ディレクトリーでも、任意のカスタム・ロケーションでもかまいません。これは IBM Security Directory Integrator 実行時のカレント・フォルダーです。ソリューションで使用するすべての相対パスは、このソリューション・ディレクトリーから展開されます。

LDAPSync.zip には、LDAPSync ソリューション用の以下のファイルが含まれています。

LDAPSync.xml

IBM Security Directory Integrator サーバーによってロードされ実行される構成ファイル。

LDAPSync.properties

ソース・システムおよびターゲット・システムへの接続と、ソリューションの動作を制御する各種設定が含まれるテキスト・ファイル。

person.map

ユーザー項目のマッピング・ファイル。

group.map

グループ項目のマッピング・ファイル。

organizationalunit.map

organizationalUnit コンテナ項目のマッピング・ファイル。

organization.map

organization コンテナ項目のマッピング・ファイル。

dcobject.map

dcObject コンテナ項目のマッピング・ファイル。

country.map

country コンテナ項目のマッピング・ファイル。

customScript.js

マッピング・ファイルのスクリプト関数と変数を保管するために使用する JavaScript ファイル。

LDAPSync の構成

LDAPSync ソリューションを構成するには、フローの動作を制御する接続の設定とプロパティを指定する必要があります。

このタスクについて

この手順の各例は、以下のサンプル・シナリオに基づいています。

現在 3 つのシステムに存在する認証データおよび許可データを、1 つの中央 ID ストアにマイグレーションすることが必要です。これら 3 つのソース・システムとは、1 つの Sun Directory Server と 2 つの Active Directory ドメイン・コントローラーです。データの初期マイグレーション後に、ソースで発生する変更に対してターゲット IBM Security Directory Server を同期させる必要があります。

さまざまなコンポーネントやフローを識別するために、例では以下の名前を使用します。

- SunFlow は、Sun Directory Server からターゲット IBM Security Directory Server へのフローです。
- AD1Flow は、1 番目の Active Directory ドメイン・コントローラーから IBM Security Directory Server へのフローです。
- AD2Flow は、2 番目の Active Directory ドメイン・コントローラーから IBM Security Directory Server へのフローです。
- SDS は、すべてのフローのターゲット IBM Security Directory Server です。
- SunDS は、SunFlow という名前のフローのソース・エンドポイントです。
- AD1 は、AD1Flow という名前のフローのソース・エンドポイントです。
- AD2 は、AD2Flow という名前のフローのソース・エンドポイントです。

手順

1. 接続および構成の設定を指定するには、LDAPSync.properties ファイルの LDAPSync ソリューション・プロパティを編集します。770 ページの『LDAPSync プロパティ』を参照してください。
2. 必要な各フローの名前を **global.flows** プロパティに指定します。各フローの名前はスペースなしの 1 語で指定してください。以下に例を示します。

```
global.flows=AD1Flow,AD2Flow,SunFlow
```

この例では、プロパティ設定によって 3 つのフローが定義されており、3 つのデータ転送が並行して行われます。

3. 各ソース・エンドポイントをフローに割り当てます。以下に例を示します。

```
AD1Flow.source.endpoint=AD1
AD2Flow.source.endpoint=AD2
SunFlow.source.endpoint=SunDS
```

4. フローのターゲット・ディレクトリーを指定します。

すべてのフローについてターゲットは同じなので、フローごとに個別に構成する代わりに、フローを指定せずに単一のプロパティを使用できます。

LDAPSync は最初にフロー固有のプロパティー設定を探します。フロー固有のプロパティーが見つからない場合は、フローが指定されていない基本のプロパティーをデフォルトで使用します。

以下に例を示します。

```
target.endpoint=SDS
```

5. ターゲット・ディレクトリー・サーバーの接続設定を LDAPSync.properties ファイルに指定します。以下に例を示します。

```
ep.SDS.ldap.url=ldap://ed.ewidgets.com:1389
ep.SDS.ldap.user=cn=Directory Manager
{protect}-ep.SDS.ldap.password=secret123a
ep.SDS.ldap.searchBase=dc=ewidgets,dc=com
```

パスワード・プロパティーの先頭に {protect}- トークンを使用して、プロパティー・ファイルを再書き込みし、このプロパティーを暗号化します。

エンドポイントのプロパティーを指定する場合、プロパティーの完全な名前の **source**。部分または **target**。部分を削除します。ソース・エンドポイントかターゲット・エンドポイントかは、エンドポイントをどのようにフローに割り当てるかによります。

6. ターゲット・ディレクトリー・サーバーの SSL 接続を構成するには、以下のアクションを実行します。

- a. ldaps プロトコルと SSL 接続のポート番号を、**target.ldap.url** パラメーター設定に指定します。以下に例を示します。

```
target.ldap.url=ldaps://ed.ewidgets.com:689
```

- b. **target.ldap.SSL** を true に設定します。以下に例を示します。

```
target.ldap.SSL=true
```

- c. IBM Security Directory Integrator の solution.properties ファイルで **javax.net.ssl.keyStore** プロパティーを使用して鍵ストアを指定します。以下に例を示します。

```
javax.net.ssl.keyStore=publicKeys.jks
```

ファイル・パスは publicKeys.jks に対する相対パスです。IBM Security Directory Integrator での相対パスのルートはソリューション・ディレクトリーです。したがって、鍵ストア・ファイルはソリューション・ディレクトリー内にあります。

- d. クライアント証明書を、IBM Security Directory Server から、コネクタによって使用される IBM Security Directory Integrator 鍵ストアにインポートします。証明書は、keytool.exe プログラムを使用してインポートできます。このプログラムは、IBM Security Directory Integrator のインストール・フォルダーの jvm/jre/bin ディレクトリーにあります。以下に例を示します。

```
keytool -import -file SDSclient_cert.der -keystore publicKeys.jks
-keypass ewldg3ts!
```

7. 3 つのソース・エンドポイントの接続パラメーターを指定します。以下に例を示します。

```
ep.AD1.ldap.url=ldap://dca1pha.acme.com:389
...
ep.AD2.ldap.url=ldap://9.122.14.33:689
...
ep.Sun.ldap.url=ldap://sunds.acme.com:1389
...
```

- Active Directory ソース・エンドポイントの変更検出のための検索ベースを構成します。以下に例を示します。

```
ep.AD1.ad.searchBase=dc=acme1.com
ep.AD2.ad.searchBase=dc=acme2.com
```

- 各ソース・エンドポイントの変更検出のタイプを指定します。

```
ep.AD1.changeDetectionType=AD
ep.AD2.changeDetectionType=AD
ep.Sun.changeDetectionType=Sun
```

- 各項目タイプのオブジェクト・クラスを指定します (該当する場合)。

LDAPSync ソリューションは、ソースから読みとった各項目のオブジェクト・クラス属性を比較します。属性を、**source.userObjectClass**、**source.groupObjectClass**、**source.container.objectClasses** の 3 つのプロパティの値と比較して、ユーザー項目か、グループ項目か、コンテナ項目かを判別します。Sun Directory Server はすべての項目タイプに対してデフォルトのオブジェクト・クラスを使用します。デフォルトは、ユーザーの場合は `inetOrgPerson`、グループの場合は `groupOfUniqueNames`、コンテナ・クラスの場合は `organization`、`organizationalUnit`、`dcObject`、`country` です。したがって、このエンドポイントまたはフローにはプロパティ設定は不要です。ただし、Active Directory の場合は、オブジェクト・クラスを指定する必要があります。以下に例を示します。

```
ep.AD1.UserObjectClass=User
ep.AD1.groupObjectClass=Group
ep.AD2.UserObjectClass=User
ep.AD2.groupObjectClass=Group
```

- 統合フローを指定し、各フローのソース・エンドポイントを割り当てます。以下に例を示します。

```
global.flows=SunFlow,AD1Flow,AD2Flow
SunFlow.source.endpoint=Sun
AD1Flow.source.endpoint=AD1
AD2Flow.source.endpoint=AD2
```

- すべてのフローのターゲット・ディレクトリーを指定します。ターゲットはすべてのフローについて同一であるため、フローを指定せずにプロパティ名を使用することで、すべてのフローに 1 つの項目のみを使用できます。以下に例を示します。

```
target.endpoint=SDS
```

- IBM Security Directory Server 項目の RDN として使用する **uid** 属性を定義します。また、IBM Security Directory Server ターゲットでユーザー項目およびグループ項目を作成するために使用するオブジェクト・クラスを定義します。以下に例を示します。

```
target.userRDN=uid
source.userRDN=cn
target.userObjectClass=inetOrgPerson,ewidgetsPerson
target.groupObjectClass=groupOfUniqueNames
```

この例では、補助クラス `ewidgetsPerson` があるために、ターゲットでユーザー項目を作成するには、複数のオブジェクト・クラスが必要です。したがって、値はオブジェクト・クラス名のコンマ区切りのリストとして指定されます。

14. フロー固有の以下の設定を指定します。
 - a. 項目がソース階層をミラーリングするかフラット化するか。
 - b. 各フローがその項目を書き込むサフィックス。
 - c. 各フローの各項目タイプ用のマッピング・ファイル。

この例では、各ソース・システムの項目をターゲット・ディレクトリー内の異なる複数のコンテナに書き込む必要があります。ソース階層をフラット化するために、**`global.preserveSourceContainers`** プロパティーが `false` に設定されます。一部のフローについてはソース階層をミラーリングし、それ以外のフローについてはフラット化する場合は、各フローの **`global.preserveSourceContainers`** プロパティーを個別に設定できます。

```
global.preserveSourceContainers=false
SunFlow.suffixForUsers=ou=employees,dc=ewidgets,dc=com
SunFlow.suffixForGroups=ou=groups,dc=ewidgets,dc=com
AD1Flow.suffixForUsers=ou=employeesAD1,dc=ewidgets,dc=com
AD1Flow.suffixForGroups=ou=groupsAD1,dc=ewidgets,dc=com
AD1Flow.person.mapFile=ad_person.map
AD2Flow.suffixForUsers=ou=employeesAD2,dc=ewidgets,dc=com
AD2Flow.suffixForGroups=ou=groupsAD2,dc=ewidgets,dc=com
AD2Flow.person.mapFile=ad_person.map
```

指定の `ad_person.map` ファイルが `LDAPSync` ディレクトリー内に存在することを確認します。見つからない場合は、エラーとなります。

`Sun Directory Server` フローには特定のユーザー・マップ・ファイルは構成されていないため、デフォルトのユーザー・マップ・ファイル `person.map` を使用します。このファイルは `inetOrgPerson` スキーマ間のマッピング用にセットアップされています。

いずれのフローにもグループ・マップが指定されていないため、すべてのフローでデフォルトのグループ・マップ・ファイル `group.map` を使用します。

15. 各フローの項目のマイグレーション元であるソース・コンテナを指定します。**`source.containersToMigrate`** プロパティーの値として、セミコロンで区切ったリストを指定します。以下に例を示します。

```
AD1Flow.source.containersToMigrate=cn=Users;cn=Groups;cn=Deleted Objects
AD2Flow.source.containersToMigrate=cn=Users;cn=Groups;cn=Deleted Objects
SunFlow.source.containersToMigrate=ou=people;ou=groups
```

この例では、`Active Directory` ソースに対して `CN=Deleted Objects` コンテナが指定されています。このシナリオでは同期中に削除操作を処理する必要があります。

不要なサブコンテナが存在する場合は、**`source.containersToSkip`** を指定することもできます。これら両方の値は、項目の `DN` を使用したサブストリングの比較で、ソリューションの範囲内にあるか境界の外にあるかを検査するために使用されます。

16. `Active Directory` に由来するユーザー項目には `uid` 属性がないため、この値を指定するために `cn` 属性を使用することを指定します。以下に例を示します。

```
AD1Flow.source.userRDN=cn
AD2Flow.source.userRDN=cn
```

- オプション: ユーザー、グループ、コンテナの各項目のマッピング・ルールを変更します。これらは拡張子が .map のファイルで定義されています。
- オプション: マッピング・ファイルでカスタム JavaScript 関数を使用する場合は、その関数を customScript.js ファイルに追加します。

LDAPSync の実行

ibmdisrv ユーティリティーを使用して LDAPSync コマンドを実行し、ソース・ディレクトリーとターゲット・ディレクトリーの間でデータのシミュレーション、マイグレーション、同期を行います。

手順

- LDAPSync ソリューション設定の構成後に、TestConnections AssemblyLine を実行して接続性をテストできます。コマンド行引数で LDAPSync 構成 XML ファイルのパスを指定して、IBM Security Directory Integrator サーバーを始動します。

```
ibmdisrv -c LDAPSync/LDAPSync.xml -r TestConnections
```

接続設定が正しくない場合、このコマンドはエラー・メッセージを返します。正常に接続されている場合は、以下の例のようなメッセージが表示されます。

```
> Checking for property (ep.Sun.ldap.url) = ldap://9.118.46.245:1389
> Checking for property (ep.Sun.ldap.user) = cn=Directory Manager
> Checking for property (ep.Sun.ldap.password) = chirag123lab#
> Checking for property (ep.Sun.ldap.searchBase) = o=americas,dc=acme.com
> Initializing SourceLDAP with searchbase: o=americas,dc=acme.com...
! success !
> Searching with SourceLDAP...
! success !
> Checking for property (ep.SDS.ldap.url) = ldap://9.118.46.242:1389
> Checking for property (ep.SDS.ldap.user) = cn=root
> Checking for property (ep.SDS.ldap.password) = *****
> Checking for property (SunFlow.target.ldap.searchBase) = ou=Source1,ou=0slo,
o=sample
> Initializing TargetLDAP with searchbase: ou=Source1,ou=0slo,o=sample...
! success !
> Searching with TargetLDAP...
! success !
> Initializing ChangeDetection_SUN with searchbase: cn=changelog...
! success !
> Searching with ChangeDetection_SUN...
! success !
> Reading a change entry with ChangeDetection_SUN ...
! success !
> Checking for property (ep.Sun.ldap.searchBase) = o=americas,dc=acme.com
> Confirming Source container exists (ep.Sun.ldap.searchBase) = o=americas,
dc=acme.com
> Checking for property (SunFlow.target.ldap.searchBase) = ou=Source1,
ou=0slo,o=sample
> Confirming Target container exists (SunFlow.target.ldap.searchBase) =
ou=Source1,ou=0slo,o=sample
> Checking for property (ep.Sun.container.objectClasses) =
ou=organizationalUnit, dc=dcObject, c=country, o=organization
> Checking for property (ep.Sun.containersToMigrate) = ou=Groups;ou=People
> Checking for property (ep.Sun.userObjectClass) = person
> Checking for property (ep.Sun.groupObjectClass) = groupofuniquenames
> Checking for map files
:
```

成功しました。すべての接続は正しく機能しました。

LDAPSync の構成で複数のフローが指定されている場合、このテストは各フローに対して実行されます。

2. マイグレーションのシミュレーションを実行して、LDAPSync ソリューションが必要な機能を果たすことと、ターゲット・ディレクトリーに項目が正しく書き込まれることを確認します。シミュレーションは以下のいずれかの方法で実行できます。

- LDAPSync.properties ファイルで **simulate** プロパティを input に設定してから **LDAPMigrate** を実行する。
- コマンド行から **LDAPMigrate** を実行するときに、引数 **-0** に simulate を指定する。

```
ibmdisrv -c LDAPSync/LDAPSync.xml -r LDAPMigrate -0 simulate
```

シミュレーションの実行結果は要約レポートに表示されますが、ターゲットにはデータは書き込まれません。以下の省略した出力例では、SunFlow とラベル付けされたフローの要約のみを示します。複数のフローが存在する場合、出力には各フローのレポートが含まれます。

```
: --> Starting migration for SunFlow - flattening container hierarchy
: --> containers to migrate: ou=Groups;ou=People
: *** SIMULATED RUN - NO DATA WILL BE MODIFIED ***
: * showing progress every 25 entries
: Processing #25 currently working on entry of type: person
: Processing #50 currently working on entry of type: person
: > migrating group entries using search filter: (objectClass=groupofuniqu
enames)
: **** Simulation Only - no data has been changed in the target ****
:
:
===== Summary for migration =====
- Persons Total: 51 Add: 51
- Groups Total: 3 Add: 3
- Containers Total: 2 Add: 2
-----
Errors: 0
Warnings: 0
=====
```

3. **LDAPMigrate** を再度実行して、データの実際のマイグレーションを行います。コマンド行から **LDAPMigrate** を実行するときに、引数 **-0** に actual を指定します。

```
ibmdisrv -c LDAPSync/LDAPSync.xml -r LDAPMigrate -0 actual
```

実際の実行では、通常、少なくとも初回はシミュレーションと同じ結果がレポートされます。その後マイグレーションを試行すると、IBM Security Directory Integrator はターゲットに項目が既に存在することを検出します。ソースから読み取られた値と属性が同じである場合は、不要な更新がスキップされます。要約には処理されるソース項目が引き続きリストされますが、追加または変更されるのは、新規項目またはターゲット・システムとは異なる項目のみです。

LDAPMigrate を actual モードで実行すると、**ResetChangeState** 操作も実行されます。

4. 2 つのシステムの同期を維持するように LDAPSync 同期操作のスケジュールを設定します。
 - a. ソースの変更ログのタイムアウト値を設定することで、同期を定期的に停止します。以下に例を示します。

```
source.ldap.changeLogTimeout=1800
```

このプロパティは、1800 秒 (30 分) 以内に変更が検出されない場合、同期は終了され、スケジューラーによって再始動できるようにしています。

- b. **ibmdisrv** ユーティリティを使用してサーバーの新規インスタンスを開始し、LDAPSync を実行します。ご使用のオペレーティング・システムに備わ

っている、Windows タスク スケジューラや Cron ジョブ (スケジュール済みタスク) などのスケジューリング・プログラムを使用して、同期のスケジュールを設定できます。

```
ibmdisrv -c LDAPSync/LDAPSync.xml -r LDAPSync -0 actual
```

LDAPSync では LDAPMigrate と同様の要約レポートは表示されませんが、変更を検出して処理するたびにその情報をログに記録します。

5. オプション: 新規変更のみをピックアップして転送するために、変更検出状態をリセットすることが必要な場合があります。

例えば、ソース・システムまたはターゲット・システムがバックアップからリストアされたり、データが再ロードされたりする場合があります。その場合は、フルマイグレーションを再実行することが必要になります。マイグレーション後、処理された最終の変更に関して LDAPSync が保管した情報は無効になるため、リセットする必要があります。現在の変更状態をリセットするには以下のコマンドを実行します。

```
ibmdisrv -c LDAPSync/LDAPSync.xml -r ResetChangeState -0 actual
```

LDAPSync 操作

LDAPSync 操作で **ibmdisrv** ユーティリティを使用して、接続のテスト、データのマイグレーション、マイグレーションしたデータの同期、変更状態情報のリセットを行うことができます。

構文

LDAPSync 操作で **ibmdisrv** ユーティリティを実行するには、以下の構文を使用します。

```
ibmdisrv -c LDAPSync/LDAPSync.xml -r LDAPSync operation [Arguments]
```

操作

TestConnections

ソース・ディレクトリーおよびターゲット・ディレクトリーに対する接続プロパティをテストします。

LDAPMigrate

ソースからターゲットにデータをマイグレーションします。

LDAPSync

同期サービスを開始します。

ResetChangeState

同期サービスのために保管されている状態情報をリセットして、これまでの変更を無視するようにします。このコマンドの実行後は、LDAPSync は新規変更のみをモニターするようになります。このサービスの開始後に発生した変更のみが同期されます。LDAPSync の開始前に行われた変更は無視されません。

引数

LDAPSync コマンドに以下のコマンド行引数を使用できます。

- 0 このパラメーターは、以下のいずれかの値に設定します。
 - -0 simulate: 同期のシミュレーションを実行する場合。
 - -0 actual: 実際の同期を実行する場合。

注: この引数は、**global.simulate** プロパティー設定をオーバーライドします。

- 1 このパラメーターに整数値 (*nnn*) を設定すると、処理した項目数が *nnn* に達するたびに、LDAPMigrate 操作で状況が表示されます。

このパラメーターを例えば -1 1000 と指定すると、状況メッセージが 1000 項目ごとにログに記録されます。

- 2 このパラメーターには、この同期に含めるフローのコンマ区切りのリストを設定します。

このパラメーターを例えば -2 AD1,AD2 と指定すると、AD1 および AD2 という名前のフローで同期操作が実行されます。

注: このパラメーターが有効なのは、**global.flows** プロパティーでフローが指定されている場合のみです。

例

LDAPSync の構成後に接続設定をテストするには、以下のコマンドを実行します。

```
ibmdisrv -c LDAPSync/LDAPSync.xml -r TestConnections
```

マイグレーションをシミュレートするには、以下のコマンドを実行します。

```
ibmdisrv -c LDAPSync/LDAPSync.xml -r LDAPMigrate -0 simulate
```

すべてのフローについてソース・エンドポイントからターゲットに項目をマイグレーションするには、以下のコマンドを実行します。

```
ibmdisrv -c LDAPSync/LDAPSync.xml -r LDAPMigrate -0 actual
```

特定のフローについてソース・エンドポイントからターゲットに項目をマイグレーションするには、以下のコマンドを実行します。

```
ibmdisrv -c LDAPSync/LDAPSync.xml -r LDAPMigrate -0 actual -2 flow_name
```

初期マイグレーションの後でソース・エンドポイントからターゲットに対して項目の同期を行うには、以下のコマンドを実行します。

```
ibmdisrv -c LDAPSync/LDAPSync.xml -r LDAPSync -0 actual
```

現在の変更状態をリセットするには、以下のコマンドを実行します。

LDAPSync プロパティー

ソース・システムおよびターゲット・システムでの LDAPSync ソリューションおよび接続のパラメーターの動作は、LDAPSync.properties ファイル内の設定で制御されます。

リストされているすべてのプロパティーをプロパティー・ファイルで設定する必要があります。そうしないと、ソリューションは機能しません。

プロパティの変更後に、IBM Security Directory Integrator サーバーを再始動して、変更を有効にする必要があります。

グローバル設定

以下のグローバル設定は、ソリューションで何を行うかと、ログ・ファイルをどのように生成するかを制御します。

global.simulate

マイグレーションのシミュレーションを実行するか、実際のマイグレーションを実行するかを示します。

マイグレーションのシミュレーションを行って、実際のマイグレーションで何が起きるかについてのレポートを取得するには、このプロパティを `true` に設定します。ターゲット・システムにはデータは書き込まれません。

実際のマイグレーションを実行する場合はこのプロパティを `false` に設定します。

デフォルト値は `false` です。

注: このプロパティは、値 `simulate` または `actual` を指定したコマンド行引数 `-0` でオーバーライドされます。

global.preserveSourceContainers

ソリューションの DN 変換の動作を制御します。

ソース・ディレクトリー内の指定の基本サフィックス下にあるコンテナ階層をミラーリングする場合は、このプロパティを `true` に設定します。

指定のターゲット・コンテナを使用する場合は、このプロパティを `false` に設定します。 **target.suffixForUsers** プロパティおよび

target.suffixForGroups プロパティに指定するコンテナが、ターゲットに書き込まれるユーザー項目およびグループ項目のコンテナとして使用されます。これらのパラメーターで指定されるサフィックス・ノードが、ターゲット・ディレクトリー内に存在することが必要です。

このプロパティは、必要に応じてフローごとまたはエンドポイントごとに指定できます。

デフォルト値は `false` です。

global.logDirectory

ソリューション・ログ・ファイルが作成されるディレクトリー・パスを指定します。

このパラメーターのデフォルト値は、相対パス `LDAPSync/logs/` です。

global.maxLogFiles

ログ・ファイルのロールオーバー履歴内に保持するファイルの数を指定します。

デフォルト値は `20` です。

global.showProgressCount

進行状況メッセージがログに記録される前に処理される項目の数を指定します。

例えば、このプロパティを `250` に設定すると、`250` 項目が処理されるたびに進行状況メッセージがログに記録されます。この値を `0` に設定するか、値を設定しないでおくと、進行状況メッセージはログに記録されません。

このプロパティは、必要に応じてフローごとまたはエンドポイントごとに指定できます。

デフォルトではこの値は空であるため、進行状況メッセージはログに記録されません。

global.flows

マイグレーションおよび同期の個々のフローが複数ある場合に ID を定義します。このプロパティはオプションです。

LDAPSync ソリューションは、複数のデータ・フローを処理するように構成できます。例えば、複数のソース・システムからのフローや、複数の LDAP サーバーをターゲットとするフローなどです。そのような複数のフローに名前を付けるためにこのプロパティを使用します。例えば、AD1,AD2,Sun のように 3 つの異なるフローを定義します。*FlowID* という接頭部が付いたその他のプロパティは、すべて指定のフローのみに適用されます。フロー修飾子が付けられていないプロパティは、独自のプロパティ設定を持たないすべてのフローに適用されます。

フロー ID では大/小文字の区別があります。この ID を他のプロパティの接頭部とする場合は、このプロパティに指定したのと同じスペルにしなければなりません。

ログ・ファイルには、フロー ID と下線文字 (_) で接頭部が付けられます。

ep という値は予約されているため、フロー ID には使用しないでください。

デフォルト値はブランクです。これは、ソース・システムからターゲットへの、名前がない単一のフローが存在することを意味します。

マイグレーション中に作成されたログには接頭部 M_ が付きます。同期中に作成されたログは S_ で始まります。

ソースの設定

ソース・プロパティは、ソース・ディレクトリーの接続と処理を制御します。

フローごとにすべてのソース・プロパティを指定できます。ただし、エンドポイントに対してプロパティを定義することもできます。その場合、そのプロパティがフローに割り当てられます。エンドポイントにプロパティを指定する場合は、プロパティ名から *source.* を削除して、代わりに *ep.flow.* をサフィックスとして使用する必要があります。例: AD1Flow.source.ldap.url=ldap://dcalpha.acme.com:389 または ep.AD1.ldap.url=ldap://dcalpha.acme.com:389。

source.ldap.url

ソース・システムの LDAP URL を指定します。SSL が必要な場合は、プロトコル指定子 *ldaps://* を *ldap://* の代わりに使用します。

source.ldap.user

ソース・システムに接続するためのユーザー名を指定します。

source.ldap.password

指定された LDAP ユーザー名のパスワードを指定します。

source.ldap.searchBase

マイグレーションおよび同期のために項目を読み取る、ソース・ディレクトリー内のノードの DN を指定します。

Active Directory の場合、この値は、Active Directory DIT のルート・サフィックスに設定する必要があります。そうしないと、変更の削除は検出されません。

source.container.objectClasses

マイグレーションするコンテナ・オブジェクト・クラスのコンマ区切りリストを指定します。

デフォルト値は `ou=organizationalUnit, dc=dcObject, c=country, o=organization` です。

このプロパティが有効になるのは、**global.preserveSourceContainers** プロパティが `true` に設定されている場合のみです。

source.containersToMigrate

項目をマイグレーションして同期を行うコンテナの、セミコロンで区切ったリストを指定します。

各コンテナの指定は、単にコンテナに対する RDN をリストしても、その項目の完全な DN 値の一部でもかまいません。

デフォルト値は `ou=Groups;ou=People` です。

source.containersToSkip

マイグレーションも同期も行わないコンテナの、セミコロンで区切ったリスト(ストリング)を指定します。

このリストは、項目 DN を最初に **source.containersToMigrate** プロパティ内のリストに照らして検査した後に適用されます。

各コンテナの指定は、単にコンテナに対する RDN をリストしても、その項目の完全な DN 値の一部でもかまいません。

デフォルト値は `ou=Groups;ou=People` です。

source.userObjectClass

ソース・ディレクトリー内のユーザー項目を識別する `objectClass` を指定します。

デフォルト値は `person` です。

source.groupObjectClass

ソース・ディレクトリー内のグループ項目を識別する `objectClass` を指定します。

デフォルト値は `groupOfUniqueNames` です。

source.ldap.pageSize

ページ検索結果のサイズを指定します。このプロパティは、ページ検索の戻りをサポートし、検索の戻りのサイズを制限する、Active Directory のようなシステムを対象とするオプションのプロパティです。ディレクトリー全体にわたって処理を繰り返すために、検索ページのサイズは、LDAP サーバーのサイズ制限または管理制限より小さい値に設定する必要があります。

デフォルトでは、このプロパティはブランクのままです。

source.ldap.binaryAttributes

ソリューションで処理するバイナリー属性を指定します。

これらのバイナリー属性は、標準の `inetOrgPerson` バイナリー属性以外のもので
す。ソースとして `Active Directory` を使用する場合は、このプロパティーに
`objectGUID` バイナリー属性を指定することも必要です。

デフォルトでは、このプロパティーはブランクのままです。

source.changeDetectionType

`LDAPSync` の変更検出のメカニズムを定義します。このプロパティーは必須で
す。

以下の設定が有効です。

- Sun
- SDS (IBM Security Directory Server の場合)
- AD
- デルタ

これら以外の値を指定すると、エラーが返されます。

デフォルトでは、このプロパティーはブランクのままです。

source.userRDN

ターゲット内のユーザー項目の `RDN` にマップされている属性を指定します。
値を指定しない場合は、`target.userRDN` プロパティー値と同じ値になります。

source.ad.searchBase

`Active Directory` の検索ベースを指定します。

このパラメーターは、`Active Directory` での変更検出を処理します。このパラメ
ーターを `Active Directory DIT` のルート・サフィックスに設定して、
`CN=Deleted` オブジェクト・コンテナーおよび削除変更が検出されるようにする
必要があります。

source.ldap.searchBase プロパティーは引き続き使用されており、項目がマイ
グレーションまたは同期されるコンテナーを参照していることが必要です。

注:

削除済み項目を処理するには、最初に `Active Directory` ドメイン・コントローラ
ーを構成する必要があります。詳しくは、Microsoft サポート Web サイトのト
ピック『*Viewing deleted objects in Active Directory*』を参照してください。

デフォルトでは、このプロパティーはブランクのままです。

source.ldap.useNotifications

ソース・ディレクトリー内の変更通知をサブスクライブするかどうかを指定しま
す。

このプロパティーを `true` に設定して変更通知をサブスクライブすると、
source.ldap.secondsForPolling および **source.ldap.changelogTimeout** は無視
されます。

デフォルト値は `true` です。

source.ldap.secondsForPolling

ソース・ディレクトリーでの変更をポーリングする間隔を秒数で指定します。

このプロパティーの値は **source.ldap.changelogTimeout** の設定より小さくする
ことが必要です。

source.ldap.useNotifications が true に設定されている場合、このプロパティは無効です。

デフォルト値は 10 です。

source.ldap.changelogTimeout

ソース・ディレクトリーでの新規変更の発生を待機する時間を秒数で指定します。

このプロパティの値は **source.ldap.secondsForPolling** の設定値より大きくする必要があります。

source.ldap.useNotifications が true に設定されている場合、このプロパティは無効です。

デフォルト値は 1800 です。

source.ldap.stateKey

このキー値を使用して変更検出の繰り返し状態を保管します。このプロパティの値は、固有性を確保するために自動的に計算されます。

supportPTA

ソース・エンドポイントで LDAP バインド操作がサポートされていることを示します。これは、IBM Security Directory Server からのパススルー認証に使用できます。

ターゲットの設定

ターゲット・プロパティは、ターゲット・ディレクトリーの接続設定と処理を指定します。すべてのターゲット・プロパティは、必要に応じてエンドポイントごとまたはフローごとに指定できます。エンドポイントに対して指定する場合は、プロパティ名から **target.** を削除します。

target.ldap.url

ターゲット・システムへの LDAP URL を指定します。SSL が必要な場合は、プロトコル指定子 **ldaps://** を **ldap://** の代わりに使用します。

target.ldap.user

ターゲット・システムに接続するためのユーザー名を指定します。

target.ldap.password

指定されたユーザー名のパスワードを指定します。

target.ldap.searchBase

ターゲット LDAP ディレクトリーのルート・サフィックスを指定します。

global.preserveSourceContainers が true に設定されている場合、**target.ldap.searchBase** プロパティは、ソースからコンテナ階層が書き込まれるターゲット・コンテナを指定します。

target.ldap.binaryAttributes

ソリューションで処理するバイナリ属性を指定します。

これらのバイナリ属性は、標準の **inetOrgPerson** バイナリ属性以外のものです。

デフォルトでは、このプロパティはブランクのままです。

target.userObjectClass

ターゲット・ディレクトリー内のユーザー項目を作成するためのオブジェクト・クラスを指定します。例えば `inetOrgPerson` です。

オブジェクト・クラス名のコンマ区切りリストを指定することもできます。

target.userRDN

ユーザー項目の RDN として使用する属性を指定します。

target.groupObjectClass

ターゲット・ディレクトリー内のグループ項目を作成するためのオブジェクト・クラスを指定します。例えば `groupOfUniqueNames` です。

オブジェクト・クラス名のコンマ区切りリストを指定することもできます。

target.groupMemberAttribute

メンバーの DN を保管するターゲット・ディレクトリー内のグループ項目の属性の名前を指定します。

例: `uniqueMember` または `member`。

デフォルト値は `uniqueMember` です。

target.suffixForUsers

ターゲット・システム内のユーザー項目の DN に追加するサフィックスを指定します。

global.preserveSourceContainers が `false` に設定されている場合、このプロパティーは必須です。

global.preserveSourceContainers が `true` に設定されている場合、**target.ldap.searchBase** プロパティーは、ソース内にあるコンテナ階層が書き込まれる、ターゲット・システム内のコンテナを指定します。

target.suffixForGroups

ターゲット・システム内のグループ項目の DN に追加するサフィックスを指定します。

global.preserveSourceContainers が `false` に設定されている場合、このプロパティーは必須です。

global.preserveSourceContainers が `true` に設定されている場合、**target.ldap.searchBase** プロパティーは、ソース内にあるコンテナ階層が書き込まれる、ターゲット・システム内のコンテナを指定します。

target.entry_type.mapFile

特定のタイプの項目のマップ・ファイルを指定します。ユーザー項目の場合は `person`、グループ項目の場合は `group` を指定できます。コンテナの場合、**entry_type** は小文字のオブジェクト・クラス名にする必要があります。例: `target.dcoobject.mapFile`。

パスを指定しないと、ファイルはデフォルトの `LDAPSync` ディレクトリー内にあると想定されます。

拡張カスタマイズ設定

以下のプロパティーは、カスタム `AssemblyLine`、リンケージ・クラス、および属性に対して追加のカスタマイズ・オプションを提供します。

source.entryTypes

マイグレーション対象の項目のタイプを指定します。値は、以下のキーワードのコンマ区切りのリストです。

- Person (または user)
- Group
- Container

デフォルト値は `person,group,container` です。

このプロパティはオプションです。

source.read.person.AL

ユーザー項目を読み取る `AssemblyLine` の名前を指定します。

デフォルト値は `MigrateUsers` です。

このプロパティはオプションです。

source.read.group.AL

グループ項目を読み取る `AssemblyLine` の名前を指定します。

デフォルト値は `MigrateGroups` です。

このプロパティはオプションです。

source.read.container.AL

コンテナ項目を読み取る `AssemblyLine` の名前を指定します。

デフォルト値は `MigrateContainers` です。

このプロパティはオプションです。

target.ldap.auxLinkedEntryClassName

ターゲット内に作成される項目の補助クラスの名前を指定します。このクラスは、ソース項目からのリンケージ情報を保管するための属性を提供します。

デフォルト値は `activeDirectoryLinkedEntry` です。

target.ldap.auxLinkedDNAttribute

ソース項目の元の DN を保管するための、ターゲット・リンケージ補助クラス内の属性を指定します。

デフォルト値は `adDn` です。

target.ldap.auxLinkedGUIDAttribute

ソース項目の固有 ID を保管するための、ターゲット・リンケージ補助クラス内の属性を指定します。例えば、Active Directory 項目の `objectGUID` など。

デフォルト値は `adObjectGUIDStr` です。

source.ldap.auxLinkedGUIDAttribute

上にリストしたリンケージ属性に保管する固有 ID を提供する、ソース項目内の属性を指定します。

target.ldap.enableForPTA

パススルー認証属性を各項目に書き込むかどうかを指定します。このオプションを有効にするには、値を `true` に設定します。

また、項目に補助オブジェクト・クラス `ibm-ptaReferral` があることも必要です。このプロパティが `true` の場合、この補助クラスは、LDAPSync ソリユ

ーションによって作成される項目に追加されます。**target.isSDS** プロパティを **false** に設定しないでください。設定すると、パススルー認証属性は書き込まれません。

デフォルト値は **true** です。

このプロパティはオプションです。

target.isSDS

target.isTDS

ターゲット・ディレクトリーが IBM Security Directory Server かどうかを示します。このプロパティの値を **true** に設定しない場合は、リンクされている属性もパススルー認証属性も書き込まれません。

デフォルト値は **true** です。

このプロパティはオプションです。

LDAPSync ログ・ファイル

LDAPSync ログ・ファイルを使用して同期操作のトラブルシューティングを行います。

LDAPSync ソリューションでは LDAPSync/logs フォルダー内に一連のログ・ファイルが作成され、操作中にコンソール・メッセージが表示されます。その他のログ・ファイルが例外発生時に作成されます。例えば、グループのメンバーがターゲット内に見つからない場合や、グループ・メンバーへの参照が切れている場合、メッセージは GroupMembersMissing.log ファイルに書き込まれます。

システム・ログ・ファイル

システム・ログ・ファイルは IBM Security Directory Integrator によって書き込まれます。それらのファイルは、*sdi_solution_dir*logs フォルダー内にあります。

ibmdi.log

各 IBM Security Directory Integrator AssemblyLine がそれぞれのソリューション・ログに書き込むすべてのメッセージと、サーバー・レベルのメッセージが含まれます。

ibmditk.log

IBM Security Directory Integrator の開発環境である構成エディターによって生成されるログ項目が含まれます。

ソリューション・ログ・ファイル

ソリューションのログは、ソリューション設計の一環として AssemblyLine によって書き込まれます。

LDAPSync ソリューションは、ログ・ファイルを *sdi_solution_dir*/LDAPSync/logs フォルダー内に書き込みます。LDAPMigrate や LDAPSync などの AssemblyLine を実行すると、その AssemblyLine と同じ名前のログ・ファイルが作成されます。

LDAPSync ソリューションは以下のログ・ファイルを作成します。

EntriesNotMigrated.ldif

マイグレーション中にターゲットに正常に書き込まれなかった項目が含まれます。

このファイルの以前のバージョンの名前は `EntriesNotMigrated.old.timestamp.ldif` に変更されます。ここで *timestamp* は、そのファイルが変更された日時です。

このログの名前の先頭はフロー ID と下線文字になります。定義済みのフローが存在しない場合は、ファイル名の前に `M_` が付きます。

EntriesNotSynchronized.ldif

同期中にターゲットに正常に書き込まれなかった項目が含まれます。

このファイルの以前のバージョンの名前は `EntriesNotSynchronized.old.timestamp.ldif` に変更されます。ここで *timestamp* は、そのファイルが変更された日時です。

このログの名前の先頭はフロー ID と下線文字になります。定義済みのフローが存在しない場合は、ファイル名の前に `S_` が付きます。

GroupMembersMissing.log

マイグレーション中または同期中にスキップされなかったグループ・メンバーのリストが含まれます。グループ項目の `member` 属性には DN のリストが含まれます。各属性は、そのメンバーのユーザー項目またはグループ項目を参照します。参照先の項目がターゲット・ディレクトリー内にはない場合は、スキップされて、このファイルに DN が記録されます。

このログの以前のバージョンの名前は `GroupMembersMissing.old.timestamp.log` に変更されます。ここで *timestamp* は、そのファイルが変更された日時です。

このログの名前の先頭はフロー ID と下線文字になります。定義済みのフローが存在しない場合、マイグレーション中に作成されたログの場合はファイル名の前に `M_` が付き、同期中に作成されたログの場合はファイル名の前に `S_` が付きます。

LDAPMigrate

LDAPMigrate が実行されるたびにフローから生成されるメッセージが含まれます。フローが実行されるたびに書き込まれるログ・ファイルはもう 1 つあります。このファイルの名前には接頭部としてフロー ID が付きます。例：`SunFlow_LDAPMigrate`。

このログに含まれるのは特定のフローからのメッセージのみですが、`LDAPMigrate.log` にはすべてのフローからのメッセージが含まれます。コンテナがマイグレーションされると、`MigrateContainers.log` も作成されます。ユーザー項目またはグループ項目が処理される場合は、`MigrateUsers.log` および `MigrateGroups.log` も書き込まれます。

このログの以前のバージョンの名前はカウンターを使用して変更されます。カウンターの最大値は `global.maxLogFiles` プロパティで指定します。

LDAPSync

LDAPSync が実行されるたびにフローから生成されるメッセージが含まれま

す。フローが実行されるたびに書き込まれるログ・ファイルはもう 1 つあります。このファイルの名前には接頭部としてフロー ID が付きます。例: SunFlow_LDAPSync。

このログに含まれるのは特定のフローからのメッセージのみですが、LDAPSync.log にはすべてのフローからのメッセージが含まれます。それに加えて、WriteToLDAP.log ファイルも作成されます。

このログの以前のバージョンの名前はカウンターを使用して変更されます。カウンターの最大値は global.maxLogFiles プロパティーで指定します。

MigrateContainers.log

コンテナのマイグレーション時にログに記録されるメッセージが含まれます。**LDAPMigrate** を実行してコンテナ項目が処理されると、このログ・ファイルが作成されます。WriteToLDAP.log ファイルも作成されます。

このログの名前の先頭はフロー ID と下線文字になります。定義済みのフローが存在しない場合は、ファイル名の前に M_ が付きます。

このログの以前のバージョンの名前はカウンターを使用して変更されます。カウンターの最大値は global.maxLogFiles プロパティーで指定します。

MigrateUsers.log

ユーザー項目のマイグレーション時にログに記録されるメッセージが含まれます。**LDAPMigrate** を実行してユーザー項目が処理されると、このログ・ファイルが作成されます。WriteToLDAP.log ファイルも作成されます。

このログの名前の先頭はフロー ID と下線文字になります。定義済みのフローが存在しない場合は、ファイル名の前に M_ が付きます。

このログの以前のバージョンの名前はカウンターを使用して変更されます。カウンターの最大値は global.maxLogFiles プロパティーで指定します。

MigrateGroups.log

グループ項目のマイグレーション時にログに記録されるメッセージが含まれます。**LDAPMigrate** を実行してグループ項目が処理されると、このログ・ファイルが作成されます。WriteToLDAP.log ファイルも作成されます。

このログの名前の先頭はフロー ID と下線文字になります。定義済みのフローが存在しない場合は、ファイル名の前に M_ が付きます。

このログの以前のバージョンの名前はカウンターを使用して変更されます。カウンターの最大値は global.maxLogFiles プロパティーで指定します。

ResetChangeState

変更状態情報がいつリセットされたかに関するログが含まれます。このログ・ファイルは、**ResetChangeState** が実行されたときに作成されます。

このログの名前の先頭はフロー ID と下線文字になります。定義済みのフローが存在しない場合は、ファイル名の前に M_ が付きます。

TestConnections.log

接続設定の検証結果が含まれます。このログ・ファイルは、**TestConnections** が実行されるたびに書き込まれます。

このログの以前のバージョンの名前はカウンターを使用して変更されます。カウンターの最大値は global.maxLogFiles プロパティーで指定します。

WriteToLDAP.log

ターゲット・ディレクトリーを更新するすべての操作をログに記録します。**LDAPMigrate** や **LDAPSync** などの **AssemblyLine** が実行されたときに書き込まれます。

このログの以前のバージョンの名前はカウンターを使用して変更されます。カウンターの最大値は `global.maxLogFiles` プロパティーで指定します。

このログの名前の先頭はフロー ID と下線文字になります。定義済みのフローが存在しない場合、マイグレーション中に作成されたログの場合はファイル名の前に `M_` が付き、同期中に作成されたログの場合はファイル名の前に `S_` が付きます。

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]

アカウントのアンロック
パスワード・ポリシー 671
アクセシビリティ ix
アクセス権 559
LDAP 操作 552
アクセス制御リスト (ACL) 546
アクセスの設定 160
アクセス評価
特定規則 556
アクセス・コントロール 525
動的スキーマ 68
アクセス・コントロール情報 547
アクセス・コントロール・リスト 397
アプリケーション・サーバー
組み込みバージョンの IBM
WebSphere Application Server -
Express 19
Apache Tomcat 19
アプリケーション・サーバー、構成
セキュリティ・レベル 225
FIPS モード 225
暗号、セキュア・プロトコル
SSLv3/TLS 1.0 198
暗号、セキュリティ・プロトコル
SSLv3 197
TLS 1.0 197
TLS 1.1 197
TLS 1.2 197
暗号化
片方向暗号化
crypt 232
SHA-1 232
SHA-2 232
スキーマ管理 60
属性 60
両方向暗号化
AES128 232
AES192 232
AES256 232
レベル 182
SSL 182
暗号化設定 61

暗号化属性
コマンド行 62
アンロック 248
移行
鍵リング・ファイル 179
逸失および検出
エラー・ログ 504
逸失および検出エラー・ログ 514
逸失および検出の設定
変更 504
逸失および検出ログ 504
変更 506
一般化時刻 83
イベント通知 133, 134
コマンド行 134
使用可能化 132
使用不可化 132
インターフェース
PKCS#11 180
インポート
鍵 175
運用属性
サーバー 70
パスワード・ポリシー 669
永続検索 94
検索 131
エクスポート
鍵 174
エスケープ規則 12
エラー
ldap 617
エラー処理
複製 324
エラー番号 617
エラー・コード 617
エラー・ログ
コマンド行 510
エンドポイント 761
オブジェクト ID
OID 35
オブジェクトの削除
コマンド行 46
オブジェクト・クラス 35, 37, 38
グループ 577
コピー 43
削除 46
追加 38
表示 37
変更 40
補助 539
IBMAttributeTypes 47

オブジェクト・クラス (続き)
IBMsubschema 67
オブジェクト・クラスのコピー
コマンド行 45
Web 管理ツール 43
オブジェクト・クラスの削除
Web 管理ツール 46
オブジェクト・クラスの追加
コマンド行 40
Web 管理ツール 38
オブジェクト・クラス・タイプ
構造化 36
抽象 36
補助 36
オブジェクト・フィルター 552
オブジェクト・フィルター形式 552
オプション
directory 545
オフライン復元 728, 729
オフライン・バックアップ 728
オフライン・バックアップおよび復元の手
順
ディレクトリー・データベース 723
オンライン
資料 vii
用語 vii
オンライン・バックアップ 729
オンライン・バックアップおよび復元
概要 724

[カ行]

階層の例 574
外部認証局 157
鍵
インポート 175
エクスポート 174
既存の鍵の認証要求 178
公開 167
削除 172
自己署名 173
情報の表示 171
データベース・パスワードの変更 171
デフォルト 172
トラステッド・ルート 176
トラステッド・ルートの除去 177
秘密 167
鍵データベース 170
インポート、証明書 227
設定 179

- 鍵データベース、jks
 - エクスポート、証明書 229
- 鍵データベース・ファイル 161
- 鍵ペア 167, 168
- 鍵リング・ファイル
 - 移行 161, 179
- 拡張
 - 検索 542
- 拡張された DN の処理 12
- 拡張操作
 - OID 636
- 拡張バックアップ 468
 - インスタンス、ディレクトリー・サーバー 468
- カスタマイズされたプラグイン 432
- カスタム・ロケーション 478
- 仮想リスト・ビュー 130
 - 項目 130
- 簡易検索と拡張検索
 - idsldapsearch 544
- 監査
 - エラー・ログ 488, 493, 495
 - 使用不可化 496
 - 監査エラー・ログ 488, 493, 495
 - 使用不可化 496
 - 監査ログ
 - コマンド行 511
 - 監査ログの設定 511
 - 監査ログを使用不可にする
 - コマンド行 496
- 管理 13, 381, 382
 - アーカイブ・ログ
 - 例 735
 - サーバー・パフォーマンス 119, 120
 - 名前 85
 - パスワード 85
 - 複製 421
- 管理、レルム 606
- 管理、ログ
 - ibm-slapdLog 479
- 管理アカウント 248
- 管理グループ 436, 601
 - コマンド行 297
 - 使用可能化 297
 - 使用不可化 297
 - メンバーの除去 301
 - メンバーの追加 298
 - メンバーの変更 299
 - Web 管理ツール 297
- 管理グループ・メンバー 441
 - コマンド行 300
 - 変更 300
- 管理グループ・メンバーの情報
 - Web 管理ツール 300
- 管理サーバー 19, 510, 511
 - エラー・ログ 481
- 管理サーバー (続き)
 - 監査ログ 484
 - 使用不可化 487
 - ディレクトリー管理サーバーのインスタンスの始動 14
 - ディレクトリー管理サーバーのインスタンスの停止 14
 - ログ設定 483
 - idsdiradm 13
 - SSL セキュリティー 740
- 管理サーバー監査ログ 484
 - コマンド行 486, 487
 - 使用可能 484
 - 使用不可化 487
 - Web 管理ツール 484, 487
- 管理サーバー・エラー・ログ 481
- 管理サーバー・ログ
 - 変更 481
- 管理者
 - 管理者グループ 291
 - レルム 600
- 管理者項目 600
- 管理者の識別名およびパスワード
 - コマンド行 86
- 管理者の追加
 - Web 管理者グループ 601
- 管理者パスワード
 - 文字、サポート対象 246
- 管理パスワード・ポリシー 247
- 管理ロックアウト・ポリシー 247
- 関連付け
 - サーバーと参照との 303
- 疑似 DN 551
- 疑似 DN の例 551
- 規則
 - 索引付け 50
 - 属性 50
- 既存の属性の変更
 - 手作業手順 57
- 既存のパスワード・ポリシー 252
- 既存のピア・サーバー
 - 変換 425
- キャッシュ
 - グループ・メンバーのキャッシュ 106
 - 項目 104
 - フィルター 105
 - ACL 105
- キャッシュ・ステータス 104
- キャッシュ・プロパティー、管理
 - Web 管理ツール 142
- キュー
 - 複製 419
- キューの詳細 420
- 共通のスキーマ 34
- 許可されない変更
 - スキーマ 69
- 許可されない変更 (続き)
 - オブジェクト・クラス 69
 - 構文 80
 - 属性 70
 - 突き合わせ規則 80
- 区画項目 445
- 区画索引値の割り当て
 - サーバー 447
- 区画ベース 445
- クライアント
 - SSL セキュリティー 748
- クライアント認証 161, 163
- クライアント・ユーティリティー
 - Suite B モード 218
 - TLS 1.2 署名およびハッシュ・アルゴリズム 217
- クライアント・ユーティリティー、暗号構成
 - SSLv3 216
 - TLS 1.0 216
 - TLS 1.1 216
 - TLS 1.2 216
- クライアント・ユーティリティー、構成
 - Suite B モード 219
 - TLS 1.2 署名およびハッシュ・アルゴリズム 218
- クライアント・ユーティリティー、セキュア・プロトコル
 - SSLv3 213
 - TLS 1.0 213
 - TLS 1.1 213
 - TLS 1.2 213
- クライアント・ユーティリティー、プロトコル構成
 - SSLv3 215
 - TLS 1.0 215
 - TLS 1.1 215
 - TLS 1.2 215
- グループ 569, 570, 588, 593, 599, 613, 615
 - オブジェクト・クラス 577
 - 検索制限 588
 - 混成 573
 - 作成 605
 - 静的 570
 - 属性タイプ 578
 - 動的 571
 - ネストされた 572
 - パスワード・ポリシー 237
 - プロキシ許可
 - コピー 597
 - 作成 594
 - 除去 598
 - 変更 596
 - メンバー項目の編集 584
 - メンバーシップ 573, 585

- グループ、管理 613
- グループ項目 583
 - メンバー、追加 583
 - メンバーの除去 585
- グループのコピー
 - Web 管理ツール 614
- グループの情報 614
- グループの追加
 - Web 管理ツール 613
- グループ・タスク
 - 検査 582
- グループ・パスワード・ポリシー 238
- グループ・メンバーシップ、追加 585
- グループ・メンバー・キャッシュ
 - 項目キャッシュ 144
 - 固有メンバー属性 144
- グローバル
 - パスワード・ポリシー 236
- グローバル管理グループ 5, 436, 437
- グローバル管理者グループ 437
 - 作成 438
 - 追加 438
- グローバル・セキュリティー
 - gskcapiamd 163
 - iKeyman 167
- グローバル・ポリシー 441
- グローバル・ログ設定
 - コマンド行 481
 - 編集 480, 481
- ゲートウェイ 372
- ゲートウェイ・サーバー 425
- ゲートウェイ・トポロジー
 - コマンド行 375
 - 作成 370
- 継承
 - オブジェクト・クラス 36
- 結合
 - LDAPSync 770
- 決定 574
- 言語タグ 530
 - 言語タグ記述子
 - 除去 533
 - 言語タグを関連付けられない属性 531
 - 言語タグを含む属性
 - 検索 532
 - 使用可能化 117
 - 使用不可化 117
 - タグの除去
 - 言語タグ 533
- 言語タグ、追加
 - 属性 532
- 検査
 - 項目 81
- 検索 542, 611, 613
 - 永続検索 131
 - 拡張 542

- 検索 (続き)
 - 拡張された制御 126
 - 簡易 542
 - サイズ制限 123, 125, 588
 - 時間制限 123, 125, 588
 - 手動 544
 - 設定 123, 125
 - ソート 123, 125
 - ディレクトリー項目 541
 - ページ付け結果 128
 - ページング 123, 125
 - ページングおよびソート 126
- 検索制限グループ 588, 591, 592, 596
 - 構造化オブジェクト・クラス 589
 - コピー 592
 - 除去 592
 - Web 管理ツール 589
- 検索制限グループ、コピー
 - コマンド行 592, 596
- 検索制限グループの除去
 - idsldapdelete 593
 - Web 管理 593
- 検索制限グループの変更
 - Web 管理 591
- 検索制限の管理 525
- 検索の設定 122
- 検索フィルター・エレメント
 - 数 119
- 研修 ix
- 検証 19
 - Web 管理ツール 19
- 合意
 - 複製 325
- 高可用性
 - シナリオ 753
- 構成 141, 439, 446, 665
 - DIGEST-MD5 259
- 構成専用モード 17
 - コマンド行 19
 - 始動する方法 18
 - 要件 18
 - Web 管理 19
 - Web 管理を使用して始動 18
- 構成ツール
 - エラー・ログ 501
 - バックアップ 389
- 構成ツールのログ 501
 - コマンド行 513
- 構成ツール・ログ設定
 - 変更 501, 502
 - Web 管理ツール 501
- 構成ファイル 141
- 構文 54
 - 識別名 11
 - 属性 62
 - バックス正規形式 (BNF) 11

- 構文 (続き)
 - ACL 549
- 項目 572, 578, 585
 - 追加 526
 - 補助オブジェクト・クラスの削除 540
 - 補助オブジェクト・クラスの追加 539
 - ログの管理 517
- 項目、コピー
 - コマンド行 538
 - Web 管理ツール 537
- 項目、作成
 - 参照 303
- 項目、追加
 - コマンド行 527
 - Web 管理 526
- 項目キャッシュ
 - コマンド行 142
 - Web 管理ツール 142
- 項目の ACL の編集 538
- 項目の検査
 - スキーマを照合する 81
- 項目のコピー 537
- 項目の削除 534
 - Web 管理 534
- 項目の追加 433
- 項目の所有者 565, 566
- 項目の場所
 - Web 管理ツール 445
- 項目の変更
 - コマンド行 535
 - サーバー管理 596
 - Web 管理 535
- 考慮事項
 - 機能 760
- 互換性
 - iPlanet 82
- コピー 385
 - 複製フィルター - 一般 384
- コピーの作成 252
- 個別
 - パスワード・ポリシー 237
- コマンド
 - idsldapdelete 535
 - idsldapmodify 534, 541, 597
 - idsldapmodrdn 536
- コマンド行
 - イベント通知 133, 134
 - オブジェクト・クラス 38, 42
 - 管理
 - サーバー・パフォーマンス 120
 - 管理グループ
 - メンバーの除去 301
 - サフィックスの追加 438
 - サブツリーの作成 352
 - 使用可能化 133, 136
 - 使用不可化 137

- コマンド行 (続き)
 - 除去 148
 - サブフィックス 139
 - 属性 67
 - スキーマ 38
 - 属性 148
 - 属性キャッシュ 148
 - 適用
 - 最小 ulimit 122
 - トランザクション・サポート 136, 137
 - 表示 38, 42
 - ユーザー項目の作成および追加 438
 - logs 495
- コマンド行ユーティリティ 566
- 固有属性 64, 66
 - 作成 64
- 固有属性、除去 66
- 固有属性の作成
 - コマンド行 65
- 混成グループ 573
- コンソール 23
 - 管理 29
 - サーバーの除去 31
 - サーバーの追加 30
 - サーバーの変更 30
 - パスワードの変更 29
 - プロパティの変更 31
 - ログインの変更 29
 - ログオフ 24
- コンソールへのログイン 21

[サ行]

- サーバー
 - 運用属性 70
 - 参照 301
 - 始動 86
 - 停止 86
 - SSL セキュリティ 748
- サーバーおよびクライアントの認証 153
- サーバー管理 13
 - 項目の変更 596
 - バックアップ 469
 - リストア 469
- サーバー管理の使用 592
- サーバー機能の表示
 - ルート DSE 108
- サーバー状況 88
 - 決定 88, 95
 - 作業キュー 92
 - システム情報 90
 - 操作カウント 90
 - ディレクトリー・キャッシュ候補 107
 - ディレクトリー・キャッシュ属性 106
 - トランザクション・カウント 92
- サーバー状況 (続き)
 - トレースおよびログ 94
 - 汎用サーバー・ステータス 89
 - ワーカー・ステータス 93
- サーバー証明書 157
- サーバー接続
 - 管理 112, 113
- サーバー認証 153
 - SDS 155
- サーバーの始動 86
 - 構成専用モード 17
- サーバーの自動始動 15
- サーバーの始動/停止 86, 509
- サーバーの追加 349, 402
- サーバーの停止 86
- サーバーの複製 349, 402
 - ゲートウェイ 349, 402
 - ピア 349, 402
 - マスター 349, 402
- サーバー・インスタンス 108, 111
- サーバー・エラー・ログ
 - コマンド行 514
- サーバー・トレース
 - 開始 508
 - 停止 508
- サーバー・トレースの開始 508
- サーバー・トレースの停止 508
- サーバー・パフォーマンス
 - 設定 119
- サーバー・プロパティ
 - 設定 116
- サーバー・ポートの変更
 - コマンド行 118
 - Web 管理ツール 117
- サーバー・ログ
 - コマンド行 508
 - 変更 508
- サーバー・ログ設定
 - 変更 501
- 最小 ulimit
 - 適用 120, 122
- 索引付け
 - 規則 50
- 削除
 - 鍵 172
 - パスワード・ポリシー 253
- 作成 591, 594, 600
 - サブツリー (subtree)
 - コマンド行 359
 - 新規の複製されたサブツリー 363
 - デフォルト参照 307
- サブフィックス 137
 - 除去 139
 - 追加 138
- サブフィックスの追加 435
 - コマンド行 138, 438

- サブフィックスの追加 (続き)
 - Web 管理ツール 138
- サブクラス化 36
- サブジェクト 550
- サブスキーマ項目 67
- サブツリー
 - 複製 394
- サブツリー (subtree)
 - 編集 397
- サブツリー複製の考慮 569
- サブライヤー情報 335, 414
 - 追加 415
 - 編集 416
- サポートされ、使用可能になっている機能
 - OID 625
- 参照
 - 項目、作成 303
 - サーバー 301
 - サーバーの関連付け 303
 - 除去 309
 - 他のサーバー 303
 - デフォルト
 - 作成 306
 - 分散、ネーム・スペース 304
 - 変更 308
 - LDAP ディレクトリー 302
 - Web 管理ツール 308
- 参照オブジェクト 304
- 参照整合性プラグイン
 - コマンド 755
- サンプル LDIF ファイル
 - フィルターに掛けられていない
 - ACL 705
 - ACL のフィルター操作 705
- 資格情報
 - 作成 331
 - 複製 397
- 識別 440, 447
- 識別名 1, 10
 - 疑似 551
- 時刻
 - 標準 83
 - UTC 83
- 自己署名鍵 173
- 自己署名証明書、作成
 - cms 鍵データベース 223
 - jks 鍵データベース 223
- システム情報 103
- 事前監査レコード
 - 構成 488
- 実行
 - ディレクトリー・サーバー 472, 474
 - バックアップ 472, 474
- 始動
 - 複製 336
 - モード 19

- 自動フェイルバック 451
- 始動または停止 521
- シナリオ
 - パススルー認証 277, 279, 280, 285, 286
- シナリオ・ベースのヘルプ・ファイル
 - Web 管理ツール 32
- 使用可能化 133, 135, 136
- 状況
 - サーバー 88
 - 接続 111
- 使用不可化 134, 136
- 証明書 167, 170
- 証明書要求 168, 173
- 除外
 - 複製トポロジー情報 387
- 除去 148, 607, 610, 613, 615
 - サフィックス 139
 - サプライヤー情報 416
 - 属性 66, 67
 - デフォルト参照 307
- 所有者 565
 - 所有者の除去 566
 - 所有者の追加 565
- 所有者の除去
 - 所有者 566
- 所有者の追加
 - 所有者 565
- 資料
 - アクセス、オンライン vii
 - 本製品用のリスト vii
- 新規のゲートウェイ・サーバー
 - 作成 424
- 新規の複製されたサブツリー
 - 構成済みデータベース 337
 - コマンド行 363
 - 作成 337
- スキーマ
 - オブジェクト・クラス 35
 - コピー 43
 - 削除 46
 - 属性 37
 - 追加 38
 - 定義 35
 - 表示 37
 - 変更 40
- 共通 34
 - サポート 34
- コマンド行 38, 52
- サブスキーマ項目 67
- 属性 46
 - 暗号化属性 60
 - コピー 57
 - 削除 59
 - 追加 52
 - 表示 51
- スキーマ (続き)
 - 属性 (続き)
 - 変更 54, 55, 56
 - 属性タイプ 33
 - 動的
 - changes 68
 - ファイル
 - 属性タイプ 33
 - changes
 - 許可されない 69
 - IBM Security Directory Server 713
 - Web 管理ツール 37, 51
- スキーマに関する考慮事項 757
- スキーマの更新 441
- スケジューリング
 - directory server のバックアップ 474
- スケジュール
 - 週次 417
 - 日次 418
- 制御
 - OID 638
- 静的グループ 570
- 静的グループ項目
 - 作成 578
- セキュア・プロトコル、クライアント・ユーザーティエリー
 - SSLv3 213
 - TLS 1.0 213
 - TLS 1.1 213
 - TLS 1.2 213
- セキュア・プロトコル、ディレクトリー・サーバー
 - SSLv3 188
 - TLS 1.0 188
 - TLS 1.1 188
 - TLS 1.2 188
- セキュリティー 163, 167
 - 鍵データベースの設定 179
 - 自己署名サーバー証明書 159
 - パスワード・ポリシー 236
 - Kerberos 254
 - SSL 151, 154
 - TLS 154
- セキュリティー設定
 - Web 管理ツール 151
- セキュリティー設定、構成
 - ディレクトリー・サーバー 186
- セキュリティー・プロトコル、構成
 - SSLv3 192
 - TLS 1.0 192
 - TLS 1.1 192
 - TLS 1.2 192
 - Web 管理ツール 222
- セキュリティー・プロトコル、Web 管理ツール
 - SSLv3 195
- セキュリティー・プロトコル、Web 管理ツール (続き)
 - TLS 1.0 195
 - TLS 1.1 195
 - TLS 1.2 195
- 接続 111
 - サービス妨害の防止 114
 - プロパティ 114
- 接続プロパティ
 - 管理 114
 - コマンド行 115
 - Web 管理ツール 114
- 設定 13, 163, 435
 - 暗号化の SSL レベル 184
 - 鍵データベース 179, 180
 - グローバル・パスワード・ポリシー 249
 - サーバー 157
 - 認証 157
 - SSL 179, 180
 - TLS 179, 180
- 設定の復元
 - テーブルのフィルター 26
- ソート済み検索制御 126
- 相互運用性サポート 670
- 相互運用性のガイドライン
 - 相互運用性
 - TDS および z/OS IBM TDS 757
- 相対識別名 10
- 属性 46, 51, 52, 148
 - キャッシュ 146
 - 構文 62
 - コピー 57
 - 固有 64
 - 索引付け規則 50
 - 削除 59
 - 追加 52
 - バイナリー 528
 - パスワード・ポリシー 243
 - 表示 51
 - 複数値 528
 - 複製 62
 - 変更 54, 55, 56
 - ユーザー・アプリケーション 79
 - ibm-slapdLogArchivePath 479
 - ibm-slapdLogMaxArchives 479
 - ibm-slapdLogSizeThreshold 479
 - MAY 82
 - MUST 82
- 属性、構成
 - 複製、運用属性 341
- 属性キャッシュ 146, 148
 - 属性の除去 145
 - 属性の追加 145
- 属性選択
 - パスワード・ポリシー 249

- 属性タイプ
 - グループ 578
 - スキーマ・ファイル 33
- 属性のコピー
 - コマンド行 57, 58
- 属性の削除 59
 - Web 管理ツール 59
- 属性のセット 46
- 属性の追加 54
 - Web 管理ツール 146

[タ行]

- 他のサーバー
 - 参照 303
- タブ 420
- 単一のデフォルト参照
 - コマンド行 310
 - 削除 310
- 追加 52, 385, 606
 - パスワード・ポリシー 249
- 追加、フィルター ACL 563
- 追加情報 669
- 通知
 - イベント 132
- 突き合わせ規則
 - 同等性 49
- データ交換フォーマット 641
- データの区画化 433
- データのコピー
 - レプリカ 333
- データの追加 433
- データの分割
 - 区画 443, 447
- データベース
 - バックアップ・ファイル 389
 - リカバリー 388
 - シングル・サーバー障害 391
 - 大規模障害 392
 - リストア 390
 - コマンド行 390
 - Web 管理ツール 390
- データベース接続
 - 数 119
- データベースの復元 390
- テーブル
 - 「アクションの選択」メニュー 25
 - 検索 27
 - 再配列 28
 - ソート 26
 - テーブルのアイコン 24
 - フィルター 27
 - ベージング 26
 - Web 管理ツール 24
- テーブルのフィルター 26
- テーブル・スペース 718, 722

- 定義 566
 - デフォルト参照 308
- ディレクトリー
 - 分散 425
- ディレクトリー管理 525, 534
 - 項目 526
 - 項目の ACL の編集 538
 - 項目のコピー 537
 - 項目の変更 535
 - ディレクトリー項目 525
 - ディレクトリー・ツリー、ブラウズ 525
- ディレクトリー管理サーバーのインスタンスの始動 14
- ディレクトリー管理サーバーのインスタンスの停止 14
- ディレクトリー項目 59, 525
 - インポート 759
 - エクスポート 759
 - 検索 541
- ディレクトリー属性キャッシュ
 - コマンド行 148
- ディレクトリーの概要 1
 - ディレクトリーのセキュリティ 2
 - ディレクトリー・クライアントとディレクトリー・サーバー 2
- ディレクトリーの参照
 - コマンド行 308
- ディレクトリーの定義 1
- ディレクトリー・サーバー
 - エラー・ログ 506
 - 管理グループ 291
 - デフォルト・ログのパス 477
 - ロギング
 - Web 管理ツール 22
 - NIST SP 800-131A への移行 185
- ディレクトリー・サーバー、一般情報
 - Suite B モード 202
 - TLS 1.2 署名およびハッシュ・アルゴリズム 198
- ディレクトリー・サーバー、構成
 - セキュリティ設定 186
 - SSLv3 192
 - Suite B モード 205
 - TLS 1.0 192
 - TLS 1.1 192
 - TLS 1.2 192
 - TLS 1.2 署名およびハッシュ・アルゴリズム 199
- ディレクトリー・サーバー、セキュリティ設定
 - 構成 186
- ディレクトリー・サーバー、トポロジー
 - NIST SP 800-131A 208

- ディレクトリー・サーバー、バインド用の固有の属性
 - 一般情報 261
 - 監査ログ・エントリー 261
 - 構成 263
 - 構成の例 263
- ディレクトリー・サーバー、NIST SP 800-131A
 - 相互運用性 209
- ディレクトリー・サーバー、Web 管理ツール
 - Suite B モード 207
 - TLS 1.2 署名およびハッシュ・アルゴリズム 201
- ディレクトリー・サーバーのバックアップおよび復元 466
- ディレクトリー・サーバー・インスタンスの始動
 - AIX 16
 - LINUX 16
 - Solaris 16
- ディレクトリー・サーバー・エラー・ログ 506
- ディレクトリー・スキーマ (directory schema) 718
- ディレクトリー・ツリー 525
- ディレクトリー・データベース 718
- 適用
 - 最小 ulimit 120, 122
- デフォルト・ログ設定
 - 変更 480
- 転送サーバー 356
 - Web 管理ツール 357
- 伝搬
 - ACL 555
- テンプレート 599, 607, 610
 - 作成 602
 - 追加 604
 - レルム 604
- テンプレート、管理 607
- 同期 441
 - LDAPSync 761
- 同期化
 - インスタンス 703
 - 両方向暗号化 703
- 統合
 - LDAPSync 761
- 動的
 - changes
 - スキーマ 68
 - 動的グループ 571, 572
 - memberURL の編集 587
 - 動的グループ項目 580
 - 動的グループ項目、作成 580
 - 動的スキーマ
 - アクセス・コントロール 68

動的スキーマ (続き)
突き合わせ規則 49
複製 69
changes 68
動的に変更される属性 713
トポロジー
複製 315
トポロジー管理
複製 401
トラステッド・ルート 176
トラブルシューティング ix
トランザクション
設定 135
トランザクション・カウント 92
トランザクション・サポート 135, 136
コマンド行 135
使用可能化 135
使用不可化 135
Web 管理ツール 135
トレース 86, 509
トレース機能 497
パフォーマンスのプロファイル作成
497

[ナ行]

認証
クライアント 161
サーバー 153
サーバーおよびクライアント 153
パススルー 266
認証局 167, 168
識別名 176
ネーム・スペース、バインディング
分散 304
ネストされたグループ 572
ネストされたグループ項目 581
ネストされたグループ項目、作成 581

[ハ行]

バージョン 1
LDIF サポート 642
バイナリー属性 528
バイナリー・データ
コマンド行 530
Web 管理ツール 528
バイナリー・データ、追加
コマンド行 530
バインド操作
一般 261
エラー・コード 261
バインド操作の固有の属性
一般情報 261
監査ログの例 261

バインド操作の固有の属性 (続き)
監査ログ・エントリ 261
構成 261
構成の例 263
パススルー認証 261
パススルー、サーバー 266
パススルー認証
オブジェクト・クラス 269
拡張 286
構成 182, 288
コマンド行 182
シナリオ 277
属性 269
トラブルシューティング 290
パススルー認証、構成
グローバル・カタログ 286
固有属性、作成 275
固有属性、終了 274
固有属性、存在 278
属性マッピング 274, 275, 278, 282
パススルー・サーバーでの DN 突き合
わせ 279
パスワードの移行 278
ユーザー項目、認証サーバーではなし
279
DN 値のマッピング 284
ibm-ptaReferral オブジェクト・クラス
282, 284
パスワード
管理 85
管理者 85
グループ 237
グローバル 236
個別 237
コンソール管理者 29
セキュリティ 236
ibmslapd.conf 246
パスワード暗号化
Web 管理ツール 235
パスワード属性 246
パスワードの変更
pwdsafemodify 254
パスワード・ポリシー 237, 250, 251,
253, 450, 669
アカウントのアンロック 671
運用属性 669, 672
オーバーライド 671
既存のパスワード・ポリシー 252
グローバル 248
項目に対する追加/更新 674
コピーの作成 252
照会 670
使用可能 253
属性 243
評価 242
複製 672

パスワード・ポリシー (続き)
複製、運用属性 339
パスワード・ポリシー、評価 237
パスワード・ポリシー運用属性
複製、構成 342
パスワード・ポリシー設定 1 250
パスワード・ポリシー設定 2 251
パスワード・ポリシー設定 3 251
パスワード・ポリシーの応答制御 670
パスワード・モニター
Web 管理ツール 150
バックアップおよび復元 717
方法 734
バックアップ複製 455
バックアップ・ファイルの作成
コマンド行 389
バックエンド・サーバー 435, 438
パフォーマンス 119
パフォーマンスのプロファイル作成 497
パフォーマンス・データの監査
コマンド行 499
使用可能化 499
Web 管理ツール 499
ピアツーピア
複製 362
ピアツーピアを使用した複雑なトポロジー
作成 362
ピア複製 372
ピア複製を持つ単純なトポロジー
作成 349
必須属性の定義 675
必要な許可 552
非フィルター ACL 548
評価 237, 238
パスワード・ポリシー 242
表示 32, 37, 38, 51, 52, 104, 445, 510,
511, 512, 513, 514, 559
エラー・ログ 509
フィルター 381, 383, 542
フィルター ACL、除去 565
フィルター属性 382
フィルターに掛けられていない ACL 561
サンプル LDIF ファイル 705
除去 562
フィルターに掛けられていない ACL、除
去 562
フィルターに掛けられていない ACL、追
加 561
フィルターに掛けられていない ACL、編
集 561
フィルターに処理されていない ACL 547
フィルターの追加 381
フィルター・キャッシュ
Web 管理ツール 143
フィルター・ベースの ACL 548
フェイルオーバー 451

- 複雑なトポロジー 372
 - 複数值、追加 528
 - 複製 320, 381
 - 運用属性 672
 - エラー処理 324
 - エラー・テーブル 393
 - 概要 317
 - カスケード複製 317
 - ゲートウェイ複製 319
 - シンプル複製 317
 - ピアツーピア複製 318
 - 複製競合の解決 320
 - キュー 419
 - ゲートウェイ・サーバーの管理 410
 - ゲートウェイ・トポロジーのセットアップ 370
 - 合意の編集 411
 - 考慮事項 724
 - コマンド行タスク 421
 - ゲートウェイ・サーバーの作成 424
 - 構成情報 421
 - サブツリーのサプライヤー DN およびパスワード 421
 - 状況のモニター 422
 - サーバー情報 412
 - サーバーの移動またはプロモート 408
 - サーバーの除去 407
 - サーバーの役割 315
 - サーバー・エラー 413
 - サブツリー 394
 - サブツリーの 330
 - サブツリーの除去 396
 - サブツリーの静止 396
 - サブツリーの追加 394
 - サブツリーの編集 395
 - サブツリーの編集 395
 - サブツリーの編集 395
 - サプライヤー情報 335, 414
 - 資格情報 397
 - 資格情報 ACL の管理 401
 - 資格情報の除去 401
 - 資格情報の追加 397
 - 資格情報の変更 400
 - スキーマ更新とパスワード・ポリシー更新 327
 - スケジュール 417
 - 属性 62
 - 動的スキーマ 69
 - トポロジー管理 401
 - トポロジーの表示 401
 - パスワード・ポリシー 672
 - ピアツーピアを使用した複雑なトポロジー 362
 - ピア複製を持つ単純なトポロジー 349
 - フィルターの追加 381
 - 複数のパスワード・ポリシー属性 672
 - 複製スケジュール 411
 - 複製 (続き)
 - 部分複製 380
 - プロパティの変更 415
 - マスター - 転送 - レプリカ 356
 - マスター - レプリカ・トポロジーの作成 328
 - マスターのデモート 409
 - マスター/レプリカの構成解除 368
 - マスター・サーバー 330
 - マルチスレッド 392
 - 用語 313
 - リカバリー手順 388
 - レプリカ 332, 405
 - 複製、構成
 - ibm-
 - slapdReplicateSecurityAttributes、ibm-replicareferralURL 342
 - 複製、パスワード・ポリシー
 - 運用属性 339
 - 運用属性、ibm-
 - replicateSecurityAttribute 345
 - 構成、属性 341
 - バインド・シナリオ 343
 - ibm-
 - replicateSecurityAttribute、false 345
 - ibm-replicateSecurityAttribute、true 345
 - 複製競合
 - 解決 323, 324
 - 使用可能 323
 - 使用不可 323
 - Security Directory Server 6.1 324
 - Web 管理ツール 323
 - 複製競合の解決 320
 - 複製の管理 394
 - 複製の構成
 - 考慮事項 326
 - 複製フィルター 385
 - コピー 384
 - コマンド行 385
 - フィルター対象属性 384
 - 複製フィルター - 一般 383
 - 複製フィルター - フィルター対象属性 385
 - 複製フィルターの追加
 - フィルター対象属性 382
 - 複製フィルターの追加 - 一般 381
 - 複製方式
 - マルチスレッド 392
 - 部分 320
 - フロー 761
 - プロキシ管理 445
 - プロキシ許可 525, 593
 - プロキシ許可グループ 594, 597
 - プロキシ許可グループ、コピー
 - コマンド行 597
 - Web 管理ツール 597
- プロキシ許可グループの除去
 - idsldapdelete 598
 - Web 管理 598
- プロキシ・サーバー 439, 440, 446, 447
 - バックアップ 454
 - フェイルオーバー 454
- プロパティの管理 32
- プロモート 409
 - レプリカ・サーバー 409
- 分散
 - ネーム・スペース、バインディング 304
- 分散ディレクトリー 425
 - 区画項目 435
 - グローバル・ポリシー・トポロジー作成 460
 - 作成 435, 439
 - 情報の同期化 434
 - データの分割化 461
 - パスワード・ポリシー 450
 - バックアップ複製 455
 - サーバー・グループ 457
 - バックエンド・サーバー 435
 - フェイルオーバーおよびロード・バランシング 451
 - 複製トポロジー
 - 作成 459
 - 複製の開始 466
 - プロキシ 426, 430, 431, 435, 439, 455, 457
 - プロキシでのトランザクション 465
 - プロキシ・サーバー
 - 作成 461
 - 正常性チェック状況 453
 - 正常性チェック・スレッド 452
 - 分割したデータ
 - ロード 461
 - 分割データ 430
 - 分散ディレクトリーのセットアップ・ツール 432
 - モニター検索 462
 - DN 区画化プラグイン 431
 - LDIF ファイル
 - 作成 458
 - RDN ハッシュ 430
- 分散ディレクトリー・サーバー 440, 447
- ページング 26
- 変換 425
- 変更 308
 - コマンド行 591
 - サーバー・ログ設定 507
 - レプリカ 356
 - ibm-slapdDNPartitionPlugin 432
 - referral 309
 - Web 管理ツール 591

変更、フィルター ACL 563
 変更、ポートの 117
 変更ログ・データベース 722
 編集 61, 383, 384, 606, 607, 610, 612, 614
 アクセス・コントロール・リスト 397
 サブツリー (subtree) 397
 パスワード・ポリシー 252
 フィルター 383
 保管 170
 補助オブジェクト・クラス
 削除 540
 追加 539
 補助オブジェクト・クラス、追加
 コマンド行 540
 Web 管理ツール 539
 補助オブジェクト・クラスの削除 540
 Web 管理 541
 補助オブジェクト・クラスの追加 539

[マ行]

マスター - レプリカ・トポロジー
 作成 328
 マスターレプリカ
 構成解除 368
 マルチスレッド
 複製 392
 メッセージ
 エラー 617
 メンバー、追加 583
 メンバーシップ 437
 メンバーシップの管理 585
 メンバーシップ用ユーザー項目
 作成 438
 追加 438
 メンバーの管理 583
 メンバーの除去
 グループ項目 585
 メンバーの追加
 管理グループ 298, 299
 コマンド行 299
 Web 管理ツール 298
 モード 19
 検証 19
 コマンド行 19
 モニター
 サービス・ステータス 95
 システム情報 103
 接続 102
 changelog 102
 モニター検索 462
 問題判別 ix

[ヤ行]

役割 569, 588
 ユーザー 599, 611, 613
 ユーザー、管理 611
 ユーザー関連タスク
 テンプレート 599
 ユーザーおよびグループ 599
 レルム 599
 ユーザー項目の作成 437
 ユーザー項目の追加 437
 ユーザー情報 612
 ユーザーの追加
 Web 管理ツール 611
 ユーザー・アプリケーション
 属性 79
 ユーザー・テンプレートの追加
 Web 管理ツール 607
 有効所有者 560
 有効なアクセス制御リスト 559
 用語 vii, 313

[ラ行]

ランゲージ・サポート 643
 リカバリー
 データベース 388
 両方向暗号化
 インスタンス 703
 同期化 703
 ルート DSE
 検索 108, 111
 属性 623
 ルート DSE の属性 108, 111
 例 385, 572
 疑似 DN 551
 バックアップ 736
 リストア 736
 ロールフォワード 736
 DB2 736
 LDIF 641
 バージョン 1 642
 レプリカ 357
 サーバーの作成 310
 レプリカ・サーバー 409
 レプリカ・サーバーからマスターへ 409
 レルム 599, 606, 607
 管理者 600
 作成 599
 追加 604
 テンプレート 604
 ユーザーの追加 605
 Web 管理ツール 606
 レルム内 611, 613
 レルムの管理グループ 600
 ロード・バランシング 451, 454

ロールフォワード 724
 ログ
 コマンド行 510
 ログ管理ツール
 idslogmgmt 516
 ログ設定
 デフォルト
 変更 480
 ログの管理 521, 724
 項目 517
 ログのパス
 デフォルト 477
 ログの表示 509
 Web 管理ツール 509

[ワ行]

ワーカー
 サーバー状況 101
 ワーカー・ステータス 93
 割り当て
 区画索引値 444

A

ACI 機構
 OID 636
 ACI 情報 546
 ACI の管理
 ACI または entryOwner の変更 567
 ACI または entryOwner 568
 取得 568
 delete 568
 ACI または entryOwner の変更
 ACI の管理 567
 ACL 546, 548, 566, 607, 610
 構文 549
 伝搬 555
 フィルターに掛けられていない 561
 フィルターに処理された 563
 フィルター・ベース 547
 ACL キャッシュ
 手順 144
 ACL キャッシュ・サイズ 119
 ACL の管理 566
 ACL のフィルター操作 547, 563
 サンプル LDIF ファイル 705
 除去 565
 ACL のプロパティ 558
 ACL のプロパティ、表示 558
 Active Directory
 同期 659
 Active Directory との同期
 実行 665
 使用されるファイル 661

Active Directory との同期 (続き)

使用する場合の手順 660

Active Directory 665

SSL 接続の使用 665

ASCII 文字

暗号化シード・ストリングで使用可能な 647

33 から 126 647

B

bulkload

エラー・ログ 499

Bulkload ログ

コマンド行 512

変更 500

C

CBE および CARS

ログ管理属性 518

CBE および CARS のログ管理

Web 管理ツール 518

CBE 機能と CARS 機能

コマンド行 521

CBE フォーマット

output 517

changelog 102

cms 鍵データベース、作成

自己署名証明書 223

D

DB2

エラー・ログ 503

共通の問題 736

バックアップ 727, 736

リストア 727, 736

ロールフォワード 736

DB2 エラー・ログ 503

DB2 パスワード

更新 149

コマンド行 150

パスワード・モニター 149

モニター 149

Web 管理ツール 149

DB2 ログ

コマンド行 513

DB2 ログ設定

変更 503, 504

Web 管理ツール 503

delete 383

DIGEST-MD5 259

構成 259

DIGEST-MD5 メカニズム

作成 260

Web 管理ツール 259

directory

オプション 545

directory server のバックアップ

構成 471

directory server の復元

コマンド行 475

DN 10

疑似 551

DN エスケープ文字 12

E

entryOwner 546

entryOwner 情報 546

G

group membership 574, 586

除去 586

GSKit、鍵データベース

インポート、証明書 227

H

HTTPS

WebSphere Application Server 組み込みバージョン 7.x 739

I

IANA 文字セット 643

IBM

ソフトウェア・サポート ix

Support Assistant ix

IBM Security Directory Integrator 651

IBM Security Directory Server 1, 160,

675, 717

スキーマ定義属性 73

スキーマの検査 80

スキーマの照会 67

制限付き属性 72

ディレクトリー通信の保護 151

ディレクトリー・アクセス権限の保護

231

ルート DSE の属性 73

SSL セキュリティー 740

IBM Security Directory スキーマ

管理 33

IBMAttributeTypes

オブジェクト・クラス 47

ibmdisrv

LDAPSync 767

ibmslapd オプション 19

ibmslapd.conf 137

パスワード 246

IBMsubschema 67

ID マッピング

Kerberos 257

idsbulkload 499

エラー・ログ 499

idsdiradm

管理サーバー 13

idsexop 116

idsldapdelete 535, 593, 598

idsldapmodify 55, 56, 116, 534, 541, 597

searchTimeLimit の変更 591

idsldapmodrdn 536

idsldapsearch 95, 544

idslogmgmt

ログ管理ツール 516

idslogmgmt.log 478

idsslapd オプション 19

idsslapd.conf 137

idssnmp 656

コマンド行 656

ikeycmd、鍵データベース

エクスポート、証明書 229

iPlanet

互換性 82

文法 82

ipv4 649

Ipv6 649

J

jks 鍵データベース、構成

Web 管理ツール 222

jks 鍵データベース、作成

自己署名証明書 223

K

Kerberos 254

ID マッピング 257

Kerberos 項目

コマンド行 256

セキュリティーのプロパティー 255

Web 管理ツール 255

L

LDAP

バックアップおよび復元の手順 722

LDAP クライアント 160

LDAP ディレクトリー 546

参照 302

ldapmodify 488

LDAPSync
 移行 767
 インストール 762
 エンドポイント 761
 概要 761
 カスタマイズ 770
 構成 763
 シミュレーション 767
 設定 770
 操作 769
 ターゲット 761
 同期 767
 引数 769
 フロー 761
 プロパティ 770
 logs 778
 LDIF 641, 757
 LDIF 構文 546
 LDIF ファイル 55, 56, 439
 logs
 逸失および検出 476
 エラー
 逸失および検出 504
 監査 488, 493, 495, 496
 管理サーバー 481
 構成ツール 501
 ディレクトリー・サーバー 506
 表示 509
 bulkload 499
 DB2 503
 idsbulkload 499
 監査 476
 管理サーバー 484, 487
 管理サーバー監査 476
 管理サーバー・エラー 476
 構成ツール 476
 サーバー・エラー 476
 使用不可化 487, 496
 デフォルト設定 476
 ログ管理ツール 478
 bulkload 476
 DB2 476
 idslogmgmt 478
 ログ管理ツール 478
 LDAPSync 778

N

NIST SP 800-131A
 一般情報 184
 NIST SP 800-131A、移行
 クライアント・ユーティリティー 212
 ディレクトリー・サーバー 185

O

OID
 オブジェクト ID 35
 拡張操作 636
 サポートされ、使用可能になっている
 機能 625
 制御 638
 ルート DSE 623
 ACI 機構 636
 ownerPropagate 546

P

PKCS#11
 インターフェース 180
 Web 管理ツール 181
 PKCS#11 インターフェース
 構成 181
 サーバー 181

Q

QRadar
 ログ管理属性 518

R

RDN 10
 ref 属性 302
 referral
 オブジェクト・クラス 302
 ref 属性 302

S

searchTimeLimit の変更 591
 Secure Sockets Layer 151
 Security Directory Server 718, 722, 724,
 728
 データベース定義 717
 ディレクトリー・スキーマ (directory
 schema) 717
 Security Directory Server の概要 3
 Simple Network Management Protocol 651
 SNMP 651
 SNMP ロギング 656
 SSL 151, 155
 SSL シナリオ
 管理サーバー 740
 クライアントおよびサーバー 748
 IBM Security Directory Server 740
 SSL セキュリティー 739, 740, 748
 SSL 証明書取り消し検査
 コマンド行 231

SSL 証明書取り消し検査 (続き)
 使用可能化 230
 SSL 通信
 コマンド行 154

T

TLS 151
 tombstone
 コマンド行 141
 Web 管理ツール 141
 Transaction Layer Security 151

U

URL フォーマット
 ipv4 649
 ipv6 649
 UTC 時刻 83
 UTF-8 530, 643

W

Web アドレス・プロトコル
 ipv4 649
 ipv6 649
 Web 管理
 検索制限グループの除去 593
 検索制限グループの変更 591
 項目の削除 534
 項目の変更 535
 プロキシ許可グループの除去 598
 補助オブジェクト・クラスの削除 541
 Web 管理、項目の追加 526
 Web 管理コンソール 23
 logs 477
 Web 管理サーバー 13
 Web 管理タスク 394
 Web 管理ツール
 イベント通知 133
 オブジェクト・クラス 37, 40
 管理
 サーバー・パフォーマンス 119
 管理、コンソール 29
 管理グループ
 メンバーの除去 301
 キャッシュ・プロパティ、管理 142
 コンソール 21
 サーバー状況
 決定 88
 サーバー・インスタンス 108
 最小 ulimit
 適用 122
 サフィックス
 除去 139

Web 管理ツール (続き)

実行

ディレクトリー・サーバー 474

バックアップ 474

始動 20

始動または停止 521

使用可能化 133, 135

使用不可化 137

除去 148

属性 66

スキーマ 37

設定

鍵データベース 179

SSL 179

TLS 179

セットアップ 28

属性 148

属性キャッシュ 148

トランザクション・サポート 135,

137

表示 37, 40

プロキシ・サーバーのセットアップ

439

ルート DSE

検索 108

ルート DSE の属性 108

ログの管理 521

logs 493

Web 管理ツール、鍵データベース構成

jks 222

Web 管理ツール、構成

セキュリティー・プロトコル 222

jks 鍵データベース 222

SSLv3 195

Suite B モード 207

TLS 1.0 195

TLS 1.1 195

TLS 1.2 195

TLS 1.2 署名およびハッシュ・アルゴ

リズム 201

webadmin 検索 32

Windows サービス・アイコン

コマンド行 87

Windows システム 15

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の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)[®] 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 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

SA88-4190-02



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