

Sun Java System Directory Server Enterprise Edition 6.3 インス トールガイド



Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 820-5398
2008年4月

本書で説明する製品で使用されている技術に関連した知的所有権は、Sun Microsystems, Inc. に帰属します。特に、制限を受けることなく、この知的所有権には、米国特許、および米国をはじめとする他の国々で申請中の特許が含まれています。

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

本製品には、サードパーティーが開発した技術が含まれている場合があります。

本製品の一部は Berkeley BSD システムより派生したもので、カリフォルニア大学よりライセンスを受けています。UNIX は、X/Open Company, Ltd. が独占的にライセンスしている米国ならびにほかの国における登録商標です。

Sun、Sun Microsystems、Sun のロゴマーク、Solaris のロゴマーク、Java Coffee Cup のロゴマーク、docs.sun.com、Java、Solaris は、米国およびその他の国における米国 Sun Microsystems, Inc. (以下、米国 Sun Microsystems 社とします) の商標もしくは登録商標です。Sun のロゴマークおよび Solaris は、米国 Sun Microsystems 社の登録商標です。すべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している同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。SPARC 商標が付いた製品は、米国 Sun Microsystems 社が開発したアーキテクチャーに基づくものです。

OPEN LOOK および SunTM Graphical User Interface は、米国 Sun Microsystems 社が自社のユーザーおよびライセンス実施権者向けに開発しました。米国 Sun Microsystems 社は、コンピュータ産業用のビジュアルまたはグラフィカルユーザーインターフェースの概念の研究開発における米国 Xerox 社の先駆者としての成果を認めるものです。米国 Sun Microsystems 社は米国 Xerox 社から Xerox Graphical User Interface の非独占的ライセンスを取得しており、このライセンスは、OPEN LOOK GUI を実装するか、または米国 Sun Microsystems 社の書面によるライセンス契約に従う米国 Sun Microsystems 社のライセンス実施権者にも適用されます。

この製品は、米国の輸出規制に関する法規の適用および管理下にあり、また、米国以外の国の輸出および輸入規制に関する法規の制限を受ける場合があります。核、ミサイル、生物化学兵器もしくは原子力船に関連した使用またはかかる使用者への提供は、直接的にも間接的にも、禁止されています。このソフトウェアを、米国の輸出禁止国へ輸出または再輸出すること、および米国輸出制限対象リスト(輸出が禁止されている個人リスト、特別に指定された国籍者リストを含む)に指定された、法人、または団体に輸出または再輸出することは一切禁止されています。

本書は、「現状のまま」をベースとして提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も行われないものとします。

目次

はじめに	11
パート I	
Directory Service Control Center、Directory Proxy Server、Directory Server、および Directory Server Resource Kit のインストール	23
1 Directory Server Enterprise Edition 6.3 のインストール	25
インストール手順のクイックリファレンス	25
ソフトウェアのインストール	27
ネイティブパッケージを使用して Directory Server Enterprise Edition をインストールする	28
ZIP 形式の配布を使用して Directory Server Enterprise Edition をインストールする	45
Directory Service Control Center を使い始める	55
環境変数	63
サーバーインスタンスの作成	64
▼ DSCC を使用して Directory Server インスタンスを作成する	65
▼ コマンド行から Directory Server インスタンスを作成する	67
▼ DSCC を使用して Directory Proxy Server インスタンスを作成する	71
▼ コマンド行から Directory Proxy Server インスタンスを作成する	73
Solaris 10 システムで Sun 暗号化フレームワークを使用する	77
▼ Solaris 10 システムで暗号化ハードウェアとともに Directory Server を使用する ...	77
▼ Solaris 10 システムで暗号化ハードウェアとともに Directory Proxy Server を使用する	79
2 Directory Server Enterprise Edition 6.3 のアンインストール	81
サーバーインスタンスの削除	81
▼ DSCC を使用して Directory Proxy Server インスタンスを削除する	82
▼ コマンド行から Directory Proxy Server インスタンスを削除する	82

▼ DSCC を使用して Directory Server インスタンスを削除する	83
▼ コマンド行から Directory Server インスタンスを削除する	83
ソフトウェアの削除	84
▼ ネイティブパッケージからインストールした Directory Service Control Center を削除する	84
▼ ネイティブパッケージからインストールした Directory Server または Directory Proxy Server を削除する	85
▼ ZIP 形式の配布からインストールしたソフトウェアを削除する	85
▼ ZIP 形式の配布からインストールしたソフトウェアを強制的に削除する	86
Directory Server Enterprise Edition 6.3 のダウングレード手順	86
ネイティブパッケージを使用して Directory Server Enterprise Edition をダウングレードする	86
ZIP 形式の配布を使用して Directory Server Enterprise Edition をダウングレードする	89
パート II Identity Synchronization for Windows のインストール	91
3 製品の理解	95
製品の特徴	96
システムコンポーネント	97
ウォッチドッグプロセス	98
コア	98
コネクタ	101
コネクタサブコンポーネント	101
Message Queue	102
システムコンポーネントの分散	103
コア	103
ディレクトリサーバーコネクタおよびプラグイン	103
Active Directory コネクタ	104
Windows NT コネクタおよびサブコンポーネント	105
Identity Synchronization for Windows がディレクトリソースでの変更を検出する方法	106
ディレクトリサーバーコネクタが変更を検出する方法	106
Active Directory コネクタが変更を検出する方法	107
Windows NT コネクタが変更を検出する方法	108
パスワード更新の伝播	109

信頼できる同期	111
配備の例:2台のマシン構成	112
物理的な配備	114
コンポーネントの分散	114
4 インストールの準備	117
インストールの概要	118
コアのインストール	120
製品の設定	121
Directory Server の準備	121
コネクタのインストールおよびディレクトリサーバープラグインの設定	121
既存ユーザーの同期	122
設定の概要	123
ディレクトリ	123
同期設定	123
オブジェクトクラス	124
属性および属性マッピング	124
同期ユーザーリスト	126
Active Directory とのパスワードの同期	127
パスワードポリシーの要求	127
SSL 動作のための Windows の設定	133
インストールおよび設定の決定	134
コアのインストール	134
コアの設定	134
コネクタのインストールおよびディレクトリサーバープラグインの設定	135
コマンド行ユーティリティーの使用	136
インストールチェックリスト	137
5 コアの実インストール	141
始める前に	141
インストールプログラムの起動	142
Solaris SPARC の場合	142
Solaris x86 の場合	143
Windows の場合	143
Red Hat Linux の場合	144

コアのインストール	144
▼ インストールウィザードを使用して Identity Synchronization for Windows コアコン ポーネントをインストールする	145
6 コアリソースの設定	155
設定の概要	155
Identity Synchronization for Windows コンソールを開く	156
▼ Identity Synchronization for Windows コンソールを開く	157
ディレクトリソースの作成	160
▼ ディレクトリソースを作成する	160
Sun Java System ディレクトリソースの作成	161
Sun ディレクトリソースの準備	168
Active Directory ソースの作成	172
Windows NT SAM ディレクトリソースの作成	180
ユーザー属性の選択とマッピング	183
属性の選択とマッピング	183
パラメータ化されたデフォルト属性値の作成	185
スキーマソースの変更	186
システム間でのユーザー属性の伝播	189
オブジェクト作成のフローの指定	189
オブジェクト変更のフローの指定	195
グループ同期の設定	203
アカウントのロックアウトおよびロックアウト解除の設定と同期	205
削除のフロー方法の指定	208
同期ユーザーリストの作成	209
▼ サーバー間でユーザータイプを識別してリンクさせる	209
設定の保存	214
▼ コンソールパネルから現在の設定を保存する	214
7 コネクタのインストール	217
始める前に	217
インストールプログラムの実行	218
▼ インストールプログラムを再起動して実行する	218
コネクタのインストール	220
ディレクトリサーバーコネクタのインストール	220

Active Directory コネクタのインストール	226
Windows NT コネクタのインストール	229
8 既存のユーザーおよびユーザーグループの同期	231
既存のユーザーおよびグループの入力に基づくインストール後の手順	232
idsync resync の使用	232
ユーザーまたはグループの再同期	233
ユーザーのリンク	233
idsync resync のオプション	234
セントラルログで結果の確認	238
同期の起動および停止	238
▼同期を起動または停止する	238
再同期されたユーザー/グループ	239
サービスの起動および停止	239
9 ソフトウェアの削除	241
アンインストールの計画	241
ソフトウェアのアンインストール	242
コネクタのアンインストール	243
▼コアをアンインストールする	244
コンソールの手動アンインストール	247
Solaris または Linux システムでの操作	247
Windows システムでの操作	247
10 セキュリティーの設定	249
セキュリティの概要	249
設定パスワードの指定	250
SSL の使用	250
信頼できる SSL 証明書の要求	251
生成された 3DES キー	251
SSL および 3DES キーでの保護の概要	251
Message Queue のアクセス制御	253
ディレクトリ資格	254
持続的記憶領域保護の概要	254

セキュリティの強化	255
設定パスワード	255
設定ディレクトリの資格の作成	256
Message Queue のクライアント証明書の検証	256
Message Queue の自己署名付き SSL 証明書	257
Message Queue ブローカへのアクセス	257
設定ディレクトリ証明書の検証	257
設定ディレクトリへのアクセスの制限	257
レプリケートされた設定のセキュリティ保護	258
idsync certinfo の使用	260
引数	260
使い方	261
Directory Server での SSL の有効化	262
▼ Directory Server で SSL を有効にする	262
Directory Server の証明書データベースからの CA 証明書の取得	263
(Solaris プラットフォームで dsadm コマンドを使用した) Directory Server からの CA 証明書の取得	263
Active Directory コネクタでの SSL の有効化	264
Active Directory 証明書の取得	264
Active Directory 証明書のコネクタの証明書データベースへの追加	266
Directory Server への Active Directory 証明書の追加	267
▼ Active Directory CA 証明書を Directory Server 証明書データベースに追加する	267
ディレクトリサーバーコネクタへの Directory Server 証明書の追加	268
▼ Directory Server 証明書をディレクトリサーバーコネクタに追加する	268
11 監査ファイルとエラーファイルの理解	269
ログの理解	269
ログタイプ	270
ログの読み取り	273
ログファイルの設定	274
▼ 配備のログを設定する	274
ディレクトリソースの状態の表示	276
▼ ディレクトリソースの状態を表示する	276
インストール状態と設定状態の表示	278
▼ インストールと設定のプロセスの残りの手順を表示する	278

	監査ログとエラーログの表示	279
	▼ エラーログを表示する	279
	Windows NT マシンでの監査の有効化	280
	▼ Windows NT マシンで監査ログを有効にする	280
パート III	Identity Synchronization for Windows 付録	281
A	Identity Synchronization for Windows コマンド行ユーティリティーの使用	283
	共通機能	283
	Idsync サブコマンドに共通の引数	283
	パスワードの入力	286
	ヘルプの使用	286
	idsync コマンドの使用	286
	certinfo の使用	288
	changepw の使用	289
	importcnf の使用	290
	prepds の使用	291
	printstat の使用	294
	resetconn の使用	295
	resync の使用	296
	groupsync の使用	299
	accountlockout の使用	299
	dspluginconfig の使用	300
	startsync の使用	300
	stopsync の使用	301
	forcepwhcg 移行ユーティリティーの使用	302
	▼ forcepwhcg コマンド行ユーティリティーを実行する	302
B	Identity Synchronization for Windows LinkUsers XML ドキュメントの例	305
	例 1: linkusers-simple.cfg	305
	例 2: linkusers.cfg	306
C	Solaris 上での root 以外での Identity Synchronization for Windows サービスの実行	309
	root 以外のユーザーとしてのサービスの実行	309

▼ root 以外のユーザーとしてサービスを実行する	309
D Identity Synchronization for Windows の同期ユーザーリストの定義と設定	311
同期ユーザーリストの定義の理解	311
複数の Windows ドメインの設定	313
▼ 複数の Windows ドメインを設定する	314
E レプリケートされた環境での Identity Synchronization for Windows のインストールの注	
意点	317
レプリケーションの設定	317
▼ レプリケーショントポロジを設定する	318
SSL を介したレプリケーションの設定	319
▼ レプリケーション動作がすべて SSL 接続を介して実行されるようレプリケー	
ションにかかわる Directory Server を設定する	319
MMR 環境での Identity Synchronization for Windows の設定	320
▼ MMR 環境で Identity Synchronization for Windows を設定する	320
 索引	 323

はじめに

インストールガイドでは、Directory Server Enterprise Edition の Directory Service Control Center、Directory Proxy Server、Directory Server、Directory Server Resource Kit、および Identity Synchronization for Windows の各コンポーネントのインストール手順について説明します。

対象読者

評価目的のみで Directory Server Enterprise Edition ソフトウェアをインストールする場合、このガイドではなく、[『Sun Java System Directory Server Enterprise Edition 6.3 Evaluation Guide』](#) を参照してください。

このインストールガイドは Directory Proxy Server、Directory Server、Directory Server Resource Kit、Directory Service Control Center、および Identity Synchronization for Windows ソフトウェアを配備する管理者を対象としています。このマニュアルでは、Identity Synchronization for Windows の設定についても説明します。

このガイドは、他の Java Enterprise System (Java ES) 製品とのインストールについては説明していません。Directory Server および Directory Service Control Center ソフトウェアを Java ES ソフトウェアとともにインストールしようとしている場合は、<http://docs.sun.com/coll/1286.3> にある Java ES ソフトウェアのインストールの説明をお読みください。

このガイドは Directory Editor ソフトウェアのインストールについては説明していません。Directory Editor ソフトウェアのインストールを計画している場合は、まず、[『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』](#) の「Directory Editor の既知の問題点と制限事項」をお読みください。その後、[『Sun Java System Directory Editor 1 2005Q1 Installation and Configuration Guide』](#) のインストールの説明をお読みください。

必ず [『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』](#) の第 6 章「Directory Editor の修正されたバグと既知の問題点」もお読みください。

このマニュアルをお読みになる前に

『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』の関連情報を確認してください。

本稼働環境で Directory Server Enterprise Edition ソフトウェアを配備する場合は、『Sun Java System Directory Server Enterprise Edition 6.3 配備計画ガイド』の関連情報も確認してください。

Identity Synchronization for Windows をインストールする読者は、次の技術をよく理解しておくようにしてください。

- Directory Server
- Microsoft Active Directory または Windows NT の認証
- LDAP (Lightweight Directory Access Protocol)
- Java テクノロジ
- XML (Extensible Markup Language)
- 公開鍵暗号方式と SSL (Secure Sockets Layer) プロトコル
- イン트라ネット、エクストラネット、およびインターネットのセキュリティー
- 企業でのデジタル証明書の役割

内容の紹介

パート I 「Directory Service Control Center、Directory Proxy Server、Directory Server、および Directory Server Resource Kit のインストール」では、サポートされているシステム上での Directory Proxy Server、Directory Server、Directory Server Resource Kit、および Directory Service Control Center のインストールについて説明します。

パート II 「Identity Synchronization for Windows のインストール」では、サポートされているシステム上での Identity Synchronization for Windows のインストールについて説明します。

パート III 「Identity Synchronization for Windows 付録」では、Identity Synchronization for Windows を使用するために必要なあらゆる追加情報について説明します。

Directory Server Enterprise Edition マニュアルセット

この Directory Server Enterprise Edition マニュアルセットでは、Sun Java System Directory Server Enterprise Edition を使用してディレクトリサービスを評価、設計、配備、および管理する方法について説明します。Directory Server Enterprise Edition 用のクライアントアプリケーションを開発する方法も示します。Directory Server Enterprise Edition マニュアルセットは <http://docs.sun.com/coll/1224.4> から入手できます。

Directory Server Enterprise Edition について理解を深めるには、次の表に示すドキュメントを順番に参照してください。

表 P-1 Directory Server Enterprise Edition マニュアル

マニュアルタイトル	内容
『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』	既知の問題を含め、Directory Server Enterprise Edition についての最新情報を提供しています。
『Sun Java System Directory Server Enterprise Edition 7.0 Documentation Center 』	マニュアルセットの重要な領域へのリンクを提供しています。
『Sun Java System Directory Server Enterprise Edition 6.3 Evaluation Guide 』	このリリースの重要な機能を紹介します。これらの機能の仕組みや提供される利点を、単独システムに実装可能な架空の配備のコンテキストに沿って例示します。
『Sun Java System Directory Server Enterprise Edition 6.3 配備計画ガイド』	Directory Server Enterprise Edition をベースとする、可用性と拡張性に優れたディレクトリサービスを計画および設計する方法について説明します。配備の計画および設計の基本的な概念および原則を提示します。ソリューションのライフサイクルについて検討し、Directory Server Enterprise Edition ベースのソリューションを計画するために使用する概略レベルのサンプルおよび戦略を提供します。
『Sun Java System Directory Server Enterprise Edition 6.3 インストールガイド』	<p>Directory Server Enterprise Edition ソフトウェアのインストール方法について説明します。インストールするコンポーネントを選択する方法、インストール後にそれらのコンポーネントを設定する方法、および設定したコンポーネントが正しく機能することを検証する方法を示します。</p> <p>Directory Editor のインストール手順については、http://docs.sun.com/coll/DirEdit_05q1 を参照してください。</p> <p>Directory Editor をインストールする前に、『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』の Directory Editor についての情報を必ずお読みください。</p>
『Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide 』	Directory Server、Directory Proxy Server、および Identity Synchronization for Windows の以前のバージョンから移行する手順を示します。
『Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド』	<p>Directory Server Enterprise Edition をコマンド行から管理するための手順を示します。</p> <p>Directory Service Control Center (DSCC) を使用して Directory Server Enterprise Edition を管理する際のヒントおよび手順については、DSCC のオンラインヘルプを参照してください。</p> <p>Directory Editor の管理手順については、http://docs.sun.com/coll/DirEdit_05q1 を参照してください。</p> <p>Identity Synchronization for Windows のインストールおよび設定の手順については、パート II 「Identity Synchronization for Windows のインストール」を参照してください。</p>

表 P-1 Directory Server Enterprise Edition マニュアル (続き)

マニュアルタイトル	内容
『Sun Java System Directory Server Enterprise Edition 6.3 Developer's Guide』	Directory Server Enterprise Edition の一部として提供されるツールおよび API を利用して、ディレクトリクライアントアプリケーションを開発する方法を示します。
『Sun Java System Directory Server Enterprise Edition 6.3 Reference』	Directory Server Enterprise Edition の技術および概念の基礎を紹介します。コンポーネント、アーキテクチャー、プロセス、および機能について説明しています。開発者 API への参照も示しています。
『Sun Java System Directory Server Enterprise Edition 6.3 Man Page Reference』	Directory Server Enterprise Edition を通じて利用可能なコマンド行ツール、スキーマオブジェクト、およびその他の公開インタフェースについて説明しています。このマニュアルの個別の節を、オンラインマニュアルページとしてインストールすることができます。
『Sun Java System Directory Server Enterprise Edition 6.3トラブルシューティングガイド』	さまざまなツールを使用して問題の範囲を特定し、データを収集し、問題部分の障害追跡を行う手順について説明しています。
『Sun Java System Identity Synchronization for Windows 6.0 Deployment Planning Guide』	Identity Synchronization for Windows の計画と配備に関する一般的なガイドラインやベストプラクティスを示しています。

関連資料

SLAMD 分散負荷生成エンジンとは、ネットワークベースのアプリケーションの負荷テストを実行し、パフォーマンスを分析するために設計された Java™ アプリケーションです。SLAMD は当初 Sun Microsystems, Inc. によって、LDAP ディレクトリサーバーのパフォーマンスをベンチマークおよび分析する目的で開発されました。

SLAMD は、OSI が承認したオープンソースライセンスである Sun Public License のもとでオープンソースアプリケーションとして公開されています。SLAMD についての情報を入手するには、<http://www.slamd.com/> を参照してください。SLAMD は java.net プロジェクトとしても公開されています。<https://slamd.dev.java.net/> を参照してください。

Java Naming and Directory Interface (JNDI) 技術は、LDAP および DSML v2 を利用した、Java アプリケーションからのディレクトリサーバーへのアクセスをサポートします。JNDI の詳細については、<http://java.sun.com/products/jndi/> を参照してください。『JNDI チュートリアル』には、JNDI の使用方法についての詳しい説明およびサンプルを収録しています。このチュートリアルは <http://java.sun.com/products/jndi/tutorial/> から入手できます。

Directory Server Enterprise Edition のライセンス形態には、スタンドアロン製品、Sun Java Enterprise System のコンポーネント、Sun Java Identity Management Suite などの Sun 製品群の一部、または Sun からのほかのソフトウェア製品へのアドオンパッケージがあります。Java Enterprise System は、ネットワークまたはインターネット環境で分散配備されるエンタープライズアプリケーションをサポートするソフトウェアインフラストラクチャーです。Directory Server Enterprise Edition が Java Enterprise System の

コンポーネントとしてライセンスされる場合、<http://docs.sun.com/coll/1286.3> から入手可能なシステムマニュアルに目を通してください。

Identity Synchronization for Windows は Message Queue を制限されたライセンスで使用します。Message Queue のマニュアルは <http://docs.sun.com/coll/1307.2> から入手できます。

Identity Synchronization for Windows は、Microsoft Windows のパスワードポリシーを管理するための製品です。

- Windows Server 2003 のパスワードポリシーについての情報は、[Microsoft TechNet Web サイト](#)で公開されています。
- Microsoft 証明書サービスのエンタープライズルート認証局に関する情報は、[Microsoft サポートオンライン Web サイト](#)で公開されています。
- Microsoft システムでの LDAP over SSL の設定に関する情報は、[Microsoft サポートオンライン Web サイト](#)で公開されています。

再配布可能なファイル

Directory Server Enterprise Edition では、お客様による再配布が可能なファイルは提供されません。

デフォルトのパスとコマンドの場所

この節では、マニュアルで使用するデフォルトのパスについて説明し、オペレーティングシステムや配備タイプによって異なるコマンドの場所を示します。

デフォルトのパス

次の表では、このマニュアルで使用するデフォルトのパスについて説明します。インストールされるファイルの詳細な説明については、次の製品マニュアルを参照してください。

- 『Sun Java System Directory Server Enterprise Edition 6.3 Reference』の第 14 章「Directory Server File Reference」
- 『Sun Java System Directory Server Enterprise Edition 6.3 Reference』の第 25 章「Directory Proxy Server File Reference」
- 『Sun Java System Directory Server Enterprise Edition 6.3 Reference』の付録 A「Directory Server Resource Kit File Reference」

表P-2 デフォルトのパス

プレースホルダ	説明	デフォルト値
<i>install-path</i>	Directory Server Enterprise Edition ソフトウェアのベースインストールディレクトリを表します。 ソフトウェアは、このベース <i>install-path</i> の下位のディレクトリにインストールされます。たとえば、Directory Server ソフトウェアは <i>install-path</i> /ds6/ にインストールされます。	<i>dsee_deploy(1M)</i> を使用して ZIP 形式の配布パッケージからインストールするとき、デフォルトの <i>install-path</i> は現在のディレクトリです。 <i>install-path</i> は、 <i>dsee_deploy</i> コマンドの <i>-i</i> オプションを使用して設定できます。Java Enterprise System インストーラを使用する場合など、ネイティブパッケージ配布からインストールする場合、デフォルトの <i>install-path</i> は次のいずれかの場所になります。 <ul style="list-style-type: none"> ■ Solaris システム - /opt/SUNWdsee/ ■ Red Hat システム - /opt/sun/ ■ Windows システム - C:\Program Files\Sun\JavaES5\DSEE
<i>instance-path</i>	Directory Proxy Server または Directory Server のインスタンスのフルパスを表します。 このマニュアルでは、Directory Server には /local/ds/ を、Directory Proxy Server には /local/dps/ を使用します。	デフォルトのパスはありません。ただしインスタンスのパスは、常にローカルファイルシステム上に存在します。 推奨されるディレクトリは次のとおりです。 /var (Solaris システム) /global (Sun Cluster を使用する場合)
<i>serverroot</i>	Identity Synchronization for Windows のインストール先の親ディレクトリを表します	インストールごとに異なります。Directory Server では、 <i>serverroot</i> の概念が存在しなくなったことに注意してください。
<i>isw-hostname</i>	Identity Synchronization for Windows インスタンスのディレクトリを表します	インストールごとに異なります
<i>/path/to/cert8.db</i>	Identity Synchronization for Windows でのクライアントの証明書データベースのデフォルトのパスおよびファイル名を表します	<i>current-working-dir</i> /cert8.db
<i>serverroot/isw-hostname/logs/</i>	システムマネージャー、各コネクタ、および Central Logger のログを Identity Synchronization for Windows がローカルに保存する場所のデフォルトパスを表します	インストールごとに異なります
<i>serverroot/isw-hostname/logs/central/</i>	Identity Synchronization for Windows センtralログのデフォルトパスを表します	インストールごとに異なります

コマンドの場所

次の表に、Directory Server Enterprise Edition のマニュアル内で使用されている各種コマンドの場所を示します。これらの各コマンドの詳細については、それぞれのマニュアルページを参照してください。

表 P-3 コマンドの場所

コマンド	Java ES ネイティブパッケージ配布	ZIP 形式の配布パッケージ
cacaoadm	Solaris - /usr/sbin/cacaoadm	Solaris - <i>install-path/dsee6/cacao_2/usr/sbin/cacaoadm</i>
	Red Hat - /opt/sun/cacao/bin/cacaoadm	Red Hat, HP-UX - <i>install-path/dsee6/cacao_2/cacao/bin/cacaoadm</i>
	Windows - <i>install-path\share\cacao_2\bin\cacaoadm.bat</i>	Windows - <i>install-path\dsee6\cacao_2\bin\cacaoadm.bat</i>
certutil	Solaris - /usr/sfw/bin/certutil	<i>install-path/dsee6/bin/certutil</i>
	Red Hat - /opt/sun/private/bin/certutil	
dpadm(1M)	<i>install-path/dps6/bin/dpadm</i>	<i>install-path/dps6/bin/dpadm</i>
dpconf(1M)	<i>install-path/dps6/bin/dpconf</i>	<i>install-path/dps6/bin/dpconf</i>
dsadm(1M)	<i>install-path/ds6/bin/dsadm</i>	<i>install-path/ds6/bin/dsadm</i>
dscmmon(1M)	<i>install-path/dscc6/bin/dscmmon</i>	<i>install-path/dscc6/bin/dscmmon</i>
dsccreg(1M)	<i>install-path/dscc6/bin/dsccreg</i>	<i>install-path/dscc6/bin/dsccreg</i>
dscsetup(1M)	<i>install-path/dscc6/bin/dscsetup</i>	<i>install-path/dscc6/bin/dscsetup</i>
dsconf(1M)	<i>install-path/ds6/bin/dsconf</i>	<i>install-path/ds6/bin/dsconf</i>
dsee_deploy(1M)	提供されていません	<i>install-path/dsee6/bin/dsee_deploy</i>
dsmig(1M)	<i>install-path/ds6/bin/dsmig</i>	<i>install-path/ds6/bin/dsmig</i>
entrycmp(1)	<i>install-path/ds6/bin/entrycmp</i>	<i>install-path/ds6/bin/entrycmp</i>
fildif(1)	<i>install-path/ds6/bin/fildif</i>	<i>install-path/ds6/bin/fildif</i>
idsktune(1M)	提供されていません	zip 形式の配布パッケージを解凍したディレクトリにあります
insync(1)	<i>install-path/ds6/bin/insync</i>	<i>install-path/ds6/bin/insync</i>

表 P-3 コマンドの場所 (続き)

コマンド	Java ES ネイティブパッケージ配布	ZIP 形式の配布パッケージ
<code>ns-accountstatus(1M)</code>	<code>install-path/ds6/bin/ns-accountstatus</code>	<code>install-path/ds6/bin/ns-accountstatus</code>
<code>ns-activate(1M)</code>	<code>install-path/ds6/bin/ns-activate</code>	<code>install-path/ds6/bin/ns-activate</code>
<code>ns-inactivate(1M)</code>	<code>install-path/ds6/bin/ns-inactivate</code>	<code>install-path/ds6/bin/ns-inactivate</code>
<code>repldisc(1)</code>	<code>install-path/ds6/bin/repldisc</code>	<code>install-path/ds6/bin/repldisc</code>
<code>schema_push(1M)</code>	<code>install-path/ds6/bin/schema_push</code>	<code>install-path/ds6/bin/schema_push</code>
<code>smcwebserver</code>	Solaris, Linux - <code>/usr/sbin/smcwebserver</code>	このコマンドは、ネイティブパッケージ配布を使用してインストールされる DSCC のみに関係します。
	Windows - <code>install-path\share\webconsole\bin\smcwebserver</code>	
<code>wcadmin</code>	Solaris, Linux - <code>/usr/sbin/wcadmin</code>	このコマンドは、ネイティブパッケージ配布を使用してインストールされる DSCC のみに関係します。
	Windows - <code>install-path\share\webconsole\bin\wcadmin</code>	

表記上の規則

このマニュアルでは、次のような字体や記号を特別な意味を持つものとして使用します。

表 P-4 表記上の規則

字体または記号	意味	例
<code>AaBbCc123</code>	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。	<code>.login</code> ファイルを編集します。 <code>ls -a</code> を使用してすべてのファイルを表示します。 <code>machine_name% you have mail.</code>
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します。	<code>machine_name% su</code> Password:
<i>aabbcc123</i>	変数を示します。実際に使用する特定の名称または値で置き換えます。	ファイルを削除するには、 <code>rm filename</code> と入力します。

表 P-4 表記上の規則 (続き)

字体または記号	意味	例
『』	参照する書名を示します。	『コードマネージャー・ユーザーズガイド』を参照してください。
「」	参照する章、節、ボタンやメニュー名、強調する単語を示します。	第5章「衝突の回避」を参照してください。 この操作ができるのは、「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	sun% grep '^#define \ XV_VERSION_STRING'

コード例は次のように表示されます。

- C シェル

```
machine_name% command y|n [filename]
```

- C シェルのスーパーユーザー

```
machine_name# command y|n [filename]
```

- Bourne シェルおよび Korn シェル

```
$ command y|n [filename]
```

- Bourne シェルおよび Korn シェルのスーパーユーザー

```
# command y|n [filename]
```

[] は省略可能な項目を示します。上記の例は、*filename* は省略してもよいことを示しています。

| は区切り文字 (セパレータ) です。この文字で分割されている引数のうち 1 つだけを指定します。

キーボードのキー名は英文で、頭文字を大文字で示します (例: Shift キーを押します)。ただし、キーボードによっては Enter キーが Return キーの動作をします。

ダッシュ (-) は 2 つのキーを同時に押すことを示します。たとえば、Ctrl-D は Control キーを押したまま D キーを押すことを意味します。

コマンド例のシェルプロンプト

次の表は、デフォルトのシステムプロンプトとスーパーユーザープロンプトを示しています。

表 P-5 \ 枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。

シェル	プロンプト
UNIX および Linux システムの C シェル	machine_name%
UNIX および Linux システムの C シェルのスーパーユーザー	machine_name#
UNIX および Linux システムの Bourne シェルおよび Korn シェル	\$
UNIX および Linux システムの Bourne シェルおよび Korn シェルのスーパーユーザー	#
Microsoft Windows のコマンド行	C:\

記号の規則

次の表は、この用語集で使用される記号の一覧です。

表 P-6 記号の規則

記号	説明	例	意味
[]	省略可能な引数やコマンドオプションが含まれます。	ls [-l]	-l オプションは必須ではありません。
{ }	必須のコマンドオプションの選択肢を囲みます。	-d {y n}	-d オプションには y 引数か n 引数のいずれかを使用する必要があります。
\${ }	変数参照を示します。	\${com.sun.javaRoot}	com.sun.javaRoot 変数の値を参照します。
-	同時に押すキーを示します。	Control-A	Control キーを押しながら A キーを押します。
+	順番に押すキーを示します。	Ctrl+A+N	Control キーを押してから放し、それに続くキーを押します。
→	グラフィカルユーザーインタフェースでのメニュー項目の選択順序を示します。	「ファイル」→「新規」 →「テンプレート」	「ファイル」メニューから「新規」を選択します。「新規」サブメニューから「テンプレート」を選択します。

マニュアル、サポート、およびトレーニング

Sunのサービス	URL	内容
マニュアル	http://jp.sun.com/documentation/	PDF 文書および HTML 文書をダウンロードできます。
サポートおよび トレーニング	http://jp.sun.com/supporttraining/	技術サポート、パッチのダウンロード、および Sun のトレーニングコース情報を提供します。

パート I

Directory Service Control Center、Directory Proxy Server、Directory Server、および Directory Server Resource Kit のインストール

次の章で構成されています。

- [第1章「Directory Server Enterprise Edition 6.3のインストール」](#)では、サポートされるシステムに Directory Service Control Center、Directory Proxy Server、Directory Server、および Directory Server Resource Kit をインストールする方法について説明します。
また、既存のソフトウェアインストールをアップグレードする詳細な手順についても説明します
- [第2章「Directory Server Enterprise Edition 6.3のアンインストール」](#)では、Directory Proxy Server、Directory Server、Directory Server Resource Kit、および Directory Service Control Center を削除する方法について説明します。
また、以前のソフトウェアインストールにダウングレードする詳細な手順についても説明します

Identity Synchronization for Windows ソフトウェアのインストールについては、[パート II 「Identity Synchronization for Windows のインストール」](#) を参照してください。

このガイドは、他の Java Enterprise System (Java ES) 製品とのインストールについては説明していません。Directory Server および Directory Service Control Center ソフトウェアを Java ES ソフトウェアとともにインストールしようとしている場合は、<http://docs.sun.com/coll/1286.3> にある Java ES ソフトウェアのインストールの説明をお読みください。

このガイドは Directory Editor ソフトウェアのインストールについては説明していません。Directory Editor ソフトウェアのインストールを計画している場合は、まず、『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』の「Directory Editor の既知の問題点と制限事項」をお読みください。その後、『Sun Java System Directory Editor 1 2005Q1 Installation and Configuration Guide』のインストールの説明をお読みください。

必ず『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』の第 6 章「Directory Editor の修正されたバグと既知の問題点」もお読みください。

Directory Server Enterprise Edition 6.3 のインストール

この章では、Directory Server Enterprise Edition 6.3 ソフトウェアのインストールについて説明します。

この章の内容は次のとおりです。

- 25 ページの「[インストール手順のクイックリファレンス](#)」では、Directory Server Enterprise Edition 6.3 をインストールまたはアップグレードする必要条件の詳細について説明します。
- 27 ページの「[ソフトウェアのインストール](#)」では、Directory Server Enterprise Edition ソフトウェアをインストールする詳細な手順について説明します。また、Directory Server Enterprise Edition 6.0、6.1、および 6.2 インストールをアップグレードする詳細な手順についても説明します。
- 64 ページの「[サーバーインスタンスの作成](#)」では、ソフトウェアのインストール後にサーバーインスタンスを作成する詳細な手順について説明します。
- 77 ページの「[Solaris 10 システムで Sun 暗号化フレームワークを使用する](#)」では、SSL ハードウェアアクセラレーションを使用する配備の手順について説明します。

この章の最後では、インストールしたソフトウェアが想定どおりに動作することを検証します。そのあとに、『[Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド](#)』で説明されているとおりのソフトウェアの構成に進むことができます。

インストール手順のクイックリファレンス

この節では、Directory Server Enterprise Edition 6.3 をインストールまたはアップグレードする必要条件の詳細について説明します。

次の表から、現在のインストールおよびインストールに使用している配布のタイプを基に、Directory Server Enterprise Edition 6.3 のインストールまたはアップグレードに関連する情報に直接アクセスできます。

以前の Directory Server Enterprise Edition バージョン	ソフトウェア配布	関連情報
なし、または 5.x	ネイティブ (Solaris および Linux)	<p>次の順序で情報を確認します。</p> <ol style="list-style-type: none"> 27 ページの「ソフトウェアのインストール」を参照して、Directory Server Enterprise Edition 6.2 をインストールします。 42 ページの「ネイティブパッケージを使用して Directory Server Enterprise Edition をアップグレードする」を参照して、バージョン 6.3 にアップグレードします。 <p>5.x を使用している場合は、Directory Server インスタンスを 6.3 に移行する必要があります。『Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide』を参照してください。</p>
なし、または 5.x	ネイティブ (Windows)	<p>次の順序で情報を確認します。</p> <ol style="list-style-type: none"> 『Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide』を参照して、Directory Server Enterprise Edition 6.0 をインストールします。 42 ページの「ネイティブパッケージを使用して Directory Server Enterprise Edition をアップグレードする」を参照して、バージョン 6.3 にアップグレードします。 <p>5.x を使用している場合は、Directory Server インスタンスを 6.3 に移行する必要があります。『Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide』を参照してください。</p>

以前の Directory Server Enterprise Edition バージョン	ソフトウェア配布	関連情報
なし、または 5.x	ZIP	<p>45 ページの「ZIP 形式の配布から Directory Server Enterprise Edition 6.3 をインストールする」を参照して、Directory Server Enterprise Edition 6.3 をインストールします。</p> <p>51 ページの「ZIP 形式の配布から Directory Service Control Center をインストールする」も参照してください</p> <p>5.x を使用している場合は、Directory Server インスタンスを 6.3 に移行する必要があります。『Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide』を参照してください。</p>
6.0、6.1、または 6.2	ネイティブ	<p>42 ページの「ネイティブパッケージを使用して Directory Server Enterprise Edition をアップグレードする」を参照して、バージョン 6.3 にアップグレードします。</p>
6.0、6.1、または 6.2	ZIP	<p>45 ページの「ZIP 形式の配布から Directory Server Enterprise Edition 6.3 をインストールする」を参照して、Directory Server Enterprise Edition 6.3 をインストールします。</p> <p>51 ページの「ZIP 形式の配布から Directory Service Control Center をインストールする」も参照してください</p>

ソフトウェアのインストール

この節では、基本的なインストールについて説明します。サーバーソフトウェアをインストールしたら、サーバーインスタンスの作成手順について、64 ページの「サーバーインスタンスの作成」を参照してください。

- 28 ページの「ネイティブパッケージを使用して Directory Server Enterprise Edition をインストールする」
- 45 ページの「ZIP 形式の配布を使用して Directory Server Enterprise Edition をインストールする」
- 55 ページの「Directory Service Control Center を使い始める」

インストールに進む前に、『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』の「オペレーティングシステムの要件」を確認してください

このガイドでは、Directory Editor ソフトウェアのインストールについては説明しません。Directory Editor ソフトウェアをインストールする場合は、『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』の「Directory Editor の既知の問題点と制限事項」を先に読んでから『Sun Java System Directory Editor 1 2005Q1 Installation and Configuration Guide』に記載のインストール手順を確認してください。

Directory Server Enterprise Edition は、フランス語、ドイツ語、スペイン語、日本語、韓国語、簡体字中国語、繁体字中国語でインストールすることもできます。多言語パッケージのインストール手順については、以降の節で必要に応じて説明します。

ネイティブパッケージを使用して Directory Server Enterprise Edition をインストールする

ネイティブパッケージを使用して Directory Server Enterprise Edition 6.3 をインストールするには、コンピュータに 6.0、6.1、または 6.2 がインストールされている状態で 6.3 にアップグレードしてください。Directory Server Enterprise Edition 6.3 を正常にインストールするには、次の手順を参照してください。

1. Directory Server Enterprise Edition 6.0、6.1、または 6.2 をインストールします。このガイドでは、Directory Server Enterprise Edition 6.2 の場合のインストール手順を示します。

Windows の場合は、Directory Server Enterprise Edition 6.2 を直接インストールすることができないため、バージョン 6.0 をインストールしてから 6.3 に直接アップグレードします。

2. Directory Server Enterprise Edition 6.3 に正常にアップグレードするために、すべての共有コンポーネントをアップグレードします。詳細は、39 ページの「パッチを使用して共有コンポーネントをアップグレードする」を参照してください。
3. 42 ページの「ネイティブパッケージを使用して Directory Server Enterprise Edition をアップグレードする」で説明されている各パッチを適用して Directory Server Enterprise Edition インストールを 6.3 にアップグレードします。

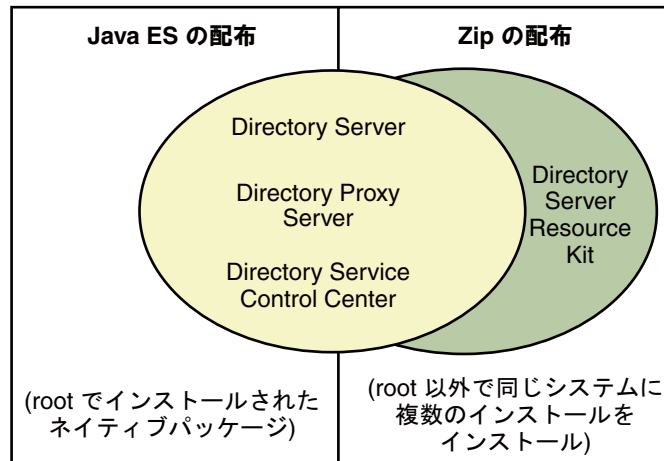
Directory Service Control Center、Directory Server、および Directory Proxy Server は同じホストにインストールできますが、以降の手順では、これら 3 つのコンポーネントが別々のコンピュータにインストールされているものとします。3 つのコンポーネントすべてを同じコンピュータにインストールする場合は、以降の手順で示されるコンポーネントの選択画面で、3 つのコンポーネントすべてをインストール対象として選択してください。

▼ ネイティブパッケージから Directory Server のみをインストールする

この手順では、Directory Server をネイティブパッケージからインストールする方法について説明します。この手順を実行するには、root である必要があります。

注 - Directory Service Control Center をインストール済みの場合は、Directory Server がネイティブパッケージから自動的にインストールされています。DSCC と一緒にインストールされた Directory Server ソフトウェアを使用して、システムに独自の追加 Directory Server インスタンスを作成できます。

始める前に このインストール用に、次の図に示す Java Enterprise System Update 1 配布を入手します。

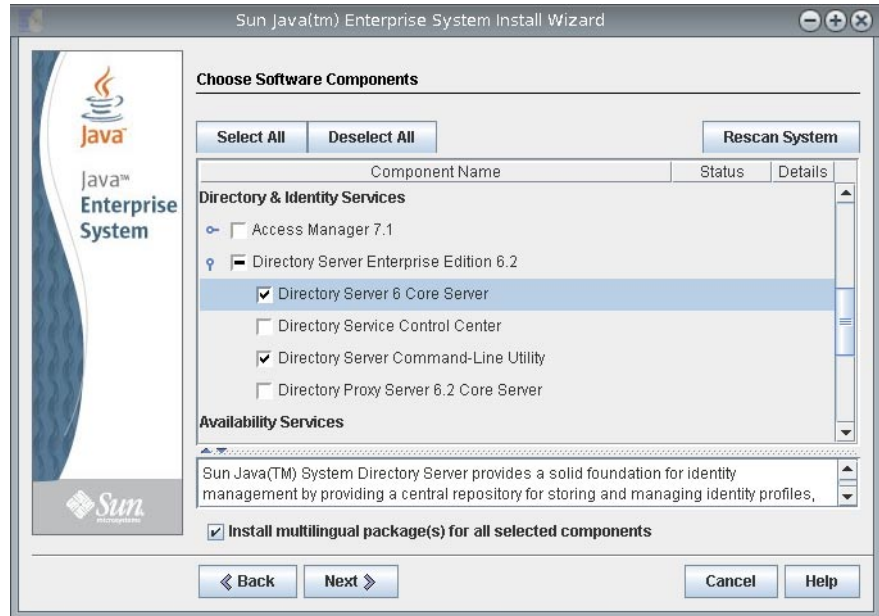


インストールに必要なすべての情報を次のワークシートに記入します。

必須情報	ヒント	解答
Directory Server のインストール先システムの完全修飾されたホスト名	例: ds.example.com	
(省略可能) Directory Service Control Center からアクセスするための cacao 共通エージェントコンテナのポート番号	デフォルト: 11162	

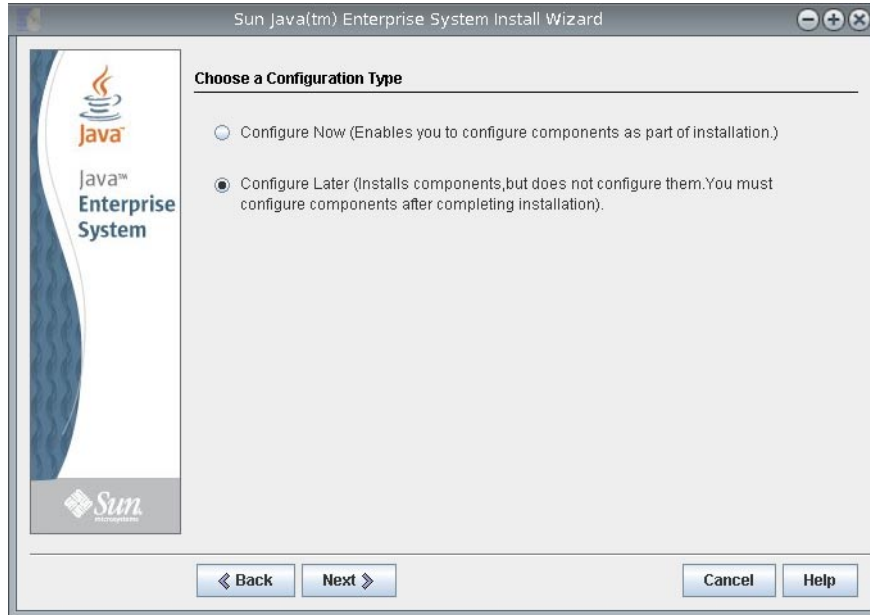
必須情報	ヒント	解答
Directory Server インスタンスの作成先のファイルシステムパス	例: /local/ds/ インスタンスを作成できるのはローカルファイルシステム上のみです。NFSなどのネットワークマウントのファイルシステム上に作成しないでください。 各パスは、以後 <i>instance-path</i> と呼ばれます。	
LDAP ポート番号	デフォルト: root でインストールする場合は 389、root 以外でインストールする場合は 1389	
LDAP/SSL ポート番号	デフォルト: root でインストールする場合は 636、root 以外でインストールする場合は 1636	
ディレクトリマネージャー DN	デフォルト: cn=Directory Manager	
ディレクトリマネージャーのパスワード	8 文字以上の長さが必要	
ベースサフィックス DN	例: dc=example,dc=com	
(UNIX システム) サーバーユーザー (uid)	例: noaccess	
(UNIX システム) サーバークループ (gid)	例: noaccess	

- 1 使用しているプラットフォームに必要なパッチまたはサービスパックをインストールします。
『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』の「オペレーティングシステムの要件」を参照してください。
- 2 **Java Enterprise System** の配布を使用して、**Java ES** インストーラを root として実行します。
root# `./installer`
- 3 **Directory Server** コンポーネントをインストール対象として選択します。



多言語パッケージをインストールしない場合は、「選択したすべてのコンポーネントに多言語パッケージをインストール」チェックボックスを選択解除します。

- 4 ソフトウェアを6.3にアップグレードするため、あとで設定することを選択します。

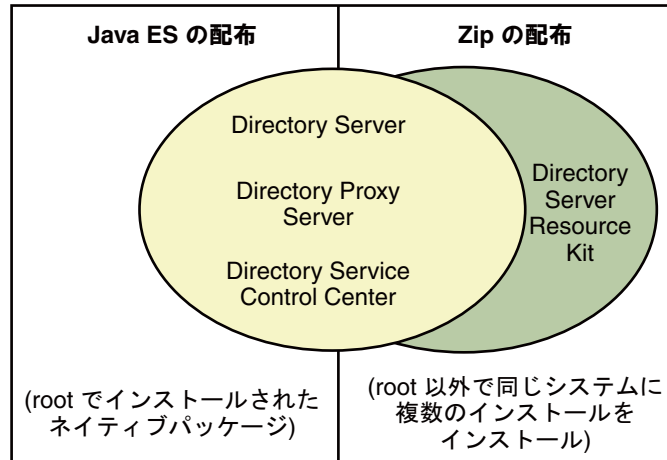


5 Java ES インストーラによるインストール作業を完了します。

▼ ネイティブパッケージから **Directory Proxy Server** のみをインストールする

この手順では、Directory Proxy Server をネイティブパッケージからインストールする方法について説明します。この手順を実行するには、root である必要があります。

始める前に このインストール用に、次の図に示す Java Enterprise System Update 1 配布を入手します。

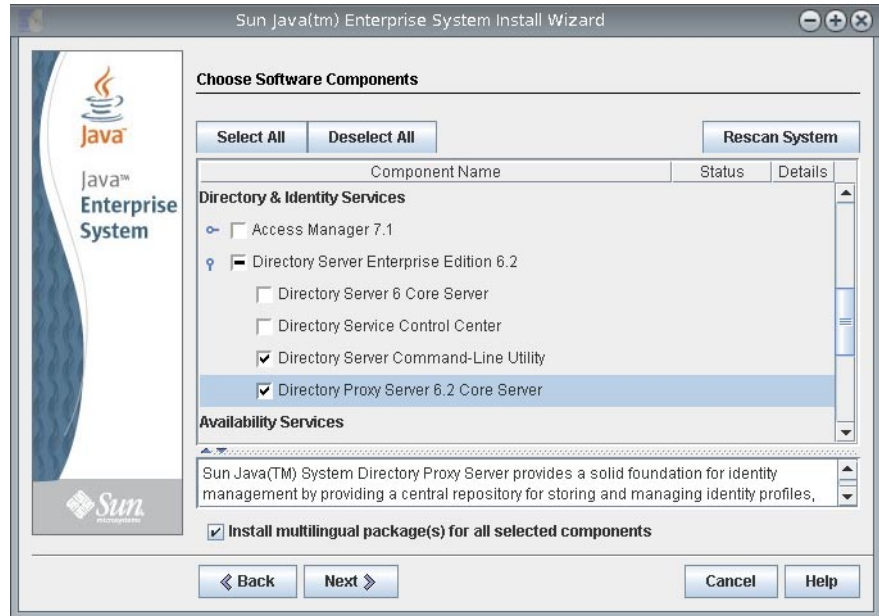


インストールに必要なすべての情報を次のワークシートに記入します。

必須情報	ヒント	解答
Directory Proxy Server のインストール先システムの完全修飾されたホスト名	例: dps.example.com	
(省略可能) Directory Service Control Center からアクセスするための cacao 共通エージェントコンテナのポート番号	デフォルト: 11162	
Directory Proxy Server インスタンスの作成先のファイルシステムパス	例: /local/dps/ インスタンスを作成できるのはローカルファイルシステム上のみです。NFSなどのネットワークマウントのファイルシステム上に作成しないでください。 各パスは、以後 <i>instance-path</i> と呼ばれます。	
LDAP ポート番号	デフォルト: root でインストールする場合は 389、root 以外でインストールする場合は 1389	

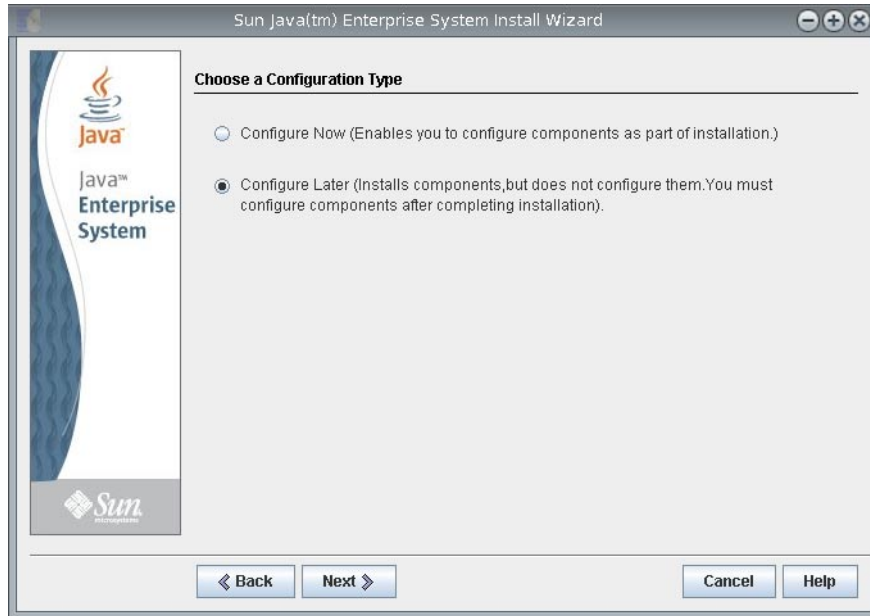
必須情報	ヒント	解答
LDAP/SSL ポート番号	デフォルト: root でインストールする場合は 636、root 以外でインストールする場合は 1636	
ディレクトリプロキシマネージャ DN	デフォルト: cn=Proxy Manager	
ディレクトリプロキシマネージャのパスワード	8 文字以上の長さが必要	
(UNIX プラットフォーム) サーバーユーザー (uid)	例: noaccess	
(UNIX プラットフォーム) ユーザーグループ (gid)	例: noaccess	
(省略可能) 各サーバーがプロキシを通してアクセスするための接続情報	例: ds1.example.com:1389、 ds2.example.com:1636	

- 1 使用しているプラットフォームに必要なパッチまたはサービスパックをインストールします。
『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』の「オペレーティングシステムの要件」を参照してください。
- 2 **Java Enterprise System** の配布を使用して、**Java ES** インストーラを root として実行します。
root# ./installer
- 3 **Directory Proxy Server** コンポーネントをインストール対象として選択します。



多言語パッケージをインストールしない場合は、「選択したすべてのコンポーネントに多言語パッケージをインストール」チェックボックスを選択解除します。

- 4 ソフトウェアを6.3にアップグレードするため、あとで設定することを選択します。



5 Java ES インストーラによるインストール作業を完了します。

▼ ネイティブパッケージから **Directory Service Control Center** をインストールする

この手順では、Directory Service Control Center (DSCC) およびリモート管理コマンド行ツールをインストールする方法について説明します。

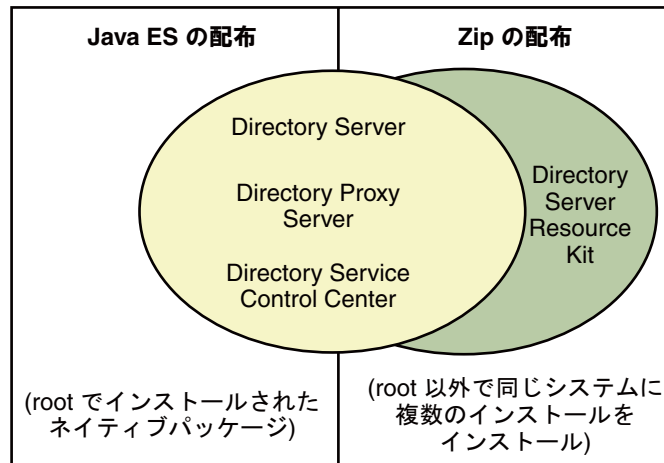
この手順を実行するには、root である必要があります。

また、ソフトウェアパッケージに付属の WAR ファイルを配備することで、ZIP 形式の配布を使用して Directory Service Control Center をインストールすることもできます。詳細は、51 ページの「ZIP 形式の配布から Directory Service Control Center をインストールする」を参照してください。

DSCC をインストールする場合は、Directory Server がネイティブパッケージから自動的にインストールされます。DSCC では、専用の Directory Server ローカルインスタンスを使用して、ディレクトリサービス設定に関する情報を格納します。このインスタンスは、DSCC レジストリと呼ばれます。

DSCC と一緒にインストールされた Directory Server ソフトウェアを使用して、システムに独自の追加 Directory Server インスタンスを作成できます。

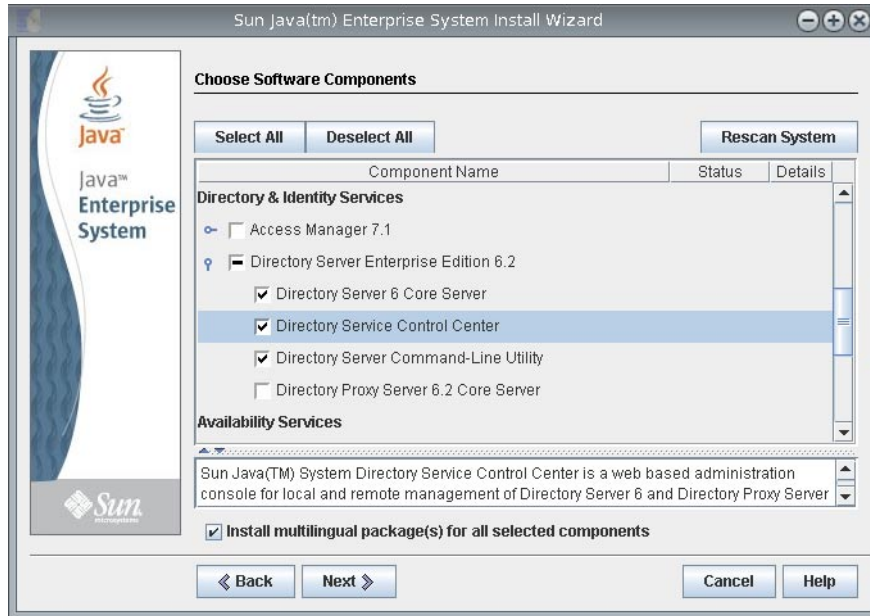
始める前に このインストール用に、次の図に示す Java Enterprise System Update 1 配布を入手します。



インストールに必要なすべての情報を次のワークシートに記入します。

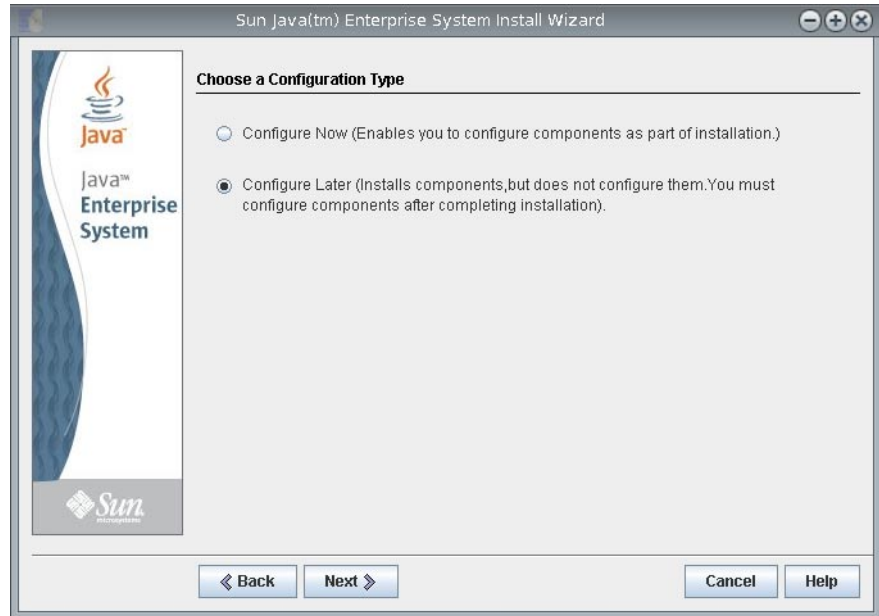
必要な情報	ヒント	実際の設定値
DSCC をインストールするシステムのホスト名		
システムの root パスワード		
Java Web コンソール URL	デフォルト: https://hostname:6789	
Directory Service Manager パスワード		

- 1 使用しているプラットフォームに必要なパッチまたはサービスパックをインストールします。
『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』の「オペレーティングシステムの要件」を参照してください。
- 2 **Java Enterprise System** 配布を使用して、**Java ES** インストーラを root として実行します。
./installer
- 3 **Directory Service Control Center** コンポーネントをインストール対象として選択します。



多言語パッケージをインストールしない場合は、「選択したすべてのコンポーネントに多言語パッケージをインストール」チェックボックスを選択解除します。

- 4 ソフトウェアを6.3にアップグレードするため、あとで設定することを選択します。



- 5 Java ES インストーラによるインストール作業を完了します。
ネイティブパッケージがシステムにインストールされます。
- 6 55 ページの「[Directory Service Control Center を使い始める](#)」を参照してください。

▼ パッチを使用して共有コンポーネントをアップグレードする

始める前に ネイティブパッケージを使用して Directory Server Enterprise Edition を 6.3 にアップグレードする前に、共有コンポーネントをアップグレードします。この手順を実行するには、root である必要があります。

パッチを使用すると、Solaris、Linux、および Windows 上の共有コンポーネントをアップグレードできます。Linux でパッチをインストールするには、利用可能な場合は `installpatch` を使用します。

要件に従ってプラットフォームを選択し、そのプラットフォーム用に指定されたすべてのパッチをインストールします。新しいパッチバージョンが利用可能になった場合は、表に示すバージョンではなく新しいバージョンを使用してください。

説明	Solaris 10 SPARC および Solaris 9 SPARC	Solaris 10 x86、AMD x64、および Solaris 9 x86	Linux
ICU (International Components for Unicode)	119810-04 (Solaris 10) 114677-14 (Solaris 9)	119811-04 (Solaris 10) 114678-14 (Solaris 9)	126368-03
Sun Java Web Console (SJWC)	125952-05 (Solaris 10) 125950-05 (Solaris 9)	125953-05 (Solaris 10) 125951-05 (Solaris 9)	125954-05
ネットワークセキュリティサービス/Netscape ポータブルランタイム/Java Security Services (NSS/NSPR/JSS)	詳細なパッチ情報については、後述の表を参照してください。	詳細なパッチ情報については、後述の表を参照してください。	121656-14
Java Dynamic Management™ Kit Runtime	119044-03	119044-03	119046-03
共通エージェントコンテナランタイム	123893-04	123896-04	123899-03
Sun Java Monitoring Framework (MFWK)	125444-11	125446-11 (Solaris 10 64 ビットおよび Solaris 10 32 ビット) 125445-11 (Solaris 10 32 ビットおよび Solaris 9 32 ビット)	125447-11

使用しているシステムの SUNWpr および SUNWtls のパッケージバージョンを取得して、適切な NSS/NSPR/JSS パッチを選択します。

```
# pkginfo -l SUNWpr | grep VERSION
# pkginfo -l SUNWtls | grep VERSION
```

次に、次の表から適切なパッチシリーズを選択します。

Solaris	パッケージバージョン	ネットワークセキュリティサービス/Netscape ポータブルランタイム/Java Security Services (NSS/NSPR/JSS) のパッチ
Solaris 9 SPARC	SUNWpr: VERSION=4.1.2,REV=2002.09.03.00.17 SUNWtls: VERSION=3.3.2,REV=2002.09.18.12.49	119211-14

Solaris	パッケージバージョン	ネットワークセキュリティーサービス/Netscape ポータブルランタイム/Java Security Services (NSS/NSPR/JSS) のパッチ
Solaris 9 x86	SUNWpr: VERSION=4.1.3,REV=2003.01.09.13.59 SUNWtls: VERSION=3.3.3,REV=2003.01.09.17.07	119212-14
Solaris 10 SPARC	SUNWpr: VERSION=4.5.1,REV=2004.11.05.02.30 SUNWtls: VERSION=3.9.5,REV=2005.01.14.17.27	119213-14
Solaris 10 x86	SUNWpr: VERSION=4.5.1,REV=2004.11.05.03.44 SUNWtls: VERSION=3.9.5,REV=2005.01.14.19.03	119214-14
Solaris 9 SPARC および Solaris 10 SPARC	SUNWpr: VERSION=4.6.4,REV=2006.11.16.20.40 SUNWtls: VERSION=3.11.4,REV=2006.11.16.20.40	125358-03
Solaris 9 x86 および Solaris 10 x86	SUNWpr: VERSION=4.6.4,REV=2006.11.16.21.41 SUNWtls: VERSION=3.11.4,REV=2006.11.16.21.41	125359-03

Windows の場合、共通エージェントコンテナランタイム共有コンポーネントをアップグレードする前に、次のコマンドを実行します。

```
cacaoadm.exe prepare-uninstall
```

説明	Windows
Windows Installer パッチ	126910-02
Sun Java Web Console (SJWC)	125955-05
ネットワークセキュリティーサービス/Netscape ポータブルランタイム/Java Security Services (NSS/NSPR/JSS)	125923-03
共通エージェントコンテナランタイム	126183-04

説明	Windows
Sun Java Monitoring Framework (MFWK)	125449-09

Directory Server Enterprise Edition 6.2 を 6.3 にアップグレードする前に、共通エージェントコンテナ共有コンポーネントのみをアップグレードします。

- 1 共有コンポーネントを使用しているすべてのプロセスを終了します。
- 2 該当する場合は、共有コンポーネントを終了します。
- 3 前述の表に示す最新のアップグレードパッチを入手します。
パッチを入手する方法の詳細は、『[Sun Java System Directory Server Enterprise Edition 6.3 リリースノート](#)』の「ソフトウェアの入手」を参照してください。
- 4 共有コンポーネントの適切なパッチを適用します。
パッチをインストールする手順の詳細は、README.patchID ファイルを参照してください。
- 5 パッチのアップグレードが成功したことを確認します。
確認手順については、README.patchID ファイルを参照してください。
- 6 該当する場合は、共有コンポーネントを再起動します。

▼ ネイティブパッケージを使用して Directory Server Enterprise Edition をアップグレードする

始める前に すべての共有コンポーネントが最新であることを確認します。詳細は、[39 ページ](#)の「パッチを使用して共有コンポーネントをアップグレードする」を参照してください。

すでに Directory Server Enterprise Edition 6.0、6.1、または 6.2 がインストールされている場合は、次の手順でバージョン 6.3 にアップグレードします。

これらの手順を実行するには、root である必要があります。

Directory Server Enterprise Edition のアップグレードを終えても、Directory Server インスタンス、Directory Proxy Server インスタンス、および設定情報はすべて影響を受けません。

さまざまなプラットフォームで Directory Server Enterprise Edition をアップグレードするのに必要なパッチ番号を次の表に示します。新しいパッチバージョンが利用可能になった場合は、表に示すバージョンではなく新しいバージョンを使用してください。

説明	Directory Server Enterprise Edition コア	Directory Server Enterprise Edition ローカライゼーション
パッチ ID: Solaris SPARC	125276-07	125937-06
パッチ ID: Solaris 9 x86	125277-07	125938-06
パッチ ID: Solaris 10 x86 または AMD x64	125278-07	125938-06
パッチ ID: Linux	125309-07	125939-06
パッチ ID: Windows	125311-07	125311-07
Windows 用の Directory Server Enterprise Edition 6.1 パッチは提供されませんでした。そのため、このパッチは 6.1 インストールのアップグレードに適用されません。		

注 - ローカライズされた Directory Server Enterprise Edition を正常に動作させるために、コアのパッチをインストールする前にローカライズされたパッチをインストールしてください。

各ローカライゼーションパッチには、選択したプラットフォームでサポートされるすべての言語が含まれます。

1 DSCC レジストリを停止します。

■ Solaris の場合

```
# dsadm stop /var/opt/SUNWdsee/dscc6/dcc/ads
```

■ Linux の場合

```
# dsadm stop /var/opt/sun/dscc6/dcc/ads
```

■ Windows の場合

```
dsadm.exe stop C:\Program Files\Sun\JavaES5\DSEE\var\dscc6\dcc\ads
```

2 Directory Server および Directory Proxy Server の実行中のインスタンスをすべて停止します。

3 共有コンポーネントをアップグレードします。39 ページの「パッチを使用して共有コンポーネントをアップグレードする」を参照してください。

- 4 **Directory Server Enterprise Edition 6.3** パッチをダウンロードします。
詳細は、『[Sun Java System Directory Server Enterprise Edition 6.3 リリースノート](#)』の「ソフトウェアの入手」を参照してください。
- 5 パッチを保存したディレクトリに移動します。
- 6 次のコマンドを実行してパッチをインストールします。
 - Solaris OS
Directory Server Enterprise Edition をアップグレードする前に、119254-38 (Solaris 10 SPARC の場合) または 119255-38 (Solaris 10 x86 の場合) をインストールします。
パッチのダウンロードについては、『[Sun Java System Directory Server Enterprise Edition 6.3 リリースノート](#)』の「ソフトウェアの入手」を参照してください。
または、Directory Server Enterprise Edition アップグレードパッチの適用時に、Solaris 10 SPARC および Solaris 10 x86 で `patchadd` コマンドに `-G` を指定して実行します。
例: `# patchadd -G patch-id`
ほかの Solaris OS の場合は、次のコマンドを使用します。
`# patchadd patch-id`
 - Linux
 - a. `installpatch` ファイルの存在するディレクトリを開きます。
 - b. `installpatch` を実行します。

`# ./installpatch`
インストール中に `installpatch` でエラーが表示されたら、エラーを解決してパッチを再インストールしてください。
 - Windows
 - a. `patch-id.exe` 実行可能ファイルの存在するフォルダを開きます。
 - b. `patch-id.exe` をダブルクリックします。

ローカライズ版のパッチは、ベースパッチに同梱されています。
パッチのインストールに成功したら、次のコマンドを実行します。

`# dscsetup console-unreg`
`# dscsetup console-reg`
- 7 必要に応じて **Directory Server** インスタンスおよび **Directory Proxy Server** インスタンスを起動します。
- 8 **DSCC** レジストリを再起動します。

- Solaris の場合

```
# dsadm start /var/opt/SUNWdsee/dscc6/dcc/ads
```

- Linux の場合

```
# dsadm start /var/opt/sun/dscc6/dcc/ads
```

- Windows の場合

```
dsadm.exe start C:\Program Files\Sun\JavaES5\DSEE\var\dscc6\dcc\ads
```

次の手順 ソフトウェアのインストール後に、[63 ページの「環境変数」](#)を参照してください。

ZIP 形式の配布を使用して Directory Server Enterprise Edition をインストールする

インストールプロセス中に、Directory Server Enterprise Edition がコンピュータにすでにインストールされていることが `dsee_deploy` によって検出された場合は、以前のインストールが自動的にアップグレードされます。Directory Server Enterprise Edition インストールディレクトリが存在する場合は Directory Server Enterprise Edition 6.3 にアップグレードする前にバックアップします。あとで以前の Directory Server Enterprise Edition インストールを復元することはできません。

Directory Server Enterprise Edition 6.3 の ZIP バージョンにより、Directory Server Enterprise Edition の以前の部分インストールはすべて削除されます。

ZIP 形式の配布は、`root` 以外のユーザーとしてインストールできます。

▼ ZIP 形式の配布から Directory Server Enterprise Edition 6.3 をインストールする

始める前に **SuSE Linux** の場合:

- Directory Server Enterprise Edition for SuSE Linux は、ZIP 形式の配布でのみ利用できません。Identity Synchronization for Windows および Directory Editor コンポーネントはサポートされません。
- SuSE Linux 9 の場合、システムに SP4 がインストールされている必要があります。SuSE Linux 9 コンピュータに SP4 がインストールされていない場合は、オペレーティングシステムをアップグレードしてください。次のいずれかの手順で Directory Server Enterprise Edition をインストールできます。
 - この節での説明に従って、Directory Server Enterprise Edition 6.3 の ZIP 形式の配布を SuSE Linux 9 SP4 システムに直接インストールします。

- 以前の Directory Server Enterprise Edition 6.2 の ZIP 形式のインストールをアップグレードします。Directory Server Enterprise Edition 6.2 では SuSE Linux SP3 のみがサポートされるため、Directory Server Enterprise Edition を 6.3 にアップグレードする前に、オペレーティングシステムを SuSE Linux SP4 にアップグレードします。詳細は、54 ページの「ZIP 形式の配布から Directory Server Enterprise Edition をアップグレードする」の節を参照してください。
- SuSE 64 ビットの場合、cacao が起動するには .pam-32bit-9-yyyyymmddhhmm.rpm がが必要です。システムにまだインストールされていない場合は、インストールしてください。
- SuSE Linux Enterprise Server の /etc/profile.d/ には、インストールされたソフトウェアに応じて適切な環境を自動的に設定する、一連のスクリプトがあります。したがって、コマンドを使用して製品を動作させる前に、次の Java 環境変数を空にリセットします。
 - JAVA_BINDIR
 - JAVA_HOME
 - JRE_HOME
 - JAVA_ROOT

HP-UX の場合:

- コンピュータに HP-UX 11.23 がインストールされている必要があります。インストールされていない場合は、オペレーティングシステムをアップグレードしてください。次のいずれかの手順で Directory Server Enterprise Edition をインストールできます。
 - この節での説明に従って、Directory Server Enterprise Edition 6.3 の ZIP 形式の配布を HP-UX 11.23 システムに直接インストールします。
 - 以前の Directory Server Enterprise Edition 6.0 または 6.1 の ZIP 形式のインストールをアップグレードします。Directory Server Enterprise Edition 6.0 および 6.1 では HP-UX 11.11 のみがサポートされるため Directory Server Enterprise Edition を 6.3 にアップグレードする前に、オペレーティングシステムを HP-UX 11.23 にアップグレードしてください。詳細は、54 ページの「ZIP 形式の配布から Directory Server Enterprise Edition をアップグレードする」の節を参照してください。

ZIP 形式の配布でのパッチの表

使用しているシステムに適した ZIP 形式のパッチに関する情報については、次の表を参照してください。新しいパッチバージョンが利用可能になった場合は、表に示すバージョンではなく新しいバージョンを使用してください。

オペレーティングシステム	パッチ番号
Solaris SPARC	126748-04
Solaris 9 x86	126749-04
Solaris 10 x86 および AMD x64	126750-04
Red Hat Linux	126751-04
SuSE Linux	126751-04
HP-UX	126752-04
Windows	126753-04

すべての多言語ファイルが上記のパッチに含まれています。

インストールを開始する前に、次のワークシートに記入します。

必要な情報	ヒント	実際の設定値
次の項目をインストールするシステムの完全修飾ホスト名	例:	
<ul style="list-style-type: none"> ■ Directory Server ■ Directory Proxy Server 	<ul style="list-style-type: none"> ■ ds.example.com ■ dps.example.com 	
(省略可能) Directory Service Control Centerからのアクセスに使用する共通エージェントコンテナのポート番号	デフォルト: 11162	
次の項目のインスタンスを作成するファイルシステムのパス	例:	
<ul style="list-style-type: none"> ■ Directory Server ■ Directory Proxy Server 	<ul style="list-style-type: none"> ■ /local/ds/ ■ /local/dps/ 	
	<p>インスタンスを作成できるのはローカルファイルシステム上のみです。NFSなどのネットワークマウントのファイルシステム上に作成しないでください。</p> <p>各パスは、以後 <i>instance-path</i> と呼ばれます。</p>	

必要な情報	ヒント	実際の設定値
LDAP ポート番号	デフォルト: root でインストールする場合は 389、root 以外でインストールする場合は 1389	
LDAP または SSL のポート番号	デフォルト: root でインストールする場合は 636、root 以外でインストールする場合は 1636	
ディレクトリマネージャー DN	デフォルト: cn=Directory Manager	
ディレクトリプロキシマネージャー DN	デフォルト: cn=Proxy Manager	
ディレクトリマネージャーのパスワード	8 文字以上を指定します	
ディレクトリプロキシマネージャーのパスワード	8 文字以上を指定します	
ベースサフィックス DN	例: dc=example,dc=com	
(UNIX システム) サーバーユーザー (uid)	例: noaccess	
(UNIX システム) サーバークループ (gid)	例: noaccess	
(省略可能) 各サーバーがプロキシ経由でアクセスするための接続情報	例: ds1.example.com:1389, ds2.example.com:1636	

デフォルトで、ZIP 形式のインストールの場合のユーザーおよびグループ ID は、インストールを実行するユーザーの ID になります。

- 1 このインストール用に ZIP 形式の配布を入手します。
- 2 使用しているプラットフォームで必要なパッチまたはサービスパックをインストールします。
『Sun Java System Directory Server Enterprise Edition 6.3 リリースノート』の「オペレーティングシステムの要件」を参照してください。

- 3 `dsee_deploy` コマンドを含む ZIP 配布ディレクトリに変更します。
- 4 `dsee_deploy(1M)` コマンドを使用し、ソフトウェアをインストールします。

```
$ ./dsee_deploy install -i install-path options
```


Windows の場合は、`dsee_deploy` コマンドが格納されている ZIP 形式の配布のフォルダを参照し、次のコマンドを実行します。

```
dsee_deploy install -i install-path options
```

たとえば、次のコマンドを実行すると、`/local` ディレクトリにコンポーネントがインストールされます。このとき、このディレクトリに対して書き込みアクセス権を持っていることが前提となります。

```
$ ./dsee_deploy install -i /local
```

`--no-inter` オプションを使用して、非対話モードでインストールすることもできます。この場合、確認なしでライセンスを受諾します。非対話モードは、サイレントインストールを行う場合に特に便利です。

この手順によって、共通エージェントコンテナ、`cacao`、およびローカルの Directory Service Control Center エージェントがインストールされるので、DSCC を使用してサーバーインスタンスを作成できるようになります。以前のコマンドは、デフォルトのポート、`11162` を使用して共通エージェントコンテナをインストールしていない場合のみ正しく動作します。

以前に同じシステム上に DSCC をインストールしている場合、デフォルトポートを使用する共通エージェントコンテナがすでにインストールされています。`-p` オプションを使用して別のポートを指定します。

```
$ ./dsee_deploy install -i /local -p 11169
```

インストールプロセス中に、WAR ファイルがシステムに保存されます。WAR ファイルには、アプリケーションサーバーで配備されたときに Web コンソールを使用したサーバーインスタンスへのアクセスおよび管理を可能にする、DSCC Web アプリケーションが格納されています。機能は、ネイティブパッケージの場合の DSCC と似ています。WAR ファイルの詳細は、[51 ページの「ZIP 形式の配布から Directory Service Control Center をインストールする」](#)を参照してください。

インストールプロセス中に、多言語パッケージもインストールされます。

5 (省略可能) ディレクトリ内のサンプルデータをロードします。

コマンド行ツールを使用するサンプルは、使用しているディレクトリの `dc=example,dc=com` サフィックスに存在するサンプルデータを使用します。

`dc=example,dc=com` サフィックスを作成することで、必要なデータの一部を設定できます。これで、サフィックスに `ds6/ldif/Example.ldif` ファイルのエントリを設定できます。

a. 新しい Directory Server インスタンスを作成して、インスタンスを起動します。

```
$ dsadm create -p port -P SSL-port instance-path
$ dsadm start instance-path
```

- b. Example.ldif ファイルで、サンプルに必要なバインドパスワードを確認します。
- c. 次のコマンドを実行し、サフィックスを作成して Example.ldif の内容をディレクトリにロードします。

```
$ dsconf create-suffix -h localhost -p 1389 dc=example,dc=com
$ dsconf import -h localhost -p 1389 install-path/ds6/ldif/Example.ldif \
dc=example,dc=com
```

詳細は、67 ページの「コマンド行から Directory Server インスタンスを作成する」を参照してください。

- d. **makeldif(1)** コマンドと次のテンプレートを使用して、サンプル用のテストデータを生成します。

```
define suffix=dc=example,dc=com
define maildomain=example.com

branch: ou=test,[suffix]
subordinateTemplate: person:100

template: person
rdnAttr: uid
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
givenName: <first>
sn: <last>
cn: {givenName} {sn}
initials: {givenName:1}{sn:1}
employeeNumber: <sequential>
uid: test{employeeNumber}
mail: {uid}@{maildomain}
userPassword: auth{employeeNumber}{employeeNumber}
telephoneNumber: <random>
description: This is the description for {cn}.
```

- e. テンプレートの内容を template.ldif にコピーし、次のようなコマンドを使用して test.ldif にデータを生成し、その内容をディレクトリにロードします。

```
$ cd install-path/dsrk6/bin/example_files/
$ ../makeldif -t test.template -o test.ldif
Processing complete.
101 total entries written.
$ ../ldapmodify -a -c -D uid=hmiller,dc=example,dc=com -w - -f test.ldif
Enter bind password:
...
```

Example.ldif を参照すると、hmiller のパスワードが hillock であることがわかります。

次の手順 ソフトウェアのインストール後に、63 ページの「環境変数」を参照してください。

ZIP 形式の配布から **Directory Service Control Center** をインストールする

Directory Server Enterprise Edition の ZIP 形式の配布には、Directory Service Control Center (DSCC) Web アプリケーションを格納した WAR ファイル (dsc6.war) が含まれます。WAR ファイルは、次の作業を実行できるように、アプリケーションサーバーとともに配備されます。

- DSCC をホストするシステムのオペレーティングシステムのログインアカウントなしで DSCC に接続します。
- アプリケーションサーバーが DSCC を有効にするため、root 権限なしで DSCC を配備します。

WAR ファイルでは、次のアプリケーションサーバーをサポートします。

- Sun Java System Application Server 8.2
- Tomcat 5.5

次の 2 つの手順では、WAR ファイルをそれぞれ Sun Java System Application Server と Tomcat で配備する方法について説明します。

▼ **Sun Java System Application Server** で WAR ファイルを配備する

Directory Server Enterprise Edition のインストール後、WAR ファイル dsc6.war は次の場所にあります。

```
install-path/var/dsc6/
```

1 DSCC レジストリを初期化します。

```
$ install-path/dsc6/bin/dsc6setup ads-create
Choose password for Directory Service Manager:
Confirm password for Directory Service Manager:
Creating DSCC registry...
DSCC Registry has been created successfully
```

2 アプリケーションサーバーインスタンスを作成します。

```
$ mkdir /local/domainroot
$ setenv AS_DOMAINS_ROOT /local/domainroot
$ cd app-server-install-path/bin
$ asadmin create-domain --domaindir ${AS_DOMAINS_ROOT} --adminport 3737 \
--adminuser boss dsc6
```

3 server.policy ファイルを編集します。

a. server.policy ファイルを開きます。

```
$ vi ${AS_DOMAINS_ROOT}/dsccl/config/server.policy
```

b. 次の文を、ファイルの末尾に追加します。

```
// Permissions for Directory Service Control Center
grant codeBase "file:${com.sun.aas.instanceRoot}/applications/j2ee-modules/dsccl/"
{
    permission java.security.AllPermission;
};
```

これでアプリケーションサーバーが設定されて、すべての Java アクセス権が DSCC アプリケーションに付与されます。

4 アプリケーションサーバーインスタンスに WAR ファイルを配備します。

```
$ asadmin start-domain --domaindir ${AS_DOMAINS_ROOT} --user username dsccl
$ cp install-path/var/dsccl6/dsccl.war ${AS_DOMAINS_ROOT}/dsccl/autodeploy
```

アプリケーションサーバーインスタンスの作成と設定、および WAR ファイルの配備についての詳細は、Sun Java System Application Server のオンラインヘルプを参照してください。

5 DSCC を開きます。

アプリケーションサーバーの設定に応じて、`http://hostname:8080/dsccl` または `https://hostname:8181/dsccl` を使用します。

Directory Service Manager のログインページが表示されます。

55 ページの「[Directory Service Control Center を使い始める](#)」を参照してください。

▼ Tomcat で WAR ファイルを配備する

Directory Server Enterprise Edition のインストール後、WAR ファイル `dsccl.war` は `install-path/var/dsccl6/` にあります。

`dsccl.war` は、ほかの Web アプリケーションと同様の方法でインストールしますが、次の設定が異なります。

- アプリケーションは、`dscclsetup ads-create` コマンドを使用して作成された DSCC レジストリと通信する必要があります。
- `web.xml` の `enablePooling` パラメータ値を `false` に設定して、Tomcat サーバーインスタンスでタグプールを無効にします。

Solaris 10 システムの Tomcat で DSCC をインストールする方法について次の例に示します。

1 DSCCレジストリを初期化します。

```
$ install-path/dsc6/bin/dscsetup ads-create
Choose password for Directory Service Manager:
Confirm password for Directory Service Manager:
Creating DSCC registry...
DSCC Registry has been created successfully
```

2 Tomcat インストールおよびインスタンスを特定します。

```
$ setenv CATALINA_HOME tomcat-install-path
$ setenv CATALINA_BASE tomcat-instance-path
$ setenv JAVA_HOME jdk-home-dir
```

Tomcat のインストールおよびインスタンスの作成については、Tomcat のドキュメントを参照してください。

3 WAR ファイルを配備します。

次のようにして dsc ディレクトリを作成します。

```
$ mkdir ${CATALINA_BASE}/webapps/dsc
```

dsc.war ファイルを新しく作成した dsc フォルダにコピーし、dsc.war ファイルを解凍します。

```
$ unzip -d ${CATALINA_BASE}/webapps/dsc install-path/var/dsc6/dsc.war
```

次に示す強調表示されたテキストを \${CATALINA_BASE}/conf/web.xml ファイルに追加します。

```
...
    <servlet>
        <servlet-name>jsp</servlet-name>
        <servlet-class>org.apache.jasper.servlet.JspServlet</servlet-class>
        <init-param>
            <param-name>fork</param-name>
            <param-value>>false</param-value>
        </init-param>
        <init-param>
            <param-name>xpoweredBy</param-name>
            <param-value>>false</param-value>
        </init-param>
    ...
    <init-param>
        <param-name>enablePooling</param-name>
        <param-value>>false</param-value>
    </init-param>
    <load-on-startup>3</load-on-startup>
</servlet>
....
```

startup.sh (Windows の場合は tomcat5.exe) のアクセス権を確認し、次のコマンドを実行します。

```
$ ${CATALINA_HOME}/bin/startup.sh
```

- 4 http://hostname:8080/dscc を使用して **DSCC** に接続します。
Directory Service Manager のログインページが表示されます。
55 ページの「[Directory Service Control Center を使い始める](#)」を参照してください。

▼ ZIP 形式の配布から **Directory Server Enterprise Edition** をアップグレードする

始める前に Directory Server Enterprise Edition インストールをアップグレードする手順と違いはありませんが、正確には、以前のインストールが検出された場合は dsee_deploy コマンドによってインストールが自動的に更新されます。ただし SuSE Linux 9 および HP-UX の場合は、Directory Server Enterprise Edition インストールをアップグレードする前に、オペレーティングシステムをそれぞれ SuSE Linux 9 SP4 および HP-UX 11.23 にアップグレードします。Directory Server Enterprise Edition インストールを 6.3 に正常にアップグレードする方法については、次の手順を参照してください。

- 1 パッチ対象のインストールを使用して作成された **cacao**、**Directory Server**、および **Directory Proxy Server** の実行中のインスタンスを停止します。また、**WAR** ファイルと **DSCC** レジストリ用のアプリケーションサーバーも停止します。
- 2 **SuSE Linux 9** および **HP-UX** の場合は、オペレーティングシステムをアップグレードします。
 - Directory Server Enterprise Edition 6.2 インストールを 6.3 にアップグレードするためには、SuSE Linux 9 SP3 を SuSE Linux 9 SP4 にアップグレードします。
SuSE 64 ビットの場合、cacao が起動するには .pam-32bit-9-yyymmddhhmm.rpm が必要です。システムにまだインストールされていない場合は、インストールしてください。
 - Directory Server Enterprise Edition 6.0 または 6.1 インストールを 6.3 にアップグレードするために、HP-UX 11.11 を HP-UX 11.23 にアップグレードします。

オペレーティングシステムをアップグレードする方法、Directory Server Enterprise Edition のインストールされるパーティションを保持する方法、最新のパッチバンドルの入手先については、それぞれのドキュメントを参照してください。

- 3 **Directory Server Enterprise Edition** を 6.3 にアップグレードします。
 - Directory Server Enterprise Edition 6.3 の ZIP 形式の配布から dsee_deploy コマンドを使用します。install-path と cacao ポートは、以前のインストールと同じ設定にします。dsee_deploy コマンドにより、cacao および DSCC レジストリが再起動されます。

詳細については、45 ページの「ZIP 形式の配布から Directory Server Enterprise Edition 6.3 をインストールする」を参照してください。

- 次のコマンドを使用して、アプリケーションサーバーに dscs.war ファイルを配備します。

詳細については、Sun Java System Application Server の場合は手順 4、Tomcat アプリケーションサーバーの場合は手順 3 を参照してください。

- Directory Server インスタンス、Directory Proxy Server インスタンス、および WAR ファイル用のアプリケーションサーバーを再起動します。
- 4 オペレーティングシステムのアップグレードと Directory Server Enterprise Edition のインストールの両方を終えた場合のみ、デーモンを起動します。

参照 サポートされるほかのオペレーティングシステムで Directory Server Enterprise Edition を 6.3 にアップグレードする場合の手順は、インストール手順と似ています。詳細については、45 ページの「ZIP 形式の配布から Directory Server Enterprise Edition 6.3 をインストールする」を参照してください。

Directory Service Control Center を使い始める

ネイティブパッケージまたは ZIP 形式の配布を使用して Directory Service Control Center をインストールしたら、次の手順を使用して使い始めたり、Directory Service Control Center へのアクセス時に問題が発生したらトラブルシューティングしたりします。

▼ Directory Service Control Center を使い始める

- 1 dscssetup initialize コマンドを使用して DSCC を初期化します。たとえば Solaris システムの場合、次のコマンドで初期化を実行します。

```
root# /opt/SUNWdsee/dscs6/bin/dscssetup initialize
***
Registering DSCC Application in Sun Java(TM) Web Console
This operation is going to stop Sun Java(TM) Web Console.
Do you want to continue ? [y,n] y
Stopping Sun Java(TM) Web Console...
Registration is on-going. Please wait...
DSCC is registered in Sun Java(TM) Web Console
Restarting Sun Java(TM) Web Console
Please wait : this may take several seconds...
Sun Java(TM) Web Console restarted successfully
***
Registering DSCC Agent in Cacao...
Checking Cacao status...
```

```
Starting Cacao...
DSCC agent has been successfully registered in Cacao.
***
Choose password for Directory Service Manager:
Confirm password for Directory Service Manager:
Creating DSCC registry...
DSCC Registry has been created successfully
***
```

dscctest コマンドは、*install-path/dscctest/bin/dscctest* にあります。使用しているシステムのデフォルトの *install-path* を判断するには、15 ページの「デフォルトのパス」を参照してください。

Windows の場合は次のコマンドを実行します。

```
install-path\dscctest\bin>dscctest.exe initialize
```

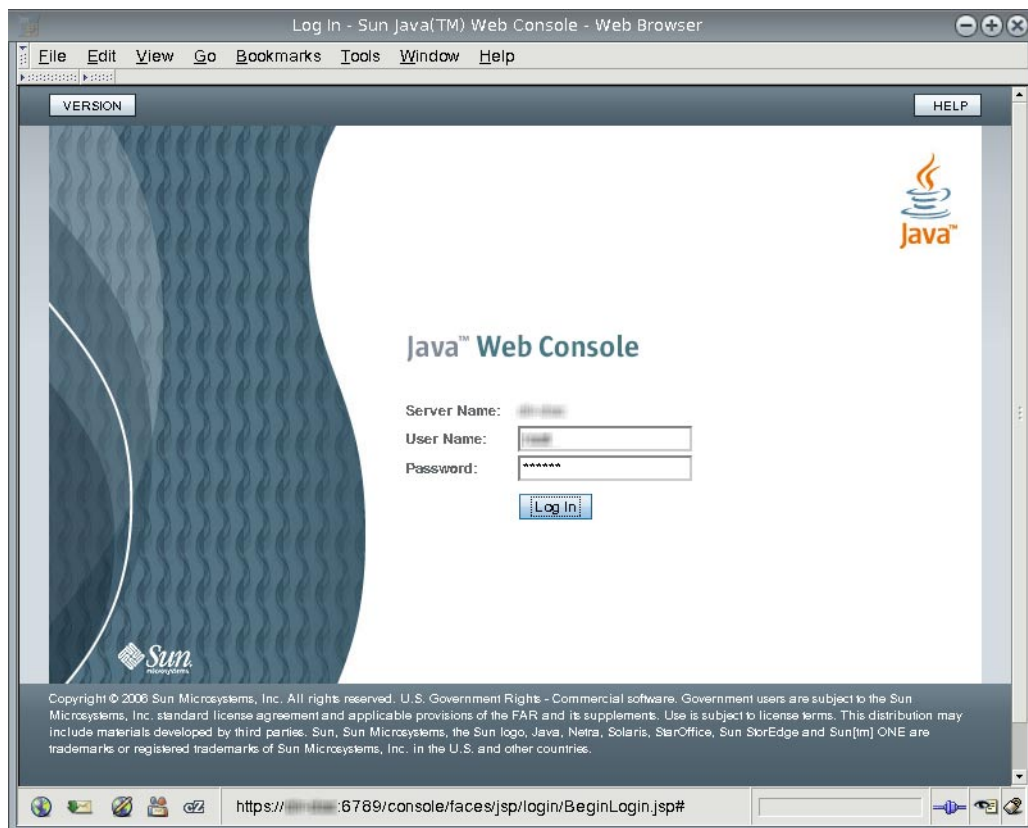
2 ブラウザで **Java Web** コンソールを使用して、**DSCC** にアクセスします。

別のロケールでコンソールにアクセスするには、ブラウザの優先する言語を設定します。ブラウザの優先する言語の設定については、個々のブラウザのドキュメントを参照してください。

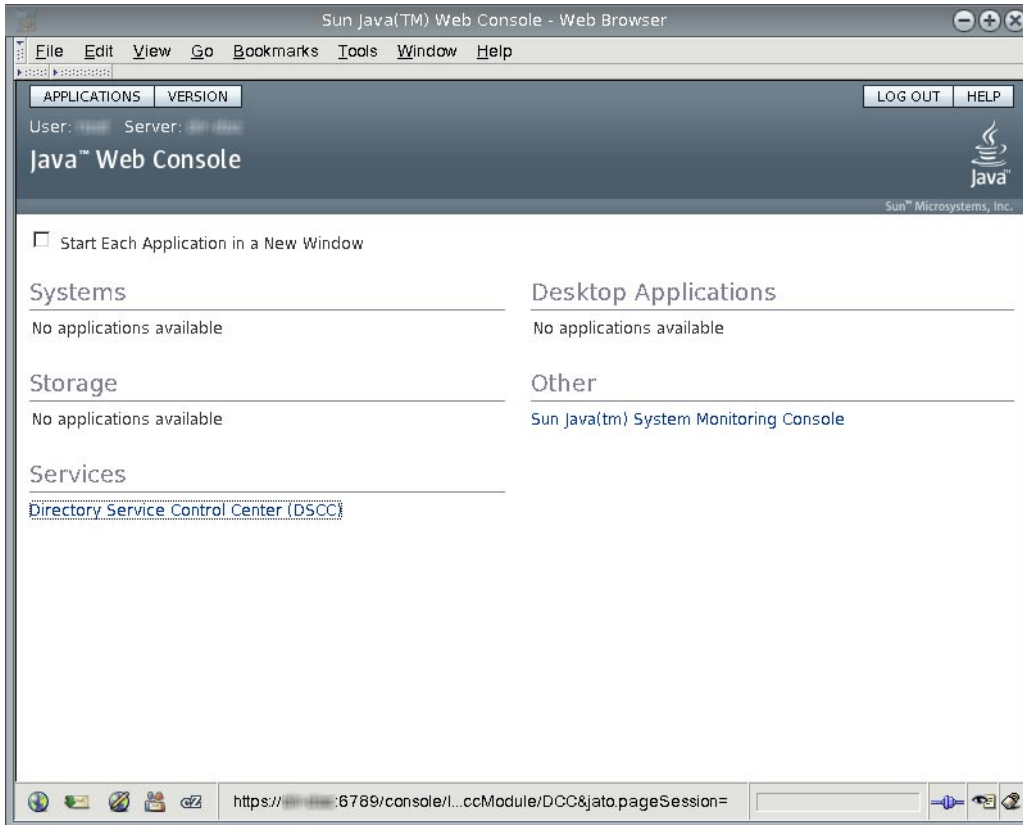
a. オペレーティングシステムのログイン情報またはサーバーの **root** ログイン情報を使用して、**Java Web** コンソールにログインします。

サーバーの **root** ログイン情報を使用して Java Web コンソールにログインしない場合、サーバーインスタンスの起動など一部の作業を実行する際に **root** 権限を持っていることが要求されます。

デフォルトで、Java Web コンソールにアクセスする URL は、`https://hostname:6789` です

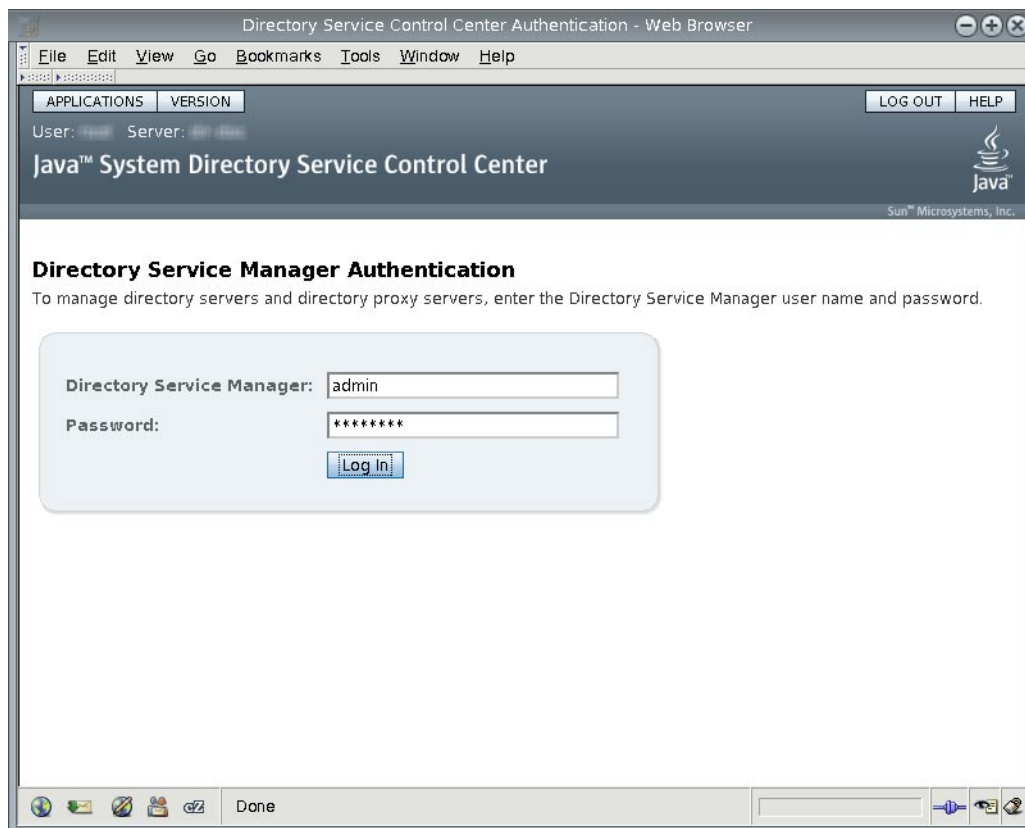


b. Directory Service Control Center のリンクをクリックします。



c. **Directory Service Manager** として **DSCC** にログインします。

Directory Service Manager のエントリは DSCC レジストリに格納されます。Directory Service Manager は DSCC に対する管理者アクセス権を持ちます。また、Directory Service Manager は、DSCC に登録されたサーバーインスタンスに対する管理者アクセス権も持ちます。



- d. **Directory Service Control Center** を使用してサーバーの管理を始めます。



- 3 **Directory Service Control Center** が実行中になったら、システムのリブート時に **Java Web** コンソールを再起動できるようにします。

Solaris システムの場合、次のコマンドでリブート時に再起動できるようになります。

```
root# /usr/sbin/smcwebserver enable
```

Windows の場合、次のコマンドでリブート時に再起動できるようになります。

```
C:\install-path\share\webconsole\bin>smcwebserver enable
```

使用しているシステムでのこのコマンドの正確な場所については、17 ページの「[コマンドの場所](#)」を参照してください。

- 4 (省略可能) 共通エージェントコンテナ cacao がオペレーティングシステムのリブート時に再起動するようにします。

```
root# cacaoadm enable
```

Windows では次のコマンドを実行して cacao を有効にします。

ネイティブパッケージでのインストールの場合:

```
C:\install-path\share\cacao_2bin>cacaoadm enable -i instance-path -f password.txt
```

ZIP 形式による配布でのインストールの場合:

```
C:\install-path\see6\cacao_2bin>cacaoadm enable -i instance-path -f password.txt
```

共通エージェントコンテナを有効にしない場合、オペレーティングシステムでは、リブート後にその cacao インスタンスが処理するサーバーと通信するために DSCC を使用できません。

▼ Directory Service Control Center へのアクセスをトラブルシューティングする

Directory Service Control Center へのアクセスに問題がある場合は、ネイティブパッケージを使用して Directory Service Control Center をインストールしたホストで、次の手順を実行します。

この手順を実行するには、root である必要があります。

- 1 Directory Service Control Center が適切に初期化されていることを確認します。

ネイティブパッケージの場合:

```
root# /opt/SUNWdsee/dsc6/bin/dscsetup status
***
DSCC Application is registered in Sun Java (TM) Web Console
***
DSCC Agent is registered in Cacao
***
DSCC Registry has been created
Path of DSCC registry is /var/opt/SUNWdsee/dsc6/dcc/ads
Port of DSCC registry is 3998
***
```

ZIP 形式の配布の場合:

```
$ install-path/dsc6/bin/dscsetup status
***
Sun Java (TM) Web Console is not installed
***
DSCC Agent is registered in Cacao
Cacao uses a custom port number (11168)
```

```
***
DSCC Registry has been created
Path of DSCC registry is /var/opt/SUNWdsee/dscc6/dcc/ads
Port of DSCC registry is 3998
***
```

Windows では次のコマンドを実行して、DSCC の状態を確認します。

```
C:\install-path\dscc6\bin>dscsetup.exe status
```

Solaris オペレーティングシステムでのネイティブパッケージのデフォルトのインストールパスは、`/opt/SUNWdsee` です。使用しているオペレーティングシステムでのデフォルトのインストールパスについては、[15 ページの「デフォルトのパス」](#)を参照してください。

DSCC の初期化に問題がある場合は、`dscsetup(1M)` コマンドを使用して問題を解決します。

- 2 ネイティブパッケージによるインストールの場合: **Java Web** コンソールの状態を確認し、まだ実行中でない場合は `smcwebserver` コマンドを使用して起動します。

```
root# /usr/sbin/smcwebserver status
Sun Java(TM) Web Console is stopped
root# /usr/sbin/smcwebserver start
Starting Sun Java(TM) Web Console Version 3.0.2 ...
The console is running.
```

Windows の場合は次のコマンドを実行して、Java Web コンソールの状態を確認し、必要に応じて起動します。

```
C:\install-path\share\webconsole\bin>smcwebserver status
C:\install-path\share\webconsole\bin>smcwebserver start
```

- 3 **DSCC** エージェントに関するエラーが表示された場合は、共通エージェントコンテナを確認します。

`cacaoadm(1M)` のマニュアルページでは、このコマンドが返すエラーコードについて説明されています。使用しているシステムでのこのコマンドの正確な場所については、[17 ページの「コマンドの場所」](#)を参照してください。

ネイティブパッケージによるインストールでは `root` として、ZIP 形式によるインストールではインストールを実行したユーザーとして、`cacaoadm` コマンドを実行してください。

```
root# /usr/sbin/cacaoadm status
default instance is DISABLED at system startup.
Smf monitoring process:
26129
Uptime: 0 day(s), 3:16
```

Directory Server をインストールすると、共通エージェントコンテナが自動的に起動します。ただし、リブートした場合は、共通エージェントコンテナを次のようにして手動で起動する必要がある場合があります。

```
# cacaoadm start
```

Windows では次のコマンドを使用して、共通エージェントコンテナの状態を確認します。

- ネイティブパッケージの場合

```
C:\install-path\share\cacao_2\bin>cacaoadm status
```

- ZIP 形式の配布の場合

```
C:\install-path\dsee6\cacao_2\bin>cacaoadm status
```

共通エージェントコンテナの詳細は、『[Sun Java Enterprise System 5 監視ガイド \(UNIX 版\)](#)』を参照してください。

環境変数

この節では、簡単にサーバーインスタンスを作成したり Directory Server Resource Kit やソフトウェア開発キットを使用したりするために設定できる環境変数の一覧を示します。

環境変数	格納する内容	適用先
DIR_PROXY_HOST	管理ツールで使用する Directory Proxy Server のホスト名	dpconf(1M) コマンド
DIR_PROXY_PORT	管理ツールで使用する Directory Proxy Server のポート番号	dpconf(1M) コマンド
DIRSERV_HOST	管理ツールで使用する Directory Server のホスト名	dsconf(1M) コマンド
DIRSERV_PORT	管理ツールで使用する Directory Server のポート番号	dsconf(1M) コマンド
LDAP_ADMIN_PWF	ディレクトリ管理者のパスワードが格納されたファイルへのパス Directory Service Control Center に登録されたすべてのサーバーを管理するには、この環境変数に Directory Service Manager パスワードが格納されたファイルを設定します。	dpconf(1M)、dsconf(1M) コマンド

環境変数	格納する内容	適用先
LDAP_ADMIN_USER	ディレクトリ管理者の DN Directory Service Control Center に登録されたすべてのサーバーを管理するには、この環境変数に cn=admin, cn=Administrators, cn=dscs を設定します。 DSCC をインストールしていない場合、Directory Server に cn=admin, cn=Administrators, cn=config、Directory Proxy Server に cn=Proxy Manager を使用します。	dpconf(1M)、dsconf(1M) コマンド
MANPATH	/opt/SUNWdsee/dsee6/man (Solaris SPARC)	man コマンドを使用して参照するオンラインのマニュアルページ
MANSECT	次のうち、MANSECT 環境変数に含まれていないセクションをすべて追加します。 1:1m:4:5dsconf:5dpconf:5dssd:5dsat:5dsoc または、man コマンドの使用時に、明示的に検索するセクションを指定します。	man コマンドでは、デフォルトで検索するセクションを特定するために MANSECT 環境変数を使用できます。
PATH (Solaris SPARC)	install-path/dps6/bin	Directory Proxy Server コマンド
	install-path/ds6/bin	Directory Server コマンド
	install-path/dscs6/bin	Directory Service Control Center コマンド
	install-path/dsrk6/bin	Directory Server Resource Kit および LDAP クライアントコマンド

サーバーインスタンスの作成

27 ページの「ソフトウェアのインストール」での説明に従ってサーバーソフトウェアをインストールしたら、サーバーインスタンスを作成します。ここでは、次の内容について説明します。

- 65 ページの「DSCC を使用して Directory Server インスタンスを作成する」
- 67 ページの「コマンド行から Directory Server インスタンスを作成する」
- 71 ページの「DSCC を使用して Directory Proxy Server インスタンスを作成する」
- 73 ページの「コマンド行から Directory Proxy Server インスタンスを作成する」

▼ DSCC を使用して Directory Server インスタンスを作成する

始める前に 27 ページの「ソフトウェアのインストール」での説明に従って、コンポーネントソフトウェアをインストールします。

root 以外のユーザーがサーバーインスタンスを作成できます。

- 1 **Java Web** コンソールから **Directory Service Control Center** にアクセスします。

ローカルシステムでの Java Web コンソールのデフォルトの URL は、`https://hostname:6789` です。

ZIP 形式の配布から Directory Server Enterprise Edition をインストールした場合は、アプリケーションサーバーの設定に応じて `http://hostname:8080/dsc` または `https://hostname:8181/dsc` を使用して DSCC にアクセスします。

- 2 **Directory Service Control Center** の「新規サーバー」ウィザードの指示に従って、サーバーインスタンスを作成します。

注-インスタンスのパスでは、ASCII以外の文字はサポートされません。

Windows 2003 プライマリドメインコントローラにインスタンスを正常に作成するには、「実行時のユーザー ID」に *domainname\username* と入力します。

▼ コマンド行から **Directory Server** インスタンスを作成する

この手順では、`dsadm` コマンドを使用して、ローカルホストにサーバーインスタンスを作成します。次に、`dsconf` コマンドを使用して、データを設定するサフィックスを作成します。

`root` 以外のユーザーがサーバーインスタンスを作成できます。

Directory Server インスタンスには、ディレクトリクライアントアプリケーションに回答するために必要な設定およびデータが含まれています。インスタンスを起動または停止するとき、サーバープロセスを起動または停止します。サーバープロセスとは、そのインスタンスによって管理されるデータに対応するディレクトリクライアント要求を処理するものです。

`dsadm` コマンドを使用すると、Directory Server インスタンスおよびそのインスタンスに属するローカルホスト上のファイルを管理できます。このコマンドでは、ネットワークを介してサーバーを管理することはできず、ローカルホスト上での直接管理のみを行えます。`dsadm` コマンドには、重要な各管理作業を行うためのサブコマンドがあります。詳細は、[dsadm\(1M\)](#)を参照してください。

`dsconf` コマンドは、LDAP クライアントです。このコマンドを使用すると、実行している Directory Server インスタンスのほぼすべてのサーバー設定をコマンド行から構成できます。サーバーがローカルホスト上に存在する場合でも、ネットワーク全体でアクセス可能な別のホストに存在する場合でも、設定を構成できます。`dsconf` コマンドには、重要な各設定作業を行うためのサブコマンドがあります。詳細は、[dsconf\(1M\)](#)を参照してください。

始める前に `コンポーネントソフトウェアをインストールし、27 ページの「ソフトウェアのインストール」での説明に従って PATH を設定します。`

1 新しい **Directory Server** インスタンスを作成します。

```
$ dsadm create -p port -P SSL-port instance-path
```

たとえば、`ds` インスタンスを既存のディレクトリ `/local/` に作成するには、次のコマンドを実行します。新しいインスタンスのデフォルトポートは、`root` ユーザーの場合で LDAP が 389、LDAPS が 636、`root` 以外のユーザーの場合で LDAP が 1389、LDAPS が 1636 です。

```
$ dsadm create /local/ds
```

ディレクトリマネージャーのパスワードを選択:

ディレクトリマネージャーのパスワードを確認:

インスタンスを起動するには「`dsadm start '/ /local/ds'`」を使用します

ネットワークファイルシステムではなくローカルファイルシステム上のディレクトリにインスタンスが作成されます。

2 インスタンスを起動します。

```
$ dsadm start instance-path
```

たとえば、/local/ds/ の下にあるインスタンスを起動するには、次のコマンドを実行します。

```
$ dsadm start /local/ds
Server started: pid=2845
```

3 新しいインスタンスのルート DSE (DSA 固有のエントリ) の読み取りができることを確認します。

```
$ ldapsearch -h hostname -p 1389 -b "" -s base "(objectclass=*)"
version: 1
dn:
objectClass: top
...
supportedLDAPVersion: 2
supportedLDAPVersion: 3
vendorName: Sun Microsystems, Inc.
vendorVersion: Sun-Java(tm)-System-Directory/6.3
...
```

注- この時点で、サーバーインスタンスが動作しています。ただし、サーバーインスタンスはあとで設定します。このインスタンスは Directory Service Control Center に登録されていません。

4 (省略可能) Directory Server Enterprise Edition 5 インスタンスによるレプリケーショントポロジに属さないかぎり、新しいパスワードポリシーモードを使用します。

サーバーインスタンスは、スタンドアロンである可能性があります。または、すでに新しいパスワードポリシーモードに移行済みのレプリケーショントポロジに属している可能性もあります。どちらの場合も、この手順を実行してください。

```
$ dsconf pwd-compat -h hostname -p 1389 to-DS6-migration-mode
```

サーバーによって提供された証明書 "CN=hostname, CN=1636, CN=Directory Server, O=Sun Microsystems" は信頼できません。

受け入れは「y」、1 回だけ受け入れは「Y」、拒否は「n」、詳細を表示は「d」を入力: Y

"cn=Directory Manager" のパスワードを入力:

```
## パスワードポリシー互換の変更を開始しています。
```

```
## パスワードポリシー互換の変更が完了しました。
```

タスクが完了しました (slapd 終了コード: 0)。

```
$ dsconf pwd-compat -p 1389 to-DS6-mode
```

"cn=Directory Manager" のパスワードを入力:

```
## パスワードポリシー互換の変更を開始しています。
```

```
## パスワードポリシー互換の変更が完了しました。
```

タスクが完了しました (slapd 終了コード: 0)。

5 (省略可能) サンプルのサフィックスを準備します。

a. 空のサフィックスを作成します。

たとえば、ルートが `dc=example,dc=com` であるサフィックスを作成するには、次のコマンドを実行します。

```
$ dsconf create-suffix -h hostname -p 1389 dc=example,dc=com
"cn=Directory Manager" のパスワードを入力:
$
```

b. LDIF データでサフィックスを設定します。

別の Directory Server インスタンスからレプリケートされたデータでサフィックスを設定する場合は、この手順を飛ばします。

たとえば、作成したサフィックスを `Example.ldif` からのサンプルデータで設定するには、次のコマンドを実行します。

```
$ dsconf import -h hostname -p 1389 install-path/ds6/ldif/Example.ldif \ dc=example,dc=com "cn=Directory Manager" のパスワードを入力: サフィックス「dc=example,dc=com」の既存のデータが新しいデータで上書きされます。レプリケートされたサフィックスで初期化を実行する必要があります。続行しますか [y/n] ? y
## Index buffering enabled with bucket size 40
## Beginning import job...
## Processing file "install-path/ds6/ldif/Example.ldif"
## Finished scanning file "install-path/ds6/ldif/Example.ldif" (160 entries)
## Workers finished; cleaning up...
## Workers cleaned up.
## Cleaning up producer thread...
## Indexing complete.
## Starting numsubordinates attribute generation. This may take a while, please wait for further activity reports.
## Numsubordinates attribute generation complete. Flushing caches...
## Closing files...
## Import complete. Processed 160 entries in 4 seconds. (40.00 entries/sec) タスクが完了しました (slapd 終了コード: 0)。
```

c. 新しいインスタンスでデータを検索します。

```
$ ldapsearch -h hostname -p 1389 -b dc=example,dc=com "(uid=bjensen)"
version: 1
dn: uid=bjensen, ou=People, dc=example,dc=com
cn: Barbara Jensen
cn: Babs Jensen
sn: Jensen
givenName: Barbara
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
ou: Product Development
```

```
ou: People
l: Cupertino
uid: bjensen
mail: bjensen@example.com
telephoneNumber: +1 408 555 1862
facsimileTelephoneNumber: +1 408 555 1992
roomNumber: 0209
```

6 (省略可能) 次のいずれかの方法を使用して、サーバーインスタンスを **Directory Service Control Center** に登録します。

- **DSCC** にログインし、「ディレクトリサーバー」タブの「サーバー」タブで「既存のサーバーの登録」アクションを使用します。

インストールした配布の種類やアプリケーションサーバーの設定方法に応じて、URL <https://hostname:6789>、<http://hostname:8080/dscc>、または <https://hostname:8181/dscc> を使用して **DSCC** にアクセスします。

- `dsccreg add-server` コマンドを使用します。

```
$ dsccreg add-server -h hostname --description "My DS" /local/ds
Enter DSCC administrator's password:
/local/ds is an instance of DS
Enter password of "cn=Directory Manager" for /local/ds:
This operation will restart /local/ds.
Do you want to continue ? (y/n) y
Connecting to /local/ds
Enabling DSCC access to /local/ds
Restarting /local/ds
Registering /local/ds in DSCC on hostname.
```

コマンドの詳細は、[dsccreg\(1M\)](#)を参照してください。

7 (省略可能) **Java Enterprise System** 配布を使用してネイティブパッケージからインストールした場合は、オペレーティングシステムのリブート時にサーバーが再起動できるようにします。

Solaris 10 および Windows システムでは、`dsadm enable-service` コマンドを使用します。

```
root# dsadm enable-service /local/ds
```

Solaris 9 および Red Hat システムでは、`dsadm autostart` コマンドを使用します。

```
root# dsadm autostart /local/ds
```

ZIP 形式の配布を使用してインストールした場合は、たとえばシステムの起動時に実行されるスクリプトを使用して、手動でこの手順を実行してください。

次の手順 サフィックスをさらに追加したり、ほかのサーバーインスタンスとのレプリケーションを設定したり、インスタンスを調整したりできるほか、通常はその他の設定操作に進むことができます。

グラフィカルユーザーインターフェースを使用して Directory Server を設定するヒントについては、Directory Service Control Center のオンラインヘルプを参照してください。

コマンド行の管理ツールを使用して Directory Server を設定する手順については、『Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド』のパート I 「Directory Server の管理」を参照してください。

▼ DSCC を使用して Directory Proxy Server インスタンスを作成する

root 以外のユーザーがサーバーインスタンスを作成できます。

始める前に 27 ページの「ソフトウェアのインストール」での説明に従って、コンポーネントソフトウェアをインストールします。

- 1 **Java Web** コンソールから **Directory Service Control Center** にアクセスします。

ローカルシステムでの Java Web コンソールのデフォルトの URL は `https://hostname:6789` です。

ZIP 形式の配布から Directory Server Enterprise Edition をインストールした場合は、アプリケーションサーバーの設定に応じて `http://hostname:8080/dscc` または `https://hostname:8181/dscc` を使用して DSCC にアクセスします。

- 2 **Directory Service Control Center** の「新規サーバー」ウィザードの指示に従って、サーバーインスタンスを作成します。

注-インスタンスのパスでは、ASCII以外の文字はサポートされません。

Windows 2003 プライマリドメインコントローラにインスタンスを正常に作成するには、「実行時のユーザー ID」に *domainname\username* と入力します。

▼ コマンド行から Directory Proxy Server インスタンスを作成する

この手順では、`dpadm` コマンドを使用して、ローカルホストにサーバーインスタンスを作成します。次に `dpconf` コマンドを使用して、インスタンスを設定します。

`root` 以外のユーザーがサーバーインスタンスを作成できます。

データビューを使用してデータソースに対するディレクトリクライアントアプリケーションの要求をプロキシ処理するように、Directory Proxy Server インスタンスを設定します。インスタンスを起動または停止するときは、ディレクトリクライアントアプリケーションの要求をプロキシ処理するサーバープロセスを起動または停止します。

`dpadm` コマンドを使用すると、Directory Proxy Server インスタンスおよびそのインスタンスに属するローカルホスト上のファイルを管理できます。このコマンドでは、ネットワーク越しにサーバーを管理することはできず、ローカルホストを直接管理できるだけです。`dpadm` コマンドには、重要な各管理作業を行うためのサブコマンドがあります。詳細は、[dpadm\(1M\)](#)を参照してください。

`dpconf` コマンドは、LDAP クライアントです。このコマンドを使用すると、実行している Directory Proxy Server インスタンスのほぼすべてのサーバー設定をコマンド行から構成できます。サーバーがローカルホスト上に存在する場合でも、ネットワーク全体でアクセス可能な別のホストに存在する場合でも、設定を構成できます。`dpconf` コマンドには、重要な各設定作業を行うためのサブコマンドがあります。詳細は、[dpconf\(1M\)](#)を参照してください。

始める前に [コンポーネントソフトウェアをインストールし、27 ページの「ソフトウェアのインストール」](#)での説明に従って `PATH` を設定します。

1 新しい Directory Proxy Server インスタンスを作成します。

```
$ dpadm create -p port -P SSL-port instance-path
```

たとえば、Directory Proxy Server インスタンスを既存のディレクトリ `/local/dps` に作成するには、次のコマンドを実行します。デフォルトポートは、`root` ユーザーの場合で LDAP が 389、LDAPS が 636、`root` 以外のユーザーの場合で LDAP が 1389、LDAPS が 1636 です。

```
$ dpadm create -p 1390 -P 1637 /local/dps
```

プロキシマネージャーのパスワードを選択:

プロキシマネージャーのパスワードを確認:

インスタンスを起動するには「`dpadm start /local/dps`」を使用します

ネットワークファイルシステムではなくローカルファイルシステム上のディレクトリにインスタンスを作成してください。

2 インスタンスを起動します。

```
$ dpadm start instance-path
```

たとえば、`/local/dps/` の下にあるインスタンスを起動するには、次のコマンドを実行します。

```
$ dpadm start /local/dps
```

```
...
```

```
Directory Proxy Server インスタンス '/local/dps' が起動しました: pid=28732
```

3 新しいインスタンスのルート DSE の読み取りができることを確認します。

```
$ ldapsearch -h hostname -p 1390 -b "" -s base "(objectclass=*)"
```

```
version: 1
```

```
dn:
```

```
objectClass: top
```

```
objectClass: extensibleObject
```

```
supportedLDAPVersion: 2
```

```
supportedLDAPVersion: 3
```

```
...
```

```
vendorName: Sun Microsystems, Inc
```

```
vendorVersion: Directory Proxy Server 6.3
```

```
...
```

注- この時点で、サーバーインスタンスが動作しています。ただし、サーバーインスタンスはあとで設定します。このインスタンスは Directory Service Control Center に登録されていません。

4 (省略可能) Directory Proxy Server インスタンスが LDAP プロキシとして動作するようにします。

a. LDAP データソースを作成します。

たとえば、67 ページの「[コマンド行から Directory Server インスタンスを作成する](#)」でローカルホストに作成されたディレクトリインスタンスを指すデータソース My DS を作成するには、次のコマンドを実行します。

```
$ dpconf create-ldap-data-source -h hostname -p 1390 "My DS" hostname:1389
```

サーバーによって提供された証明書 "CN=hostname:1390" は信頼できません。

受け入れは「Y」、1 回だけ受け入れは「y」、拒否は「n」、詳細を表示は「d」を入力: Y

"cn=Proxy Manager" のパスワードを入力:

b. LDAP データソースプールを作成します。

```
$ dpconf create-ldap-data-source-pool -h hostname -p 1390 "My Pool"
"cn=Proxy Manager" のパスワードを入力:
```

- c. LDAP データソースを LDAP データソースプールに接続します。

```
$ dpconf attach-ldap-data-source -h hostname -p 1390 "My Pool" "My DS"  
"cn=Proxy Manager" のパスワードを入力:
```

- d. LDAP データソースプールを使用して LDAP データビューを作成します。

たとえば、クライアントアプリケーションでサフィックス `dc=example,dc=com` を認識できるようにするデータビュー `My View` を作成するには、次のコマンドを実行します。

```
$ dpconf create-ldap-data-view -h hostname -p 1390 "My View" \  
"My Pool" dc=example,dc=com  
"cn=Proxy Manager" のパスワードを入力:
```

- e. LDAP データソースを有効にします。

```
$ dpconf set-ldap-data-source-prop -h hostname -p 1390 "My DS" is-enabled:true  
"cn=Proxy Manager" のパスワードを入力:
```

- f. 変更内容を有効にするために、サーバーを再起動します。

```
$ dpadm restart /local/dps
```

- g. LDAP データソースの検索を有効にします。

```
$ dpconf set-attached-ldap-data-source-prop -h hostname -p 1390 \  
"My Pool" "My DS" search-weight:100  
"cn=Proxy Manager" のパスワードを入力:
```

- h. 新しいインスタンスを介してディレクトリデータの読み取りができることを確認します。

```
$ ldapsearch -h hostname -p 1390 -b dc=example,dc=com "(uid=bjensen)"  
version: 1  
dn: uid=bjensen, ou=People, dc=example,dc=com  
cn: Barbara Jensen  
cn: Babs Jensen  
sn: Jensen  
givenName: Barbara  
objectClass: top  
objectClass: person  
objectClass: organizationalPerson  
objectClass: inetOrgPerson  
ou: Product Development  
ou: People  
l: Cupertino  
uid: bjensen  
mail: bjensen@example.com  
telephoneNumber: +1 408 555 1862  
facsimileTelephoneNumber: +1 408 555 1992  
roomNumber: 0209
```

注-LDAP 検索操作は、作成したデータビューで処理されるサフィックスに対して動作し、その他のサフィックスに対しては動作しません。データビューが設定されていないサフィックスを検索すると、サーバーからエラーが返ります。

```
$ ldapsearch -h hostname -p 1390 -b o=example.com "(uid=bjensen)"
ldap_search: Operations error
ldap_search: additional info: Unable to retrieve a backend SEARCH
connection to process the search request
```

Directory Proxy Server を設定する詳細は、『[Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド](#)』のパート II 「[Directory Proxy Server の管理](#)」を参照してください。

- 5 (省略可能) 次のいずれかの方法を使用して、サーバーインスタンスを **Directory Service Control Center** に登録します。

- **DSCC** にログインし、「プロキシサーバー」タブで「既存のサーバーの登録」アクションを使用します。

インストールした配布の種類やアプリケーションサーバーの設定方法に応じて、URL <https://hostname:6789>、<http://hostname:8080/dsc>、または <https://hostname:8181/dsc> を使用して **DSCC** にアクセスします。

- `dscrcg add-server` コマンドを使用します。

```
$ dscrcg add-server -h hostname --description "My Proxy" /local/dps
Enter DSCC administrator's password:
/local/dps is an instance of DPS
Enter password of "cn=Proxy Manager" for /local/dps:
Connecting to /local/dps
Enabling DSCC access to /local/dps
Registering /local/dps in DSCC on hostname.
```

コマンドの詳細は、[dscrcg\(1M\)](#)を参照してください。

- 6 (省略可能) **Java Enterprise System** 配布を使用してネイティブパッケージからインストールした場合は、オペレーティングシステムのリブート時にサーバーが再起動できるようにします。

Solaris 10 および Windows システムでは、`dpadm enable-service` コマンドを使用します。

```
root# dpadm enable-service /local/dps
```

Solaris 9 および Red Hat システムでは、`dpadm autostart` コマンドを使用します。

```
root# dpadm autostart /local/dps
```

ZIP 形式の配布を使用してインストールした場合は、システムの起動時に実行されるスクリプトを使用して、手動でこの手順を実行してください。

次の手順 さらにデータソースやデータビューの設定を続けることができます。また、負荷分散やデータ配布などのサーバー機能を設定することもできます。

グラフィカルユーザーインターフェースを使用して Directory Proxy Server を設定するヒントについては、Directory Service Control Center のオンラインヘルプを参照してください。

コマンド行の管理ツールを使用して Directory Proxy Server を設定する手順については、『Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド』のパート II 「Directory Proxy Server の管理」を参照してください。

Solaris 10 システムで Sun 暗号化フレームワークを使用する

この節では、Solaris 10 システム上の Sun 暗号化フレームワークと Directory Server および Directory Proxy Server を使用して、Sun 暗号化アクセラレータカードを使用する方法について簡単に説明します。フレームワークの詳細は、関連ドキュメントを参照してください。

▼ Solaris 10 システムで暗号化ハードウェアとともに Directory Server を使用する

始める前に この手順では、Sun 暗号化アクセラレータハードウェアとともに使用することを前提としています。次の手順は、Directory Server インスタンスを実行するユーザーと同じユーザーで実行してください。

- 1 `pktool setpin` コマンドを使用して、暗号化フレームワークにアクセスするときに使用する PIN を設定します。
Directory Server を実行しているユーザーと同じユーザーとして PIN を設定します。
- 2 現在の Directory Server 証明書を PKCS#12 ファイルにエクスポートします。
Directory Server インスタンスが `/local/ds/` の下にある場合、次のコマンドを実行するとこの手順を実行する方法が示されます。

```
$ dsadm export-cert -o cert-file /local/ds defaultCert
```

- 3 鍵データにアクセスするときに適切なトークンを使用するように **Directory Server** を設定します。

通常、トークンは Sun Metaslot です。

```
$ dsconf set-server-prop 'ssl-rsa-security-device:Sun Metaslot'
```

- 4 **Directory Server** を停止します。

```
$ dsadm stop /local/ds
```

- 5 (省略可能) **Directory Server** インスタンスの既存の証明書データベースにその他の証明書がない場合は、証明書データベースを削除します。

```
$ rm -f /local/ds/alias/*.db
```

この省略可能な手順によって、証明書がソフトウェアデータベースに確実に格納されなくなります。

- 6 **Solaris** 暗号化フレームワークによって管理される新しい証明書データベースを作成します。

証明書を削除しなかった場合は、この例の `modutil -create` 行を実行する必要はありません。

```
$ /usr/sfw/bin/64/modutil -create -dbdir /local/ds/alias -dbprefix slapd-
$ /usr/sfw/bin/64/modutil -add "Solaris Kernel Crypto Driver" -libfile \
  /usr/lib/64/libpkcs11.so -dbdir /local/ds/alias -dbprefix slapd-
$ /usr/sfw/bin/64/modutil -enable "Solaris Kernel Crypto Driver" \
  -dbdir /local/ds/alias -dbprefix slapd-
```

- 7 エクスポートした **PKCS#12** 証明書をインポートします。

```
$ /usr/sfw/bin/64/pk12util -i cert-file \
  -d /local/ds/alias -P slapd- -h "Sun Metaslot"
$ /usr/sfw/bin/64/certutil -M -n "Sun Metaslot:defaultCert" -t CTu \
  -d /local/ds/alias -P slapd-
```

アクセラレータボードに FIPS 140-2 キーストアがある場合は、デバイス上で非公開鍵が生成される必要があります。たとえば、Sun 暗号化アクセラレータ 4000 および 6000 ボードには、FIPS 140-2 キーストアがあります。正確なプロセスはボードによって異なります。

- 8 暗号化フレームワークへのアクセスに必要な **PIN** が含まれるパスワードファイルを作成します。

これは、手順 1 でパスワードを変更した場合のみ必要です。

```
$ echo "Sun Metaslot:password" > /local/ds/alias/slapd-pin.txt
```

- 9 **Directory Server** を起動します。

```
$ dsadm start /local/ds
```

▼ Solaris 10 システムで暗号化ハードウェアとともに Directory Proxy Server を使用する

始める前に この手順では、Sun 暗号化アクセラレータハードウェアとともに使用することを前提としています。次の手順は、Directory Proxy Server インスタンスを実行するユーザーと同じユーザーで実行してください。

- 1 Directory Proxy Server を停止します。

```
$ dpadm stop /local/dps
```

- 2 証明書データベースのパスワード保存を無効にします。

```
$ dpadm set-flags /local/dps cert-pwd-prompt=on
```

証明書データベースのパスワードを選択:

証明書データベースのパスワードを確認:

- 3 `pktool setpin` コマンドを使用して、暗号化フレームワークにアクセスするときに使用する PIN を設定します。

証明書データベースのパスワード保存を無効にしたときに入力したパスワードと同じパスワードを使用します。

- 4 キーストアとして暗号化フレームワークを使用して鍵ペアを生成します。

```
$ keytool -genkeypair -alias defaultDPScert  
-dname "ou=dps server,dc=example,dc=com" -keyalg RSA -sigalg MD5withRSA  
-validity 3652 -storetype PKCS11 -keystore NONE -storepass pin-password
```

`pin-password` は、`pktool setpin` コマンドを使用して PIN として設定したパスワードです。

- 5 Directory Proxy Server 設定ファイルを編集して、次の属性をベースエントリ `cn=config` に追加します。

```
serverCertificateNickName: defaultDPScert  
certificateKeyStore: NONE  
certificateKeyStoreType: PKCS11
```

- 6 Directory Proxy Server を起動します。

```
$ dpadm start /local/dps
```


Directory Server Enterprise Edition 6.3 のアンインストール

この章では、Directory Server Enterprise Edition ソフトウェアの削除について説明します。

この章の内容は次のとおりです。

- 81 ページの「サーバーインスタンスの削除」では、削除するソフトウェアに依存するサーバーインスタンスの削除について説明します。
- 84 ページの「ソフトウェアの削除」では、サーバーインスタンスを削除したあとでソフトウェアを削除する方法について説明します。
- 86 ページの「Directory Server Enterprise Edition 6.3 のダウングレード手順」では、Directory Server Enterprise Edition インストールをダウングレードする方法について説明します。

サーバーインスタンスの削除

システム上のサーバーインスタンスで使用される Directory Server Enterprise Edition ソフトウェアを削除する前に、すべてのサーバーインスタンスを削除します。

- 82 ページの「DSCC を使用して Directory Proxy Server インスタンスを削除する」
- 82 ページの「コマンド行から Directory Proxy Server インスタンスを削除する」
- 83 ページの「DSCC を使用して Directory Server インスタンスを削除する」
- 83 ページの「コマンド行から Directory Server インスタンスを削除する」

▼ DSCC を使用して Directory Proxy Server インスタンスを削除する

- 1 **Java Web** コンソールから **Directory Service Control Center** にアクセスします。
ローカルシステムでの Java Web コンソールのデフォルトの URL は、<https://hostname:6789> です。

ZIP 形式の配布から Directory Server Enterprise Edition をインストールした場合は、アプリケーションサーバーの設定に応じて <http://hostname:8080/dscc> または <https://hostname:8181/dscc> を使用して DSCC にアクセスします。
- 2 アクションドロップダウンリストの「削除」コマンドを使用してサーバーインスタンスを削除します。

▼ コマンド行から Directory Proxy Server インスタンスを削除する

- 1 (省略可能) DSCC を使用してサーバーインスタンスを管理していた場合は、サーバーの登録を削除します。

```
$ dsccreg remove-server -h hostname /local/dps
Enter DSCC administrator's password:
/local/dps is an instance of DPS
Enter password of "cn=Proxy Manager" for /local/dps:
Unregistering /local/dps from DSCC on hostname.
Connecting to /local/dps
Disabling DSCC access to /local/dps
```

詳細は、[dsccreg\(1M\)](#)を参照してください

- 2 サーバーインスタンスを削除します。

```
$ dpadm delete /local/dps
Directory Proxy Server インスタンス '/local/dps' が停止しました
Directory Proxy Server インスタンス '/local/dps' が削除されました。
```

参照 システム上のすべてのサーバーインスタンスを削除したら、[84 ページ](#)の「ソフトウェアの削除」に進めます。

▼ DSCC を使用して Directory Server インスタンスを削除する

Directory Server インスタンスを削除すると、そのインスタンスによって管理されるすべてのディレクトリデータベースを含む、すべてのインスタンスファイルが削除されます。インスタンスを削除する前に、『[Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド](#)』の第9章「[Directory Server のバックアップと復元](#)」での説明に従ってデータをバックアップしてください。

- 1 **Java Web** コンソールから **Directory Service Control Center** にアクセスします。

ローカルシステムでの Java Web コンソールのデフォルトの URL は、`https://hostname:6789` です。

Directory Server Enterprise Edition を ZIP 形式の配布からインストールした場合は、アプリケーションサーバーの設定方法に応じて、`http://hostname:8080/dscc` または `https://hostname:8181/dscc` を使用して Directory Service Control Center にアクセスします。

- 2 アクションドロップダウンリストの「削除」コマンドを使用してサーバーインスタンスを削除します。

▼ コマンド行から Directory Server インスタンスを削除する

Directory Server インスタンスを削除すると、そのインスタンスによって管理されるすべてのディレクトリデータベースを含む、すべてのインスタンスファイルが削除されます。インスタンスを削除する前に、『[Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド](#)』の第9章「[Directory Server のバックアップと復元](#)」での説明に従ってデータをバックアップしてください。

- 1 (省略可能) **DSCC** を使用してサーバーインスタンスを管理していた場合は、サーバーの登録を削除します。

```
$ dsccreg remove-server -h hostname /local/ds
Enter DSCC administrator's password:
/local/ds is an instance of DS
Enter password of "cn=Directory Manager" for /local/ds:
This operation will restart /local/ds.
Do you want to continue ? (y/n) y
Unregistering /local/ds from DSCC on hostname.
Connecting to /local/ds
Disabling DSCC access to /local/ds
Restarting /local/ds
```

詳細は、[dsccreg\(1M\)](#)を参照してください

- 2 サーバーインスタンスを削除します。

```
$ dsadm delete /local/ds
サーバーが停止しました
/local/ds が削除されました
```

参照 システム上のすべてのサーバーインスタンスを削除したら、[84 ページの「ソフトウェアの削除」](#)に進めます。

ソフトウェアの削除

インストールされている製品コンポーネントに依存するサーバーインスタンスをすべて削除したら、コンポーネントソフトウェアを削除できます。

- 84 ページの「ネイティブパッケージからインストールした Directory Service Control Center を削除する」
- 85 ページの「ネイティブパッケージからインストールした Directory Server または Directory Proxy Server を削除する」
- 85 ページの「ZIP 形式の配布からインストールしたソフトウェアを削除する」
- 86 ページの「ZIP 形式の配布からインストールしたソフトウェアを強制的に削除する」

▼ ネイティブパッケージからインストールした Directory Service Control Center を削除する

すべての DSCC を削除することで、システムから Directory Server パッケージも削除されます。

- 1 `dscsetup dismantle` コマンドを使用して **DSCC** を設定解除します。
たとえば、Solaris システムの場合は次のコマンドを使用して DSCC を取り除きます。

```
root# /opt/SUNWdsee/dsc6/bin/dscsetup dismantle
***
Unregistering DSCC Application from Sun Java(TM) Web Console...
This operation is going to stop Sun Java(TM) Web Console.
Do you want to continue ? [y,n] y
Stopping Sun Java(TM) Web Console...
Unregistration is on-going. Please wait...
/var/opt/SUNWdsee/dsc6/dcc has not been removed
DSCC Application has been unregistered from Sun Java(TM) Web Console
Restarting Sun Java(TM) Web Console
Please wait : this may take several seconds...
Sun Java(TM) Web Console restarted successfully
***
```

Windows の場合は次のコマンドを使用して DSCC を取り除きます。

```
C:\install-path\dsc6\bin>dsc6setup.exe dismantle
```

Solaris の `dsc6setup` コマンドは、`install-path/dsc6/bin/dsc6setup` にあります。使用しているシステムのデフォルトの `install-path` を判断するには、15 ページの「デフォルトのパス」を参照してください。

2 Java ES インストーラを使用して Directory Service Control Center を削除します。

手順については、<http://docs.sun.com/coll/1286.3> にある Java Enterprise System マニュアルを参照してください。

ZIP 形式の配布を使用してインストールした Directory Service Control Center は、前述の手順ではアンインストールされません。DSCC をアンインストールする必要がある場合は、Web アプリケーションを削除する方法について、それぞれのアプリケーションサーバーのマニュアルを参照してください。

▼ ネイティブパッケージからインストールした Directory Server または Directory Proxy Server を削除する

● Java ES インストーラを使用してソフトウェアを削除します。

手順については、<http://docs.sun.com/coll/1286.3> にある Java Enterprise System マニュアルを参照してください。

▼ ZIP 形式の配布からインストールしたソフトウェアを削除する

● `dsee_deploy(1M)` コマンドを使用してソフトウェアを削除します。

`root` 以外のユーザーが ZIP 形式の配布ソフトウェアをインストールした場合は、そのユーザーもソフトウェアを削除できます。

たとえば、`/local` の下にインストールされたすべての Directory Server Enterprise Edition ソフトウェアを削除するには、次のコマンドを実行します。

```
$ /local/dsee6/bin/dsee_deploy uninstall -i /local
```

Windows の場合、次のコマンドを実行して、ソフトウェアをアンインストールします。

```
C:\install-path\dsee6\bin\dsee_deploy uninstall -i install-path
```

参照 サポートされるコンポーネントの完全なリストについては、[dsee_deploy\(1M\)](#)を参照してください。

▼ ZIP 形式の配布からインストールしたソフトウェアを強制的に削除する

始める前に ZIP 形式の配布からソフトウェアをインストールした場合は、インストールしたファイルを削除することでソフトウェアを強制的に削除できます。

root 以外のユーザーが ZIP 形式の配布ソフトウェアをインストールした場合は、そのユーザーもソフトウェアを削除できます。

ネイティブパッケージからインストールしたファイルは直接削除しないでください。

- システムのコマンドを使用してコンポーネントを削除します。

```
$ rm -rf install-path
```

Windows の場合、次のコマンドを使用して、コンポーネントを削除します。

```
C:\>del /s install-path
```

```
C:\>del install-path
```

Directory Server Enterprise Edition 6.3 のダウングレード手順

Directory Server Enterprise Edition 6.3 にアップグレードしたら、以前の Directory Server Enterprise Edition インストールを復元できます。この節では、Directory Server Enterprise Edition インストールをダウングレードする方法の詳細について説明します。

ネイティブパッケージを使用して Directory Server Enterprise Edition をダウングレードする

Directory Server Enterprise Edition をダウングレードすると、Directory Server Enterprise Edition インストールの動作する以前のコピーが復元され、Directory Server Enterprise Edition 6.3 にアップグレードする前の設定情報すべてが保持されます。

Directory Server Enterprise Edition をダウングレードするには、次の手順に従います。

1. 実行中のサーバーインスタンスをすべて停止します。

2. 次のコマンドを実行してパッチを削除します。

ローカリゼーションパッチを削除したあとに、ベースパッチを削除してシステムを整理します。各プラットフォームのパッチ ID については、45 ページの「ZIP 形式の配布から Directory Server Enterprise Edition 6.3 をインストールする」の節の「ZIP 形式の配布でのパッチの表」を参照してください。

- Solaris OS

```
# patchrm patch-id
```

- Linux. Directory Server Enterprise Edition 6.2、6.1、または 6.0 の .rpm ファイルが格納されているディレクトリに移動し、次の表に示されているすべての rpm ファイルに対して次のコマンドを繰り返し実行します。選択する rpm ファイルのセットは、使用していた Directory Server Enterprise Edition の以前のインストールによって異なります。

ダウングレードしたら 6.0、6.1、または 6.2 の rpm ファイルがすべて揃っていることを確認する必要があります。rpm ファイルのサブセットをダウングレードすると、インストールが破損します。

```
# rpm -U --oldpackage rpm-file-name
```

たとえば、Directory Server Enterprise Edition 6.2 ベースインストールにダウングレードする場合は、次の表で対応するセルに示されているすべての rpm ファイルに対して、前述のコマンドを繰り返し実行します。コマンドを実行するときは、順序を変更しないでください。6.2 および 6.1 ベースのファイルおよびローカライズされたファイルの一覧を次の表に示します。

ローカライズされた 6.2 rpm ファイル	sun-ldap-console-gui-l10n-6.2-6.i386.rpm sun-ldap-console-gui-help-l10n-6.2-6.i386.rpm sun-ldap-proxy-client-l10n-6.2-6.i386.rpm sun-ldap-proxy-l10n-6.2-6.i386.rpm sun-ldap-directory-client-l10n-6.2-6.i386.rpm sun-ldap-directory-l10n-6.2-6.i386.rpm sun-ldap-shared-l10n-6.2-6.i386.rpm
---------------------------	--

ベース 6.2 rpm ファイル	sun-ldap-console-gui-6.2-5.i386.rpm sun-ldap-console-gui-help-6.2-5.i386.rpm sun-ldap-console-agent-6.2-5.i386.rpm sun-ldap-console-cli-6.2-5.i386.rpm sun-ldap-proxy-man-6.2-5.i386.rpm sun-ldap-proxy-client-6.2-5.i386.rpm sun-ldap-proxy-config-6.2-5.i386.rpm sun-ldap-proxy-6.2-5.i386.rpm sun-ldap-directory-man-6.2-5.i386.rpm sun-ldap-directory-client-6.2-4.i386.rpm sun-ldap-directory-config-6.2-5.i386.rpm sun-ldap-directory-6.2-5.i386.rpm sun-ldap-shared-6.2-5.i386.rpm
ローカライズされた 6.1 rpm ファイル	sun-ldap-console-gui-l10n-6.1-3.i386.rpm sun-ldap-console-gui-help-l10n-6.1-3.i386.rpm sun-ldap-proxy-client-l10n-6.1-3.i386.rpm sun-ldap-proxy-l10n-6.1-3.i386.rpm sun-ldap-directory-client-l10n-6.1-3.i386.rpm sun-ldap-directory-l10n-6.1-3.i386.rpm sun-ldap-shared-l10n-6.1-3.i386.rpm
ベース 6.1 rpm ファイル	sun-ldap-console-gui-6.1-2.i386.rpm sun-ldap-console-gui-help-6.1-2.i386.rpm sun-ldap-console-agent-6.1-2.i386.rpm sun-ldap-console-cli-6.1-2.i386.rpm sun-ldap-proxy-man-6.1-2.i386.rpm sun-ldap-proxy-client-6.1-2.i386.rpm sun-ldap-proxy-config-6.1-2.i386.rpm sun-ldap-proxy-6.1-2.i386.rpm sun-ldap-directory-man-6.1-2.i386.rpm sun-ldap-directory-client-6.1-2.i386.rpm sun-ldap-directory-config-6.1-2.i386.rpm sun-ldap-directory-6.1-2.i386.rpm sun-ldap-shared-6.1-2.i386.rpm

- Windows。Uninstall_patch-id.bat ファイルをダブルクリックしてパッチを削除します。Uninstall_patch-id.bat ファイルは、パッチが保存されたフォルダに格納されています。

ZIP 形式の配布を使用して Directory Server Enterprise Edition をダウングレードする

Directory Server Enterprise Edition 6.3 インストールは、以前のバージョンにダウングレードされません。以前の Directory Server Enterprise Edition バージョンに戻す必要がある場合は、Directory Server Enterprise Edition 6.3 にアップグレードする前に保存したバックアップコピーを復元します。

Directory Server Enterprise Edition を完全に削除するには、[85 ページの「ZIP 形式の配布からインストールしたソフトウェアを削除する」](#)を参照してください。

パート II

Identity Synchronization for Windows のインストール

Sun Java System Identity Synchronization for Windows 6.0 を使用すると、パスワードやその他の指定されたユーザー属性を Sun Java System Directory Server とその他のシステムとの間で受け渡すことができます。

本ガイドのこの部では、Identity Synchronization for Windows を本稼働環境で使用するようインストールおよび設定する方法について説明します。

新機能および Identity Synchronization for Windows のこのリリースの拡張機能の最新情報については、『[Sun Java System Directory Server Enterprise Edition 6.3 リリースノート](#)』を参照してください。

注- このドキュメントに記載のユーザーインターフェースは、将来の製品バージョンで変更されることがあります。

次の章で構成されています。

- [第3章「製品の理解」](#)では、Identity Synchronization for Windows 製品の機能、システムコンポーネントとその配布、コマンド行ユーティリティー、および配備の例について説明します。
- [第4章「インストールの準備」](#)では、インストールと設定のプロセス、および製品インストールの準備時に知っておく必要のある情報について説明します。
- [第5章「コアのインストール」](#)では、Identity Synchronization for Windows のインストールプログラムを使用する方法、およびコアコンポーネントをインストールする方法について説明します。
- [第6章「コアリソースの設定」](#)では、コンソールを使用してコアリソースを追加および設定する方法について説明します。
- [第7章「コネクタのインストール」](#)では、Identity Synchronization for Windows コネクタおよびディレクトリサーバープラグインをインストールする手順について説明します。
- [第8章「既存のユーザーおよびユーザーグループの同期」](#)では、新しい Identity Synchronization for Windows インストールに対して既存のユーザーおよびユーザーグループをリンクおよび再同期する方法について説明します。
- [第9章「ソフトウェアの削除」](#)では、アンインストールを準備する方法とコンソールを手動でアンインストールする方法を含む、Identity Synchronization for Windows を削除する方法について説明します。
- [第10章「セキュリティの設定」](#)では、セキュリティ保護されたシステムを設定する方法について説明します。この章では、セキュリティの強化、レプリケートされた設定のセキュリティ保護、SSLの有効化、および証明書データベースへの Active Directory CA 証明書の追加を行う方法について説明します。
- [第11章「監査ファイルとエラーファイルの理解」](#)では、ログレベルの設定方法、ログファイルの表示方法と理解方法、およびディレクトリソースの状態を含む、監査ログおよびエラーログについて説明します。
- [付録A「Identity Synchronization for Windows コマンド行ユーティリティーの使用」](#)では、さまざまな作業を実行するコマンド行を使用する方法について説明します。
- [付録B「Identity Synchronization for Windows LinkUsers XML ドキュメントの例」](#)では、配備をカスタマイズするために使用できる Linkusers XML 設定ファイルの例について説明します。
- [付録C「Solaris 上での root 以外での Identity Synchronization for Windows サービスの実行」](#)では、Solaris オペレーティングシステムで Identity Synchronization for Windows サービスを root 以外のユーザーとして実行する方法について説明します。
- [付録D「Identity Synchronization for Windows の同期ユーザーリストの定義と設定」](#)では、同期ユーザーリストおよび複数ドメイン構成について説明します。

- 付録E 「レプリケートされた環境での Identity Synchronization for Windows のインストールの注意点」では、マルチマスターレプリケーション配備を設定およびセキュリティ保護するために必要な手順の概要について説明します。

Directory Server、Directory Proxy Server、および Directory Server Resource Kit をインストールする方法については、パートI 「Directory Service Control Center、Directory Proxy Server、Directory Server、および Directory Server Resource Kit のインストール」を参照してください。

製品の理解

Sun Java™ System Identity Synchronization for Windows 6.0 は、Sun Java System Directory Server と次の間で双方向のパスワードおよびユーザー属性の同期を提供します。

- Windows 2000 または Windows 2003 Server Active Directory
- Windows NT SAM レジストリ

Identity Synchronization for Windows 6.0 では、Sun Java System Directory Server 6.3、6.2、6.1、6.0、および 5.2 Patch 5 をサポートします。

Sun Java System Identity Synchronization for Windows では、次のような方法で同期イベントを処理します。

- 安全に。パスワードを平文で送信しません。また、システムへのアクセスは管理者のみに制限されています。
- 強固に。個々のコンポーネントが一時的に利用できないときでも、ディレクトリは同期状態が維持されます。
- 効率よく。ディレクトリサーバーへの負荷がほとんどない同期方式が使用されます。

Sun Java System Identity Synchronization for Windows バージョン 6.0 をインストール (または移行) する前に、この章で説明する概念を理解しておくことをお勧めします。この章は次の節で構成されます。

- 96 ページの「製品の特徴」
- 97 ページの「システムコンポーネント」
- 103 ページの「システムコンポーネントの分散」
- 106 ページの「Identity Synchronization for Windows がディレクトリソースでの変更を検出する方法」
- 112 ページの「配備の例: 2 台のマシン構成」

製品の特徴

Sun Java System Identity Synchronization for Windows では、次の特徴および機能を備えています。

- パスワードの双方向同期。次のディレクトリソース間でユーザーパスワードを同期できます。
 - Sun Java System Directory Server と Windows Active Directory
 - Sun Java System Directory Server と Windows NT

パスワードを同期すると、ユーザーはログイン認証でこれらのディレクトリソースを使用するアプリケーションにアクセスできるため、ユーザーが覚えるパスワードは1つだけで済みます。また、ユーザーが定期的にパスワードを更新する必要がある場合でも、パスワードを更新するのは1箇所だけです。

- ユーザー属性の双方向同期。あるディレクトリ環境で選択された属性を作成、変更、および削除して、その値をほかのディレクトリ環境に自動的に伝播させることができます。
- ユーザーアカウント作成の双方向同期。あるディレクトリ環境でユーザーアカウントを作成または削除して、その新しいアカウントをほかのディレクトリ環境に自動的に伝播させることができます。
- グループの双方向同期。グループの作成や削除を同期したり、Directory Server ソースと Active Directory ソースの間でそのグループとユーザーの関連付けまたは関連付け解除を行ったりすることができます。
- オブジェクトの双方向の削除、有効化、および無効化。Directory Server ソースと Active Directory ソースの間でオブジェクトの削除、有効化、および無効化のフローを制御できます。
- アカウントのロックアウトおよびロックアウト解除の双方向同期。Directory Server ソースと Active Directory ソースの間でアカウントのロックアウトおよびロックアウト解除を同期できます。
- 複数ドメインとの同期。複数の Active Directory ドメイン、複数の Windows NT ドメイン、および複数の Active Directory フォレストと同期できます。
- システムの集中監査。インストールおよび構成の状態、毎日のシステム運用、および配備関連のエラー状況を1箇所の中央の場所から監視できます。

Windows ディレクトリのエントリを変更したり、ディレクトリを使用してアプリケーションを変更したりする必要はありません。

Directory Server と Active Directory の間で同期するために Identity Synchronization for Windows を使用している場合は、Windows オペレーティングシステムにコンポーネントをインストールする必要はありません。

Directory Server と Windows NT の間で同期している場合は、Windows NT オペレーティングシステムにこの製品の NT コンポーネントをインストールしてください。

注 - Windows NT では次の機能を利用できません。

- グループの双方向同期
- オブジェクトの双方向の削除、有効化、無効化
- アカウントのロックアウトおよびロックアウト解除の双方向同期

システムコンポーネント

次の図に示すように、Identity Synchronization for Windows は一連のコアコンポーネント、および任意の数の個々のコネクタとコネクタサブコンポーネントで構成されます。これらのシステムコンポーネントは、Sun Java System Directory Server (Directory Server) ディレクトリと Windows ディレクトリの間でパスワードおよびユーザー属性の更新を同期することに対応しています。

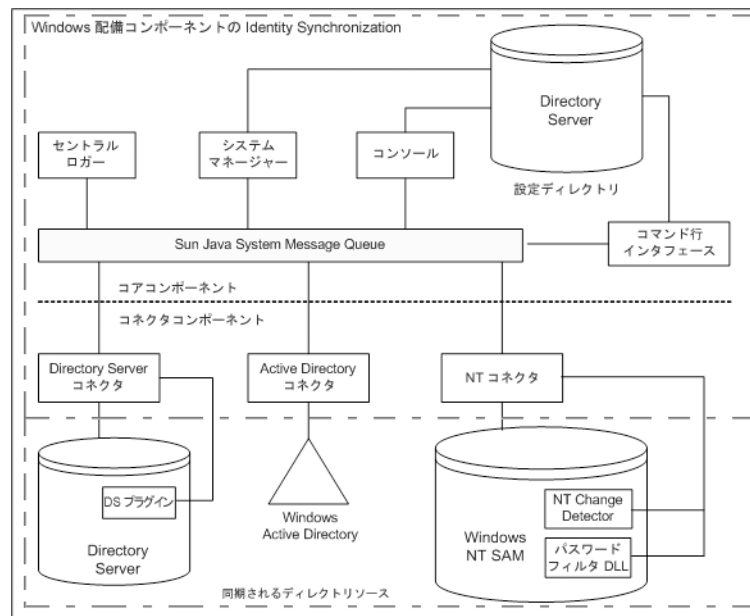


図 3-1 システムコンポーネント

この節では、これらの Identity Synchronization for Windows コンポーネントについて定義し、説明します。

- 98 ページの「ウォッチドッグプロセス」
- 98 ページの「コア」

- 101 ページの「コネクタ」
- 101 ページの「コネクタサブコンポーネント」
- 102 ページの「Message Queue」

ウォッチドッグプロセス

ウォッチドッグとは、個々のバックグラウンド Java プロセスを起動、再起動、および停止する、Identity Synchronization for Windows Java テクノロジベースのプロセス (Java プロセス) です。ウォッチドッグは、セントラルロガー、システムマネージャー、およびコネクタを起動および監視します。ウォッチドッグは、サブコンポーネント、Message Queue、または Identity Synchronization for Windows コンソールを監視しません。

ウォッチドッグは、コアコンポーネントをインストールした場所にインストールされ、Solaris™ ソフトウェアデーモン、Red Hat Linux デーモン、または Windows サービスとして起動できます。

コア

Identity Synchronization for Windows をインストールするときは、先にコアコンポーネントをインストールしてから、使用している環境に合わせて設定します。

コアコンポーネントは、次のコンポーネントで構成されます。

- 98 ページの「設定ディレクトリ」
- 99 ページの「コンソール」
- 99 ページの「コマンド行ユーティリティ」
- 100 ページの「システムマネージャー」
- 100 ページの「セントラルロガー」

設定ディレクトリ

Identity Synchronization for Windows は、自身の設定データを Directory Server の設定ディレクトリに格納します。設定ディレクトリはインストールされません。

コンソール、システムマネージャー、コマンド行ユーティリティ、およびインストーラのいずれも、次のような製品の設定データを設定ディレクトリで読み書きします。

- 各コンポーネントの健全性に関するインストール情報
- ディレクトリ、ドメイン、コネクタ、およびディレクトリサーバープラグインの設定情報
- コネクタの状態
- ユーザーやグループの作成、削除、および属性変更の指示を記述した同期設定

- 同期される属性および Active Directory と Directory Server の間、または Windows NT と Directory Server の間の属性マッピング
- 各ディレクトリトポロジでの同期ユーザーリスト (SUL)
- ログ設定

コンソール

Identity Synchronization for Windows では、製品コンポーネントの設定および管理タスクのすべてを集中化するコンソールを提供しています。

コンソールを使用すると、次の操作を実行できます。

- 同期されるディレクトリソースを設定する
- パスワードだけでなく、同期されるユーザーエントリ属性のマッピングを定義する
- ディレクトリまたはドメイントポロジ内のユーザーおよび属性を同期の対象または対象外として指定する
- システム状態を監視する
- 同期を開始および停止する

コマンド行ユーティリティー

Identity Synchronization for Windows では、次のタスクをコマンド行から直接実行できるようにするコマンド行ユーティリティーも提供します。

- 設定および SSL (Secure Sockets Layer) 設定に基づいて証明書情報を表示する
- Identity Synchronization for Windows の設定パスワードを変更する
- 指定された Directory Server ソースについてディレクトリサーバープラグインを設定する
- Sun Java System Directory Server ソースを Identity Synchronization for Windows で使用できるように準備する
- インストールまたは設定プロセスを完了させるために必要な手順を表示したり、インストール済みのコネクタ、システムマネージャー、および Message Queue の状態を表示したりする
- 設定ディレクトリでのコネクタの状態をアンインストール済みにリセットする
- インストールプロセスの一環として、2つのディレクトリで既存のユーザーを同期およびリンクしたり、ディレクトリを事前に生成したりする
- アカウントのロックアウトを有効または無効にする
- グループの同期を有効または無効にする
- 同期を開始および停止する

製品のコマンド行ユーティリティーの詳細とその使用方法については、付録 A 「Identity Synchronization for Windows コマンド行ユーティリティーの使用」を参照してください。

システムマネージャー

Identity Synchronization for Windows システムマネージャーは、次の処理を実行する独立した Java プロセスです。

- 製品のバックエンドのネットワーク機能を利用して、コネクタに設定の更新を動的に配信する
- 各コネクタとコネクタのすべてのサブコンポーネントについて状態を維持する
- 2つのディレクトリを最初に同期するときに使用される `idsync resync` 処理を調整する

セントラルロガー

コネクタは、遠隔の地域に広く分散されるようにインストールできます。そのため、すべてのロギング情報を集中化することには、管理上大きな価値があります。このように集中化することで、管理者は同期アクティビティーを監視したり、エラーを検出したり、システム全体の健全性を評価したりすることが一箇所から行えるようになります。

管理者は、セントラルロガーのログを使用して、次のようなタスクを実行できます。

- システムが正常に実行していることを検証する
- 個々のコンポーネントやシステム全体の問題を検出して解決する
- 個々またはシステム全体の同期アクティビティーを監査する
- ディレクトリソース間でユーザーのパスワードの同期を追跡する

ログの種類には、次の2種類があります。

- 監査ログ。システムの毎日のアクティビティーに関する情報を提供します。ユーザーのパスワードがディレクトリ間で同期されるといったイベントが含まれます。監査ログに記録される情報のレベルを制御するには、ログメッセージで提供される詳細度を増減させます。
- エラーログ。深刻なエラーおよび警告であるとみなされる状況に関する情報が提供されます。エラーログのすべてのエントリは注目に値するため、エラーが記録されないようにすることはできません。エラー状況が発生すると、必ずエラーログに記載されます。

注 - Identity Synchronization for Windows では、すべてのエラーログメッセージが監査ログにも書き込まれるため、ほかのイベントとの相関性がわかりやすくなります。

コネクタ

コネクタは、単一のデータソースタイプでの同期プロセスを管理する Java プロセスです。コネクタは、データソースでユーザーによる変更を検出し、Message Queue を介してこれらの変更をリモートコネクタに発行します。

Identity Synchronization for Windows では、次のディレクトリ固有のコネクタを提供します。これらのコネクタは、ディレクトリやドメイン間でユーザー属性およびパスワード更新を双方向に同期します。

- **ディレクトリサーバーコネクタ**。Directory Server の単一ルートサフィックス (たとえば、サフィックス/データベース) をサポートします。
- **Active Directory コネクタ**。Windows 2000 または Windows 2003 Server Active Directory ソースの単一インスタンスをサポートします。複数のコネクタを使用することで追加ドメインに対応できます。
- **Windows NT コネクタ**。Windows NT の単一ドメインをサポートします。

注-ウォッチドッグは、コネクタをインストールした場所にインストールされ、コネクタを起動、再起動、および停止します。詳細については、[98 ページの「ウォッチドッグプロセス」](#)を参照してください。

コネクタサブコンポーネント

サブコンポーネントは、コネクタとは独立して実行される軽量プロセスまたはライブラリです。コネクタは、Directory Server や Windows NT の内部でパスワードを収集するといった遠隔からアクセスできないネイティブリソースにアクセスするためにサブコンポーネントを使用します。

次のコネクタサブコンポーネントは、同期されるディレクトリで設定またはインストールされ、暗号化された接続を介して対応するコネクタと通信します。

- [101 ページの「ディレクトリサーバープラグイン」](#)
- [102 ページの「Windows NT コネクタサブコンポーネント」](#)

注- Active Directory コネクタは、サブコンポーネントを必要としません。

ディレクトリサーバープラグイン

ディレクトリサーバープラグインは、ディレクトリサーバーコネクタのサブコンポーネントです。同期される Directory Server ごとにディレクトリサーバープラグインを設定します。

このプラグインには、次の機能があります。

- 旧バージョン形式の更新履歴ログに暗号化されたパスワードを格納して、ディレクトリサーバーコネクタの変更検出機能を拡張する
- Active Directory と Directory Server の間のユーザー属性およびパスワードの同期について、双方向サポートを提供する (109 ページの「オンデマンドパスワード同期を使用した平文パスワードの取得」を参照)

注 - これまで Identity Synchronization for Windows では、2 方向のマルチマスターレプリケーション (MMR) のみをサポートしていました。これからは N 方向の MMR 環境でもディレクトリサーバープラグインが機能します。

Windows NT コネクタサブコンポーネント

使用しているインストールで Windows NT SAM レジストリとの同期が必要な場合は、Identity Synchronization for Windows のインストールプログラムによって、Windows NT コネクタとともに次の項目がプライマリドメインコントローラ (PDC) にインストールされます。

- 変更検出機能。セキュリティログを監視してユーザーエントリやパスワードの変更イベントを検出して、その変更をコネクタに渡します。
- パスワードフィルタ DLL。Windows NT ドメインコントローラで行われたパスワードの変更を収集して、安全に NT コネクタに渡します。

Message Queue

Identity Synchronization for Windows では、パブリッシュ/サブスクライブモデルの持続的なメッセージキューメカニズムである Sun Java System Message Queue (Message Queue) を使用して、属性およびパスワードの変更をディレクトリソース間で伝播させます。Message Queue は、ディレクトリソースの同期を管理するコネクタに対して、管理情報および設定情報も配信します。

Message Queue は、Java Message Service オープン標準を実装した企業向けのメッセージングシステムです。この仕様では、Java アプリケーションが分散環境でメッセージを作成、送信、受信、および読み取る共通の方法を提供する、一連のプログラミングインタフェースを記述しています。

Message Queue は、共通のメッセージサービスを使用してメッセージを交換するメッセージの発行元とサブスクライバで構成されます。このサービスは、1 つ以上の専用のメッセージブローカから成ります。メッセージブローカはメッセージキューへのアクセス制御、アクティブな発行元およびサブスクライバに関する情報の維持、およびメッセージが配信されたことの確認を行います。

Message Queue は次の処理を行います。

- コネクタ間の信頼関係を確立する

- すべてのコンポーネントのセキュリティーアクセス制御を単純化する
- エンドツーエンドでのパスワード暗号化を容易にする
- すべてのパスワード更新メッセージが確実に配信されるようにする
- コネクタ間通信での複雑さやセキュリティーリスクを低減する
- 中央当局が設定情報を配布できるようにする
- 集中化された場所ですべてのコネクタログの集約に対応できるようにする

システムコンポーネントの分散

効果的に配備を開発する前に、Identity Synchronization for Windows コンポーネントの編成と製品の動作について理解します。この節の内容は次のとおりです。

- [103 ページの「コア」](#)
- [103 ページの「ディレクトリサーバーコネクタおよびプラグイン」](#)
- [104 ページの「Active Directory コネクタ」](#)
- [105 ページの「Windows NT コネクタおよびサブコンポーネント」](#)

この節および[112 ページの「配備の例: 2 台のマシン構成」](#)で説明する基本概念を理解するにあたって、より複雑で高度なシナリオに対する配備戦略を作成するための情報を推測できるようにしてください。そのようなシナリオには、Active Directory と Windows NT の混在環境やマルチサーバー環境などがあります。

コア

注 – Sun Java System Message Queue 3.6 Enterprise Edition は、コアをインストールする予定のマシンと同じマシンにインストールしてください。

サポートされるオペレーティングシステムのディレクトリサーバーのいずれかに、すべてのコアコンポーネントを1回だけインストールします。Identity Synchronization for Windows では、管理サーバーがマシンにインストールされていない場合はインストールされます。

ディレクトリサーバーコネクタおよびプラグイン

ディレクトリサーバーコネクタは、サポートされるオペレーティングシステムのいずれにでもインストールできます。ディレクトリサーバーコネクタは、同期される Directory Server が実行されているマシンと同じマシンにインストールする必要はありません。ただし、設定された Directory Server ソースごとにディレクトリサーバーコネクタを1つインストールします。

同期される Directory Server が存在するホストごとにディレクトリサーバープラグインを設定してください。

注 - Directory Server ソースごとに1つのディレクトリサーバーコネクタがインストールされます。ただし、ディレクトリサーバープラグインは同期される各マスター、ハブ、コンシューマレプリカに対して設定するようにしてください。

Active Directory コネクタ

Active Directory コネクタは、サポートされるオペレーティングシステムのいずれにでもインストールできます。Windows を実行しているマシンに Active Directory コネクタをインストールする必要はありません。ただし、Active Directory ドメインごとに Active Directory コネクタを1つインストールしてください。コンポーネントの分散例については、次の図を参照してください。

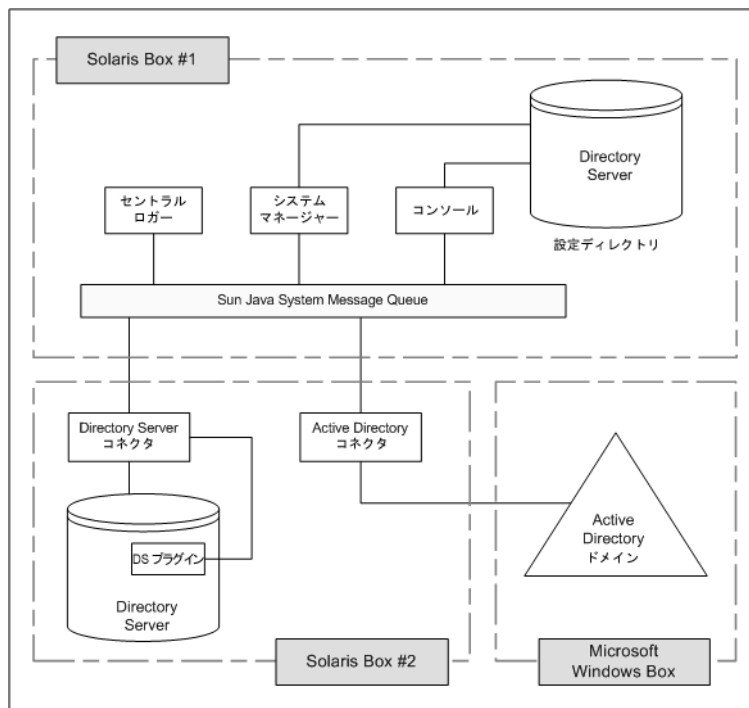


図 3-2 Directory Server および Active Directory のコンポーネントの分散

Windows NT コネクタおよびサブコンポーネント

Windows NT SAM レジストリと同期するには、Windows NT コネクタをプライマリドメインコントローラ (PDC) にインストールしてください。NT ドメインの PDC には、コネクタのほかに変更検出機能 およびパスワードフィルタ DLL という 2 つの NT コネクタサブコンポーネントもインストールプログラムによってインストールされます。1 つの NT コネクタは、1 つの NT ドメインに対してユーザーとパスワードを同期します。コンポーネントの分散例については、次の図を参照してください。

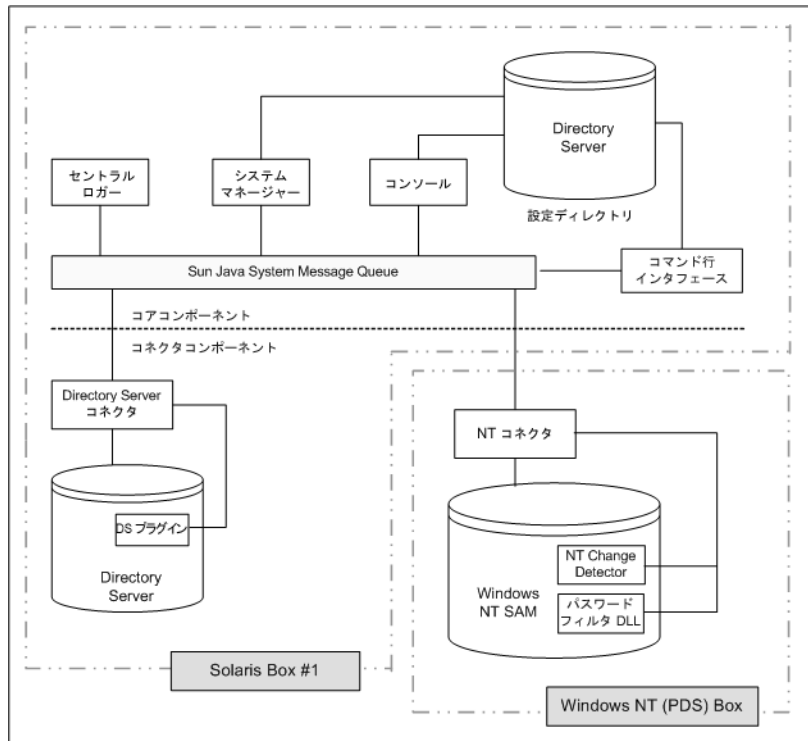


図 3-3 Directory Server と Windows NT のコンポーネントの分散

Identity Synchronization for Windows がディレクトリソースでの変更を検出する方法

この節では、ユーザーエン트리およびパスワードの変更が Sun Java System Directory Server (Directory Server)、Windows Active Directory、および Windows NT のコネクタによって検出される方法について説明します。

ここで説明する内容は、次のとおりです。

- 106 ページの「ディレクトリサーバーコネクタが変更を検出する方法」
- 107 ページの「Active Directory コネクタが変更を検出する方法」
- 108 ページの「Windows NT コネクタが変更を検出する方法」
- 109 ページの「パスワード更新の伝播」
- 111 ページの「信頼できる同期」

ディレクトリサーバーコネクタが変更を検出する方法

ディレクトリサーバーコネクタは、Directory Server の旧バージョン形式の更新履歴ログを LDAP を介して検証し、ユーザーエン트리およびパスワードの変更イベントを検出します。ディレクトリサーバープラグインを使用すると、コネクタは次の処理を実行できます。

旧バージョン形式の更新履歴ログの詳細については、『[Sun Java System Directory Server Enterprise Edition 6.3 Reference](#)』の「[Replication and the Retro Change Log Plug-In](#)」を参照してください。

- 平文パスワードを暗号化して旧バージョン形式の更新履歴ログで利用できるようにするために、平文パスワードを収集する。プラグインのない状態では、ハッシュされたパスワードだけが旧バージョン形式の更新履歴ログに記録されています。ハッシュされたパスワードは同期できません。
- Active Directory との オンデマンドパスワード同期を実行する。Identity Synchronization for Windows コンポーネントを Windows トポロジにインストールする必要はありません (109 ページの「[オンデマンドパスワード同期を使用した平文パスワードの取得](#)」を参照)。

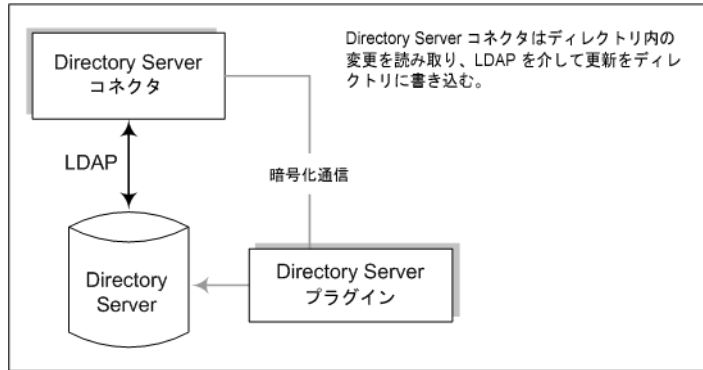


図 3-4 ディレクトリサーバーコネクタが変更を検出する方法

Active Directory コネクタが変更を検出する方法

Windows 2000/2003 Server Active Directory コネクタは、Active Directory USNChanged および PwdLastSet 属性値を検証してユーザーエントリおよびパスワードの変更を検出します。

Directory Server の旧バージョン形式の更新履歴ログとは異なり、エントリで属性を変更しても、Active Directory は変更された属性を報告しません。代わりに、Active Directory では USNchanged 属性の増加させることでエントリの変更を識別します。個々の属性に対する変更を検出するために、Active Directory コネクタはオブジェクトキャッシュと呼ばれるインプロセスデータベースを使用します。オブジェクトキャッシュは、各 Active Directory エントリのハッシュされたコピーを格納し、コネクタがエントリで変更された属性を正確に判断できるようにします。

Active Directory コネクタを Windows にインストールする必要はありません。これらのコネクタは、Solaris や Red Hat Linux などほかのオペレーティングシステム上でも実行でき、LDAP を介して遠隔から変更を加えたり検出したりすることができます。

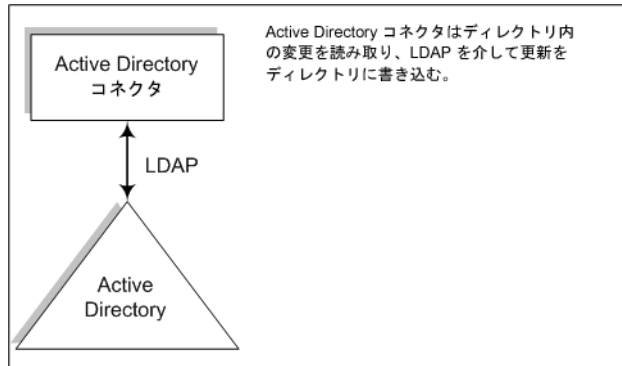


図 3-5 Active Directory コネクタが変更を検出する方法

Windows NT コネクタが変更を検出する方法

Windows NT コネクタは、ユーザーオブジェクトに関する監査イベントのセキュリティローグを検証してユーザーエン트리およびパスワードの変更を検出します。監査は有効にしてください。有効にしない場合、Identity Synchronization for Windows で Windows NT マシンからのログメッセージを読み取れません。監査ログの記録が有効であることを確認するには、[280 ページの「Windows NT マシンでの監査の有効化」](#)を参照してください。

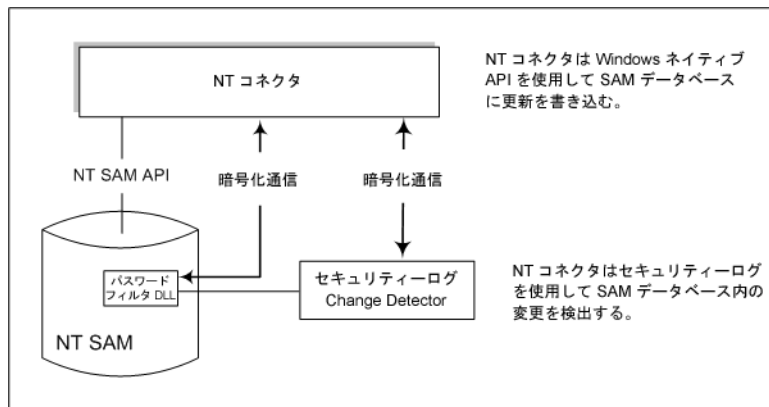


図 3-6 Windows NT コネクタが変更を検出する方法

変更検出機能およびパスワードフィルタ DLL のサブコンポーネントの説明については、[102 ページの「Windows NT コネクタサブコンポーネント」](#)を参照してください。

パスワード更新の伝播

この節では、平文パスワードを取得する2つの方法について説明します。平文パスワードは、Windows ソースと Directory Server ソースとの間でパスワードの変更を伝播させるために必要です。

パスワードフィルタ DLL を使用した平文パスワードの取得

Windows NT コネクタは、Sun Java System Directory Server にパスワードの更新を伝播させるために平文パスワードを取得する必要があります。ただし、Windows ディレクトリから平文パスワードを抽出することはできません。パスワードがディレクトリに格納される時点で、すでにパスワードは暗号化されています。

Windows NT では、ディレクトリに永続的に格納される前に平文パスワードをコンポーネントが収集できるようにするパスワードフィルタ DLL インタフェースを提供します。

オンデマンドパスワード同期を使用した平文パスワードの取得

Active Directory では、Windows NT と同じパスワードフィルタをサポートしていますが、Windows NT で使用されるプライマリドメインコントローラではなく各ドメインコントローラにパスワードフィルタ DLL をインストールしてください。これは、インストールでの過大な負担となる可能性があるため、Identity Synchronization for Windows ではオンデマンドパスワード同期と呼ばれる別の手法を使用して、パスワードの変更を Active Directory から Directory Server に同期します。

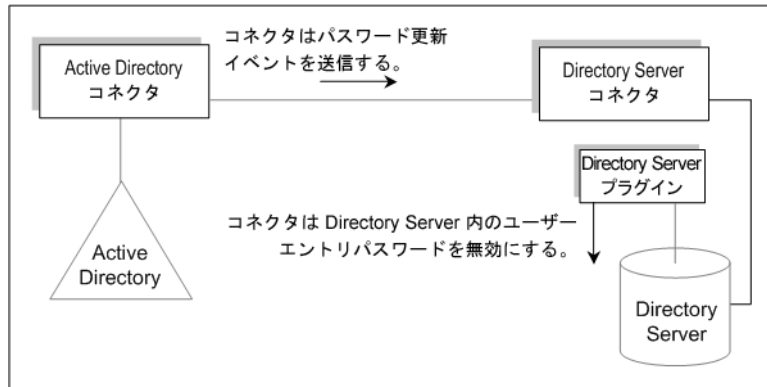
オンデマンドパスワード同期では、ユーザーが Windows 2000/2003 でパスワードを変更したあとでログインを試みたときに Directory Server 上で新しいパスワードの値を取得するための方法が提供されます。

また、パスワードフィルタ DLL を使用せずに Active Directory 上でパスワードを同期することもできます。

オンデマンドパスワード同期のプロセスは次のとおりです。

1. ユーザーは、Windows を実行しているマシンで Ctrl-Alt-Del を押し、自分のパスワードを変更します。新しいパスワードが Active Directory に格納されます。
2. Active Directory コネクタは、スケジュールされた間隔でシステムをポーリングします。

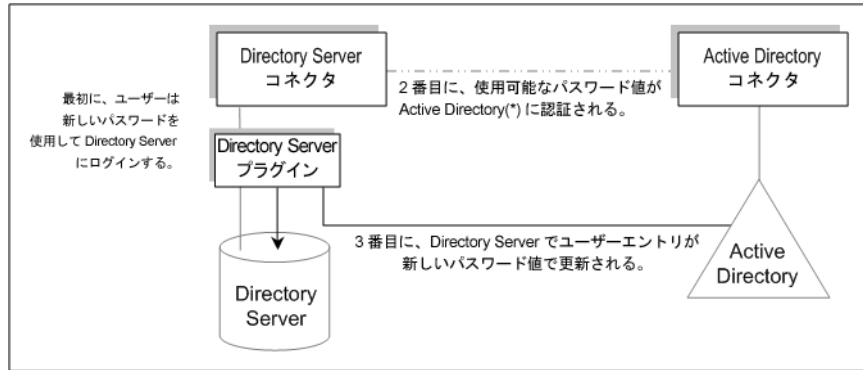
コネクタは、USNchanged (Update Sequence Number) および PwdLastSet 属性に対する変更に基づいてパスワードの変更を検出すると、パスワードの変更に関するメッセージを Message Queue に発行します。メッセージは、SSL 暗号化チャネル上を転送されます。



3. ディレクトリサーバーコネクタは、SSL を介して Message Queue からパスワードの変更メッセージを受信します。
4. ディレクトリサーバーコネクタは、ユーザーエントリの `dspswvalide` 属性を `true` に設定します。これにより、古いパスワードは無効になり、パスワードの変更がディレクトリサーバープラグインに通知されます。
5. ユーザーがログインを試みると、Sun Java System ディレクトリサーバープラグインは、Directory Server に対して認証を求める LDAP アプリケーション (Portal Server など) を使用して、Directory Server エントリのパスワードの値が無効であることを検出します。
6. ディレクトリサーバープラグインは、Active Directory で対応するユーザーを検索します。プラグインは、ユーザーが見つかったとき、ユーザーが Directory Server へのログインを試みたときに入力されたパスワードを使って、Active Directory へのバインドを試みます。

注- オンデマンドパスワード同期では、Directory Server に対してアプリケーションで SASL Digest-MD5 などのより複雑な認証メカニズムを使用する代わりに、単純認証を使用する必要があります。

7. Active Directory に対するバインドに成功すると、ディレクトリサーバープラグインは、パスワードを設定し、Directory Server 上のユーザーエントリから無効なパスワードフラグを取り除いて、ユーザーがログインできるようにします。



注 - ユーザー認証に失敗すると、ユーザーエントリのパスワードは Directory Server に残り、Directory Server および Active Directory 上のパスワードは、ユーザーが有効なパスワードでログインするまで一致しません。有効なパスワードは、Active Directory に対して認証されたパスワードです。

信頼できる同期

Identity Synchronization for Windows では、コンポーネントが一時的に利用不可になった場合にもユーザーの変更イベントを確実に逃さないように多くの予防策をとっています。Identity Synchronization for Windows の信頼性は、TCP ネットワークプロトコルに似ています。TCP は、緩く断続的に接続されたネットワークであっても、最終的にすべてのデータが正常に配信されることを保証しています。一時的なネットワーク停止中に送信されたデータは、ネットワークがダウンしている間はキューに入れられ、接続が復元してから再配信されます。Identity Synchronization for Windows は、次のいずれかのコンポーネントが一時的に利用不可になっても、ユーザーの変更イベントを最終的に検出して適用します。

- コネクタ
- Directory Server
- Message Queue
- Active Directory ドメインコントローラ
- Windows NT プライマリドメインコントローラ
- システムマネージャー
- 設定ディレクトリ

これらのコンポーネントのいずれかが利用できなくなると、Identity Synchronization for Windows では、影響を受けるコンポーネントが利用できるようになってパスワードを始めとするすべての変更を含むようになるまで同期を遅らせます。このバージョンの Identity Synchronization for Windows では、Sun™ Cluster ソフトウェアやその他の真の高可用性ソリューションをサポートしません。ユーザーは Identity

Synchronization for Windows と直接対話しないため、高可用性は通常必要ありません。壊滅的な失敗が発生した場合は、Identity Synchronization for Windows コンポーネントを再インストールし、idsync resync コマンドを使用してすべてのディレクトリソースを再同期できます。

ほとんどの状況では、コンポーネントが利用できなくなると、同期イベントがキューに入れられ、コンポーネントが利用可能になったときだけ同期イベントが適用されます。このプロセスには、2つの例外があります。

- マルチマスターレプリケーション (MMR) の Directory Server 環境では、Windows ユーザーに対する外部の変更を優先または副 Directory Server に対して同期できません。
優先ディレクトリサーバーを利用できない場合、Directory Server コレクタは MMR トポロジから利用可能な副サーバーのいずれかに変更を適用します。
- Active Directory コネクタは、1 台の Active Directory ドメインコントローラのみと通信できますが、ディレクトリサーバープラグインはオンデマンドパスワード同期の実行中にすべての Active Directory ドメインコントローラ間で失敗することがあります。フェイルオーバーが最も重要なのはこのためです。ディレクトリサーバープラグインがユーザーの新しいパスワードを検証するために Active Directory ドメインコントローラに接続できない場合、ユーザーは Directory Server にログインできません。

配備の例: 2 台のマシン構成

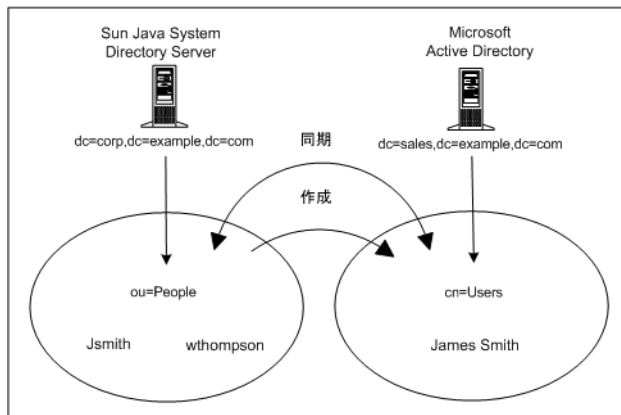
この節では、Identity Synchronization for Windows がユーザーオブジェクトの作成および双方向のパスワード変更操作を Directory Server ソースと Active Directory ソースの間で同期するとき使用する配備シナリオについて説明します。

この配備シナリオは、2 台のマシンで構成されます。

- Sun Java System Directory Server を実行しているマシン (ホスト名: corp.example.com)
- Windows 2000 Server で Active Directory を実行しているマシン (ホスト名: sales.example.com)

注 - このシナリオでは Windows NT を使用していませんが、Identity Synchronization for Windows では NT ドメインとの同期もサポートしています。

この配備シナリオで使用される同期の要件 (ノード構造と関連の属性値) を次の図に示します。



このシナリオでは、次のような2つの目標があります。

- ユーザーのパスワードをユーザーサブツリー (Directory Server では ou=people、Active Directory では cn=users) 間で双方向に同期すること。つまり、ユーザーのパスワードが一方のディレクトリで変更されると、他方のディレクトリで関連ユーザーにパスワードの変更が同期されます。

たとえば Directory Server で ou=people コンテナの uid=Jsmith のパスワードを変更すると、新しいパスワードは Active Directory で cn=users コンテナの cn=James Smith に自動的に同期されます。

- ユーザーオブジェクトの作成操作を Directory Server ピープルサブツリーから Active Directory ユーザーサブツリーへの方向のみで同期すること。

たとえば指定された一連の属性で新しいユーザー uid=WThompson を ou=People コンテナに作成する場合、Identity Synchronization for Windows は Active Directory で同じ属性を使用して新しいアカウント cn=William Thompson を cn=Users コンテナに作成します。

注 - Identity Synchronization for Windows では、同じタイプの複数の同期ソースをサポートします。たとえば配備や複数の Active Directory ドメインで複数の Directory Server を使用できます。

作成、変更、および削除の同期設定は、ディレクトリの全体でグローバルであり、個々のディレクトリソースに対して指定することはできません。ユーザーオブジェクトの作成を Directory Server から Active Directory へ同期する場合、すべての Directory Server からインストール時に設定したすべての Active Directory ドメインや Windows NT ドメインにユーザーオブジェクトの作成が伝播します。

物理的な配備

すべての製品コンポーネントを単一の Solaris システム上に物理的に配備して、Active Directory ドメインはコンポーネントがインストールされていない別の Active Directory ドメインコントローラに配置した様子を次の図に示します。

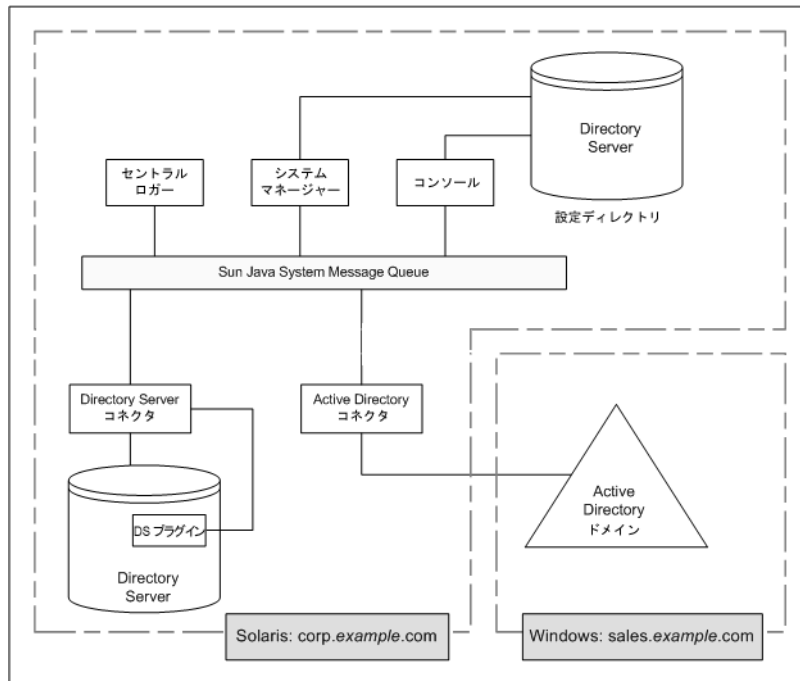


図 3-7 Directory Server および Active Directory のシナリオ

コンポーネントの分散

corp.example.com は、Solaris オペレーティングシステム上に Directory Server をインストールしたマシンです。同期される Directory Server インスタンスのルートサフィックスは dc=corp,dc=example,dc=com です。

このトポロジは次を含みます。

- Identity Synchronization for Windows コアコンポーネント
- Identity Synchronization for Windows ディレクトリサーバーコネクタ
- Identity Synchronization for Windows ディレクトリサーバープラグイン

- Identity Synchronization for Windows 設定ディレクトリ (同期される Directory Server インスタンスとは別の Directory Server インスタンス上にある)
sales.example.com は、同期される Active Directory ドメインです。

◆◆◆ 第 4 章

インストールの準備

Identity Synchronization for Windows 6.0 をインストールする前、または Sun Java System Identity Synchronization for Windows 1 2004Q3 SP1 からバージョン 6.0 に移行する前に、インストールおよび設定プロセスを理解してください。

Identity Synchronization for Windows のインストール要件については、『[Sun Java System Directory Server Enterprise Edition 6.3 リリースノート](#)』の第 5 章「[Identity Synchronization for Windows の修正されたバグと既知の問題点](#)」を参照してください。

Identity Synchronization for Windows は、フランス語、ドイツ語、スペイン語、日本語、韓国語、簡体字中国語、繁体字中国語でインストールすることもできます。すべての言語が同じ配布にバンドルされています。

Identity Synchronization for Windows で多言語をサポートする場合は、UTF-8 エンコーディングを使用してください。

この章の内容は次のとおりです。

- 118 ページの「インストールの概要」
- 123 ページの「設定の概要」
- 127 ページの「Active Directory とのパスワードの同期」
- 133 ページの「SSL 動作のための Windows の設定」
- 134 ページの「インストールおよび設定の決定」
- 137 ページの「インストールチェックリスト」

インストールの概要

この節では、Identity Synchronization for Windows の単一ホストインストール手順について説明します。

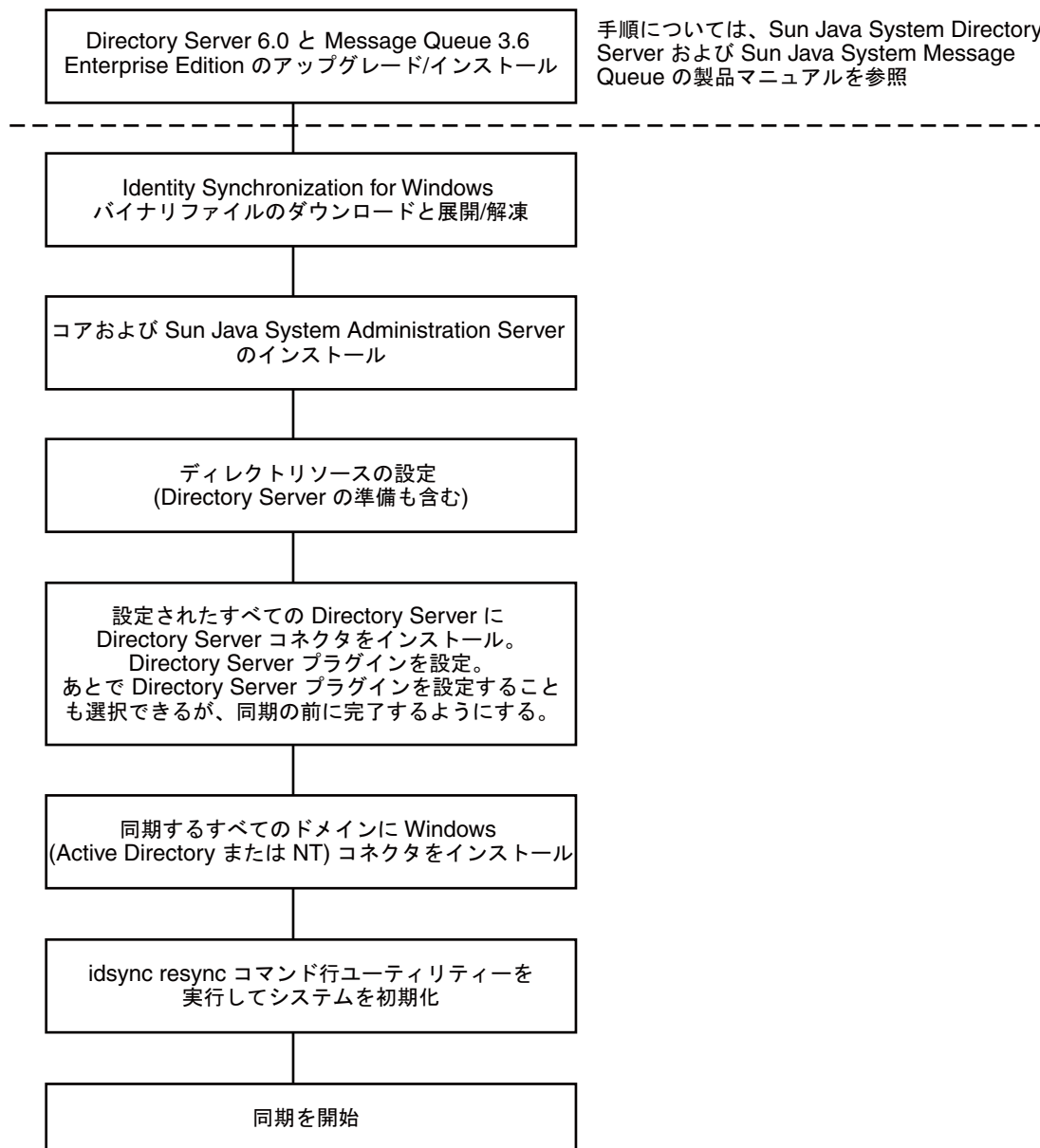


図 4-1 単一ホストインストール手順

一部のコンポーネントは、特定の順序でインストールします。そのため、すべてのインストール手順を注意深く読むようにしてください。

Identity Synchronization for Windows には実行手順リストが用意されており、インストールおよび設定プロセスを通して表示されます。この情報パネルには、製品のインストールおよび設定を成功させるために従う必要のあるすべての手順が表示されます。

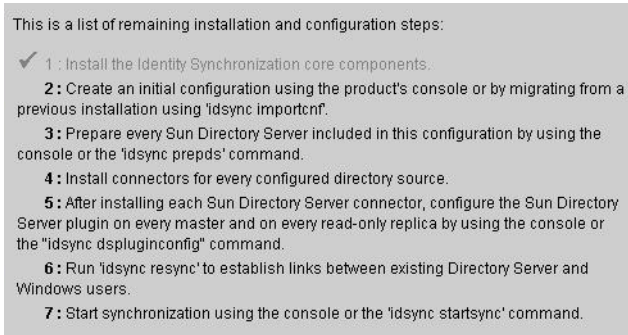


図 4-2 Identity Synchronization for Windows のインストールおよび設定の実行手順リスト

インストールおよび設定のプロセスが進むにつれて、リストで完了したすべての手順が図 6-2 に示すようにグレー表示されます。

この節の残りの部分では、インストールおよび設定のプロセスの概要について説明します。

コアのインストール

コアをインストールすると、次のコンポーネントがインストールされます。

- **Sun Java System Administration Server**。ディレクトリサーバープラグインを設定し、管理フレームワークを提供します。
- **コンソール**。製品コンポーネントの設定および管理タスクのすべてを実行するための、集中化された場所を提供します。
- **セントラルロガー**。中央の場所にすべての監査およびエラーのログ情報を集約します。
- **システムマネージャー**。設定の更新をコネクタに動的に配信し、各コネクタの状態を保守します。
- コアをインストールする手順については、[第5章「コアのインストール」](#)で説明します。

製品の設定

コアをインストールしたらコンソールを使用して、同期されるディレクトリソースなど設備の特性のすべてを集中化された場所から初期設定します。

ディレクトリリソースを設定する手順については、[第6章「コアリソースの設定」](#)を参照してください。

Directory Server の準備

ディレクトリサーバーコネクタをインストールする前に、同期されている優先および副 Directory Server のそれぞれについて Sun Java System Directory Server ソースを準備してください。

このタスクはコンソールから実行することも、`idsync prepds` サブコマンドを使用してコマンド行から実行することもできます。

Directory Server を準備する手順については、[168 ページの「Sun ディレクトリソースの準備」](#)で説明します。

コネクタのインストールおよびディレクトリサーバープラグインの設定

トポロジで設定されているディレクトリの数に応じて、任意の数のコネクタをインストールできます。コンソールとインストールプログラムの両方で、同期されるディレクトリとコネクタを関連付けるためにディレクトリラベルが使用されます。次の表に、ラベルの命名規則を示します。

表 4-1 ラベルの命名規則

コネクタのタイプ	ディレクトリソースのラベル	サブコンポーネント
ディレクトリサーバーコネクタ	ルートサフィックスまたはサフィックス/データベース	ディレクトリサーバープラグイン 同期されているルートサフィックスについて Directory Server (マスターまたはコンシューマ) ごとにプラグインを1つ設定します。
AD コネクタ	ドメイン名	なし

表 4-1 ラベルの命名規則 (続き)

コネクタのタイプ	ディレクトリソースのラベル	サブコンポーネント
NT コネクタ	ドメイン名	Windows NT コネクタとともに自動でインストールされます。Change Detector およびパスワードフィルタ DLL サブコンポーネントが同じインストールと一緒にインストールされます。 Windows NT コネクタは、グラフィカルユーザーインターフェース (GUI) インストーラを使用してインストールしてください。

表 4-2 ラベルの命名例

コネクタ名	ディレクトリソース
CNN100	ou=isw_data1 の SunDS1
CNN101	AD1
CNN102	ou-isw_data2 の SunDS1
CNN103	SunDS2

コネクタをインストールおよび設定する手順については、[第 5 章「コアのインストール」](#)を参照してください。

既存ユーザーの同期

コネクタ、プラグイン、およびサブコンポーネントをインストールしたら、既存ユーザーの配備をブートストラップするために `idsync resync` コマンド行ユーティリティを実行してください。このコマンドは、管理者が指定したマッチングルールを使用して、次の処理を実行します。

- 既存のエントリをリンクする (ユーザーをリンクする詳細については、[233 ページの「ユーザーのリンク」](#)を参照)
- リモートディレクトリの内容で空のディレクトリに生成する
- Windows ディレクトリと Directory Server ディレクトリの両方のエントリが一意に識別されて、相互にリンクされている場合に、2つの既存ユーザーの入力の間でパスワードを含む属性値を一括同期する

配備で既存ユーザーを同期する手順については、[第 8 章「既存のユーザーおよびユーザーグループの同期」](#)を参照してください。

設定の概要

製品をインストールしたら、次の操作を含む製品の配備を設定します。

- 同期されるディレクトリおよびグローバルカタログの設定
- 属性の変更およびオブジェクトの有効化/無効化に関する同期設定の指定
- グループ同期の設定の指定
- アカウントのロックアウトおよびロックアウト解除の同期設定の指定
- (オプション) 設定されたディレクトリ間でユーザーエントリを作成および削除する同期設定の指定

この節では、次の設定要素について概念の概要を説明します。

- ディレクトリ
- 同期設定
- オブジェクトクラス
- 属性および属性マッピング
- 同期ユーザーリスト

注 - 関連する設定手順の一部については、第6章「コアリソースの設定」で説明します。

ディレクトリ

ディレクトリは、次を表します。

- 1つ以上の Sun Java System Directory Server での単一ルートサフィックス (サフィックス/データベース)
- Windows 2000 または Windows 2003 Server Active Directory フォレストでの単一 Active Directory ドメイン
- 単一 Windows NT ドメイン

ディレクトリタイプごとに任意の数を設定できます。

同期設定

同期設定を使用して、オブジェクトの作成、オブジェクトの削除、パスワードなどの属性の変更が Directory Server ディレクトリと Windows ディレクトリの間で伝播する方向を制御します。同期フローオプションは次のとおりです。

- Directory Server から Active Directory/Windows NT
- Active Directory/Windows NT から Directory Server

- 双方向

注 - Active Directory および Windows NT が含まれる設定では、Windows NT と Directory Server の間、および Active Directory と Directory Server の間の作成または変更で、異なる同期設定を指定する設定を保存することはできません。

オブジェクトクラス

リソースを設定するときは、オブジェクトクラスに基づいて同期するエントリを指定します。オブジェクトクラスは、どの属性が Directory Server と Active Directory の両方で同期できるかを決定します。

注 - オブジェクトクラスは、Windows NT には該当しません。

Identity Synchronization for Windows では、2 種類のオブジェクトクラスをサポートします。

- **Structural** オブジェクトクラス。選択された Directory Server から作成または同期される各エントリには、1 つ以上の Structural オブジェクトクラスが必要です。ドロップダウンメニューから Structural オブジェクトクラスを選択します。Directory Server では inetorgperson、Active Directory では User がデフォルトです。
- **Auxiliary** オブジェクトクラス。
 - Directory Server では、選択された構造クラスを拡張するために「利用可能な Auxiliary オブジェクトクラス」リストから 1 つ以上のオブジェクトクラスを選択できます。構造クラスは、同期の追加属性を提供します。
 - Active Directory は、Auxiliary オブジェクトクラスによってさらに限定的になります。選択された Structural オブジェクトクラスで有効なすべての Auxiliary オブジェクトクラスの属性を同期で使用できます。

オブジェクトクラスおよび属性を設定する手順については、[第 6 章「コアリソースの設定」](#)を参照してください。

属性および属性マッピング

属性は、ユーザーエントリを説明する情報を保持します。各属性は、1 つのラベルと 1 つ以上の値があり、属性値として格納可能な情報の種類について標準の構文に従います。

属性はコンソールから定義できます。[第 6 章「コアリソースの設定」](#)を参照してください。

属性タイプ

Identity Synchronization for Windows は、重要および作成ユーザー属性を次のように同期します。

- 重要属性。指定された変更同期設定に従って、属性が変更されたときは常に Directory Server ディレクトリと Windows ディレクトリの間で同期されます。
- 作成属性。指定されたオブジェクト作成同期設定に従って、新しいユーザーが作成されるときは常に Directory Server ディレクトリと Windows ディレクトリの間で同期されます。

必須の作成属性とは、対象ディレクトリで作成アクションを正常に完了するために「必須」であるとみなされる属性です。たとえば、Active Directory では、作成時に `cn` と `samaccountname` の両方が有効な値であることが期待されます。Directory Server では `user` オブジェクトクラスの `inetorgperson` を設定している場合、Identity Synchronization for Windows では、`cn` および `sn` が作成の必須属性であることが期待されます。

元のディレクトリから伝播される属性に値がない場合のみ、作成属性のデフォルトによってデフォルト値で対象ディレクトリの作成属性が更新されます。作成属性のデフォルトは、別の属性値を基にすることができます。[125 ページの「パラメータ化された属性のデフォルト値」](#)を参照してください。

注 - 重要属性は、作成属性として自動的に同期されますが、逆は自動的に同期されません。作成属性は、ユーザー作成時のみ同期されます。

パラメータ化された属性のデフォルト値

Identity Synchronization for Windows では、作成属性に対して別の作成属性または重要属性を使用して、パラメータ化されたデフォルト値を作成できます。

パラメータ化されたデフォルト属性値を作成するには、式文字列で既存の作成属性または重要属性の名前の前後にパーセント記号を付けて囲みます (`%attribute_name%`)。たとえば、`homedir=/home/%uid%` または `cn=%givenName%.%sn%` のようにします。

これらの属性のデフォルト値を作成するときは、次のガイドラインに従ってください。

- 作成式で複数の属性を使用することはできますが (`cn=%givenName%.%sn%`)、`%attribute_name%` の属性は単一の値を持つ必要があります。
- `A=0` の場合、`B` は、デフォルト値 1 つだけを持つことができます。
- パーセント記号を通常の文字として使用する場合は、円記号 (`\%`) を使用します。たとえば `diskUsage=0\%` のようにします。
- 循環式の置換条件を持つ式は使用しないでください (たとえば `sn=%uid%` および `uid=%sn%`)。

属性のマッピング

同期する属性を定義したら、Directory Server と Active Directory/Windows NT システムの間で属性名をマッピングし、相互に属性を同期できるようにします。たとえば Sun の `inetorgperson` 属性を Active Directory の `user` 属性にマッピングします。

重要属性と作成属性の両方で属性マップを使用し、それぞれのディレクトリタイプのすべての「必須の作成属性」で属性マップを設定してください。

同期ユーザーリスト

Directory Server ディレクトリと Windows ディレクトリの両方で同期される特定ユーザーを定義するには、同期ユーザーリスト (SUL) を作成します。これらの定義により、平坦なディレクトリ情報ツリー (DIT) から階層型のディレクトリツリーへの同期が可能になります。

同期ユーザーリストの定義には、次の概念が使用されます。

- ベース DN (Windows NT には該当しない)。別の SUL がより具体的である場合やフィルタによって除外されない場合に、その DN 内のすべてのユーザーが含まれます。
- フィルタ。ユーザーのエントリ内の属性を使用して、ユーザーを同期から除外するか、同じベース DN を持つユーザーを複数の SUL に分割します。このフィルタは、LDAP フィルタ構文を使用します。
- 作成式 (Windows NT には該当しない)。新しいユーザーの作成先 DN を構築します。たとえば `cn=%cn%,ou=sales,dc=example,dc=com` としたときに、`%cn%` は、既存のユーザーエントリの `cn` の値で置換されます。作成式は、ベース DN で終わらせます。

SUL には 2 つの定義が含まれ、それぞれの定義ではディレクトリタイプのトポロジに関連して同期されるユーザーのグループを識別します。

- 一方の定義では、同期される Directory Server ユーザーを識別します (たとえば `ou=people,dc=example,dc=com`)。
- もう一方の定義では、同期される Windows ユーザーを識別します (たとえば `cn=users,dc=example,dc=com`)。

SUL の作成を準備する場合は、次の点を確認してください。

- 同期するユーザー。
- 同期から除外するユーザー。
- 新しいユーザーの作成先。

SUL を作成する詳細については、[付録 D 「Identity Synchronization for Windows の同期ユーザーリストの定義と設定」](#) を参照してください。

Active Directory とのパスワードの同期

Windows 2000 でのデフォルトのパスワードポリシーは Windows 2003 で変更され、強力なパスワードがデフォルトで要求されます。

Identity Synchronization for Windows のサービスでは、たとえば Directory Server から Active Directory に対する `resync -c` の実行時のように、パスワードを持たないエントリの作成が必要なことがあります。したがって、Active Directory (Windows 2000 または 2003 の場合) または Directory Server でパスワードポリシーが有効な場合は、ユーザー作成エラーが発生することがあります。

Active Directory または Directory Server でパスワードポリシーを無効にする必要はありませんが、パスワードポリシーの要求に関連した問題を理解してください。

Windows 2003 Server Standard または Enterprise Edition 上の Active Directory とパスワードを同期する場合は、次のインストールの情報が重要です。

- Windows にインストールする場合は、Active Directory コネクタを Solaris OS、Red Hat Linux、または Windows にインストールできます。

注 - Active Directory コネクタは、Windows 2000 と Windows 2003 Server の両方の Active Directory と連携します。

- Windows 2003 でディレクトリソース、グローバルカタログ、および同期ユーザーリストを作成する手順は、Windows 2000 の Active Directory での手順と同じです。
- Windows Server 2003 では、デフォルトのパスワードポリシーで強力なパスワードが要求されますが、これは Windows 2000 でのデフォルトのパスワードポリシーと異なります。

パスワードポリシーの要求

この節では、Windows 2000、Windows 2003 Server、および Sun Java System Directory Server の Active Directory のパスワードポリシーが同期の結果に与える影響について説明します。

そのトポロジで要求されるパスワードポリシーを満たす Active Directory (または Directory Server) でユーザーを作成する場合は、ユーザーを2つのシステム間で適切に作成および同期することができます。両方のディレクトリソースでパスワードポリシーが有効な場合、パスワードは両方のディレクトリソースのポリシーを満たす必要があります。そうでないと同期されたユーザー作成は失敗します。

- Active Directory でパスワードポリシー機能を有効にする場合は、Directory Server で同様の設定または同一のパスワードポリシーを有効にするようにしてください。

- Active Directory と Directory Server の両方で一貫性のあるパスワードポリシーを作成できない場合は、パスワードおよびユーザー作成で信頼できるソースであるとみなすディレクトリソースでパスワードポリシーを有効にするようにしてください。ただし、一部のパスワードポリシー設定が原因で、ユーザーが想定どおりに作成できないことがあります。

注 - Identity Synchronization for Windows はパスワードの期限切れを同期しません。

この節の内容は次のとおりです。

- [128 ページの「Directory Server のパスワードポリシー」](#)
- [128 ページの「Active Directory パスワードポリシー」](#)
- [129 ページの「パスワードなしのアカウントの作成」](#)
- [132 ページの「パスワードポリシーの例」](#)
- [133 ページの「エラーメッセージ」](#)

Directory Server のパスワードポリシー

Directory Server パスワードポリシーに違反するパスワードを使用して Active Directory でユーザーを作成すると、それらのユーザーは Directory Server で作成および同期されますが、エントリはパスワードなしで作成されます。パスワードは新しいユーザーが Directory Server にログインするまで設定されません(ログインでオンデマンドパスワード同期がトリガーされる)。この時点では、パスワードが Directory Server パスワードポリシーに違反しているため、ログインは失敗します。

この状態から回復するには、次のいずれかを行います。

- Active Directory への次回ログイン時に、ユーザーにパスワードを変更してもらいます。
- Active Directory でユーザーパスワードを変更し、新しいパスワードが Directory Server パスワードポリシーの要件を満たすようにします。

Active Directory パスワードポリシー

Active Directory パスワードポリシーと一致しない Active Directory でユーザーを作成する場合、それらのユーザーは、Directory Server で作成されます。

- Active Directory では、実際にユーザーを「一時的に」作成し、パスワードがパスワードポリシーの要件を満たさない場合にエントリを削除します。従って、Active Directory コネクタはこの一時的な追加を確認して、Directory Server にユーザーを作成します。ユーザーは Directory Server でパスワードを持たないため、そのユーザーとしてはだれもログインできません。また、これらのエントリは Active Directory で有効なエントリにリンクされません。削除が Active Directory から Directory Server へ同期されると、一時的に作成されたユーザーが自動的に削除されます。

- ユーザーは、パスワードなしで Directory Server に作成されます。Directory Server は、エントリにパスワードが含まれていないかぎり、ユーザーの作成でパスワードポリシーを要求しません。

この状況から回復するには、Active Directory から Directory Server へ削除を同期することが推奨されます。または、ユーザーを Directory Server から削除してから、Active Directory パスワードポリシーに従うパスワードを使用して Active Directory にユーザーを追加できます。この方法では確実に、ユーザーが Directory Server で作成されて、適切にリンクされます。Directory Server ユーザーが Active Directory にはじめてログインしてパスワードを変更すると、そのパスワードは無効化されます。
- ユーザーを Directory Server から削除せずに Active Directory ユーザーを新しいパスワードで再度追加しようとすると、ユーザーはすでに Directory Server に存在するため、Directory Server への追加は失敗します。エントリはリンクされないため、2つの個別のアカウントをリンクするために `idsync resync` コマンドを実行してください。

`idsync resync` コマンドを実行する場合は、Directory Server のエントリにリンクされた Active Directory のアカウントのパスワードをリセットしてください。パスワードをリセットすると、Directory Server でそれらのパスワードが無効になり、次回ユーザーが新しい Active Directory パスワードを使用して Directory Server に対して認証を求めるときにオンデマンド同期が行われて Directory Server パスワードが更新されます。

パスワードなしのアカウントの作成

再同期のような特定の状況では、Identity Synchronization for Windows はパスワードなしでアカウントを作成します。

Directory Server

Identity Synchronization for Windows がパスワードなしで Directory Server にエントリを作成するときは、`userpassword` 属性を `{PSWSYNC}*INVALID*PASSWORD*` に設定します。パスワードがリセットされるまで、ユーザーは Directory Server にログインできません。例外は、`resync` を `-i NEW_USERS` または `NEW_LINKED_USERS` オプションを指定して実行するときです。この場合、`resync` によって新しいユーザーのパスワードは無効になり、次回ユーザーがログインするときにはオンデマンドパスワード同期がトリガーされます。

Active Directory

Identity Synchronization for Windows がパスワードなしで Active Directory にエントリを作成するときは、Active Directory パスワードポリシーを満たすようにランダムに選択された、強力なパスワードにユーザーのパスワードを設定します。この場合、警告メッセージがログに記録され、パスワードがリセットされるまでユーザーは Active Directory にログインできません。

Identity Synchronization for Windows の操作時に発生する可能性のあるシナリオの一部を次の表に示します。

この節では、パスワードポリシーが同期および再同期に与える影響について説明します。

これらの表は、すべての可能な設定シナリオを説明することを目的としていません。システムの設定はさまざまであるためです。この情報をガイドラインとして使用することで、パスワードが確実に同期され続けるようにすることができます。

表 4-3 パスワードポリシーが同期動作に与える影響

シナリオ	結果				
ユーザーの元の作成場所	ユーザーがパスワードポリシーを満たす場所		ユーザーの作成場所		
	Directory Server	Active Directory	Directory Server	Active Directory	説明
Active Directory	可	可	可	可	
	可	不可	可(「説明」を参照)	不可	ユーザーは Directory Server に作成されます。ただし、削除が Active Directory から Directory Server へ同期される場合、このユーザーはただちに削除されます。 128 ページの「Active Directory パスワードポリシー」 の情報を参照してください。
	不可	可	可	可	128 ページの「Active Directory パスワードポリシー」 の情報を参照してください。

表 4-3 パスワードポリシーが同期動作に与える影響 (続き)

シナリオ		結果				
ユーザーの元の作成場所	ユーザーがパスワードポリシーを満たす場所	Directory Server	Active Directory	Directory Server	Active Directory	説明
		不可	不可	可 (「説明」を参照)	不可	ユーザーは Directory Server に作成されま す。ただし、削除が Active Directory から Directory Server へ同 期される場合、この ユーザーはただちに 削除されます。 128 ページの「Active Directory パスワード ポリシー」の情報を 参照してください。
Directory Server		可	可	可	可	
		可	不可	可	不可	
		不可	可	不可	不可	
		不可	不可	不可	不可	

表 4-4 パスワードポリシーが再同期動作に与える影響

シナリオ		結果				
Resync コマンド	ユーザーがパスワードポリシーを満たす場所	Directory Server	Active Directory	Directory Server	Active Directory	説明
resync -c -o Sun		N/A	可			ユーザーは Active Directory に作成されま すが、ログインできません。 129 ページの「パスワードなしのアカウ ントの作成」を参照してください。
		N/A	不可			ユーザーは Active Directory に作成されま すが、ログインできません。 129 ページの「パスワードなしのアカウ ントの作成」を参照してください。

表 4-4 パスワードポリシーが再同期動作に与える影響 (続き)

シナリオ				結果
Resync コマンド	ユーザーがパスワードポリシーを満たす場所	Directory Server	Active Directory	
resync -c -i NEW_USERS NEW_LINKED_USERS	可		N/A	
	不可		N/A	ユーザーは Directory Server に作成されますが、パスワードが Directory Server パスワードポリシーに違反しているため、ログインできません。 129 ページの「パスワードなしのアカウントの作成」 を参照してください。
resync -c	可		N/A	ユーザーは Directory Server に作成されますが、新しいパスワード値が Active Directory または Directory Server で設定されるまでログインできません。 129 ページの「パスワードなしのアカウントの作成」 を参照してください。
	不可		N/A	ユーザーは Directory Server に作成されますが、新しいパスワード値が Active Directory または Directory Server で設定されるまでログインできません。 129 ページの「パスワードなしのアカウントの作成」 を参照してください。

パスワードポリシーの例

この節では、Active Directory および Directory Server のパスワードポリシーの例について説明します。

Directory Server のパスワードポリシー

- ユーザーはリセット後にパスワードを変更する必要があります
- ユーザーはパスワードを変更することができます
- 20 個のパスワードを履歴に保存します
- パスワードの有効期限は 30 日です
- パスワードの有効期限が切れる 5 日前に警告を送信します
- パスワード構文を確認します: パスワードは最短 7 文字です

Active Directory パスワードポリシー

- パスワードの履歴を記録する: 20 日
- パスワードの有効期間: 30 日
- パスワードの変更禁止期間: 0 日
- 最小パスワード長: 7 文字
- パスワードは、複雑さの要件を満たす必要がある: 有効

エラーメッセージ

コアシステムのセントラルロガーの `audit.log` ファイルで、次のエラーメッセージを確認します。

```
Unable to update password on DS due to password policy during  
on-demand synchronization:
```

```
WARNING 125 CNN100 hostname "DS Plugin (SUBC100):  
unable to update password of entry 'cn=John Doe,ou=people,o=sun',  
reason: possible conflict with local password policy"
```

注 - Windows 2003 のパスワードポリシーの詳細は、

<http://www.microsoft.com/japan/technet/windowsserver/2003/technologies/directory/activedirectory/stepbystep/strngpw.mspx> を参照してください。

Sun Java System Directory Server のパスワードポリシーの詳細については、『Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド』の第 8 章「Directory Server のパスワードポリシー」を参照してください。

SSL 動作のための Windows の設定

Directory Server から Windows Active Directory へパスワードの変更を伝播させる計画を立てている場合は、SSL を使用するように各 Active Directory を設定し、高度暗号化パックをインストールしてください。

Active Directory で LDAP over SSL を有効にしている場合は、Identity Synchronization for Windows Active Directory コネクタインストーラが Active Directory コネクタの SSL を自動的に設定できます。証明書は、次の URL で説明されているように、Microsoft 証明書サービスのエンタープライズルート認証局から自動的に取得できます。

<http://support.microsoft.com/kb/247078/ja>

ただし、技術メモ <http://support.microsoft.com/default.aspx?scid=kb;en-us;321051> で説明されているように、LDAP over SSL はより簡単に設定できます。

この場合、SSL 通信を行うために信頼できる証明書が必要であると判断したときは、[264 ページの「Active Directory コネクタでの SSL の有効化」](#)で説明するように、コネクタの証明書データベースに証明書を手動でインストールします。

インストールおよび設定の決定

この節では、インストールおよび設定の概要、および Identity Synchronization for Windows の配備時の選択内容の詳細について説明します。この節で説明するすべての情報を確認のうえ、インストールプロセスを開始する前にインストールチェックリストを完成してください。

コアのインストール

コアをインストールするときは、次の情報を指定します。

- 設定ディレクトリのホストおよびポート。Identity Synchronization for Windows 設定情報が格納される Directory Server インスタンスの設定ディレクトリのホストおよびポートを指定します。
設定ディレクトリのポートとして SSL ポートを指定できます。その場合は、インストールプロセス時に SSL のポートを指定してください。
- ルートサフィックス。設定ディレクトリのルートサフィックスを指定します。すべての設定情報がこのサフィックスの下に格納されます。
- 管理者の名前およびパスワード。設定 Directory Server にアクセスするための資格を指定します。
- 設定パスワード。機密性のある設定情報を保護するためのセキュアなパスワードを指定します。
- ファイルシステムディレクトリ。Identity Synchronization for Windows をインストールする場所を指定します。コアは Directory Server 管理サーバーと同じディレクトリにインストールしてください。
- 未使用のポート番号。Message Queue インスタンス用に利用可能なポート番号を指定します。
- 管理サーバー。管理サーバー管理者が Directory Server にすでに存在する場合は、そのユーザー名およびパスワードを指定します。

コアの設定

コアを設定するときは、次の情報を指定します。

- **Sun Java System** ディレクトリスキーマ。設定ディレクトリからロードする Directory Server データを指定します。

- ユーザーオブジェクトクラス (**Directory Server** のみ)。ユーザータイプを判断するために使用されるユーザーオブジェクトクラスを指定します。Identity Synchronization for Windows は、このオブジェクトクラスに基づいて、パスワード属性を含む属性のリストを派生します。このリストは、スキーマから生成されます。
- 同期される属性。Directory Server と Windows のディレクトリソースの間で同期されるユーザーエントリ属性を指定します。
- 変更、作成、および削除のフロー。変更、作成、および削除が Directory Server と Windows のディレクトリソースの間で伝播する方法を指定します。
 - Directory Server から Active Directory/Windows NT
 - Active Directory/Windows NT から Directory Server
 - 双方向
オブジェクトの有効化および無効化が Directory Server と Windows のディレクトリソースの間で伝播される場合に同期するかどうか、およびそれらのオブジェクトの同期方式を指定します。
- グローバルカタログ。グローバルカタログ (Active Directory のトポロジおよびスキーマ情報のリポジトリ) を指定します。
- **Active Directory** スキーマコントローラ。Windows グローバルカタログから取得される Active Directory スキーマソースの完全修飾ドメイン名 (FQDN) を指定します。
- 設定ディレクトリ。Identity Synchronization for Windows 設定を格納する Directory Server を指定します。
- **Active Directory** ソース。Active Directory ドメインを同期するために使用するソースを指定します。
- **Windows NT** のプライマリドメインコントローラ。同期する Windows NT ドメイン、および各ドメインのプライマリドメインコントローラの名前を指定します。
- 同期ユーザーリスト。LDAP DIT およびフィルタ情報を使用して、Directory Server、Active Directory、および Windows NT で同期されるユーザーを指定します。
- **Sun Java System Directory Server**。同期されるユーザーを格納する Directory Server インスタンスを指定します。

コネクタのインストールおよびディレクトリサーバープラグインの設定

コネクタおよびディレクトリサーバープラグインをインストールするときは、次の情報を指定します。

- 設定ディレクトリのホストおよびポート。Identity Synchronization for Windows 設定情報が格納される Directory Server インスタンスの設定ディレクトリのホストおよびポートを指定します。
- ルートサフィックス。設定ディレクトリのルートサフィックスを指定します。コアのインストール時に指定したルートサフィックスを使用します。
- 管理者の名前およびパスワード。Directory Server にアクセスするための資格を指定します。
- 設定パスワード。機密性のある設定情報を保護するためのセキュアなパスワードを指定します。
- ファイルシステムディレクトリ。Identity Synchronization for Windows をインストールする場所を指定します。同じマシンにインストールされるすべてのコンポーネントは、インストールパスを同じにします。
- ディレクトリソース。コネクタまたはプラグインをインストールするディレクトリソースを指定します。

Directory Server および Windows NT のコネクタをインストールする場合は、未使用のポートを指定します。

ディレクトリサーバーコネクタおよびプラグインをインストールする場合は、そのコネクタおよびプラグインに対応する Directory Server のホスト、ポート、および資格を指定します。

コマンド行ユーティリティーの使用

Identity Synchronization for Windows では、idsync スクリプトで次のサブコマンドを使用して、コマンド行からさまざまなタスクを実行できます。

- certinfo — 設定および SSL 設定に基づいて証明書情報を表示します。
- changepw — Identity Synchronization for Windows 設定パスワードを変更します。
- prepds — Identity Synchronization for Windows が使用できるように Sun Java System Directory Server ソースを準備します。
- printstat — インストールされているコネクタ、システムマネージャー、および Message Queue の状態を出力します。
インストールプロセスを完了するために実行する必要があるインストールおよび設定の残りの手順を表示するために printstat コマンドを使用することもできます。
- resetconn — ハードウェアまたはアンインストールのエラー時のみ、設定ディレクトリのコネクタの状態をアンインストール済みに戻します。
- resync — インストールプロセスの一環として、既存ユーザーを再同期およびリンクしたり、ディレクトリを事前に生成したりします。

- dspluginconfig — ディレクトリサーバープラグインを設定または設定解除します。
- groupsync — グループの同期を有効または無効にします。
- accountlockout — アカウントのロックアウト機能を有効または無効にします。
- startsync — 同期を開始します。
- stopsync — 同期を停止します。

これらのユーティリティの詳細については、[付録 A 「Identity Synchronization for Windows コマンド行ユーティリティの使用」](#)を参照してください。

インストールチェックリスト

これらのチェックリストを使用して、インストールプロセスを準備してください。Identity Synchronization for Windows をインストールする前に、チェックリストを印刷して適切な情報を記録します。

表 4-5 コアのインストールチェックリスト

必要な情報	エントリ
設定ディレクトリのホストおよびポート	
設定ディレクトリのルートサフィックス (たとえば dc=example,dc=com)	
Identity Synchronization for Windows をインストールするファイルシステムディレクトリ	
設定 Directory Server の管理者の名前およびパスワード	
機密性のある設定情報を保護するためのセキュアな設定パスワード	
Message Queue インスタンス用のポート番号	
管理サーバーのユーザー名およびパスワード	

表 4-6 コアの設定チェックリスト

必要な情報	エントリ
Active Directory グローバルカタログ (該当する場合)	
Directory Server スキーマサーバー	
Directory Server ユーザー構造および Auxiliary オブジェクトクラス	
同期される属性	
ユーザーエントリ作成のフロー	

表 4-6 コアの設定チェックリスト (続き)

必要な情報	エントリ
ユーザーエントリ変更のフロー	
ユーザーエントリ有効化および無効化のフロー	
ユーザーエントリ削除のフロー	
Sun Java System Directory Server ディレクトリソース	
Active Directory	
同期ユーザーリスト	
Windows ソースフィルタの作成式	
Sun Java System ソースフィルタの作成式	
管理サーバーのユーザー名およびパスワード	

コネクタおよびディレクトリサーバープラグインのインストールチェックリスト

必要な情報	エントリ
設定ディレクトリのホストおよびポート	
設定ディレクトリのルートサフィックス	
コネクタをインストールするファイルシステムディレクトリ	
設定 Directory Server の管理者の名前およびパスワード	
機密性のある設定情報を保護するためのセキュアな設定パスワード	
ディレクトリソース	
Directory Server および Windows NT 用の未使用ポート	
コネクタおよびプラグインに対応する Directory Server のホスト、ポート、および資格	

ユーザーのリンクのチェックリスト

必要な情報	エントリ
リンクされる同期ユーザーリスト。	
同等のユーザーを一致させるために使用する属性	
XML 設定ファイル	

再同期チェックリスト

必要な情報	エン트리
同期ユーザーリストの選択	
同期ソース	
対応するユーザーが宛先のディレクトリソースに見つからない場合にユーザーエント리를自動的に作成するか	
Directory Server パスワードを無効にするか	
指定された LDAP フィルタに一致していて選択された SUL に含まれるユーザーだけを同期するか	

コアのインストール

この章では、Identity Synchronization for Windows のインストールプログラムを使用する方法、および Identity Synchronization for Windows コアコンポーネントをインストールする方法について説明します。

この章は次の項目から構成されています。

- 141 ページの「始める前に」
- 142 ページの「インストールプログラムの起動」
- 144 ページの「コアのインストール」

始める前に

Identity Synchronization for Windows インストールプロセスを始める前に、次の点を確認してください。

- 第4章「インストールの準備」を読みます。この章では、インストールの前提条件、チェックリスト、管理者特権の要件などについて説明します。
- Java Runtime Environment (JRE) は、この製品に付属していません。必要な場合は、Java Development Kit を次の場所からダウンロードできます。

<http://java.sun.com> または <http://www.java.com>

Identity Synchronization for Windows インストールプログラムを Solaris、Linux、または Windows 2000/2003 システムで実行するには、JRE 1.5.0_09 またはそれ以降をインストールしてください。

注 - Directory Server 6.x が Java ES とともにインストールされている場合、JRE 1.5.0_09 はコンピュータにすでにインストールされています。

- **Windows** システムの場合のみ: コアのインストールを開始する前に、開いている「サービス」コントロールパネルのウィンドウはすべて閉じます。そうしないとインストールに失敗します。
- **Solaris** システムの場合: Message Queue と Identity Synchronization for Windows を同じディレクトリにインストールしないでください。
- **Red Hat Linux** システムの場合: Message Queue と Identity Synchronization for Windows を同じディレクトリにインストールしないでください。

インストールプログラムの起動

この節では、次のプラットフォームで Identity Synchronization for Windows インストールプログラムをダウンロードして展開 (解凍) し、実行する方法について説明します。

- 142 ページの「Solaris SPARC の場合」
- 143 ページの「Solaris x86 の場合」
- 143 ページの「Windows の場合」
- 144 ページの「Red Hat Linux の場合」

Solaris SPARC の場合

Solaris SPARC オペレーティングシステムで Identity Synchronization for Windows インストールプログラムを準備して実行するには、次の手順を使用します。

▼ Solaris SPARC で Identity Synchronization for Windows を実行する

- 1 **root** としてログインします。
- 2 **Solaris SPARC** 用の配布メディア上で、インストールプログラム `DSEE_Identity_Synchronization_for_Windows` が格納されているディレクトリに変更します。
- 3 `./runInstaller.sh` と入力してインストールプログラムを実行します。
インストールプログラムをテキストベースモードで実行するには、次のように入力します。

```
./runInstaller.sh -nodisplay
```

`runInstaller.sh` プログラムを実行すると、Identity Synchronization for Windows ではパスワードを自動的にマスクして、平文で表示されないようにします。

Solaris x86 の場合

▼ Solaris x86 で Identity Synchronization for Windows を準備して実行する

- 1 rootとしてログインします。
- 2 Solaris x86用の配布メディア上で、インストールプログラム DSEE_Identity_Synchronization_for_Windows が格納されているディレクトリに変更します。
- 3 `./runInstaller.sh` と入力してインストールプログラムを実行します。
インストールプログラムをテキストベースモードで実行するには、次のように入力します。

```
./runInstaller.sh -nodisplay
```

`runInstaller.sh` プログラムを実行すると、Identity Synchronization for Windows ではパスワードを自動的にマスクして、平文で表示されないようにします。

Windows の場合

Windows オペレーティングシステムで Identity Synchronization for Windows インストールプログラムを準備して実行するには、次の手順を使用します。

▼ Windows で Identity Synchronization for Windows を実行する

- 1 管理者としてログインします。
- 2 Windows用の配布メディア上で、インストールプログラム DSEE_Identity_Synchronization_for_Windows が格納されているディレクトリに変更します。
- 3 `setup.exe` と入力してインストールプログラムを実行します。
Identity Synchronization for Windows インストールウィザードが表示されます。

注- 管理サーバールートにコアをインストールすると、Identity Synchronization for Windows ウィザードによってディレクトリパスや名前などのインストールに必要なほとんどの情報が検出され、ウィザードパネルの特定フィールドに自動的に入力されます。

情報が足りないまたは正しくない場合は、手動で必要な情報を入力できます。

次の節に進み、コアをインストールします。

Red Hat Linux の場合

Red Hat Linux オペレーティングシステムで Identity Synchronization for Windows インストールプログラムを準備して実行するには、次の手順を使用します。

▼ Linux で Identity Synchronization for Windows を準備して実行する

- 1 **root** としてログインします。
- 2 **Red Hat** 用の配布メディア上で、インストールプログラム `DSEE_Identity_Synchronization_for_Windows` が格納されているディレクトリに変更します。
- 3 `./installer.sh` と入力してインストールプログラムを実行します。
インストールプログラムをテキストベースモードで実行するには、次のように入力します。

```
./installer.sh -nodisplay
```

`installer.sh` プログラムを実行すると、Identity Synchronization for Windows ではパスワードを自動的にマスクして、平文で表示されないようにします。

コアのインストール

この節では、Solaris、Linux、および Windows のオペレーティングシステムで Identity Synchronization for Windows コアをインストールするプロセスについて説明します。

コアをインストールする前に、次の要件を確認するようにしてください。

- **Solaris** システムの場合: Solaris サービスをインストールして実行するには、**root** 権限が必要です。
- **Red Hat Linux** システムの場合: Linux サービスをインストールして実行するには、**root** 権限が必要です。

- **Windows 2000/2003** システムの場合: Identity Synchronization for Windows をインストールするには、管理者権限が必要です。

注 - プログラムは root としてインストールする必要がありますが、インストール後は、root 以外のユーザーとして Solaris および Linux サービスを実行するようにソフトウェアを設定できます。(付録 B 「Identity Synchronization for Windows LinkUsers XML ドキュメントの例」を参照)

コアをインストールするディレクトリには、管理サーバー (バージョン 5 2004Q2 またはそれ以上) で管理される既存のサーバールートが存在する必要があります。そうでない場合、インストールプログラムは失敗します。Directory Server 5 2004Q2 インストールプログラムを使用して管理サーバーをインストールできます。

注 - Identity Synchronization for Windows 6.0 の場合、インストーラは既存の Sun Java System Administration Server があるかどうかを確認します。インストールされていない場合、インストーラはコアをインストールする一環として Sun Java System Administration Server をインストールします。

▼ インストールウィザードを使用して **Identity Synchronization for Windows** コアコンポーネントをインストールする

- 1 「ようこそ」画面で、表示された情報を読み、「次へ」をクリックして「ソフトウェア使用許諾契約」パネルに進みます。
- 2 ライセンス条項を確認し、次のいずれかを選択します。
 - 「はい(ライセンスに同意する)」を選択すると、ライセンス条項に同意して次のパネルに進みます。
 - 「いいえ」を選択すると、設定プロセスを中止し、インストールプログラムを終了します。
- 3 「設定ディレクトリの位置」パネルが表示されたら、設定ディレクトリの場所を指定します。

Core Install: Configuration Location

Specify information about the configuration directory and root context where the Sun Java(TM) System Identity Synchronization for Windows will be stored or is already stored.

Configuration Directory Host:

Configuration Directory Port: Secure Port

Configuration Root Suffix: Refresh

図 5-1 設定ディレクトリの場所の指定

次の情報を入力します。

- 「設定ディレクトリホスト」: Identity Synchronization for Windows 設定情報が格納される、ローカルの管理サーバーと連携した Sun Java System Directory Server インスタンスの完全修飾ドメイン名 (FQDN) を入力します。

ローカルマシン上のインスタンスまたは別のマシンで実行しているインスタンスを指定できます。

Identity Synchronization for Windows では、管理サーバーが遠隔にインストールされている Directory Server インスタンスにアクセスできます。

注- 資格またはホスト名が無効であるという警告を避けるため、インストールプログラムを実行しているマシンに対して DNS 解決可能なホスト名を指定する必要があります。

- 「設定ディレクトリポート」: 設定ディレクトリがインストールされるポートを指定します。(デフォルトのポートは 389)
セキュリティ保護された通信を可能にするには、「セキュリティ保護されたポート」オプションを有効にして SSL ポートを指定します。(デフォルトの SSL ポートは 636)。
設定ディレクトリが SSL に対応していると判断されると、すべての Identity Synchronization for Windows コンポーネントは設定ディレクトリとの通信に SSL を使用します。

注 - Identity Synchronization for Windows は、設定 Directory Server に機密性の高い設定情報を送信する前に、その情報を暗号化します。

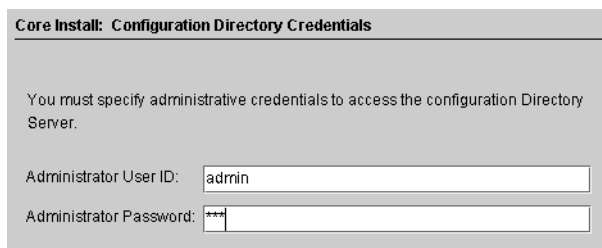
ただし、コンソールと設定ディレクトリの間でさらにトランスポートの暗号化を図る場合は、管理サーバーと設定 Directory Server の両方で SSL を有効にする必要があります。次に、Directory Server コンソールを認証する管理サーバーとの間でセキュリティー保護された通信を設定します。(詳細については、『*Sun Java System Administration Server 5 2004Q2 Administration Guide*』を参照)。

コアコンポーネントの一部としてインストール(および設定)された Sun Java System Administration Server は、非 SSL モードでインストールされます。

- 「設定ルートサフィックス」: メニューから Identity Synchronization for Windows 設定を格納するルートサフィックスを選択します。

注 - ルートサフィックスが検出できず、情報を手動で入力する必要がある場合(またはデフォルト値を変更する場合)、「更新」をクリックしてルートサフィックスのリストを再生成してください。指定するルートサフィックスは、設定 Directory Server に存在する必要があります。

- 4 「次へ」をクリックして「設定ディレクトリのクレデンシャル」パネルを開きます。



Core Install: Configuration Directory Credentials

You must specify administrative credentials to access the configuration Directory Server.

Administrator User ID:

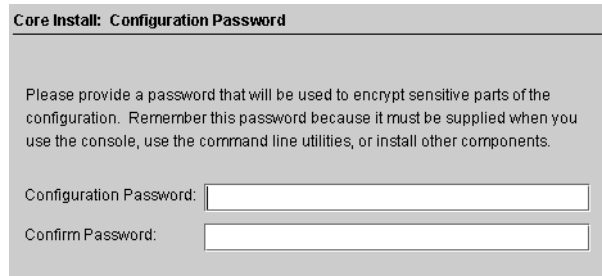
Administrator Password:

図 5-2 管理者の資格の指定

- 5 設定ディレクトリの管理者のユーザー ID およびパスワードを入力します。
 - ユーザー ID として admin と入力した場合は、ユーザー ID を DN として指定する必要はありません。
 - その他のユーザー ID を使用する場合は、その ID を完全 DN として指定します。たとえば、`cn=Directory Manager` のようになります。

注 - 設定ディレクトリと通信するために SSL を使用していない場合 (144 ページの「コアのインストール」を参照)、これらの資格は暗号化なしで送信されます。

- 6 完了したら、「次へ」をクリックして、「設定パスワード」パネルを開きます。



Core Install: Configuration Password

Please provide a password that will be used to encrypt sensitive parts of the configuration. Remember this password because it must be supplied when you use the console, use the command line utilities, or install other components.

Configuration Password:

Confirm Password:

図 5-3 設定パスワードの指定

- 7 資格情報などの機密性の高い設定情報を暗号化するために使用するパスワードを入力し、確認してください。完了したら、「次へ」をクリックします。

注 - このパスワードは、次のときに必要になるため覚えておく必要があります。

- Identity Synchronization for Windows コンソールへのアクセス
- 設定の作成または編集
- コンポーネントのインストール
- 任意のコマンド行ユーティリティーの実行

設定パスワードの変更については、289 ページの「[changepw の使用](#)」を参照してください。

「Java ホームの選択」パネルが表示されます (144 ページの「コアのインストール」を参照)。インストールされたコンポーネントで使用する Java 仮想マシンのディレクトリの場所が自動的に挿入されます。

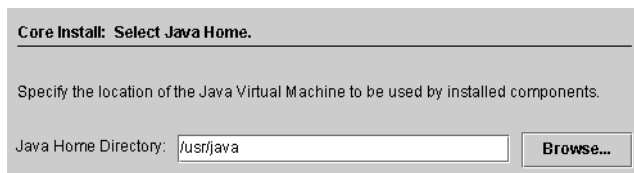


図 5-4 Java ホームのディレクトリの指定

- 8 「Java ホームディレクトリ」を確認します (JDK/JRE 1.5.0_09 またはそれ以降)。
- 場所が正しいことを確認したら、「次へ」をクリックして「インストールディレクトリの選択」パネルに進みます (144 ページの「コアのインストール」)。
 - 場所が正しくない場合は、「参照」をクリックし、Java がインストールされているディレクトリを検索して選択します。たとえば次のとおりです。
 - **Solaris** の場合: /var/java
 - **Linux** の場合: /usr/bin/java
 - **Windows** の場合: C:\Program Files\j2sdk1.5

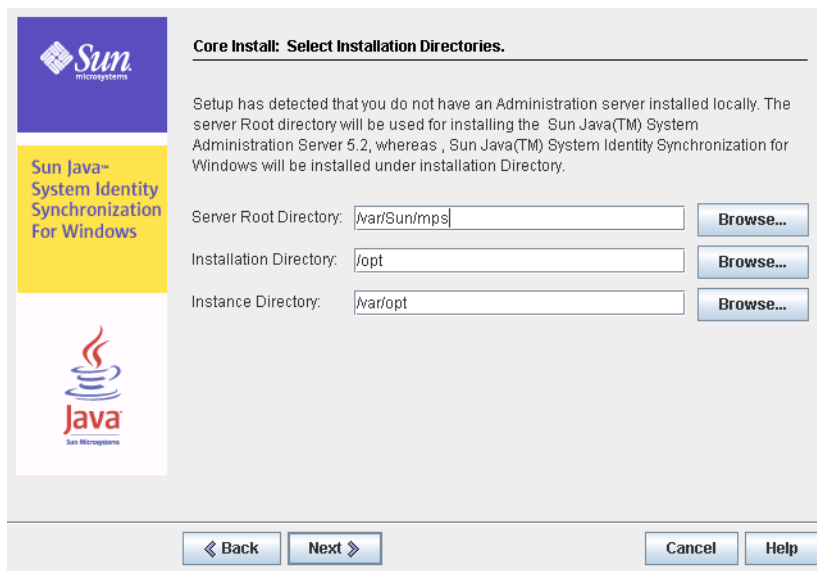


図 5-5 インストールディレクトリの指定

- 9 次の表示されるテキストフィールドに情報を入力するか、「参照」をクリックして使用可能なディレクトリを検索して選択します。

- 「サーバールートディレクトリ」:管理サーバーのインストールサーバールート
のパスおよびディレクトリ名を指定します。コンソールはこの場所にインストー
ルされます。
- 「インストールディレクトリ」(*Solaris* または *Linux* にコアをインストールする
ときのみ利用可能):インストールディレクトリのパスおよびディレクトリ名を指定
します。コアのバイナリ、ライブラリ、および実行可能ファイルはこのディレク
トリにインストールされます。
- 「インスタンスディレクトリ」(*Solaris* または *Linux* にコアをインストールする
ときのみ利用可能):インスタンスディレクトリのパスおよびディレクトリ名を指定
します。変更される設定情報(ログファイルなど)はこのディレクトリに格納され
ます。

注 - Windows オペレーティングシステムで利用可能なサーバールートディレクトリは
1つだけであり、すべての製品がその場所にインストールされます。

注 - 手順3で指定した設定ディレクトリのホストおよびポート番号に対応する管理
サーバーが見つからない場合、管理サーバーのインストーラはコアインストールの
一部として管理サーバーをインストールします。割り当てられた管理サーバーの
ポートのデフォルトポート番号は、設定ディレクトリのポートに1を足した番号に
なります。

10 「次へ」をクリックして「**Message Queue**の設定」パネルに進みます。

注 - Identity Synchronization for Windows のインストールを開始する前に、Message
Queue 3.6 Enterprise Edition をインストールしておくようにしてください。

Solaris システムの場合: Message Queue と Identity Synchronization for Windows を同じ
ディレクトリにインストールしないでください。

Linux システムの場合: Message Queue と Identity Synchronization for Windows を同じ
ディレクトリにインストールしないでください。

Windows システムの場合: コアのインストールを続行する前に、開いている「サービ
ス」コントロールパネルのウィンドウはすべて閉じます。そうしないとコアのイン
ストールに失敗します。

図 5-6 Message Queue の設定

- 11 表示されるテキストフィールドに次の情報を入力するか、「参照」をクリックして使用可能なディレクトリを検索して選択します。
 - 「インストールディレクトリ」: Message Queue のインストールディレクトリのパスを指定します。
 - 「設定ディレクトリ」: Message Queue インスタンスディレクトリのパスおよびディレクトリ名を指定します。
 - 「完全修飾ローカルホスト名」: ローカルホストマシンの完全修飾ドメイン名 (FQDN) を指定します。Message Queue ブローカインスタンスはホストあたり 1 つだけ実行できます。
 - 「ブローカポート番号」: Message Queue ブローカで使用される未使用のポート番号を指定します。(デフォルトのポートは 7676)

- 12 「次へ」をクリックすると、「インストール準備完了」パネルが表示されます。このパネルには、コアのインストール先ディレクトリ、コアのインストールに必要な容量など、インストールに関する情報が表示されます。
 - 表示される情報に問題がない場合は、「すぐにインストール」をクリックしてコアコンポーネントをインストールします (インストールプログラムによってバイナリ、ファイル、およびパッケージがインストールされる)。
 - 情報が正しくない場合は、「戻る」をクリックして変更します。
インストール中であることを示すメッセージが短く表示されます。次に「コンポーネントの設定」パネルが表示され、設定データが指定された設定 Directory Server に追加されます。この操作では、次の処理が行われます。
 - Message Queue ブローカインスタンスの作成
 - 設定ディレクトリへのスキーマのアップロード
 - 設定ディレクトリへの配備固有の設定情報のアップロード

この操作には数分かかり、定期的な一時停止する可能性があります。そのため、プロセスに10分以上かからないかぎり問題はありません。インストールプログラムの状態を監視するには、進捗バーを確認します。

- 13 コンポーネントの設定操作が完了したら、「インストール概要」パネルが表示されます。**Identity Synchronization for Windows** が正しくインストールされたことを確認します。

「詳細」ボタンをクリックすると、インストールされたファイルとインストール先のリストが表示されます。

- 14 「次へ」をクリックすると、**Identity Synchronization for Windows** のインストールおよび設定を正常に実行するために必要な残りの手順がプログラムによって判断されます。

ロード中であることを示すメッセージおよび「残りのインストール手順」パネルがそれぞれ短く表示されたあとに、次のパネル(118ページの「インストールの概要」)が表示されます。このパネルには、残りのインストールおよび設定の手順の実行手順リストが表示されます。このパネルには、コンソールの「状態」タブからもアクセスできます。

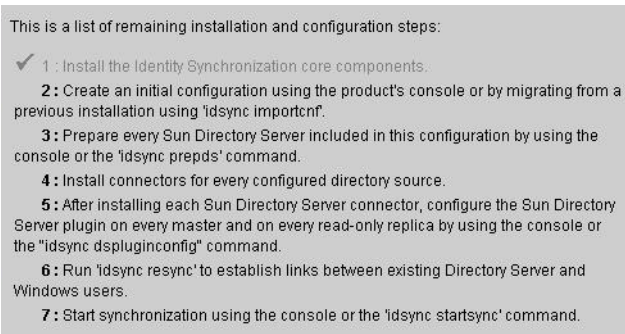


図 5-7 Identity Synchronization for Windows のインストールおよび設定の実行手順リスト

インストールおよび設定のプロセスを通じて実行手順のパネルの表示が繰り返されます。リストですべての完了した手順はグレー表示されます。

この時点までは、実行手順リストには汎用的な手順のリストが表示されます。設定を保存すると、使用している配備向けにカスタマイズされた手順のリストが表示されます(たとえば、インストールする必要のあるコネクタ)。

- 15 手順のリストを確認して「次へ」をクリックすると、「コンソールオプションの起動」パネルが表示され、コアのインストールが完了したことが示されます。

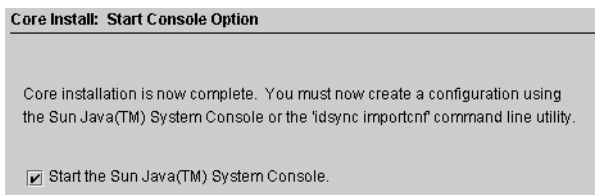


図 5-8 コンソールの起動

- 16 次に、コアコンポーネントを設定します。これは、**Sun Java System** コンソールから実行できます。「**Sun Java System** コンソールを起動します」オプションはデフォルトで有効です。

Identity Synchronization for Windows バージョン 1.0 または SP1 から Sun Java System Identity Synchronization for Windows 6.0 へ移行する場合は、`idsync importcnf` コマンド行ユーティリティを使用して、エクスポートされたバージョン 1.0 または SP1 の設定 XML ドキュメントをインポートできます。

- 17 「完了」をクリックします。
- 18 コンソールを使用することにした場合は、「**Sun Java System** コンソールログイン」ダイアログボックスが表示されます (144 ページの「コアのインストール」を参照)。

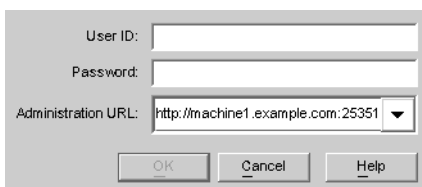


図 5-9 コンソールへのログイン

コンソールにログインするために次の情報を入力します。

- 「ユーザー ID」: マシンに管理サーバーのインストール時に指定した管理者のユーザー ID を入力します。
- 「パスワード」: 管理サーバーのインストール時に指定した管理者のパスワードを入力します。
- 「管理 URL」: 管理サーバーの URL の現在の場所を次の書式で入力します。

`http://hostname.your_domain.domain:port_number`

各表記の意味は次のとおりです。

- `hostname.your_domain.domain` は、管理サーバーのインストール時に選択したコンピュータのホスト名です。
- `port_number` は、管理サーバー用に指定したポートです。

- 19 資格を入力したら、「OK」をクリックしてダイアログボックスを閉じます。
- 20 設定パスワードの入力が求められます。パスワードを入力し、「OK」をクリックします。
「Sun Java System サーバーコンソール」ウィンドウが表示されたら、コアの設定を開始できます。手順については、「[第6章「コアリソースの設定」](#)」を参照してください。

コアリソースの設定

Identity Synchronization for Windows コアをインストールしたら、ただちにコアリソースの初期設定を行います。

この章では、コンソールを使用してコアリソースを追加および設定する方法について説明します。この章は、次の節で構成されています。

- 155 ページの「設定の概要」
- 156 ページの「Identity Synchronization for Windows コンソールを開く」
- 160 ページの「ディレクトリソースの作成」
- 183 ページの「ユーザー属性の選択とマッピング」
- 189 ページの「システム間でのユーザー属性の伝播」
- 209 ページの「同期ユーザーリストの作成」
- 214 ページの「設定の保存」

注 - コアリソースを効率的に設定するため、Directory Server と Active Directory の設定および操作方法を理解しておきます。

これらのリソースは、特に明記されていないかぎり、特定の順序で設定する必要はありません。ただし、製品に精通するまでは、この章で説明する順序で設定を行う方が時間の節約となり、エラーも防止できます。

設定の概要

この節では、配備に必要なコアリソースを設定する手順について説明します。

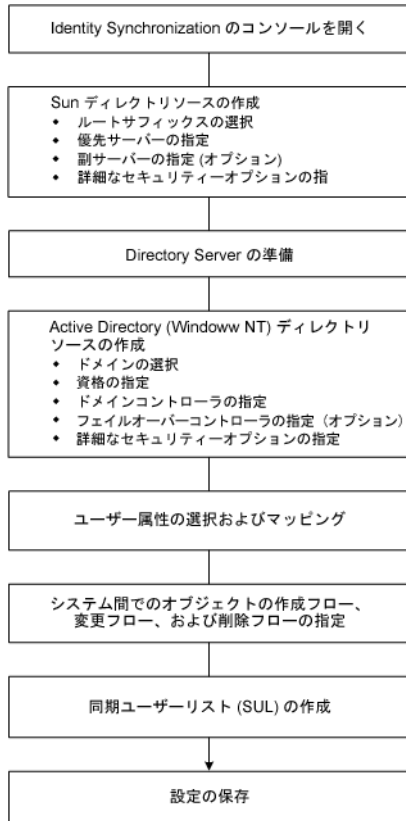


図 6-1 配備に必要なコアリソースの設定

Identity Synchronization for Windows コンソールを開く

Sun Java System サーバーコンソールウィンドウには、管理の対象となるすべてのサーバーおよびリソースの一覧と、システムに関する情報が表示されます。

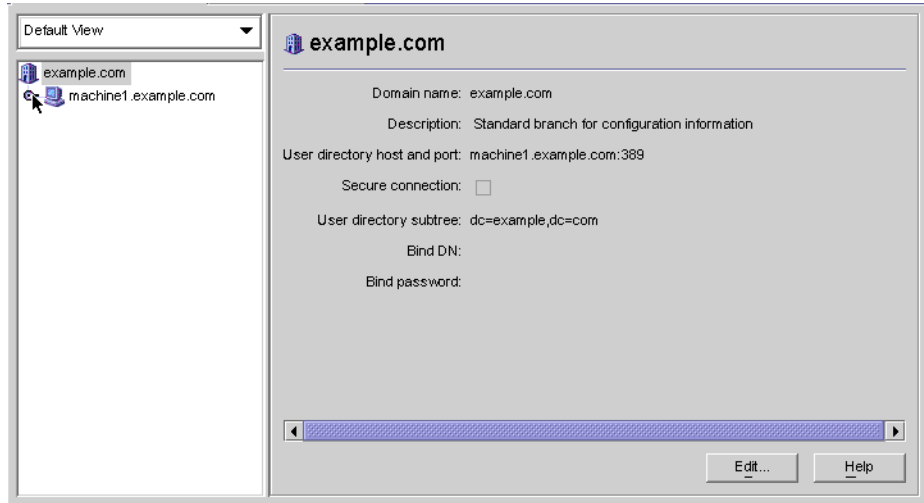


図 6-2 Sun Java System サーバーコンソール

注 - Sun Java System サーバーコンソールにまだログインしていない場合は、[図 5-9](#)を参照し、ログインしてください。

▼ Identity Synchronization for Windows コンソールを開く

- 1 「サーバーとアプリケーション」タブのナビゲーションツリーで、**Identity Synchronization for Windows** インスタンスが属するサーバーグループが含まれているホスト名のノードを選択します。
- 2 「サーバーグループ」ノードを展開し、「**Identity Synchronization for Windows**」ノードを選択します。

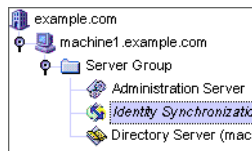


図 6-3 サーバーグループの展開

情報パネルの内容が、Identity Synchronization for Windows とシステムに関する情報に切り替わります。

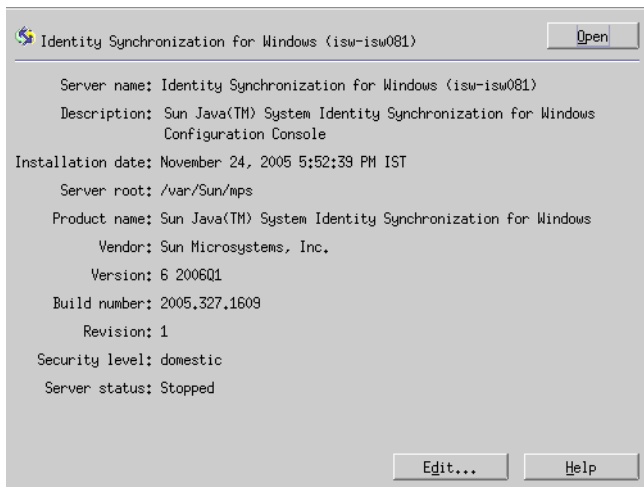


図 6-4 情報パネル

- 3 パネルの右上端にある「開く」ボタンをクリックします。

注-パネルの下部にある「編集」ボタンをクリックすると、サーバー名と説明を編集できます。

- 4 コアのインストール時に指定した設定パスワードの入力を求められます。パスワードを入力し、「OK」をクリックします。

次のような Identity Synchronization for Windows コンソールが表示されます。

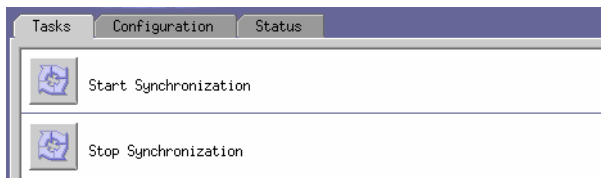


図 6-5 コンソール: 「タスク」タブ

このウィンドウには、3つのタブがあります。

- 「タスク」(デフォルト): このタブでは、Sun と Windows のシステム間の同期を起動および停止します。サービスの起動と停止については、238 ページの「同期の起動および停止」を参照してください。

注-同期サービスの起動と停止を、Windows サービスの開始と停止と混同しないでください。

Windows サービスを開始または停止するときは、Windows の「スタート」メニューから「コントロールパネル」→「管理ツール」→「コンピュータの管理」→「サービスとアプリケーション」→「サービス」の順にアクセスします。

- 「設定」: このタブでは、システムの同期を設定します。
- 「状態」: このタブでは、次の操作を行います。
 - コネクタなどのシステムコンポーネントの状態を監視する。
 - 設定時および同期時に Identity Synchronization for Windows が生成する監査ログとエラーログを表示する。
 - インストールと設定の実行手順リストの更新とチェックを行う。

5 「設定」タブを選択します。

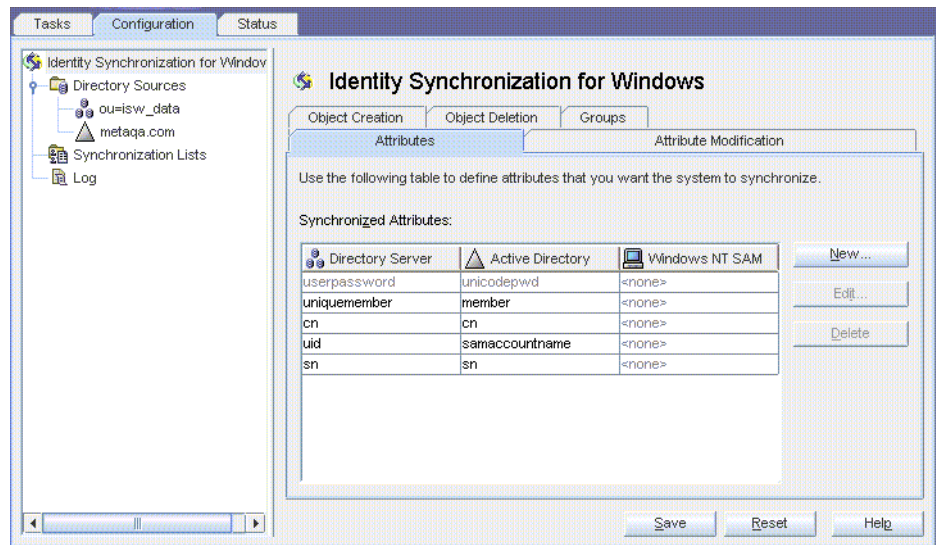


図 6-6 コンソール: 「設定」タブ

「設定」パネルは、次のタブから構成されます。

- 「属性」: このタブでは、システム間で同期させる属性を指定します。

- 「属性の修正」:このタブでは、パスワード、属性変更、およびオブジェクトの無効化をシステム間で伝播させる方法を指定します。
- 「オブジェクトの作成」:このタブでは、新しく作成されたパスワードと属性をシステム間で伝播させる方法、および同期時に Identity Synchronization for Windows が作成するオブジェクトの初期値を指定します。
- 「オブジェクトの削除」:このタブでは、削除されたパスワードと属性をシステム間で伝播させる方法を指定します。

少なくとも1つの Sun Java System Directory Server ディレクトリソースと、少なくとも1つの Windows サーバーディレクトリソース (Active Directory または Windows NT) を設定します。手順については、次の節を参照してください。

ディレクトリソースの作成

▼ ディレクトリソースを作成する

同期対象のソースに基づいて、次の順序でディレクトリソースを作成します。

- 1 [161 ページの「Sun Java System ディレクトリソースの作成」](#)
- 2 [168 ページの「Sun ディレクトリソースの準備」](#)
- 3 [172 ページの「Active Directory ソースの作成」](#)
- 4 [180 ページの「Windows NT SAM ディレクトリソースの作成」](#)

注 - 少なくとも1つの Sun Java System ディレクトリソースと、少なくとも1つの Windows ディレクトリソース (Active Directory、NT SAM のいずれかまたは両方) を設定してください。

ナビゲーションツリーで「ディレクトリソース」ノードを選択して「ディレクトリソース」パネルを表示します。

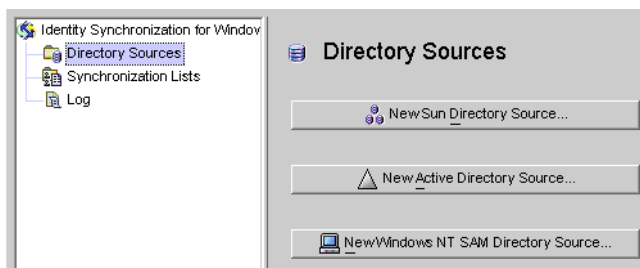


図 6-7 「ディレクトリソース」パネルへのアクセス

Sun Java System ディレクトリソースの作成

各 Sun Java System ディレクトリソースは、複数のサーバーから構成されるレプリケーション環境に配備できるコネクタおよびプラグインセットと関連付けられています。ディレクトリサーバーコネクタでは、Windows ディレクトリソースから優先サーバー(マスター)に変更を同期できます。優先サーバーがダウンした場合は、優先サーバーが復帰するまで、副サーバーリスト内に設定されている順序に従って、副サーバーに変更がフェイルオーバーされます。Directory Server レプリケーションでは、優先サーバー(マスター)から、トポロジ内に設定されているその他の優先副サーバーに変更がレプリケートされます。どのディレクトリサーバープラグインでも Windows ディレクトリソースによるパスワード妥当性チェックが可能であり、ユーザーはどのサーバーからでもパスワードを変更できます。

▼ 新しい Sun Java System ディレクトリソースを作成する

- 1 「新規 Sun ディレクトリソース」ボタンをクリックして、「Sun Java System ディレクトリソースの定義」ウィザードを起動します。

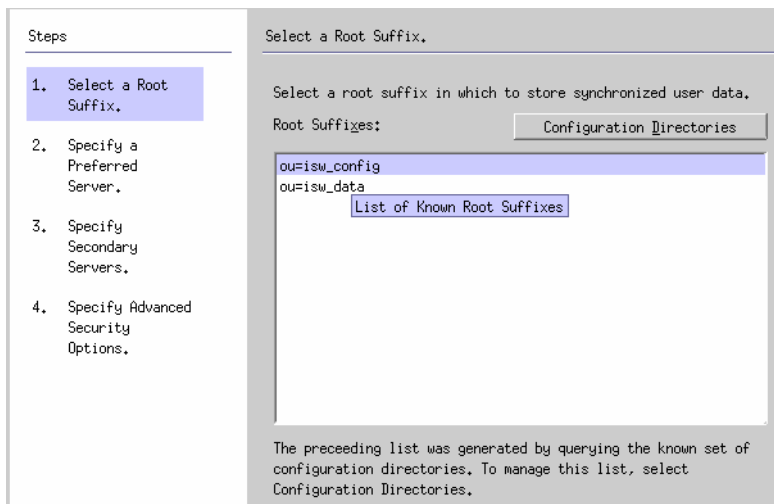


図 6-8 ルートサフィックスの選択

既知の設定ディレクトリソースセットが照会され、既存のルートサフィックス (ネーミングコンテキストとも呼ばれる) が一覧に表示されます。

デフォルトでは、製品がインストールされている設定ディレクトリが認識され、その設定ディレクトリで認識されているルートサフィックスが一覧に表示されます。

- 2 一覧から、ユーザーが配置されているルートサフィックスを選択します。複数のルートサフィックスが表示される場合は、ユーザーが配置されているルートサフィックスを選択します。「次へ」をクリックします。

同期対象のルートサフィックスが、Identity Synchronization for Windows に登録されている設定ディレクトリと関連付けられていない場合は、次の手順に従って新しい設定ディレクトリを指定します。

- a. 「設定ディレクトリ」ボタンをクリックし、新しい設定ディレクトリを指定します。
- b. 「設定ディレクトリ」ダイアログボックス(手順 3)が表示されたら、「新規」ボタンをクリックして「新規設定ディレクトリ」ダイアログボックスを開きます。

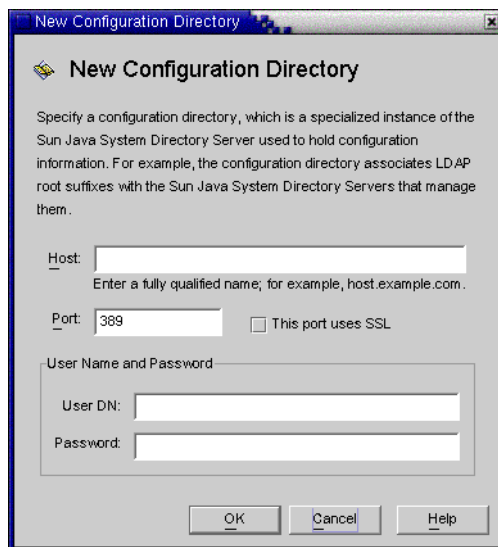


図 6-9 新しい設定ディレクトリの選択

- c. 次の情報を入力し、「OK」をクリックします。変更が保存され、ダイアログボックスが閉じます。
- 「ホスト」:完全修飾ホスト名を入力します。
例: **machine1.example.com**
 - 「ポート」:有効な未使用の LDAP ポート番号を入力します。(デフォルトは 389)
Identity Synchronization for Windows で設定ディレクトリとの通信に SSL (Secure Socket Layer) を使用する場合は、「このポートに SSL を使用する」ボックスにチェックマークを付けます。
 - 「ユーザー DN」:管理者の(バインド)識別名を入力します。たとえば、**uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot** のように指定します。
 - 「パスワード」:管理者のパスワードを入力します。
- 指定された設定ディレクトリが照会され、そのディレクトリが管理するすべてのディレクトリサーバーが特定されます。

注 - Identity Synchronization for Windows では、Sun Java System Directory Server ソースごとに1つのルートサフィックスのみがサポートされます。

設定ディレクトリの編集と削除

「設定ディレクトリ」ダイアログボックスでは、次のように、設定ディレクトリの一覧を管理することもできます。

- 一覧から設定ディレクトリを選択し、「編集」ボタンをクリックします。「設定ディレクトリの編集」ダイアログが表示され、ホスト、ポート、セキュリティー保護されたポート、ユーザー名、パスワードの各パラメータを変更できます。
 - 一覧から設定ディレクトリを選択して「削除」をクリックすると、そのディレクトリが一覧から削除されます。
- d. 「OK」をクリックして「設定ディレクトリ」ダイアログボックスを閉じます。新しく選択した設定ディレクトリのルートサフィックスが一覧に表示されます。

Directory Server ではデフォルトで、マシンの DNS ドメインエントリのコンポーネントに対応するプレフィックスを持つルートサフィックスが作成されます。次の形式のサフィックスが使用されます。

`dc=your_machine's_DNS_domain_name`

つまり、マシンのドメインが `example.com` であれば、サーバーのサフィックスを `dc=example`, `dc=com` に設定するようにします。選択したサフィックスで命名するエントリは、ディレクトリ内にすでに存在している必要があります。

- e. ルートサフィックスを選択し、「次へ」をクリックします。

「優先サーバーの指定」パネルが表示されます (161 ページの「Sun Java System ディレクトリソースの作成」を参照)。

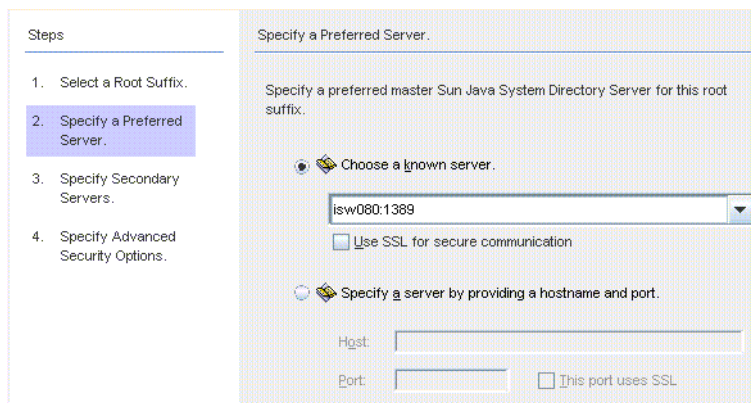


図 6-10 優先サーバーの指定

Identity Synchronization for Windows は、優先 Directory Server を使用して、Directory Server マスターに加えられた変更を検出します。優先サーバーは、Windows システムで加えられた変更が Sun Java System Directory Server システムに適用される一次的な場所としても機能します。

優先マスターサーバーに障害が発生した場合は、優先サーバー(マスター)がオンラインに復帰するまで、副サーバーに変更を格納できます。

3 次のいずれかの方法で、優先サーバーを選択します。

- 「既知のサーバーの選択」オプションを選択し、ドロップダウンリストからサーバー名を選択します。

注-リストには、稼働している Directory Server のみが表示されます。サーバーが一時的にダウンしている場合は、「ホスト名とポートを入力してサーバーを指定」オプションを選択し、サーバー情報を手動で入力します。

Directory Server が通信に SSL を使用するように設定する場合は、「セキュア通信に SSL を使用」ボックスを有効にします。ただし、この機能を有効にすると、インストール後に追加の設定手順が必要になります。詳細については、[262 ページの「Directory Server での SSL の有効化」](#)を参照してください。

- 「ホスト名とポートを入力してサーバーを指定」オプションを選択し、サーバーのホスト名とポートを各テキストフィールドに入力します。

指定したポートで SSL を使用する場合は、「このポートに SSL を使用する」チェックボックスにチェックマークを付けます。

4 「次へ」をクリックして「二次サーバーを指定します。」パネルを表示します。

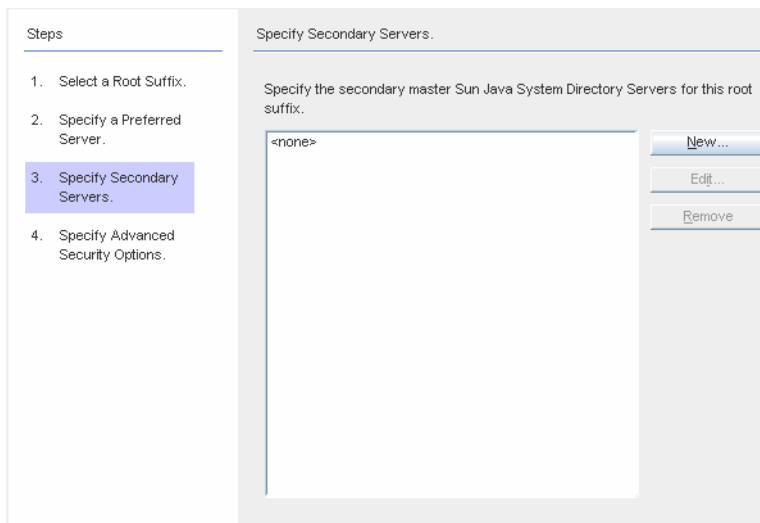


図 6-11 フェイルオーバーサポート用の副サーバーの指定

副サーバーを追加、編集、または削除できます。

- 「新規」ボタンをクリックすると、「Sunディレクトリソースを追加」ダイアログボックスが表示されます。ホスト名、ポート、ユーザーDN、パスワードを入力し、「OK」をクリックします。これらのフィールドの詳細については、[手順c](#)を参照してください。
 - 「編集」ボタンをクリックすると、「Sunディレクトリソースを編集」ダイアログボックスが表示されます。ホスト名、ポート、ユーザーDN、パスワードを入力し、「OK」をクリックします。これらのフィールドの詳細については、[手順c](#)を参照してください。
 - 「二次サーバー」の一覧で、削除するサーバーを選択し、「削除」ボタンをクリックします。
- 5 副 **Directory Server** を指定するには、一覧からサーバー名を選択し、「次へ」をクリックします。

注-

- 指定する Directory Server が稼働していない場合、サーバー名は一覧に表示されません。
- Sun ディレクトリソースの優先サーバーと副サーバーの両方に、同じホスト名とポートを使用しないでください。
- セキュリティー保護されたポート機能を有効にすると、インストール後に追加の設定手順が必要になります。詳細については、[262 ページの「Directory Server での SSL の有効化」](#)を参照してください。

副サーバーを指定しない場合は、「次へ」をクリックしてください。

- 6 セキュリティーで保護された SSL 通信を使用する場合は、次の注意を読み、どちらか一方または両方のオプションにチェックマークを付けます。

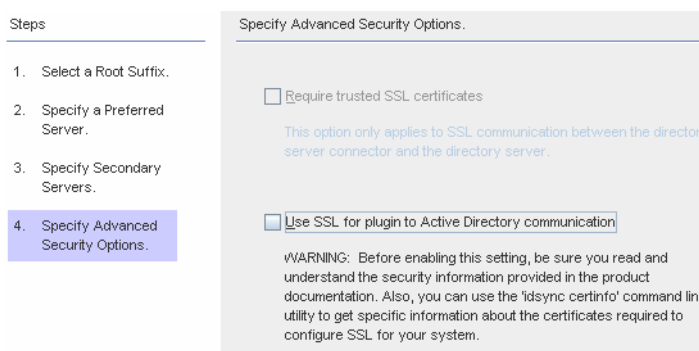


図 6-12 拡張セキュリティーオプションの指定

注-ユーザーバインドまたはパスワード変更を行う各 Directory Server (マスター、レプリカ、またはハブ) にディレクトリサーバープラグインをインストールします。

ディレクトリサーバープラグインでパスワードと属性を Active Directory と同期させる場合は、ユーザーとそのパスワードを検索するために、プラグインを Active Directory にバインドします。また、プラグインによって、セントラルログと Directory Server のログにログメッセージが書き込まれます。デフォルトでは、これらの通信に SSL は使用されません。

- チャネル通信のみを暗号化する場合、またはチャネル通信を暗号化し、証明書を使用して Directory Server とディレクトリサーバーコネクタの間で参加者の ID を確実に検証するには、「信頼できる SSL の証明書を要求」ボックスにチェックマークを付けます。

証明書を信頼しない場合は、チェックマークを外します。

- Active Directory ディレクトリサーバープラグインと Active Directory の間の通信にセキュリティで保護された SSL を使用する場合は、「プラグインと Active Directory の通信に SSL を使用」ボックスにチェックマークを付けます。

これらの機能を有効にすると、インストール後に追加設定が必要になります。262 ページの「[Directory Server での SSL の有効化](#)」を参照してください。

- 各ディレクトリサーバープラグインとコネクタのいずれかまたは両方の証明書データベースに追加する証明書は、`idsync certinfo` コマンド行ユーティリティを使用して確認できます。288 ページの「[certinfo の使用](#)」を参照してください。
- 主 Directory Server と副 Directory Server がマルチマスターレプリケーション (MMR) 配備の一部である場合は、付録 E 「[レプリケートされた環境での Identity Synchronization for Windows のインストールの注意点](#)」を参照してください。

- 7 「拡張セキュリティオプションの指定」パネルの設定が完了したら、「完了」をクリックします。

ナビゲーションツリーの「ディレクトリソース」の下に、選択したディレクトリソースが追加され、「Directory Server の準備を直ちに行いますか？」ダイアログボックスが表示されます。

Identity Synchronization for Windows で使用できるように Directory Server を準備します。この作業は今実行しても、あとで実行してもかまいません。ただし、コネクタをインストールする前に Directory Server の準備を完了してください。コネクタのインストール手順については、第 7 章「[コネクタのインストール](#)」を参照してください。

- Directory Server の準備をすぐに行う場合は「はい」をクリックしてウィザードを起動し、168 ページの「[Sun ディレクトリソースの準備](#)」に進みます。
- この作業をあとで行う場合は「いいえ」をクリックし、172 ページの「[Active Directory ソースの作成](#)」に進みます。

Sun ディレクトリソースの準備

この節では、Identity Synchronization for Windows で使用できるように Sun ディレクトリソースを準備する方法について説明します。

Directory Server の準備では次の作業を行います。

- 優先ホストで使用できる旧バージョン形式の更新履歴ログデータベースとアクセス制御インスタンスを作成する
- 優先ホストで使用できるコネクタユーザーとユーザーアクセス制御インスタンスを作成する
- 優先ホストと副ホストで等価インデックスを作成する

注-

- コンソールを使用する代わりに `idsync prepds` コマンド行ユーティリティーを使用して Directory Server を準備することもできます。詳細については、[291 ページの「prepds の使用」](#)を参照してください。
- `idsync prepds` コマンド行ユーティリティーを使用して Directory Server を準備するには、使用するホストとサフィックスの把握とディレクトリマネージャーの資格が必要になります。

Directory Server の準備には、「Directory Server の準備」ウィザードを使用できません。

図 6-13 ディレクトリマネージャーの資格の入力

注- このウィザードにアクセスするには、次のいずれかの方法を使用します。

- 「Directory Server の準備を直ちに行いますか？」ダイアログボックスが表示されたときに「はい」ボタンをクリックします。
- 「設定」タブの「Sun ディレクトリソース」パネルで「Directory Server の準備」ボタンをクリックします。

▼ Directory Server ソースを準備する

- 1 ディレクトリマネージャーアカウントの次の資格を入力します。
 - 「ディレクトリマネージャーユーザー名」

- 「ディレクトリマネージャーパスワード」
副ホストを使用している場合は (MMR 構成)、「二次ホスト」オプションが設定可能になるので、これらのホストの資格も指定します。
- 2 入力が完了したら、「次へ」をクリックして「準備設定の指定」パネルを表示します。

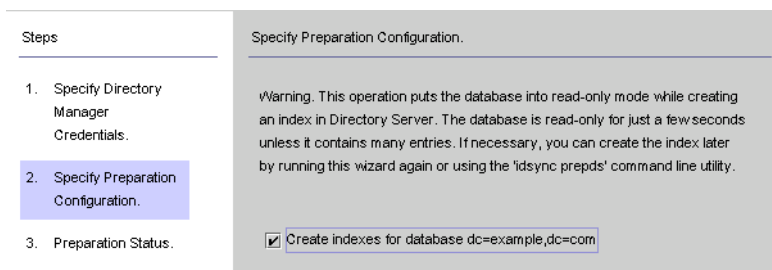


図 6-14 準備設定の指定

警告メッセージを読み、Directory Server インデックスをすぐに作成するか、あとで作成するかを決めます。

注 -

- データベースのサイズによっては、この処理に少し時間がかかることがあります。
 - データベースが読み取り専用モードの場合は、データベース内の情報を更新できません。
 - データベースをオフラインにすると、インデックスを高速に作成できます。
 - インデックスをすぐに作成するときは、「データベース <データベース名> のインデックスの作成」ボックスにチェックマークを付け、「次へ」をクリックします。
 - インデックスをあとで(手動またはもう一度ウィザードを実行して)作成する場合は、「データベース <データベース名> のインデックスの作成」ボックスのチェックマークを外し、「次へ」をクリックします。
- 3 「準備状態」パネルが表示され、Directory Server の準備の進捗状況に関する情報が示されます。
- メッセージ区画の下部に「成功」メッセージが表示されたら、「完了」をクリックします。

- エラーメッセージが表示された場合は、指摘された問題を解決してから、操作を続行します。詳細については、エラーログ(「状態」タブを参照)を確認してください。
- 4 コンソールの「設定」タブに戻ります。ナビゲーションツリーで **Sun** ディレクトリソースノードを選択し、「**Sun** ディレクトリソース」パネルを表示します。

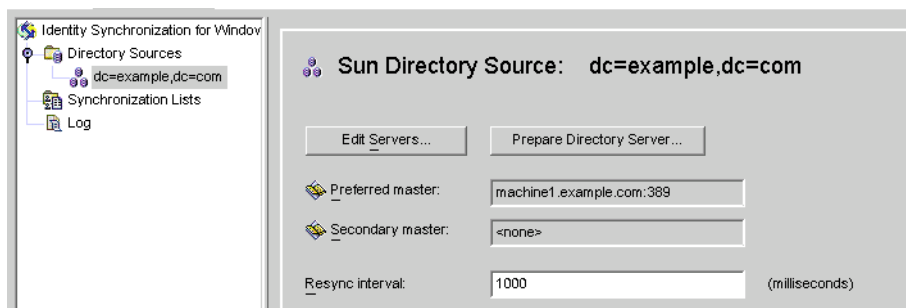


図 6-15 「Sun ディレクトリソース」パネル

このパネルから、次のタスクを実行できます。

- 「サーバーの編集」: このボタンをクリックすると、「Sun Java System ディレクトリソースの定義」パネルが表示され、サーバーの設定パラメータを変更できます。操作方法については、161 ページの「Sun Java System ディレクトリソースの作成」を参照してください。

注-優先 Sun ディレクトリソースの旧バージョン形式の更新履歴ログデータベースを再作成する場合、デフォルトのアクセス制御設定が適用されるとディレクトリサーバーコネクタはデータベースの内容を読み込みません。

新しい旧バージョン形式の更新履歴ログデータベースのアクセス制御設定を復元するには、idsync prepds を実行するか、またはコンソールで適切な Sun ディレクトリソースを選択して「Directory Server の準備」ボタンをクリックします。

- 「**Directory Server** の準備」: Directory Server を準備するときは、このボタンをクリックし、168 ページの「Sun ディレクトリソースの準備」の操作手順に従います。
インデックスが削除された場合や、旧バージョン形式の更新履歴ログデータベースを失った場合など、最初にサーバーを準備したあとで Directory Server に変更が生じたときは、サーバーの準備を再度実行できます。
- 再同期間隔: ディレクトリサーバーコネクタが変更を確認する頻度を指定します。(デフォルトは 1000 ミリ秒)

- 5 同期対象の **Sun Java System Directory Server** エンタープライズ内のユーザー入力ごとに **Directory Server** ディレクトリソースを追加します。
完了したら、少なくとも1つの Windows ディレクトリソースを作成します。
 - Active Directory ディレクトリソースを作成する場合は、172 ページの「**Active Directory ソースの作成**」に進みます。
 - Windows NT ディレクトリソースを作成する場合は、180 ページの「**Windows NT SAM ディレクトリソースの作成**」に進みます。

Active Directory ソースの作成

Active Directory ディレクトリソースは、ネットワーク上で同期させる Windows ドメインごとに追加するようにしてください。

Active Directory の各配備には、すべての Active Directory ドメインに適用されるグローバル情報がすべて記録されたグローバルカタログが、少なくとも1つあります。グローバルカタログにアクセスするには、デフォルトのアクセス権を変更していなければ、通常ユーザーに与えられている権限で十分です。

注 - 各 Active Directory サーバーをグローバルカタログとし、配備に複数のグローバルカタログを持たせることもできますが、指定が必要なグローバルカタログの数は1つだけです。

▼ ネットワークに **Windows Active Directory** サーバーを設定および作成する

ネットワークに Windows Active Directory サーバーが存在する場合は、次の手順を実行します。

- 1 ナビゲーションツリーで「ディレクトリソース」ノードを選択し、「ディレクトリソース」パネルの「新規 **Active Directory** ソース」ボタンをクリックします。
「Windows グローバルカタログ」ダイアログボックスが表示されます。

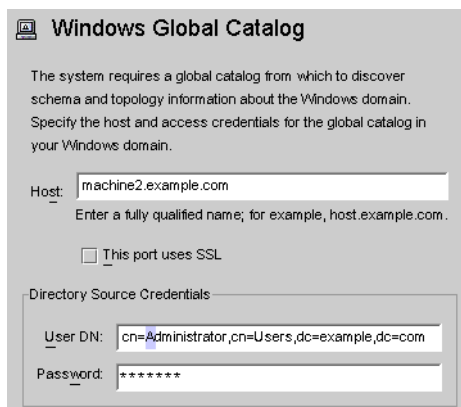


図 6-16 「Windows グローバルカタログ」ダイアログボックス

- 2 次の情報を入力し、「OK」をクリックします。
 - 「ホスト」: Active Directory フォレストのグローバルカタログを保持するマシンの完全修飾ホスト名を入力します。
例: **machine2.example.com**
 - 「このポートに SSL を使用する」: Identity Synchronization for Windows でグローバルカタログとの通信に SSL ポートを使用する場合は、このオプションを有効にします。
 - 「ユーザー DN」: 管理者の (バインド) 完全修飾識別名を入力します。スキーマを参照し、システムで使用できる Active Directory ドメインを特定できる資格があれば、どのような DN でも指定できます。
例: **cn=Administrator,cn=Users,dc=example,dc=com**
 - 「パスワード」: 指定したユーザーのパスワードを入力します。
- 3 次のような「Active Directory ソースの定義」ウィザードが表示されます。

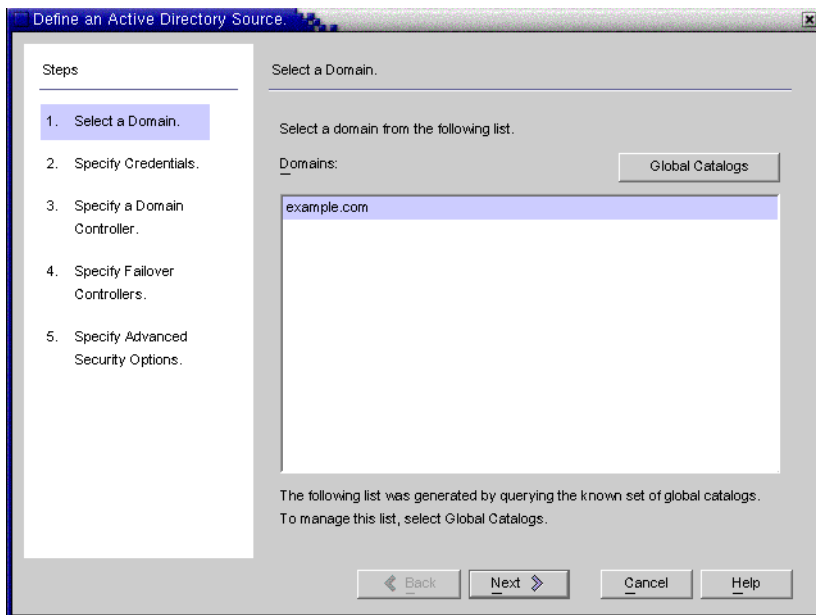


図 6-17 「Active Directory ソースの定義」ウィザード

Active Directory グローバルカタログが照会されて、存在するその他のドメインが特定され、それらのドメインが「ドメイン」の一覧に表示されます。

- 4 一覧から名前を選択して **Active Directory** ドメインを指定し、「OK」をクリックします。

使用するドメインが一覧に表示されない場合は、次の手順を使用して、そのドメインを認識するグローバルカタログを追加します。

 - a. 「グローバルカタログ」ボタンをクリックして「グローバルカタログ」ウィザードを表示します。

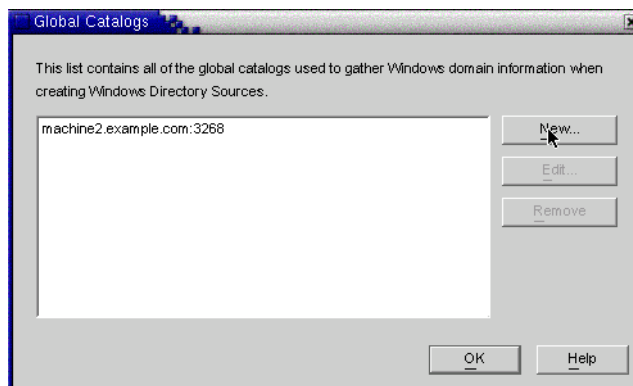


図 6-18 新しいグローバルカタログの指定

- b. 「新規」ボタンをクリックします。
 - c. 「Windows グローバルカタログ」ダイアログボックスが表示されるので、グローバルカタログのホスト名と、ディレクトリソースの資格(手順 2 を参照)を入力し、「OK」をクリックします。
 - d. 「グローバルカタログ」の一覧に新しいグローバルカタログとポートが表示されます。カタログ名を選択し、「OK」をクリックします。
 - e. さらにグローバルカタログ(ドメイン)をシステムに追加する場合は、これらの手順を繰り返します。
 - f. 完了したら、「ドメインの選択」区画の「次へ」ボタンをクリックします。
- 5 「クレデンシャルの指定」パネルが表示されたら、「ユーザー DN」フィールドの値を確認します

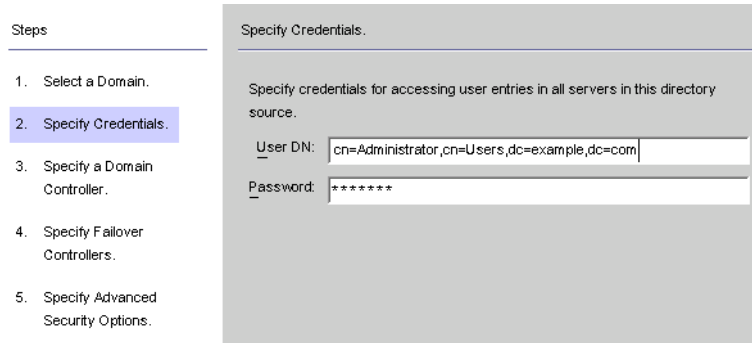


図 6-19 この Active Directory ソースの資格の指定

管理者の識別名が「ユーザー DN」フィールドに自動的に入力されない場合、または自動入力された管理者の資格を使用しない場合は、ユーザー DN とパスワードを手動で入力します。

Active Directory ソースを設定するときは、Active Directory コネクタが Active Directory との接続に使用できるユーザー名とパスワードを指定します。

注 - コネクタには特定のアクセス権が必要です。次に示すように、最小限の権限は、同期の方向によって異なります。

- Active Directory から Directory Server への同期フローのみを設定する場合は、Active Directory コネクタ用に指定するユーザーには多くの特別な権限は必要ありません。通常のユーザーに、同期対象ドメインで「すべてのプロパティーを読み取る」権限が追加されているだけで十分です。
- Directory Server から Active Directory への同期フローを設定する場合は、同期によって Active Directory 内のユーザーエントリが変更されるため、コネクタユーザーにはもっと多くの権限が必要になります。この設定では、コネクタユーザーは「フルコントロール」権限を持つユーザーか、または管理者グループのメンバーにします。

-
- 6 「次へ」をクリックし、「ドメインコントローラの指定」パネルを開きます。

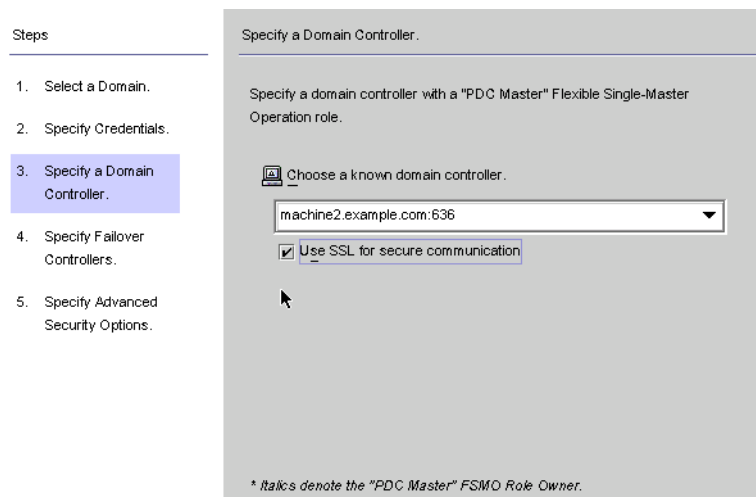


図 6-20 ドメインコントローラの指定

このパネルでは、指定したドメイン内で同期するコントローラを選択します。ドメインコントローラ概念は、Directory Server の優先サーバーに似ています。

選択している Active Directory ドメインに複数のドメインコントローラがあるときは、同期のプライマリドメインコントローラ FSMO (Flexible Single Master Operation) ロールを持つドメインコントローラを選択します。

デフォルトでは、すべてのドメインコントローラで行われたパスワード変更はただちにプライマリドメインコントローラ FSMO ロール所有者にレプリケートされ、このドメインコントローラを選択すると、パスワード変更はただちに Identity Synchronization for Windows によって Directory Server と同期されます。

配備によっては、PDC との間に大きなネットワーク「距離」があるために同期が大幅に遅れるので、Windows レジストリに `AvoidPdcOnWan` 属性が設定されることがあります。詳細については、*Microsoft* サポート技術情報の記事 232690 を参照してください。

- 7 ドロップダウンリストからドメインコントローラを選択します。
- 8 **Identity Synchronization for Windows** コネクタがドメインコントローラとの通信にセキュリティ保護されたポートを使用するように設定する場合は、「セキュア通信に SSL を使用」ボックスにチェックマークを付けます。

注 - Microsoft Certificate Server を使用する場合は、Active Directory コネクタに CA 証明書が自動的にインストールされます。それ以外の場合は、Active Directory コネクタに CA 証明書を手動で追加します (264 ページの「Active Directory コネクタでの SSL の有効化」を参照)。初期設定後にフローの設定を変更する場合にも、この手順を適用します。

- 9 完了したら、「次へ」をクリックします。

「フェイルオーバーコントローラの指定」パネルが表示されます (172 ページの「Active Directory ソースの作成」を参照)。このパネルでは、任意の数のフェイルオーバードメインコントローラを指定できます。

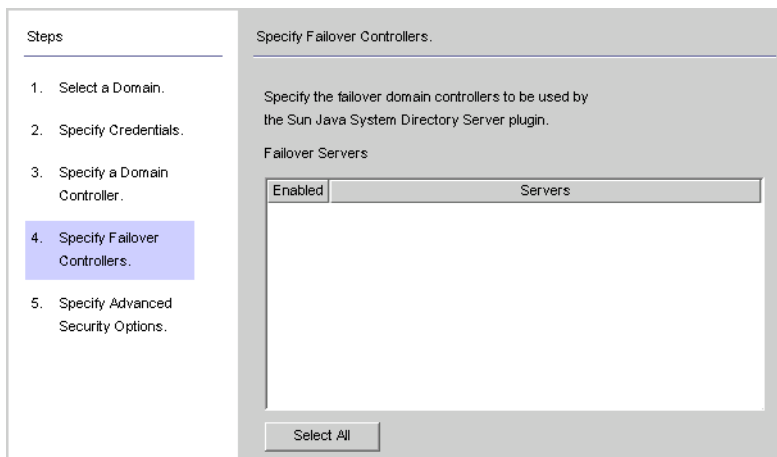


図 6-21 フェイルオーバーコントローラの指定

Active Directory コネクタが通信する Active Directory ドメインコントローラは 1 つだけであるため、Identity Synchronization for Windows では、そのコネクタで適用されるフェイルオーバーの変更はサポートされません。ただし、ディレクトリサーバープラグインは、Directory Server のパスワード変更を検証するときに、任意の数のドメインコントローラと通信します。

Directory Server は、Active Directory ドメインコントローラへの接続を試行し、そのドメインコントローラが使用できない場合は、指定されたフェイルオーバードメインコントローラへの接続を繰り返し試行します。

- 10 「フェイルオーバーサーバー」の一覧から 1 つまたは複数のサーバー名を選択するか、または「すべてを選択」ボタンをクリックして一覧のすべてのサーバーを指定し、「次へ」をクリックします。

- 11 「拡張セキュリティーオプションの指定」パネルが表示されます。
- 「信頼できる SSL の証明書を要求」オプションは、「ドメインコントローラの指定」パネルで「セキュア通信に SSL を使用」ボックスを有効にした場合にのみアクティブ (選択可能な状態) になります。

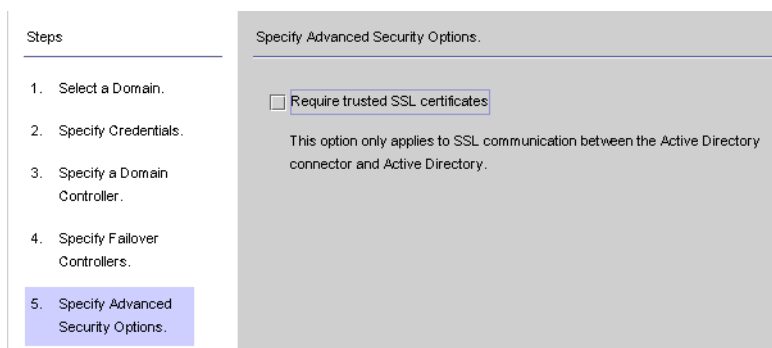


図 6-22 拡張セキュリティーオプションの指定

- 「信頼できる SSL の証明書を要求」ボックスが無効になっている場合 (デフォルト設定)、Active Directory コネクタは SSL 経由で Active Directory に接続し、Active Directory から渡された証明書が信頼されているかどうかを検証しません。
このオプションを無効にすると、Active Directory 証明書データベースに Active Directory 証明書をインストールする必要がなくなるので、セットアップ手順が簡単になります。
- 「信頼できる SSL の証明書を要求」ボックスを有効にすると、Active Directory コネクタは SSL 経由で Active Directory に接続し、Active Directory から渡された証明書が信頼されているかどうかを検証します。

注 - コネクタの証明書データベースに Active Directory 証明書を追加してください。手順については、[266 ページの「Active Directory 証明書のコネクタの証明書データベースへの追加」](#)を参照してください。

- 12 「拡張セキュリティーオプション」パネルの設定が完了したら、「完了」をクリックします。
- ナビゲーションツリーの「ディレクトリソース」の下に、新しく指定した Active Directory ディレクトリソースが追加されます。
- 13 その Active Directory ディレクトリソースノードを選択し、「Active Directory ソース」パネルを表示します。

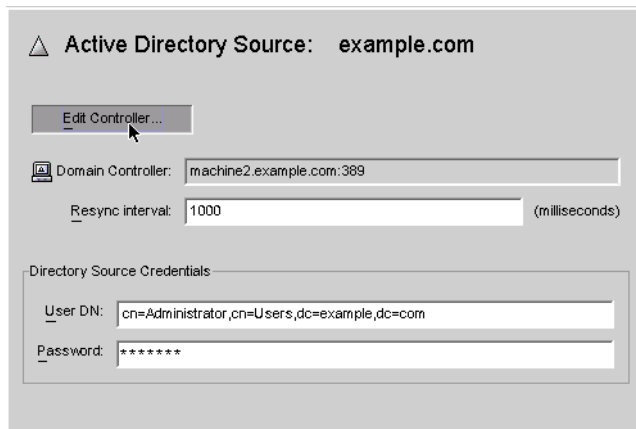


図 6-23 「Active Directory ソース」 パネル

このパネルから、次のタスクを実行できます。

- 「コントローラの編集」: このボタンをクリックすると、「ドメインコントローラの指定」パネルが再度開き、ドメインコントローラの設定パラメータを変更できます。操作方法については、[172 ページの「Active Directory ソースの作成」](#)を参照してください。
- 「再同期間隔」: Active Directory コネクタが変更を確認する頻度を指定します。(デフォルトは 1000 ミリ秒)
- 「ディレクトリソースのクレデンシャル」: 指定されているユーザー DN とパスワードのいずれかまたは両方を変更します。

Windows NT SAM ディレクトリソースの作成

この節では、Identity Synchronization for Windows を配備できる Windows NT SAM ディレクトリソースの作成方法を説明します。

▼ Windows NT に Identity Synchronization for Windows を配備する

- 1 ナビゲーションツリーで「ディレクトリソース」ノードを選択し、「新規 Windows NT SAM ディレクトリソース」ボタンをクリックします。



図 6-24 「ディレクトリソース」パネル

- 2 「Windows NT SAM ディレクトリソースの定義」パネルが表示されたら、指示に従って Windows NT ドメイン名を確認し、「ドメイン」フィールドに一意的な NT ディレクトリソースドメイン名を入力します。完了したら、「次へ」をクリックします。

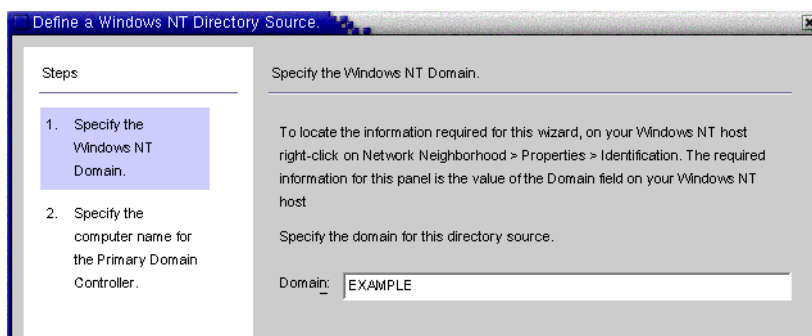


図 6-25 Windows NT SAM ドメイン名の指定

- 3 「プライマリドメインコントローラのコンピュータ名の指定」パネルが表示されたら、指示に従ってプライマリドメインコントローラのコンピュータ名を確認し、「コンピュータ名」フィールドにその情報を入力します。

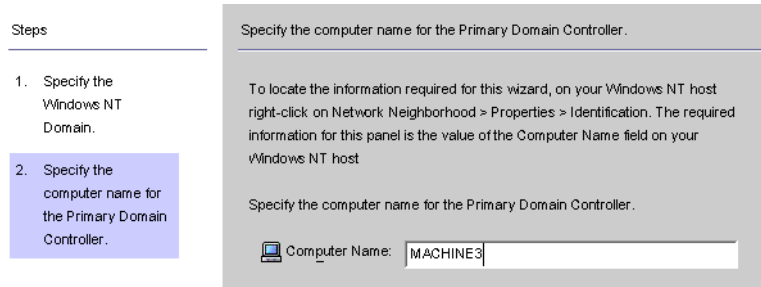


図 6-26 プライマリドメインコントローラ名の指定

4 「完了」をクリックします。

ナビゲーションツリーの「ディレクトリソース」の下に、新しく指定した Windows NT SAM ディレクトリソースが追加されます。新しいディレクトリソースのノードを選択して「Windows NT SAM ディレクトリソース」パネルを表示します。

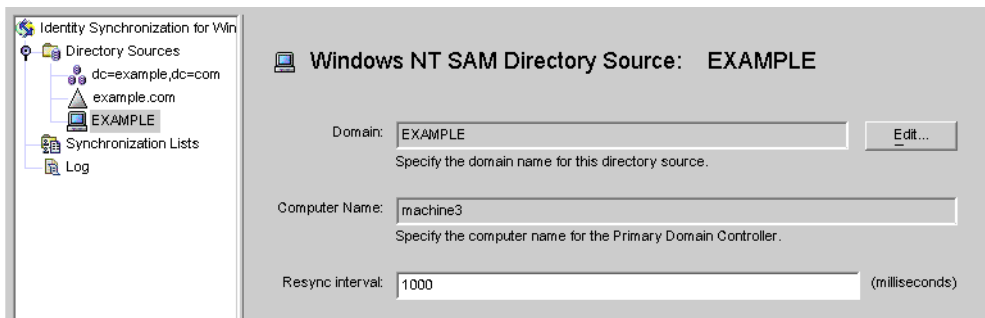


図 6-27 「Windows NT SAM ディレクトリソース」パネル

このパネルから、次のタスクを実行できます。

- 「編集」: このボタンをクリックすると、「ドメインコントローラの指定」パネルが再度開き、ドメインコントローラの設定パラメータを変更できます。操作方法については、[172 ページの「Active Directory ソースの作成」](#)を参照してください。
- 「再同期間隔」: Windows NT に加えられた変更を Identity Synchronization for Windows が確認する頻度を指定します。(デフォルトは 1000 ミリ秒)

5 ネットワーク上の Windows NT マシンごとに Windows NT ディレクトリソースを追加します。

Windows NT SAM ディレクトリソースの作成が完了したら、同期対象にする属性の選択とマッピングを行うことができます。[183 ページの「ユーザー属性の選択とマッピング」](#)に進みます。

ユーザー属性の選択とマッピング

Directory Server と Windows のディレクトリソースの作成と設定が完了したら、同期対象にするユーザー属性を選択し、それらの属性をシステム間でマッピングします。

この節で説明する内容は次のとおりです。

- 183 ページの「属性の選択とマッピング」
- 185 ページの「パラメータ化されたデフォルト属性値の作成」
- 186 ページの「スキーマソースの変更」

属性の選択とマッピング

次の2種類の属性があります。

- 重要: ユーザーエントリの作成または変更時にシステム間で同期される属性。
- 作成: ユーザーエントリの作成時にのみシステム間で同期される属性。

各プラットフォームで使用されるスキーマによっては、一部の作成属性は必須となります。これらの属性は、パスワードの同期に必要とされるので、Active Directory サーバー上で user オブジェクトクラスエントリを正しく作成するために、Directory Server 属性にマッピングします。

この節では、同期対象にするユーザー属性を選択する方法、およびそれらの属性を1対1の関係でマッピングする方法について説明します。この属性マッピングにより、Directory Server の属性を指定すると、Active Directory 環境と Windows NT 環境のいずれかまたは両方の対応する属性が表示され (Active Directory または Windows NT の属性を指定すると、Directory Server 環境の対応する属性が表示される)、対応する Windows 属性の値が同期されるようになります。

▼ 同期対象の属性を選択してマッピングする

- 1 ナビゲーションツリーの最上部にある「Identity Synchronization for Windows」ノードを選択します。

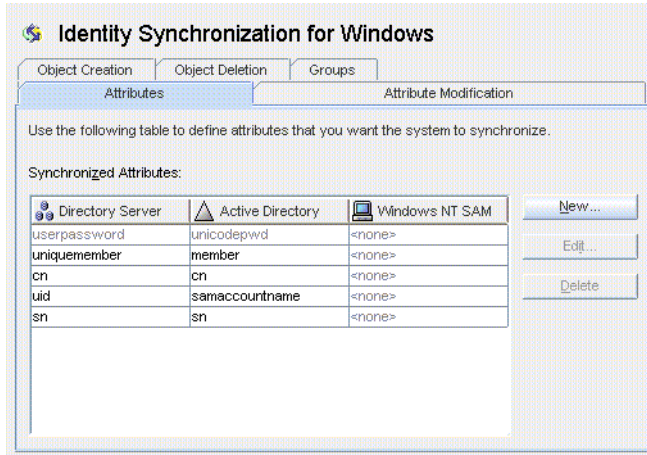


図 6-28 「属性」タブ

注 - グループ同期機能が有効になっている場合、Directory Server の *uniquemember* 属性と Active Directory の *member* 属性は内部的にマッピングされ、前の図のようにコンソールに表示されます。

- 「属性」タブを選択し、「新規」ボタンをクリックします。
「有効属性マッピングの定義」ダイアログボックスが表示されます。このダイアログボックスで、Directory Server から Windows システム (Active Directory と Windows NT のいずれかまたは両方) に属性をマッピングします。

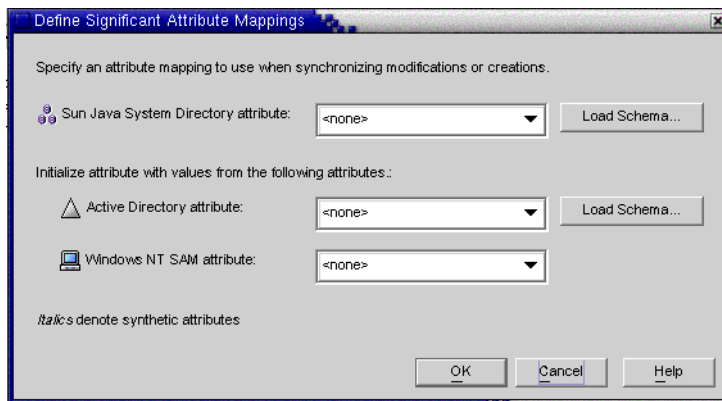


図 6-29 重要属性マッピングの定義

注 - どの作成属性が Directory Server (または Active Directory) の必須作成属性となるかは、Sun 側 (または Active Directory 側) のユーザーエントリに設定されているオブジェクトクラスによって異なります。

Directory Server のデフォルトのオブジェクトクラスには *inetOrgPerson* が自動的に使用され、Active Directory のスキーマはグローバルカタログの指定時に読み込まれます。そのため、デフォルトのスキーマを変更する場合以外は、「スキーマの読み込み」ボタンを使用しません。

デフォルトのスキーマソースを変更する場合は、186 ページの「スキーマソースの変更」を参照してください。

- 3 Sun Java System の属性ドロップダウンリストから属性を選択し (たとえば、*cn* など)、それに対応する属性を **Active Directory** と **Windows NT SAM** のいずれかまたは両方の属性ドロップダウンメニューから選択します。
- 4 完了したら、「OK」をクリックします。
- 5 別の属性を指定する場合は、手順 2～4 を繰り返します。

完了後の同期対象属性の表は、次の図のようになります。この図では、Directory Server の *userpassword*、*cn*、および *telephonenumber* 属性が、Active Directory の *unicodepwd*、*cn*、および *telephonenumber* 属性にマッピングされたことが示されています。

Directory Server	Active Directory	Windows NT SAM
<i>userpassword</i>	<i>unicodepwd</i>	<i>user_password</i>
<i>cn</i>	<i>cn</i>	<none>
<i>telephonenumber</i>	<i>telephonenumber</i>	<none>

図 6-30 完了後の同期対象属性の表

パラメータ化されたデフォルト属性値の作成

Identity Synchronization for Windows では、別の作成属性または重要属性を使用して、パラメータ化されたデフォルト属性値を作成できます。

パラメータ化されたデフォルト属性値を作成するには、式文字列内の既存の作成属性または重要属性の名前の前後にパーセント記号を付けます (*%attribute_name%*)。たとえば、*homedir=/home/%uid%* や *cn=%givenName% %sn%* のようにします。

これらの属性値を作成した場合、次のように使用できます。

- 1 つの作成式で複数の属性を使用できます (*cn=%givenName% %sn%*)。
- *A=0* の場合、*B* はデフォルト値を 1 つだけ持つことができます。

- パーセント記号を通常の文字として使用する場合は、円記号(\)を使用します。たとえば `diskUsage=0\%` のようにします。
- 循環式の置換条件を持つ式を使用しないでください。たとえば、`description=%uid%` を指定する場合は、`uid=%description%` を使用できません。

注-グループ同期が有効になっている場合は、次のことを確認してください。

1. Active Directory でサポートされる作成式は `cn=%cn%` です。
2. 作成式はユーザーとグループの両方に共通であるため、作成式には、グループオブジェクトクラスに属する有効な属性名も含まれます。

例: Directory Server では、属性 `sn` は `groupofuniquenames` オブジェクトクラスに属しません。したがって、グループオブジェクトでは、次の作成式は無効になります。(ただし、ユーザーオブジェクトでは正しく機能する。)

```
cn=%cn%.%sn%
```

3. 作成式に使用される属性には、作成されるすべてのユーザー/グループエントリの値を指定します。この値をコンソールで指定できない場合は、コマンド行インタフェースを使用して指定できます。

スキーマソースの変更

デフォルトのスキーマソースが自動的に設定されますが、デフォルトスキーマを変更できます。

▼ デフォルトのスキーマソースを変更する

- 1 「有効属性マッピングの定義」ダイアログボックスで、「スキーマの読み込み」ボタンをクリックします。
「スキーマソースの選択」パネルが表示されます。

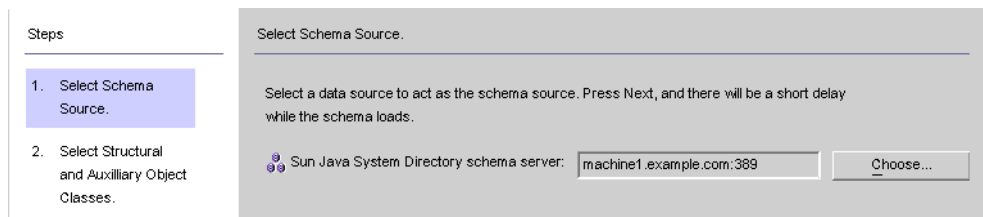


図 6-31 スキーマソースの選択

このパネルでは、スキーマの読み込み元の Sun Java System Directory Server スキーマサーバーを指定しますこのスキーマには、システムで使用できるオブジェクトクラスが含まれており、これらのオブジェクトクラスによって、ユーザーがシステムで使用できる属性が定義されます。

「Sun Java System ディレクトリスキーマサーバー」フィールドには、デフォルトの設定ディレクトリが自動的に入力されます。

- 2 別のサーバーを選択する場合は、「選択」ボタンをクリックします。

「Sun スキーマホストの選択」ダイアログボックスが表示されます。このダイアログボックスには、ディレクトリソースの管理情報を集めた設定ディレクトリの一覧が表示されます。

このダイアログボックスでは、次の操作を実行できます。

- 新しい設定ディレクトリを作成して一覧に追加する。
「新規」をクリックし、「新規設定ディレクトリ」ダイアログボックスが表示されたら、ホスト、ポート、ユーザー DN、およびパスワードを指定します。完了したら、「OK」をクリックします。
 - 既存のディレクトリを編集する。
「編集」をクリックし、「設定ディレクトリの編集」ダイアログボックスが表示されたら、ホスト、ポート、ユーザー DN、パスワードのいずれかまたはすべてを変更できます。完了したら、「OK」をクリックします。
 - ディレクトリを一覧から削除する。
一覧からディレクトリ名を選択し、「削除」ボタンをクリックします。
- 3 一覧からサーバーを選択し、「OK」をクリックします。通常、スキーマソースには Sun 同期ホストの 1 つを選択することをお勧めします。
 - 4 「次へ」ボタンをクリックして、「Structural および Auxiliary オブジェクトクラスの選択」パネルを表示します。

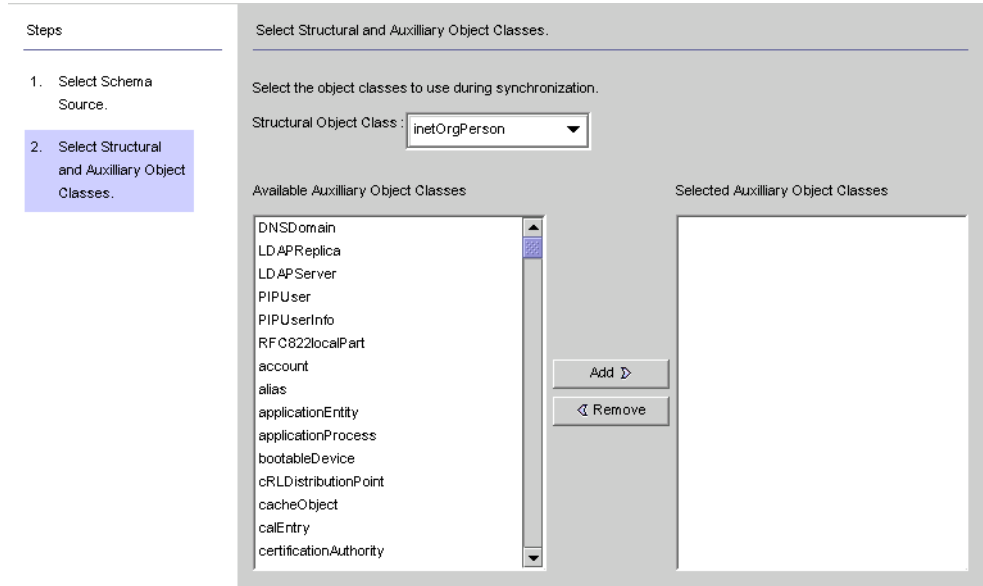


図 6-32 Structural オブジェクトクラスと Auxiliary オブジェクトクラスの選択

このパネルでは、次のように、同期対象にするオブジェクトクラスを指定します。

- **Structural** オブジェクトクラス: 選択した Directory Server から作成または同期されるエントリごとに、少なくとも 1 つの Structural オブジェクトクラスを指定します。
- **Auxiliary** オブジェクトクラス: このオブジェクトクラスでは、選択した構造クラスを補強し、同期に関する追加属性を指定します。

Structural オブジェクトクラスと Auxiliary オブジェクトクラスを指定するには、次の手順に従います。

- a. **Structural** オブジェクトクラスをドロップダウンリストから選択します。(デフォルトは *inetorgperson*)
- b. 「利用可能な **Auxiliary** オブジェクトクラス」の一覧で 1 つまたは複数のオブジェクトクラスを選択し、「追加」をクリックして選択項目を「選択された **Auxiliary** オブジェクトクラス」の一覧に移動します。

選択されたオブジェクトクラスによって、重要属性または作成属性として選択できる Directory Server ソース属性が決まります。また、必須作成属性も、ここで選択されたオブジェクトクラスによって決まります。

「選択された **Auxiliary** オブジェクトクラス」の一覧から選択項目を削除するには、そのオブジェクトクラス名を選択し、「削除」ボタンをクリックします。

- c. 完了したら、「完了」をクリックします。スキーマおよび選択したオブジェクトクラスが読み込まれます。

システム間でのユーザー属性の伝播

同期対象のユーザー属性の選択とマッピングが完了したら、Directory Server システムと Windows システム間で属性の作成、変更、および削除を伝播させる方法(フロー)を Identity Synchronization for Windows に指示します。

デフォルトでは、Identity Synchronization for Windows は次のように動作します。

- Windows から Sun Java System Directory Server への同期のみを行う
- パスワード属性のみ同期を行う (前の節で重要属性を指定している場合を除く)
- エントリの作成または削除の同期を行わない

ここでは、システム間での属性の同期を設定する方法について説明します。ここで説明する内容は、次のとおりです。

- [189 ページの「オブジェクト作成のフローの指定」](#)
- [195 ページの「オブジェクト変更のフローの指定」](#)
- [203 ページの「グループ同期の設定」](#)
- [205 ページの「アカウントのロックアウトおよびロックアウト解除の設定と同期」](#)
- [208 ページの「削除のフロー方法の指定」](#)

オブジェクト作成のフローの指定

▼ **Directory Server** システムと **Active Directory** システムの間でオブジェクト作成を伝播させる方法を指定する

- 1 「オブジェクトの作成」タブをクリックします。

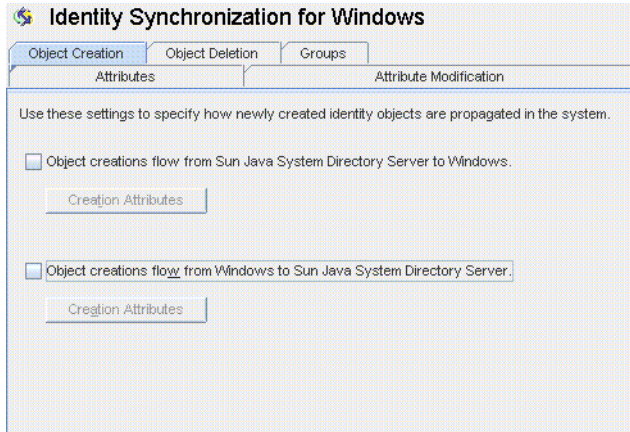


図 6-33 作成の選択と伝播

- 2 次のように、作成のフローを有効または無効にできます。
 - Directory Server 環境から Windows サーバーに作成を伝播させる場合は、「オブジェクト作成は **Sun Java System Directory Server** から **Windows** に伝播される」にチェックマークを付けます。
 - Windows 環境から Directory Server に作成を伝播させる場合は、「オブジェクト作成は **Windows** から **Sun Java System Directory Server** に伝播される」にチェックマークを付けます。
 - 双方向のフローを設定する場合は、両方のオプションにチェックマークを付けます。
 - システム間でユーザーの作成を伝播させない場合は、どちらのオプションにもチェックマークを付けません。(デフォルト)。
- 3 システム間で同期させる作成属性を追加、編集、または削除するには、選択されているオプションの下にある「作成属性」ボタンをクリックします。
「作成属性のマッピングと値」ダイアログボックスが表示されます。

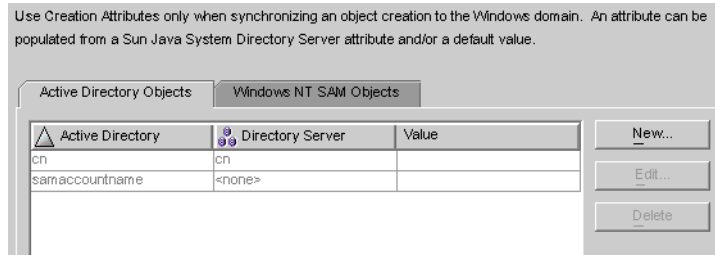


図 6-34 作成属性のマッピングと値: Directory Server から Windows

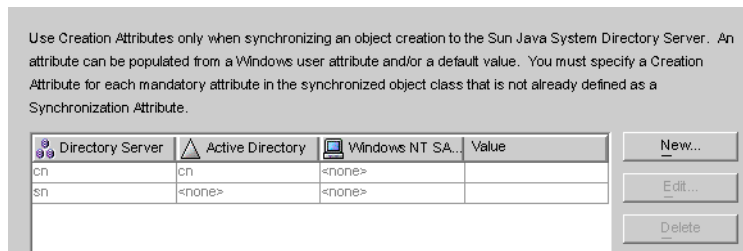


図 6-35 作成属性のマッピングと値: Windows から Directory Server

どちらかのダイアログボックスを使用して、新しい作成属性の指定、既存の属性の編集または削除を行うことができます。詳細については、191 ページの「新しい作成属性の指定」を参照してください。

注-ユーザーオブジェクトクラスの必須属性に関するスキーマ制約を満たすために、ユーザー作成時にシステム間で伝播させる追加の属性を指定する場合があります。

183 ページの「ユーザー属性の選択とマッピング」で説明したように、必須属性を変更属性として指定した場合は、追加の属性は必要ありません。

新しい作成属性の指定

次に、作成属性を追加し、Active Directory から Directory Server にマッピングする方法について説明します。Directory Server から Windows、または Windows から Directory Server に伝播させる作成属性を追加してマッピングする場合も、同様の手順になります。

▼ 新しい作成属性を指定する

- 1 「作成属性のマッピングと値」ダイアログボックスの「新規」ボタンをクリックします。
「作成属性のマッピングと値の定義」ダイアログボックスが表示されます。

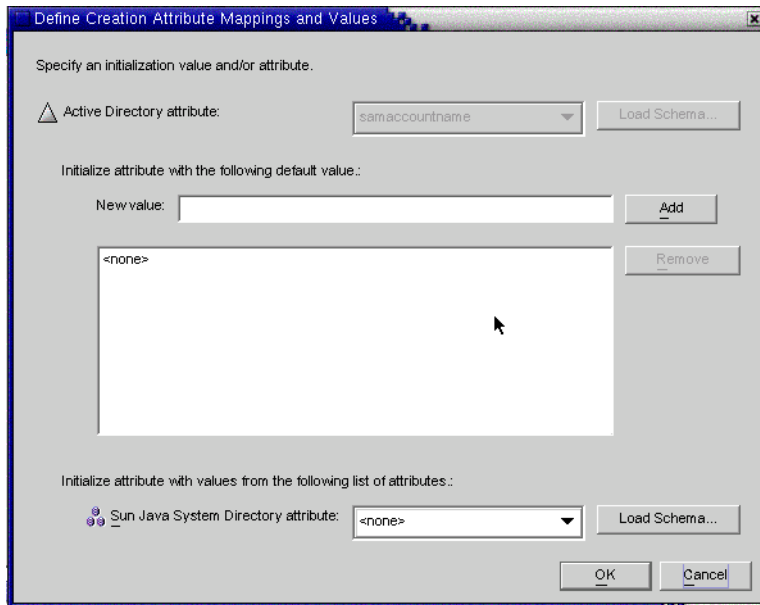


図 6-36 作成属性のマッピングと値の定義

- 2 「Active Directory 属性」ドロップダウンリストから属性値を選択します。



図 6-37 新しい Active Directory 属性の選択

Identity Synchronization for Windows では、属性が複数の値を受け付ける場合は、複数の値で属性を初期化できます。

たとえば、会社に3つのファックス番号がある場合、Sun Java System Directory Server と Active Directory の両方に facsimiletelephonenumber 属性を指定して、3つの番号を指定できます。

どの属性が複数の値を受け付けるかを把握しておきます。複数の値を受け付けない属性に複数の値を追加しようとすると、プログラムによるオブジェクト作成の実行時にエラーが発生します。

- 3 「新しい値」フィールドに値を入力し、「追加」をクリックします
一覧に属性値が追加されます。複数の属性値を追加する場合は、必要な回数だけこの手順を繰り返します。

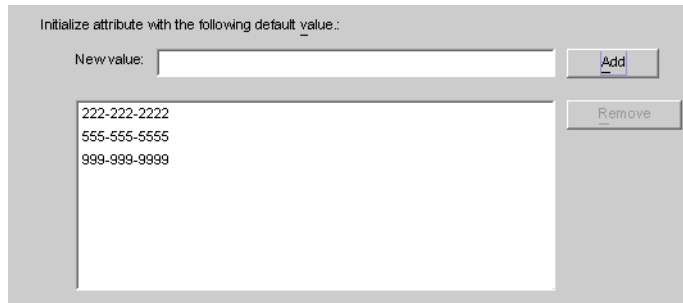


図 6-38 作成属性の複数の値の指定

- 4 属性を **Directory Server** にマッピングするには、「**Sun Java System** ディレクトリ属性」ドロップダウンリストから属性名を選択します。

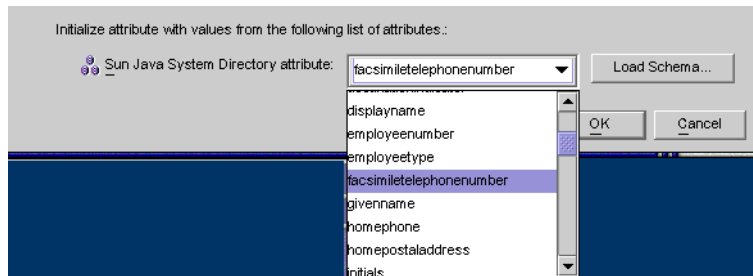


図 6-39 Directory Server 属性のマッピング

- 5 完了したら、「OK」をクリックします。
この例では、完了後の作成属性とマッピングの表は次の図のようになります。

△ Active Directory	☺ Directory Server	Value
cn	cn	
samaccountname	<none>	
facsimiletelephonenumber	facsimiletelephonenumber	[222-222-2222,555-555-55...

図 6-40 操作完了後の作成属性とマッピングの表

- 別の属性を指定する場合は、同じ手順を繰り返します。

既存の属性の編集

▼ 作成属性のマッピングまたは値を編集する

- 「オブジェクトの作成」タブをクリックし、選択されている作成オプションの下にある「作成属性」ボタンをクリックします。
- 「作成属性のマッピングと値」ダイアログボックスが表示されたら、表から属性を選択し、「編集」ボタンをクリックします。
「作成属性のマッピングと値の定義」ダイアログボックスが表示されます。
- ドロップダウンメニューを使用して、**Directory Server** と **Active Directory** (または **Windows NT**) の間の既存のマッピングを変更します。
たとえば、Sun Java System Directory Server の homephone 属性が Active Directory の othertelephone 属性にマッピングされている場合に、Active Directory 属性のドロップダウンリストを使用して、マッピング対象を homephone 属性に変更できます。
- 属性値を追加または削除することもできます。
 - 値を追加するには、「新しい値」フィールドに情報を入力し、「追加」をクリックします。
 - 値を削除するには、一覧から値を選択し、「削除」をクリックします。
- 完了したら、「OK」をクリックします。変更が適用され、「作成属性のマッピングと値の定義」ダイアログボックスが閉じます。
- もう一度「OK」をクリックして「作成属性のマッピングと値」ダイアログボックスを閉じます。

属性の削除

▼ 作成属性のマッピングまたは値を削除する

- 「オブジェクトの作成」タブをクリックし、選択されている作成オプションの下にある「作成属性」ボタンをクリックします。

- 2 「作成属性のマッピングと値」ダイアログボックスが表示されたら、表から属性を選択し、「削除」ボタンをクリックします。
属性がただちに表から削除されます。
- 3 完了したら、「OK」をクリックして「作成属性のマッピングと値」ダイアログボックスを閉じます。

オブジェクト変更のフローの指定

Sun システムと Windows システムの間でユーザー属性とパスワードの変更を伝播させる方法(フロー)を制御する場合は、「属性の修正」タブを使用します。

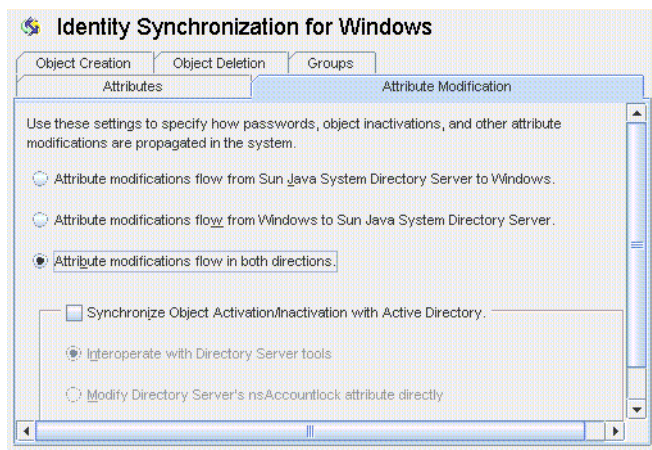


図 6-41 「属性の修正」タブ

このタブでは、次の設定を行います。

- Directory Server と Windows のディレクトリソース間で変更を伝播させる方向を指定する。
- Directory Server と Active Directory のソース間で、オブジェクトの有効化と無効化 (Active Directory では有効と無効) を同期させるかどうかを制御し、ユーザーアカウントを有効および無効にする方法を指定します。

注 - アカウントの状態を Windows NT ディレクトリソースと同期させることはできません。

方向の指定

次のいずれかのボタンを選択することで、Directory Server 環境と Windows 環境で加えられた変更をシステム間で伝播させる方法を制御します。

- 「属性の修正は **Sun Java System Directory Server** から **Windows** に伝播される」 : Directory Server 環境で加えられた変更が Windows サーバーに伝播します。
- 「属性の修正は **Windows** から **Sun Java System Directory Server** に伝播される」 (デフォルト): Windows 環境で加えられた変更が Directory Server に伝播します。
- 「属性の修正は両方向に伝播される」 : 変更は環境間で双方向に伝播します。

オブジェクトの有効化と無効化の設定と同期

「オブジェクトの有効化/無効化を Active directory と同期する」ボックスにチェックマークを付けると、Directory Server と Active Directory のソース間でオブジェクトの有効化と無効化 (Active Directory では有効と無効) を同期させることができます。

注 - 有効化と無効化を Windows NT ディレクトリソースと同期させることはできません。

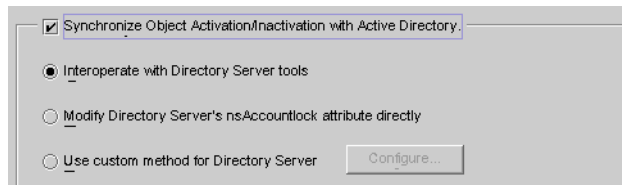


図 6-42 オブジェクトの有効化と無効化の同期

▼ オブジェクトの有効化と無効化を同期させる

- 1 「オブジェクトの有効化/無効化を **Active directory** と同期する」ボックスにチェックマークを付けます。
- 2 次のいずれかのオプションを有効にして、**Identity Synchronization for Windows** でオブジェクトの有効化と無効化を検出し、同期させる方法を指定します。
 - 197 ページの「Directory Server ツールとの相互運用」
 - 198 ページの「Directory Server の nsAccountLock 属性の直接修正」

注 - これらのオプションは相互に排他的です。

- 199 ページの「Directory Server のカスタムメソッドの使用」

Directory Server ツールとの相互運用

Directory Server コンソールまたはコマンド行ツールを使用してオブジェクトを有効化または無効化する場合は、このオプションを選択します。このオプションを選択すると、Identity Synchronization for Windows では `nsAccountLock` 属性を直接設定または削除できなくなります。また、ほかのロール (`cn=nsdisabledrole`, `database suffix` など)、またはほかのロール内に入れ子にされたロール (`cn=nsdisabledrole`, `database suffix` や `cn=nsmanageddisabledrole`, `database suffix` など) を使用して無効化されたオブジェクトも検出できなくなります。

- Identity Synchronization for Windows では、オブジェクトを有効にする場合、`nsroledn` 属性から `cn=nsmanageddisabledrole`, `database suffix` 値が削除されます。
- オブジェクトを無効にする場合は、`nsroledn` に `cn=nsmanageddisabledrole`, `database suffix` 値が追加されます。

注 - 「Directory Server ツールと相互運用」オプションを有効にすると、Identity Synchronization for Windows では `nsAccountLock` 属性を直接設定または削除できなくなります。さらに、ほかのロールによって無効にされたオブジェクトも検出できなくなります。

たとえば、`cn=nsdisabledrole`, `database suffix` などのロール、またはほかのロール内で入れ子にされている `cn=nsdisabledrole`, `database suffix` や `cn=nsmanageddisabledrole`, `database suffix` などのロールがこれに該当します。

「Directory Server ツールとの相互運用」の表に、「Directory Server ツールと相互運用」オプションを有効にした場合に Identity Synchronization for Windows がオブジェクトの有効化と無効化どのようにを検出し、同期させるかを示します。

表 6-1 Directory Server ツールとの相互運用

有効化	無効化
Identity Synchronization for Windows は、オブジェクトから <code>cn=nsmanageddisabledrole</code> , <code>database suffix</code> ロールが削除された場合にのみ有効化を検出します。	Identity Synchronization for Windows は、エントリの <code>nsroledn</code> 属性に <code>cn=nsmanageddisabledrole</code> , <code>database suffix</code> ロールが含まれる場合にのみ無効化を検出します。

表 6-1 Directory Server ツールとの相互運用

(続き)

Active Directory からのオブジェクト有効化を同期させる場合、Identity Synchronization for Windows は、オブジェクトから <code>cn=nsmanageddisabledrole</code> , <code>database suffix</code> ロールを削除することでオブジェクトを有効化します。	Active Directory からのオブジェクト無効化を同期させる場合、Identity Synchronization for Windows は、オブジェクトに <code>cn=nsmanageddisabledrole</code> , <code>database suffix</code> ロールを追加することでオブジェクトを無効化します。
--	---

Directory Server の nsAccountLock 属性の直接修正

Directory Server の有効化と無効化が Directory Server のオペレーショナル属性 nsAccountLock に基づく場合は、この方法を使用します。

注 - 「Directory Server の nsAccountLock 属性を直接修正」オプションを有効にすると、Identity Synchronization for Windows では、Directory Server コンソールまたはコマンド行ユーティリティーを使用して有効化または無効化されたオブジェクトが検出されなくなります。

この属性は、オブジェクトの状態を次のように制御します。

- nsAccountLock=true の場合、オブジェクトは無効化されており、ユーザーはログインできません。
- nsAccountLock=false の場合 (または値がない場合)、オブジェクトは有効化されています。

「Directory Server の nsAccountLock 属性の直接修正」の表に、「Directory Server の nsAccountLock 属性を直接修正」オプションを有効にした場合に Identity Synchronization for Windows がオブジェクトの有効化と無効化をどのように検出し、同期させるかを示します。

表 6-2 Directory Server の nsAccountLock 属性の直接修正

有効化	無効化
Identity Synchronization for Windows は、nsAccountLock 属性が true に設定されている場合のみ、無効化されたオブジェクトを検出します。	Identity Synchronization for Windows は、nsAccountLock 属性に値がないか、または false に設定されている場合のみ、有効化されたオブジェクトを検出します。
Active Directory からのオブジェクト無効化の同期時に、Identity Synchronization for Windows は nsAccountLock 属性を削除します。	Active Directory からのオブジェクト有効化の同期時に、Identity Synchronization for Windows は nsAccountLock 属性を true に設定します。

Directory Server のカスタムメソッドの使用

Directory Server の有効化と無効化が Sun Java System Access Manager (従来の Sun JES Identity Server) などの外部アプリケーションによって排他的に制御される場合は、この方法を使用します。

Directory Server のカスタムメソッドを設定する場合は、次の方法を指定します。

- 外部アプリケーションによって Directory Server 内のオブジェクトが有効化または無効化されたことを Identity Synchronization for Windows が検出する方法。
- Active Directory から Directory Server への同期時に、Identity Synchronization for Windows がオブジェクトを有効化または無効化する方法。

注 - 「Directory Server のカスタムメソッドを使用」オプションを有効にすると、ディレクトリへのアクセスが Access Manager などの外部アプリケーションによって制御されている場合を除き、Identity Synchronization for Windows はオブジェクトをディレクトリからロックアウトできなくなります。

有効化と無効化のカスタムメソッドを設定するには、「設定」ボタンをクリックして「Directory Server のカスタムメソッドの設定」ダイアログボックスを表示します。

Configure a custom method for activating and inactivating Directory Server objects.

Activation state attribute :

Values used by Identity Synchronization for Windows to **detect** an object's activation state.

Value	State
No Value	Activated
All Other Values	Inactivated

Values used by Identity Synchronization for Windows to **set** an object's activation state.

Activated value :

Inactivated value :

図 6-43 有効化と無効化のカスタムメソッドの設定

このダイアログボックスには次の機能があります。

- 「アクティブ化状態の属性」ドロップダウンリスト: このリストでは、Directory Server と Active Directory の間で有効化と無効化を同期するときに Identity Synchronization for Windows が使用する属性を指定します。
このリストには、現在選択している Directory Server の Structural オブジェクトクラスと Auxiliary オブジェクトクラスのスキーマに含まれるすべての属性が表示されます。
- 「値」と「状態」の表: この表では、選択した属性と関連付けられている値がどのような場合に有効化または無効化されるかを指定します。
 - 「値」列: この列では、「新規」ボタンと「削除」ボタンを使用して、有効化または無効化の状態を示すために使用される属性値を指定します。
この列には、次の2つの値が自動的に表示されます。
 - 「値なし」: 有効化状態属性に値がない場合。
 - 「ほかのすべての値」: 有効化状態属性に値があるが、その値が、値と状態の表に指定されていない場合。
 - 「状態」列: この列では、同じ行の「値」のエントリが一致した場合に、オブジェクトを有効とみなすか無効とみなすかを指定します。

値	状態	結果
値なし	有効	属性が存在しないか、または値を持たない場合に、有効なオブジェクトとして検出されます。
	無効	属性が存在しないか、または値を持たない場合に、無効なオブジェクトとして検出されます。
user-defined 値	有効	属性が user-defined 属性を持つ場合に、有効なオブジェクトとして検出されます。
	無効	属性が user-defined 属性を持つ場合に、無効なオブジェクトとして検出されます。
ほかのすべての値:	有効	属性が持つ値が表に指定されていない場合に、有効なオブジェクトとして検出されます。
	無効	属性が持つ値が表に指定されていない場合に、無効なオブジェクトとして検出されます。

- 「新規」ボタン: 「値」列に新しい値を追加する場合は、このボタンをクリックします。
- 「削除」ボタン: 「値」列からエントリを削除する場合は、そのエントリを選択して、このボタンをクリックします。
- 「有効化される値」および「無効化される値」ドロップダウンリスト: この2つのリストでは、Identity Synchronization for Windows がオブジェクトの状態を設定するときに使用する値を指定します。

有効化と無効化の同期

▼ **Directory Server** と **Active Directory** の間でオブジェクトの状態を検出し、同期するように **Identity Synchronization for Windows** を設定する

- 1 「アクティブ化状態の属性」ドロップダウンリストから属性を選択します。
- 2 「新規」ボタンをクリックし、表の「値」列に値を追加します。
- 3 「値」列の各エントリと同じ行の「状態」列をクリックし、表示されるドロップダウンリストから「有効」または「無効」を選択します。

Value	State
No Value	Activated
active	Inactivated
All Other Values	Activated
	Inactivated

図 6-44 状態の選択

たとえば、Access Manager を使用している場合は、次のように指定します。

- 4 「アクティブ化状態の属性」ドロップダウンリストから `inetuserstatus` 属性を選択します。
- 5 「新規」ボタンをクリックし、表の「値」列に `active`、`inactive`、および `deleted` の各属性値を入力します
- 6 各値に対応する「状態」列をクリックし、次のように、「有効」または「無効」を選択します。
 - 「値なし」: 有効
 - 「`active`」: 有効
 - 「`inactive`」: 無効
 - 「`deleted`」: 無効
 - 「ほかのすべての値」: 無効

199 ページの「[Directory Server のカスタムメソッドの使用](#)」では、この `inetuserstatus` の例に基づいて、「Directory Server のカスタムメソッドを使用」オプションを有効にした場合に Identity Synchronization for Windows が有効化と無効化の検出と同期を行う方法を説明します。

値	状態	結果
値なし	有効	inetuserstatus 属性が存在しないか、または値を持たない場合に、有効なオブジェクトとして検出されます。
active	有効	属性値が active の場合に、有効なオブジェクトとして検出されます。
inactive	無効	属性値が inactive の場合に、無効なオブジェクトとして検出されます。
deleted	無効	属性値が deleted の場合に、無効なオブジェクトとして検出されます。
ほかのすべての値:	無効	属性が持つ値が表に指定されていない場合に、無効なオブジェクトとして検出されます。

有効化と無効化の設定

「値」と「状態」の表を設定すると、「有効化される値」と「無効化される値」のドロップダウンリストが自動的に次のように生成されます。

- 「有効化される値」リストには、状態が「有効」のすべての値が含まれます（「値なし」、「**active**」など）。
- 「無効化される値」リストには、状態が「無効」のすべての値が含まれます（「**inactive**」、「**deleted**」など）。
- 「ほかのすべての値」の値はどちらのリストにも含まれません。

Active Directory から同期されるオブジェクトを Identity Synchronization for Windows が有効化または無効化する方法を指定するには、「有効化される値」と「無効化される値」のいずれかまたは両方のドロップダウンリストから値を選択します。

- 「有効化される値」: オブジェクトの有効化状態を制御します。
 - 「値なし」: オブジェクトに「**active**」の値が含まれていない場合、Identity Synchronization for Windows は Directory Server 側の状態を有効に設定します。
 - 「**active**」: オブジェクトに「**active**」の値が含まれている場合、Identity Synchronization for Windows は Directory Server 側の状態を有効に設定します。
- 「無効化される値」: オブジェクトの有効化状態を制御します。
 - 「**inactive**」または「**deleted**」: Identity Synchronization for Windows は Directory Server 側のオブジェクトの状態を無効に設定します。
 - 「なし」: 有効な設定ではありません。値を選択してください。

注- 無効化される値を指定してください。指定しない場合、設定は無効となります。

設定が完了した「Directory Server のカスタムメソッドの設定」ダイアログボックスの図を次に示します。

Configure a custom method for activating and inactivating Directory Server objects.

Activation state attribute : inetuserstatus

Values used by Identity Synchronization for Windows to **detect** an object's activation state.

Value	State
No Value	Activated
active	Activated
inactive	Inactivated
deleted	Inactivated
All Other Values	Inactivated

Buttons: New, Remove

Values used by Identity Synchronization for Windows to **set** an object's activation state.

Activated value : No Value

Inactivated value : inactive

図 6-45 設定が完了したダイアログボックスの例

グループ同期の設定

Directory Server と Active Directory 間のグループ同期を有効にすると、グループの作成、グループの削除、およびグループ内のメンバーシップの変更を同期できます。

注 - Windows NT ディレクトリソースでは、グループ同期はサポートされません。

▼ グループを同期する

- 1 「グループ」タブで、「グループ同期を使用可能にする」チェックボックスにチェックマークを付けます。
- 2 次のいずれかのグループ同期方法を選択し、**Identity Synchronization for Windows** でさまざまなグループの検出と同期を行う方法を指定します。
 - ドメイングローバルセキュリティー
 - ドメイングローバル配布

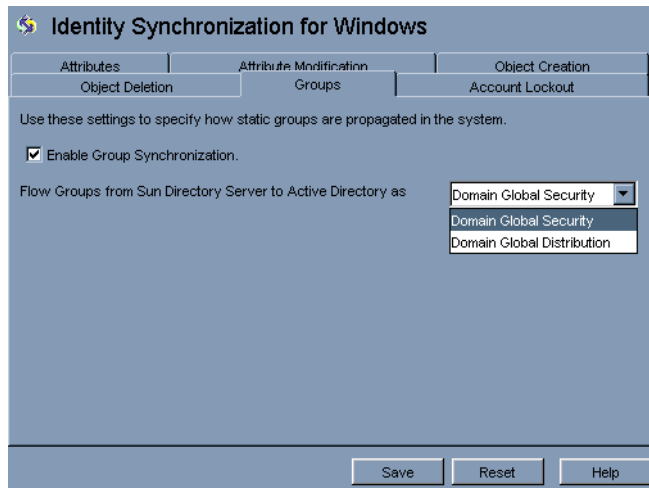


図 6-46 グループ同期の有効化

注- ドメイングローバルセキュリティ、ドメイングローバル配布、および Active Directory の詳細については、Microsoft Active Directory のドキュメントを参照してください。

Directory Server と Active Directory の間でグループに関する変更を検出して同期するための Identity Synchronization for Windows の設定

グループ同期に関する属性を手動でマッピングする必要はありません。「保存」をクリックすると、属性は自動的にマッピングされます。

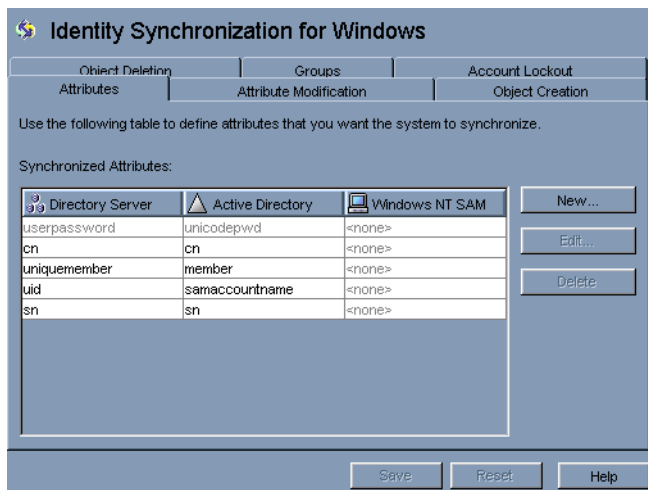


図 6-47 グループ同期の属性マッピング

注 -

1. userpassword 属性と unicodepwd 属性のマッピングを変更しないでください。
2. グループ同期を無効にするには、「グループ同期を使用可能にする」チェックボックスのチェックマークを外します。
3. または、コマンド行ツールの `idsync groupsync` を使用してグループ同期の有効と無効を切り替えることもできます。詳細については、付録 A 「Identity Synchronization for Windows コマンド行ユーティリティーの使用」を参照してください。

アカウントのロックアウトおよびロックアウト解除の設定と同期

アカウントのロックアウト機能を有効にするには、次の操作を行います。

- Active Directory と Directory Server の両方に同じパスワードポリシーを設定する。
- アカウントのロックアウトを有効にする。
- Directory Server と Active Directory で異なっている属性を対応付ける。

Identity Synchronization for Windows では、Active Directory と Directory Server の間で次のイベント同期を行うことができます。

- ロックアウトイベントの同期 (Active Directory から Directory Server へ)
- ロックアウトイベントの同期 (Directory Server から Active Directory へ)

- 手動でのロックアウト解除イベントの同期 (Active Directory から Directory Server へ)
- 手動でのロックアウト解除イベントの同期 (Directory Server から Active Directory へ)

注 - Windows NT ディレクトリサーバーでは、アカウントのロックアウトとロックアウト解除の同期はサポートされません。

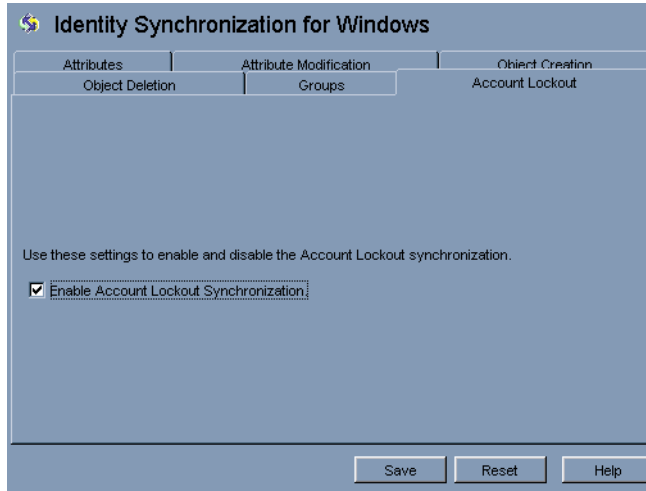
アカウントのロックアウトに必要な前提条件

アカウントのロックアウト機能を有効にする前に、両方のコンポーネントで属性 `lockoutDuration` を同じ値に設定してください。また、分散セットアップに関するすべてのシステム間で時刻が一致していることも確認してください。時刻が一致していないと、`lockoutDuration` の設定がシステム間の時刻差よりも短い場合に、ロックアウトイベントが期限切れとなる可能性があります。

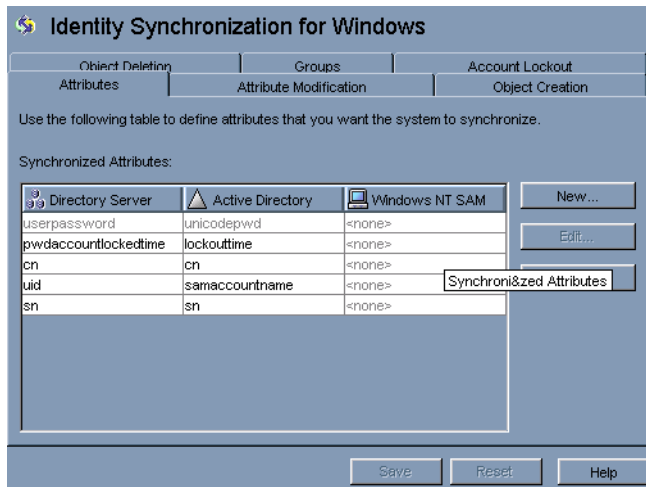
注 - Active Directory と Directory Server の両方に同じパスワードポリシーを設定してください。たとえば、Active Directory のパスワードポリシーで永続的なロックアウトが指定されている場合は、Directory Server でも同じパスワードポリシーを設定するようにしてください。

アカウントのロックアウト機能の使用

Directory Server と Active Directory の間のアカウントロックアウトの同期を有効にします。



アカウントのロックアウトを有効にするために、Directory Server の `pwdaccountlockedtime` 属性と Active Directory の `lockoutTime` 属性を明示的にマッピングする必要はありません。Identity Synchronization for Windows の設定パネルの「アカウントのロックアウト」タブで、「アカウントロックアウト同期を有効にする」チェックボックスにチェックマークを付けます。



注 - コマンド行ツールの **idsync accountlockout** を使用してアカウントロックアウトの同期の有効と無効を切り替えることもできます。詳細については、[付録 A 「Identity Synchronization for Windows コマンド行ユーティリティーの使用」](#) を参照してください。

削除のフロー方法の指定

Directory Server システムと Active Directory システムの間でユーザーエントリの削除を伝播させる方法を指定するには、「オブジェクトの削除」タブを使用します

注 - Windows NT ではオブジェクト削除のフローを指定できません。

▼ Directory Server システムと Active Directory システム間でのエントリ削除のフロー方法を指定する

- 1 ナビゲーション区画の最上部にある「Identity Synchronization for Windows」ノードを選択し、「オブジェクトの削除」タブをクリックします

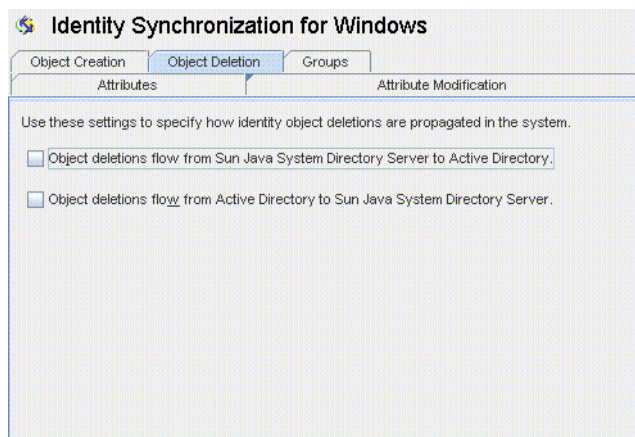


図 6-48 ユーザーエントリの削除の伝播

- 2 次のように削除のフローを有効または無効にします。
 - Sun Directory Server 環境から Active Directory サーバーに削除を伝播させる場合は、「オブジェクトの削除は **Sun Java System Directory Server** から **Active Directory** に伝播される」にチェックマークを付けます。

- Active Directory 環境から Sun Directory Server に削除を伝播させる場合は、「オブジェクトの削除は **Active Directory** から **Sun Java System Directory Server** に伝播される」にチェックマークを付けます。
- 双方向のフローを設定する場合は、両方のオプションにチェックマークを付けます。
- システム間でユーザーの削除を伝播させない場合は、どちらのオプションにもチェックマークを付けません (デフォルト設定)。

同期ユーザーリストの作成

同期ユーザーリスト (SUL) では、Active Directory と Sun Directory Server で同期の対象にするユーザーを指定します。SUL に指定されたすべてのエントリーはコネクタを通過し、その SUL に設定されている制約と照合して評価されます。

各 SUL には2つの要素が含まれます。1つは同期対象の Directory Server ユーザーを識別し、もう1つは同期対象の Windows ユーザーを識別します。

注 - Directory Server のユーザーを複数の Active Directory ドメインと同期させる場合は、Active Directory ドメインごとに SUL を定義します。

定義のコンポーネント、複数の SUL を定義する方法、複数の SUL を処理する方法、複数の Windows ドメインのサポートを設定する方法など、SUL の定義と設定の詳細については、[付録 D 「Identity Synchronization for Windows の同期ユーザーリストの定義と設定」](#)を参照してください。

どちらの SUL 要素にも、同期対象のユーザーを識別するための3つの定義が含まれます。

- ベース DN: 同期対象のユーザーの場所 (NT には該当しない)
- ネーミング属性: 新規作成ユーザー (作成式) に使用される属性 (NT には該当しない)
- フィルタ: 指定されたユーザーを同期対象から除外します。

▼ サーバー間でユーザータイプを識別してリンクさせる

- 1 ナビゲーションツリーで「同期リスト」ノードを選択し、「新規同期ユーザーリスト」ボタンをクリックします。

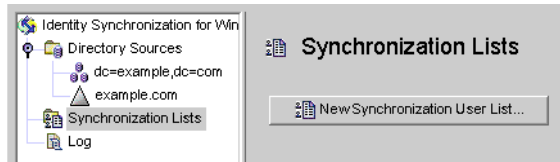


図 6-49 同期ユーザーリストの新規作成

「同期ユーザーリストの定義」ウィザードが表示されます。

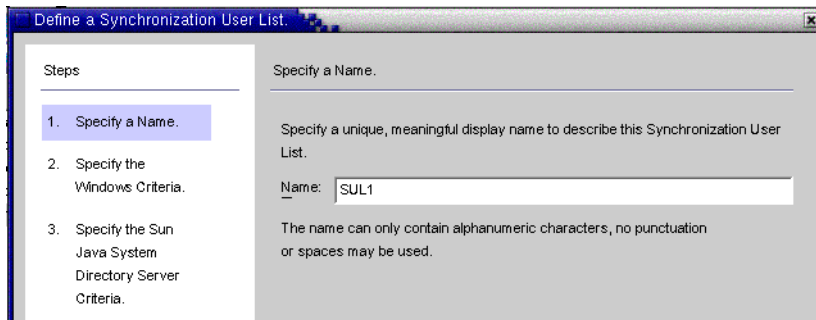


図 6-50 SUL名の指定

デフォルトでは、最初の同期ユーザーリストの名前は *SUL1* になります。

- デフォルトの名前をそのまま使用する場合は、「次へ」をクリックします。
- 別の名前を使用する場合は、「名前」フィールドに別の名前を入力してから、「次へ」をクリックします。
- SUL名には空白文字や句読文字を使用しないでください。
- システム内で一意の名前を指定してください。

「Windowsの条件の指定」パネルが表示されます。

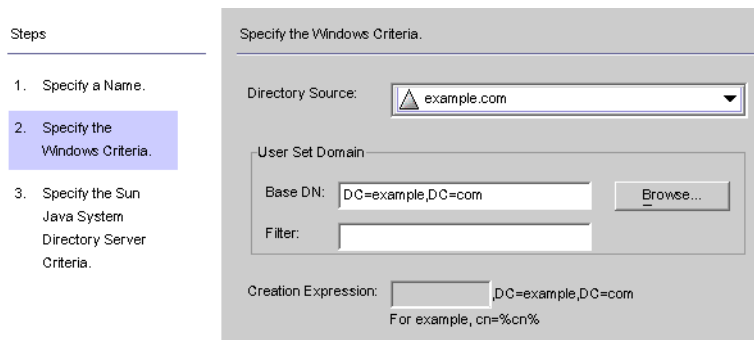


図 6-51 Windows の条件の指定

- 2 ドロップダウンリストから **Windows** ディレクトリソースを選択します。

注 - 「完了」 ボタンをクリックして SUL を作成したあとで、この SUL に含まれる Active Directory または Directory Server のディレクトリソースを編集することはできません。グループ同期機能が有効になっている場合、「Sun Java System Directory Server の条件の指定」 パネルの作成式は `uid=%uid%` または `cn=%cn%` になります。

- 3 「ユーザーセットドメイン」は、同期対象となるすべてのユーザーのセットです。次のいずれかの方法で、「ユーザーセットドメイン」の「ベース DN」を入力します。
 - テキストフィールドに名前を入力します (たとえば、**DC=example,DC=com**)。
 - 「参照」 ボタンをクリックして「セットベース DN」 ダイアログボックスを開き、ベース DN を探して選択します。
フィルタを使用して明示的に除外しないかぎり、指定したベース DN の下のすべてのユーザーがこの SUL に含まれます。

注 - Windows NT マシンでは、ベース DN と作成式は使用できません。

「完了」 ボタンをクリックして SUL を作成したあとで、この SUL に含まれる Active Directory または Directory Server のディレクトリソースを編集することはできません。グループ同期機能が有効になっている場合、「Sun Java System Directory Server の条件の指定」 パネルの作成式は `uid=%uid%` になります。

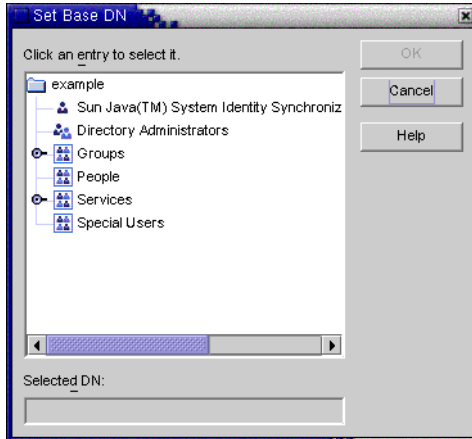


図 6-52 ベース DN の選択

- 4 等価フィルタ、プレゼンスフィルタ、または部分文字列フィルタを入力して、このベース DN 内で同期対象にするユーザーを指定できます。たとえば、複数の同期ユーザーリストで同じベース DN を使用する場合は、フィルタを使用してリストを区別できます。

等価フィルタの構文は、LDAP クエリの構文に似ています。ただし、等価部分文字列で使用できる文字は *、&、|、=、! だけです。たとえば、次のフィルタを使用して、SUL から管理者を除外できます。

(!(cn=Administrator))

「作成式」フィールドは自動的に生成されるはずですが。

注 - 作成式は、新しいエントリが Active Directory から Directory Server に伝播するとき使用される親 DN とネーミング属性を定義します。

ユーザー属性の作成が Active Directory から Directory Server に伝播するように設定していない場合は、Sun のディレクトリで作成式を使用できません。詳細については、189 ページの「オブジェクト作成のフローの指定」を参照してください。

- 5 作成式が指定されていない場合、または既存のエントリを変更する場合は、**Windows Active Directory** のすべての同期ユーザーリストに適用される作成式を入力できます。次にその例を示します。

cn=%cn% ,cl=users,dc=example,dc=com

作成式を変更する場合は、同期対象にする属性を選択します。必要に応じて、「オブジェクトの作成」タブに戻り、「作成属性」ボタンをクリックして、この属性の追加とマッピングを行ってください。

- 6 「次へ」をクリックして、**Sun Java System Directory Server** の条件を指定します。

- 7 「Sun Java System Directory Server の条件の指定」パネルが表示されたら、手順2～5を繰り返して、Directory Server の条件を指定します。

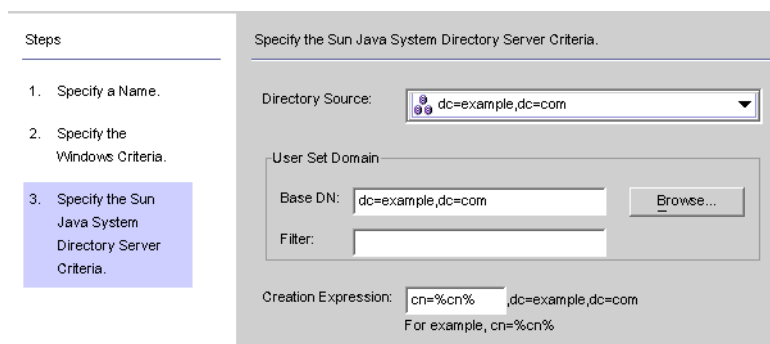


図 6-53 Directory Server の条件の指定

注- 「完了」 ボタンをクリックして SUL を作成したあとで、この SUL に含まれる Active Directory または Directory Server のディレクトリソースを編集することはできません。

- 8 完了したら、「完了」をクリックします。
- 9 ナビゲーションツリーに新しい **SUL** ノードが追加され、「設定」タブに「同期リスト」パネルが表示されます。

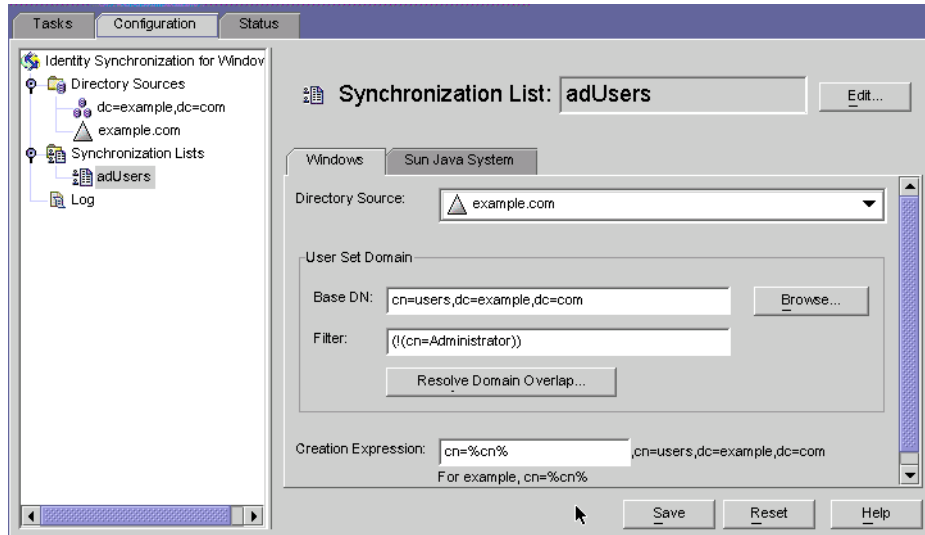


図 6-54 「同期リスト」パネル

- 10 ユーザーが複数のリストと一致する場合は、「ドメイン重複の解決」ボタンをクリックして同期ユーザーリストの設定を定義します。
- 11 ネットワーク内の、**Directory Server**を除くすべてのディレクトリソースを格納する同期ユーザーリストを作成します。

設定の保存

▼ コンソールパネルから現在の設定を保存する

- 1 「保存」をクリックして、現時点での設定を保存します。
- 2 設定が評価され、「設定の妥当性状態」ウィンドウが表示されます。

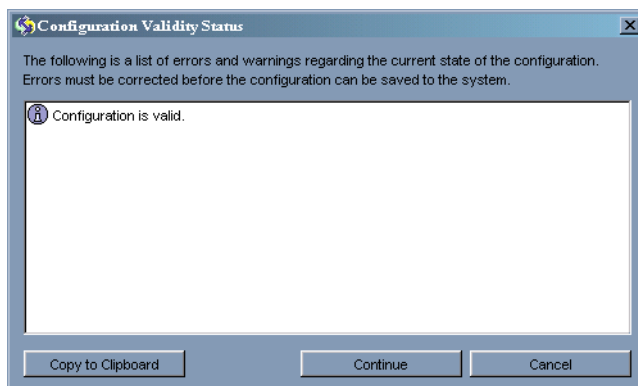


図 6-55 「設定の妥当性状態」ウィンドウ

このパネルでは、設定が有効であるか、または修正が必要な設定上の問題があるかを確認します。

設定ディレクトリの情報が書き換えられ、システムマネージャーに通知されるため、設定の保存には数分かかることがあります。

システムマネージャー(コアコンポーネント)は、情報を必要とするコンポーネントに設定情報を配布します。

注-設定の検証エラーは赤、警告は黄色で示されます。

- エラーがある状態では、設定を保存できません。
- 警告がある状態では、設定を保存できますが、保存前に警告を解消しておくことをお勧めします。

3 設定が有効であれば、「続行」をクリックして設定を保存します。

「コネクタのインストール方法」ダイアログボックスが表示され、Identity Synchronization for Windows のコネクタとサブコンポーネントのインストールに関する手順が示されます。

この一覧は、この時点で更新され、配備に応じてカスタマイズされた実行手順リストが表示されるようになっていきます。(この時点までは、汎用の手順が示されていた。)実行手順リストへのアクセスと更新は、Identity Synchronization for Windows コンソールの「状態」タブでも行えます。

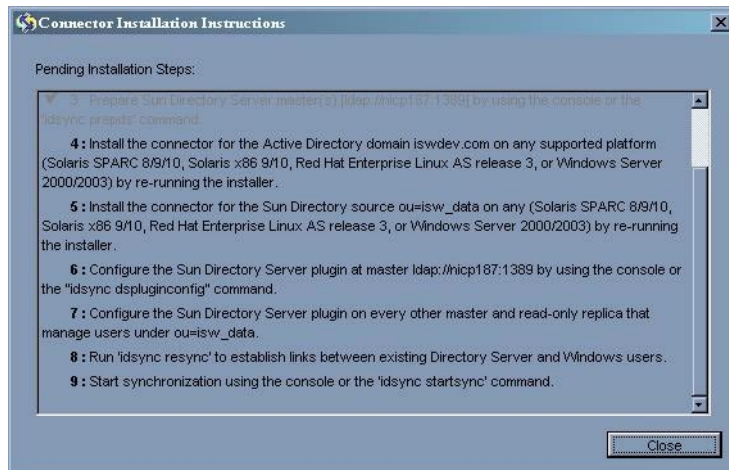


図 6-56 コネクタのインストール手順

- 4 表示される情報をよく読み、「OK」をクリックします。

コアの初期設定が完了したら、Identity Synchronization for Windows のコネクタとサブコンポーネントをインストールできます。手順については、第 3 章「製品の理解」を参照してください。

コネクタのインストール

この章では、Identity Synchronization for Windows コネクタのインストール手順について説明します。ここで説明する内容は、次のとおりです。

- 217 ページの「始める前に」
- 218 ページの「インストールプログラムの実行」
- 220 ページの「コネクタのインストール」

Identity Synchronization for Windows は、ディレクトリソース間でのユーザーパスワードの同期にコネクタを使用し、コネクタによる変更検出の強化と双方向同期のサポートにサブコンポーネントを使用します。

始める前に

コネクタの設定プロセスを開始する前に、次の事項に注意してください。

- インストールプロセスを開始する前にコンソールを閉じます。コネクタのインストール時にコンソールが開いていると、コンポーネントがサーバーに設定データを追加している状態が競合として認識され、エラーメッセージが出力されます。
- Active Directory コネクタにはサブコンポーネントはありません。
- Windows NT のコネクタとサブコンポーネントは同時にインストールされます。
- Directory Server または Active Directory のコネクタは、コアと同じマシンにインストールしても、別のマシンにインストールしてもかまいません。Windows NT のコネクタは、同期対象ドメインのプライマリドメインコントローラ (PDC) にインストールします。
- コネクタをコアと同じマシンにインストールする場合、コネクタは自動的にコアと同じディレクトリにインストールされます。
- コネクタを別のマシンにインストールする場合は、コアのインストール時に提供された設定ディレクトリ情報を指定するよう求められます。

インストールするコネクタごとに、インストールプログラムを実行します。

たとえば、ディレクトリサーバーコネクタと Active Directory コネクタをインストールする場合は、コアのインストール後、コネクタのインストールプログラムを2回実行します。

インストールプログラムの実行

インストールするコネクタごとに、次の手順を繰り返します。

▼ インストールプログラムを再起動して実行する

- 1 コネクタをインストールするマシンで、次のようにインストールプログラムを再実行します。
 - **Solaris** の場合: `installer` ディレクトリに移動し、`./runInstaller.sh` と入力してインストールプログラムを実行します。

注-インストールプログラムをテキストベースモードで実行するには、`./runInstaller.sh -nodisplay` と入力します。

`runInstaller.sh` プログラムを実行すると、Identity Synchronization for Windows ではパスワードを自動的にマスクして、平文で表示されないようにします。

- **Linux** の場合: `installer` ディレクトリに移動し、`./installer.sh` と入力してインストールプログラムを実行します。

注-インストールプログラムをテキストベースモードで実行するには、`./installer.sh -nodisplay` と入力します。

`installer.sh` プログラムを実行すると、Identity Synchronization for Windows ではパスワードを自動的にマスクして、平文で表示されないようにします。

- **Windows** の場合: `installer` ディレクトリに移動し、`setup.exe` と入力してインストールプログラムを実行します。
- 2 「ようこそ」画面で、表示された情報を読み、「次へ」をクリックして「ソフトウェア使用許諾契約」パネルに進みます。
 - 3 ライセンス条項を確認し、次のいずれかを選択します。
 - 「はい(ライセンス契約書に同意する)」を選択すると、ライセンス条項に同意して次のパネルに進みます。

- 「いいえ」を選択すると、設定プロセスを中止し、インストールプログラムを終了します。
- 4 「Sun Java System Directory Server」パネルが表示されます。設定ディレクトリの場所を次のように指定します。
- 「設定ディレクトリホスト」: Identity Synchronization for Windows の設定情報を格納する Sun Java System Directory Server インスタンス (管理サーバーに関連する) の完全修飾ドメイン名 (FQDN) を入力します。コアのインストール時に指定したインスタンスと同じインスタンスを指定します。
 - 「設定ディレクトリポート」 (デフォルトは 389): 設定ディレクトリのポートを指定します。デフォルトの設定のままにしても、別の使用可能なポートに変更してもかまいません。

コアと設定ディレクトリの間で SSL (Secure Socket Layer) を有効にするには、「セキュリティ保護されたポート」オプションを有効にし、SSL ポートを指定します (デフォルトの SSL ポートは 636)。このオプションを有効にすると、機密情報が平文でネットワーク上に送信されるのを防ぐことができます。
 - 「設定ルートサフィックス」: コアのインストール時に指定したルートサフィックスをメニューから選択します。Identity Synchronization for Windows の設定は、このルートサフィックスに格納されます。

注- ルートサフィックスが検出されず、サーバー情報を手動で入力する場合は、「更新」をクリックしてルートサフィックスのリストを再生成します。

- 5 「次へ」をクリックして「設定ディレクトリのクレデンシャル」パネルを開きます。
- 6 設定ディレクトリの管理者のユーザー ID およびパスワードを入力します。
- ユーザー ID として admin と入力した場合は、ユーザー ID を DN として指定する必要はありません。
 - その他のユーザー ID を使用する場合は、その ID を完全 DN として指定します。たとえば、*cn=Directory Manager* のようになります。

注- SSL を有効にしていない場合、これらの資格は暗号化されずに送信されます。

- 7 「次へ」をクリックして「設定パスワード」パネルを開きます。このパネルでは、コアのインストール時に指定した設定パスワードを入力します。
- また、このマシンにコアがインストールされていない場合は、Java ホームディレクトリの場所を指定するように求められます (144 ページの「コアのインストール」を参照)。

- 8 完了したら、「次へ」をクリックします。

注- これ以後のインストール手順は、インストールするコネクタの種類によって異なります。

コネクタのインストール

ここでは、3種類の Identity Synchronization for Windows コネクタをインストールする方法について説明します。

- [220 ページの「ディレクトリサーバーコネクタのインストール」](#)
- [226 ページの「Active Directory コネクタのインストール」](#)
- [229 ページの「Windows NT コネクタのインストール」](#)

注- コネクタは特定の順序でインストールする必要はありませんが、複数のコネクタを同時にインストールしないでください。

ディレクトリサーバーコネクタのインストール

[218 ページの「インストールプログラムの実行」](#)に示された手順を完了すると、次のパネルが表示されます。

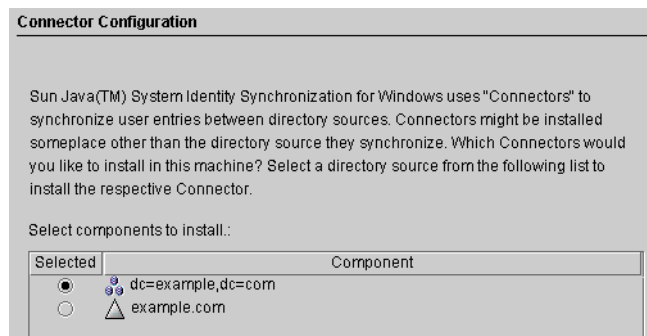


図7-1 ディレクトリサーバーコネクタの選択

「インストールするコンポーネントを選択します。」の一覧には、まだインストールされていないコネクタコンポーネントのみが表示されます。たとえば、ディレクトリサーバーコネクタ (dc=example,dc=com) をインストールしたあとは、このエントリは一覧から削除されます。

次の表に、ディレクトリソースエントリの例を示します。

表7-1 ディレクトリソースの例

ディレクトリソース	エントリの例
Sun Java System Directory Server	dc=example,dc=com
Windows Active Directory	example.com
Windows NT SAM	EXAMPLE

▼ ディレクトリサーバーコネクタをインストールする

- 1 ディレクトリサーバーコネクタコンポーネントの横にあるボタンを有効にし、「次へ」をクリックします。
「Directory Server コネクタのクレデンシャル」パネルが表示されます。

Directory Server Connector Credentials

Enter the directory manager credentials for the Sun Java(TM) System Directory Server(s) associated with the connector being installed.

Primary: ldap://machine1.example.com:389

Primary Directory Server User DN:

Primary Directory Server Password:

Secondary: none

Secondary Directory Server User DN:

Secondary Directory Server Password:

注 - ユーザー DN のフィールドには、完全指定のディレクトリマネージャー識別名が自動的に入力されますが、この情報は必要に応じて変更できます。

次の情報を入力します。

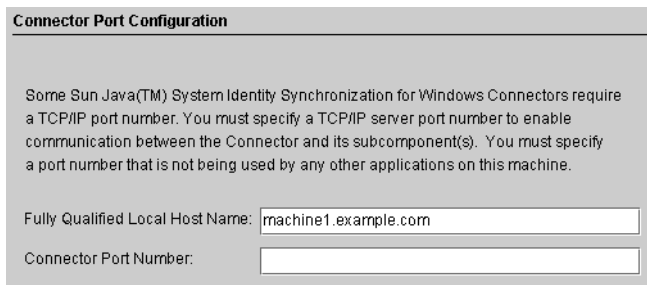
- 「一次 **Directory Server** ユーザー DN」: デフォルトのユーザー DN を変更する必要がある場合は、完全指定のディレクトリマネージャー識別名を入力します。
- 「一次 **Directory Server** パスワード」: ディレクトリマネージャーのパスワードを入力します。

副マスターを使用している場合は、「二次 Directory Server ユーザー DN」と「二次 Directory Server パスワード」のフィールドが入力可能になります。このディレクトリマネージャーの DN フィールドには、「一次 Directory Server ユーザー

DN」および「一次 Directory Server パスワード」フィールドと同じエントリが自動的に入力されます。この情報は必要に応じて変更できます。

Directory Server が準備済みでデータの同期が可能な状態であることが検証されます。Directory Server の準備 (168 ページの「Sun ディレクトリソースの準備」) が完了している場合、コネクタが Directory Server との接続に使用するアカウント (たとえば、`uid=PSWConnector,suffix`) が作成されます。

- 2 「次へ」をクリックして、「コネクタポートの設定」区画に進みます。



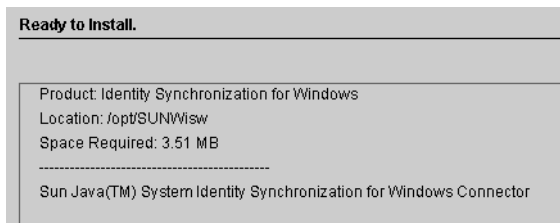
Connector Port Configuration

Some Sun Java(TM) System Identity Synchronization for Windows Connectors require a TCP/IP port number. You must specify a TCP/IP server port number to enable communication between the Connector and its subcomponent(s). You must specify a port number that is not being used by any other applications on this machine.

Fully Qualified Local Host Name:

Connector Port Number:

- 3 ドメイン名を含む完全修飾ローカルホスト名と、コネクタが待機する使用可能なポート番号を指定します。すでに使用されているポートを指定すると、エラーメッセージが表示されます。
- 4 「次へ」をクリックして「インストール準備完了」区画を表示します。この区画には、コネクタのインストール場所と、インストールに必要なディスク容量が表示されます。問題がなければ、「すぐにインストール」ボタンをクリックします。



Ready to Install.

Product: Identity Synchronization for Windows
Location: /opt/SUNWIsW
Space Required: 3.51 MB

Sun Java(TM) System Identity Synchronization for Windows Connector

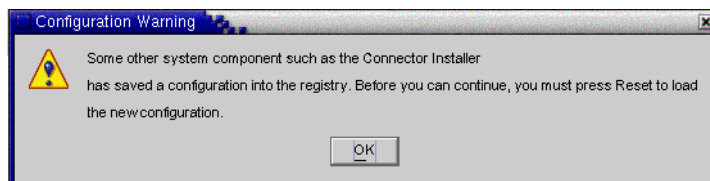
注-コアをローカルマシンにインストールした場合、「インストール準備完了」区画には、コネクタのインストールに必要な容量が0と表示されます。これは、コアのインストール時にコネクタバイナリがすでにインストールされているためです。それ以上インストールするバイナリが存在しないため、追加容量も必要ありません。

コアをインストールしたマシンとは異なるマシンにコネクタをインストールする場合は、「インストール準備完了」区画に、ローカルマシンへのコネクタのインストールに必要な容量が表示されます。

コネクタのインストールは、次の2つのステップを経て完了します。

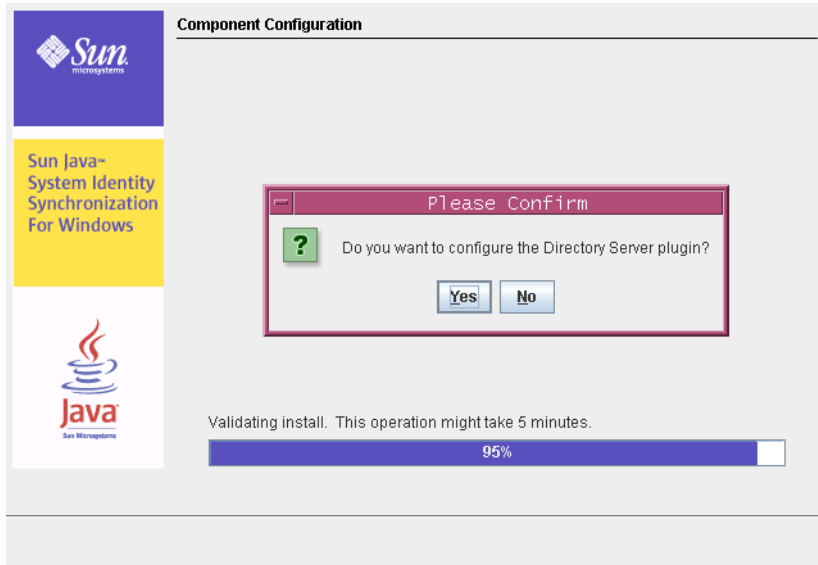
- バイナリがインストールされる間、「インストール中」区画と進捗バーが表示されます。
- 次に、「コンポーネントの設定」区画に進捗バーが表示されます。このステップの完了には数分かかります。

注-インストールを開始する前にコンソールを閉じなかった場合は、次の警告が表示されます(220 ページの「ディレクトリサーバーコネクタのインストール」)。コンソールで「リセット」をクリックし、コネクタの設定を読み込み直してください。



両方のステップが完了すると、「インストール概要」区画が表示されます。

注-ディレクトリサーバープラグインは、優先ホストおよび副ホスト(存在する場合)に対して設定されます。



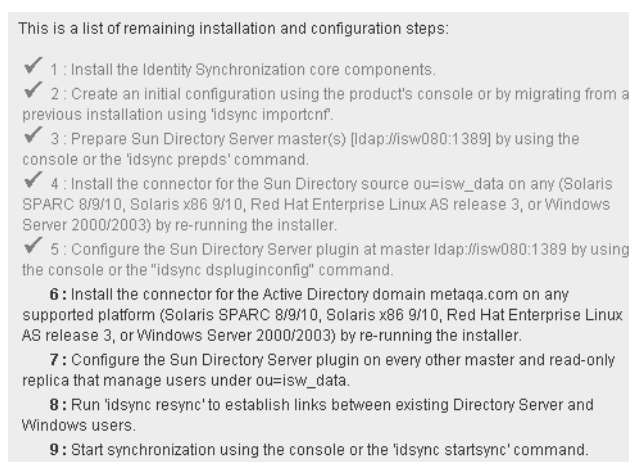
注 -

- a. 「はい」をクリックすると、ディレクトリサーバープラグインがすべてのホスト (優先ホストと副ホスト) で設定されます。
 - b. 「いいえ」をクリックすると、あとでコマンド行ツールの `idsync dspluginconfig` を使用して設定できます。詳細については、[付録 A 「Identity Synchronization for Windows コマンド行ユーティリティーの使用」](#) を参照してください。
-
- 5 インストールログを表示する場合は、「詳細」ボタンをクリックします。
- **Solaris** の場合: インストールログは `/var/sadm/install/logs/` に書き込まれます。
 - **Linux** の場合: インストールログは `/var/sadm/install/logs/` に書き込まれます。
 - **Windows** の場合: インストールログは `%TEMP%` ディレクトリに書き込まれます。このディレクトリは、通常、`C:\Documents and Settings\Administrator` の下にある `Local Settings` フォルダのサブディレクトリです。

注 - Windows 2000 Advanced Server などの一部の Windows システムでは、Local Settings フォルダは隠しフォルダになっています。

このフォルダと Temp サブディレクトリを表示するには、Windows エクスプローラを開き、メニューバーから「ツール」→「フォルダ オプション」を選択します。「フォルダ オプション」ダイアログボックスが表示されたら、「表示」タブをクリックし、「すべてのファイルとフォルダを表示する」オプションを有効にします。

- 6 「次へ」をクリックします。「実行手順リスト」パネルに、正しく完了した手順と、未完了の手順の一覧が表示されます。



- 7 表示内容を確認したら、「完了」をクリックします。

ディレクトリサーバーコネクタのインストール後、リソースの設定時(第6章「コアリソースの設定」)に設定したその他のコネクタをインストールできます。

- 追加のディレクトリサーバーコネクタをインストールする場合: 218 ページの「インストールプログラムの実行」の手順に従ってインストールプログラムを再起動し、手順1から手順7を繰り返します。
- Active Directory コネクタをインストールする場合: 226 ページの「Active Directory コネクタのインストール」に進みます。
- Windows NT コネクタをインストールする場合: 229 ページの「Windows NT コネクタのインストール」に進みます。

連鎖サフィックスが存在する場合の Identity Synchronization for Windows プラグインの設定

この設定は、Identity Synchronization for Windows プラグインをインストールする Directory Server インスタンスに連鎖サフィックスが存在する場合にのみ必要になります。Identity Synchronization for Windows プラグインが連鎖サフィックスを検索するように設定されていない場合、Identity Synchronization for Windows をインストールした Directory Server で実行される MODIFY 操作および BIND 操作は失敗します。

連鎖サフィックスが作成される Directory Server インスタンスで、次の操作を実行します。

ldapmodify ユーティリティを使用して、次の LDIF スクリプトを実行します。

```
dn: cn=config,cn=chaining database,cn=plugins,cn=config
changetype: modify
add: nspossiblechainingcomponents
nspossiblechainingcomponents: cn=pswsync,cn=plugins,cn=config
```

同じ操作を、次の手順を使用して実行することもできます。

1. 「設定」タブを選択します。
2. 左側の区画に表示されている「データ」ノードをクリックします。
3. 右側の区画で「連鎖」タブを選択します。
4. 連鎖を許可されているコンポーネントに Identity Synchronization for Windows プラグイン (cn=pswsync,cn=plugins,cn=config) を追加します。
5. 変更を保存して終了します。

Active Directory コネクタのインストール

ディレクトリサーバーコネクタのインストール後、ほかにもインストールするコネクタが設定されている場合は、「コネクタの設定」区画が表示される前に、それらのコネクタをインストールするオプションが表示されます。

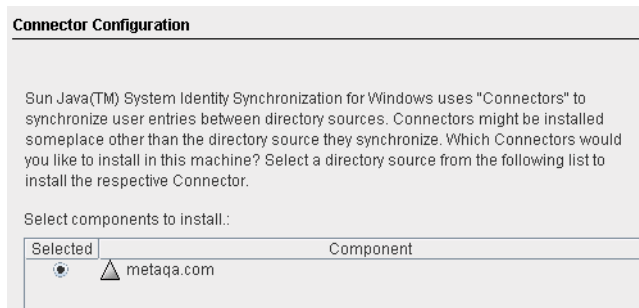
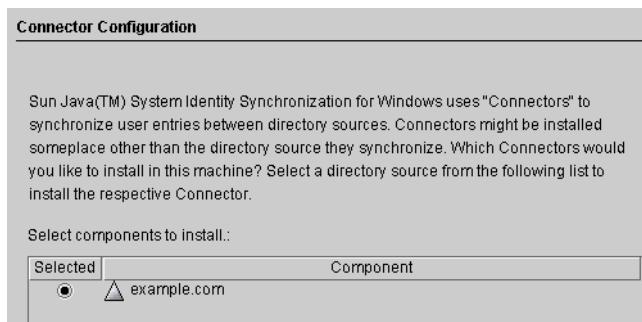


図 7-2 コネクタの選択

コンポーネントの一覧には、まだインストールされていないコネクタコンポーネントのみが表示されます。たとえば、ディレクトリサーバーコネクタ(この場合は dc=example,dc=com)をすでにインストールしている場合、このコンポーネントは一覧に表示されません。

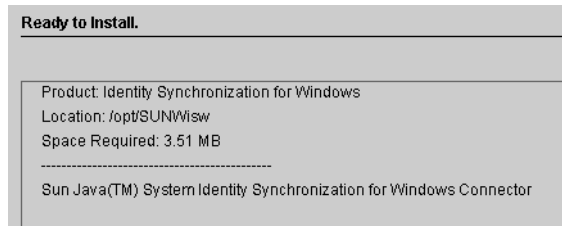
▼ Active Directory コネクタをインストールする

- 1 「コネクタ」 ボタンを有効にし、「次へ」をクリックします。
「コネクタの設定」パネルが表示されます。



「インストールするコンポーネントを選択します。」の一覧には、まだインストールされていないコネクタコンポーネントのみが表示されます。たとえば、ディレクトリサーバーコネクタ(この場合は dc=example,dc=com)をインストールしたあとは、このエントリは一覧から削除されます。

- 2 **Active Directory** コンポーネントの横にあるボタンを有効にし、「次へ」をクリックします。
「インストール準備完了」区画に、コネクタのインストール場所とインストールに必要なディスク容量が表示されます。



注- コアをローカルマシンにインストールした場合、「インストール準備完了」区画には、コネクタのインストールに必要な容量が0と表示されます。これは、コアのインストール時にコネクタバイナリがすでにインストールされているためです。それ以上インストールするバイナリが存在しないため、追加容量も必要ありません。

コアをインストールしたマシンとは異なるマシンにコネクタをインストールする場合は、「インストール準備完了」区画に、ローカルマシンへのコネクタのインストールに必要な容量が表示されます。

- 3 問題がなければ、「すぐにインストール」ボタンをクリックします。
バイナリがインストールされる間、「インストール中」区画と進捗バーが表示され、次に、インストールが完了したことを確認するための「インストール概要」区画が表示されます。
- 4 インストールログを表示する場合は、「詳細」ボタンをクリックします。
 - **Solaris** の場合: インストールログは /var/sadm/install/logs/ に書き込まれます。
 - **Linux** の場合: インストールログは /var/sadm/install/logs/ に書き込まれます。
 - **Windows** の場合: インストールログは %TEMP% ディレクトリに書き込まれます。このディレクトリは、C:\Documents and Settings\Administrator の下にある Local Settings フォルダのサブディレクトリです。

注 - Windows 2000 Advanced Server などの一部の Windows システムでは、Local Settings フォルダは隠しフォルダになっています。

このフォルダと Temp サブディレクトリを表示するには、Windows エクスプローラを開き、メニューバーから「ツール」→「フォルダオプション」を選択します。「フォルダオプション」ダイアログボックスが表示されたら、「表示」タブをクリックし、「すべてのファイルとフォルダを表示する」オプションを有効にします。

- 5 「次へ」をクリックします。「実行手順リスト」パネルに、正しく完了した手順と、未完了の手順の一覧が表示されます。

This is a list of remaining installation and configuration steps:

- ✓ 1 : Install the Identity Synchronization core components.
- ✓ 2 : Create an initial configuration using the product's console or by migrating from a previous installation using 'idsync importcnf'.
- ✓ 3 : Prepare Sun Directory Server master(s) [ldap://sw080:1389] by using the console or the 'idsync prepds' command.
- ✓ 4 : Install the connector for the Active Directory domain metaqa.com on any supported platform (Solaris SPARC 8/9/10, Solaris x86 9/10, Red Hat Enterprise Linux AS release 3, or Windows Server 2000/2003) by re-running the installer.
- ✓ 5 : Install the connector for the Sun Directory source ou=isw_data on any (Solaris SPARC 8/9/10, Solaris x86 9/10, Red Hat Enterprise Linux AS release 3, or Windows Server 2000/2003) by re-running the installer.
- ✓ 6 : Configure the Sun Directory Server plugin at master ldap://sw080:1389 by using the console or the "idsync dspluginconfig" command.
- 7 : Configure the Sun Directory Server plugin on every other master and read-only replica that manage users under ou=isw_data.
- 8 : Run 'idsync resync' to establish links between existing Directory Server and Windows users.
- 9 : Start synchronization using the console or the 'idsync startsync' command.

- 6 表示内容を確認したら、「完了」をクリックしてインストールプログラムを終了します。

Active Directory コネクタのインストール後、リソースの設定時(第6章「コアリソースの設定」)に設定したその他のコネクタをインストールできます。

- 追加の Active Directory コネクタをインストールする場合: インストールプログラムを再起動し(218 ページの「インストールプログラムの実行」を参照)、同じ手順を繰り返します。
- Windows NT コネクタをインストールする場合: 229 ページの「Windows NT コネクタのインストール」に進みます。
- 追加のディレクトリサーバーコネクタをインストールする場合: 218 ページの「インストールプログラムの実行」の手順に従ってインストールプログラムを再起動し、手順1から手順6を繰り返します。

Windows NT コネクタのインストール

Windows NT コネクタは、設定したドメインのプライマリドメインコントローラ(PDC)にインストールします。

▼ Windows NT コネクタと NT サブコンポーネントをインストールする

- 1 「Windows NT コネクタ」 ボタンを有効にし、「次へ」をクリックします。

- 2 「コネクタポートの設定」区画が表示されたら、ドメイン名を含む完全修飾ローカルホスト名と、コネクタが待機する使用可能なポート番号を入力します。すでに使用されているポートを指定すると、エラーメッセージが表示されます。
- 3 完了したら、「次へ」をクリックします。
「インストール準備完了」区画に、コネクタのインストール場所と、必要なディスク容量が表示されます。
- 4 問題がなければ、「すぐにインストール」ボタンをクリックします。
コネクタのインストールは、次の2つのステップを経て完了します。
 - バイナリがインストールされる間、「インストール中」区画と進捗バーが表示されます。
 - 次に、「コンポーネントの設定」区画に進捗バーが表示されます。このステップの完了には数分かかります。

注-インストールを開始する前にコンソールを閉じなかった場合は、警告が表示されます(220 ページの「ディレクトリサーバーコネクタのインストール」を参照)。コンソールで「リセット」をクリックし、コネクタの設定を読み込み直してください。

両方のステップが完了すると、「インストール概要」区画が表示されます。

- 5 インストールログを表示する場合は、「詳細」ボタンをクリックします。
インストールログは%TEMP%ディレクトリに書き込まれます。ほとんどの Windows NT システムでは、このディレクトリは c:\TEMP です。
- 6 「閉じる」をクリックしてインストールプログラムを終了します。
Windows NT コネクタのインストール後、リソースの設定時(第6章「コアリソースの設定」)に設定したその他のコネクタをインストールできます。
 - 追加の Windows NT コネクタをインストールする場合は、インストールプログラムを再起動します。218 ページの「インストールプログラムの実行」を参照し、手順1から手順6を繰り返します。
 - ディレクトリサーバーコネクタをインストールする場合は、220 ページの「ディレクトリサーバーコネクタのインストール」を参照してください。
 - Active Directory コネクタをインストールする場合は、226 ページの「Active Directory コネクタのインストール」を参照してください。

既存のユーザーおよびユーザーグループの同期

Identity Synchronization for Windows のコマンド行ユーティリティには、既存のユーザーまたはグループで配備をブートストラップする `idsync resync` サブコマンドが用意されています。このコマンドは、管理者固有のマッチングルールを使用して、既存エントリのリンク、遠隔ディレクトリの内容で空のディレクトリに生成、または2つの既存のユーザーおよびグループの入力の間で属性値 (パスワードを含む) の一括同期を行います

この章では、`idsync resync` サブコマンドを使用して新しい Identity Synchronization for Windows インストールで既存のユーザーおよびグループを同期する方法について説明します。また、同期およびサービスを開始および停止する手順についても説明します。ここで説明する内容は、次のとおりです。

- 232 ページの「[idsync resync の使用](#)」
- 238 ページの「[セントラルログで結果の確認](#)」
- 238 ページの「[同期の起動および停止](#)」
- 239 ページの「[サービスの起動および停止](#)」

注- 既存ユーザーを同期する前に、コアおよびコネクタのインストールを完了してください。

`idsync resync` サブコマンドの詳細については、[付録 A 「Identity Synchronization for Windows コマンド行ユーティリティの使用」](#) を参照してください。

「既存のユーザーおよびユーザーグループの同期」では、既存のユーザーおよびグループの入力に基づいて実行するインストール後の手順について概要を説明します。

既存のユーザーおよびグループの入力に基づくインストール後の手順

表 8-1 既存のユーザーの入力に基づくインストール後の手順

ユーザーの存在場所		インストール後の手順	
Windows	Directory Server	既存ユーザーを同期	既存ユーザーを同期しない
いいえ	いいえ	なし	なし
いいえ	はい	<code>idsync resync -o Sun -c</code> を実行して既存の Directory Server ユーザーを Windows に作成します。	なし
はい	いいえ	<code>idsync resync -c</code> を実行して既存の Windows ユーザーを Directory Server に作成します。	<code>idsync resync -u</code> を実行してコネクタのユーザーエントリのローカルキャッシュに生成します。
はい	はい	<code>idsync resync -f <filename> -k</code> を実行してユーザーだけをリンクし、次に <code>idsync resync -o Sun</code> を実行して既存のユーザーを Directory Server から再同期します。	<code>idsync resync -u</code> を実行してコネクタのユーザーエントリのローカルキャッシュに生成します。

注- グループ同期が有効な場合、グループはユーザーの同期方法と同様の方法で同期されます。

idsync resync の使用

この節では、同期プロセス、`idsync resync` サブコマンドを使用するための適切な構文、およびプロセスが正常に完了したことの確認方法について説明します。ここで説明する内容は、次のとおりです。

- 233 ページの「ユーザーまたはグループの再同期」
- 233 ページの「ユーザーのリンク」
- 234 ページの「idsync resync のオプション」
- 238 ページの「セントラルログで結果の確認」

ユーザーまたはグループの再同期

2つのディレクトリソースが同期しなくなったときは、ユーザーエントリを再同期します。idsync resync コマンドを使用して、2つのディレクトリソースでユーザーとユーザーグループの作成、およびユーザーとユーザーグループの属性の同期を行います。具体的には、idsync resync コマンドを使用して、既存の Active Directory または Windows NT SAM ドメインユーザーを空の Directory Server に生成することができます。

idsync resync コマンドは、次のいずれの方法でも使用できます。

- Directory Server および Windows にユーザーが存在する場合は、idsync resync コマンドを実行してそれらのユーザーを同期します。
- 既存のユーザーを Directory Server に同期しない場合は、-u 引数を指定して idsync resync を実行し、オブジェクトキャッシュのみを更新し、Windows のエントリを Directory Server に同期しないようにします。
- 既存の Windows ユーザーがあり、idsync resync を実行しない場合は、これらのユーザーに対する変更は伝播することもしないこともあります。フロー設定によっては、これらのユーザーが Directory Server に自動的に作成されることもあります。idsync resync コマンドをすでに実行した場合でも、このコマンドをもう一度実行してください。

注 - パスワードを同期するために idsync resync コマンドを使用できません。ただし Active Directory 環境でオンデマンドパスワード同期を強制するために Directory Server パスワードを無効化する場合を除きます。

グループ同期機能が有効な場合は、ユーザーとそのユーザーに関連付けられたグループの両方が、設定されたデータソース間で同期されます。グループ同期で resync コマンドを使用するときは、追加オプションは必要ありません。

ユーザーのリンク

Active Directory および Directory Server にユーザーを入力して、同期の開始前に Active Directory および Directory Server のコネクタをインストールしたら、idsync resync コマンドを使用して、すべての既存ユーザーが2つのディレクトリソース間で必ずリンクされているようにしてください。

リンクとは次のことを意味します。Identity Synchronization for Windows では、次の一意で不変の識別子を格納することにより、Directory Server と Windows の同じユーザーを関連付けます。

- 各 Directory Server ユーザーエントリの dspswuserlink 属性
- 各 Active Directory ユーザーの objectguid 属性

- 各 Windows NT SAM ユーザーのドメイン名と RID の組み合わせ

これらの不変な識別子を使用することで、Identity Synchronization for Windows では uid や cn などほかの重要な識別子を同期できます。dpswuserlink 属性は、次のときに生成されます。

- Identity Synchronization for Windows が Directory Server に新しいユーザーを作成したとき (新しいユーザーが Windows から同期されたか idsync resync -c を実行したあと)
- Identity Synchronization for Windows が Windows に新しいユーザーを作成したとき (新しいユーザーが Directory Server から同期されたか idsync resync -c -o Sun を実行したあと)
- この章で説明するように、idsync resync -c -f を実行して Directory Server と Windows にすでに存在するエントリをリンクしたとき。

既存ユーザーをリンクするには、2つのディレクトリ間でユーザーを一致させるルールを指定します。たとえば、2つのディレクトリでユーザーエントリをリンクするには、姓と名の両方を、両方のディレクトリエントリで一致させます。

ユーザーエントリのリンクとデータ競合の解決は、科学的というよりも技術的に説明されることがあります。相対するディレクトリソースの2ユーザーを idsync resync サブコマンドでリンクできないのには多くの理由があり、その大半はリンクされるディレクトリ内のデータの一貫性に起因します。

idsync resync を使用する1つの方針は、-n 引数を使用することです。この場合、セーフモードで実行されるため、実際には変更せずに操作の影響を確認できます。セーフモードで実行することにより、ユーザーマッチング条件の最適な組み合わせが見つかるまで、リンク条件を少しずつ調整できます。

ただし、リンクの正確さとリンクの範囲を通して実現されるバランスがあることに注意するようにしてください。

たとえば両方のディレクトリソースに従業員 ID または社会保障番号が含まれている場合に、この番号だけを含むリンク条件から開始するとします。リンクの正確さを向上させるには、条件に姓の属性も含めるべきだと考えるかもしれません。しかし、ID 単独では一致するエントリが、データ内の姓の値に整合性がないために一致しなくなり、そのためにリンクが失われる可能性があります。リンクできなかったエントリのデータをきれいにする作業を実行する必要が生じます。

注-グループ同期が有効な場合、グループはユーザーのリンク方法と同様の方法でリンクされます。

idsync resync のオプション

idsync resync コマンドでは、次のオプションを使用できます。

表 8-2 idsync resync の使用法

引数	意味
-a <ldap-filter>	同期されるエントリを制限するように LDAP フィルタを指定します。フィルタは、再同期操作のソースに適用されます。たとえば <code>idsync resync -o Sun -a "uid=*"</code> と指定すると、uid 属性を持つすべての Directory Server ユーザーが Active Directory に同期されます。
-l <sul-to-sync>	再同期する個別の同期ユーザーリスト (SUL) を指定します。 注: 複数の SUL ID を指定して複数の SUL を再同期できます。SUL ID を指定しない場合は、使用している SUL のすべてが再同期されません。
-o (Sun Windows)	再同期動作のソースを指定します。 <ul style="list-style-type: none"> ■ Sun: Windows エントリの属性値を Sun Java System Directory Server のディレクトリソースエントリの対応する属性値に設定します。 ■ Windows: Sun Java System Directory Server エントリの属性値を Windows ディレクトリソースエントリの対応する属性値に設定します。 (デフォルトは <i>Windows</i>)
-c	対応するユーザーが宛先で見つからない場合にユーザーエントリを自動的に作成します。 <ul style="list-style-type: none"> ■ Active Directory または Windows NT で作成されたユーザーに対して、暗号でセキュリティー保護されたパスワードをランダムに生成します。 ■ -i オプションを指定しない限り、Directory Server で作成されたユーザーに対して、特別なパスワード値 (<code>{PSWSYNC} *INVALID PASSWORD*</code>) を自動的に作成します 注: その方向で作成を設定していない場合であっても、Identity Synchronization for Windows はユーザーを作成しようとします。たとえば、Windows から Sun への同期 (またはその逆方向) を Identity Synchronization for Windows で設定していない場合でも、-c 引数を指定すれば Identity Synchronization for Windows は見つからなかったユーザーを作成しようとします。
-i (ALL_USERS NEW_USERS)	Sun ディレクトリソースで同期されたユーザーエントリのパスワードをリセットします。次回ユーザーパスワードが必要になったときに、それらのユーザーに対して現在のドメイン内でパスワード同期が実行されます。 <ul style="list-style-type: none"> ■ ALL_USERS: 同期されたすべてのユーザーに対してオンデマンドパスワード同期が実行されます。 ■ NEW_USERS: 新しく作成されたユーザーのみに対してオンデマンドパスワード同期が実行されます。

表 8-2 idsync resync の使用法 (続き)

引数	意味
-u	オブジェクトキャッシュを更新します。 この引数は、Windows ディレクトリソースのみでユーザーエントリのローカルキャッシュを更新します。既存の Windows ユーザーは Directory Server で作成されません。この引数を使用する場合、Windows ユーザーエントリは Directory Server ユーザーエントリと同期されません。この引数は、再同期ソースが Windows の場合のみ有効です。
-x	ソースエントリに一致しないすべての宛先ユーザーエントリを削除します。
-n	実際の変更を行わずに操作の影響をプレビューできるようにセーフモードで実行します。

表 8-3 idsync resync によって Directory Server でユーザーのパスワードが無効になるか

	Active Directory と Directory Server にユーザーのエントリがあり、リンクされている場合。	Active Directory と Directory Server にユーザーのエントリがあり、リンクされていない場合。	Active Directory にユーザーのエントリがあるが、Directory Server にはない場合。
-i ALL_USERS	はい	はい	はい
-i NEW_USERS	いいえ	いいえ	はい
No -i value	いいえ	いいえ	いいえ

次の表に、さまざまな引数を組み合わせたときの結果について例を示します。-h、-p、-D、-w、-、および-s 引数は、デフォルトであり、簡潔にするため省略しています。

表 8-4 idsync resync の使用例

引数	結果
idsync resync	resync の使用法の説明を表示します。
idsync resync -i ALL_USERS	すべてのユーザーのパスワードを無効にし、オンデマンドパスワード同期を実行します (Active Directory 環境のみで有効)。 混在環境 (Active Directory と NT ドメインの両方) では、明示的に Active Directory SUL を示してください。

表 8-4 idsync resync の使用例 (続き)

引数	結果
<code>idsync resync</code>	resync の使用法の説明を表示します。
<code>idsync resync -c -i NEW_USERS</code>	Directory Server で見つからなかったユーザーを作成し、それらのユーザーのパスワードを無効にしてオンデマンドパスワード同期を実行します。このコマンドを使用すると、既存の Windows ユーザーが空の Directory Server インスタンスに生成されます。
<code>idsync resync -c -l SUL_sales -l SUL_finance</code>	SUL_sales SUL および SUL_finance SUL のみについて、すべての既存の Active Directory ユーザーを Directory Server に作成します。ただしオンデマンドパスワード同期は実行されません。
<code>idsync resync -n</code>	セーフモードで実行し、変更を実際には行わずに resync 操作の影響を確認できるようにします。
<code>idsync resync -o Sun -a "(sn=Smith)"</code>	Windows で、姓 (sn) が Smith であるすべての Directory Server ユーザーを同期します。
<code>idsync resync -u</code>	Windows コネクタのみのオブジェクトキャッシュを更新して、既存のユーザーが Directory Server で作成されないようにします。実際に同期されるユーザーはありません。
<code>idsync resync -f link.cfg</code>	link.cfg ファイルで指定されたリンク条件に基づいて、リンクされていないユーザーをリンクします。Identity Synchronization for Windows はユーザーを作成または変更しませんが、新しくリンクされるユーザーの Directory Server パスワードは Active Directory ユーザーのパスワードに設定されます。

注 - `idsync resync` を使用してユーザーをリンクするときは、インデックスが作成された属性を操作に使用するようになっています。インデックスが作成されていない属性は、パフォーマンスに影響を与える可能性があります。

UserMatchingCriteria セットに複数の属性があり、それらのうち少なくとも 1 つでインデックスが作成されていれば、パフォーマンスはおそらく許容できます。ただし、UserMatchingCriteria でインデックスが作成された属性がない場合、大きなディレクトリではパフォーマンスが許容できなくなります。

セントラルログで結果の確認

すべての `idsync resync` 操作の結果は、`resync.log` という名前の特殊なセントラルログに報告されます。このログには、正しくリンクされて同期されたユーザー、リンクに失敗したユーザー、および以前にリンクされたユーザーのすべてが一覧表示されます。

注 - あらかじめ存在する特殊な Active Directory ユーザー (Administrator や Guest など) は、このログに失敗として記録されることがあります。

同期の起動および停止

同期の起動および停止によって個別の Java プロセス、デーモン、またはサービスは起動または停止されません。同期を起動すると、同期を停止しても操作は一時停止するだけです。同期を再起動すると、同期が停止した時点から再開され、変更は失われません。

▼ 同期を起動または停止する

- 1 Sun Java System Server コンソールのナビゲーション区画で、**Identity Synchronization for Windows** インスタンスを選択します。
- 2 **Identity Synchronization for Windows** 区画が表示されたら、右上の「開く」ボタンをクリックします。
- 3 要求されたら、設定パスワードを入力します。
- 4 「タスク」タブを選択します。

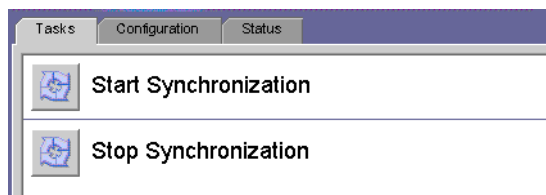


図 8-1 同期の起動および停止

- 同期を起動するには、「同期の起動」をクリックします。
- 同期を停止するには、「同期の停止」をクリックします。

注 - `idsync startsync` および `idsync stopsync` コマンド行ユーティリティーを使用して同期を起動および停止することもできます。詳細な手順については、[300 ページの「startsync の使用」](#) および [301 ページの「stopsync の使用」](#) を参照してください

再同期されたユーザー/グループ

グループを再同期するには、コンソールまたはコマンド行インタフェースを使用してグループ同期機能を有効にします。

グループ同期機能を有効にする方法については、[203 ページの「グループ同期の設定」](#) を参照してください

サービスの起動および停止

Identity Synchronization for Windows および Message Queue は、Solaris および Linux ではデーモンとして、Windows ではサービスとしてインストールされます。これらのプロセスは、システムのブート時に自動的に起動しますが、次のようにして手動で起動および停止することもできます。

- **Solaris** の場合: コマンド行から、次のように入力します。
 - `/etc/init.d/isw start` と入力すると、すべての Identity Synchronization for Windows プロセスを起動します。
 - `/etc/init.d/isw stop` と入力すると、すべての Identity Synchronization for Windows プロセスを停止します。
 - `/etc/init.d/imq start` と入力すると、Message Queue ブローカを起動します。
 - `/etc/init.d/imq stop` と入力すると、Message Queue ブローカを停止します。
- **Linux** の場合: コマンド行から、次のように入力します。
 - `/etc/init.d/isw start` と入力すると、すべての Identity Synchronization for Windows プロセスを起動します。
 - `/etc/init.d/isw stop` と入力すると、すべての Identity Synchronization for Windows プロセスを停止します。
 - `/etc/init.d/imq start` と入力すると、Message Queue ブローカを起動します。
 - `/etc/init.d/imq stop` と入力すると、Message Queue ブローカを停止します。
- **Windows** の場合:
 - Windows の「スタート」メニューから次の操作を実行します。
 1. 「スタート」 → 「設定」 → 「コントロールパネル」 → 「管理ツール」 を選択します。

2. 「管理ツール」ダイアログボックスが表示されたら、「サービス」アイコンをダブルクリックして「サービス」ダイアログボックスを開きます。
 3. メニューバーから「Identity Synchronization for Windows」を選択し、次に「操作」→「開始」(または「停止」)を選択します。iMQブローカについて繰り返します。
- コマンド行から `net` コマンドを入力してサービスを制御します。

注 - Identity Synchronization for Windows デーモン/サービスを停止したあとは、もう一度起動するまで 30 秒待機してください。コネクタが安全にシャットダウンするには数秒かかることがあります。

ソフトウェアの削除

この章では、Identity Synchronization for Windows 6.0 を削除する手順を説明します。この章の内容は次のとおりです。

- 241 ページの「アンインストールの計画」
- 242 ページの「ソフトウェアのアンインストール」
- 247 ページの「コンソールの手動アンインストール」

アンインストールの計画

ソフトウェアを削除する前に、次の点を確認してください。

- 関連するコネクタをアンインストールする前に、サブコンポーネントとディレクトリサーバープラグインをアンインストールします。また、コアをアンインストールする前に、すべてのコネクタをアンインストールします。Active Directory コネクタには、アンインストールするサブコンポーネントはありません。いずれかのコンポーネントを正しい順序でアンインストールしなかった場合、その他のコンポーネントを選択してアンインストールすることができなくなります。たとえば、コネクタを先にアンインストールしなければ、コアを選択してアンインストールすることはできません。
- コアをアンインストールする前に、ディレクトリサーバープラグインをアンインストールします。
コアを先にアンインストールすると、プラグインのビットは削除されますが、Directory Server からは登録解除されず、手動で `cn=pswsync,cn=plugins,cn=config` を削除しないかぎり、Directory Server を起動できなくなります。
- 主サーバーと副サーバーのほかにレプリカを使用するレプリケート環境では、ディレクトリサーバープラグインをアンインストールしたあとに、サーバーを再起動してください。
- 各コネクタはどのような順序でアンインストールしてもかまいません。

- Sun Java System ディレクトリサーバーコネクタまたは Windows コネクタをアンインストールしたあとは、追加の手順を実行して、別のマシンにコネクタを再インストールするか、または別のサーバーポートを使用するように設定します。
この場合、対応するすべてのサブコンポーネントをアンインストールおよび再インストールし、コアがインストールされている Identity Synchronization for Windows デモンまたはサービスを再開します (239 ページの「サービスの起動および停止」を参照)。
- Windows 2000 および NT プラットフォームでは、`isw-hostname` ディレクトリにある `uninstall.cmd` スクリプトを実行します。このバッチファイルは、管理者として実行します。
- Solaris または Linux オペレーティングシステムでは、インストールディレクトリ (デフォルトでは `/opt/SUN/isw`) にある `Uninstall.sh` スクリプトを実行します。このスクリプトは、`root` として実行します。

注-手順に従って製品のコンポーネントとサブコンポーネントを明示的にアンインストールし、すべてのコンポーネントが正しくアンインストールされたことを確認してください。

ソフトウェアのアンインストール

システムには、次のいずれかまたはすべての Identity Synchronization for Windows コンポーネントがインストールされている場合があります。

- Active Directory コネクタ
- ディレクトリサーバーコネクタおよびプラグイン
- コア

Windows NT システムには、Windows NT コネクタとサブコンポーネントが含まれている場合があります。

Solaris の場合は `runUninstaller.sh`、Linux の場合は `uninstaller.sh`、Windows の場合は `uninstall.cmd` を使用して、すべてのコネクタとサブコンポーネントを削除してから、コアを削除します (インストールされている場合)。

ここでは、次の手順について説明します。

- 243 ページの「コネクタのアンインストール」
- 244 ページの「コアをアンインストールする」

コネクタのアンインストール

▼ コネクタをアンインストールする

- 1 アンインストールプログラム (**Solaris** の場合は `runUninstaller.sh`、**Linux** の場合は `uninstaller.sh`、**Windows** の場合は `uninstall.cmd`) を起動します。
これらのプログラムは、インストールディレクトリ (デフォルトでは `/opt/SUNWisw` ディレクトリ) にあります。
- 2 「ようこそ」画面で「次へ」をクリックします。
- 3 設定ディレクトリのホスト名とポート番号を入力します。
 - 設定ディレクトリのルートサフィックスを選択します。必要な場合は、「更新」をクリックしてサフィックスのリストを表示します。
 - アンインストールプログラムと設定ディレクトリサーバーの間の通信をセキュリティー保護する場合は、「セキュリティー保護されたポート」ボックスにチェックマークを付け、**Directory Server** の SSL ポート番号を指定します。
- 4 設定ディレクトリの管理者の名前とパスワードを入力します。
- 5 アンインストールするコネクタを選択します。

注- 選択したコネクタは、ターゲットホストに存在している必要があります。

- 6 「次へ」をクリックして、さらにアンインストール関連の作業を行います。
- 7 概要ウィンドウが表示されます。このウィンドウに表示される指示に従います。
 - **Solaris** システムの場合: アンインストールログは `/var/sadm/install/logs/` に書き込まれます。
 - **Linux** システムの場合: アンインストールログは `/var/sadm/install/logs/` に書き込まれます。
 - **Windows** システムの場合: アンインストールログは `%TEMP%` ディレクトリに書き込まれます。このディレクトリは、次の場所にある **Local Settings** フォルダのサブディレクトリです。
`C:\Documents and Settings\Administrator`

注 - Windows 2000 Advanced Server などの一部の Windows システムでは、Local Settings フォルダは隠しフォルダになっています。このフォルダと Temp サブディレクトリを表示するには、次の手順に従います。

Windows エクスプローラを開き、メニューバーから「ツール」→「フォルダオプション」を選択します。「フォルダオプション」ダイアログボックスが表示されたら、「表示」タブをクリックし、「すべてのファイルとフォルダを表示する」オプションを有効にします。

- 8 「閉じる」をクリックしてプログラムを終了します。
- 9 ターゲットホストにインストールされているコネクタがそれ以上存在しない場合は、`isw-hostname` フォルダを安全に削除できます。
- 10 コネクタがインストールされているすべてのホストに対して、[243 ページの「コネクタのアンインストール」](#)の手順を繰り返します。

▼ コアをアンインストールする

注 - コアをアンインストールする前に、ディレクトリサーバープラグインをアンインストールしてください。

プラグインより先にコアをアンインストールすると、プラグインのビットは削除されますが、Directory Server からは登録解除されないため、手動で `cn=pswsync,cn=plugins,cn=config` を削除しないかぎり、Directory Server を起動できなくなります。

コアをアンインストールするには、次の手順を使用します。

- 1 アンインストールプログラムを起動します。
 - Windows マシンの場合:
 - a. 「スタート」ボタンをクリックし、「設定」→「コントロール パネル」の順に選択します。
 - b. 「プログラムの追加と削除」をダブルクリックします。
 - c. 「プログラムの追加と削除」ウィンドウで、「Identity Synchronization for Windows」を選択し、「削除」をクリックします。

- **Solaris** の場合は `runUninstaller.sh`、**Linux** の場合は `uninstaller.sh`、**Windows** の場合は `uninstall.cmd` を実行します。
これらのプログラムは、インストールディレクトリ (デフォルトでは、Solaris の場合は `/opt/SUNWisw` ディレクトリ、Linux の場合は `/opt/sun/isw` ディレクトリ) にあります。
- 2 「ようこそ」画面で「次へ」をクリックします。
 - 3 設定ディレクトリのホスト名とポート番号を入力します。
 - a. 設定ディレクトリのルートサフィックスを選択します。必要な場合は、「更新」をクリックしてサフィックスのリストを表示します。
 - b. アンインストールプログラムと設定ディレクトリサーバーの間の通信をセキュリティ保護する場合は、「セキュリティ保護されたポート」ボックスにチェックマークを付け、**Directory Server** の **SSL** ポート番号を指定します。
 - 4 設定ディレクトリの管理者の名前とパスワードを入力します。
 - 5 アンインストールするコアを選択し、「次へ」をクリックします。
 - 6 設定ディレクトリの **URL** を入力し、「更新」をクリックして、ドロップダウンリストから適切なルートサフィックスを選択します。
 - 7 「次へ」をクリックして、さらにアンインストール関連の作業を行います。
 - 8 概要ウィンドウが表示されます。このウィンドウに表示される指示に従います。
 - a. **Solaris** システムの場合: アンインストールログは `/var/sadm/install/logs/` に書き込まれます。
 - b. **Linux** システムの場合: アンインストールログは `/var/sadm/install/logs/` に書き込まれます。
 - c. **Windows** システムの場合: アンインストールログは `%TEMP%` ディレクトリに書き込まれます。このディレクトリは、次の場所にある Local Settings フォルダのサブディレクトリです。
`C:\Documents and Settings\Administrator`

注 - Windows 2000 Advanced Server などの一部の Windows システムでは、Local Settings フォルダは隠しフォルダになっています。

このフォルダと Temp サブディレクトリを表示するには、次の手順に従います。

Windows エクスプローラを開き、メニューバーから「ツール」→「フォルダオプション」を選択します。「フォルダオプション」ダイアログボックスが表示されたら、「表示」タブをクリックし、「すべてのファイルとフォルダを表示する」オプションを有効にします。

9 「閉じる」をクリックしてプログラムを終了します。

注 - ハードドライブの障害によりコネクタファイルを失った場合など、何らかの理由で特定のコネクタに対してアンインストールを実行できない場合は、idsync resetconn サブコマンドを使用します(295 ページの「resetconn の使用」を参照)。

このコマンドを実行すると、設定ディレクトリ内のコネクタの状態がアンインストール済みになりリセットされるので、そのコネクタを別の場所に再インストールできるようになります。resetconn サブコマンドでは、設定ディレクトリにアクセスするその他のコマンドと同様に、次の2つのオプションを指定できます。

- **-e dir-source**: リセットするディレクトリソースの名前を指定します。インストーラでは、ディレクトリソース名によってコネクタが識別されます。
- **-n** (セーフモード): 実際の処理を行わずに、コマンドに指定された引数が正しいかどうかを示します。

コマンドの例を次に示します。

```
idsync resetconn -D "cn=Directory Manager" -w [-h CR-hostname]
[-p 389] [-s dc=example,dc=sun,dc=com] -q [-Z] [-P "cert8.db"]
[-m "secmod.db"] -e "dc=central, dc=example,dc=com" [-n]
```

resetconn の出力は次のようになります。

注意: このプログラムは、指定されたディレクトリソース 'dc=central,dc=example,dc=com' に関連するコネクタのインストール状態を UNINSTALLED にリセットします。コネクタの状態を UNINSTALLED に変更するのは最後の手段です。これは、コネクタをアンインストールすることが目的ではありません。通常は、そのコネクタを使用するマシンを失い、アンインストールを実行できない場合に使用します。また、このプログラムは既存の設定を書き換えます。これは少し手間のかかるプロセスです。処理を進める前に、コンソール、実行中のインストーラ、およびその他すべてのアイデンティティ同期プロセスを停止します。また、設定レジストリ内の ou=Services ツリーをバックアップのために ldif ファイルにエクスポートします。コネクタのインストーラ設定をリセットしてよろしいですか (y/n)?

コンソールの手動アンインストール

その他の Identity Synchronization for Windows コンポーネントをすべて削除したあとに、コンソールを手動でアンインストールしなければならない場合があります。

Solaris または Linux システムでの操作

▼ Solaris または Linux からコンソールをアンインストールする

- 1 設定ディレクトリから次のサブツリーを削除します。

```
cn=Sun Java (TM) System Identity Synchronization for Windows,  
cn=server_group,cn=hostname,  
ou=domain_name, o=netscaperoot
```

- 2 インストールされたすべてのコンソールで、次のディレクトリから、プレフィックスが *isw* の *.jar* ファイルをすべて削除します。

```
serverroot/server/java/jars
```

Windows システムでの操作

▼ Windows Active Directory または NT システムからコンソールをアンインストールする

- 1 設定ディレクトリから次のサブツリーを削除します。

```
cn=Sun Java (TM) System Identity Synchronization for Windows,  
cn=server_group, cn=hostname,  
ou=domain_name, o=netscaperoot
```

- 2 インストールされたすべてのコンソールで、次のディレクトリから、プレフィックスが *isw* の *.jar* ファイルをすべて削除します。

```
serverroot/server/java/jars
```


◆◆◆ 第 10 章

セキュリティの設定

この章では、使用している配備のセキュリティの設定に関する重要な情報について説明します。ここで説明する内容は、次のとおりです。

- 249 ページの「セキュリティの概要」
- 255 ページの「セキュリティの強化」
- 258 ページの「レプリケートされた設定のセキュリティ保護」
- 260 ページの「idsync certinfo の使用」
- 262 ページの「Directory Server での SSL の有効化」
- 264 ページの「Active Directory コネクタでの SSL の有効化」
- 267 ページの「Directory Server への Active Directory 証明書の追加」
- 268 ページの「ディレクトリサーバーコネクタへの Directory Server 証明書の追加」

注 - この章は、公開鍵暗号方式と SSL (Secure Sockets Layer) プロトコルの基本概念をよく理解し、イントラネット、エクストラネット、インターネットセキュリティ、エンタープライズでのデジタル証明書の役割の概念を理解していることを前提としています。これらの概念を理解していない場合は、*Managing Servers with iPlanet Console 5.0* のマニュアルのセキュリティ関連の付録を参照してください。

セキュリティの概要

パスワードは機密情報です。このため、Identity Synchronization for Windows は、同期されるディレクトリにアクセスするためのユーザーと管理のパスワード資格が危険にさらされないように、セキュリティ上の予防策を講じます。

ここでは、次のセキュリティ対策について説明します。

- 250 ページの「設定パスワードの指定」
- 250 ページの「SSL の使用」
- 251 ページの「生成された 3DES キー」
- 251 ページの「SSL および 3DES キーでの保護の概要」

- 253 ページの「Message Queue のアクセス制御」
- 254 ページの「ディレクトリ資格」
- 254 ページの「持続的記憶領域保護の概要」

このセキュリティ対策は、次のイベントの発生を防ぐことを目的としています。

- 盗聴者によるネットワーク上での平文パスワードの傍受
- ユーザーの平文パスワードの傍受と同様、ユーザーのパスワードを選択した値に変更するための攻撃者によるコネクタへの操作
- Identity Synchronization for Windows の特権が必要なコンポーネントへの攻撃者によるアクセス
- 特権のないユーザーによるディスクに格納されたファイルからのパスワードの回復
- 侵入者によるシステムのコンピュータの1つから取り外されたハードディスクからのパスワードの回復これは同期されたパスワードや、ディレクトリへのアクセスに使用するシステムパスワードの可能性があります。

設定パスワードの指定

製品の設定ディレクトリに格納されている間やネットワーク上で転送される間に機密情報を保護するために、Identity Synchronization for Windows は設定パスワードを使用します。管理者はコアのインストール時に設定パスワードを指定します。コンソールを開いたり、Identity Synchronization for Windows インストールプログラムを実行する場合にこのパスワードを指定します。

注-システムマネージャーはコネクタに渡す前に設定パスワードにアクセスする必要があります。このため、システムマネージャーはこのパスワードを初期設定ファイルに格納します。

ファイルシステムのアクセス制御は、非特権ユーザーがシステムマネージャーの初期設定ファイルにアクセスできないようにします。Identity Synchronization for Windows インストールプログラムは、このパスワードにパスワードポリシーを強制しません。

設定パスワードの選択時にセキュリティを強化するには、255 ページの「セキュリティの強化」を参照してください。

SSL の使用

コンポーネントが LDAP を使用するあらゆる場所で LDAP over SSL を使用するよう Identity Synchronization for Windows を設定できます。Message Queue へのアクセスはすべて SSL で保護されます。

Directory Server から Active Directory に同期するときは、Active Directory コネクタと Active Directory 間で SSL を使用します。

信頼できる SSL 証明書の要求

デフォルトでは、SSL を使用するよう設定されたコネクタは、信頼できない証明書、期限切れの証明書、および無効な証明書も含めて、Directory Server サーバーや Active Directory サーバーが返すあらゆる SSL 証明書を受け入れます。コネクタとサーバー間のネットワークトラフィックはすべて暗号化されますが、コネクタは本当の Active Directory または Directory Server に偽装したサーバーを検出しません。

コネクタが信頼できる証明書のみを受け入れるようにするには、コンソールを使用して「ディレクトリソースの設定」ウィザードの「拡張セキュリティオプションの指定」パネルにある「信頼できる SSL の証明書を要求」オプションを有効にします (172 ページの「Active Directory ソースの作成」を参照)。このオプションを有効にしたあと、idsync certinfo で報告された適切な CA 証明書をコネクタの証明書データベースに追加します。

生成された 3DES キー

設定パスワードから生成された 3DES キーは、製品の設定ディレクトリですべての機密情報をセキュリティ保護するために使用されます。ログメッセージを除いて、Message Queue に入れられるメッセージはすべてトピックごとの 3DES キーで暗号化されます。コネクタとサブコンポーネント間でやり取りされるメッセージは、セッションごとの 3DES キーで暗号化されます。ディレクトリサーバープラグインは、3DES キーでユーザーパスワードの変更をすべて暗号化します。

SSL および 3DES キーでの保護の概要

251 ページの「SSL および 3DES キーでの保護の概要」では、Identity Synchronization for Windows がネットワーク上でやり取りされる機密情報を保護する方法をまとめています。

表 10-1 ネットワークセキュリティを使用した機密情報の保護

使用する保護方法	次の情報タイプ間
----------	----------

表 10-1 ネットワークセキュリティを使用した機密情報の保護 (続き)

LDAP over SSL (オプション)	<ul style="list-style-type: none">■ ディレクトリサーバーコネクタと Directory Server、Active Directory コネクタと Active Directory■ ディレクトリサーバープラグインと Active Directory■ コマンド行インタフェースと製品の設定ディレクトリ■ コンソールと製品の設定ディレクトリ■ コンソールと Active Directory グローバルカタログ■ コンソールと Active Directory ドメインまたは同期される Directory Server■ Message Queue ブローカと製品の設定ディレクトリ■ コネクタ、システムマネージャー、セントラルロガー、コマンド行インタフェース、およびコンソールは LDAPS を介して Message Queue を認証できません。■ インストーラと設定 Directory Server■ インストーラと Active Directory■ インストーラと同期される Directory Server
3DES キーでの暗号化 (デフォルト)	<ul style="list-style-type: none">■ ディレクトリサーバーコネクタとディレクトリサーバープラグイン (すべてのデータ)■ Windows NT コネクタ、Windows NT パスワードフィルタ DLL、Windows NT 変更検出機能 (すべてのデータ)■ 製品の設定ディレクトリにあるすべての機密情報■ コネクタとサブコンポーネント間でやり取りされるすべてのメッセージ (セッションごとの 3DES キーで暗号化)■ Message Queue でやり取りされるログ以外のすべてのメッセージ

251 ページの「[SSL および 3DES キーでの保護の概要](#)」には、この節で説明するセキュリティ機能の概要が記載されています。

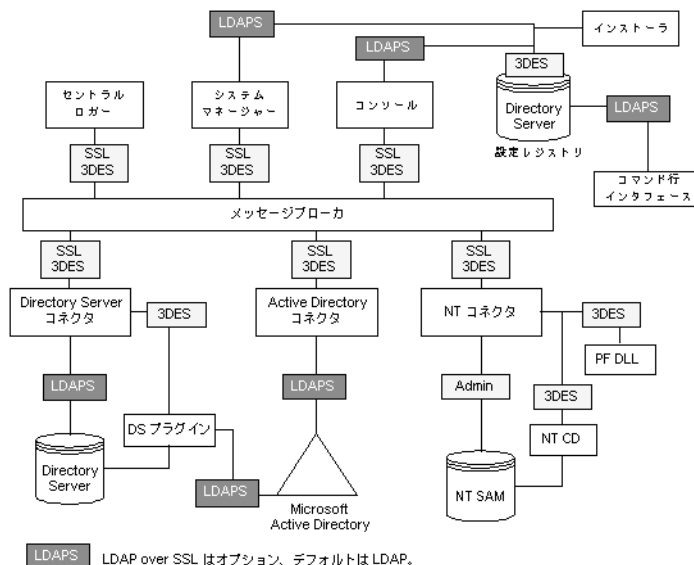


図 10-1 Identity Synchronization for Windows のセキュリティ概要

Message Queue のアクセス制御

Identity Synchronization for Windows は Message Queue のアクセス制御を使用して、各コネクタが受信するメッセージを信頼できるよう、メッセージのサブスクリプションとパブリッシングへの承認されていないアクセスを防止します。

Message Queue ブローカにアクセスするために、Message Queue とコネクタのみが認識する固有のユーザー名とパスワードが提供されます。Message Queue でやり取りされる各メッセージは、トピックごとに 3DES キーで暗号化され、メッセージの内容を保護し、トピックキーを知らない部外者が重要なメッセージを送信できないようにします。これらの対策によって、(a) 攻撃者が偽造したパスワード同期メッセージをコネクタに送信し、(b) 攻撃者がコネクタを偽装して、実際のパスワードの更新を受信しないようにします。

注-デフォルトでは、コネクタやシステムマネージャーのような Message Queue のクライアントは Message Queue ブローカが返すあらゆる SSL 証明書を受け入れます。Message Queue の証明書の検証とその他の Message Queue 関連のセキュリティの問題の詳細については、255 ページの「セキュリティの強化」を参照してください。

ディレクトリ資格

特権資格は、Active Directory と、同期される Directory Server でパスワードを変更するためにコネクタに必要です。これらの特権資格は、製品の設定ディレクトリに格納される前に暗号化されます。

持続的記憶領域保護の概要

254 ページの「[持続的記憶領域保護の概要](#)」では、Identity Synchronization for Windows がディスクに格納された機密情報を保護する方法をまとめています。

表 10-2 持続的記憶領域保護

持続的記憶領域	機密情報	保護
設定 Directory Server に格納された製品の設定	ディレクトリにアクセスするための資格と Message Queue ごとのトピック 3DES キーが製品の設定ディレクトリに格納されます。	製品の設定ディレクトリに格納された機密情報はすべて設定パスワードで生成された 3DES キーで暗号化されます。製品の設定ディレクトリをさらに保護するための推奨事項については、 255 ページの「セキュリティの強化」 を参照してください。
Directory Server の旧バージョン形式の変更ログ	ディレクトリサーバープラグインは、Directory Server の旧バージョン形式の変更ログに書き込む前にパスワードの変更を取得して暗号化します。	ディレクトリサーバープラグインは、ユーザーパスワードの変更をすべて各配備に固有の 3DES キーで暗号化します。
Message Queue ブローカの持続的記憶領域	Message Queue ブローカは、全コネクタ間でやり取りされるパスワード同期メッセージを格納します。	ログメッセージを除いて、持続メッセージはすべてトピックごとの 3DES キーで暗号化されます。
Message Queue ブローカのディレクトリ資格	Message Queue ブローカは、製品の設定ディレクトリに対してユーザーを認証します。これは、コアインストール中に提供されたディレクトリ管理者のユーザー名とパスワードを使用して設定ディレクトリに接続します。	ディレクトリパスワードは、ファイルシステムアクセス制御によって保護されるパスワードファイルに格納されます。
システムマネージャーのブートファイル	システムマネージャーのブートファイルには、設定にアクセスするための情報が含まれています。これには、設定パスワードとコアインストール中に提供されたディレクトリ管理者のユーザー名とパスワードが含まれます。	このファイルはファイルシステムアクセス制御によって保護されます。
コネクタとセントラルロガーのブートファイル	各コネクタとセントラルロガーには Message Queue にアクセスするための資格を持った初期設定ファイルがあります。	これらのファイルはファイルシステムアクセス制御によって保護されます。

表 10-2 持続的記憶領域保護 (続き)

持続的記憶領域	機密情報	保護
ディレクトリサーバープラグインのブート設定	cn=config に格納されるプラグインの設定には、コネクタに接続するための資格が含まれます。	cn=config サブツリーは、ACI によって保護されます。このツリーをミラー化する dse.ldif ファイルはファイルシステムアクセス制御によって保護されます。
NT パスワードフィルタ DLL および NT 変更検出機能のブート設定	Windows レジストリに格納される NT サブコネクトの設定には、コネクタに接続するための資格が含まれます。	PDC レジストリへのアクセスがセキュリティ保護されていない場合、これらのレジストリキーはアクセス制御で保護できません。
Windows コネクタのオブジェクトキャッシュ	Windows コネクタはハッシュされたユーザーのパスワードをコネクタのオブジェクトキャッシュに格納します。	パスワードは平文では格納されず、MD5 ハッシュで暗号化されます。これらのデータベースファイルはファイルシステムアクセス制御によって保護されます。(255 ページの「セキュリティの強化」を参照)

セキュリティの強化

この節では、製品の現在のリリースでの潜在的なセキュリティの弱点と、製品のデフォルト設定以外でセキュリティを拡張および強化する方法の推奨事項について説明します。次について説明します。

- 255 ページの「設定パスワード」
- 256 ページの「設定ディレクトリの資格の作成」
- 256 ページの「Message Queue のクライアント証明書を検証」
- 257 ページの「Message Queue の自己署名付き SSL 証明書」
- 257 ページの「Message Queue ブローカへのアクセス」
- 257 ページの「設定ディレクトリ証明書の検証」
- 257 ページの「設定ディレクトリへのアクセスの制限」

設定パスワード

設定パスワードは機密の設定情報を保護するために使用しますが、インストールプログラムはこのパスワードに対していずれのパスワードポリシーを強制しません。このパスワードがいくつかの厳しいガイドラインに従い、簡単に推測できない複雑なパスワードを選択し、強力なパスワードのための標準的なポリシーガイドラインを遵守してください。

たとえば、8文字以上で、大文字、小文字、英数字以外の文字を含むようにしてください。自分の名前や頭文字、日付などを含めないようにしてください。

設定ディレクトリの資格の作成

製品の設定ディレクトリがある Directory Server にアクセスするには、資格が構成管理者グループ内に必要です。しかし、何らかの理由で *admin* 以外の資格を作成する必要がある場合は、次を考慮します。

インストールプログラムはコンソール管理サブツリーに格納されたユーザーの資格を必要とします。しかし、コアインストールプログラムは *admin* 以外のユーザーを「`uid=admin,ou=Administrators, ou=TopologyManagement, o=NetscapeRoot`」に拡張しません。このため、コアインストール中に DN 全体を指定してください。

▼ *admin* 以外の新しいユーザーを作成する

- 1 次の場所にユーザーを作成します。

`ou=Administrators, ou=TopologyManagement, o=NetscapeRoot`

- 2 新しい資格を構成管理者グループに追加します。
- 3 製品の設定ディレクトリが格納されている **Directory Server** へのアクセスをこのユーザーのみに許可するか構成管理者グループのすべてのユーザーに許可するよう **ACI** を設定します。
- 4 コアインストール中に **DN** 全体を指定します。

Directory Server でのアクセス制御の管理の詳細については、『[Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド](#)』の第7章「**Directory Server のアクセス制御**」を参照してください。

Message Queue のクライアント証明書の検証

デフォルトで、コネクタやシステムマネージャーなど Message Queue のクライアントは、Message Queue ブローカが返した SSL 証明書をすべて受け入れます。

▼ Message Queue のクライアント証明書を検証する

- 1 この設定をオーバーライドして Message Queue のクライアントが Message Queue ブローカの証明書を検証するようにするには、次を編集します。

`installation_root/resources/WatchList.properties`

- 2 `Watchlist.properties` で各プロセスの **JVM** 引数に次を追加します。
`-Djavax.net.ssl.trustStore=keystore_path-DimqSSLIsHostTrusted=false`

3 Identity Synchronization for Windows デーモンまたはサービスを再起動します。

`javax.net.ssl.trustStore` プロパティはブローカの証明書を信頼する JSEE キーストアをポイントするようにしてください。たとえば、`/etc/imq/keystore` はブローカによって使用されるキーストアと同じため、コアがインストールされたマシン上で使用できます。

Message Queue の自己署名付き SSL 証明書

デフォルトで、Message Queue ブローカは自己署名付き SSL 証明書を使用します。別の証明書をインストールするには、Java に付属の `keytool` ユーティリティを使用し、ブローカのキーストア (Solaris の場合

`/var/imq/instances/isw-broker/etc/keystore`、Linux の場合

`/var/opt/sun/mq/instances/isw-broker/etc/keystore`、Windows 2000 の場合

`mq_installation_root /var/instances/isw-broker/etc/keystore`) を変更します。証明書のエイリアスは `imq` にします。

Message Queue ブローカへのアクセス

Message Queue はデフォルトで、そのポートマッパーを除くすべてのサービスに対して動的ポートを使用します。ファイアウォールを介してブローカにアクセスしたり、ブローカに接続できるホストのセットを制限したりするには、ブローカがすべてのサービスに対して固定ポートを使用している必要があります。

このためには、`imq.service_name protocol_type .port` ブローカ設定プロパティを設定します。詳細は、『*Sun Java System Message Queue 管理ガイド*』を参照してください。

設定ディレクトリ証明書の検証

システムマネージャーは、SSL を介した製品の設定ディレクトリへの接続時にすべての証明書を受け入れます。Message Queue ブローカも SSL を介した製品の設定ディレクトリへの接続時にすべての証明書を受け入れます。現在、システムマネージャーまたは Message Queue ブローカに製品の設定ディレクトリの SSL 証明書を検証させる方法はありません。

設定ディレクトリへのアクセスの制限

コアのインストール時に、製品の設定ディレクトリが格納された Directory Server への情報の追加プロセスには、アクセス制御情報の追加は含まれません。アクセスを設定の管理者のみに制限するには、次の ACI を使用できます。

```
(targetattr = "*")
(target = "ldap://ou=IdentitySynchronization,
ou=Services,dc=example,dc=com")
(version 3.0;acl "Test";deny (all)
(groupdn != "ldap://cn=Configuration Administrators,
ou=Groups, ou=TopologyManagement, o=NetscapeRoot");)
```

Directory Server でのアクセス制御の管理の詳細については、『[Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド](#)』の第7章「[Directory Server のアクセス制御](#)」を参照してください。

レプリケートされた設定のセキュリティー保護

レプリケーションを使用して Directory Server に接続する配備は、[249 ページ](#)の「[セキュリティーの概要](#)」で指定した規則に従います。この節では、レプリケートされた設定の例を示し、この設定で SSL の使用を有効にする方法を説明します。

注-レプリケートされた設定の計画、配備、セキュリティー保護の概要については、[付録 D 「Identity Synchronization for Windows の同期ユーザーリストの定義と設定」](#)を参照してください。

[258 ページ](#)の「[レプリケートされた設定のセキュリティー保護](#)」では、CA 証明書を必要とする設定コンポーネントをリストし、どこでどの証明書が必要かを識別します。

表 10-3 CA 証明書を必要とする MMR 設定コンポーネント

コンポーネント	必要な CA 証明書
Directory Server のレプリケートされた優先マスター	Active Directory システム
Directory Server のレプリケートされた副マスター	Active Directory システム
読み取り専用の Directory Server のハブ	Directory Server のレプリケートされた優先マスター Directory Server のレプリケートされた副マスター
ディレクトリサーバーコネクタ	Directory Server のレプリケートされた優先マスター Directory Server のレプリケートされた副マスター
Active Directory コネクタ	Active Directory システム

レプリケートされた設定には、MMR 設定にインストールされた Identity Synchronization for Windows が表示されます。MMR 設定には、複数の Directory Server の読み取り専用ハブまたはコンシューマを備えた 2 つのレプリケートされた

Directory Server のマスターがあります。各 Directory Server にはプラグインがあり、ディレクトリサーバーコネクタ、Active Directory システム、Active Directory コネクタはそれぞれ1つだけ存在します。

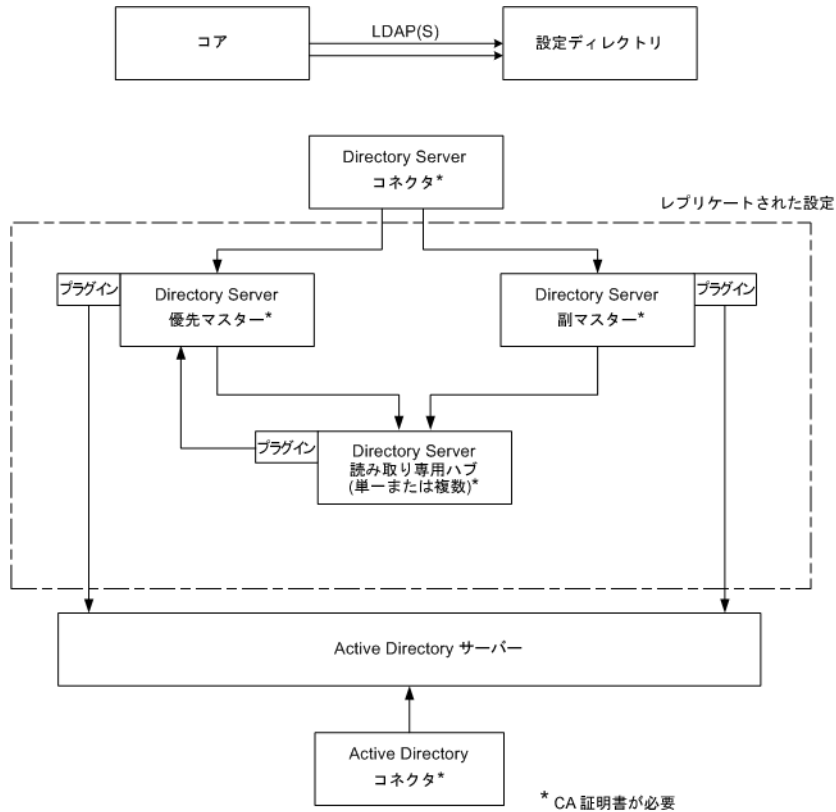


図 10-2 レプリケートされた設定

Directory Server ソースが SSL 用に設定されている場合、レプリカ Directory Server が優先 Directory Server および副 Directory Server の両方の証明書を信頼する必要があります。これは、Directory Server ハブまたは読み取り専用レプリカとともにシステムにインストールするタイプ other のすべてのディレクトリサーバープラグインに該当します。

注 - ディレクトリサーバープラグインはその関連付けられた Directory Server と同じ CA 証明書にアクセスできます。

上図は 2 つの Directory Server マスターの場合です。しかし、複数のマスターが含まれるように拡張できます。

idsync certinfo の使用

idsync certinfo ユーティリティーを使用し、現在の Identity Synchronization for Windows SSL 設定に基づいてどの証明書が必要かを判断できます。各証明書データベースで必要な証明書についての情報を取得するには、idsync certinfo を実行します。

注 - SSL 用に Directory Server ソースを設定する場合、レプリカ Directory Server が、すべてのディレクトリサブコンポーネントまたはプラグインについて、優先 Directory Server と副 Directory Server の両方のソース証明書を信頼する必要があります。

Identity Synchronization for Windows が (すべての証明書を信頼する設定を有効にして) SSL 接続を確立しようとし、SSL ネゴシエーション段階でサーバーに示された証明書で提供されたホスト名がサーバーのホスト名と一致しない場合、Identity Synchronization for Windows コネクタは接続の確立を拒否します。

Identity Synchronization for Windows 設定のディレクトリソースホスト名は常に、そのディレクトリソースに使用される証明書に組み込まれたホスト名と一致する必要があります。

引数

「引数」では、idsync certinfo サブコマンドとともに使用できる引数について説明します。

表 10-4 certinfo 引数

引数	説明
-h <i>CR-hostname</i>	設定ディレクトリのホスト名を指定します。この引数は、デフォルトでコアインストール中に指定された値になります。
-p <i>CR-port-no</i>	設定ディレクトリの LDAP ポート番号を指定します。(デフォルトは 389)

表 10-4 certinfo 引数 (続き)

引数	説明
<code>-D bind-DN</code>	設定ディレクトリのバインド識別名 (DN) を指定します。この引数は、デフォルトでコアインストール中に指定された値になります。
<code>-w bind-password -</code>	設定ディレクトリのバインドパスワードを指定します。- 値はパスワードを標準入力 (STDIN) から読み取ります。
<code>-s rootsuffix</code>	設定ディレクトリのルートサフィックスを指定します。ここで、ルートサフィックスは <code>dc=example,dc=com</code> のような識別名です。この引数は、デフォルトでコアインストール中に指定された値になります。
<code>-q configuration_password</code>	設定パスワードを指定します。- 値はパスワードを標準入力 (STDIN) から読み取ります。

使い方

次の例は、idsync certinfo を使用して、SSL 通信で実行するよう指定されたシステムコンポーネントを検索します。この例の結果は、2つのコネクタ (CNN101 と CNN100) を識別し、適切な CA 証明書をインポートする場所について指示します。

```
:\Program Files\Sun\MPS\isw-
hostname\bin idsync certinfo -h
CR-hostname -p 389 -D
"cn=Directory Manager" -w dirmanager -s dc=example,dc=com
-q password
コネクタ: CNN101
証明書データベースの場所: C:\Program Files\Sun\MPS\isw-
hostname\etc\CNN101
Active Directory から「Active Directory CA」証明書を取得し、
次のサーバーの Active Directory コネクタ証明書データベースに
インポートします。
ldaps://hostname.example.com:636
コネクタ: CNN100 証明書データベースの場所:
C:\Program Files\Sun\MPS\isw-
hostname\etc\CNN100
Directory Server 証明書データベースから「Directory Server CA」
証明書をエクスポートし、次のディレクトリサーバーコネクタ証明書
データベースにインポートします。
ldaps://hostname.example.com:636
次の Active Directory サーバーから「Active Directory CA」証明書を
エクスポートします。
hostname.example.sun.com:389
そして、次のサーバーの Directory Server サーバー証明書データ
ベースにインポートします。
ldaps://hostname.example.com:638
成功
```

Directory Server での SSL の有効化

次の手順に従って、自己署名付き証明書を使用して Directory Server で SSL を有効にします。

注-わかりやすいように手順を省略しています。詳細については、『[Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド](#)』を参照してください。

- Windows では、*ISW-host-name* \shared\bin フォルダにある Identity Synchronization for Windows 6.0 に付属の certutil バージョンを使用します。
 - Solaris では、certutil がデフォルトで /usr/sfw/bin にインストールされます。
 - Linux では、certutil はデフォルトで /opt/sun/private/bin にインストールされます。
-

▼ Directory Server で SSL を有効にする

Directory Server で SSL を有効にするには、次の手順を参照してください。

- 1 DS インスタンスを作成します。

```
/opt/SUNWdsee/ds6/bin/dsadm create -p non-ldap-port -P ldap-secure-port  
<DS-server-root>/slapd-<hostname>
```

- 2 インスタンスを起動します。

```
/opt/SUNWdsee/ds6/bin/dsadm start <DS-server-root>/slapd-<hostname >
```

- 3 自己署名付き証明書を作成します。

```
/opt/SUNWdsee/ds6/bin/dsadm add-selfsign-cert -S "cn=<machine name with  
domain>, o=<preferred root suffix>"/<DS-server-root>/slapd-<hostname>/<certificate name>
```

ここで、S は個別の証明書を作成してそれをデータベースに追加し、2 番目の変数は Directory Server インスタンスのパスを示し、最後の変数は証明書エイリアス用です。

- 4 この証明書にサーバーのプロパティを設定します。

```
/opt/SUNWdsee/ds6/bin/dsconf set-server-prop -p non-ldap-port  
ssl-rsa-cert-name:<certificate name>
```

- 5 DS を再起動します。

```
/opt/SUNWdsee/ds6/bin/dsadm restart /<DS-server-root>/slapd-<hostname >/
```

- 6 ここで、DSを停止してデフォルト証明書を削除します(これによって上記で生成された証明書がデフォルト証明書になる)。

```
/opt/SUNWdsee/ds6/bin/dsadm stop /<DS-server-root>/slapd-< hostname>/
```

- 7 ここでデフォルト証明書を削除します。

```
/opt/SUNWdsee/ds6/bin/dsadm remove-cert /<DS-server-root>/slapd-< hostname>/  
defaultCert
```

ここで、最初の変数はslapdパスを示し、2番目の変数は証明書のエイリアスを示します。上記のデフォルト証明書をエクスポートする場合は、次のコマンドを実行します。

```
/opt/SUNWdsee/ds6/bin/dsadm export-cert -o /<any path>/slapd-cert.export  
/<DS-server-root>/slapd-< hostname>/ <original default cert alias>
```

ここで、oは出力ファイル(/<any path>/slapd-cert.export)、2番目の変数はslapdパスを示し、3番目の変数は証明書エイリアスを示します。

Directory Serverの証明書データベースからのCA証明書の取得

必ずDirectory ServerでSSLを有効にしてください。ディレクトリサーバーコネクタの証明書データベースにインポートできるようにDirectory Server証明書を一時ファイルにエクスポートするには、次のコマンドを発行します。

```
<ISW-server-root>\shared\bin\certutil.exe -L -d .  
-P slapd-hostname- -n server-cert -a \ > C:\s-cert.txt
```

ISW-server-rootは、ISW-hostnameディレクトリのあるパスです。

これらの例は、サーバーのルート直下のエイリアスディレクトリで実行します。それ以外の場合、Directory Serverは証明書データベースを見つけられません。

(Solarisプラットフォームでdsadmコマンドを使用した) Directory ServerからのCA証明書の取得

必ずDirectory ServerでSSLを有効にしてください。CA証明書を取得するには、次のコマンドを発行します。

```
/opt/SUNWdsee/ds6/bin/dsadm export-cert -o /<any path>  
/slapd-cert.export /<DS-server-root>/slapd-<hostname>/  
<original default cert alias>
```

Active Directory コネクタでの SSL の有効化

Identity Synchronization for Windows は自動的に Active Directory SSL 証明書を SSL 経由で取得し、それらをコネクタの証明書データベースにコネクタに指定した資格と同じものでインポートします。

しかし、エラーが発生 (たとえば、無効な資格が見つかった、または SSL 証明書が見つからなかったなど) した場合は、Active Directory CA 証明書を取得して、それをコネクタの証明書データベースに追加できます。手順については次を参照してください。

- 264 ページの「Active Directory 証明書の取得」
- 266 ページの「Active Directory 証明書のコネクタの証明書データベースへの追加」

Active Directory 証明書の取得

エラーが発生した場合、次に説明するように certutil (Windows 2000/2003 に付属のプログラム) または LDAP を使用して Active Directory 証明書を取得できます。

注 - この節で説明する certutil コマンドは、前述の Directory Server に付属の certutil コマンドとは異なります。

Windows の certutil の使用

▼ certutil プログラムを使用して Active Directory 証明書を取得する

- 1 Active Directory マシンから次のコマンドを実行して証明書をエクスポートします。
`C:\>certutil -ca.cert cacert.bin`
- 2 その後 cacert.bin ファイルを証明書データベースにインポートできます。

LDAP の使用

▼ LDAP を使用して Active Directory 証明書を取得する

- 1 Active Directory に対して次の検索を行います。
`ldapsearch -h CR-hostname -D administrator_DN -w administrator_password
-b "cn=configuration,dc=put,dc=your,dc=domain,dc=here" "cacertificate=*`
ここで、`administrator_DN` は次のようになります。

```
cn=administrator,cn=users,dc=put,dc=your,dc=domain,dc=here
```


この例で、ドメイン名は *put.your.domain.name.here* です。

いくつかのエントリが検索フィルタに一致します。この DN で `cn=Certification Authorities, cn=Public Key Services` を使用したエントリがおそらく必要です。

- 2 テキストエディタを開いて、最初の **CA** 証明書属性の最初の値を切り取ります (**Base64** で符号化されたテキストブロックになります)。値(テキストブロック)をテキストエディタに貼り付けます(値のみ)。どの行も空白から始まらないようにコンテンツを編集します。
- 3 最初の行の前に `-----BEGIN CERTIFICATE-----`、最後の行のあとに `-----END CERTIFICATE-----` を追加します。次の例を参照してください。

```
-----BEGIN CERTIFICATE-----
MIIDvjCCA2igAwIBAgIQDgoyk+Tu14NGoQnxhmNHLjANBgk
qhkiG9w0BAQUFADCbjjEeMBwGCSqGSIb3DQEJARYPYmVydG
9sZEBzdW4uY29tMQswCQYDVQQGEwJVUzELMAkGA1UECBMCV
FgxDzANBGNVBAcTBkF1c3RpbjEZMBcGA1UEChMQU3VvIE1p
Y3Jvc3lzdGVtczEQMA4GA1UECXMHaVBSYw5ldDEUMBIGA1U
EAXMLUmVzdGF1cmFudHMwHhcNMDIwMTEwMDA1NDA5WhcNMT
IwMTEwMDA1OTQ2WjCBjjEeMBwGCSqGSIb3DQEJARYPYmVyd
G9sZEBzdW4uY29tMQswCQYDVQQGEwJVUzELMAkGA1UECBMCV
FgxDzANBGNVBAcTBkF1c3RpbjEZMBcGA1UEChMQU3VvIE1p
Y3Jvc3lzdGVtczEQMA4GA1UECXMHaVBSYw5ldDEUMBIGA1U
EAXMLUmVzdGF1cmFudHMwXDANBgkqhkiG9w0BAQEFAANLAD
BIAkEAYekZa8gwwhw3rLK3eV/12St1DVUsg31L0u3CnB8cM
HQZXlgiUgtQ0hm2kpZ4nEhwCAHhFLD3iIhIP4BGWQFjcwID
AQABo4IBnjCCAZowEwYJKwYBBAGCNxQCBAYeBABAEEwCwY
DVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBB
YEFJ5Bgt60yppq7T80ykw4LH6ws2d/IMIIBMGYDVR0fBIIBK
TCCASUwgdOggdCggc2GgcpsZGFwOi8vL0NOPVJlcl3RhdXJh
bnRzLENOPWRvd2l0Y2hlcixDTj1DRFAsQ049UHVibGljJTI
wS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZm
lndXJhdGlvbixEQz1yZXN0YXVyYW50cyxEQz1jZW50cmFsL
RPXN1bixEQz1jb20/Y2VydGlmawNhdGV5ZXZvY2F0aW9u
TGldD9iYXNlP29iamVjdGNSYXNzPWNSTERpc3RyYWJ1dG1
vb1BvaW50ME2gS6BJhkdodHRwOi8vZG93aXRjaGvYLnJlc3
RhdXJhbRzLmNlbnRyYwuc3VuLmNvbS9DZXJ0Rw5yb2xsL
1Jlc3RhdXJhbRzLmNybDAQBGRBgkrBgEEAYI3FQEEAwIBADAN
BgkqhkiG9w0BAQUFAANBAL5R9R+ONDdVHWu/5Sd9Tn9dpxN
8oegjS88ztv1HD6XSTDzGTuaaVebSZV3I+ghSInsgQBh0gW
4fGRwaI BvePI4=
-----END CERTIFICATE-----
```

- 4 証明書をファイル (`ad-cert.txt` など) に保存します。

- その後、このファイル (ad-cert.txt など) を証明書データベースにインポートできます。次の節 266 ページの「**Active Directory 証明書のコネクタの証明書データベースへの追加**」に進みます。

Active Directory 証明書のコネクタの証明書データベースへの追加

この手順は、Active Directory コネクタのインストール後にコネクタに対して SSL を有効にしている場合、またはインストール中に無効な資格が指定された場合にのみ使用します。

▼ Active Directory 証明書をコネクタの証明書データベースに追加する

- Active Directory コネクタがインストールされたマシンで **Identity Synchronization for Windows** サービス/デーモンを停止します。
- 次のいずれかの方法で **Active Directory CA** 証明書を取得します。
 - 264 ページの「**Windows の certutil の使用**」
 - 264 ページの「**LDAP の使用**」
- Active Directory コネクタのコネクタ ID が **CNN101** (コネクタ ID からその ID が管理するディレクトリソースへのマッピングについては logs/central/error.log を参照) であると仮定して、それがインストールされたマシンの証明書データベースディレクトリに移動して、証明書をファイルをインポートします。
 - certutil を使用して証明書を取得した場合は、次のように入力します。

```
<ISW-server-root>\shared\bin\certutil.exe -A -d . -n ad-ca-cert -t C,, -i \cacert.bin
```
 - LDAP を使用して証明書を取得した場合は、次のように入力します。

```
<ISW-server-root>\shared\bin\certutil.exe -A -d . -n ad-ca-cert -t C,,  
-a -i \ad-cert.txt
```

ISW-server-root は、ISW-hostname ディレクトリのあるパスです。

Solaris では、次の方法で dsadm コマンドを使用して証明書をインポートできます。

```
/opt/SUNWdsee/ds6/bin/dsadm add-cert -C <DS-server-root>/slapd-<hostname>/ ad-ca-cert cacert.bin
```

ここで、ad-ca-cert はインポート後に割り当てられた証明書の名前で、cacert.bin はインポートしようとしている証明書です。

- Identity Synchronization for Windows** サービス/デーモンを再起動します。

注 - Directory Server の `certutil.exe` は Directory Server のインストール時に自動的にインストールされるため、Directory Server のないマシンにインストールされたコネクタに CA 証明書を追加することはできません。

少なくとも、Active Directory コネクタがインストールされたサーバーに、Directory Server パッケージから Sun Java System サーバーの基本ライブラリと Sun Java System サーバーの基本システムライブラリをインストールする必要があります。管理サーバーや Directory Server のコンポーネントをインストールする必要はありません。

また、アンインストールできるように、コンソールで JRE サブコンポーネントを選択します。

Directory Server への Active Directory 証明書の追加

注 - 必ず Directory Server で SSL を有効にしてください。

▼ Active Directory CA 証明書を Directory Server 証明書データベースに追加する

- 1 次のいずれかの方法で Active Directory CA 証明書を取得します。
 - 264 ページの「Windows の `certutil` の使用」
 - 264 ページの「LDAP の使用」
- 2 Directory Server を停止します。
- 3 `cacert.bin` を Windows の場合は `<DS-server-root>\slapd-hostname\alias` フォルダにインポートします。Solaris と Linux の場合は、`<DS-server-root>/slapd-hostname/alias` ディレクトリにインポートします。
- 4 Directory Server がインストールされたマシンで、次の手順に従って Active Directory CA 証明書をインポートします。
 - `certutil` を使用して証明書を取得した場合は、次のように入力します。

```
<ISW_server_root>\shared\bin\certutil.exe -A -d .  
-P slapd-hostname- -n ad-ca-cert -t C,, -i \cacert.bin
```

- 証明書が LDAP を使用して取得された場合は、次のように入力します。

```
<ISW_server_root>\shared\bin\certutil.exe -A -d .  
-P slapd-hostname- -n ad-ca-cert -t C,, -a -i \ad-cert.txt
```

ISW-server-root は、ISW-hostname ディレクトリのあるパスです。

- 証明書が Solaris 上で dsadm コマンドを使用して取得された場合は、次のように入力します。

```
/opt/SUNWdsee/ds6/bin/dsadm add-cert -C <DS-server-root>  
/slapd-<hostname>/ ad-ca-cert cacert.bin
```

ここで、ad-ca-cert はインポート後に割り当てられた証明書の名前で、cacert.bin はインポートしようとしている証明書です。

- 5 Directory Server を起動します。

ディレクトリサーバーコネクタへの Directory Server 証明書の追加

ディレクトリサーバープラグインと Active Directory 間で SSL 通信を有効にしている場合は、Active Directory CA 証明書を各 Directory Server マスターの証明書データベースに追加します。

▼ Directory Server 証明書をディレクトリサーバーコネクタに追加する

- 1 ディレクトリサーバーコネクタがインストールされたマシンで **Identity Synchronization for Windows** サービス/デーモンを停止します。
- 2 **Directory Server CA** 証明書を取得します。
- 3 **Directory Server** のコネクタ ID が **CNN100** (コネクタ ID からその ID が管理するディレクトリソースへのマッピングについては logs/example/error.log を参照) であると仮定して、それがインストールされたマシンの証明書データベースディレクトリに移動して cacert.bin ファイルをインポートします。

```
<ISW_server_root>\shared\bin\certutil.exe -A -d . -n ds-cert -t C,, -i C:\s-cert
```

ISW-server-root は、ISW-hostname ディレクトリのあるパスです。

- 4 **Identity Synchronization for Windows** サービス/デーモンを再起動します。

監査ファイルとエラーファイルの理解

Identity Synchronization for Windows は、インストールや設定の状態、毎日のシステム動作、配備に関連するエラー状況についての情報を提供します。

この章では、次の節でこの情報にアクセスして理解する方法について説明します。

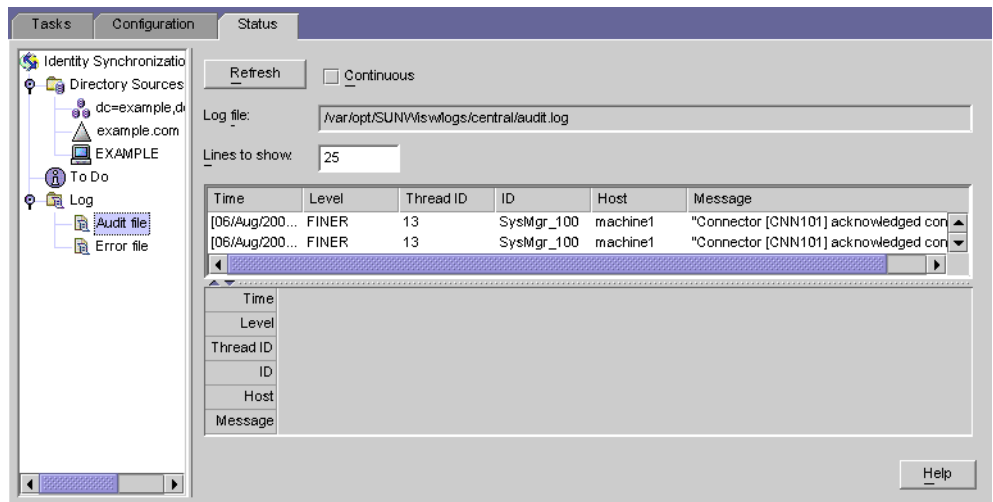
- 269 ページの「ログの理解」
- 274 ページの「ログファイルの設定」
- 276 ページの「ディレクトリソースの状態の表示」
- 278 ページの「インストール状態と設定状態の表示」
- 279 ページの「監査ログとエラーログの表示」
- 280 ページの「Windows NT マシンでの監査の有効化」

ログの理解

Identity Synchronization for Windows のコンソールの「状態」タブでさまざまな種類の情報を表示できます。

左側のナビゲーションツリー区画の次のノードの1つを選択すると、「状態」タブに表示される内容がその項目に固有の情報に変わります。

- ディレクトリソース: ディレクトリソースの状態情報を表示するには、そのディレクトリソースノード (dc=example、dc=com など) を選択します。
- **To Do:** Identity Synchronization for Windows を正常にインストールし、設定するために必要な手順のリストを表示するにはこのノードを選択します (終了した手順はグレー表示される)。
- 監査ファイル: 毎日のシステム運用の状態 (エラー状況を含む) を表示するには、このノードを選択します。
- エラーファイル: システムのエラー状況についての情報を表示するには、このノードを選択します。エラーログは、基本的にエラーエントリのみが表示されるフィルタとして機能します。



ログタイプ

この節では、Identity Synchronization for Windows で使用できるさまざまなログについて説明します。

- 270 ページの「セントラルログ」
- 271 ページの「ローカルコンポーネントログ」
- 272 ページの「ローカル Windows NT サブコンポーネントログ」
- 272 ページの「ディレクトリサーバープラグインログ」

セントラルログ

Identity Synchronization for Windows コンポーネントが Message Queue にアクセスできるかぎり 監査とエラーのメッセージはすべて Identity Synchronization for Windows のセントラルロガーに記録されます。結果として、すべてのコンポーネントのメッセージを含むこれらのセントラルログが監視のための一次ログとなります。

セントラルログは、コアがインストールされたマシンの次のディレクトリに配置されます。

- **Solaris** の場合: `/var/opt/SUNWiwsw/logs`
- **Linux** の場合: `/var/opt/sun/ismw/logs`
- **Windows** の場合: `installation_root/ismw-machine_name/logs/central/`

表 11-1 Identity Synchronization for Windows のログタイプ

ログ名	説明
error.log	警告と重要なメッセージが報告されます。
audit.log	各同期イベントについてのメッセージを含む error.log のスーパーセット。
resync.log	resync コマンドによって生成されたメッセージが報告されます。

各セントラルログには、各コンポーネント ID についての情報も含まれます。次にその例を示します。

```
[2003/03/14 14:48:23.296 -0600] INFO 13
"System Component Information:
SysMgr_100 is the system manager (CORE);
console is the Product Console User Interface;
CNN100 is the connector that manages
[example.com (ldaps:// server1.example.com:636)];
CNN101 is the connector that manages
[dc=example,dc=com (ldap:// server2.example.com:389)];"
```

セントラルロガーに加えて、各コンポーネントには独自のローカルログがあります。セントラルロガーに記録できない場合は、これらのローカルログを使用して、コネクタで問題を診断できます。

ローカルコンポーネントログ

各コネクタ、システムマネージャー、セントラルロガーには次のローカルログがあります。

表 11-2 ローカルログ

ログ名	説明
audit.log	各同期イベントについてのメッセージを含む error.log のスーパーセット。これらのメッセージはセントラル audit.log にも書き込まれます。
error.log	警告と重要なメッセージが報告されます。これらのメッセージはセントラル error.log にも書き込まれます。

これらのローカルログは次のサブディレクトリに配置されます。

- **Solaris** の場合: /var/opt/SUNWisw/logs
- **Linux** の場合: /var/opt/sun/isw/logs
- **Windows** の場合: *installation_root/isw-machine_name* /logs/central/
sysmgr および clogger100 (セントラルロガー) ディレクトリは、コアがインストールされたマシンにあります。

Identity Synchronization for Windows は、次のように日付を含むログファイルに現在のログを移動し、これらのローカルコンポーネントログを毎日ローテーションします。

```
audit_2004_08_06.log
```

注 - デフォルトで Identity Synchronization for Windows はコネクタログを 10 日後に削除します。Log.properties の `com.sun.directory.wps.logging.maxmiumDaysToKeepOldLogs` 値を編集し、サービスデーモンを再起動すると、この期間を延長できます。

ローカル Windows NT サブコンポーネントログ

次の Windows NT サブコンポーネントにもローカルログがあります。

- Windows NT 変更検出機能 DLL
- パスワードフィルタ DLL

これらのサブコンポーネントログは、次のディレクトリの SUBC1XX (たとえば、SUBC100) サブディレクトリにあります。

```
installation_root/isw-machine_name/logs/
```

Identity Synchronization for Windows はこれらのファイルのサイズを 1M バイトに制限し、最新の 10 のログのみを維持します。

ディレクトリサーバープラグインログ

ディレクトリサーバープラグインは、ディレクトリサーバーコネクタを介してセントラルログにログ情報を記録します。また、Directory Server ログ機能を介してもログ情報を記録します。この結果、ローカルディレクトリサーバープラグインログメッセージは、Directory Server エラーログにも保存されます。

Directory Server は他のディレクトリサーバープラグインとコンポーネントからの情報をエラーログに保存します。Identity Synchronization for Windows ディレクトリサーバープラグインからのメッセージを特定するために、`isw` 文字列を含む行をフィルタで除外できます。

デフォルトでは、最低限のプラグインメッセージのみがエラーログに表示されません。次に例を示します。

```
[14/Jun/2004:17:08:36 -0500] - ERROR<38747> - isw - conn=-1  
op=-1 msgId=-1 - Plug-ins unable to establish connection to DS Connector  
at attila:1388, will retry later
```


▼ エラーログの詳細レベルを変更する

次のように DSCC を使用して、Directory Server エラーログのデフォルトの詳細レベルを変更できます。

- 1 **Directory Service Control Center** にログインします。
- 2 「ディレクトリサーバー」タブページでログレベルを設定するサーバーをクリックします。
- 3 「サーバー設定」タブを選択してから「エラーロギング」タブを選択します。
- 4 「一般」→「ログに追加する項目」セクションで「プラグイン」を選択します。
- 5 「保存」をクリックします。

コマンド行を使用してプラグインのログ記録を有効にできます。

```
$ dsconf set-log-prop errors level:err-plugins
```

Directory Server のログ記録の詳細については、『[Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド](#)』の第 15 章「Directory Server のログ」を参照してください。

ログの読み取り

どのログメッセージにも次の情報が含まれています。

- **時刻:** ログエントリが生成された日時を示します。次に例を示します。


```
[13/Aug/2004:06:14:36:753 -0500]
```
- **レベル:** ログメッセージの重要度と詳細レベルを示します。Identity Synchronization for Windows は、次のログレベルを使用します。

表 11-3 ログレベル

ログレベル	説明
INFO	これらのメッセージは、各操作について最低限の情報を提供するため、システムが正しく実行されていることを確認できます。たとえば、変更が検出された時や同期が発生した時を確認できます。これらのメッセージは常に監査ログに記録されます。
FINE	これらのメッセージには、システム全体の各操作についてもう少し詳細な情報が含まれます。

表 11-3 ログレベル (続き)

FINER	これらのメッセージには、システム全体の各動作についてさらに詳細な情報が含まれます。すべてのコンポーネントでログレベルを「FINER」に調整すると、パフォーマンスに影響を与える場合があります。
FINEST	これらのメッセージには、システム全体の各動作についてもっとも詳細な情報が含まれます。すべてのコンポーネントでログレベルを「FINEST」に調整すると、パフォーマンスに大きく影響する場合があります。

- スレッド識別子: イベントを発生させた関数の Java スレッド識別子を表示します。
- ID: イベントを発生させたコンポーネント (コンソール、システムマネージャーなど) を特定します。
- ホスト: イベントを発生させたホスト名を表示します。
- メッセージ: イベントに関連する監査またはエラーの情報を表示します。次に例を示します。

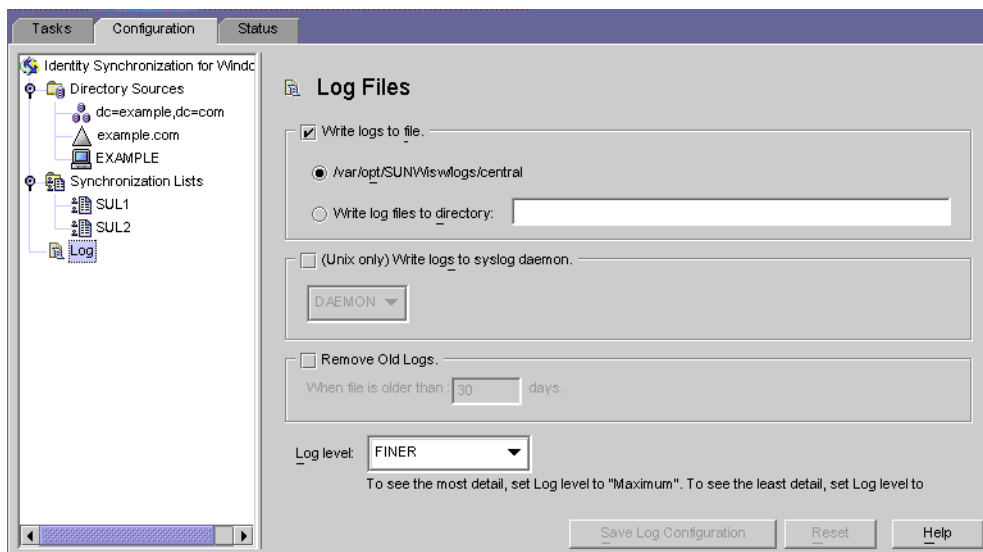
```

“Resetting Central Logger configuration ...”
“System manager is shutting down.”
“Processing request (ID=ID_number
from the console to stop synchronization.”
    
```

ログファイルの設定

▼ 配備のログを設定する

- 1 コンソールを開き「設定」タブを選択します。
- 2 ナビゲーションツリー区画で「ログ」ノードが表示されるまでノードを展開します。
- 3 「ログ」ノードを選択します。「設定」タブに「ログファイル」パネルが表示されます。



- 4 「ログファイル」区画を使用して、次のようにログファイルを設定します。
- 「ログをファイルに書き込む」このオプションを有効にすると、ログがコアホスト上のファイルに書き込まれます。
このオプションを選択したあと、次を実行できます。
 - デフォルトログディレクトリとファイル(たとえば、`/var/opt/SUNWisw/logs/central`)を有効にします。
 - 「ログファイルを書き込むディレクトリ」オプションを有効にしてから、ログファイルのパスとファイル名を指定します。

注-コンソールは、指定されたログファイルの場所が実際に存在するかどうか確認しません。存在しない場合は、セントラルロガーがログディレクトリを作成しようとします。このため、ログを表示しようとするまで存在しないログの場所を指定して保存したことはわかりません。ログの表示を何度か試行したあと、コンソールが指定した場所にログを見つけれないというメッセージが表示されます。

- **Solaris** の場合のみ – 「*syslog* デーモンにログを書き込む」: Identity Synchronization for Windows が Solaris プラットフォーム上にある場合にこのオプションを有効にします。ドロップダウンリストを使用してログを書き込むカテゴリを選択します。(デフォルトは *DAEMON*)

注- このオプションを選択すると、Identity Synchronization for Windows はすべてを syslog に書き込みますが、syslog はデフォルトによって WARNING と SEVERE のメッセージのみをログ記録するよう設定されています。

INFO メッセージを記録するように syslog を設定するには、`/etc/syslog.conf` を編集し、次の行を変更します。

```
*.err;kern.debug;daemon.notice;mail.crit /var/adm/messages
```

から

```
*.err;kern.debug;daemon.notice;daemon.info;mail.crit /var/adm/messages
```

この変更を行ったあと、次のように syslog デーモンを再起動します。

```
/etc/init.d/syslog stop ; /etc/init.d/syslog start
```

FINE、FINER、および FINEST ログを有効にするには、セミコロンで区切ったりストに `daemon.debug` を入れます。

- 「古いログの削除」: ログファイルの数は(1日に1つずつ)無限に増え続けます。ディスク容量を使い果たさないように、このオプションを有効にして、プログラムがセントラルログファイルから古いログを削除できる時を指定します。たとえば、30日と指定すると、Identity Synchronization for Windows は31日目にすべてのファイルを削除します。
 - 「ログレベル」: ドロップダウンリストを使用してシステムログで確認できる詳細レベルを選択します。(273ページの「ログの読み取り」を参照)
- 5 「ログ設定の保存」 ボタンをクリックして、選択したオプションに基づいてログファイルを作成します。

ディレクトリソースの状態の表示

▼ ディレクトリソースの状態を表示する

- 1 Identity Synchronization for Windows コンソールから「状態」タブを選択します。
- 2 ナビゲーションツリー区画で「ディレクトリソース」ノードを展開してから、ディレクトリソースノード (`dc=example`、`dc=com` など) を選択します。
「状態」タブの内容が選択したディレクトリソースに関連した情報に変わります。



注-ディレクトリソースの状態を表示している場合は、基本的にそのディレクトリソースに関連付けられたコネクタの状態を表示しています。

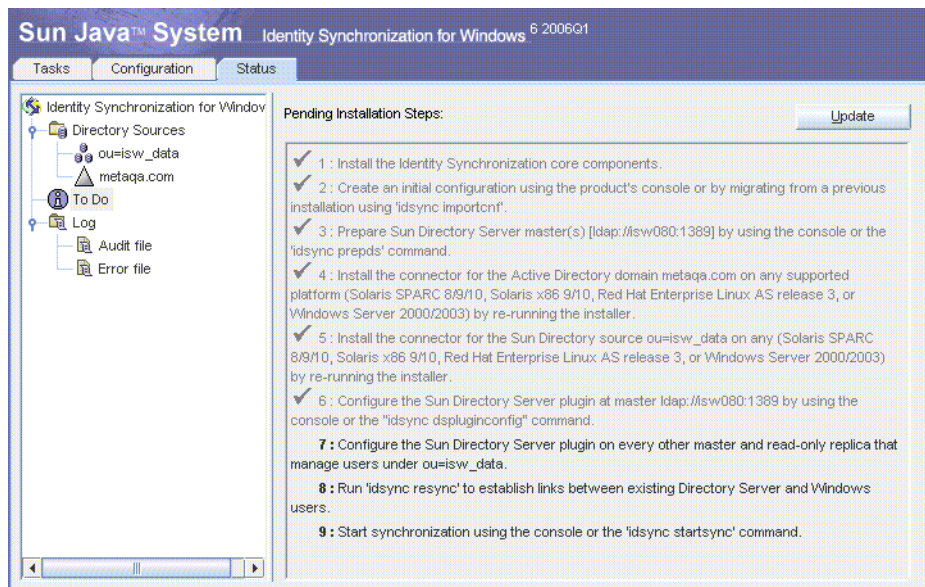
このタブの情報を更新するには、「更新」をクリックします。「状態」タブには次の情報が表示されます。

- 「状態」:ディレクトリソースの現在の状態を反映します。有効な状態は次のとおりです。
 - 「**Uninstalled**」:コネクタはインストールされていません。
 - 「**Installed**」:コネクタはインストールされていますが、実行時設定をまだ受け取っていないため、同期の準備ができていません。コネクタが1分以上この状態のままの場合は、問題が発生している可能性があります。
 - 「**Ready**」:コネクタは同期の準備ができていますが、現在どのオブジェクトとも同期していません。同期が開始されていない場合や、同期が開始されたがすべてのサブコンポーネントがコネクタとの接続を確立していない場合、コネクタは「Ready」状態のままになります。
 - 「**Syncing**」:コネクタはオブジェクトと同期中です。変更が同期していないと気付いた場合は、エラーの場合があるため、エラーログを確認してください。
- 「**Active**」:ディレクトリソースがアクティブかダウンしているかを示します。
- 「**前回の通信**」:このディレクトリソースのコネクタからの最後の応答の時間を示します。

インストール状態と設定状態の表示

▼ インストールと設定のプロセスの残りの手順を表示する

- 1 **Identity Synchronization for Windows** コンソールから「状態」タブを選択します。
- 2 ナビゲーションツリー区画で「**To Do**」ノードを展開します。
インストールと設定の手順のチェックリストを表示するように「状態」タブの内容が変わります(たとえば、276 ページの「ディレクトリソースの状態の表示」を参照)。

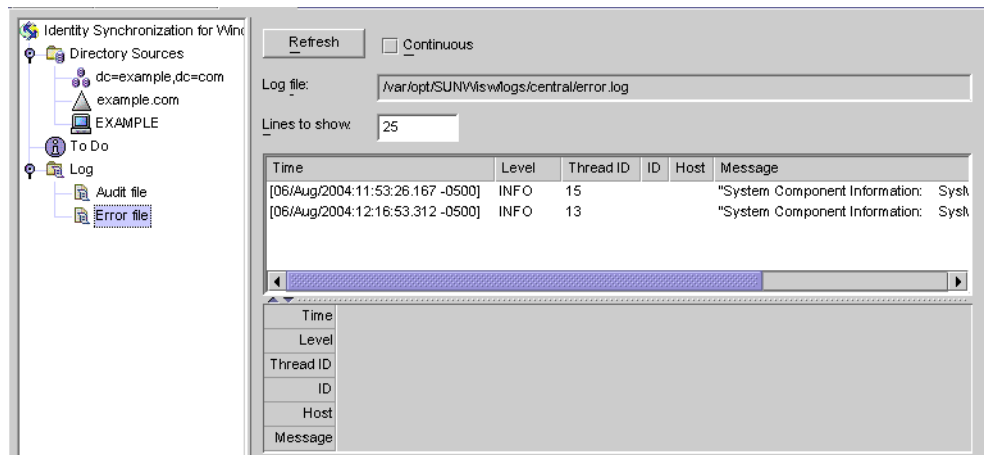


- 3 右上の「更新」ボタンをクリックしてリストを更新します。
手順を完了すると、チェックマークが付き、グレー表示されます。インストールと設定のプロセスを正常に完了するには、残りの手順を完了してください。

監査ログとエラーログの表示

▼ エラーログを表示する

- 1 **Identity Synchronization for Windows** コンソールから「状態」タブを選択します。
- 2 ナビゲーションツリー区画で「監査ファイル」ノードまたは「エラーファイル」ノードを展開します。
「状態」タブの内容が変わり、現在のログが表示されます。



「更新」をクリックして最新の監査またはエラー情報をロードします。

「状態」タブには次の情報が表示されます。

- 「継続」:常に最新の監査およびエラーの情報を更新して表示します。
- 「ログファイル」:読み取られる監査またはエラーのログのフルパス名を表示します。次に例を示します。

C:\Program Files\Sun\MPS\ismw-hostname\logs\central\audit.log

- 「表示する行」:表示する監査またはエラーのエントリ数を指定します。(デフォルトは25。)

Windows NT マシンでの監査の有効化

配備内に Windows NT マシンがある場合は、監査が有効になっているかを確認します。有効になっていないと、Identity Synchronization for Windows はそのマシンからのメッセージをログ記録できません。

▼ Windows NT マシンで監査ログを有効にする

- 1 Windows NT の「スタート」メニューから「プログラム」、「管理ツール」、「ドメインユーザーマネージャ」の順に選択します。
- 2 「ユーザーマネージャ」ダイアログボックスが表示されたら、メニューバーから「ポリシー」、「監査」の順に選択します。
「監査ポリシー」ダイアログボックスが表示されます。
- 3 「監査するイベント」ボタンを有効にしてから、「成功」ボックスと「失敗」ボックスを有効にします。
- 4 「OK」をクリックしてダイアログボックスを閉じます。
これらの設定は再度変更するまで有効のままです。

（ パート III

Identity Synchronization for Windows 付録

Identity Synchronization for Windows コマンド行ユーティリティーの使用

Identity Synchronization for Windows では、コマンド行からさまざまなタスクを実行できます。この付録では、Identity Synchronization for Windows コマンド行ユーティリティーを使用してさまざまなタスクを実行する方法について説明します。この節は次の項目から構成されています。

- 283 ページの「共通機能」
- 286 ページの「idsync コマンドの使用」
- 302 ページの「forcepwchg 移行ユーティリティーの使用」

共通機能

Identity Synchronization for Windows コマンド行ユーティリティーは次の機能を共有します。

- 283 ページの「Idsync サブコマンドに共通の引数」
- 286 ページの「パスワードの入力」
- 286 ページの「ヘルプの使用」

Idsync サブコマンドに共通の引数

この節では、ほとんどのコマンド行ユーティリティーに共通の引数(オプション)について説明します。情報を次の表にまとめます。

- Idsync サブコマンドに共通の引数 `idsync` サブコマンド (`preps` を除く) すべてと移行ツールに共通の次の引数について説明します。

```
-D bind-DN -w bind-password | - [-h Configuration Directory-hostname]
[-p Configuration Directory-port-no] [-s rootsuffix] [-Z] [-P cert-db-path]
[-m secmod-db-path]
```

注 - 括弧 [] はオプションの引数を示します。

Identity Synchronization for Windows インストールプログラムは、インストール中に指定した情報に基づいて自動的にデフォルト値を `-h`、`-p`、`-D`、および `-s` 引数に書き込みます。ただし、コマンド行に別の値を指定すると、デフォルト値をオーバーライドできます。

複数バイト文字をサポートするために、Identity Synchronization for Windows は、コマンド行インタフェース (CLI) 環境ファイルの `-s rootsuffix` と `-D bind-DN` のデフォルト値を base64 で符号化します。rootsuffix のデフォルトは変更しないようにしてください。バインド DN のデフォルトは、コマンド行でオーバーライドするか、CLI 環境ファイル内の適切な base64 で符号化された値で更新できます。

- SSL を使用して設定 Directory Server にアクセスするための共通の引数: Secure Socket Layer (SSL) を使用した設定 Directory Server への安全なアクセスについての情報を提供するオプションの引数について説明します。これらの引数は、すべての `idsync` サブコマンドと移行ツールにも共通です。
- 設定ディレクトリに関連する共通の引数: 設定ディレクトリに関連する引数について説明します。これらの引数は、複数の `idsync` サブコマンドと移行ツールに共通です。

表 A-1 すべてのサブコンポーネントに共通の引数

引数	説明
<code>-h Configuration Directory-hostname</code>	設定ディレクトリのホスト名を指定します。この引数は、デフォルトでコアインストール中に指定された値になります。
<code>-p Configuration Directory-port</code>	設定ディレクトリの LDAP ポート番号を指定します。
<code>-D bind-DN</code>	設定ディレクトリのバインド識別名 (DN) を指定します。この引数は、デフォルトでコアインストール中に指定された値になります。
<code>-w bind-password -</code>	設定ディレクトリのバインドパスワードを指定します。- 値はパスワードを標準入力 (STDIN) から読み取ります。
<code>-s rootsuffix</code>	設定ディレクトリのルートサフィックスを指定します。ここで、ルートサフィックスは <code>dc=example,dc=com</code> のような識別名です。この引数は、デフォルトでコアインストール中に指定された値になります。
<code>-q configuration_password -</code>	設定パスワードを指定します。- 値はパスワードが標準入力 (STDIN) から読み取られることを意味します。 この引数は、 <code>preps</code> 以外のすべてのサブコマンドに必須です。

表 A-2 すべてのサブコマンドに共通の SSL 関連の引数

引数	説明
-z	SSL がセキュリティー保護された通信の提供に使用されるよう指定します。コマンド行インタフェースまたは優先/副 Directory Server にアクセスする設定ディレクトリに接続するときに、証明書ベースのクライアント認証を提供します。
-P <i>cert-db-path</i>	<p>クライアントの証明書データベースのパスとファイル名を指定します。</p> <p>この証明書データベースには、Directory Server の証明書データベースの署名に使用する CA 証明書が含まれている必要があります。</p> <p>-z を指定するが、-P を使用しない場合、<i>cert-db-path</i> はデフォルトで <i>current-working-directory/cert8.db</i> になります。</p> <p>注: 指定されたディレクトリで Identity Synchronization for Windows が証明書データベースファイルを見つけられない場合、プログラムは次の 3 つのファイルで構成された「空白」のデータベースをそのディレクトリに作成します。 <i>cert8.db</i>、<i>key3.db</i>、および <i>secmod.db</i>。</p>
-m <i>secmod-db-path</i>	<p>セキュリティーモジュールデータベースへのパスを指定します。次に例を示します。</p> <p><i>/var/Sun/MPS/slapd-serverID/secmod.db</i></p> <p>セキュリティーモジュールデータベースが証明書データベースとは別のディレクトリにある場合にのみこの引数を指定します。</p>

表 A-3 設定ディレクトリの引数

引数	説明
-a <i>ldap_filter</i> <i>forcepwchg</i> および <i>resync</i> サブコマンドと共に使用します。	ユーザーをソース SUL から取得する場合に使用する LDAP フィルタを指定し、ユーザーが指定された SUL 内にあるかどうかを判断する前に、焦点のユーザーのサブセットを処理がディレクトリソースから取得できるようにします。
-f <i>filename</i> <i>export10cnf</i> 、 <i>importcnf</i> 、および <i>resync</i> サブコマンドと共に使用します。	設定 XML ドキュメントファイルの名前を指定します。
-n <i>forcepwchg</i> 、 <i>importcnf</i> 、および <i>resetconn</i> サブコマンドと共に使用します。	実際の変更を行わずに操作の影響をプレビューできるようにセーフモードで実行します。

パスワードの入力

パスワード引数 (`-w bind-password` または `-q configuration_password` など) が必要な場合は常に、「-」引数を使用してパスワードプログラムに STDIN からパスワードを読み取るよう通知できます。

「-」値を複数のパスワードオプションに使用すると、引数の順序に基づいて `idsync` によってパスワードが求められます。

この場合、プログラムは `bind-password` が最初で `configuration-password` が次であることを期待します。

ヘルプの使用

次のコマンドの1つを使用して、`idsync` またはそのサブコマンドの使用情報をコマンドコンソールに表示できます。

- `-help`
- `--help`
- `-?`

使用情報の表示方法

- `idsync` (有効なサブコマンドのリストを含む) については、コマンドプロンプトに前述のヘルプオプションの1つを入力して改行キーを押します。
- サブコマンドについては、コマンドプロンプトでサブコマンドのあとにヘルプオプションを入力して改行キーを押します。

idsync コマンドの使用

`idsync` コマンドとサブコマンドを使用して Identity Synchronization for Windows コマンド行ユーティリティを実行します。

注 - `idsync` コマンドは、引数を Directory Server に送信する前に、すべての DN 値引数 (バインド DN やサフィックス名など) をそのウィンドウに対して指定された文字セットから UTF-8 に変換します。

サフィックス名にエスケープ文字として円記号を使用しないでください。

UTF-8 文字を Solaris 上と Linux 上で指定するには、端末ウィンドウに UTF-8 に基づいたロケールが必要です。環境変数の `LC_CTYPE` と `LANG.are` を正しく設定する必要があります。

特に別途記載されていないかぎり、次のいずれかの方法でサブコマンドとともに `idsync` コマンドを実行できます。

■ **Solaris** の場合:

1. 端末ウィンドウを開いて `cd` と入力して `/opt/SUNWisw/bin` ディレクトリに移動します。
2. 次のようにサブコマンドを1つ付けて `idsync` コマンドを実行します。

`idsync subcommand`

■ **Linux** の場合:

1. 端末ウィンドウを開いて `cd` と入力して `/opt/sun/isw/bin` ディレクトリに移動します。
2. 次のようにサブコマンドを1つ付けて `idsync` コマンドを実行します。

`idsync subcommand`

■ **Windows** の場合:

1. コマンドウィンドウを開き、`cd` と入力して `install_path\isw-hostname\bin` ディレクトリに移動します。
2. 次のようにサブコマンドを1つ付けて `idsync` コマンドを実行します。

`idsync subcommand`

286 ページの「[idsync コマンドの使用](#)」に `idsync` ユーティリティのサブコマンドとその目的をすべてリストします。

表A-4 idsync サブコマンドのクイックリファレンス

サブコマンド	目的
<code>certinfo</code>	設定と SSL 設定に基づいて証明書情報を表示します (288 ページの「 certinfo の使用 」を参照)
<code>changepw</code>	Identity Synchronization for Windows 設定パスワードを変更します (289 ページの「 changepw の使用 」を参照)
<code>importcnf</code>	エクスポートした Identity Synchronization for Windows バージョン 1.0 設定 XML ドキュメントをインポートします (290 ページの「 importcnf の使用 」を参照)
<code>prepds</code>	Identity Synchronization for Windows で使用するよう Sun Java System Directory Server ソースを準備します (291 ページの「 prepds の使用 」参照)
<code>printstat</code>	インストール/設定プロセスを完了するために必要な手順のリストを表示します。また、インストールされたコネクタ、システムマネージャー、および Message Queue の状態も表示します (294 ページの「 printstat の使用 」を参照)
<code>resetconn</code>	設定ディレクトリのコネクタの状態をアンインストール済みにもリセットします (295 ページの「 resetconn の使用 」を参照)

表 A-4 idsync サブコマンドのクイックリファレンス (続き)

サブコマンド	目的
resync	インストールプロセスの一環として、既存のユーザーまたはグループをリンクおよび再同期したり、ディレクトリを事前に生成したりします (296 ページの「resync の使用」を参照)
groupsync	あるディレクトリソースから別のディレクトリソースへのユーザーとグループ間のグループ情報を同期します (299 ページの「groupsync の使用」を参照)
accountlockout	Directory Server と Active Directory ソース間のアカウントロックアウトとロックアウト解除を同期します (299 ページの「accountlockout の使用」を参照)
dspluginconfig	指定されたホスト上でディレクトリサーバープラグインを設定および設定解除します (300 ページの「dspluginconfig の使用」を参照)
startsync	同期を開始します (300 ページの「startsync の使用」を参照)
stopsync	同期を停止します (301 ページの「stopsync の使用」を参照)

certinfo の使用

certinfo サブコマンドを使用して設定と SSL 設定に基づいて証明書情報を表示できます。この情報は、各コネクタおよび/またはディレクトリサーバープラグインの証明書データベースに追加する必要のある証明書の決定に役立ちます。

証明書情報を表示するには、端末ウィンドウ(またはコマンドウィンドウ)を開いて、次のように **idsync certinfo** コマンドを入力します。

```
idsync certinfo [bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z]
[-P cert-db-path] [-m secmod-db-path]
```

注 - certinfo サブコマンドはコネクタおよび Directory Server の証明書データベースへアクセスできないため、リストされている必要な一部の手順はすでに実行されている場合があります。

次に例を示します。

```
idsync certinfo -w admin-password -q configuration-password
```

注 - certinfo 引数の詳細については、283 ページの「Idsync サブコマンドに共通の引数」を参照してください。

changepw の使用

changepw サブコマンドを使用して Identity Synchronization for Windows 設定パスワードを変更できます。

▼ Identity Synchronization for Windows の設定パスワードを変更する

- 1 Identity Synchronization for Windows プロセス(システムマネージャー、セントラルロガー、コネクタ、コンソール、インストーラ/アンインストーラなど)をすべて停止します。
- 2 プロセスをすべて停止したあと、設定ディレクトリを ldif にエクスポートして、ou=Services ツリーをバックアップします。
- 3 次のように **idsync changepw** コマンドを入力します。

```
idsync changepw [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password
[-Z] [-P cert-db-path] [-m secmod-db-path]
-b new password | - [-y]次に例を示します。
```

```
idsync changepw -w admin password -q old config password -b -q new config password
```

次の引数は、changepw に固有です。

引数	説明
-b <i>password</i>	新しい設定パスワードを指定します。- 値はパスワードを標準入力 (STDIN) から読み取ります。
[-y]	コマンドの確認を求めるプロンプトメッセージを出力しません。

- 4 端末ウィンドウに表示されるメッセージに応答します。次にその例を示します。

本当に設定パスワードの変更を行いますか (y/n)? yes

システムを再起動する前に -

\$PSWHOME/resources/SystemManagerBootParams.cfg ファイルを編集で、
「deploymentPassword」の値を変更します。

成功

- システムを再起動する前に、SystemManagerBootParams.cfg ファイルを変更してください。
 \$PSWHOME\resources (ここで \$PSWHOME は *isw-installation* ディレクトリ) 内の SystemManagerBootParams.cfg ファイルには、システムマネージャーが設定ディレクトリへの接続に使用する設定パスワードが含まれます。
 たとえば、次のようにパスワードを変更できます。
 変更前: `Parameter name="manager.configReg.deploymentPassword" value="oldpassword"/`
 変更後: `Parameter name="manager.configReg.deploymentPassword" value="newpassword"/`
- プログラムがエラーを報告した場合は、289 ページの「[changepw の使用](#)」の `ldif` を使用して設定ディレクトリを復元し、再試行してください。エラーのもっとも一般的な理由は、設定ディレクトリをホストしている **Directory Server** がパスワードの変更中に使用できなくなることです。

importcnf の使用

コア (第 5 章「コアのインストール」) をインストールしたあと、`idsync importcnf` サブコマンドを使用して、コア設定情報を含むエクスポートされた Identity Synchronization for Windows バージョン 1.0 または 1.1 (SP1) 設定 XML ファイルをインポートします。

バージョン 1.0 の設定 XML ファイルをインポートするには、端末ウィンドウ (またはコマンドウィンドウ) を開いて、**idsync importcnf** コマンドを次のように入力します。

```
idsync importcnf [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z] [-P cert-db-path]
[-m secmod-db-path] -f filename [-n]
```

次に例を示します。

```
idsync importcnf -w admin_password -q configuration_password -f "MyConfig.cfg"
```

次の引数は `importcnf` に固有です。

表 A-5 `idsync importcnf` の引数

引数	説明
<code>-f filename</code>	設定 XML ドキュメントの名前を指定します。

表 A-5 idsync importcnf の引数 (続き)

引数	説明
-n	実際の変更を行わずに操作の影響をプレビューできるようにセーフモードで実行します。

注 - その他の `importcnf` 引数の詳細については、283 ページの「[Idsync サブコマンドに共通の引数](#)」を参照してください。

バージョン 1.0 の設定 XML ファイルをインポートしたあと、同期するために `prepds` をすべての Directory Server ソース上で実行します (291 ページの「[prepds の使用](#)」のコネクタとサブコンポーネントを参照)。

prepds の使用

コンソールまたは `prepds` サブコマンドを使用して Identity Synchronization for Windows が使用する Sun Java System Directory Server ソースを準備します。ディレクトリサーバーコネクタをインストールする前に、`prepds` を実行してください。

`idsync prepds` サブコマンドを実行すると、適切な ACI が `cn=changelog` エントリに提供されます。このエントリは旧バージョン形式の変更ログデータベースのルートノードです。

Identity Synchronization for Windows が使用する 優先マスター Directory Server を準備する場合は、ディレクトリマネージャー 証明書を指定します。

ディレクトリマネージャーユーザーは、Directory Server インスタンスのあらゆる場所へのフルアクセス権を持つ Directory Server の特別なユーザーです。ACI はディレクトリマネージャーユーザーには適用されません。

たとえば、ディレクトリマネージャーのみが旧バージョン形式の変更ログデータベースへのアクセス制御を設定できます。これが、優先マスターサーバーに対して Identity Synchronization for Windows がディレクトリマネージャーの証明書を必要とする理由の 1 つです。

注 - 優先 Sun ディレクトリソースの旧バージョン形式の更新履歴ログデータベースを再作成する場合、デフォルトのアクセス制御設定が適用されるとディレクトリサーバーコネクタはデータベースの内容を読み込みません。

旧バージョン形式の変更ログデータベースのアクセス制御設定を復元するには、`idsync prepds` を実行するか、またはコンソールで適切な Sun ディレクトリソースを選択して「Directory Server の準備」ボタンをクリックします。

指定した時間のあと、変更ログのエントリを自動的に削除する(または切り取る)ようシステムを設定できます。コマンド行から `cn=Retro ChangeLog Plug-in`, `cn=plugins`, `cn=config` の `nsslapd-changelogmaxage` 設定属性を変更します。

`nsslapd-changelogmaxage`: *IntegerTimeunit*

引数の意味はそれぞれ次のとおりです。

- **Integer** は数字です。
- **Timeunit** は、秒の場合は `s`、分の場合は `m`、時間の場合は `h`、日の場合は `d`、週の場合は `w` です。Integer 変数と Timeunit 変数の間には空白を挿入しません。
たとえば、`nsslapd-changelogmaxage: 2d` のようになります。
詳細は、『Sun Java System Directory Server 5 2004Q2 管理ガイド』の「レプリケーションの管理」の章を参照してください。
- 管理資格を使用して副サーバーを準備できます。

使用するホストとサフィックスを知る必要があるため、`idsync prepds` を実行する前に必ず Identity Synchronization for Windows 設定を計画してください。

ディレクトリサーバーコネクタとプラグインがすでにインストール、設定、同期されている Directory Server のサフィックスで `idsync prepds` を実行すると、ディレクトリサーバーコネクタをインストールするかどうか尋ねるメッセージが表示されません。このメッセージは無視してください。

Sun Java System Directory Server ソースを準備するには、端末ウィンドウ(またはコマンドウィンドウ)を開いて、次のように **idsync prepds** コマンドを入力します。

単一ホストの場合:

```
idsync prepds [-h <hostname>] [-p <port>] [-D <Directory Manager DN>] -w <password>  
-s <database suffix> [-x] [-Z] [-P <cert db path>] [-m <secmod db path>]
```

複数ホストの場合:

```
idsync prepds -F <filename of Host info> -s <root suffix> [-x] [-Z]  
[-P <cert db path>] [-m <secmod db path>] [-3]
```

次に例を示します。

```
isw-hostname\bin>idsync prepds -F isw-hostname\samples\Hosts.xml \
-s ou=isw_data
```

注 -prepds サブコマンドの場合のみ、次の表で説明するように -h、-p、-D、-w、および -s 引数が再定義されています。さらに、-q 引数は該当しません。

291 ページの「[prepds の使用](#)」では、idsync prepds に固有の引数について説明します。

表 A-6 prepds の引数

引数	説明
-h <i>name</i>	優先ホストとして機能する Directory Server インスタンスの DNS 名を指定します。
-p <i>port</i>	優先ホストとして機能する Directory Server インスタンスのポート番号を指定します。(デフォルトは 389。)
-j <i>name</i> (オプション)	副ホストとして機能する Directory Server インスタンスの DNS 名を指定します (Sun Java System Directory Server 5 2004Q2 マルチマスターレプリケーション (MMR) 環境に該当)。
-r <i>port</i> (オプション)	副ホストとして機能する Directory Server のポートを指定します (Sun Java System Directory Server 5 2004Q2 マルチマスターレプリケーション (MMR) 環境に該当)。(デフォルトは 389。)
-D <i>dn</i>	優先ホストのディレクトリマネージャーユーザーの識別名を指定します。
-w <i>password</i>	優先ホストのディレクトリマネージャーユーザーのパスワードを指定します。-値はパスワードを標準入力 (STDIN) から読み取ります。
-E <i>admin-DN</i>	副ホストのディレクトリマネージャーユーザーの識別名を指定します。
-u <i>password</i>	副ホストのディレクトリマネージャーユーザーのパスワードを指定します。-値はパスワードを標準入力 (STDIN) から読み取ります。
-s <i>rootsuffix</i>	インデックスの追加に使用するルートサフィックス (ユーザーを同期するルートサフィックス) を指定します。 注: 優先および副ホストのデータベース名は変わることがありますが、サフィックスは変わりません。このため、プログラムは各ホストのデータベース名を見つけて、それをインデックスの追加に使用できます。
-x	dspswuserlink 属性の等価インデックスおよびプレゼンスインデックスをデータベースに追加しません。
-F <i>filename of Host info</i>	複数ホスト環境の場合、ホスト情報を含むファイル名を指定します。

(たとえば、優先マスター、副マスター、および2つのコンシューマのある)レプリケートされた環境で `idsync prepds` を実行している場合、優先マスターと副マスターに対して `idsync prepds` を1度だけ実行します。

▼ idsync prepds を実行する

- 1 **Directory Server** のレプリケーションが起動し、実行されていることと確認します (該当する場合)。
- 2 次のように、コンソールまたはコマンド行から `idsync prepds` を実行します。

```
idsync prepds -h M1.example.com -p 389 -j M2.example.com -r 389.
```

M1 上で `idsync prepds` コマンドを実行すると、次の処理を行うことができます。

- RCL を有効化および拡張してより多くの属性を取得する (`dspswuserlink` など)。RCL は M1 上でのみ必要です。
- スキーマを拡張する。
- ACI で `uid=pswconnector, suffix user` を追加する。
- インデックス指定が完了するまで **Directory Server** を一時的に読み取り専用モードにする `dspswuserlink` 属性にインデックスを追加する。
停止時間を避けるためにインデックスは後で追加することができますが、ディレクトリサーバーコネクタをインストールする前にインデックスを追加する必要があります。

M2 にインデックスを追加する。

注-

- レプリケーションによって **Identity Synchronization for Windows** がスキーマ情報と `uid=pswconnector` を優先マスターから副マスターと2つのコンシューマに確実にコピーします。
- ディレクトリサーバーコネクタを1度インストールしてください。ディレクトリサーバープラグインはすべてのディレクトリにインストールします。
- インデックス指定は、優先マスターと副マスターでのみ必要です。レプリケーションはインデックス指定設定を優先マスターから副マスターに転送しません。

printstat の使用

`printstat` サブコンポーネントを使用して次を実行できます。

- インストールと設定のプロセスを完了するために実行する必要がある残りの手順のリストを表示する。

- インストールしたコネクタ、システムマネージャー、および Message Queue の状態を印刷する。

可能な状態設定は次のとおりです。

- 「**Uninstalled**」:コネクタはインストールされていません。
- 「**Installed**」:コネクタはインストールされていますが、実行時設定をまだ受け取っていないため、同期の準備ができていません。
- 「**Ready**」:コネクタは同期の準備ができていますが、まだどのオブジェクトとも同期していません。
- 「**Syncing**」:コネクタはオブジェクトと同期中です。

インストール済みのコネクタ、システムマネージャー、Message Queue の状態を印刷するには、端末ウィンドウ(またはコマンドウィンドウ)を開き、次のように **idsync printstat** コマンドを入力します。

```
idsync printstat [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z]
[-P cert-db-path] [-m secmod-db-path]
```

次に例を示します。

```
idsync printstat -w admin password -q configuration password
```

resetconn の使用

resetconn サブコマンドを使用して、設定ディレクトリのコネクタの状態をアンインストール済みにリセットできます。たとえば、ハードウェアの障害によってコネクタをアンインストールできない場合、resetconn を使用してコネクタの状態をアンインストール済みに変更すると、そのコネクタを再インストールできます。

注 - resetconn サブコマンドは、ハードウェアやアンインストーラの障害時にのみ使用することを目的としています。

コマンド行からコネクタの状態をリセットするには、端末ウィンドウ(またはコマンドウィンドウ)を開いて、次のように **idsync resetconn** コマンドを入力します。

```
idsync resetconn [-D bind-DN] -w bind-password\> | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z] [-P cert-db-path]
[-m secmod-db-path] -e directory-source-name [-n]
```

次に例を示します。

```
idsync resetconn -w admin password -q configuration_password -e "dc=example,dc=com"
```

291 ページの「[preps の使用](#)」では、resetconn に固有の引数について説明します。

表 A-7 idsync resetconn の引数

引数	説明
-e <i>dir-source</i>	リセットするディレクトリソースの名前を指定します。
-n	実際の変更を行わずに操作の影響をプレビューできるようにセーフモードで実行します。

注 - idsync printstat を使用してディレクトリソースの名前を見つけることができます。

その他の resetconn 引数の詳細については、283 ページの「[Idsync サブコマンドに共通の引数](#)」を参照してください。

resync の使用

resync サブコマンドを使用して既存のユーザーで配備をブートストラップできます。このコマンドは、管理者が指定したマッチングルールを使用して、次を実行します。

- 既存のエントリをリンクする
- 空のディレクトリにリモートディレクトリの内容を生成する
- 2つの既存のユーザー入力間で属性値を一括同期する
- (グループ同期機能を有効な場合) 既存のグループとグループに関連付けられたユーザーを一括同期する

注 - ユーザーのリンクと同期の詳細については、第3章「[製品の理解](#)」を参照してください。

既存のユーザーを再同期してディレクトリに事前に生成するには、端末ウィンドウ (またはコマンドウィンドウ) を開いて次のように **idsync resync** コマンドを入力します。

```
idsync resync [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z] [-P cert-db-path]
[-m secmod-db-path] [-n] [-f xml filename for linking] [-k] [-a ldap-filter]
```



```
[ -l sul-to-sync ] [ -o Sun | Windows ] [ -c ] [ -x ]
[ -u ] [ -i ALL_USERS | NEW_USERS | NEW_LINKED_USERS ]
```

次に例を示します。

```
idsync resync -w admin password -q configuration_password
```

296 ページの「[resync の使用](#)」では、resync に固有の引数について説明します。

表 A-8 idsync resync の使用

引数	意味
-f <i>filename</i>	Identity Synchronization for Windows によって提供される指定された XML 設定ファイルの 1 つを使用して、リンクされていないユーザー エントリ間にリンクを作成します (付録 B 「 Identity Synchronization for Windows LinkUsers XML ドキュメントの例 」を参照)。
-k	リンクしていないユーザー間にリンクを作成するだけです (ユーザーを作成したり、既存のユーザーを変更したりすることはない)。
-a <i>ldap-filter</i>	同期するエントリを制限するための LDAP フィルタを指定します。フィルタは、再同期動作のソースに適用されます。たとえば、idsync resync -o Sun -a "uid=*" を指定すると、uid 属性を持つすべての Directory Server ユーザーが Active Directory と同期します。
-l <i>sul-to-sync</i>	再同期する個別の同期ユーザーリスト (SUL) を指定します。 注: 複数の SUL ID を指定して複数の SUL を再同期できます。SUL ID を指定しない場合は、使用している SUL のすべてが再同期されません。
-o (Sun Windows)	再同期動作のソースを指定します。 <ul style="list-style-type: none"> ■ Sun: Windows エントリの属性値を Sun Java System Directory Server のディレクトリソースエントリの対応する属性値に設定します。 ■ Windows: Sun Java System Directory Server エントリの属性値を Windows ディレクトリソースエントリの対応する属性値に設定します。 (デフォルトは <i>Windows</i>)
-c	対応するユーザーが宛先で見つからない場合にユーザーエントリを自動的に作成します。 <ul style="list-style-type: none"> ■ Active Directory または Windows NT で作成されたユーザーに対してランダムにパスワードを生成します。 ■ Directory Server で作成したユーザーに対して特別なパスワード値 ((PSWSYNC) *INVALID PASSWORD*) を自動的に作成します (-i オプションを指定しないかぎり)。

表 A-8 idsync resync の使用 (続き)

引数	意味
-i (ALL_USERS NEW_USERS NEW_LINKED_USERS)	<p>Sun ディレクトリソースで同期するユーザーエントリのパスワードをリセットし、次にユーザーパスワードが必要なときに、これらのユーザーに対して現在のドメイン内でのパスワード同期を実行します。</p> <ul style="list-style-type: none"> ■ ALL_USERS: 同期されたすべてのユーザーに対してオンデマンドパスワード同期が実行されます。 ■ NEW_USERS: 新しく作成されたユーザーのみに対してオンデマンドパスワード同期が実行されます。 ■ NEW_LINKED_USERS: 新しく作成されたユーザーと新しくリンクされたユーザーすべてに対してオンデマンドパスワード同期が実行されます。
-u	<p>オブジェクトキャッシュを更新するだけです。エントリは変更しません。</p> <p>この引数は、Windows ディレクトリソースのユーザーエントリのローカルキャッシュのみを更新します。これによって、既存の Windows ユーザーが Directory Server で作成されるのを防ぎます。この引数を使用する場合、Windows ユーザーエントリは Directory Server ユーザーエントリと同期されません。この引数は、再同期ソースが Windows の場合のみ有効です。</p>
-x	<p>ソースエントリに一致しないすべての宛先ユーザーエントリを削除します。</p>
-n	<p>実際の変更を行わずに操作の影響をプレビューできるようにセーフモードで実行します。</p>

注-

- 使用状態を表示するには、引数なしで `idsync resync` を実行します。
- `resync` 引数の詳細については、283 ページの「[Idsync サブコマンドに共通の引数](#)」を参照してください。
- 既存のユーザーの再同期については、第 3 章「[製品の理解](#)」を参照してください。

`resync` を実行したあと、セントラル audit log の `resync.log` ファイルを確認します。エラー結果の場合は、『[Sun Java System Directory Server Enterprise Edition 6.3 トラブルシューティングガイド](#)』の第 7 章「[Identity Synchronization for Windows のトラブルシューティング](#)」を参照してください。

groupsync の使用

groupsync サブコマンドを使用して Active Directory と Directory Server 間でグループを同期できます。

グループの同期を有効または無効にするには、**idsync groupsync** コマンドを入力します。

次に例を示します。

```
idsync groupsync -{e/d} -D <bind DN> -w <bind password> [-h <CD hostname>]  
[-p <CD port no>] -s <rootsuffix> [-Z] -q <configuration password> -t <AD group type>
```

表 A-9 groupsync の引数

引数	意味
<i>-{e/d}</i>	グループの同期を有効にする場合は e、無効にする場合は d を選択します。
<i>-t</i>	Active Directory でグループタイプを指定します。たとえば、「distribution」または「security」のいずれかを選択できます。

accountlockout の使用

accountlockout サブコマンドを使用して Active Directory と Directory Server 間のアカウントのロックアウトとロックアウト解除を同期できます。

アカウントのロックアウトを有効または無効にするには、**idsync accountlockout** コマンドを入力します。

次に例を示します。

```
idsync accountlockout -{e/d} -D <Directory Manager DN> -w <bind-password>  
-h <Configuration Directory-hostname> -p <Configuration Directory-port-no>  
-s <rootsuffix> [-Z] [-P <cert db path>] [-m <secmod db path>]  
-q <configuration password> -t <max lockout attempts>
```

表 A-10 accountlockout の引数

引数	意味
<i>-{e/d}</i>	アカウントロックアウトの同期を有効にする場合は e、無効にする場合は d を選択します。

表 A-10 accountlockout の引数 (続き)

引数	意味
-t	Active Directory コネクタが実行するロックアウトの最大試行回数を指定します。

dspluginconfig の使用

dspluginconfig サブコマンドを使用して、指定された Directory Server データソースでディレクトリサーバープラグインを設定または設定解除できます。

ディレクトリサーバープラグインを設定または設定解除するには、**idsync dspluginconfig** コマンドを入力します。

次に例を示します。

```
idsync dspluginconfig -{C/U} -D <bind DN> -w <bind password | ->
[-h <CD hostname>] [-p <CD port no>] [-s <configuration suffix>]
[-Z] [-P <cert db path>] [-m <secmod db path> ] [-d <ds plugin hostname>]
[-r <ds plugin port>] [-u <ds plugin user>] [-x <ds plugin user password>]
[-o <database suffix>] [-q <configuration password | ->]
```

表 A-11 dspluginconfig の引数

引数	意味
-{C/U}	ディレクトリサーバープラグインを設定する場合はC、設定解除する場合はUを選択します。
-d	プラグインを設定する必要がある Directory Server データソースのホスト名
-r	プラグインを設定する必要がある Directory Server データソースのポート番号
-u	プラグインを設定する必要がある Directory Server データソースの管理者
-x	プラグインを設定する必要がある Directory Server データソースの管理者のパスワード
-o	Directory Server データソースのデータサフィックス。

startsync の使用

startsync サブコマンドを使用して、コマンド行から同期を開始できます。

同期を開始するには、端末ウィンドウ (またはコマンドウィンドウ) を開いて、次のように **idsync startsync** コマンドを入力します。

```
idsync startsync [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z]
[-P cert-db-path] [-m secmod-db-path]
```

次に例を示します。

```
idsync startsync -w admin password -q configuration_password
```

300 ページの「startsync の使用」では、startsync に固有の引数について説明します。

表 A-12 idsync startsync の引数

引数	説明
[-y]	コマンドの確認を求めるプロンプトメッセージを出力しません。

注 - その他の startsync 引数の詳細については、283 ページの「Idsync サブコマンドに共通の引数」を参照してください。

stopsync の使用

stopsync サブコマンドを使用して、コマンド行から同期を停止できます。

同期を停止するには、端末ウィンドウ (またはコマンドウィンドウ) を開いて、次のように **idsync stopsync** コマンドを入力します。

```
idsync stopsync [-D bind-DN] -w bind-password | -
[-h Configuration Directory-hostname] [-p Configuration Directory-port-no]
[-s rootsuffix] -q configuration_password [-Z]
[-P cert-db-path] [-m secmod-db-path]
```

次に例を示します。

```
idsync stopsync -w admin password -q configuration_password
```

注 - stopsync 引数の詳細については、283 ページの「Idsync サブコマンドに共通の引数」を参照してください。

forcepwchg 移行ユーティリティーの使用

移行中にパスワードを変更したユーザーは、Windows NT および Directory Server で別のパスワードを持つこととなります。forcepwchg ユーティリティーを使用して、Identity Synchronization for Windows バージョン 1.0 からバージョン 6.0 への移行プロセス中にパスワードを変更したユーザーにパスワードの変更を求めることができます。

注 - forcepwchg ユーティリティーは Windows パッケージにのみ付属しています。

forcepwchg を使用する前に、次を確認する必要があります。

- userpassword 属性に 7 ビット値を強制するための、Directory Server の 7 ビットチェックプラグインの設定を必ず解除してください。これには、Directory Server のコンソールを使用します。
- 認証に使用しているクライアントが値を使用しているロケールから UTF-8 に正しく変換する必要があります。(たとえば、Directory Server に付属の ldapsearch の -i オプション)。

▼ forcepwchg コマンド行ユーティリティーを実行する

- 1 コマンドプロンプトウィンドウを開いて、移行を実行しているホスト上の **Windows migration** ディレクトリに移動します。コネクタ、変更検出機能 **DLL**、パスワードフィルタ **DLL** のような **Identity Synchronization for Windows 1.0 NT** コンポーネントを PDC ホストにインストールしてください。
- 2 migration ディレクトリから次のように入力します。

```
java -jar forcepwchg.jar [-n] [-a] [-t <time_specification>]
```

次に例を示します。

```
forcepwchg.jar -n -a forcepwchg.jar -t 33m
```

302 ページの「[forcepwchg 移行ユーティリティーの使用](#)」では、forcepwchg に固有の引数について説明します。

オプション	説明
-n	プレビューモードを指定します。プレビューモードでユーティリティは、次を除く通常のユーザーすべての名前を表示します。 <ul style="list-style-type: none">■ -a 引数を指定した場合の組み込みアカウント(管理者とゲスト)■ -t 引数を使用して指定された期間にパスワードを変更したユーザープレビューモードでユーザーは forcepwchg を実行できます。プレビューモード以外では、管理者のみが forcepwchg を実行できます。
-a	(管理者とゲストを除く)すべてのユーザーにパスワードの変更を要求します。-t 引数を使用している場合は、この引数を使用できません。
-t <i>time_specification</i>	過去の <i>time_specification</i> の間にパスワードを変更したすべてのユーザーにパスワードの変更を強制します。ここで、 <i>time_specification</i> は次の形式にできます。 <ul style="list-style-type: none">■ <i>number</i>: 秒数 (たとえば、-t 30)■ <i>number m</i>: 分数 (たとえば、-t 25m)■ <i>number h</i>: 時間 (たとえば、-t 6h) たとえば、forcepwchg -t 6h と指定した場合、過去 6 時間以内にパスワードを変更したすべてのユーザーがパスワードを再度変更する必要があります。
-?	使用方法についての情報を表示します。

Identity Synchronization for Windows LinkUsers XML ドキュメントの例

この付録では、配備内の既存のユーザーをリンクする `idsync resync` サブコマンドで使用できる2つのXML設定ドキュメントの例を紹介します。

次のファイルはどちらもコアをインストールした `samples1` サブディレクトリに存在します。

- 305 ページの「例 1: `linkusers-simple.cfg`」(一般的な単純な設定の例)
- 306 ページの「例 2: `linkusers.cfg`」(リンク条件指定を最大限に活用するより複雑な設定の例)

環境に合わせて例を変更できます。両方のファイルに、複数のSULでのユーザーのリンク方法を含む、ユーザーにリンクするために例を変更する方法を説明したコメントが含まれています。

例 1: `linkusers-simple.cfg`

```
<!--  
    Copyright 2004 Sun Microsystems, Inc. All rights reserved  
    使用はライセンス契約の条件に基づきます。  
--\>  
<!--  
    この xml ファイルは、コマンド行から Windows の  
    ユーザーと Sun Directory Server のユーザーをリンク  
    させるために使用します。これは -f オプションとして  
    「idsync resync」スクリプトに渡されます。これは、  
    同じログイン名を持つ、つまり Directory Server uid  
    属性が Active Directory samaccountname 属性と一致する、  
    SUL1 同期ユーザーリストのユーザーをリンクさせる  
    単純なファイルです。さらに複雑なマッチングルールに  
    ついては、linkusers.cfg の例を参照してください。  
--\>
```

```

<UserLinkingOperationList\>
  <UserLinkingOperation parent.attr="UserLinkingOperation"
    sulid="SUL1"\>
    <UserMatchingCriteria parent.attr="UserMatchingCriteria"\>
      <AttributeMap parent.attr="AttributeMap"\>
        <AttributeDescription parent.attr="SunAttribute"
          name="uid"/\>
        <AttributeDescription parent.attr="WindowsAttribute"
          name="samaccountname"/\>
      </AttributeMap\>
    </UserMatchingCriteria\>
  </UserLinkingOperation\>
</UserLinkingOperationList\>

```

例 2: linkusers.cfg

```

<?xml version ="1.0" encoding="UTF-8"?\>
<!--
    Copyright 2004 Sun Microsystems, Inc.
    All rights reserved
    使用はライセンス契約の条件に基づきます。
--\>
<!--
    この xml ファイルは、コマンド行から Windows の
    ユーザーと Sun Directory Server のユーザーを
    リンクさせるために使用します。これは -f オプション
    として \qidsync resync\q スクリプトに渡されます。
--\>
<!--
    次のパラメータ allowLinkingOutOfScope が true の場合、
    Windows ユーザーを users\q 同期ユーザーリスト外の
    Sun Directory Server ユーザーにリンクできます。
    デフォルトは false です。
--\>
<UserLinkingOperationList allowLinkingOutOfScope="false"\>

<!--
    UserLinkingOperation はリンクする単一の SUL の
    設定をカプセル化します。これには、SUL ID と、
    一致させる属性のリストが含まれます。リンク
    させる各 SUL に対して個別の UserLinkingOperation を
    指定してください。
--\>
<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL1"\>

```

```

<!--
  UserMatchingCriteria は、リンクさせるユーザーに対して
  一致する必要がある属性のリストをカプセル化します。--\>
<!--
  この UserMatchingCriteria を使用して、2 人のユーザーを一致させる場合、
  それらのユーザーは同じ givenName と同じ sn を持っている必要があります。--\>
<UserMatchingCriteria parent.attr="UserMatchingCriteria">
  <AttributeMap parent.attr="AttributeMap">
    <AttributeDescription parent.attr="SunAttribute" name="sn"/>
    <AttributeDescription parent.attr="WindowsAttribute" name="sn"/>
  </AttributeMap> <AttributeMap parent.attr="AttributeMap">
    <AttributeDescription parent.attr="SunAttribute" name="givenName"/>
    <AttributeDescription parent.attr="WindowsAttribute"
      name="givenName"/> </AttributeMap></UserMatchingCriteria>
<!--
  単一の SUL に対して複数の UserMatchingCriteria を
  指定できます。これらは論理和として扱われます。この例では、
  リンクさせるユーザーの (givenName\qs と sn\qs が一致する
  (上記参照)) または (従業員 (Number|ID) が一致する) 必要が
  あります。指定された属性、employeeNumber は DS 属性の
  名前です。--\>
<!--
  この UserMatchingCriteria は、employeeNumber が DS のインデックスが
  作成された属性ではないためコメントアウトされています。
  UserMatchingCriteria で使用される属性すべてについて、インデックスを
  作成するようにしてください。
<UserMatchingCriteria parent.attr="UserMatchingCriteria">
  <AttributeMap parent.attr="AttributeMap">
    <AttributeDescription parent.attr=
      "SunAttribute" name="employeeNumber"/>
    <AttributeDescription parent.attr=
      "WindowsAttribute" name="employeeID"/>
  </AttributeMap>
</UserMatchingCriteria>
--\>
</UserLinkingOperation>
<!--
  複数の SUL がリンクされる場合、それぞれに対して個別の
  UserLinkingOperation が指定されます。
  ここで示すように、各 UserLinkingOperation は別の
  UserMatchingCriteria を使用できます。この例では、SUL2
  のユーザーは sn と employeeNumber が一致した場合にのみ
  リンクされます。
  注: 例の設定が単一の SUL しか持たないため、
  この UserLinkingOperation は現在コメントアウト
  されています。

```

```
<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL2"\>
  <UserMatchingCriteria parent.attr="UserMatchingCriteria"\>
    <AttributeMap parent.attr="AttributeMap"\>
      <AttributeDescription parent.attr="SunAttribute" name="sn"/>
      <AttributeDescription parent.attr="WindowsAttribute" name="sn"/>
    </AttributeMap\>
    <AttributeMap parent.attr="AttributeMap"\>
      <AttributeDescription parent.attr=
        "SunAttribute" name="employeeNumber"/>
      <AttributeDescription parent.attr=
        "WindowsAttribute" name="employeeID"/>
    </AttributeMap\>
  </UserMatchingCriteria\>
</UserLinkingOperation\>
--\>
</UserLinkingOperationList\>
```

Solaris 上での root 以外での Identity Synchronization for Windows サービスの実行

Solaris および Red Hat システムで Identity Synchronization for Windows サービスをインストールおよび実行するには、root 特権が必要です。

しかし、製品をインストールしたあと、root 以外のユーザーとしてプログラムサービスを実行できるようソフトウェアを設定できます。

root 以外のユーザーとしてのサービスの実行

注 - root 以外としてサービスを実行するには、Identity Synchronization for Windows インスタンスディレクトリの下すべてのディレクトリのアクセス権を変更します。デフォルトディレクトリは /var/opt/SUNWisw です。

▼ root 以外のユーザーとしてサービスを実行する

Identity Synchronization for Windows サービスをインストールおよび実行するには root である必要がありますが、root 以外のユーザーとしてプログラムサービスを実行できるようソフトウェアを設定できます。

- 1 (省略可能) UNIX の useradd コマンドを使用して **Identity Synchronization for Windows** にユーザーアカウントを作成します。

nobody ユーザーを使用してサービスを実行することもできます。この手順の残りの例は、iswuser というユーザーを作成したと仮定しています。

- 2 **Sun Java System** ディレクトリサーバーコネクタをインストールするには、インストール時にコネクタに非特権ポートを選択します。

たとえば、1025 以上のポートを使用できます。サーバーが root 以外のユーザーとして実行されている場合、LDAP にはポート 1389 をお勧めします。LDAP over SSL にはポート 1636 をお勧めします。

注- 残りの手順のコマンドはすべて root として実行します。

- 3 コンポーネントをすべてインストールしたあと、次のコマンドを実行して **Identity Synchronization for Windows** を停止します。
`/etc/init.d/isw stop`
- 4 インスタンスディレクトリの所有権を更新してください。たとえば、製品を `/var/opt/SUNWisw` にインストールした場合は次のようになります。
`chown -R iswuser /var/opt/SUNWisw`

`chown -R iswuser /opt/SUNWisw`
- 5 テキストエディタで `/etc/init.d/isw` ファイルを開き、次の行を
`"$EXEC_START_WATCHDOG" "$JAVA_PATH" "$INSTALL_DIR" "$CONFIG_DIR"`
次の行で置き換えます。

`su iswuser -c "$EXEC_START_WATCHDOG '$JAVA_PATH' '$INSTALL_DIR' '$CONFIG_DIR'"`
- 6 次のコマンドを実行してサービスを再起動します。
`/etc/init.d/isw start`
- 7 次のコマンドを実行して、割り当てられたユーザーの **userid** を使用してコンポーネントが実行されていることを確認します。
`ps -ef | grep iswuser`

Identity Synchronization for Windows の同期ユーザーリストの定義と設定

この付録では、同期ユーザーリスト (SUL) の定義の補足情報を記載し、複数のドメインを設定する方法について説明します。ここで説明する内容は、次のとおりです。

- 311 ページの「同期ユーザーリストの定義の理解」
- 313 ページの「複数の Windows ドメインの設定」

同期ユーザーリストの定義の理解

同期ユーザーリスト (SUL) にはすべて、2つの定義が含まれています。1つは同期する Directory Server ユーザーを識別し、もう1つは同期する Windows ユーザーを識別します。

各定義は同期するディレクトリ内のユーザー、同期から除外するユーザー、新しいユーザーの作成場所を識別します。

注 - Identity Synchronization for Windows コンソールを使用して選択したオブジェクトクラスによっても、同期されるユーザーが決まります。プログラムは、選択したオブジェクトクラスを持つこれらのユーザーのみを同期します。これには、選択したオブジェクトクラスのサブクラスを持つユーザーも含まれます。

たとえば、inetorgperson オブジェクトクラスは organizationalPerson オブジェクトクラスのサブクラスであるため、organizationalPerson オブジェクトクラスを選択すると、Identity Synchronization for Windows によってユーザーが inetorgperson オブジェクトクラスと同期されます。

311 ページの「同期ユーザーリストの定義の理解」では、SUL 定義コンポーネントについて説明します。

表D-1 SUL定義コンポーネント

コンポーネント	定義	設定できる		
		Sun	AD	NT
Base DN	同期されるすべてのユーザーの親LDAPノードを定義します。 同期ユーザーリストのベースDNには、ユーザーが同期ユーザーリストのフィルタで除外されているか、ユーザーのDNがより具体的な同期ユーザーリストで一致していないかぎり、そのDNのユーザーがすべて含まれます。たとえば、 <code>ou=sales,dc=example,dc=com</code> のようになります。	可能	可能	不可
Filter	ユーザーを同期ユーザーリストに含める、または除外するために使用するLDAPのようなフィルタを定義します。フィルタには、 <code>&</code> 、 <code> </code> 、 <code>!</code> 、 <code>=</code> 、および <code>*</code> の各演算子を含めることができます。 <code>\>=</code> と <code><=</code> の各演算子はサポートされていません。比較はすべて大文字と小文字を区別しない文字列比較を使用して行われます。 たとえば、 <code>(&(employeeType=manager)(st=CA))</code> には、カリフォルニアのマネージャーのみが含まれます。	可能	可能	可能
Creation Expression	新しく作成されたユーザーの親DNとネーミング属性を定義します(作成を有効にしている場合のみ該当)。 作成式には、同期ユーザーリストのベースDNを含めます。たとえば、 <code>cn=%cn%,ou=sales,dc=example,dc=com</code> のようになります。ここで、 <code>%cn%</code> トークンは作成されるユーザーエントリの値に置き換えられます。	可能	可能	不可

注 - 複数の Active Directory ドメインを持つ Sun Java System Directory Server でユーザーを同期するには、Active Directory ドメインごとに SUL を少なくとも 1 つ定義します。

グループ同期が有効になっている場合は、次のことを確認してください。

1. Active Directory でサポートされる作成式は `cn=%cn%` です。
2. 作成式はユーザーとグループの両方に共通であるため、作成式にはグループオブジェクトクラスに属する有効な属性名を含めてください。

次に例を示します。

属性 `sn` は、Directory Server の `groupofuniquenames` オブジェクトクラスの一部ではありません。したがって、グループオブジェクトでは、次の作成式は無効になります。(ただし、ユーザーオブジェクトでは正しく機能する。)

```
cn=%cn%.%sn%
```

3. 作成式に使用される属性には、作成されるすべてのユーザー/グループエントリの値を指定します。値が指定されないと、ユーザー/グループオブジェクトが同期されず、該当するメッセージがセントラルログに記録されます。
-

複数の SUL を定義した場合、各 SUL 定義を繰り返し一致させることで Identity Synchronization for Windows によって SUL 内のメンバーシップが決定されます。プログラムはより具体的なベース DN を持つ SUL 定義を最初に調べます。たとえば、プログラムは `dc=example,dc=com` の前に `ou=sales,dc=example,dc=com` に対する一致をテストします。

2 つの SUL 定義のベース DN が同じでフィルタが異なる場合、Identity Synchronization for Windows はどのフィルタを最初にテストするか自動的に決定できません。このため、ドメイン重複の解決機能を使用して 2 つの SUL 定義の順序を決定してください。ユーザーが SUL 定義のベース DN と一致したが、そのベース DN のいずれのフィルタも一致しない場合、ユーザーが具体性が低いベース DN のフィルタを一致させた場合でもプログラムはそのユーザーを同期から除外します。

複数の Windows ドメインの設定

複数の Windows ドメインが同じ Directory Server コンテナ (`ou=people,dc=example,dc=com` など) に同期するのをサポートするために、Identity Synchronization for Windows はドメイン情報を含む「合成」Windows 属性を使用します。

- Active Directory ドメインの場合、Identity Synchronization for Windows は Directory Server にエントリを同期する前に Active Directory ドメイン名 (`east.example.com` など) に `activedirectorydomainname` 属性を設定します。

- Windows NT ドメインの場合、Identity Synchronization for Windows は Directory Server にエントリを同期する前に Windows NT ドメイン名 (NTEXAMPLE など) に user_nt_domain_name 属性を設定します。

これらの属性は実際に Windows ユーザーエントリに表示されませんが、Identity Synchronization for Windows コンソールで同期に使用でき、Directory Server のユーザー属性にマップできます。Identity Synchronization for Windows がドメイン属性をマップすると、これらが同期の間に Directory Server エントリで設定され、同期ユーザーリスト (SUL) フィルタで使用できます。

次の例は、Identity Synchronization for Windows がこれらの属性を使用する方法を示しています。この例では、3つの Windows ドメイン (2つの Active Directory ドメインと1つの Windows NT ドメイン) が単一の Directory Server インスタンスと同期すると仮定してします。

▼ 複数の Windows ドメインを設定する

- 1 **Active Directory** east.example.com ドメインのユーザーは ou=people,dc=example,dc=com の **Directory Server** に同期します。
- 2 **Active Directory** west.example.com ドメインのユーザーは ou=people,dc=example,dc=com の **Directory Server** に同期します。
- 3 **Windows NT NTEXAMPLE** ドメインのユーザーは ou=people,dc=example,dc=com の **Directory Server** に同期します。

Directory Server ユーザーを作成または変更する場合、(各 Directory Server SUL に同じベース DN、ou=people,dc=example,dc=com があるため) プログラムは SUL フィルタを使用してユーザーを同期する Windows ドメインを決定します。

activedirectorydomainname 属性と user_nt_domain_name 属性によってこれらのフィルタの構築は簡単になります。

フィルタをコンソールの「属性」タブから構築する

- 4 **Directory Server** の destinationindicator 属性を **Active Directory** の activedirectorydomainname 属性と **Windows NT** の user_nt_domain_name 属性にマップします。
- 5 次の手順で各 **Windows** ドメインに **SUL** を 1 つ設定します。

EAST_SUL

Sun Java System Directory Server definition

Base DN: ou=people,dc=example,dc=com

Filter: destinationindicator=east.example.com

Creation Expression: cn=%cn%,ou=people,dc=example,dc=com

Active Directory definition (east.example.com)

Base DN: cn=users,dc=east,dc=example,dc=com

Filter: <none>

Creation Expression: cn=%cn%,cn=users,dc=east,dc=example,dc=com

WEST_SUL

Sun Java System Directory Server definition

Base DN: ou=people,dc=example,dc=com

Filter: destinationindicator=west.example.com

Creation Expression: cn=%cn%,ou=people,dc=example,dc=com

Active Directory definition (west.example.com)

Base DN: cn=users,dc=west,dc=example,dc=com

Filter: <none>

Creation Expression: cn=%cn%,cn=users,dc=west,dc=example,dc=com

NT_SUL

Sun Java System Directory Server definition

Base DN: ou=people,dc=example,dc=com

Filter: destinationindicator=NTEXAMPLE

Creation Expression: cn=%cn%,
ou=people,dc=example,dc=com

Windows NT definition (NTEXAMPLE)

Base DN: NA

Filter: <none>

Creation Expression: NA

各 Directory Server SUL 定義に同じベース DN と作成式があるが、フィルタは対応する Windows ユーザーエントリのドメインを示します。

これらの設定で Directory Server のユーザーエントリを別の Windows ドメインと同期する方法について、次のテストケースでより詳しく説明します。

- 6 **Active Directory** east.example.com ドメインで cn=Jane Test, cn=users, dc=east, dc=example, dc=com を作成します。
- 7 **Identity Synchronization for Windows** は destinationindicator=east.example.com でユーザーエントリ cn=Jane Test, ou=people, dc=example, dc=com を **Directory Server** に作成します。
- 8 **Directory Server** で cn=Jane Test, ou=people, dc=example, dc=com エントリを変更します。

- 9 **Jane Test** の `destinationindicator` 属性は `east.example.com` であるため、彼女のエントリーは `EAST_SUL` 同期ユーザーリストフィルタと一致し、変更は `east.example.com Active Directory` ドメインに同期します。

この例は、Identity Synchronization for Windows が Windows からのユーザー作成を Directory Server に同期すると仮定しています。これ以外の場合、`idsync resync` コマンドを実行して `destinationindicator` 属性を設定できます。

注 - 複数の SUL のある配備で `idsync resync -f` を使用する場合、おそらくリンク設定ファイルで `allowLinkingOutOfScope` オプションを `true` に設定する必要があります。付録 B 「[Identity Synchronization for Windows LinkUsers XML ドキュメントの例](#)」を参照してください。

この例は、`inetorgperson`、`destinationIndicator` の既存の属性を使用します。これは他の目的で使用される場合もあります。この属性がすでに使用されていたり、別のオブジェクトクラスを選択したりする場合は、ユーザーの Directory Server エントリーのいくつかの属性を `user_nt_domain_name` および/または `activedirectorydomainname` 属性にマップしてください。この値を格納するよう選択した Directory Server 属性は、残りの属性マッピング設定に使用するオブジェクトクラスに含めます。

このドメイン情報を格納するための使用していない属性がない場合は、新しいドメイン属性と Identity Synchronization for Windows で使用するその他の属性をすべてを格納する新しいオブジェクトクラスを作成してください。

レプリケートされた環境での Identity Synchronization for Windows のインストールの注意点

Identity Synchronization for Windows 6.0 は単一のレプリケートされたサフィックスでユーザーの同期をサポートします。

注- この付録では、マルチマスターレプリケーション (MMR) 配備を設定およびセキュリティ保護するために使用する手順をまとめます。この情報は、『[Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド](#)』から直接抜粋したもので、Identity Synchronization for Windows 固有の情報ではありません。

MMR 配備の設計と実装は、複雑です。配備の計画については『[Sun Java System Directory Server Enterprise Edition 6.3 配備計画ガイド](#)』、配備の実装については『[Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド](#)』を参照してください。

この付録の内容は次のとおりです。

- 317 ページの「レプリケーションの設定」
- 319 ページの「SSL を介したレプリケーションの設定」

レプリケーションの設定

注- マルチマスターレプリケーション (MMR) 環境では、Identity Synchronization for Windows によって特定の Sun ディレクトリソースに対して優先マスターおよび副マスターのサーバーを指定できます。

Directory Server は n とおりの MMR をサポートします (設定された任意の n 個のマスターでレプリケートされたデータベースを変更可能)。優先マスターでプラグインをインストールする場合、プラグインのインストール中に他のホストタイプを選択して、Directory Server インスタンスのパラメータを手動で入力する必要があります。

次の手順は、シングルサフィックスのレプリケーションを前提としています。複数のサフィックスをレプリケートしている場合は、各サーバーで並行して設定できます。つまり、各手順を繰り返して、複数のサフィックスでレプリケーションを設定できます。

▼ レプリケーショントポロジを設定する

- 1 シングルマスターを除くすべてのサーバーでレプリケーションマネージャーのエントリを定義します(または、すべてのサーバーでデフォルトのレプリケーションマネージャーを使用する)。
- 2 専用コンシューマのレプリカが作成されるすべてのサーバーでは、次の処理を行います。
 - a. コンシューマレプリカ用の空のサフィックスを作成します。
 - b. レプリケーションウィザードを使用して、サフィックスに含まれるコンシューマレプリカを有効にします。
 - c. 必要に応じて、詳細なレプリカ設定を行います。
- 3 ハブを利用する場合は、ハブのレプリカが作成されるすべてのサーバーで次の処理を行います。
 - a. ハブレプリカ用の空のサフィックスを作成します。
 - b. レプリケーションウィザードを使用して、サフィックスに含まれるハブレプリカを有効にします。
 - c. 必要に応じて、詳細なレプリカ設定を行います。
- 4 マスターレプリカが作成されるすべてのサーバーでは、次の処理を行います。
 - a. マスターレプリカとなるマスターで、サフィックスを1つ選択するか、作成します。
 - b. レプリケーションウィザードを使用して、サフィックスに含まれるマスターレプリカを有効にします。
 - c. 必要に応じて、詳細なレプリカ設定を行います。

- 5 すべてのサプライヤレプリカで、次の順序でレプリケーションアグリーメントを設定します。
 - a. マルチマスターセットのマスター間
 - b. マスターと専用コンシューマの間
 - c. マスターとハブレプリカの間。
必要に応じて、この時点で部分レプリケーションを設定することができます。
- 6 ハブレプリカとそのコンシューマとの間のレプリケーションアグリーメントを設定します。
- 7 マルチマスターレプリケーションでは、データのオリジナルコピーを含むマスターレプリカから順にすべてのマスターを初期化します。ハブとコンシューマレプリカを初期化します。

SSL を介したレプリケーションの設定

注 - この手順で、参照はすべて『[Sun Java System Directory Server Enterprise Edition 6.3 管理ガイド](#)』の章にあります。

▼ レプリケーション動作がすべて **SSL** 接続を介して実行されるようレプリケーションにかかわる **Directory Server** を設定する

- 1 サプライヤサーバーとコンシューマサーバーの両方を、**SSL** を使用するように設定します。
詳細は、第 11 章の「[Managing Authentication and Encryption](#)」を参照してください。

注 -

- サプライヤサーバー証明書が、SSL ハンドシェイク時にクライアントとして機能できない SSL サーバー専用証明書である場合、SSL を経由するレプリケーションは失敗します。
 - SSL を経由するレプリケーションは、現在のところ自己署名の証明書をサポートしていません。
-

- 2 コンシューマサーバー上のサフィックスに対してレプリケーションが設定されていない場合、第8章の「**Enabling a Consumer Replica**」を参照して有効にします。
- 3 第8章の「**Advanced Consumer Configuration**」の手順に従って、コンシューマ上で証明書のエントリのDNを別のレプリケーションマネージャーとして定義します。
- 4 サプライヤサーバー上のサフィックスに対してレプリケーションが設定されていない場合、第8章の「**Enabling a Hub Replica**」または「**Enabling a Master Replica**」を参照して有効にします。
- 5 サプライヤサーバーで新しいレプリケーションアグリーメントを作成し、セキュリティー保護されたSSLポート上のコンシューマに更新を送信します。詳細な手順については、第8章「**Creating Replication Agreements**」の手順に従ってください。セキュリティー保護されたポートをコンシューマサーバーに設定し、パスワードまたは証明書のどちらを使うかについて、SSLオプションを選択します。選択したSSLオプションのDN(レプリケーションマネージャーまたは証明書)を入力します。
レプリケーションアグリーメントの設定が完了すると、サプライヤはすべてのレプリケーション更新メッセージをSSL経由でコンシューマに送信します。証明書を使用するオプションを選んだ場合は、証明書が利用されます。SSLのアグリーメント設定を使用してコンソールからカスタマーの初期化を行う場合も、セキュリティー保護された接続が使われます。

MMR環境での Identity Synchronization for Windows の設定

▼ MMR環境で Identity Synchronization for Windows を設定する

- 1 **Identity Synchronization for Windows** コンソールからサフィックスを同期させる優先マスターと副マスターのサーバーを指定します。(161 ページの「**Sun Java System ディレクトリソースの作成**」を参照)
トポロジで他の Directory Server についての情報を指定する必要はありません。
- 2 コンソールから、または `idsync prepds` コマンド行ユーティリティーを使用して優先マスターと副マスターのサーバーを準備します。(168 ページの「**Sun ディレクトリソースの準備**」を参照)
コマンド行ユーティリティーを使用する場合は、優先サーバーと副サーバーの両方に対する引数を指定して、両方のサーバーを単一の呼び出しで準備する必要があります。

- 3 これらのディレクトリ間でレプリケートされるサフィックスのディレクトリサーバーコネクタをインストールします。(220 ページの「ディレクトリサーバーコネクタのインストール」を参照)
- 4 優先マスター、副マスター、およびレプリケートされたサフィックスでユーザーを管理するその他すべての **Directory Server** インスタンスでディレクトリサーバープラグインを設定します (300 ページの「**dspluginconfig** の使用」を参照)。

索引

数字・記号

3DES キー, 251

A

accountlockout, 引数、説明、構文, 299

ACI, 291

ACIs, 257

Active Directory

SSL、使用, 173, 179, 251, 264

SSL の使用, 173, 179, 251, 264

SSL の設定, 133, 168

SUL の作成, 209

あらかじめ存在するユーザー, 238

オブジェクトクラス, 124

オブジェクト削除のフロー, 208

オブジェクト作成のフロー, 190

オンデマンドパスワード同期, 109, 112, 233

拡張セキュリティオプション, 179, 251

グローバルカタログ, 135, 172, 173

コアの設定, 135

コネクタとドメインコントローラ間の通信, 112

コネクタのインストール, 104, 226-229

コネクタの配布, 217

コンポーネントの分散の例, 115

再同期間隔, 180

削除の同期, 208

作成式, 212

サポートされるバージョン, 95

証明書, 178, 179, 251, 258, 264

Active Directory (続き)

証明書データベース, 179

証明書のインポート, 264

信頼できる証明書, 179, 251, 258

セキュリティオプション, 179

セキュリティ保護された通信の有効化, 168

ソース

作成, 160

属性, 124, 183, 194

属性の選択, 183

属性の同期, 167, 183

属性の編集, 194

属性のマッピング, 183

ディレクトリ, 123

ディレクトリソース, 172, 221

ディレクトリソースの作成, 172

同期設定, 113, 124

特殊なユーザー, 238

ドメイン, 172, 174, 313

ドメインコントローラ, 112, 114, 177, 178, 180

ドメインコントローラ設定パラメータの編集, 180

配備, 172

配備の例, 112

パスワードの伝播, 133

パスワードの同期, 112, 127, 167

パスワードポリシー, 127, 128

フェイルオーバーサーバー, 178

複数ドメイン, 313

複数のドメイン, 313

複数のドメインコントローラの使用, 177

物理的な配備, 114

Active Directory (続き)

- プライマリドメインコントローラ FSMO ロール所有者, 177
- 変更検出, 107
- 変更の検出, 107
- ホスト, 173, 175
- 有効化と無効化の同期, 196
- ユーザー DN, 173
- ユーザー認証の失敗, 111
- ユーザーの同期, 234
- ユーザーのリンク, 233, 234
- コネクタ、インストール, 226-229

audit.log, 133

- 結果のリンクと再同期, 298
- 説明, 100, 271
- 場所, 270, 279
- 目的, 271

Auxiliary オブジェクトクラス

- 削除, 188
- 設定, 124
- 選択, 187, 188

AvoidPdcOnWan 属性, 177

B

base64 符号化, 265, 284

C

CA 証明書

- SSLの有効化, 264
- インポート, 261
- コンポーネントの要件, 258
- 自動インストール, 178
- 取得, 263, 266, 267
- 追加, 251, 268

certinfo サブコマンド

- 構文, 288
- 使用, 260
- 証明書情報の表示, 287
- 証明書の追加, 288
- 説明, 136, 287
- 引数, 260

certinfo サブコマンド (続き)

- 例, 288
- certutil
- 証明書の取得, 264
 - デフォルトの場所, 262
- changepw サブコマンド
- 構文, 289
 - 説明, 136, 287, 289
 - パスワードの変更, 289
 - 引数, 289
 - 例, 289

D

DIR_PROXY_HOST, 63

DIR_PROXY_PORT, 63

Directory Server

- Directory Server ツールと相互運用, 197
 - Identity Synchronization for Windows ソースの準備, 168-172
 - idsync prepds の使用, 287
 - SSLを経由したアクセス, 284
 - アクセス権, 176
 - オブジェクトクラス, 124
 - カスタムメソッドの使用, 199
 - コネクタ、インストール, 220
 - コネクタのインストール, 103, 220
 - コンソール, 197
 - 資格/特権, 254
 - 指定, 165
 - 準備, 121, 168, 169, 287, 292
 - セットアッププログラム, 218
 - 属性の同期, 183
 - 属性変更のフロー, 196
 - ディレクトリソースの準備, 121, 291
 - パスワードの伝播, 133, 135
 - パスワードの同期, 112
 - パスワードポリシー, 128
 - プラグインのインストール, 103
 - 変更検出, 106
- DIRSERV_HOST, 63
- DIRSERV_PORT, 63
- DLL
- NT 変更検出機能, 272

DLL (続き)

- Windows NT, 105
 - パスワードフィルタ, 109
- DN, 173
- DNS, ドメインエントリ, 164
- dspwuserlink 属性, 233, 293

E

error.log

- コネクタ ID のディレクトリソースへのマッピング, 266, 268
- 説明, 271
- 場所, 270, 279

F

- forcepwchg.jar, 302
- forcepwchg ユーティリティー
- 説明, 302
 - パスワードの変更の強制, 302
 - 引数, 302
- FSMO, 177

I

Identity Synchronization for Windows

- Directory Server ソースの準備, 168-172
- Directory Server のディレクトリソースの準備, 121, 291
- アンインストール, 241
- インストール, 117
- コンソール, 276, 278, 279
- 削除, 241
- 削除する, 92
- 信頼性, 111
- 設定プログラム, 92, 141

idsync certinfo, 260

- 構文, 288
- 証明書の追加, 288
- 説明, 288
- 引数, 288

idsync certinfo (続き)

- 例, 288

idsync changepw

- 構文, 288
- 説明, 289
- パスワードの変更, 289
- 引数, 288
- 例, 289

idsync groupsync, 引数、説明、構文, 299

idsync importcnf

- 構文, 290
- 設定ファイルのインポート, 290
- 説明, 287, 290
- 引数, 285, 290

idsync prepds

- Directory Server の準備, 121, 287
- 構文, 293
- 証明書, 291
- 説明, 136, 287

idsync printstat

- インストール/設定手順のリスト, 295
- 構文, 295
- 状態の印刷, 295
- 説明, 294
- 引数, 295

idsync resetconn

- 構文, 295
- 説明, 295
- 引数, 295

idsync resync, 122

- 2つのディレクトリソースの再同期, 233
- linkusers XML 設定ドキュメントの例, 305
- インデックスが作成された属性, 237
- 既存のユーザーの同期, 296
- 結果のロギング, 238
- 構文, 296
- 使用, 233
- 使用に関する警告, 237
- 使用例, 237
- スクリプト, 233
- 説明, 296
- 引数, 296
- 引数の例, 236

idsync startsync

構文, 300

説明, 300

引数, 300

idsync stopsync

構文, 301

説明, 301

引数, 301

idsync スクリプト、実行, 286

importcnf サブコマンド

説明, 287, 290

引数, 285, 291

imq start コマンド, 239

imq stop コマンド, 239

inetorgperson 属性, 126

install-path, 16*instance-path*, 16

isw-hostname ディレクトリ, 16

isw-hostname ディレクトリ, 242

isw start コマンド, 239

isw stop コマンド, 239

J

jar files, forcepwchg, 302

Java Development Kits、ダウンロード, 141

Java プロセス

ウォッチドッグ, 98

コネクタ, 101

コマンド行ユーティリティー, 99

コンソール, 99

再起動, 98

システムマネージャー, 100

設定ディレクトリ, 98

セントラルロガー, 100

Java ホーム、指定, 149

JNDI, 14

JRE

Java ホームのディレクトリの確認, 149

ダウンロード, 141

K

keytool ユーティリティー, 257

L

LDAP

DIT, 135

ldapsearch, 302

クエリの構文, 212

デフォルトポート, 163

フィルタ, 126, 139, 285, 297

LDAP_ADMIN_PWF, 63

LDAP_ADMIN_USER, 64

ldapsearch、使用, 302

linkusers.cfg, 305, 306-308

linkusers-simple.cfg, 305-306

LinkUsers XML ドキュメント, 305

M

MANPATH, 64

MANSECT, 64

Message Queue, 15

アクセス制御, 253

クライアント証明書の検証, 256

自己署名付き証明書, 257

証明書の受け入れ, 257

証明書の検証, 256-257

設定, 150

説明, 102

デフォルトのブローカのポート, 151

ブローカ, 102

ポート番号の指定, 150

ローカルホスト名の指定, 150

Microsoft

Certificate Server, 178

サポート技術情報の記事, 177

MMR

信頼できる同期, 112

設定, 317

設定コンポーネント, 258

N

nsAccountLock 属性, 198-199
NT SAM
 同期, 105
 ドメインユーザー, 233
 リンク用の識別子, 234
 レジストリ, 102
NT 変更検出機能 DLL, 272
NT レジストリディレクトリソース, 160

O

objectguid 属性, 233

P

PATH, 64
PDC
 FSMO ロール所有者, 177
 コネクタおよびサブコンポーネントのインストール, 105
 コンピュータ名の確認, 181
PDC コンピュータ名の確認, 181
prepds サブコマンド
 Directory Server の準備, 121, 287
 構文, 293
 証明書, 291
 説明, 136, 287
 引数, 293
 例, 292
printstat サブコマンド
 インストール手順/設定手順の表示, 287
 コネクタ状態の出力, 136
 コネクタの状態の印刷, 287
printstat サブコンポーネント
 構文, 294
 説明, 294
 引数, 294
PwdLastSet 属性, 109

R

Red Hat, インストールプログラムの実行, 144
resetconn サブコマンド, 295
 構文, 295
 コネクタ状態のリセット, 136
 コネクタの状態のリセット, 287
 説明, 295
 引数, 295
resync.log
 結果のリンクと再同期, 298
 説明, 271
 場所, 270
 リンクおよび再同期の結果, 238
resync サブコマンド, 234, 236, 297, 298, 305
 既存のユーザーの同期, 296
 構文, 296
 説明, 296
 配備のブートストラップ, 122
 引数, 296
 ユーザーのリンク/同期, 136, 288
 ユーザーのリンクおよび同期, 233

S

samples1 ディレクトリ, 305
SASL Digest-MD5, 110
Secure Sockets Layer (SSL), 249
serverroot ディレクトリ, 16
setup.exe, 218
SLAMD 分散負荷生成エンジン, 14
Solaris
 Identity Synchronization for Windows の削除, 247
 インストールプログラムの実行, 142, 143
 デーモンの起動/停止, 239
SSL
 Active Directory での使用, 251
 Active Directory の使用, 251
 Active Directory の設定, 133, 173, 179
 Directory Server へのアクセス, 284
 Windows 向けの設定, 133
 コアでの有効化, 219
 使用, 168, 250, 268
 証明書, 179, 251, 257
 信頼できる証明書の要求, 179

SSL (続き)

通信の有効化, 165, 168, 262

ポートの選択, 219

有効化, 262

startsync サブコマンド

構文, 300

説明, 300

同期の開始, 137, 288

引数, 300

STDIN、パスワードの読み取り, 286

stopsync サブコマンド

構文, 301

同期の停止, 288

引数, 301

Structural オブジェクトクラス

設定, 124

デフォルト, 124

SUL

格納, 214

管理者のフィルタリング, 212

作成, 126, 127, 209

説明, 126, 209

定義, 126, 311

定義コンポーネント, 209, 311

Sun Java System

コンソール, 156

ディレクトリソースの作成, 160, 161-168

Sun Java™, 91

System Identity Synchronization for Windows、 「*Identity Synchronization for Windows*」を参照, 91

SystemManagerBootParams.cfg ファイル, 290

T

TEMP ディレクトリ, 224

「To Do」 ノード, 278

U

uid 属性, 235

uninstall.cmd スクリプト, 242

UNIX コマンド

Java ホームの確認, 149

URL

管理サーバー, 153

設定ディレクトリ, 146, 219

user, 属性, 126

USNchanged 属性, 107, 109

UTF-8, 286, 302

W

WAR ファイル

DSCC, 51-54

アプリケーションサーバー, 51-54

WatchList.properties, 256

Web サイト

Directory Server の発行物, 133

Java Development Kit のダウンロード, 141

Microsoft 製品ドキュメント, 133

Microsoft 認証局, 133

Sun 製品ドキュメント, 91

Windows

Identity Synchronization for Windows の削除, 247

SSL の設定, 133

インストールプログラムの実行, 143-144

サービスの開始と停止, 159

ディレクトリソースの作成, 172

ディレクトリソースの選択, 211

Windows NT

監査の有効化, 280

コネクタおよびサブコンポーネントのインストール, 105

コネクタの説明, 101

ディレクトリソースの作成, 180

同期設定, 124

ドメイン名の指定, 181

変更検出, 108

レジストリ, 112

コネクタのインストール, 229

X

XML 設定ドキュメント

linkusers-simple.cfg, 305-306

エクスポートされた 1.0 設定のインポート, 153

XML 設定ドキュメント (続き)

ユーザーのリンク, 138, 297

例, 305

XML 設定ファイル, linkusers.cfg, 306-308

あ

アカウント

組み込み, 303

作成, 129, 222, 309

アカウントのロックアウト, 205

アクセス権, 176, 291

アクセス権限, 253, 257

アクセスの制限, 257

アンインストール

Identity Synchronization for Windows, 241

コア, 241, 244

コンソール, 247

サーバーインスタンスを削除する, 81-84

ソフトウェア, 241

ソフトウェアを削除する, 84-86

ディレクトリサーバープラグイン, 241

アンインストールの障害, 287

暗号化

3DES キー, 251

Message Queue のメッセージ, 251, 253

設定情報, 147, 148

チャネル通信, 167

ネットワークトラフィック, 251

平文パスワード, 106

い

移行, forcepwhg の使用, 302

インスタンスディレクトリ、デフォルト, 309-310

インストール

Active Directory コネクタ, 104, 226-229

Directory Proxy Server をネイティブパッケージから, 32-36

Directory Server をネイティブパッケージから, 28-32

Identity Synchronization for Windows, 150

インストール (続き)

Directory Server Resource Kit を ZIP 形式の配布から, 45-51

Directory Server Enterprise Edition を ZIP 形式の配布から, 45-51

Directory Service Control Center インストールのトラブルシューティング, 61-63

Directory Service Control Center をネイティブパッケージから, 36-39

Windows NT コネクタおよびサブコンポーネント, 105

決定, 134

コア, 103, 134, 144-154

コネクタ, 215, 217

サブコンポーネント, 215

実行手順リスト, 120, 152

証明書, 257

チェックリスト, 137, 139

ディレクトリ, 218

ディレクトリサーバーコネクタ, 103

ディレクトリサーバープラグイン, 103, 217

ディレクトリ、デフォルト, 242

ディレクトリの指定, 149, 151

プログラムのダウンロード, 142

ログの表示, 224, 228, 230

インストールの計画, 95

インデックス

作成, 170

追加, 293, 294

等価インデックスの作成, 168

インデックスの作成, 170

インポート

CA 証明書, 261

設定情報, 290

う

ウォッチドッグプロセス, 98

え

エイリアス、証明書, 257

エイリアスディレクトリ, 263

- エクスポート, Directory Server 証明書, 263
- エラー, 検証, 215
- エラー検出, 100

- お
- オブジェクト
 - 削除, 208
 - 削除フローの指定, 208
 - 変更のフローの指定, 195
 - 有効化と無効化の設定, 196
- オブジェクトキャッシュ, データベース, 107
- オブジェクトクラス
 - Active Directory, 124
 - Directory Server, 124
 - 構造, 124
 - 設定, 124
 - 選択, 188
 - 属性, 124, 188
 - 補助, 124
 - ユーザー, 135
- オンデマンドパスワード同期, 106, 109, 110, 112, 233
 - 認証メカニズム, 110

- か
- 開始
 - サービス, 159
 - 同期, 137, 300
- 書き込み
 - syslog デーモンへのログ, 275
 - ファイルへのログ, 275
- 拡張セキュリティーオプション, 指定, 179
- 格納
 - SUL, 214
 - 設定情報, 135, 219
- カスタムメソッド, 199
- カタログ, グローバル
 - 指定, 172, 174
 - 複数, 172
 - 保護, 252
 - 目的, 135

- 環境変数, 63-64
 - DIR_PROXY_HOST, 63
 - DIR_PROXY_PORT, 63
 - DIRSERV_HOST, 63
 - DIRSERV_PORT, 63
 - LDAP_ADMIN_PWF, 63
 - LDAP_ADMIN_USER, 64
 - MANPATH, 64
 - MANSECT, 64
 - PATH, 64
- 監査, Windows NT での有効化, 280
- 管理サーバー
 - SSL 通信の有効化, 147
 - URL の場所, 153
 - インストール, 145
 - コアのインストール, 103
- 管理者
 - Directory Server の準備, 169, 292
 - SUL からのフィルタリング, 212
 - uninstall.cmd スクリプトの実行, 242
 - アクセスの制限, 257
 - 資格/特権, 134, 136, 147, 256
 - ディレクトリソースの再同期, 233
 - (バインド) 識別名の指定, 163, 173
 - ユーザー識別名, 173
 - ユーザーのリンク, 233

- き
- 起動
 - Message Queue ブローカ, 239
 - コンソール, 152, 153
 - サービス, 239
 - デーモン, 239
 - 同期, 238
- 機密情報の保護, 254
- 旧バージョン形式の更新履歴ログデータベース
 - 再作成, 171
 - 作成, 168
 - 変更検出, 106

く

組み込みアカウント, 303
 クライアント、認証, 302
 グループ同期, 203
 グループの同期, 299
 グローバルカタログ, 135
 Active Directory, 172
 作成, 127
 指定, 172, 173, 174
 複数, 172
 保護, 252
 グローバルな同期設定, 113

け

警告、設定, 215
 軽量プロセス, 101
 検出
 エラー, 100
 変更, 101, 102, 106, 111, 165
 有効化と無効化, 196
 検証
 検証エラー, 215
 証明書, 256-257, 257
 設定, 215

こ

コア
 SSLの有効化, 219
 アンインストール, 241, 244
 インストール, 103, 134, 137, 144-154
 インストール特権, 144
 ウォッチドッグ, 98
 コンポーネント, 97, 120
 設定, 134, 137, 155
 設定する, 92
 説明, 98
 チェックリスト, 137
 高可用性の説明, 112
 更新、検出, 106
 構築、フィルタ, 314

構文

changepw サブコマンド, 289
 forcepwchg コマンド, 302
 idsync, 287
 idsync importcnf, 290
 idsync certinfo コマンド, 288
 idsync changepw コマンド, 289
 idsync prepds コマンド, 293
 idsync printstat コマンド, 295
 idsync resetconn コマンド, 295
 idsync resync コマンド, 297
 idsync startsync コマンド, 301
 idsync stopsync コマンド, 301
 LDAP クエリ, 212
 LDAP フィルタ, 126

コネクタ

Active Directory, 217
 Directory Server, 220
 idsync printstat の使用, 287
 インストール, 103, 104, 105, 215, 217
 ウォッチドッグプロセス, 98
 起動/監視, 98
 再起動, 101
 状態, 287, 295
 状態の印刷, 287, 295
 説明, 101
 双方向同期, 101
 トラブルシューティング, 271
 配布, 217
 変更の検出, 106, 107, 108

コネクタの監視, 98

コネクタの起動, 98

コネクタの状態の印刷, 295

コマンド

imq start, 239

isw stop, 239

説明, 136

コマンド行ユーティリティー

idsync resync, 233

共通機能, 283

共通の引数, 283

使用, 136, 283

説明, 99, 136, 283

パスワードの入力, 286

コンソール

- Directory Server, 197
- Identity Synchronization for Windows, 99, 158, 276, 278, 279
- Sun Java System コンソール, 156
- アンインストール, 247
- インストール, 150
- 起動, 152, 153
- コアの設定, 155
- 設定ディレクトリでの読み書き, 98
- 説明, 99, 120, 158
- 同期の起動/停止, 238
- パスワード, 148
- ログイン, 153
- ログの表示, 269

コンポーネント

- ID, 271
- コア, 98, 120
- コンソール, 99
- 設定ディレクトリ, 98
- 説明, 97
- 物理的な配備の例, 114
- 分散, 103, 114
- 分散の例, 115
- メッセージ, 270
- ローカルログ, 271
- ログレベル, 274

さ

サーバー

- Administration, 147
- 管理, 103, 145, 153
- 検索, 156
- フェイルオーバー, 178
- ホスト名, 157

サーバーインスタンスの作成

- Directory Proxy Server, 64-77
- Directory Server, 64-77

サーバーインスタンスを作成する

- Directory Proxy Server, 64-77
- Directory Server, 64-77

サービス

- 開始と停止, 159

サービス (続き)

- 起動/停止, 238, 239
- 再起動, 310
- 同期, 238
- 再起動
 - Java プロセス, 98
 - コネクタ, 101
 - サービス, 310
 - 同期, 238
- 再同期
 - 属性, 233
 - ディレクトリソース, 233
 - ユーザー, 288, 296
- 再同期間隔
 - Active Directory コネクタの設定, 180
 - NT の設定, 182
 - 「再同期間隔」, ディレクトリサーバーコネクタの設定, 171
- 再同期間隔
 - デフォルト, 171
- 削除
 - Auxiliary オブジェクトクラス, 188
 - オブジェクト, 208
 - コア, 244
 - 属性値, 194
 - ディレクトリサーバープラグイン, 241
 - 同期, 208
 - フローの指定, 208
- 作成
 - Active Directory ソース, 160, 172
 - NT レジストリディレクトリソース, 160
 - SUL, 126, 127, 209
 - Sun Java System ディレクトリソース, 160, 161-168
 - Windows 2003 Server グローバルカタログ, 127
 - Windows 2003 Server ディレクトリソース, 127
 - Windows NT ディレクトリソース, 180
 - アカウント, 129, 222, 309
 - 旧バージョン形式の更新履歴ログデータベース, 168
 - パラメータ化されたデフォルト属性値, 125
- 作成式, 126, 212
- 作成属性
 - 削除, 190

作成属性 (続き)

- 作成, 190
- 説明, 125
- パラメータ化されたデフォルト値, 125
- 必須, 183, 185
- 編集, 190
- マッピング, 193

作成のフロー

- 指定, 189, 194

作成フロー

- 設定の計画, 135
- 有効化, 112

サフィックス

- 設定, 164
- レプリケート, 317

サフィックス/データベース, 121, 123

サブコマンド

- certinfo, 260, 288
- changepw の使用, 289
- idsync, 283
- importcnf, 285, 287, 291
- importcnf の使用, 290
- resetconn, 295
- resync, 296, 298, 305
- startsync, 300
- stopsync, 301
- 説明, 287

サブコンポーネント

- printstat, 294
- インストール, 215
- 説明, 101

し

資格/権限, 指定, 175

資格/特権, 147

- Directory Server, 254
- コアのインストール, 144
- コネクタに必要, 254
- 資格の作成, 256
- 設定 Directory Server, 136
- 設定ディレクトリ, 256
- 設定ディレクトリに対する指定, 147

識別名

- 管理者, 176
- 指定, 173, 176

自己署名付き証明書, 257, 262

システム

- 監査, 96
- パスワード作成のフロー, 189, 194

システムコンポーネント

- 説明, 97
- 分散, 103

システムコンポーネントの分散, 103

システムマネージャー

- 証明書の受け入れ, 257
- 説明, 100

持続的記憶領域保護, 254

実行, idsync resync スクリプト, 233

実行可能ファイル, setup.exe, 218

実行手順ノード, 269

実行手順リスト, 120, 152, 215, 225, 228

指定

- Active Directory ドメイン, 174
- Directory Server, 165
- Java ホーム, 149
- Windows NT ドメイン名, 181
- インストールディレクトリ, 149
- オブジェクト削除のフロー, 208
- オブジェクト変更のフロー, 195
- グローバルカタログ, 172, 173, 174
- 再同期間隔, 180
- 作成のフロー, 189, 194
- 資格, 175
- 設定ディレクトリの資格, 147
- 設定ディレクトリのホスト/ポート, 146
- 設定パスワード, 250
- 属性, 124, 188
- ドメインコントローラ, 176
- フェイルオーバーコントローラ, 178
- フェイルオーバーサーバー, 178
- ポート番号, 151
- ホスト, 173
- ユーザー DN, 163, 173
- ユーザーセットドメインのベース DN, 211
- ルートサフィックス, 147

集中, システム監査, 96

重要属性

説明, 125

パラメータ化されたデフォルト値の作成, 125

準備

Directory Server, 121, 168, 291

使用

Directory Server のカスタムメソッド, 199

SSL, 250, 262, 268

ディスク容量なし, 276

障害

アンインストーラ, 287

照会

設定ディレクトリ, 162, 163

障害

ハードウェア, 287

使用情報、idsync, 286

状態

コネクタ, 295

コネクタの状態の印刷, 295

設定の有効性の状態, 214

ディレクトリソース, 277

表示, 269

「状態」タブ, 158

情報パネル, 120, 152, 159, 225, 228, 278

証明書

Active Directory, 178, 264

CA, 251, 258

certinfo サブコマンド, 288

certinfo サブコマンドの使用, 136, 287

certutil の使用, 264

Directory Server, 263

idsync certinfo の使用, 260

SSL, 179, 251, 257

インストール, 257

インポート, 266

受け入れ, 257

エイリアス, 257

エクスポート, 263

検証, 256-257, 257

自己署名付き, 257, 262

取得, 263, 264

情報の取得, 287

情報の表示, 288

追加, 268

証明書 (続き)

必要, 260

要求, 179, 251

証明書/特権、idsync prepds に必要, 291

証明書データベース

証明書の取得, 263

証明書の追加, 268

ディレクトリ, 266, 268

デフォルトパス, 16

場所の指定, 285

必要な証明書, 260

証明書の取得、certutil の使用, 264

信頼性, 111

信頼できる証明書, 179, 251

す

スキーマ

コントローラ, 135

デフォルトソースの変更, 186

スクリプト

idsync, 286

idsync resync, 233

せ

セーフモード, 234

セキュリティ

Active Directory, 179

強化, 255

設定, 249

レプリケートされた設定, 258

セキュリティの強化, 255

セキュリティ保護された通信, 168

設定

Message Queue, 150

SSL, 133

検証, 215

コア, 134, 137, 155

ファイックス, 164

実行手順リスト, 120

セキュリティ, 249

属性の同期, 189

設定 (続き)

- 配備の決定, 134
- 複数ドメイン, 311
- 複数のサフィックス, 318
- 有効化と無効化, 196
- ログファイル, 276
- 設定する, コア, 92
- 「設定」タブ, 158
- 説明, 159
- 設定ディレクトリ
 - URL, 134, 146, 219
 - アクセスの制限, 257
 - 管理者の名前/パスワード, 147, 219
 - 資格, 256
 - 資格の指定, 147
 - 照会, 162
 - 証明書の検証, 257
 - 接続, 285
 - 設定情報の暗号化, 148
 - 説明, 98, 151
 - デフォルトのポート, 146
 - ホスト/ポートの指定, 146
 - ホスト名/ポート番号, 236, 298
 - 目的, 134, 136
 - 読み書き, 98
- 設定パスワード
 - idsync changepw の使用, 289
 - 検出, 290
 - 指定, 250
 - 変更, 287, 289
 - 保護, 255
- 設定プログラム
 - Identity Synchronization for Windows, 92, 141
- セットアッププログラム
 - Directory Server, 218
 - 検出, 218
- セントラル, ログ, 270
- セントラルロガー
 - clogger 100 ディレクトリ, 271
 - 説明, 100
 - メッセージ, 270
 - 問題のトラブルシューティング, 271
 - ローカルログ, 271
- セントラルログディレクトリ, 16, 270

そ

- 相互運用, Directory Server ツール, 197
- 双方向同期, 96, 101
- ソース, Active Directory ソースの作成, 172
- 属性
 - AvoidPdcOnWan, 177
 - dspswuserlink, 233, 293
 - inetorgperson, 126
 - nsAccountLock, 198-199
 - objectguid, 233
 - PwdLastSet, 109
 - uid, 235
 - user, 126
 - USNchanged, 107, 109
 - インデックスの作成, 237
 - 再同期, 233
 - 作成, 125
 - 指定, 188
 - 重要, 125
 - 設定, 124
 - 説明, 124
 - 選択, 183
 - タイプ, 125
 - ネーミング, 209
 - パラメータ化されたデフォルト値の作成, 125
 - 必須, 作成, 185
 - 必須の作成, 125
 - 編集, 194
 - マッピング, 126, 183
 - ユーザーエントリの同期, 135, 183
- 属性のインデックスの作成, 237
- 属性変更のフロー, 196

た

- ダウンロード, インストールプログラム, 142
- 「タスク」タブ, 158
- タブ
 - 状態, 158
 - 設定, 158, 159
 - タスク, 158
- 単一ホスト配備, 118

ち

- チェックリスト, 152
- インストール, 137, 139
- チャンネル通信、暗号化, 167

つ

追加

- インデックス, 293, 294
- 管理者グループへの資格, 256
- 証明書, 268, 288
- 設定データを Directory Server へ, 151
- 属性値, 194
- ディレクトリソース, 160, 172, 182
- ユーザーを Active Directory に, 129

通信

- SSL の有効化, 165, 168
- 最後の通信, 277

て

定義

- SUL, 311
- 複数ドメイン, 311
- ユーザー, 126

停止

- Message Queue ブローカ, 239
- サービス, 159, 239
- デーモン, 239
- 同期, 137, 238, 301

ディレクトリ

- Active Directory, 123
- clogger 100 (セントラルロガー), 271
- isw-hostname, 242
- samples1, 305
- TEMP, 224
- インスタンス, 309-310
- インストール, 151, 218
- インストール用の指定, 149
- エイリアス, 263
- 事前生成, 296
- 照会, 162
- 証明書データベース, 266, 268

ディレクトリ (続き)

- 設定, 98, 134, 135, 136, 151
- 説明, 123
- セントラルログ, 270
- セントラルログを含む, 270
- ソースの再同期, 233
- デフォルトインスタンス, 309-310
- ログ, 275
- ディレクトリサーバープラグイン
 - SSL の使用, 168, 268
 - アンインストール, 241
 - インストール, 103, 104, 167, 217
 - 削除, 241
 - 証明書の追加, 288
 - セキュリティー保護された通信の有効化, 168, 268
 - 説明, 101, 167
 - 双方向同期, 102
 - パスワードの暗号化, 251
 - 変更の検出, 106
 - ログ, 272
- ディレクトリソース
 - Active Directory, 221
 - エントリの例, 220
 - 作成, 127
 - 状態, 277
 - 追加, 160, 172, 182
 - ユーザーのリンク, 233
- ディレクトリの事前生成, 296
- データベース
 - インデックスの作成, 170
 - オブジェクトキャッシュ, 107
 - 旧バージョン形式の更新履歴ログ, 168, 171
 - 証明書, 168, 251, 263, 264, 288
- デーモン
 - 起動/停止, 239
 - ログの書き込み, 275
- デフォルト
 - 3DES キーでの暗号化, 252
 - Base64 で符号化された値, 284
 - certutil の場所, 262
 - LDAP ポート, 163
 - Solaris のインストールディレクトリ, 242
 - SUL 名, 210

デフォルト (続き)

- syslog メッセージ, 276
 - インスタンスディレクトリ, 309-310
 - コマンド行ユーティリティの引数, 236
 - 再同期間隔, 171
 - 再同期ソース, 235
 - 「信頼できる SSL の証明書を要求」設定, 179
 - 設定ディレクトリのポート, 146
 - 同期フロー, 189
 - パスワードポリシー, 127
 - パラメータ化された値の作成, 125, 185
 - 表示する監査/エラーのメッセージ行, 279
 - ブローカのポート, 151
 - ルートサフィックス, 164, 284
 - ログディレクトリ, 275
 - ログの維持, 272
 - ログの書き込み, 275
- デフォルトの場所, 15-18
- 伝播
- 新しいパスワード, 190
 - パスワードの変更, 109, 133, 196
 - ユーザーの削除, 208

と

等価

- インデックス, 168, 293
- フィルタ, 212

同期

- Active Directory と, 127
- idsync resync の使用, 288
- idsync startsync の使用, 288
- idsync stopsync の使用, 288
- NT SAM, 105
- イベントメッセージ, 271
- 開始, 300
- 開始/停止, 288
- 既存ユーザー, 122
- 起動/停止, 238
- コンポーネントが利用不可になるとき, 111
- 再起動, 238
- 削除, 208
- 設定, 113, 123, 124, 189
- 双方向, 101

同期 (続き)

- 属性, 167, 183
 - 停止, 301
 - デフォルト, 189
 - パスワード, 112, 127, 167
 - 複数のドメイン, 214
 - 有効化と無効化, 196
 - ユーザーエントリ属性, 135, 183
 - ユーザーの作成, 113
 - ユーザーリストのフィルタリング, 214
 - 要件, 112
- 同期ユーザーリスト、「SUL」を参照, 209
- 特徴, 96
- 特権/資格, 134, 147
- コアのインストール, 144
 - コネクタに必要な, 254
 - 資格の作成, 256
 - 設定 Directory Server, 136
 - 設定ディレクトリ, 256
- 特権/証明書, idsync prepds に必要, 291
- ドメイン
- Active Directory, 172, 174, 313
 - NT ドメインの指定, 181
 - 重複の解決, 214
 - 複数, 313
 - 複数の設定, 311
 - ユーザーセット, 211
- ドメインコントローラ
- Active Directory, 177, 178
 - 指定, 176
 - パラメータの編集, 180
 - フェイルオーバー, 178
 - 複数の使用, 177
 - 編集, 180, 182
- ドメイン重複の解決, 214
- トラブルシューティング, セントラルロガー, 271

に

認証

- オンデマンドパスワード同期, 110
- クライアント, 302
- 失敗, 111
- 設定ディレクトリへの接続, 285

ね

ネーミング属性, 説明, 209

は

ハードウェアの障害, 287

配備

2台のマシンのシナリオ, 112

Active Directory, 172

idsync resync の実行, 122

MMR, 317

インストール/設定の決定, 134

コンポーネントの分散, 103

単一ホスト, 118

同期の要件, 112

ブートストラップ, 122

例, 114

パスワード

暗号化, 106

オンデマンドパスワード同期, 109, 112, 233

検出, 290

コマンド行ユーティリティーの入力, 286

作成, 189, 194

設定, 250

設定の変更, 289

同期, 127

パスワードなしのアカウントの作成, 129

ハッシュされた, 106

引数, 286

変更の伝播, 109, 133

変更の要求, 302

保護, 255

パスワード同期、オンデマンド, 106, 110, 233

パスワードの変更の要求, 302

パスワードフィルタサブコンポーネント, 102, 105, 109, 122, 302

パスワードポリシー

Active Directory, 128

Directory Server, 128

設定パスワードに対する, 255

デフォルトの Windows, 127

要求, 127

パスワードポリシーの要求, 127

ハッシュされたパスワード, 106

ひ

引数

certinfo, 260

changepw サブコマンド, 289

forcepwchg, 302

importcnf, 285

prepds, 293

printstat, 295

resetconn, 296

resync, 234, 236, 297, 298

stopsync, 301

コマンド行ユーティリティー, 283

パスワード, 286

必須作成属性, 183, 185

必須の作成属性, 125

平文パスワード

収集, 106

取得, 109

伝播, 109

パスワードフィルタ DLL の使用, 109

ふ

フィルタ

LDAP, 126, 139, 285, 297

SUL, 126, 135, 209

検索, 265

構築, 314

構文, 212, 312

説明, 209

等価, 212

部分文字列, 212

プレゼンス, 212

ユーザーリスト, 312

フィルタリング

同期ユーザーリスト, 214

ユーザーリスト, 212

フェイルオーバーコントローラ、指定, 178

複数ドメイン, 311

複数のドメインコントローラ, 177

部分文字列フィルタ, 212

プライマリドメインコントローラ、「PDC」を参照

- プレゼンス
 - インデックス, 293
 - フィルタ, 212
- プレフィックス, 164
- フロー
 - 削除の指定, 208
 - デフォルト, 189
 - 変更の指定, 195
- ブローカ
 - Message Queue, 102
 - アクセス, 257
 - 起動, 239
 - 停止, 239
 - ポートの指定, 151
- プログラム, セットアップ, 218
- プロセス
 - ウォッチドッグ, 98
 - 軽量, 101
 - コネクタ, 101
 - コマンド行ユーティリティー, 99
 - コンソール, 99
 - システムマネージャー, 100
 - 設定ディレクトリ, 98
 - セントラルロガー, 100
- へ
- ベース DN
 - 説明, 209
 - 複数の SUL で使用, 212
 - ユーザーセットドメインの指定, 211
 - ユーザーセットドメインのベース DN の指定, 211
- ヘルプ, 使用情報, 286
- 変更
 - 設定パスワード, 287
 - デフォルトのスキーマソース, 186
- 変更検出, 102, 106, 111
- 変更検出機能サブコンポーネント, 102, 105, 122, 302
- 変更の検出, 101, 165
- 変更, フローの指定, 195
- 編集
 - ドメインコントローラ, 180, 182
- 編集 (続き)
 - ドメインコントローラ設定パラメータ, 180
 - マッピングされた属性, 194
- ほ
- ポート番号
 - Message Queue の指定, 150, 151
 - 設定ディレクトリ, 236, 298
 - デフォルト, 151
- 保護
 - 機密情報, 252
 - グローバルカタログ, 252
 - パスワード, 255
- ホスト
 - Active Directory, 173, 175
 - 指定, 173
- ホスト名
 - サーバーグループ, 157
 - 設定ディレクトリ, 236, 298
- ま
- マッピング
 - コネクタ ID からディレクトリソースへ, 266
 - 作成属性, 193
 - 属性, 126, 183, 194
- マルチマスターレプリケーション。MMR を参照, 317
- む
- 無効化, 195
- め
- メッセージ
 - audit.log, 271
 - debug.log, 271
 - error.log, 271
 - resync.log, 271

メッセージ (続き)

- コンポーネント用, 270
- セントラルロガーに記録, 270
- 同期イベント, 271

ゆ

有効化, 195

- SSL 通信, 147, 165, 168, 219, 262

ユーザー

- Active Directory で特殊, 238
- Active Directory に追加, 129
- NTSAM ドメイン, 233
- SUL の作成, 126
- 再同期, 296
- 削除, 208
- サブツリー, 113
- 識別名, 173
- 定義, 126
- ドメインのベース DN、指定, 211
- 認証の失敗, 111
- フィルタ, 312
- フィルタリング, 212
- リンク/同期, 113, 122, 135, 138, 183, 288

ユーザー DN

- 指定, 163, 173
- 例, 163, 173

ユーザーオブジェクトクラス, 135

ユーザーのリンク

- idsync resync の使用, 288
- XML 設定ドキュメントの使用, 297

ユーティリティ

- forcepwhchg, 302
- keytool, 257
- コマンド行, 99

よ

要件, 同期, 112

り

リセット

- コネクタの状態, 287, 295

リソース, 検索, 156

る

ルートサフィックス

- 指定, 147
- 説明, 134
- ディレクトリソースのラベル, 121
- デフォルト, 164

れ

例

- forcepwhchg コマンド, 302
- idsync certinfo コマンド, 288
- idsync changepw コマンド, 289
- idsync importcnf コマンド, 290
- idsync prepds コマンド, 293
- idsync printstat コマンド, 295
- idsync resetconn コマンド, 295
- idsync resync コマンド, 297
- idsync startsync コマンド, 301
- idsync stopsync コマンド, 301
- linkusers.cfg, 306-308
- linkusers-simple.cfg, 305-306
- prepds サブコマンド, 292
- resync の引数, 236
- XML 設定ドキュメント, 305
- 監査ログのパス, 279
- セントラルログ, 271
- ディレクトリソースエントリ, 220
- ユーザーセットドメインのベース DN, 211
- ログメッセージ, 273

レプリケーション

- 設定, 258, 318
- 単一のサフィックス, 317
- ユーザーの同期, 317

ろ

- ローカルログ, 271
 - コンポーネント, 271
 - セントラルロガー, 271
- ローカルログディレクトリ, 16
- ロール所有者、プライマリドメインコントローラ
FSMO, 177
- ロギング
 - resync.log の確認, 238
 - 正しくリンクされたユーザー, 238
- ログ
 - audit.log, 271
 - resync, 271
 - resync.log, 238
 - エラー, 100, 269, 271, 279
 - 監査, 100, 271
 - 監査ファイルとエラーファイル, 269
 - 形式, 273
 - セントラルログ, 270
 - ディレクトリサーバープラグイン, 272
 - デフォルトログディレクトリ/ファイルの指
定, 275
 - 場所, 270, 279
 - 表示, 224, 228, 230, 269
 - 毎日の運用, 269
 - 読み取り, 273
 - ローカル, 271
 - ローカルコンポーネントログ, 271-272
 - ローカルサブコンポーネントログ, 272
 - ログタイプ, 270
 - ログの表示, 224, 228, 230
 - ログレベルの指定, 274
- ログイン, 153
- ログディレクトリ, 270, 275
- ログの読み取り, 273

コ

- コネクタ
 - Windows NT, 229

