Sun Java™ System Identity Synchronization for Windows リリースノート

バージョン 1 2004Q3

Part No. 817-7853

このリリースノートには、Sun Java™ System Identity Synchronization for Windows 1 2004Q3 のリリース時点で判明している重要な情報が含まれています。ここでは、新機能、拡張機能、既知の制限事項と問題点、技術的な注意事項などについて説明します。Sun Java System Identity Synchronization for Windows 1 2004Q3 を使い始める前に、このリリースノートをお読みください。

このリリースノートに含まれる内容は、次のとおりです。

このリリースノートでは、サードパーティーの URL も示し、補足的な関連情報を提供しています。

注 Sun は、このリリースノートに記載されているサードパーティーの Web サイトにアクセス可能かどうかについて責任を負いません。また、Sun は、サードパーティーのサイトまたはリソースにおいて提供される、またはそれらのサイトやリソースを通して提供される、コンテンツ、広告、製品、または他の資料に関して、その内容を保証するものではなく、責任や義務を負うものではありません。さらに、サードパーティーのサイトまたはリソースにおいて提供される、またはそれらを通して提供される、コンテンツ、商品、またはサービスの使用またはそれらへの依存によって直接的、間接的に生じた、または生じたと主張される被害や損失に関しても、責任や義務を負いません。

改訂履歴

表 1　改訂履歴

日付	変更の説明
2004 年 9 月 30 日	このリリースノートの初回のリリース

Identity Synchronization for Windows 1 2004Q3 について

Identity Synchronization for Windows は、次のディレクトリ間における双方向のパスワード同期機能を提供します。

- Sun Java™ System Directory Server と Microsoft Windows 2000/2003 Active Directory
- Sun Java System Directory Server と Windows NT SAM レジストリ

Sun Java System Directory Server (Directory Server) と Windows 2000/2003 Active Directory との同期を取る場合、すべての Identity Synchronization for Windows コンポーネントを、Solaris™ Operating System および Windows 2000 Server オペレーティングシステム環境上にインストールして実行できます。Directory Server と Windows NT との同期を取る場合、Windows NT 環境下で Windows NT コンポーネントを実行する必要があります。

この節では次の内容を説明します。

このリリースの変更点

新機能

Identity Synchronization for Windows 1 2004Q3 の新機能は次のとおりです。

- **ユーザーの削除** : Sun Java System Directory Server と Sun Java System Active Directory との間で、双方向のユーザーエントリ削除同期を設定および有効化できるようになりました。
- **Active Directory のフェイルオーバー** : オンデマンド認証中のフェイルオーバー用として、追加の Active Directory サーバーを指定できるようになりました。この機能は、ユーザーのパスワードが Active Directory 上で変更された場合に、Active Directory 側でユーザーを認証するために Identity Synchronization for Windows Directory Server プラグインによって使用されます。バージョン 1.0 では、こうしたことは不可能でした。したがって、プライマリの Active Directory サーバーが利用できない場合、Identity Synchronization for Windows Directory Server プラグインから Active Directory へのパススルー認証が失敗し、Directory Server はユーザーを認証することができませんでした。なお、こうした状況になるのは、ユーザーが Active Directory 上でパスワードを変更後、初めて Directory Server に対して認証を試みた場合だけです。
- **Active Directory のユーザーオブジェクトクラス** : Active Directory スキーマ情報用の任意の適切なオブジェクトクラス (`User` またはその拡張) を使用できるようになりました (バージョン 1.0 の場合、使用できるのは `User` オブジェクトクラスだけでした)。
- **Windows 2003 Server Active Directory のサポート** : Identity Synchronization for Windows 1 2004Q3 をインストールして設定し、Windows 2003 Server Standard Edition または Enterprise Edition のプラットフォームで動作する Active Directory によってパスワードと属性の同期を取ることができます。
- **ユーザー同期用の追加オブジェクトクラスのサポート** : Auxiliary オブジェクトクラスと Structural オブジェクトクラスに含まれる属性に対し、属性マップを定義できるようになりました。Active Directory の場合、ユーザーがどのメインオブジェクトクラス / Structural オブジェクトクラスを選択するかによって、Auxiliary クラスセットが制約されます。Directory Server の場合、その他のオブジェクトクラスもすべて使用できます。
- **移行** : バージョン 1.0 またはバージョン 1.0 SP1 からバージョン 1 2004Q3 に移行できるようになりました。
- **Solaris 9 x86 プラットフォームのサポート** : Identity Synchronization for Windows は、Solaris 9 x86 プラットフォームを完全にサポートします。
- **linkusers コマンド行 と resync コマンド行の操作** : l linkusers コマンドの機能は、resync コマンドに移行されました。resync コマンド行には 3 つのオプションが追加されています。追加されたオプションは以下のとおりです。
  - `-f <linkusers.cfg>` -- ファイルのリンク (以前は `linkusers` コマンドで使用)
  - `-k` -- リンクユーザーのみ

- `-i NEW_LINKED_USERS` -- 新しくリンクされたユーザーのパスワードをリセット。これは、Directory Server 内でリンクされるユーザーを除いて、ALL_USERS および NEW_USERS オプションと同じです。

  この新機能についての詳細は、『Identity Synchronization for Windows インストールおよび設定ガイド』を参照してください。

注 Microsoft は、2004 年 12 月いっぱいで Windows NT のサポートを完全に終了 (End of life =EOL) する予定です。したがって、Identity Synchronization for Windows 1 2004Q3 では、Windows NT に関するバグの修正は行いますが、このプラットフォームに対する新機能のサポートは行いません。

詳細については、Windows ライフサイクルサポート (http://support.microsoft.com/default.aspx?scid=fh;[ln];LifeWin) を参照してください。

製品の変更

バージョン 1 2004Q3 リリースでは、製品に対して次のような変更がなされました。

- **インストール** : Sun Java Enterprise System 2 2004Q2 のインストール時には、Identity Synchronization for Windows 1 2004Q3 で必要となる Sun Java System Message Queue Enterprise Edition と Sun Java System Directory Server がインストールされます。したがって、Identity Synchronization for Windows 1 2004Q3 をインストールする前に、Solaris システム上に Sun Java Enterprise System をインストールする必要があります。

  以前の Identity Synchronization for Windows バージョン 1.0 では Sun Java System Message Queue 3.0.1 (Message Queue) がインストールされていましたが、バージョン 1 2004Q3 ではインストールされなくなりました。

- **製品とマニュアルのブランド名の変更** : Identity Synchronization for Windows 製品と製品マニュアルのブランド名が、Sun ONE Identity Synchronization for Windows から Sun Java System Identity Synchronization for Windows へと変わりました。

パフォーマンスの向上

同期のパフォーマンスが大幅に改善されました。

マニュアルの変更点

製品とマニュアルのブランド名の変更 : Sun Java System Identity Synchronization for Windows 製品と製品マニュアルのブランド名が、Sun ONE Identity Synchronization for Windows から Sun Java System Identity Synchronization for Windows へと変わりました。

ハードウェアおよびソフトウェアの要件

オペレーティングシステムの要件

このリリースの Identity Synchronization for Windows に対するオペレーティングシステムの要件を、以下の各表に示します。

表 2　Solaris の要件

コンポーネント	Solaris の要件
コアコンポーネント	Solaris 8™ UltraSPARC® 版 (32 ビットおよび 64 ビット) Solaris 9™ SPARC® Platform Edition (32 ビットおよび 64 ビット) Solaris 9™ Operating System (Pentium II 以降に対応した x86 Platform Edition) IA-32
Sun Java™ System Directory Server 用コネクタおよび Windows Active Directory 用コネクタ	Solaris 8 UltraSPARC 版 (32 ビットおよび 64 ビット) Solaris 9 SPARC プラットフォーム版 (32 ビットおよび 64 ビット) Solaris 9™ Operating System (Pentium II 以降に対応した x86 Platform Edition) IA-32
Sun Java™ System Directory Server プラグイン	Solaris 8 UltraSPARC 版 (32 ビットおよび 64 ビット) Solaris 9 SPARC プラットフォーム版 (32 ビットおよび 64 ビット) Solaris 9™ Operating System (Pentium II 以降に対応した x86 Platform Edition) IA-32

表 3　Windows の要件

コンポーネント	Windows の要件
コア	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4 Windows Server 2003 Standard または Enterprise Edition
Sun Java™ System Directory Server 用コネクタおよび Windows Active Directory 用コネクタ	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4 Windows Server 2003 Standard または Enterprise Edition
Sun Java™ System Directory Server プラグイン	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4 Windows Server 2003 Standard または Enterprise Edition
NT コネクタおよびプラグイン (サブコンポーネント)	Windows Primary Domain Controller NT 4.0 Server SP 6A (x86 用のみ)

表 3　Windows の要件 (続き)

コンポーネント	Windows の要件
Windows 2003 Standard および Enterprise Server 上の Active Directory と同期させる場合	Windows Server 2003 Standard Edition (最新のセキュリティ更新が施されたもの) Windows Server 2003 Enterprise Edition (最新のセキュリティ更新が施されたもの)

ハードウェアの要件

Identity Synchronization for Windows を実行するハードウェア (すべてのプラットフォーム) は、次の最低要件を満たしている必要があります。

- 約 400M バイトのディスク容量 (最小インストール時)
- Identity Synchronization for Windows コンポーネントが稼働するサーバーごとに最低 512M バイトの RAM (推奨 1G バイト)

Sun Java System ソフトウェアの要件

Identity Synchronization for Windows を実行するには、次の Sun Java System ソフトウェアコンポーネントをインストールする必要があります。

- Sun Java System Message Queue Enterprise Edition バージョン 3.5 SP1 (旧 Sun ONE Message Queue)

  Identity Synchronization for Windows をインストールする前に、Message Queue Enterprise Edition バージョン 3.5 SP1 をインストールしておく必要があります。さらに、Message Queue Enterprise Edition バージョン 3.5 SP1 のインストールは、Sun Java System Directory Server 5 2004Q2 のインストールに先だって行うことをお勧めします。

  Sun Java SystemMessage Queue がすでにインストールされた環境に Identity Synchronization for Windows コアをインストールする場合、その Message Queue は Message Queue Enterprise Edition 3.5 SP1 である必要があります。不適切なバージョンの Message Queue がインストールされた環境に Identity Synchronization for Windows コアをインストールしようとすると、同期時にエラーが発生します。

- Sun Java System Directory Server バージョン 5 2004Q2 以上

  Identity Synchronization for Windows 1 2004Q3 をインストールするには、Directory Server 5 2004Q2 (5.2 パッチ 2) を実行している必要があります。

  Solaris パッケージのインストールや適用するパッチの詳細については、『Sun Java System Directory Server 5 2004Q2 リリースノート』の「重要な情報」を参照してください。

  圧縮されたアーカイブ (ZIP) インストール、パッチの方法、zip アップグレードに含まれるバグの詳細については、『Sun One Directory Server 5.2 リリースノート』の「インストールに関する注意事項」を参照してください。

Directory Server 5.2 パッチ 2 で修正されるバグのリスト (重要なバグの修正) については次のリリースノートを、あるいはすべての適用されているパッチの個々の README を参照してください。「Sun Java System Directory Server 5 2004Q2 リリースノート」

配備環境内のすべての Directory Server マスター、レプリカ、およびハブ上に、Directory Server プラグイン (サブコンポーネント) をインストールする必要があります。

Directory Server 5 2004Q2 を Solaris 上にインストールする際に必要となるパッチの最新情報については、『Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide』および『Sun Java System Directory Server 5 2004Q2 リリースノート』を参照してください。これらは次の Web サイトから入手できます。

http://docs.sun.com/db/prod/entsys?l=ja
http://docs.sun.com/db/coll/DirectoryServer_04q2

- Sun Java System Directory Server 5 2004Q2 Retrochangelog のパッチ

  Identity Synchronization for Windows 1 2004Q2 の Deirectory Server Retrochangelog と削除機能の問題を修正するには、Sun Java System Directory Server 5 2004Q2 にパッチをインストールする必要があります。正確なパッチ番号は、システム環境によって異なります。

  - Solaris Sparc パッケージ形式 : パッチ番号 117907-02 以降
  - Solaris Sparc の圧縮されたアーカイブインストール : パッチ 5077789
  - Solaris X86 パッケージ形式 : パッチ番号 117908-02 以降
  - Solaris X86 の圧縮されたアーカイブインストール : パッチ 5077789
  - Windows の圧縮されたアーカイブインストール : パッチ 5077789

  これらのパッチおよび Directory Server 環境の更新方法の詳細については、次の Identity Synchronization for Windows ダウンロードディレクトリに格納されている `README.patch` ファイルを参照してください。
  `<download_root>/patches/directory/README.patch`

- Java Runtime Environment

  J2SE Java Runtime Environment (JRE) はこの製品には含まれていません。

  - Solaris または Windows Active Directory 上で Identity Synchronization for Windows インストーラを実行するには、JRE 1.4.2_04 (またはそれ以降) をインストールする必要があります。また、JRE よりも高いパフォーマンスを示す J2SE v 1.4.2_04 SDK をインストールすることも可能です。
  - Windows NT 上には、JRE 1.4.1_03 (またはそれ以降) をインストールする必要があります。

  また、Solaris の場合、Identity Synchronization for Windows をインストールする前に、`JAVA_HOME` を 1.4.2_04 JRE (またはそれ以降) に設定しておく必要があります。設定されていない場合は、インストーラにより、`JAVA_HOME` が設定されていない旨を知らせるメッセージが表示されます。

このリリースで修正されたバグ

次の表に、Identity Synchronization for Windows 1 2004Q3 で修正されたバグを示します。

表 4 Identity Synchronization for Windows 1 2004Q3 で修正されたバグ

バグ番号	説明
インストール / アンインストール	
4881466	既存の Message Queue インスタンスが 7676 以外のポート上に存在する状態でコアコンポーネントをインストールするとエラーが発生する
4829497	プログラムのアンインストール時に削除されないファイルやフォルダがある
4820869	Windows 上でコアコンポーネントを再インストールする際に、システムを再起動する必要がある
4916789	同じ Server_Root 上にインストールされたレプリカに対して重複した Directory Server プラグイン ID が生成される
5035406	Solaris ベースのマシン上で JDK の代わりに JRE を使用した場合、コアのインストールが失敗する
4880807	`runInstaller.sh` と `runUninstaller.sh` で -nodisplay オプションが使えない
5030928	インストールプログラムが、プライマリホストとフェイルオーバーホストで別々のクレデンシャルをサポートできない
5037157	「DS プラグインのみ」のインストールを実行した場合、アンインストールスクリプトが存在しない
5050554	インストールプログラムを -nodisplay モードで開始するには変数 DISPLAY が必要
4915192	SSL 専用の Directory Server 上にコネクタをインストールできない
5052509	テキストベースのアンインストールスクリプトの実行時に削除されない Identity Synchronization 関連パッケージが存在する
4937341	Windows ベースのシステムで、追加 / 削除オプションを使用して Identity Synchronization for Windows をアンインストールできない
5056685	NT プラグインアンインストールプログラムによって、パスワードフィルタ DLL を削除できない。パスワードフィルタ DLL は、Windows が起動時に DLL を読み込まないようにして、確実に DLL が削除されるようにするために必要。これにより、コンポーネントの再インストール時に問題が発生した
4988901	インストールプログラムのパネルの中には、「戻る」ボタンをクリックすると正しいパネルを表示しないものがあった
5030567	NT コネクタのインストール時に、NT コネクタのすべてのサブコンポーネントがインストール済みであることを示すテキストを、インストールプログラムが正しく表示しない

表 4　Identity Synchronization for Windows 1 2004Q3 で修正されたバグ (続き)

バグ番号	説明
5036330	インストール時に、「ドメインを管理する組織名など、管理ドメインを表す一意の名前を入力してください。」フィールドのデフォルト値を変更すると、インストールの操作に失敗する
5041518	サブコンポーネントのインストール時に「戻る」ボタンを押すと、コネクタポートパネルにエラーメッセージが表示される
5048953/ 5049733	JAVA_HOME 値に引用符が含まれていると、アンインストールの操作に失敗する
5050691	コアのインストール時に、システムにインストールされている MQ バージョンに関して誤ったメッセージが、MQ 設定ウィンドウに表示される。「null」表示
5057716	プラグインが正常にアンインストールされても、Directory Server のプラグインパッケージやそのレジストリエントリがシステムから削除されない
5071574	Directory Server コネクタの有効なポート番号 65535 が受け入れられない
5079602	nt_dll_registrar によって Notification Packages が強制的に REG_MULTI_SZ にならない
パスワード同期	
4845844	`idsync resync` コマンドによる Directory Server から NT への同期時に、ユーザーの作成が失敗する
4937502	ネットワーク接続が頻繁に切断されると、コネクタが同期を停止することがある
4939825	Directory Server コネクタが変更済みエントリのループ検出属性を削除しない
4906752	Sun Directory Server 上で modrdn 処理の直前に作成されたユーザーが同期されない
4933861	合成属性が使用された場合、「idsync resync -c -o Sun」実行後の同期開始時に NT コネクタが過剰な動作を示す
4941200	ユーザーエントリの名前を変更しても、変更されたのが大文字と小文字の違いだけであった場合、それらのエントリは同期されない
4893525	Active Directory サーバーへのネットワーク接続が切断されると、属性の変更結果が失われる
5019327	同期オブジェクトクラスタイプのサブクラスをオブジェクトクラスに持つユーザーが、Directory Server コネクタによって同期される
4995351	Identity Synchronization for Windows による属性のマッピングが正しくない
5036025	SUL を変更してからユーザーを同期しようとすると、NullPointerException エラーがログファイルに記録され、コネクタが応答を停止する
5054654	コネクタがリセットされたり異常終了したりすると、NT のパスワードに対する変更内容が失われる
Sun Java System Message Queue	

表 4　Identity Synchronization for Windows 1 2004Q3 で修正されたバグ (続き)

バグ番号	説明
4881240	Solaris 上でユーザーディレクトリ内にインストールした場合、既存の Message Queue を使用できない
一般	
4943564 / 4939730	*Userpassword* が省略可能な属性ではない
4994145	Directory Server プラグインから利用不可能なホストへの接続テストの回数が多すぎる
5041435	「パスワードの履歴を保持」オプションを有効にした状態でオンデマンドパスワード更新を実行すると、Directory Server が応答しなくなる
4939859	ソースコネクタが Windows NT である場合、idsync linkusers/resync 実行時に LDAP フィルタオプションが無視される
4987742	競合のため、`resync` によって処理されないエントリが存在する
5048362	ログメッセージ内の改行文字が自動的に削除されない
4925575	Active Directory コネクタのインストーラが、対象ドメインが証明書ドメインに一致するかどうかをチェックしない
4901486	Identity Synchronization for Windows 1 2004Q3 では、複数の Active Directory フォレストをサポートしていなかった
コンソール関連一般	
5040094	「objectclass=< 特定のオブジェクトクラス >」から無効なフィルタエラーが報告される
5030704	Active Directory ソースの `resync` 間隔をコンソールから変更できない
5026929	必須の作成属性にデフォルト値を指定できない
4941238	ログビューアによるログレコードのパースが正しくない
5008697	cn マッピングを編集すると、既存の項目が更新されずに別の項目がリスト追加される
50134407	既存のディレクトリソースと同じ名前のディレクトリソースが作成される。エラーメッセージが表示されず、ディレクトリソースを削除できない
5026198	コンソールのログウィンドウにあった誤植が修正されている
5044529	SSL のみの Directory Server でコンソール prepds が動作しない
5045350	既存の作成属性を変更する場合に、値を <none> に設定できない
4921889	「表示」から「ツリー」オプションを再び選択すると、コンソールが通常のツリーに正しく表示されない
コネクタ	
4988028	見つからない未変更属性で Java Run Time Exception (RTE) が発生する

表 4　Identity Synchronization for Windows 1 2004Q3 で修正されたバグ (続き)

バグ番号	説明
コマンド行ユーティリティ	
5015766	idsync changepw に空のパスワードを渡すと、それ以降設定レジストリにアクセスできなくなる
4986303	-h、-p、-D、-s の各オプションに対するデフォルト値が、コマンド行インタフェースによって提供されない
5038195	設定サフィックスが無効な場合に resetconn から出力されるエラーメッセージが不適切である
5019543	設定サフィックスが無効な場合に printstat から出力されるエラーメッセージが不適切である
5024148	resetconn 実行時にコネクタの Message Queue クレデンシャルが削除されない
4941125	ソースが Sun で合成属性が同期された場合、resync によって同期ユーザーが更新される
4939484	linkusers コマンドが終了しない場合がある
5015575	コマンド行プロンプトで c コマンドを実行すると、CLI 処理が停止しない
5062028	SSL によってコアをインストールすると、コマンド行プロンプトが応答しなくなる。CLI のポートのデフォルト値が SSL ポートだった

重要な情報

ここでは、コア製品マニュアルに記載されていない最新情報を提供します。ここで説明する内容は次のとおりです。

インストールに関する注意事項

Identity Synchronization for Windows 1 2004Q3 をインストールする前に、『Sun Java™ System Identity Synchronization for Windows 1 2004Q3 インストールおよび設定ガイド』の章「インストールの準備」を必ずお読みください。

Windows 2003 Server の使用

- Windows 2003 Server Standard Edition または Enterprise Edition をプラットフォームとして使用して、Identity Synchronization for Windows 1 2004Q3 をインストールおよび設定することができます。
- Windows 2003 Server のデフォルトのパスワードポリシーは Windows 2000 のものとは異なり、厳格なパスワード入力を要求します。

Windows 2003 Server の問題点

「ユーザーは次回ログオン時にパスワード変更が必要」に対する Windows 2003 Server の動作が、Windows 2000 の動作と異なる (*4997513*)

Windows 2003 では Windows 2000 の場合と異なり、「ユーザーは次回ログオン時にパスワード変更が必要」フラグがデフォルトで設定されます。

Windows 2000/2003 上で「ユーザーは次回ログオン時にパスワード変更が必要」フラグを設定した状態でユーザーを作成すると、ユーザーがパスワードなしで Directory Server に作成されます。それらのユーザーは、次回 Active Directory にログインする際、パスワードの変更を強制されます。これにより、Directory Server 上のパスワードが無効になり、それらのユーザーが次回 Directory Server への認証を行う際にオンデマンド同期が強制実行されます。

ユーザーは、Active Directory 上でパスワードを変更するまで、Directory Server への認証を行えません。

互換性の問題

特定のリモートコンソール製品を使用して Identity Synchronization for Windows コンソールにアクセスする場合に、互換性の問題が発生する (*5077227*)

PCAnywhere 1.0.x または Remote Administration 2.1 を使用して Identity Synchronization for Windows コンソールを表示しようとするときに、問題が発生する場合があります。PCAnywhere バージョン 9.2 の場合はエラーが発生しません。問題が解決されない場合は、リモート管理ソフトウェアを削除してください。それとは別に、VNC を使用して Identity Synchronization for Windows コンソールを表示可能な場合に、何らかの問題が発生するかどうかについては判明していません。

システムまたはアプリケーションで障害が発生した場合のデータ復元の実行

ハードウェアまたはアプリケーションで障害が発生すると、同期されているディレクトリソースのいずれかにあるバックアップからデータを復元する必要が生じることがあります。

また、データ復元が完了したあとで追加の手順を実行し、同期処理が通常どおり確実に実行されるようにする必要も生じます。

一般的にコネクタには、Message Queue に伝播された最後の変更に関する情報が保持されています。

コネクタ状態と呼ばれるこのデータは、コネクタがディレクトリソースから次に読み込む必要のある変更点を判別するために使用されます。同期されたディレクトリソースのデータベースをバックアップから復元する場合、コネクタ状態は無効になります。

Active Directory や Windows NT などの Windows ベースのコネクタも、内部データベースを保持しています。このデータベースは、同期されたデータソースのコピーであり、接続されているデータソースでの変更点を判別するために使用されます。内部データベースは、Active Directory ソースまたは Windows NT システムが一旦バックアップから復元されると有効でなくなることは、容易に見分けられます。

通常は、`idsync resync` コマンドを使用して、復元されたデータソースにデータを再び格納することができます。

注	再同期機能は、1 つの例外を除いて、パスワードの同期に使用することはできません。再同期データソースが Windows の場合には、`-i ALL_USERS` オプションを使用して、Sun Java Systems Directory Server システムのパスワードを無効にすることができます。また、SUL リストには Active Directory システムのみが含まれます。

ただし特定の状況では、`idsync resync` コマンドを使用できない場合があります。

警告 以下の手順を実行する前に、同期機能が停止していることを確認してください。

双方向同期

推奨されている手順では、同期設定に従って適切な修飾子を指定し、idsync resync コマンドを使用します。resync 操作のターゲットは、復元されたディレクトリソースにしてください。

一方向同期

復元されたデータソースが同期先である場合は、双方向同期の場合と同じ手順に従って操作することができます。

復元されたデータソースが同期元である場合でも、idsync resync コマンドを使用して、復元されたディレクトリソースにデータを格納することができます。Identity Synchronization for Windows 設定の同期フロー設定値を変更する必要はありません。これは、-o <Windows|Sun> オプションを指定して idsync resync コマンドを使用することにより、設定済みのフローに依存せずに同期フローを設定できるからです。

例として、以下の状況を参考にしてください。

Sun Java Systems Directory Server と Active Directory の間に双方向同期をセットアップします。

- Microsoft Active Directory サーバーのデータベースは、バックアップから復元する必要がある
- Identity Synchronization for Windows で、この Active Directory ソースを SUL 'AD' 用に設定する
- この Active Directory ソースと Sun Directory Server ソースの間に、変更、作成、および削除の場合の双方向同期をセットアップする

1. 同期を停止します。idsync stopsync -w - -q -
2. Active Directory ソースを再同期し、変更、作成、および削除を再同期します。idsync resync -c -x -o Sun -l AD -w - -q -
3. 同期を再開します。idsync startsync -w - -q -

ディレクトリソースに特定の復元手順

Microsoft Active Directory

バックアップから Active Directory を復元可能な場合は、「双方向同期」と「一方向同期」のセクションで説明されている手順に従って操作します。

ただし、重大な障害が発生したあとは、異なるドメインコントローラを使用する必要が生じることもあります。この場合は、以下の手順に従って Active Directory コネクタの設定を更新します。

1. Identity Synchronization for Windows 管理コンソールを起動します。

2. 「設定」タブを選択します。
3. ディレクトリソースノードを展開します。
4. 適切な Active Directory ソースを選択します。
5. 「コントローラの編集 (E)」をクリックします。
6. 新しいドメインコントローラを選択します。

   選択したドメインコントローラは、ドメインの NT PDC FSMO ロール所有者にすることをお勧めします。
7. 設定を保存します。
8. Active Directory コネクタが実行されているホストで、`Identity Synchronization` サービスを停止します。
9. `<serverroot>/isw-<hostname>/persist/ADPxxx` の下にあるディレクトリを除いたすべてのファイルを削除します。`xxx` は、Active Directory コネクタの識別子で、Active Directory コネクタ識別子が CNN100 であれば 100 になります。
10. Active Directory コネクタが実行されているホストで、`Identity Synchronization` サービスを起動します。
11. 「双方向同期」または「一方向同期」のセクションにある同期フローに基づくステップに従います。

Sun Java System Directory Server

Retro Changelog データベースまたはユーザーが同期されるデータベースのいずれか、またはその両方は、重大な障害によって影響を受ける可能性があります。

1. Retro-Changelog データベース

   Retro-Changelog データベースには、Directory Server コネクタで処理できなかった変更点が存在する可能性があります。Retro Changelog データベースを復元することが必要なのは、バックアップに未処理の変更点が含まれている場合のみです。この場合のデータベースの復元は、`<serverroot>/isw-<hostname>/ADPxxx/accessor.state` ファイルの最新のエントリを、バックアップの最後の変更番号と比較することによって行われます。accessor.state の値がバックアップの変更番号以上の場合は、データベースを復元することは不要ですが、データベースを作成し直します。

   Retro-Changelog データベースを作成したら、必ず `idsync prepds` を実行するか、Identity Synchronization for Windows 管理コンソールの「Sun ディレクトリソース」ウィンドウで、「Directory Server の準備」をクリックしてください。

   Directory Server コネクタは、Retro-Changelog データベースが作成し直されていることを検出し、警告メッセージをログに記録します。このメッセージは無視しても安全です。

2. 同期されたデータベース

   同期されたデータベース用に使用可能なバックアップがない場合は、Directory Server コネクタを再インストールする必要があります。

   バックアップから同期されたデータベースを復元可能な場合は、「双方向同期」と「一方向同期」のセクションで説明されている手順に従って操作します。

Identity Synchronization for Windows 1 2004Q3 のマニュアルの更新

Identity Synchronization for Windows のオンラインマニュアルファイルにはブラウザ経由でアクセスできます。さらに、マニュアルセット全体を HTML 形式でダウンロードすることも可能です。

このファイルをダウンロードしたあと、中身を抽出して次の場所に格納します。

```
<ServerRoot>/manual/en/isw
```

ServerRoot は Sun Java System 管理サーバーの場所を表します。ServerRoot の実際のパスは、プラットフォーム、インストール、および設定に応じて異なります。ServerRoot ディレクトリには、`startconsole` プログラムが含まれています。

マニュアルセットには、*<ServerRoot>*`/manual/en/isw/index.html` から直接アクセスするか、サーバーコンソールの「ヘルプ」メニューから「ドキュメントホーム」を選択します。

ファイアウォール環境での Identity Synchronization for Windows の実行

Identity Synchronization for Windows は、ファイアウォール環境内でも実行できます。ここでは、どのサーバーポートをファイアウォール経由で公開すべきかについて、次の各節で説明します。

- Message Queue の要件
- インストーラの要件
- コアコンポーネントの要件
- コンソールの要件
- コネクタの要件
- Directory Server プラグインの要件

Message Queue の要件

Message Queue は、ポートマッパーを除くすべてのサービスで動的ポートをデフォルトで使用します。Message Queue ブローカにファイアウォール経由でアクセスするには、ブローカがすべてのサービスで固定ポートを使用する必要があります。

コアのインストール後、`imq.<service_name>.<protocol_type>.port` ブローカ設定プロパティを設定する必要があります。具体的には、`imq.ssljms.tls.port` オプションを設定する必要があります。詳細については、『Sun Java™ System Message Queue 管理ガイド』を参照してください。

インストーラの要件

Identity Synchronization for Windows のインストーラは、設定ディレクトリとして機能するディレクトリサーバーと通信できる必要があります。

- Active Directory コネクタをインストールする場合、インストーラは、Active Directory の LDAP ポート (ポート 389) にアクセスできる必要があります。
- Directory Server コネクタまたは Directory Server プラグイン (サブコンポーネント) をインストールする場合、インストーラは、Directory Server の LDAP ポート (デフォルトポート 389) にアクセスできる必要があります。

コアコンポーネントの要件

Message Queue、システムマネージャ、およびコマンド行インタフェースは、Identity Synchronization for Windows の設定情報が格納されている Directory Server にアクセスできる必要があります。

コンソールの要件

Identity Synchronization for Windows コンソールは、次の各ソフトウェアにアクセスできる必要があります。

- Active Directory (LDAP (ポート 389) または LDAPS (ポート 636) 経由)
- Active Directory グローバルカタログ (LDAP (ポート 3268) または LDAPS (ポート 3269) 経由)
- 各 Directory Server (LDAP または LDAPS 経由)
- Sun Java System 管理サーバー
- Message Queue

コネクタの要件

どのコネクタも必ず、Message Queue と通信できる必要があります。さらに次の条件を満たす必要があります。

- Active Directory コネクタは、LDAP (ポート 389) または LDAPS (ポート 636) 経由で Active Directory ドメインコントローラにアクセスできる必要があります。

- Directory Server コネクタは、LDAP (デフォルトポート 389) または LDAPS (デフォルトポート 636) 経由で Directory Server にアクセスできる必要があります。

Directory Server プラグインの要件

各 Directory Server プラグインは、Directory Server コネクタのインストール時に選択されたコネクタのサーバーポートにアクセスできる必要があります。Directory Server マスターレプリカ内で動作するプラグインは、Active Directory の LDAP (ポート 389) または LDAPS (ポート 636) に接続できる必要があります。その他の Directory Server レプリカ内で動作するプラグインは、マスター Directory Server の LDAP ポートまたは LDAPS ポートにアクセスできる必要があります。

既知の問題点と制限事項

ここでは、Identity Synchronization for Windows 1 2004Q3 に関する既知の問題点を列挙します。次の製品領域をカバーします。

インストールとアンインストール

製品のレジストリを手動で確定するための指示 (*5050004*)

製品のレジストリから Identity Synchronization for Windows への参照を削除する必要がある場合は、『Identity Synchronization for Windows インストールおよび設定ガイド』の第 7 章「アンインストールが失敗した場合の対応」で説明されている Windows NT および Windows 2000 プラットフォーム用の手順を使用してください。

名前に空白が含まれるディレクトリ内にコアをインストールした場合、Solaris スクリプトが正しく動作しない (*4801643*)

パス名に空白が含まれるディレクトリ内に Identity Synchronization for Windows コアをインストールした場合、Solaris 上のコマンド行スクリプトが正しく動作しません。

ベース DN に空白が含まれていると Message Queue ブローカが起動できない (*4892332* および *4892490*)

空白を含むサフィックス上にコアをインストールすると、Message Queue ブローカが認証に失敗します。

Message Queue インスタンスがすでに存在している環境にコアをインストールした場合の副作用 (*4882194*)

Message Queue ブローカインスタンスがすでに存在している環境にコアをインストールすると、その既存のインスタンスが影響を受ける可能性があります。
たとえば、既存の設定が次のように変更されます。

- `/etc/imq/imqbrokerd.conf` ファイルが変更され、スタートアップ時にブローカが自動的に起動するようになりますが、これにより、`/etc/init.d/imq` スクリプトから起動されるほかのブローカインスタンスがリブート時に起動されなくなります。

Message Queue ブローカ用に最低 512M バイトのメモリーが必要 (*4819519*)

Message Queue ブローカは最低 512M バイトのメモリーを必要とします。ブローカはコアの一部としてインストールされるため、コアをインストールするマシンには少なくとも 1G バイトの RAM が搭載されている必要があります。

マルチ Directory Server インスタンスインストール環境でプラグインをアンインストールしようとすると、アンインストーラが削除される (*4916035*)

2 つの Directory Server インスタンスがファイルシステム上で同じインストールルートを共有している場合は、複数のプラグインをアンインストールできません。たとえば、`/usr/sunone/servers/slapd-foxhead` と `/usr/sunone/servers/slapd-foxhead2` を共有している場合などです。

回避策

1. プラグインのインストール先 Directory Server の Directory Server コンソールを開きます。
2. 「設定」タブをクリックします。
3. `Plugins` フォルダをダブルクリックしてプラグインツリーを展開します。
4. `pswsync` をクリックし、「プラグインを有効に」チェックボックスをオフにします。
5. Directory Server を再起動します。

インストールを途中で取り消した場合、再インストール時に Active Directory コネクタの動作を決定できなくなる (*5038905*)

コネクタの設定中にインストールプログラムを取り消した場合、インストールプログラムを再度実行した際にコネクタのインストールオプションが利用できなくなります。

回避策
コマンド行プロンプトから `idsync resetconn` を実行してコネクタの設定をリセットしたあと、インストーラを再度実行してコネクタをインストールし直します。`idsync resetconn` コマンドの実行方法の詳細については、『Sun Java System Identity Synchronization for Windows インストールおよび設定ガイド』を参照してください。

製品をアンインストールしても関連するレジストリキーが削除されない (*5045237*)

コアのアンインストールを実行しても、製品レジストリファイル内の Sun Java System Identity Synchronization for Windows 関連ノードが削除されません。製品を再インストールできるようにするには、それらのノードを製品レジストリキーから手動で削除する必要があります。これらの製品レジストリキーの削除方法の詳細については、『Identity Synchronization for Windows インストールおよび設定ガイド』を参照してください。この状況は、Solaris 8 でのみ発生します。

設定レジストリに接続しないでコアをアンインストールした場合、コンソール内に Identity Synchronization for Windows 関連の参照が表示される (*5049700*)

Identity Synchronization for Windows のブラインドアンインストール (設定レジストリに接続しないアンインストール) を実行したあとコンソールを起動すると、エラーメッセージが表示されます。

インストールログが記録される Temp ディレクトリが隠しディレクトリになっていることがある (*5051905*)

Window システムによっては、`C:¥ Documents and Settings > Administrator > Local Settings` フォルダが隠しフォルダになっている場合があります。

回避策

`Local Settings` フォルダと `Temp` サブフォルダを表示するには、Windows Explorer のオプション「すべてのファイルとフォルダを表示する」を選択する必要があります。あるいは、コマンドプロンプトから `cd %TEMP%`、`cd %TMP%` のいずれかを入力することで、そのディレクトリ内のインストール関連のログファイルを表示します。続いて、メモ帳を使ってログを表示します。

ルートサフィックスに空白が含まれていると、Message Queue ブローカへの認証が失敗する (*4892903*)

Identity Synchronization for Windows の設定は、空白を含まないルートサフィックス内に格納する必要があります。これは、Message Queue の制限事項です。

回避策

コアをインストールする前に、Identity Synchronization for Windows 設定格納用の新しいルートサフィックスを作成します。

Directory Server のプラグインのインストールに失敗したあとに、そのプラグインのインストールが完了したことを示す予定表が表示される (*5081912*)

特定の状況では、プラグインのインストールに失敗しているにもかかわらず、Directory Server のプラグインがインストールされたことを示す予定表が表示されることがあります。

コネクタのアンインストール時に、アンインストールプログラムによって復元されるディスク容量が正確に表示されない (*5081823*)

アンインストールプログラムは、コネクタをアンインストールする際に、アンインストール手順後に復元されるバイト数を 0 バイトとして不正確に表示します。ディスク容量のプロパティを表示すると、復元される実際のディスク容量はゼロではないことが分かります。

インストールプログラムにより、Directory Server のプラグインインストールディレクトリが配置されているのと同じディレクトリにコンポーネントが強制的にインストールされない (*5080178*)

その Directory Server プラグインがマシンにインストールされる最初のコンポーネントになる場合は、その特定のマシンに続いてインストールされるすべてのコンポーネントは、Directory Server のプラグインと同じインストールディレクトリにインストールされる必要があります。ただし、インストールプログラムによってこの基準が強制的に履行されるわけではありません。

アンインストールプログラムが、コンポーネントをアンインストールする際に不正確な情報を表示することがある (*5079489*)

コアコンポーネントがインストールされていないマシンからコネクタをアンインストールすると、インストーラは、コアコンポーネントをアンインストールしているかのように誤って報告します。このメッセージは無視してかまいません。設定ディレクトリが存在しない状態でアンインストール手順が実行されると、Identity Synchronization for Windows コンソール参照が削除されない (*5077156*)

設定ディレクトリのない製品をアンインストールするオプションを選択すると、Sun サーバーコンソールは、Identity Synchronization for Windows コンソールへのすべての参照を保持します。製品をアンインストールしたあとでも、Identity Synchronization for Windows のアイコンがトポロジツリー内に存在し続けます。しかし、コンソールを表示しようとするとエラーが発生します。コンソールの参照を削除する方法については、『Identity Synchronization for Windows インストールおよび設定ガイド』第 8 章のセクション「コンソールの手動アンインストール」を参照してください。

アンインストールしても、server-root/isw-*lib ディレクトリと jar ファイルが削除されない (*5038284*)

アンインストールの操作を実行しても、`*.jar` ファイルを含む `lib` ディレクトリは削除されません。これらのファイルとディレクトリは手動で削除する必要があります。

インストール操作を取り消してから、再インストールすると Active Directory コネクタの動作を決定できなくなる (*5038905*)

Active Directory コネクタのインストール時にインストール操作を突然取り消してから、再インストールを試みると、Active Directory コネクタは「インストール済み」という誤ったステータスを表示します。このステータスは変わらず、同期操作は行われず、また試みられても Active Directory コネクタの再インストールは可能ではありません。

回避策

`idsync resetconn` コマンドを実行して、コネクタを再インストールする必要があります。`idsync resetconn` コマンドの実行方法の詳細については、『Identity Synchronization for Windows インストールおよび設定ガイド』を参照してください。

Sun Java Enterprise System 3 でインストールされた Directory Server 5.2p3 への Identity Synchronization for Window のインストールは失敗する (*5092530*)

コア Identity Synchronization for Windows 製品を Directory Server 5.2 P3 以降に対してインストールすることはできません。Identity Synchronization for Windows 1 2004Q3 は、Sun Java Enterprise System 3 (Directory Server 5.2 P3) をデータの同期元としてのみサポートします。

インストールリストが、インストール後にも Directory Server のプラグインを二次マスターにインストールするように求める (*5096593*)

予定表はほとんどの場合正確ですが、必要な手順を報告しなかったり、いくつかの手順が実行済みであることを認識しない場合があります。たとえば、予定表がどの Directory Server プラグインがインストールされているか、あるいはインストールする必要があるかを常に反映しているとは限りません。

FAT32 システムにインストールされた Identity Synchronization for Windows に ACL がない (*5097751*)

FAT32 フォーマットのドライブに Identity Synchronization for Windows をインストールした後に、フォルダやファイルに対する ACL をチェックすると、ACL が存在しないことがわかります。NTFS でないパーティションにインストールするのを避けることをお勧めします。

プラグインのみのアンインストールは、Directory Server の zip バージョンを使用しているときには失敗することがある (*5101589*)

プラグインのみのアンインストール操作の実行を試みるときに、Directory Server の圧縮されたアーカイブパッケージを使用していると、この操作は失敗します。

入力が求められるとき複数バイトの管理者名を使用すると、インストールの操作に失敗する (5109332)

コアインストール中に入力が求められる場合、複数バイトの LDAP 管理者名を入力すると、インストール操作に失敗します。「インストーラはスキーマファイル /var/opt/isw/SUNWisw/misc/40so-psw.out.ldif をアップロードできません。詳細については、インストーラのログファイルを確認してください。」というエラーメッセージが表示されます。インストールプロセスは停止し、ダイアログボックスウィンドウが突然終了します。

回避策

インストール操作の際には、デフォルトの「admin」LDAP 管理者名を使用してください。前回、インストールに失敗している場合には、インストールプログラムを再起動してからデフォルトの管理者名を使用してコアをインストールし直します。「Core files have been found on your machine」というメッセージが表示されます。このメッセージは無視しても問題ありません。操作を継続しインストールを完了することができます。

コネクタとプラグイン

既存のエントリを削除すると NT コネクタの同期が開始される (*4864009*)

既存の Windows ユーザー (Active Directory または NT) が存在する環境でインストールを行った場合、同期を開始する前に `idsync resync` コマンドを実行する必要があります。これにより、任意のタイミングで既存の Windows ユーザーが Directory Server に同期されるなどの不測の動作を防止できます。

コネクタが無効になった場合、コネクタを起動し直す (*4938309*)

セントラルエラーログで「`No response from connector [CNN100] for 10 minutes`」のようなメッセージが報告された場合、コネクタが稼働している Identity Synchronization for Windows デーモン / サービスを停止および再起動する必要があります。

回避策

- Solaris の場合、`/etc/init.d/isw stop` コマンドを実行したあと、`/etc/init.d/isw start` コマンドを実行します。
- Windows の場合、Sun Java System Identity Synchronization for Windows サービスを再起動します。

Directory Server プラグインの SSL を使用可能にしたあと Directory Server を再起動する (*4944804*)

Directory Server プラグイン (サブコンポーネント) の SSL (Secure Sockets Layer) を有効にし、Active Directory CA 証明書を Directory Server の証明書データベースに追加したあと、Directory Server を再起動する必要があります。再起動しなかった場合、Active Directory 上でパスワードが変更されたユーザーを認証する際に、オンデマンド同期が失敗します (サンプルのログメッセージを参照)。

Active Directory で検索タイムアウトが発生した場合、管理者は検索の制限時間を増やす必要がある (*4881182*)

Active Directory のエラーログにコネクタの検索タイムアウトエラーが含まれていた場合、Windows 2000 リソースキットの `ntdsutil` を使って、最大検索タイムアウト値を次のようにして増やしてください。

```
C:idif>ntdsutil
ntdsutil: ldap policies
ldap policy: connections
server connections: set creds example.sun.com administrator password
server connections: connect to server matar
Binding to matar as user(administrator) in domain(example.sun.com) ...
Connected to matar as user(administrator) in domain(example.sun.com) ...

server connections: quit
ldap policy: show values

Policy                          Current(New)

MaxPoolThreads                  4
```

```
MaxDatagramRecv              1024
MaxReceiveBuffer             10485760
InitRecvTimeout              120
MaxConnections               5000
MaxConnIdleTime              900
MaxActiveQueries             20
MaxPageSize                  1000
MaxQueryDuration             120
MaxTempTableSize             10000
MaxResultSetSize             262144
MaxNotificationPerConn       5
```

```
ldap policy: Set InitRecvTimeout to 2400
ldap policy: Commit Changes
```

;binary サブタイプを指定せずに作成されたバイナリ値属性は、Sun Java System Directory Server によって処理されない (*5029226*)

`userCertificate` などいくつかの属性は、作成時に ;binary オプションを必要とします。Identity Synchronization for Windows は、そのような属性の値を同期することはできますが、作成時に ;binary オプションを設定しません。このため、Sun Java System Directory Server と通信するクライアントで問題が発生する可能性があります。バイナリオプションを指定せずに作成された属性を、クライアントがバイナリオプション付きで要求した場合、Sun Java System Directory Server はそのような属性を返しません。

Identity Synchronization for Windows は、user_name 属性の作成時に使用される文字数を検証しない (*5021886*)

NT SAM では、user_name 属性で使用できる最大文字数は 20 文字ですが、Sun Java Directory Server では、ユーザー名の文字数に制限はありません。したがって、NT SAM から Sun Java Directory Server への同期は正常に処理されますが、NT SAM 上の user_name 属性にマッピングされたエントリは使用できません。NT SAM 上でエントリのプロパティを編集または表示する際に、エラーメッセージが表示されます。

コンソールとコマンド行

更新履歴ログデータベースファイルが再作成、破壊、または削除された場合、`idsync prepds` を実行する (*4921114* および *4832355*)
更新履歴ログ (Retro Change Log、RCL) データベースが削除または破壊された場合、Directory Server または Directory Server コネクタから警告メッセージが発行されます。そのようなメッセージが表示された場合、更新履歴ログを再作成し、`idsync prepds` コマンドを再実行しないと、同期が再開されません。

新しいネーミングコンテキストを選択しても、ベース DN に対する「ブラウズ」ボタンの選択肢が変わらない (*4944711*)
Identity Synchronization for Windows が 2 つ以上の Directory Server ソースと 3 つ以上の Active Directory (AD) ソースを使用するようにコンソールから設定した場合、新しい同期ユーザーリスト (Synchronized Users List、SUL) を設定する際に、ベース DN に対する「ブラウズ」ボタンの選択肢が、適切な Directory Server ソースまたは Active Directory ソースを正しく反映していない場合があります。

回避策
「ベース DN」フィールドにベース DN 名を手動で入力します。

コンソールスキーマホストは設定ディレクトリをポイントする必要がある (*4877996*)
スキーマホストを指定する場合、コア設定ディレクトリのみを使用することをお勧めします。スタンドアロンの Directory Server やリモートにあるほかの設定ディレクトリを使用しないでください。

コンソールの状態ウィンドウがログファイル表示用に 508 アクセシビリティを提供しない (*4874361*)
コンソールの状態ウィンドウのログファイルビューアに、マウスを使わないログファイル表示インタフェースが用意されていません。

回避策
ログファイルを表示するには、それらのファイルを好みのテキストエディタ (コンソールのログビューアの外側) にコピーします。

コンソール上の Message Queue の状態がシステムコンポーネントの実際の状態を正しく示していない (*4937312*)
コンソールと Message Queue ブローカ間のネットワーク接続が切断された場合、コンソール上に表示されたシステムコンポーネントの状態が正しくない可能性があります。

回避策
ネットワークで障害が発生した場合、必ずコンソールを再起動してください。また、`idsync printstat` コマンドを実行することで、Message Queue のより正確な状態を表示させることも可能です。

新しい Directory Server データソースを追加すると、その Directory Server がすでに準備済みであるにもかかわらず、その Directory Server の準備を求めるメッセージが表示される (*5029558*)

新しい Sun Java System Directory Server ソースを作成するたびに、その Directory Server ソースを準備するように求められます。そのディレクトリソースがすでに準備済みである場合、「いいえ」オプションをクリックしてかまいません。

CLI コマンド resetconn を実行すると、「リセットしています ...」というメッセージが表示され、パスワードのリセット処理が失敗し、設定情報など Directory Server ソースに関するすべての情報が削除される (*5039655*)

`resetconn` コマンド行機能の実行時にコンソールが動作していてはいけません。このコマンドの実行前にコンソールを終了しなかった場合、「リセットしています ...」というメッセージが表示されます。その場合、コンソールを終了し、再起動する必要があります。

「startsync」コマンドの実行が失敗する。「Failed to start synchronization for some of the requested directory sources...」というメッセージが表示される (*5050443*)

メモリー不足などの特定の状況下で、いくつかのコンポーネントが同期を開始できなかった場合でも、同期が正常に開始されたとコマンド行または管理コンソールが報告する場合があります。同期の問題が発生した場合、エラーログにメモリー関連のメッセージが含まれていないか確認してください。

単一値属性に複数値が設定されていると、パラメータ化された属性で障害が発生する (*5069907*)

単一値属性に 1 つの値ではなく複数の値が指定されていると、同期処理で障害が発生します。Directory Server に値が保存されるときに、エラーまたは警告メッセージが表示されます。

idsync コマンドが実行されると、パスワードがクリアテキストで画面に表示される (*4900126*)

`idsync` コマンドによってバインドパスワードと設定パスワードの入力を求めるプロンプトが表示され、それに従ってパスワードを入力すると、パスワードはクリアテキストで表示され暗号化されません。

回避策

パスワードが画面に表示されないようにするには、各パスワードを保護されたファイルに保存し、それからコマンド行に再転送します。パスワード引数のいずれかに「-」オプションが指定されていると、idsync コマンドは、コマンド行に入力されるオプションの順序でパスワード値の入力を求めるプロンプトを出します。たとえば、管理者パスワードが `adminPw` で、設定パスワードが `configPw` の場合は、以下の内容の `passwords.txt` というファイルを作成します。

```
adminPw
configPw
```

次に、コマンドを実行するための `idsync printstat -w - -q - < passwords.txt` を実行します。

ログファイルの読み込み中のエラー (*5091787*)

「状態」タブでコンソールの `audit.log` ファイルを読み込み中に、次のエラーが表示される場合があります。「未知のエラーにより、ログエントリを取得できません。Admin server may need to be restarted.」

回避策

`audit.log` ファイルは、それ以降にこのファイルの読み込みを試みるときに、アクセスされると、読み込まれます。

移行時に MMR セットアップで prepds がエラーメッセージを表示する (*5093124*)

レプリケートされた環境の移行中、`idsync prepds` はスキーマのレプリケーションが失敗したと誤って報告する場合があります (たとえば、次のようなエラーメッセージが表示される場合がある。「`ldap://preferred.example.com:389` にある優先 Sun Java System Directory Server は、`ldap://secondary.example.com:389` にある二次 Sun Java™ System Directory Server にスキーマ変更をレプリケートできませんでした。レプリケーション設定を確認してください。」この場合、もう一度同じ引数で `idsync prepds` を実行する)。もう一度 `idsync prepds` を実行したときに、同じエラーメッセージが表示される場合にだけレプリケーションの設定を調べます。

コンソールへのアクセスにリフレクション X 10.0 を使用できないことがある (*5095013*)

ボタンやテキストボックスを表示できない、またダイアログボックスのサイズも変更できないために、一部のダイアログボックスが使用できないことがあります。

コンソールのログメッセージに破壊された複数バイトの文字が表示される (*6174184*)

複数バイトの文字は、複数バイトの同期ユーザーリスト名が使用されるか、または複数バイトのサフィックスが同期している場合にだけログに記録されます。ログメッセージを正しく表示するには、UTF-8 エンコード表示対応ビューアで、ログファイルを開きます (`/var/opt/SUNWisw/logs/central/error.log`)。

設定パスワードを変更すると、「startsync」および「stopsync」コマンドが正常に機能しない。エラーメッセージが表示される (*6175396*)

`idsync changepw` コマンドを使用して Identity Synchronization for Windows の設定パスワードを変更し、マシンを再起動していない場合、`idsync startsync` および `stopsync` コマンドは正常に機能しません。コマンドは次のようなメッセージを表示します。「受信したメッセージは暗号化されていませんでした。」、そして終了コード「1」を返します。

エラーメッセージが表示されなくても、同期の開始や同期の停止の操作は行われます。これを確認するには、`idsync printstat` コマンドを実行します。しかしこの問題を防止するには、設定パスワードを変更するたびにマシンを再起動します。

パスワード同期

パスワードポリシーの問題 (*4834865* および *4811572*)

異なるディレクトリ上で使用されている複数のパスワードポリシーが、同期エラーの原因になる可能性があります。たとえば、パスワードの長さ、最小 / 最大必要文字数などです。管理者は、互換性のないパスワードポリシーを、ほかのシステムのポリシーと矛盾しないように手動で変更する必要があります。

同時に変更された対応する属性またはパスワードが、正しく同期されないことがある (*4854183* および *4808601*)

2 つのディレクトリソース間で同期されているエントリ内の特定の属性が両者で同時に変更された場合、その属性は正しく同期されない可能性があります。たとえば、次のようなイベントシーケンスを考えます。

- John Smith 氏が、Active Directory (AD) 上で自身の電話番号を 555-1111 に変更した
- この変更は Directory Server に伝播されるが、この変更が Directory Server に到着する前に、管理者が間違って、Directory Server 上で John Smith 氏の電話番号を 555-1112 に設定した
- 続いて、Active Directory 上での変更が Directory Server に適用され、John Smith 氏の電話番号が 555-1111 に設定される
- 同様に、Directory Server 上での変更が AD に伝播され、John Smith 氏の電話番号が 555-1112 に設定される

  2 つのディレクトリソースの値が互いに入れ替わり、同期されていない状態になります。

同様に、ユーザーのパスワードが Active Directory (AD) 上と Directory Server 上とでほぼ同時に変更された場合、そのパスワードは正しく同期されない可能性があります。

負荷の軽いシステム上では、2 件のパスワード変更が互いに数秒以内で発生した場合に限り、同期が失われます。もちろん、こうした状況は、AD パスワードが変更される前に Directory Server 値が設定された場合でも発生しますが、AD パスワードの変更と Directory Server 値の設定との間隔が数ミリ秒以内になる可能性は、ほとんどありません。

Active Directory の「ユーザーは次回ログオン時にパスワード変更が必要」機能の扱い (*4827180*)

管理者があるユーザーのパスワードを Active Directory (AD) 上で変更し、「user must change password at next logon」を指定した場合、ユーザーがログオンしてパスワードを変更しない限り、パスワード変更は Directory Server に同期されません。

以下の場合、ユーザー認証が失敗します。

1. あるユーザーが AD 上で自身のパスワードを変更します。そのパスワードは Directory Server に伝播され、Directory Server のパスワードが無効になります。
2. 管理者が、そのユーザーのパスワードをリセットし、「user must change password at next logon」フラグを設定します。

3. そのユーザーがステップ 1 または 2 のパスワードを使って Directory Server にログインしようとすると、処理が失敗します。AD、Directory Server のいずれかでパスワードを変更すると、Directory Server のパスワード値が更新されます。

NT または Active Directory 上で 7 ビットチェックプラグインを有効にした状態で非 ASCII パスワードを指定すると、そのパスワードが Directory Server に同期されない (*4817344*)

Directory Server 上では、userpassword 属性値で 7 ビットチェックプラグイン (サブコンポーネント) がデフォルトで有効になります。次を参照してください。
http://docs.sun.com/source/816-6699-10/plugattr.html

7 ビットクリーンでないパスワードを Windows から Directory Server に同期させ、userpasssword 属性値に対してこのプラグインを有効化および設定した場合、同期が失敗します。

パスワード値の文字エンコーディングの情報は保存されないため、非 ASCII 文字を含むパスワードを同期させる場合には注意が必要です。したがって、パスワード変更時および認証時に Windows 側のクライアントと Directory Server クライアントが同じ文字エンコーディングを使用していないと、処理が失敗します。

複数のパスワード値がサポートされない (*4807350*)

複数のユーザーパスワード値はサポートされていません。

システムマネージャが再起動しても、resync が自動的に resync プロセスを再開しない (*5077660*)

resync コマンドが実行され、システムマネージャが再起動されても、resync はプロセスを自動的に復元して再開しません。

再同期を実行すると、作成属性が削除される (*5085134*)

1 つの属性を同時に更新しても同期されない (*5077760*)

この問題が発生するのは、1 つの属性に値が追加されるのとほとんど同時に、その属性に対応するリモートディレクトリエントリ内の属性に異なる値が追加される場合です。この場合は、属性が同期されない可能性があります。

再同期を実行する際、再同期処理が中止された場合でも、Directory Server コネクタがリンクアクションを受け取らない (*4985505*)

`resync -c -o Sun` が実行されると、Active Directory に新規ユーザーが作成されたあとに LINK アクションが Directory Server に送られます。resync 処理が中止されたとしても、Directory Server コネクタはこれらの LINK アクションを受け取りません。現在、これらの LINK アクションは、すべての resync/linkusers アクションが発行されるのと同じ一時 MQ トピックで発行されます。

Directory Server Retro-Change Log プラグインの既知の問題のために、削除されたエントリが、Directory Server から Active Directory に同期されない (*5077814*)

Directory Server Retro-ChangeLog プラグインは、削除されたエントリのプラグインエントリに `dspswuserlink` を保管しない場合があります。この状況が発生した場合は、Directory Server エントリの削除されたエントリから Active Directory への同期は実行されません。

回避策
この問題を解決するには、この問題を解決するパッチを適用して Directory Server が更新されていることを確認します。この問題を解決するために必要なパッチの詳細については、「Sun Java System Directory Server 5 2004Q2 Retrochangelog のパッチ」のセクションを参照してください。

Sun Java System Message Queue

システムマネージャが Message Queue に接続できない (*4907711*)
Message Queue が稼働している 状態で、システムマネージャが Message Queue に接続できません。

回避策
コアがインストールされているマシン上で、Identity Synchronization for Windows サービス / デーモンを再起動します。

10 万ユーザーを超える配備環境では Message Queue ブローカの最大メモリーを増やす (*4924939*)
Identity Synchronization for Windows はデフォルトで、Message Queue ブローカの最大メモリーを 512M バイトに設定しますが、これは、ほとんどのインストール環境で十分な値です。ただし 10 万ユーザーを超えるインストール環境では、最大メモリーを少なくとも 1G バイトに増やさないと、最適なパフォーマンスが得られません。20 万ユーザーを超える配備環境では、メモリーを 2G バイトに増やします。

Identity Synchronization for Windows コアが Solaris 上にインストールされている場合、Message Queue ブローカのメモリー制限を増やすには、次の手順に従います。

1. 次のコマンドを発行して Message Queue ブローカを停止します。

   ```
   /etc/init.d/imq stop
   ```

2. `/etc/imq/imqbrokerd.conf` ファイルを開き、現在のデフォルトのメモリー設定を変更し、1G バイトの場合は `-Xmx512m` を `-Xmx1024m` に、2G バイトの場合は `-Xmx2048m` にします。

3. 次のコマンドを発行して Message Queue ブローカを起動します。

   ```
   /etc/init.d/imq start
   ```

Identity Synchronization for Windows コアが Windows 2000 上にインストールされている場合、Message Queue ブローカのメモリー制限を増やすには、次の手順に従います。

1. Windows サービス管理コンソールを使って Message Queue ブローカサービスを停止します。

2. <*installation-root*>/isw-<*machine-name*>/imq/bin ディレクトリに移動し、コマンド行から imqsvcadmin query コマンドを発行します。出力結果は次のようになります。

   ```
   Service iMQ Broker is installed.

   Display name:  iMQ Broker

   Start Type:  Automatic

   Binary location:  C:¥sunone¥servers¥isw-example¥imq¥bin¥imqbrokersvc

   JREHome:  c:/j2sdk1.4.2/jre/

   VM Args:  -Xmx512m

   Broker Args:  -passfile
   "C:/sunone/servers/isw-example/imq/etc/passfile.properties"

   -DimqConnectionType=TLS -port 7676 -name psw-broker
   ```

3. このコマンドの出力結果をファイルに保存します。
4. すべての Message Queue ブローカサービスをアンインストールします。それには、imqsvcadmin remove コマンドを発行します。
5. 次の手順に進む前に、コアがインストールされた Windows 2000 マシンを再起動する必要があります。
6. <*installation-root*>/isw-<*machine-name*>/imq/bin ディレクトリに移動し、先に発行した imqsvcadmin query コマンドの保存済み出力結果を参照しながら、次のコマンドを発行します。次に例を示します。

   ```
   imqsvcadmin install -jrehome c:/j2sdk1.4.2/jre/ -vmargs -Xmx1024m -args
   "-passfile C:/sunone/servers/isw-example/imq/etc/passfile.properties
   -DimqConnectionType=TLS -port 7676 -name psw-broker"
   ```

   ここで、各オプションについて説明します。

   - -args の引数は、Broker Args フィールドに基づいて入力します。
   - -jrehome の引数は、JREHome フィールドに基づいて入力します。
   - メモリーを 1G バイトに増やすには、-vmargs -Xmx1024m を使用します。
   - 64 ビット Java VM の場合に限り、メモリーを 2G バイトに増やすには、-vmargs -Xmx2048m を使用します。
     32 ビット Java VM の最大メモリ値は、-Xmx1750m です。

7. Windows サービス管理コンソールを使って Message Queue ブローカサービスを起動します。

Message Queue ブローカの起動と停止 (*4809493*)

Windows では Message Queue ブローカはサービスとして実行されます。このため、管理者は、サービスコントロールパネル経由で Message Queue ブローカサービスを制御できます。

ブローカを起動および停止するには、コアのインストール後にマシンをリブートする必要があります。なぜなら、Windows をリブートしないと、サービスマネージャプロセスが必要とする IMQ_JAVAHOME 環境変数が有効にならないからです。ただし、以上の状況が適用されるのは、コアとともに Message Queue をインストールした場合 (つまり、既存の Message Queue を使用しなかった場合) だけです。

次のコマンドを使用します。

```
/etc/init.d/imq (stop または start)
```

コアがインストールされていないマシン上の Message Queue は使用できない (*4943576*)
Identity Synchronization for Windows コアコンポーネントと Message Queue は、同じホスト上にインストールされている必要があります。

一般的な問題

同期が正常に開始されても、エラーが存在していることがある (*4814324*)
idsync startsync の戻り値が正常であっても、セントラルエラーログをチェックし、各コネクタが対応するディレクトリソースに接続できたことを確かめる必要があります。

MMR 構成の場合、設定ディレクトリとディレクトリソースを別々の Directory Server インスタンス内に配置することを強く推奨する (*4943470* および *4943480*)
マルチマスターレプリケーション (Multi-Master Replication、MMR) 構成の場合、設定ディレクトリとディレクトリソースを別々の Directory Server インスタンス内に配置するとともに、Identity Synchronization for Windows をインストールする前にレプリケーションアグリーメントを設定しておくことを、強くお勧めします。

設定ディレクトリおよび優先 Directory Server (ユーザーデータ) として同一の Directory Server インスタンスを指定し、Identity Synchronization for Windows のインストール後にレプリケーションアグリーメントを作成した場合、Identity Synchronization for Windows コアインストールによって作成されたスキーマ要素が削除される可能性があります。その場合、Identity Synchronization for Windows が動作しません。

回避策
誤って消去したスキーマを更新するには、次の手順に従います。

1. 40so-psw.ldif ファイル (インストールパッケージ用の設定レジストリのスキーマオブジェクトのみを含む) を、Directory Server インスタンスのスキーマディレクトリにコピーします。
2. 40so-psw.ldif のファイル名を変更します。

   起動時の 40so-psw.ldif 処理時に、スキーマ内のいくつかの参照が読み込まれません (その結果、サーバーが起動しない)。
3. 名前を変更したファイルを両方のマスターのスキーマディレクトリにコピーします。なお、サーバーの視点からは、スキーマエントリの変更シーケンス番号が以前と同じままであるため、スキーマはプロトコル上で変更されていません。

リンク処理で使用される属性の索引が Directory Server 内に作成される (*4814412*)

idsync resync (-f <filename> オプション) を使用してユーザーをリンクすると、idsync resync コマンドが Directory Server を検索し、Active Directory または Windows NT のユーザーに一致するユーザーを探します。idsync linkusers 処理で使用されるすべての Directory Server 属性に対し、等価インデックスが作成されます。

セントラルロガーを無効にできない (*4945507* および *4933217*)

Identity Synchronization for Windows のセントラルロガー (ファイルまたは syslog、あるいはその両方にロギング) は、ユーザーにロギングの無効化を許可するようにみえますが、実際には以前に指定された場所にロギングを続けます。

たとえば、コンソールから syslog ロギングを有効にし、ファイルロギングを無効にしたあとで、syslog ロギングを無効にしても、プログラムは syslog へのロギングを継続します。コンソールからファイルロギングを有効にし、syslog ロギングを無効にしたあとで、ファイルロギングを無効にしても、プログラムはファイルへのロギングを継続します。

「ログをファイルに書き込む」チェックボックスをオフにし、syslog を一度も使用しなかった場合も、同様の動作になります。この場合、プログラムはディレクトリへのロギングを継続します。

Identity Synchronization for Windows サービスを再起動しても効果はなく、ロギングが継続されます。

同期ユーザーリストの「ブラウズ」ボタンが正しく動作しないことがある (*4944348*)

同期ユーザーリスト (SUL) 作成ウィザードまたはエディタパネルから特定のベース DN をブラウズする場合は、「ブラウズ」ボタンを使って表示されるベース DN をダブルクリックすることをお勧めします。場合によっては、「ブラウズ」ボタンを使用した結果間違ったディレクトリが表示されることがあり、この場合は選択したベース DN が無効になります。

Active Directory におけるユーザーアカウントの無効化 (*4943785*)

Active Directory (AD) 上で、あるユーザーのユーザーアカウントを無効にし、パスワードを変更した場合、そのユーザーは AD 経由でその新しいパスワードを使って認証できなくなります。ところが、そのユーザーは、AD 上でユーザーアカウントが無効になっていても、Sun Java System Directory Server 経由ではログインできます。

設定ディレクトリのポートの変更 (*4941271*)

Identity Synchronization for Windows の設定ディレクトリとして現在使用中の Sun Java System Directory Server のポートを変更した場合、Identity Synchronization for Windows の設定を調整することで、ソフトウェアがそのポート変更を認識できるようにする必要があります。そうしないと、システムマネージャおよび Message Queue ブローカが動作しなくなります。

回避策

1. `<imq_installroot>¥imq¥var¥instances¥psw-broker¥props¥config.properties` 内のポートを変更します。
   例 : `imq.user_repository.ldap.server=<host>¥:<port>`

2. <isw_*installroot*>¥resources¥SystemManagerBootParams.cfg 内のポートを変更します。
   例 :<Parameter name="manager.configReg.hostPort" value="<*port*>"/>
3. Message Queue ブローカのサービス / デーモンを再起動します。
4. Identity Synchronization for Windows サービス / デーモンを再起動します。

ありそうもない複数値属性のサポートに制限あり (*4987930* および *4807260*)
Identity Synchronization for Windows は、ありそうもない複数値属性の同期に関しては、結果が不確定になるため、限られたサポートのみを提供します。次の制限が適用されます。

- 複数値属性の値は、1 つの単位として同期されます。たとえば、すでに 4 つの値を持つ複数値属性に別の値を追加した場合、その 5 つの値すべてが 1 つの単位として同期され、リモートの対応する属性にこれら 5 つの値が設定されます。
- 既存ユーザーのリンク時に、属性は自動的には同期されません。特定の複数値属性の値が変更された場合、そのローカルディレクトリソースの値で、リモートディレクトリソースの対応する属性の値が上書きされます。たとえば、Active Directory (AD) 上で特定のエントリの今まで空だった telephoneNumber 属性に電話番号を 1 つ追加した場合、Directory Server 上の対応するエントリの telephoneNumber 属性にこの新しい値が設定され、既存の値はすべて上書きされます。
- 複数値属性に対する同時更新は同期されません。ある複数値属性に値を追加したのとほとんど同時に、リモートディレクトリ上の対応するエントリ内のその複数値属性に異なる値が追加された場合、その属性の同期は失われます。なお、単一値属性についても同じことが言えます。
- cn 属性の変更 / 名前変更を行う場合、cn は、Directory Server では複数値属性タイプですが、AD では単一値属性タイプです。AD は、この属性タイプ (とその値) を使って、名前変更または変更する person エントリの新しい DN を生成します。コネクタは、新しい DN の作成時に複数値属性 cn のどの値を使用すべきかを知らないので、最初の値をデフォルトで送信します。最初の値は通常正しい値ではないため、AD の名前変更 / 変更処理は失敗します。

  名前変更 (ldap modrdns) を指定する際に、deleteoldrdn フラグを 0 に設定し、rdn コンポーネントの属性タイプとして cn を指定した場合、AD 側で処理が失敗します。たとえば、次のようなエントリが存在しており、このエントリが Directory Server と AD の両方で同期されたものとします。

  ```
  cn=old rdn, ou=example.com
  cn=old rdn
  ```

  続いて、Directory Server 上でこのエントリの名前を変更し、deleteoldrdn フラグに 0 を設定すると、Identity Synchronization for Windows によって、Directory Server 側のエントリが次のように変更されます。

  ```
  cn=new rdn, ou=example.com
  cn= old rdn
  cn= new rdn
  ```

  ところが、AD 側では次のようなエントリが作成され、この名前変更は失敗します。

  ```
  cn=old rdn, ou=example.com not cn=new rdn, ou=example.com
  ```

その結果、監査ログ内に次のようなエラーメッセージが出力されます。

```
[30/Jan/2004:16:41:14.831 -0600] WARNING 16  CNN100 dragon  "The action
does not have a single value for attribute cn. The corresponding user at
the remote repository might not have been created with a corresponding
attribute value, the attribute might have multiple values, or cn is not a
significant or creation attribute for this directory source.  See audit log
for more information" (Action ID=CNN101-FA6784B526-787, SN=1)
```

この処理を成功させるには、フラグを「deleteoldrdn=1」のように設定する必要があります。名前変更処理を成功させるには、次の LDAP 変更命令の例を参考にしてください。

```
dn: cn=old rdn, ou=example.com
changetype: modrdn
newrdn: cn=new rdn
deleteoldrdn: 0
```

- modify 変更タイプと add モードを使って cn 属性を変更する場合、複数の cn 属性タイプを追加するか、あるいは cn 属性タイプがすでに存在している状態で別の cn 属性タイプを追加すると、modify 処理が失敗します。たとえば、次のような cn エントリが、Directory Server と AD の両方に存在するとします。

  ```
  cn=example1, ou=example.com
  cn=example1
  ```

  このエントリに次のような LDAP 変更命令を適用します。

  ```
  dn:cn=example1, ou=example.com
  changetype: modify
  add: cn
  cn: new value
  ```

  Directory Server のエントリが次のように変更されます。

  ```
  cn=example1, ou=example.com
  cn=example1
  cn=new value
  ```

  ただし、AD 側は単一値であるため、AD 側の modify 処理は失敗します。また、コネクタは名前変更と変更を区別できないため、1 つ前のケースで示したのと同じエラーメッセージが監査ログ内に出力されます。

Active Directory の場合、AD スキーマ内である説明属性が複数値として記述されていても、その説明属性を単一値として扱う (*4938940*)

複数値の説明属性を含むエントリを Directory Server に追加した場合、Active Directory (AD) コネクタの audit.log 内に次の DSID-031D0809 エラーが出力されます。

```
[16/Oct/2003:10:02:54.998 -0500] SEVERE  29  CNN101 dragon  "Unable to
create user "cn=Aaccf Amar1072,cn=users,dc=example,dc=sun,dc=com" at
ldaps://starlingvm0.example.sun.com:636. LDAP add operation failed. Error
code: 19, reason: 00002081: AtrErr: DSID-031D0809, #1: 0: 00002081:
DSID-031D0809, problem 1005 (CONSTRAINT_ATT_TYPE), data 0, Att d
(description)
" (Action ID=CNN100-F841CDBF2A-2568, SN=8)
```

このエントリは、Directory Server 内には存在しますが、AD 内には存在しません。

この問題は Active Directory の欠陥であると思われます。詳細については、Microsoft の知識ベース内に収録された次の記事 (*286760*) を参照してください。

http://support.microsoft.com/default.aspx?scid=kb;en-us;286760&Product=win2000

回避策
そのエントリを Directory Server から削除し、問題の説明属性を単一値に変更したあと、そのエントリを再度追加します。

さらに、「作成属性のマッピングと値の定義」ダイアログボックスで、複数の属性を説明属性として初期化しないでください。

SSL 証明書が信頼されなくてもプラグインからエラーメッセージが発行されない (*4924027* および *4924705*)

マルチマスターレプリケーション (MMR) 構成で、Identity Synchronization for Windows プラグイン (サブコンポーネント) が SSL 通信を行っており、SSL の問題によって障害が発生しているのにプラグインからエラーメッセージが発行されない場合、「ピア」サーバー (ここで 「ピア」は、優先マスター、二次マスター、Active Directory のいずれか) の証明書の CA 証明書がおそらく、プラグインが動作している Directory Server の証明書データベース内に格納されていません。

`idsync certinfo` コマンド行ユーティリティを使えば、不足している証明書を特定することができます。このユーティリティは、どのデータベースでどの証明書が必要であるか (どの証明書を製品が期待しているか) を示します。

Sun Java System Directory Server 内で作成されたユーザーは、同期ユーザーリストフィルタ内のすべての属性を含んでいる必要がある (*4900568*)

Sun Java System Directory Server から Windows へエントリ作成を同期させる場合、Directory Server の同期ユーザーリスト (SUL) 定義にフィルタが含まれており、その SUL フィルタに一致しない属性値を含むエントリを作成しようとすると、属性が SUL 内に存在しないため、エントリ作成が伝播されません。そして、元の作成が伝播されないため、その Directory Server エントリは Windows 側では見つかりません。

回避策
この状況が発生すると、警告メッセージがログに出力されます。管理者は、`idsync resync -c -o Sun` を実行することで、Directory Server エントリを Windows 上に作成する必要があります。

属性が SUL フィルタに一致するようにエントリを変更すると、そのエントリに対する変更が Windows 側に伝播されます。

NetBIOS によるオンデマンド同期の遅れ (*4876741*)

Directory Server と Windows 2000 上のコアコンポーネント設定を使って 2 つの Active Directory (AD) ドメインを同期しようとすると、Directory Server プラグインのオンデマンドパスワード同期機能が AD と通信する際に遅延が発生します。AD に対するクエリのほとんどは通常、数ミリ秒かかります。パケットを追跡してみた結果、疑わしい NBNS (NetBIOS Name Service) パケットがいくつか見つかりました。

回避策

この問題を解決するには、Directory Server マシンの TCP/IP 設定にアクセスし、「NetBIOS over TCP/IP」を無効にする必要があります。

メッセージバスによって使用される Identity Synchronization for Windows の名前空間 (トピック) (*4827081*)

- `ConConfig_100`
- `CntrlLog_100`
- `SysMgr_100`
- `PSW_AuditLoggingTopic`
- `PSW_ErrorLoggingTopic`
- `PSW_LinkAuditLoggingTopic`

さらに次のトピックがあります。

- システム内の各コネクタに対して `CNN1XX_100` という形式のトピックが 1 つずつ存在します (`CNN100_100`、`CNN101_100`、`CNN102_100` など)。
- システム内の各同期ユーザーリスト (SUL) に対し、SUL 名に基づくトピックが 1 つずつ存在します (たとえば、*people* という名前の SUL に対するトピックは *people_100*)。

「グローバルカタログ」または「設定ディレクトリ」ダイアログから特定のホストを指定した場合、処理に時間がかかる場合がある (*4826109* および *4812651*)

ユーザーが名前解決できないホストを指定した場合、カーソルビジーやステータスバーなど、何らかの処理が実行中であることを示す進捗インジケータが表示されません。

NT ユーザー名は一意でなければならない (*4825636*)

NT に同期させるユーザーを Directory Server 内で作成する場合、`USER_NAME` にマップされる Directory Server 属性の値が一意であることを確認する必要があります。

アクセス制御リスト (ACL) を使って XML 設定ファイルをセキュリティ保護するようユーザーに勧める (*4812824*)

XML 設定ファイルをファイルレベルで保護します。これらのファイルにはクリアテキストのパスワード値が含まれている可能性があります。したがって、ファイルレベルの ACL など、システムで提供されているセキュリティメカニズムを使って、それらのファイルをセキュリティ保護する必要があります。

サポートされている同期ユーザーリストとデータベースの関係 (*4811577*)

Identity Synchronization for Windows は、単一の Directory Server データベースのみをサポートします。単一の Directory Server データベース内にすべての同期ユーザーリストを含める必要があります。

ログの個数は無制限に増加する (*4807451*)

ユーザーが古いログを保存または削除しない限り、Identity Synchronization for Windows の各ログファイルタイプの個数は無制限に増加します (毎日 1 個ずつ増加)。

ログは次の形式で命名されます。

- `audit_YYYY_MM_DD.log`
- `error_YYYY_MM_DD.log`

次の内容のログが保存されます。

- `audit`
- `error`

これらのログの格納場所は、次のとおりです。

- **Solaris の場合** : `/var/opt/SUNWisw/logs`
- **Windows の場合** : `<install-root>/isw-<machine-name>/logs`

特殊文字を含むエントリは Directory Server から Active Directory に同期されない (*4816867*)

ユーザー ID に 1 つ以上の特殊文字が含まれていると、Identity Synchronization for Windows がマッピングの制限によりそれらの特殊文字を解決できないか、あるいは Active Directory (AD) がユーザーを作成できません。

AD コンソールでは、次のような「ユーザーログオン名」は作成できません。

- 次の特殊文字を含んでいる : `" / [ ] : | < > ; ? %$^&*()!@#-+=~'`
- 文字数が 20 文字を超えている
- ピリオドで終わったり、コンマを含んでいる
- 1 ～ 31 の範囲の文字 (印刷不可能な文字) を含んでいる

useraccountcontrol 属性はデフォルトで、Active Directory の非ユーザーオブジェクトクラスを作成できないようにする (*5043156*)

新しいユーザーに対して選択されたオブジェクトクラスで `useraccountcontrol` 属性が使用できない場合、そのユーザーを Active Directory 内に作成できません。ただしこの制限は、Active Directory のユーザーオブジェクトクラスと任意のユーザー派生オブジェクトクラスで `useraccountcontrol` 属性が使用できる場合には適用されません。

回避策
Directory Server コンソールを使って設定ユーザーを編集します。useraccountcontrol 属性を見つけて削除します。

次に例を示します。

```
dn:
cn=130,ou=AttributeDescriptions,cn=active[2],ou=GlobalConfig,ou=1.1,ou=Ide
ntitySynchronization,ou=Services,dc=central,dc=sun,dc=com
pswVersion: 2
pswName: useraccountcontrol
pswSyntax: 1.3.6.1.4.1.1466.115.121.1.5
pswValue: 512
pswPreferCreationAttributeDefaultToAction: false
cn: 130
objectClass: pswattributedescription
objectClass: top
```

useraccountcontrol 属性への参照もすべて編集します (特に、Active Directory グローバルスキーマの pswCreationAttributeDefaultRef 属性内)。

次に例を示します。

```
dn:cn=127,ou=ActiveDirectory,ou=Globals,cn=active[2],ou=GlobalConfig,ou=1.1,o
u=IdentitySynchronization,ou=Services,dc=central,dc=sun,dc=com
```

デフォルト値は検証されない (*5051725*)
属性にはデフォルト値を指定でき、それらの値は属性作成時にディレクトリのエントリに適用できます (『Sun Java System Identity Synchronization for Windows インストールおよび設定ガイド』の「作成属性」を参照)。ただし現時点では、ユーザーが指定した属性値に対して、何の検証も行われません。単一値属性に複数の値を指定すると、エントリの同期時にオブジェクト作成エラーが発生します。属性値を指定する際には、その値が会社の LDAP スキーマに準拠していることを確認するようにしてください。

変更したユーザーが同期ユーザーリスト (SUL) に含まれるようになった場合の処理方法に一貫性がない (*4970664*)
あるユーザーを変更した結果、そのユーザーがいずれかの同期ユーザーリスト (SUL) に含まれるようになった場合 (たとえば、フィルタ 'l=Austin' が含まれている SUL が存在しており、ユーザーの属性 l に「Austin」が設定された場合)、Sun Java System Identity Synchronization for Windows によるこのユーザー更新の扱い方が、Active Directory と Sun Java System Directory Server の場合とで、次のように異なります。

- ユーザー更新が Active Directory 内で発生した場合、Identity Synchronization Directory Server コネクタによって対応するユーザーが作成されます。
- ユーザー更新が Sun Java System Directory Server 内で発生した場合、Active Directory の対応するユーザーは作成されません。resync -c -o Sun を実行すると、この問題を解決しやすくなります。

同期対象として選択したオブジェクトクラスだけではく、そのクラスを継承した Structural オブジェクトクラスのエントリも同期される (5046861)

たとえば、organizationalperson オブジェクトクラスが選択されると、inetorgperson オブジェクトクラスのユーザーも同期されます。これは、inetorgperson が organizationalperson のサブクラスだからです。

これを防ぐには、そのサブクラスを除外する次のようなフィルタを、SUL に含めます。

```
(!(objectclass=inetorgperson))
```

こうした動作は通常、resync を使って削除済みエントリを同期させる場合に問題になります。そのサブクラスも削除されてしまうためです。たとえば、Active Directory の computer オブジェクトクラスは user を継承していますが、これに対応する Directory Server エントリが存在しないため、この computer エントリが削除されます。computer エントリが同期されるのを防ぐには、それらのエントリを除外する次のようなフィルタを、SUL に含めます。

```
(!(objectclass=computer))
```

期限切れになっても、ログファイルが自動的に削除されない (*5069020*)

削除までの指定された日数より古いログファイルは削除されません。

デフォルトの作成属性値が誤って設定されているか、検証ロジックが正常に働かない (*5066657*)

Directory Server および Active Directory データソースの作成属性名が同じ場合は、一方のソースにデフォルト値を追加すると、他方のソースにも同じデフォルト値が自動的に追加されます。

回避策

コンソールの作成属性マップと作成属性を削除し、もう一度入力します。保存する前に、次の操作を実行します。

マップされた属性の名前が同じで、属性の構文 (OID) が Active Directory と Directory Server のスキーマであり、同じである場合は、次の操作を実行します。

- 属性に追加するデフォルト値は、同じにしないでください。値を追加しない場合にもこの問題が発生します。

注 デフォルト値がまったく同じ場合は、この問題は発生しません。デフォルト値が同じの場合は、作成属性とマップを削除してから再び追加しなければ、分離することはできません。

---

useraccountcontrol 属性はデフォルトで、Active Directory の非ユーザーオブジェクトクラスを作成できないようにする (*5043156*)

新しいユーザーに対して選択されたオブジェクトクラスで useraccountcontrol 属性が使用できない場合、そのユーザーを Active Directory 内に作成できません。Active Directory のユーザーオブジェクトクラスと任意のユーザー派生オブジェクトクラスで useraccountcontrol 属性が使用できるので、この制限の影響は受けません。

必須属性がある拡張クラスで InetOrgperson をマッピングできない (*5091959*)

たとえば、「Active Directory 属性 `mail` に Sun のマッピングまたは値が指定されませんでした」というエラーメッセージが表示されたとします。ここの `mail` は必須属性であり、`mail` は Sun の mail 属性にマッピングされます。

『Identity Synchronization for Windows インストールおよび設定ガイド』には、「次へ」ボタンおよび「概要」ペインについての説明がない (*5104768*)

『Identity Synchronization for Windows インストールおよび設定ガイド』には、各呼び出しの終わりに、「インストール概要」ペインの「閉じる」ボタンを使用してウィザードを終了する必要があると記載されています。しかし、このペインには「閉じる」ボタンがありません。「インストール概要」ペインから「次へ」ボタンをクリックして、インストールおよび設定の残りの実行すべき手順を説明するペインに移動します。コア以外のすべてのもののインストール操作の場合は、このペインに「終了」ボタンがあります。このボタンをリックすると、ウィザードが終了します。コアインストールの場合、このペインには「次へ」ボタンがあります。このボタンをクリックすると、コンソールを起動するかどうかを尋ねるペインに移動します。このペインから、「終了」ボタンを使用してインストールプログラムを終了できます。

WAN サポートの制限 (*5097751*)

Identity Synchronization for Windows は、制限付きで Wide Area Network (WAN) 環境に配備できます。

Directory Server プラグインを除く、すべての Identity Synchronization for Windows コンポーネントは、同じ LAN (たとえば、同じマシン) にインストールする必要があります。つまり、WAN 上に Message Queue トラフィックを行き来させてはなりません。それらのコンポーネントは、Directory Server または Active Directory ドメインコントローラを使用して WAN を介して通信できます。

WAN を介したパフォーマンスは、待ち時間とリンクの速度に依存します。接続が最低 T1 (1.544Mbps) であることと各コネクタと各コネクタが管理するディレクトリ間の待ち時間が 300 ミリ秒を超えないことをお勧めします。Active Directory と Directory Server 間に WAN がある配備では、Directory Server コネクタを Directory Server と同じ LAN にインストールし、Active Directory コネクタを WAN を介して Active Directory と通信するようにすると、パフォーマンスを向上できます。

再配布可能ファイル

Sun Java System Identity Synchronization for Windows 1 2004Q3 には、再配布可能なファイルは含まれていません。

問題の報告方法およびフィードバックの提供方法

Sun Java System Identity Synchronization for Windows に関する問題が発生した場合には、次のいずれかの方法で Sun カスタマサポートまでご連絡ください。

- Sun ソフトウェアサポートサービスオンラインの Web サイト

  http://www.sun.com/service/sunone/software

  このサイトには、知識ベース、オンラインサポートセンター、ProductTracker へのリンクのほか、保守プログラムおよびサポートの連絡先電話番号へのリンクがあります。

- 保存契約に関連する緊急電話番号

最善の問題解決のため、テクニカルサポートに連絡する際はあらかじめ次の情報をご用意ください。

- 問題が発生した箇所や動作への影響など、問題の具体的な説明
- マシン機種、OS バージョン、および、問題の原因と思われるパッチやそのほかのソフトウェアなどの製品バージョン
- 問題を再現するための具体的な手順
- エラーログやコアダンプ

コメントの送付方法

弊社ではマニュアルの改善に努力しており、お客様からのコメントおよび提案を歓迎いたします。フィードバックには、次の Web ページのフォームをご使用ください。

http://www.sun.com/hwdocs/feedback/

該当欄にマニュアルの正式タイトルと Part No. をご記入ください。Part No. は、マニュアルのタイトルページか表紙に記載されており、通常は 7 桁または 9 桁の番号です。たとえば、この Identity Synchronization for Windows バージョン 1 2004Q3 リリースノート の Part No. は 817-7853 です。

Sun が提供しているその他の情報

次の各 Web サイトには、Sun Java System に関する有用な情報が含まれています。

- Sun Java System Identity Synchronization for Windows 1 2004Q3 のマニュアル
  http://docs.sun.com/coll/S1_IdSyncForWin_1.0
- Sun Java System マニュアル
  http://docs.sun.com/prod/sunone
- Sun Java System プロフェッショナルサービス
  http://www.sun.com/service/sunps/sunone
- Sun Java System ソフトウェア製品およびサービス
  http://www.sun.com/software
- Sun Java System ソフトウェアサポートサービス
  http://www.sun.com/service/sunone/software
- Sun Java System サポートおよび知識ベース
  http://www.sun.com/service/support/software
- Sun サポートおよびトレーニングサービス
  http://training.sun.com
- Sun Java System コンサルティングおよびプロフェッショナルサービス
  http://www.sun.com/service/sunps/sunone
- Sun Java System 開発者用情報
  http://sunonedev.sun.com
- Sun 開発者サポートサービス
  http://www.sun.com/developers/support
- Sun Java System ソフトウェアトレーニング
  http://www.sun.com/software/training
- Sun ソフトウェアデータシート
  http://wwws.sun.com/software

license agreement and applicable provisions of the FAR and its supplements.

使用は、使用許諾契約の条項に従うものとします。

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、カリフォルニア大学からライセンスされている Berkeley BSD システムに基づいて開発されている場合があります。

Sun、Sun Microsystems、Sun ロゴ、Java、および Solaris は、米国およびその他の国における Sun Microsystems, Inc. の商標または登録商標です。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されている、米国およびその他の国における同社の商標または登録商標です。