Sun Java™ System Identity Server リリースノート

バージョン 6 2004Q2

Part No. 817-7133

このリリースノートには、Sun Java System Identity Server 2004Q2 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、既知の問題および制限、その他の情報などについて説明します。Identity Server 2004Q2 の使用を始める前に、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の最新バージョンは、Sun Java System マニュアル Web サイトから入手できます。

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

ソフトウェアをインストールおよび設定する前、およびそれ以降も定期的にこの Web サイトをチェックして、最新のリリースノートと製品マニュアルを確認してください。

このリリースノートは、次の節で構成されています。

このリリースノートで紹介されているサードパーティの URL を参照すると、追加および関連情報を入手できます。

注 Sun は、このリリースノートに記載されたサードパーティの Web サイトの有効性および有用性に関して責任を負いません。Sun は、これらのサイトまたはリソースで利用可能な内容、広告、製品、他の資料に関し、それらを保証することも、責任や義務を負うこともありません。Sun は、これらのサイトやリソースで利用可能な内容、製品、またはサービスを使用または信頼することに起因するいかなる直接的または間接的な損害についても責任を負いません。

リリースノート改訂履歴

表 1 改訂履歴

日付	変更の説明
2004 年 6 月 23 日	Linux サポートに対する第 2 版のリリースノート。既知の問題のリストに説明も追加
2004 年 5 月 18 日	このリリースノートの最初のリリース

Identity Server 6 2004Q2 について

Sun Java™ System Identity Server は、急速に拡大する企業の要求に対応するよう設計されたアイデンティティ管理のソリューションです。Identity Server によって、社員、提携業者、および供給業者のアイデンティティを 1 つのオンラインディレクトリに統合することができます。それによって、企業内のどの情報にだれがアクセスできるかに関するポリシーと権限を確立する手段を提供できます。Identity Server は、すべてのデータ、サービス、およびだれが何にアクセス権があるかの鍵です。つまり、内部および外部のビジネス関係にとっての鍵なのです。

このリリースでの新機能

Identity Server 2004Q2 の新機能には、次のものが含まれます (この新機能の詳細な説明については、『Sun Java System Identity Server Technical Overview』を参照)。

- 連携管理の拡張機能
  - Identity Federation Framework 1.2
  - Liberty Identity Web Services Framework 1.0
  - Identity Service Instance Specification 1.0
- SAML 1.1 のサポート
- カスタマイズされた JAAS 承認フレームワーク
- 認証の拡張機能
  - Windows デスクトップ SSO 認証サービス
  - JAAS の共用状態
  - Java Database Connectivity の認証モジュールのサンプル
  - Java Card デジタルアイデンティティ認証モジュールのサンプル
- Identity Server コンソールの拡張機能
  - 入れ子のグループのサポート
  - 集中エージェント管理
  - 表示オプションと利用可能なアクション
- Application Server のセッションフェイルオーバー
- 設定およびチューニングのスクリプト

ハードウェアおよびソフトウェアの要件

このリリースの Identity Server には、次のハードウェアおよびソフトウェアが必要です。

表 2 ハードウェアおよびソフトウェアの要件

コンポーネント	Solaris の要件
オペレーティングシステム	Solaris™ Operating System (OS)、SPARC® Platform Edition、バージョン 8 および 9
	Solaris™ 9 OS、x86 Platform Edition
	Red Hat™ Linux、Advanced Server 2.1 Update 2
RAM	512M バイト
ディスク容量	Identity Server および関連するアプリケーション用に 250M バイト

このリリースで修正されたバグ

次の表に Identity Server 2004Q2 で修正されたバグを示します。

表 3 Identity Server 2004Q2 で修正されたバグ

バグ番号	説明
4919897	匿名バインド時に認証に失敗
4794971	起動スクリプトが正しく削除されない
4922287	サブ組織名にアポストロフィが含まれているとエラーが発生
4925958, 4948665	`zh_CN.GB18030` ロケールに関する問題
4921424	韓国語文字セットのデフォルトのグローバル化設定が正しくない
4918930	未登録のサービスが登録済みのサービスとして間違ってリストに表示される

インストールに関する注意事項

このリリースの Identity Server では、Identity Server パッケージのインストールが、実行する必要のある設定手順とは別個に行われます。このリリースの場合、Identity Server の最初のインスタンスをインストールするには、Java Enterprise System インストーラを使用する必要があります。

設定スクリプト

最初の Identity Server のインスタンスをインストールした後、設定スクリプトを使用して、Sun Java System Application Server のほか Sun Java System Web Server にも追加のインスタンスを作成できます。

IS インストールおよび設定スクリプトでは次が実行されます。

- 単一のホストの Web コンテナに Identity Server インスタンスを追加して配備
- Identity Server インスタンスの再設定。例 : Identity Server インスタンスの所有者とグループの変更 (ルートから別のユーザーまたはグループに変更するなど)
- Identity Server SDK を Web アプリケーションから利用可能にする
- 追加のインスタンスのアンインストール (最初のインスタンスのアンインストールには JES アンインストーラを使用する)

詳細な手順については、『Identity Server 管理ガイド』を参照してください。なお、`amserver` コマンドのサポートは中止されました。

既知の問題点と制限事項

この節では、Identity Server 2004Q2 リリース時での、より重要な既知の問題点について説明します。この節は、次のトピックで構成されています。

インストール

ルートサフィックスのコンマによってインストールが失敗することがある (#4750396)
インストール実行中に、Identity Server のルートサフィックスを指定する際には、ルート識別名 (RDN) にコンマを使用しないでください。

認証

持続 Cookie モードのプロパティに一貫性がない (#5038544)

持続 Cookie モードでは、トークンで設定されるユーザー ID プロパティに一貫性がありません。このため、ユーザー ID プロパティに依存するポリシーエージェントにも障害が発生することがあります。

回避策

DN 値以外には `UserToken` を使用し、DN 値には `Principal` を使用してください。

管理者が親組織からのロールを追加できない (#5042217)

サブ組織の認証サービスにユーザーダイナミックプロファイル作成ロールを設定して、ダイナミックプロファイル作成が有効な状態でそのサービスにログインした場合、ユーザープロパティを表示したときに、認証サービスはサブ組織に属するロールのみを許可するため、ロールがまったく割り当てられないことになります。

プロキシプロパティを追加すると Identity Server にログインできない (#4966788)

プロキシプロパティを `server.xml` に追加して Identity Server を再起動すると、Identity Server コンソールにログインできなくなります。このことは、プロキシサーバーが Identity Server を認識できない場合にだけ発生します。

回避策

`server.xml` で `http.nonProxyHosts` を完全指定のホスト名を使ったホスト名に設定して、サーバーを再起動してください。たとえば、次のように指定します。

```
<JVMOPTIONS>-Dhttp.nonProxyHosts=Identity_Server_FQDN</JVMOPTIONS>
```

パフォーマンスの向上のために、プロキシサーバーが Identity Server を認識する場合にも、この回避策で示したプロパティを設定してください。

セッションタイムアウトページを再度読み込むと、ユーザー名とパスワードが有効なユーザーが認証される (#4697120)

ログインページで、ページがタイムアウトになってから有効なユーザー名とパスワードを入力すると、セッションタイムアウトページが表示されます。ユーザー名とパスワードを再度入力しなくてもページを再度読み込むと、このユーザーは Identity Server に認証されます。

SafeWord サーバーが複数存在する場合に、それぞれ別のディレクトリを指定する必要がある (#4756295)

複数の組織がそれぞれ独自の SafeWord サーバーを使用するように設定している場合には、それぞれ独自の `.../serverVerification` ディレクトリを SafeWord 認証サービステンプレートに指定する必要があります。デフォルト値をそのまま使用し、すべてのサーバーが同じディレクトリを使用する場合には、SafeWord サーバーを使って認証する最初の組織だけが機能します。

コマンド行ツール

SSL モードで amadmin を実行しているときに、JVM が異常終了することがある (#5009031)

サーバーをセキュリティ保護されたモードで実行しているときに、amadmin を連続して使用すると、JVM が異常終了することがあります。

このような動作が発生した場合は、Sun Java System ソフトウェアのサポートサービスにお問い合わせください。

Linux で、am2bak スクリプトと bak2am スクリプトが機能しない (#5053866)

am2bak および bak2am 復元スクリプトは、Linux で稼動する Identity Server の場合は機能しません。

回避策

1. 次のコマンドのパスを修正してください。

   ```
   ECHO=/usr/bin/echo
   ```

   これを、ECHO=/bin/echo にします。

   ```
   uid=`/usr/xpg4/bin/id -un`
   ```

   これを、uid=`/usr/bin/id -un` にします。

   ```
   /usr/bin/tar
   ```

   これを、/bin/tar にします。

   ```
   /usr/bin/rm
   ```

   これを、/bin/rm にします。

   ```
   /usr/bin/grep
   ```

   これを、/bin/grep にします。

   ```
   /usr/bin/ps
   ```

   これを、/bin/ps にします。

   ```
   /usr/bin/ls
   ```

   これを、/bin/ls にします。

2. check_for_invalid_chars() 関数を変更します。たとえば、次のように指定します。

```
check_for_invalid_chars() {
        echo "$1" | grep '[^/_.a-zA-Z0-9a-]' > /dev/null
        if [ $? = 0 ]; then
           return 1
        else
           return 0
        fi
    }
```

Linux システムで、amserver stop により amunixd プロセスが停止しない (#5050332)

Linux システムでは、/etc/init.d/amserver stop コマンドにより amunixd 認証ヘルパープロセスは停止しません。

回避策

最初に、f オプションを付けた ps コマンドを使って、amunixd プロセス ID を判別します。

```
ps -efl | grep /opt/sun/identity/share/bin/amunixd
```

次に、kill コマンドをこのプロセス ID と共に使って、amunixd プロセスを停止します。

am2bak の実行中に失敗メッセージが表示される (#5043752)

am2bak を使ってバックアッププロセスを実行すると、実際には失敗していないのに、バックアッププロセスが失敗したことを示すエラーメッセージが表示されることがあります。

amadmin が正しくないエラーメッセージを戻す (#5008960)

amadmin の import オプションが、関連するどのエラーに対しても同じエラーメッセージを誤ってスローします。

コンソールのみのインストールでは amverifyarchive がスワップしないタグがある (#4993375)

Identity Server のコンソールのみのインストールを実行する場合、amverifyarchive ユーティリティはこのスクリプトで次のタグをスワップアウトしません。

- JSSHOME
- JDK_HOME
- BASEDIR
- PRODUCT_DIR

設定

「あとで設定」オプションを選択した場合、amconfig スクリプトで地域対応の Identity Server の設定に失敗する (#5062437)

Java Enterprise System インストーラを使って地域対応バージョンの Identity Server 2004Q2 をインストールし、「あとで設定」オプションを選択すると、その後 amconfig スクリプトでの Identity Server の設定が失敗します。

回避策

amconfig スクリプトを実行する前に、Identity Server の実行に使用する Web コンテナに応じて、Web コンテナスクリプトを編集します。

1. 次の Web コンテナスクリプトを見つけます。
   - Web Server: amws61config
   - Application Server: amas70config

   どちらのスクリプトも、Solaris システムの場合は *IdentityServer_base*/SUNWam/bin ディレクトリ、Linux システムの場合は *IdentityServer_base*/identity/bin ディレクトリに格納されています。
2. Web コンテナスクリプトで、次の if 文で $DEPLOY_SRC 変数に /WEB-INF ディレクトリを追加します。

```
if [ ! -d $DEPLOY_SRC/WEB-INF ]; then
  mkdir -p $DEPLOY_SRC
  cd $DEPLOY_SRC
  jar xf $PKGDIR/$warfile
```

3. amconfig スクリプトを実行して、Identity Server を設定します。amconfig スクリプトの詳細については、『Identity Server 2004Q2 管理ガイド』を参照してください。

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

サイレントファイルオプションで amconfig を使用してはいけない (#5003430、5003386、5000964)

amconfig の対話型モードを使用しないでください。例 : amconfig -s。結果は予測できないものになります。

回避策

サイレントモードで amconfig を起動します。例 : amconfig -s *path-to-silent-file*

バックエンド名に関係なく userRoot に索引が常時作成される (#5002886)

index.ldif は、属性の索引を作成するため userRoot をハードコードします。任意のいずれかのバックエンドデータベース名にあるルートサフィックスを使って Identity Server をインストールすることができます。バックエンド名は、nsslapd-suffix=SUFFIX_NAME をフィルタとして使用するベース cn=config を使い、ldapsearch によって取得することができます。

連携

属性値が空の場合 PP Modify に例外がスローされる (#5047103)
Identity Server は、空の属性値で PP Modify を実行すると、例外をスローします。たとえば、sis-ep サンプルをテストするためにセットアップを作成して EP Modify ページを送信し、属性に値をまったく入力せずにボタンをクリックすると、例外が誤ってスローされます。

ポリシーを有効にするにはサーバーの再起動が必要 (#5045036)
連携ポリシーの実装はサーバーを再起動するまで有効にはなりません。Application Server と Web Server の両方がこれに該当します。新しくインストールした後およびポリシーを最初に実装した場合にのみ、サーバーを再起動する必要があります。

Identity Server コンソール

組織管理者として定義されたアクセス権を持つロールを作成するとエラーが発生する (#5037978)
組織管理者としてログインして、ロールを作成しアクセス権 (組織管理者ロールまたはヘルプデスク管理者ロールなどを作成) を割り当てると、エラーを受け取ります。

組織管理者のアクセス権は、組織管理者が組織内のあらゆる値を修正するのを防止するために設定されます。アクセス権のあるロールが作成されると、組織エントリの ACI に修正が試みられます。

回避策

1. インストールの後に、XML ファイルが配置されているディレクトリに移動します。デフォルトでは、それらのファイルは次のところにあります。

   `/etc/opt/SUNWam/config/xml` (Solaris)

   `/etc/opt/sun/identity/config/xml` (Linux)

2. `amAdminConsole.xml` ファイルをバックアップします。たとえば、次のように指定します。

   ```
   cp amAdminConsole.xml amAdminConsole.bak
   ```

3. `amAdminConsole.xml` を編集します。

   a. 「S1IS Organization Admin Role access allow read」で始まるすべての行を検索し、その ACI を削除します。たとえば、組織管理者ロールに使用される次のような ACI が出現するならそれらすべてを削除します。

   ```
   aci:(target="ldap:///ORGANIZATION")(targetfilter=(!(|(nsroledn=cn=Top-level
   Admin Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help Desk Admin
   Role,dc=iplanet,dc=com))))(targetattr != "nsroledn")(version 3.0; acl "S1IS
   Organization Admin Role access allow read"; allow (read,search) roledn =
   "ldap:///ROLENAME";)
   ```

b. 「S1IS Organization Admin Role access allow all」で始まるすべての行を検索し、その ACI を編集して、次のとおりこの ACI の冒頭の「*」を削除します。

```
aci:(target="ldap:///*,
```

組織管理者ロールでこの ACI が出現するならそれらすべてを編集します。たとえば、次のように指定します。

次の ACI を編集します。

```
aci:(target="ldap:///*,ORGANIZATION")(targetfilter=(!(| nsroledn=cn=Top-level
Admin Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help D esk Admin
Role,dc=iplanet,dc=com))))(targetattr != "nsroledn")(version 3.0; acl "S1IS
Organization Admin Role access allow all"; allow (all) roledn =
"ldap:///ROLENAME";)
```

次のように編集します。

```
aci:(target="ldap:///ORGANIZATION")(targetfilter=(!(|(
nsroledn=cn=Top-level Admin
Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help Desk Admin
Role,dc=iplanet,dc=com))))(targetattr !="nsroledn")(version 3.0; acl
"S1IS Organization Admin Role access allow all"; allow (all) roledn =
"ldap:///ROLENAME";)
```

c. このファイルを保存します。

4. 次のように amadmin コマンド行ツールを使用して iPlanetAMAdminConsoleService を削除します。

```
/opt/SUNWam/bin/amadmin -u "uid=amAdmin,ou=People,dc=iplanet,dc=com" -w
"iplanet1" -r "iPlanetAMAdminConsoleService"
```

5. ファイルが正常に削除されると、次のメッセージが表示されます。

```
サービススキーマを削除しています iPlanetAMAdminConsoleService

成功 0: 完了しました。
```

6. 次のように amadmin コマンド行ツールを使用して新しく修正した amAdminConsole.xml で再度同じサービスをインポートします。

```
/opt/SUNWam/bin/amadmin -u "uid=amAdmin,ou=People,dc=iplanet,dc=com" -w
"iplanet1" -s /etc/opt/SUNWam/config/xml/amAdminConsole.xml
```

7. ファイルが正常に読み込まれると、次のメッセージが表示されます。

```
サービススキーマ XML をロードしています
/etc/opt/SUNWam/config/xml/amAdminConsole.xml

成功 0: 完了しました。
```

8. Identity Server を再起動します。

コンソールサンプルがコンパイルしない (#5026635)

Identity Server コンソールサンプルの中にはコンパイルしないものがありますが、それはこのリリースで場所が変更されているためです。

回避策

既存の jato.jar パスを rules.mk ファイルで次のように変更してください。

```
$USER_DIR/share/lib/identity/console-war/WEB-INF/lib/jato.jar
```

SAML サービスでユーザーを作成できない (#5038600)

最上位レベルの管理者だけが、ユーザーの作成と SAML サービスの割り当てを同時に行うことができます。

回避策

組織管理者は SAML サービスのないユーザーを作成する必要があります。ユーザーがいったん作成されると、ユーザープロファイルページでそのサービスを追加できます。

「戻る」ボタンをクリックすると値が保存されていない (#4992972)

グループ、ロールの作成やポリシーへの条件の追加など、複数ページプロセスが存在する状態で「戻る」ボタンを選択した場合はいつでも、前のページの値は復元されません。

ポリシー管理者が自分自身のプロファイルを修正できない (#5042100)

ポリシー管理者は Identity Server コンソールから自分自身のプロファイルを修正することはできません。

回避策

ナビゲーションビューの「表示オプション」を「ユーザー」に設定し、ユーザーに対して「利用可能なアクション」を「完全アクセス」に設定してください。

ユーザー管理が無効な場合、ユーザーの検索中にコンソールでエラーになる (#5049218)

ユーザー管理が無効になっている場合に、ユーザーの検索を行うと、サーバーエラーを受け取る場合があります。

回避策

`PMAdminRoldSelect.jsp` を新しい JSP に置き換えてください。これは次の場所にあります。

IdentityServer_base`/applications/console/policy`

エンティティ記述子の検索フィルタが適切に機能しない (#4959895)

連携モジュールの「エンティティ記述子」ビューで、「検索」フィールドを使用してエンティティ記述子を検索した場合、検索結果が必ずしも正確とは限りません。

「**」検索マスクが機能しない (#4961370)

Identity Server コンソールの検索フィルタマスクとして他の文字を付けないで「**」を使用すると、その検索は失敗します。検索フィールドでは、たとえば **a または a** などの追加文字を伴う「**」を使うことができます。

連携管理モジュールのホストプロバイダの更新に関する問題 (#4915894)

連携管理モジュールで、ホストプロバイダのアイデンティティプロバイダ表示で属性を変更および保存した場合、変更は保存されますが、表示は自動的に更新されません。

回避策

別のモジュール (サービス設定など) を選択して連携管理モジュールを終了してから、連携管理モジュールに戻ります。この操作により、表示が更新されます。

コンソールでユーザー属性の変更が更新されない (#4931455)

Identity Server コンソールのナビゲーションフレームでは、データフレームで作成されたユーザー属性値を変更しても、その変更を適用した状態に更新されません。ページを手動で更新して変更した値を表示してください。

Internet Explorer に関するポートの問題 (#4864133)

Internet Explorer とは互換性がないため、Identity Server ポート番号として、http の実行時に 80 を使用したり、https の実行時に 443 を実行したりしないでください。

ロギングサービス

Java Security 有効時のロギングに関する問題 (#4926520)

Java Security が有効になっている場合、`jdk_logging.jar` が機能しないことがあります。

回避策

Java Security が有効になっているときに、1.4 より前のバージョンの J2SE SDK を使用している場合は、次の権限を java セキュリティファイルに追加してください。

```
permission java.lang.RuntimePermission shutdownHooks
```

ポリシー

リフェラルポリシールールの修正がサブ組織に反映されない (#5016725)
ルート組織のリフェラルポリシーを削除した後、サブ組織の標準ポリシーのルールが削除されません。また、削除することもできません。

nslookthrough の限度に達すると一致するエントリが戻されない (#5013538)
`nslookthrough` で定義された管理上の制限に達した後でも、一致するエントリは Identity Server コンソールに戻されません。

回避策

`nslookthroughlimit` のパラメータを調整して、エントリの数を補正します。

ポリシーがエイリアスのトークンに適用されない (#4985823)
ユーザーエイリアスを使用して、LDAP やメンバーシップではなく承認モジュールに対し Identity Server にログインし、保護されたリソースへのアクセスを試みる場合、アクセスは拒否されます。

ポリシーサンプルに関する問題 (#4923898)
ポリシーサンプルにある `Readme.html` には、サンプルが動作しない原因について記載されていません。サンプルを実行するには、`LD_LIBRARY_PATH` に `NSPR`、`NSS`、および `JSS` 共有ライブラリへのパスを含める必要があります。

環境変数 `LD_LIBRARY_PATH` を `/usr/lib/mps/secv1` (Solaris の場合) または `/opt/sun/pirvate/lib` (Linux の場合) に設定してください。この環境変数が正しく設定されていない場合は、エラーが発生します。

セッションサービス

アイドルセッションが正しくクリーンアップされない (#4959071)
アイドルセッションは、現時点では正しくクリーンアップされません。この問題を修正するためのパッチについては、サポートセンターにお問い合わせください。詳細は、「問題の報告およびフィードバックの提供方法」を参照してください。

SDK

SSL サーバーを使用する Identity Server SDK インストールの certutil の使用 (#5027614)

SSL が有効になっている Identity Server 2004Q2 サーバーを含む SDK 専用マシンから通信しようとすると、セキュリティ関連のエラーや例外が発生します。このシナリオでは、Identity Server SDK は、Web コンテナ以外に配備されているか、BEA WebLogic Server や IBM WebSphere Application Server などのサードパーティの Web コンテナに配備されています。

回避策

SDK 専用マシン上に証明書データベースを作成し、そのデータベース内に Identity Server サーバー用のルート CA 証明書をインストールします。

1. SDK 専用マシンにスーパーユーザー (root) としてログインします。
2. 必要な Netscape Security Services (NSS) パッケージがインストールされていることを確認します。
   - Solaris システム : SUNWtlsu
   - Linux システム : sun-nss RPM
3. このパッケージがインストールされていない場合は、インストールします。たとえば、次のように指定します。

   Solaris システム :

   ```
   cd JavaEnterpriseSystem_base/Solaris_arch/Product/shared_components/Packages
   pkgadd -d . SUNWtlsu
   ```

   Linux システム :

   ```
   cd JavaEnterpriseSystem_base/Linux_x86/Product/shared_components/Packages
   rpm -Uvh sun-nss-3.3.10-1.i386.rpm
   ```

4. 該当の証明書データベースのトークンパスワード用のパスワードファイルを作成します。たとえば、次のように指定します。

   Solaris システム :

   ```
   echo "cert-database-password" > /etc/opt/SUNWam/config/.wtpass
   chmod 700 /etc/opt/SUNWam/config/.wtpass
   ```

   Linux システム :

   ```
   echo "cert-database-password" > /etc/opt/sun/identity/config/.wtpass
   chmod 700 /etc/opt/sun/identity/config/.wtpass
   ```

   ここで、*cert-database-password* はトークンパスワードです。

5. LD_LIBRARY_PATH 変数をチェックします。

   Solaris システムの場合、LD_LIBRARY_PATH をチェックして、/usr/lib、/usr/lib/mps/secv1、および /usr/lib/mps ディレクトリが存在するかどうかを確認します。いずれかが存在しない場合は、不足しているディレクトリを追加します。

   Linux システムの場合、LD_LIBRARY_PATH をチェックして、/opt/sun/private/lib ディレクトリが存在するかどうかをチェックします。存在しない場合は、このディレクトリを追加します。

6. 証明書データベースツール (certutil) を使って、証明書と鍵データベースを作成します。certutil の詳細については、次の Web サイトを参照してください。

   http://mozilla.org/projects/security/pki/nss/tools/certutil.html

   たとえば、次のように指定します。

   certutil-home/certutil -N -d *cert-database-dir* -f *config-home*/.wtpass

   ここで、

   certutil-home は certutil の格納場所です。

   - Solaris システム : /usr/sfw/bin
   - Linux システム : /opt/sun/private/bin

   cert-database-dir は、証明書と鍵データベースのデータベースディレクトリです。

   config-home は、Identity Server 設定ファイルの格納場所です。

   - Solaris システム : /etc/opt/SUNWam/config
   - Linux システム : /etc/opt/sun/identity/config

7. 新しく作成した証明書データベースに、Identity Server サーバーにインストールされている SSL 証明書用のルート CA 証明書を追加します。たとえば、次のように指定します。

   certutil-home/certutil -A -n "*certificate-nickname*" -t "TCu,TCu,TCuw" -d *cert-database-dir* -a -i *path-to-file-containing-cert* -f *config-home*/.wtpass

8. エディタを使って AMConfig.properties ファイルを表示し、次の値を確認します。

   - 証明書データベースディレクトリ : com.iplanet.am.admin.cli.certdb.dir
   - プレフィックス : com.iplanet.am.admin.cli.certdb.prefix
   - パスワードファイル : com.iplanet.am.admin.cli.certdb.passfile

     正しくない場合は、必要に応じて設定を編集します。たとえば、プレフィックスの設定は空 (つまり、"") にしてください。

9. AMConfig.properties に変更を加えられていて、Identity Server SDK が Web コンテナ内に配備されている場合は、Web コンテナを再起動します。

SSL ハンドシェークが JCE プロバイダを使う DNS エイリアスで失敗する (#5038876)

subjectaltname に有効な DNS エイリアス名がある証明書が JCE プロバイダで使用される場合、SSL ハンドシェークが失敗します。

BasicEntitySearch フィルタが uid にハードコードされる (#5041529)

ユーザーネーミング属性を cn に設定して Identity Server をインストールして、Identity Server コンソールにログインし、エージェントエンティティを作成した場合、エージェントエンティティはナビゲーション区画に表示されません。これは、エンティティ検索テンプレートが uid にハードコードされるためです。

回避策

Directory Server 管理コンソールから、フィルタを uid から cn へ変更して、サーバーを再起動してください。

フィルタの init() の Identity メソッドによって Weblogic に障害が発生する (#5016283)

フィルタの init() メソッドに Identity Server 関連のコードがある場合、Weblogic サーバーは起動しません。Identity Server API は ServletFilter サーブレットの init メソッドに呼び出されています。

デフォルトでは、Identity Server は JSS をセキュリティプロバイダとして使用しますが、Weblogic は JCE を使用します。init が呼び出されると、Weblogic は JCE を使用してライセンスの妥当性検査を行うことを試みますが、JSS が初期化されます。

回避策

AMConfig.properties ファイルで、デフォルトのセキュリティ暗号化方式を JSSEncryption から JCEEncryption に変更してください。

「{SSHA}」記号で始まるすべてのパスワードが使用不可能 (#4966191)

Identity Server では、パスワードにハッシュ化された {SSHA} 記号の使用をサポートしていません。

smtp Server Port プロパティが AMConfig.properties で正しくない (#5048378)

AMConfig.properties の smtp server port プロパティは正しくありません。誤って送信されたメールは com.iplanet.am.smtpport を探します。

ネーミング属性には小文字を使用する必要がある (#4931163)

SDK の制限によって、ネーミング属性には小文字を使用する必要があります。たとえば、Identity Server インスタンスを Directory Server にインストールし、CN として定義されたユーザーネーミング属性を持つ Identity Server スキーマを読み込むと、ユーザーの作成に失敗します。

回避策

Directory Server コンソールでネーミング属性を変更してください。たとえば、作成テンプレートの basicuser ユーザーネーミング属性を、CN から cn に変更します。

グループ作成オプションを使用しても、1 つの memberURL 属性しか追加されない (#4931958)

複数 LDAP フィルタオプション (`-f`) を使用してグループを作成すると、1 つの `memberURL` 属性しか持たないグループが誤って作成されます。

サービスの登録に関する問題 (#4853809)

サービステンプレートを作成し、それらを親組織に登録してからサブ組織に登録しようとすると、親組織で登録した一部のサービスが登録されません。しかし `amConsole.access` にはそれらのサービスが登録されていると表示されます。

回避策

Identity Server コンソールを更新し、それらのサービスを再登録してください。

サービスタイプロールユーザーがログインするとサービスが消える (#4931907)

サービスタイプロールのユーザーが Identity Server にログインしたときに、Admin 開始表示が `orgDN` に設定されている場合は、サービスの登録を解除しようとすると、リストのすべてのサービスが表示から消えます。

回避策

サーバーを再起動すると、サービスが再び表示されます。

シングルサインオン

URI が一致しないと、SSO を実行できない (#4770271)

2 つの異なる Identity Server インスタンス間で配備 URI が一致しない場合には、シングルサインオンは正しく機能しません。

国際化 (i18n)

すべてのサービスを登録してもすべての利用可能なサービスが登録されないことがある (#4853809)

Identity Server コンソールからすべてのサービスを登録した場合、一部のサービスが「利用可能なサービス」に表示されないことがあります。

回避策

「追加」ボタンを 1 回以上クリックしないでください。

ポリシースキーマを持つサービスがユーザーに「追加可能」と表示される (#4996479)

サービスをユーザーに追加する場合、`wsrp` コンシューマサービスが利用可能と表示されます。しかし、選択すると、追加されず失敗します。さらに、コンシューマサービスとともに複数のサービスをチェックしている場合には、追加がすべて失敗します。

回避策

アイデンティティ管理モジュールから WSRP サービスを追加しないでください。

日本語ブラウザで認証レベルのログインが失敗する (#5013994)

認証レベルで Identity Server に初めてログインする場合、ブラウザの言語が ja に設定されていると、次の日本語ブラウザでは機能しません。

- IE6.0ja
- IE7.0ja
- Mozilla1.2.1

回避策

「認証モジュールが拒否されました。」というエラーメッセージが表示される場合、「ログインページに戻る」のリンクをクリックしないでください。代わりに、次の URL を入力してください。

`http://`*`server:port`*`/amserver/UI/Login?`*`authlevel=number`*

日本語のオンラインヘルプが誤って表示される (#5024138)

Identity Server の日本語バージョンの実行中に、言語を en_US に変更しても、日本語ヘルプコンテキストが引き続き表示されます。

回避策

`docs_en` から `docs_en_US` へのシンボリックリンクを作成してください。

ユーザー ID 生成モードが姓および名からユーザー ID を生成する (#5028750)

Identity Server はマルチバイトのユーザー ID をサポートしていません。デフォルトでは、ユーザー ID 生成モードは姓および名からユーザー ID を生成します。

クライアントディテクション機能が正しく機能しない (#5028779)

「クライアントディテクション」サービスでは、UTF-8 の削除が正しく機能しません。

回避策

UTF-8 文字セットを削除する場合、変更を行った後に Web コンテナを再起動してください。

G11NSetting が q 係数でスペースを処理しない (#5008860)

クライアントのデータの q 係数の中またはその前後にスペースがある場合、G11NSettings コードは正しくパースすることができず、次のエラーを戻します。

```
ERROR:G11NSettings::Fetchcharset() Unable toparse charset entry invalid Q q
```

ja 文字セットに対して URL にマルチバイトのロールパラメータを指定すると、ログインページでエラーが発生する (#4905708)

マルチバイトのロールを作成してから、そのマルチバイトのロールに登録されているユーザーとして URL にログインしようとすると、ログインページでエラーが発生します。

回避策

URL に指定されたマルチバイトのロールの値を認証フレームワークでデコードするには、パラメータと一緒に gx_charset を指定する必要があります。たとえば、次のように指定します。

```
http://hostname:port/amserver/UI/Login?role=manager?role=%E3%81%82%&gx_charset=utf-8
```

ログファイルが ja ロケールで文字化けする (#4882286)

次のログファイルには日本語文字が含まれており開くと文字化けします。

deploy.log および undeploy.log を除く *IdentityServer_base*/SUNWam/debug ディレクトリのすべてのファイル

URL にロケールパラメータを指定すると、文字が混在したログインページが表示される (#4915137)

WebServer と Identity Server のインスタンスが一緒にインストールされている環境で英語以外の言語のブラウザを使用している場合に、http://<host>:<port>/amserver/UI/Login?locale=en にログインすると、表示されたログインページに英語と英語以外の文字が混在します。

回避策

次のシンボリックリンクを英語ロケール用に変更します。

IdentityServer_base/SUNWam/web-apps/services/config/auth/default

次に変更した例を示します。

IdentityServer_base/SUNWam/web-apps/services/config/auth/default_en

HTTP 基本モジュールのローカライズされていないエラーメッセージ (#4921418)

HTTP 基本認証モジュールを使用してログインし、「取消し」ボタンをクリックすると、ローカライズされていないエラーメッセージが表示されます。これは Application Server に関する既知の問題で、Identity Server が Application Server に配備されている場合にのみ発生します。

Application Server が ja のときにログインウィンドウにロケールが混在する (#4932089)

ブラウザの言語設定が `en` のときに、Application Server のロケールが `ja` に設定されている場合には、Identity Server のログインウィンドウのデフォルト値は英語にはなりません。

回避策

Application Server のロケールを `en` に設定してから Application Server を実行してください。

ロックアウト通知から送信される電子メールが判読できない (#4938511)

優先ロケールが `C` 以外に設定されている Web コンテナを使用して Identity Server を実行しているときに、ユーザーがそのサーバーからロックアウトされると、判読できないロックアウト通知の電子メールが送信されます。

回避策

「ロックアウト通知を送信するための電子メールアドレス」属性に、`email` パラメータだけでなく `email|local|charset` を設定します。たとえば、次のように指定します。

```
user1@example.com|zh|GB2312
```

固定ロケールにおける競合解決レベル (#4922030)

ユーザーが特定のロケール (`zh` など) で Identity Server コンソールにログインし、「認証設定」サービスを登録し、サービスのテンプレートを作成してから、ログアウトして別のロケールで再度ログインしても、「競合の解決レベル」項目はもとのロケールの形式で間違って表示されます。

am2bak と bak2am のバージョンメッセージは英語のみ (#4930610)

このリリースの `am2bak` および `bak2am` 復元ユーティリティのバージョンメッセージは、英語だけで表示されます。

自己登録でマルチバイトの名前が機能しない (#4732470)

重複したユーザー ID およびマルチバイトの姓と名を使って自己登録 (メンバーシップ認証サービス) でユーザーを作成する場合、エラーが発生します。マルチバイトのユーザー ID はサポートされていません。

回避策

マルチバイト環境で自己登録を使用してユーザーがログインする場合、管理者はコア認証の「ユーザー ID 生成モードを有効」属性が選択されていないことを確かめる必要があります。

または

ユーザーは自己登録ログインページの「別のユーザー名を作成」オプション選択することができます。

日本語バージョンの Identity Server で Netscape 6.22 と 6.23 を使用できない (#4902421)

日本語バージョンの Identity Server 6.1 では、Netscape 6.22 または 6.23 のコンソールにログインできません。

「時間」条件の形式が変化しない (#4888416)

ポリシー定義の「時間」条件では、ロケールにかかわらず次の形式から時刻表示を変更できません。

```
Hour:Minute AM/PM
```

backup_restore.po の msgid-msgstr ペアのメッセージがローカライズされていない (#4916683)

`backup_restore.po` スクリプトの中に `msgid` と `mgstr` のペアが存在しないため、Directory Server の証明書がバックアップされていないことを通知するメッセージが表示された場合でも、Directory Server はバックアップされています。このメッセージはローカライズされていません。

クライアントディテクション画面がローカライズされていない (#4922013)

このリリースでは、「クライアントディテクション」インタフェースの「現在のスタイルのプロパティ」画面の一部がローカライズされませんでした。

更新した genericHTML クライアントプロパティが適用されない (#4922348)

「クライアントディテクション」サービスの genericHTML クライアントプロパティの文字セットのリストから UTF-8 を消去し、その変更を保存して、「クライアントディテクション」を有効にしてから、ログアウト後に再度ログインしても、ログインページは UTF-8 の文字セットのままです。

回避策

`amserver` を使用して、サーバーを手動で再起動してください。

ログファイルヘッダがローカライズされていない (#4923536)

すべてのログファイルの最初の 2 行がローカライズされていません。具体的には、`Version` セクションと `Fields` セクション、およびそれらのすべてのフィールドです。

amSSO.access の Data フィールドの値がローカライズされていない (#4923549)

`amSSO.access` ログファイルでは、`Data` フィールドのすべての値がローカライズされていません。

Exception.jsp にハードコードされたメッセージがある (#4772313)

`Exception.jsp` はローカライズされていません。つまり、ハードコードされたタイトル、エラーメッセージ、および著作権情報が含まれています。この例外的なエラー jsp ページは非常事態の場合にのみ呼び出されます。たとえば、Directory Server がダウンしたり、Identity Server サービスがまったく機能不能になり、この JSP ページのローカリゼーションが利用できない場合などです。

Cookie

Cookie なしのモードが機能しない (#4967866)
ブラウザが Identity Service にアクセスして、Cookie のサポートが無効になっており、そのブラウザが Cookie をサポートしている場合、ブラウザは以前の Identity Server Cookie の送信を続けます。これは Identity Server リソースへのアクセスが拒否される原因となります。

回避策
次の回避策の中から 1 つを選択してください。

- ブラウザの Cookie キャッシュを消去して Identity Server Cookie をすべて削除する
- ブラウザの Cookie を無効にする

Cookie ハイジャック

セッション Cookie を使用するアプリケーションが信頼できない場合、セキュリティが危険にさらされる可能性があります。
使用している Identity Server の配備で、シングルサインオン (SSO) や クロスドメインシングルサインオン (CDSSO) が有効な場合、`http(s)` セッション Cookie はユーザーのブラウザで設定されます。これらの Cookie は複数のアプリケーションで妥当性検査されます。Identity Server が複数の DNS ドメインにわたり配備されている場合、Liberty プロトコルは、認証済みの DNS ドメインから Web アプリケーションのターゲットドメインに `http(s)` セッション Cookie を転送します。

ユーザーは自動的に Web リソースにサインオンされますが、セッション Cookie を使用するアプリケーションが信頼できない場合、既知のセキュリティ上の弱点があります。アイデンティティプロバイダがユーザーについての認証、承認、およびプロファイルの情報を、サードパーティまたは社内の未承認のグループによって開発されたアプリケーションまたはサービスプロバイダに提供する場合、この弱点が現れることがあります。可能性のあるセキュリティの問題は次のとおりです。

- すべてのアプリケーションが同じ `http` セッション Cookie を共有。これによって要注意のアプリケーションがセッション Cookie をハイジャックして、別のアプリケーションに対してユーザーのように振る舞うことが可能
- アプリケーションが `https` プロトコルを使用しない場合、セッション Cookie はネットワーク盗聴されやすくなる
- 1 つのアプリケーションだけがハッキングされる場合でも、インフラストラクチャ全体が損なわれる危険にされされる状態になる
- 要注意のアプリケーションはセッション Cookie を使用して、ユーザーのプロファイル属性を取得することができ、さらに修正してしまう可能性もある。ユーザーに管理権限が付与されている場合、そのアプリケーションによって非常に多くの損害が発生する可能性がある

回避策
次のステップに従ってください。

1. Identity Server 管理コンソールを使用して各エージェントのエントリを作成します。
   a. エントリの作成が必要なエージェントを含む組織で、「表示」メニューから「エージェント」を選択し、「新規」をクリックします。
   b. 次の情報を入力してください。

      名前 : エージェントの名前またはアイデンティティを入力します。例 : i.e. `agent123`

      パスワード : エージェントのパスワードを入力します。例 : `agent123`

      パスワード (確認): パスワードを確認します。

      説明 : エージェントの簡単な説明を入力してください。たとえば、エージェントインスタンス名またはそれが保護しているアプリケーションの名前を入力できます。

      エージェントキー値 : エージェントプロパティをキーと値のペアで設定してください。このプロパティは、ユーザーに関する証明情報のアサーションを求めるエージェントの要求を受信するため、Identity Server によって使用されます。

      `agentRootURL` のプロパティ値として、ポート番号のあるエージェント URL と同じ値を入力します。`agentRootURL` 値は大文字と小文字を区別してください。

      例 : `agentRootURL=http://`*`server_name:99`*`/`

      デバイスの状態 : エージェントのデバイスの状態を入力してください。「アクティブ」に設定されている場合、エージェントは Identity Server に対して認証および通信を行うことができます。「非アクティブ」に設定されている場合、エージェントは Identity Server に対して認証を行うことができません。
   c. 「了解」をクリックします。
2. ステップ 1b で入力したパスワードに関して次のコマンドを実行してください。

   ```
   /opt/SUNWam/agents/bin/crypt_util agent123
   ```

   この結果次のような出力があります。

   ```
   WnmKUCg/y3l404ivWY6HPQ==
   ```

3. AMAgent.properties を変更し、新しい値を反映させて、エージェントを再起動します。
例：

```
# The username and password to use for the Application authentication
module.


com.sun.am.policy.am.username = agent123
com.sun.am.policy.am.password = WnmKUCg/y3l404ivWY6HPQ==


# Cross-Domain Single Sign On URL

# Is CDSSO enabled.

com.sun.am.policy.agents.cdsso-enabled=true


# This is the URL the user will be redirected to after successful login

# in a CDSSO Scenario.

com.sun.am.policy.agents.cdcservletURL =
http://server.example.com:port/amserver/cdcservlet
```

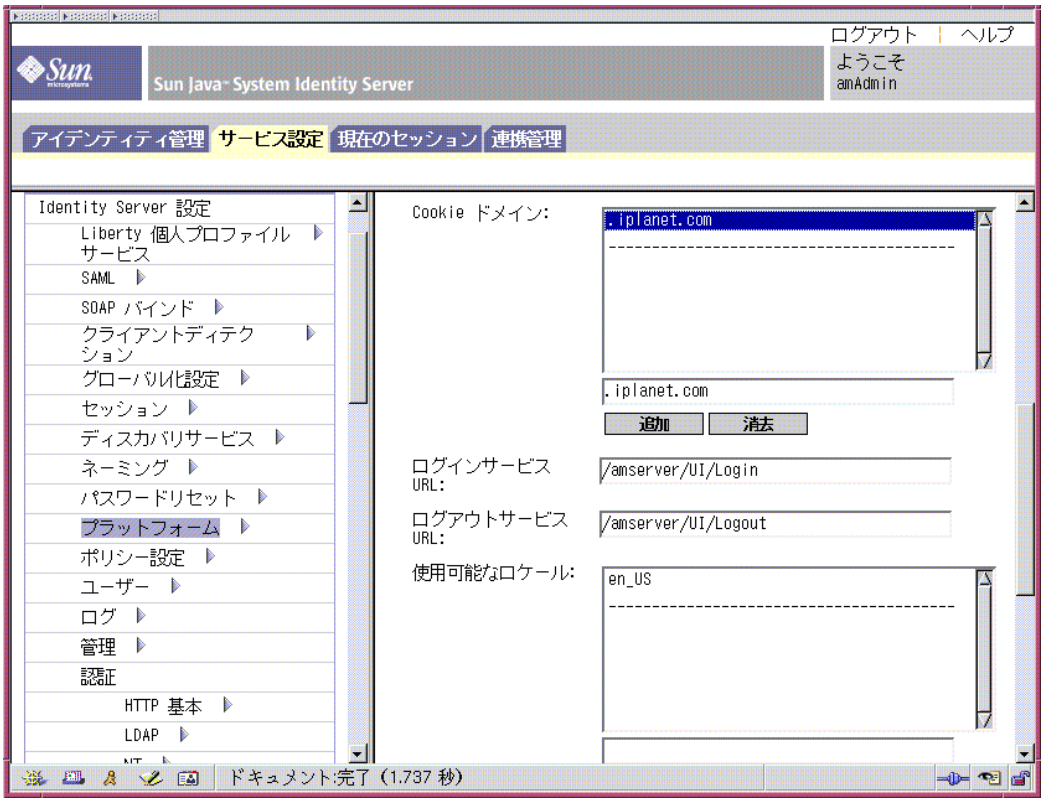
4. AMConfig.properties を変更し、新しい値を反映させて、Identity Server を再起動します。
例：

```
com.sun.identity.enableUniqueSSOTokenCookie=true

com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNS
erver


com.sun.identity.authentication.uniqueCookieDomain=example.com
```

5. Identity Server 管理コンソールで、「サービス設定」>「プラットフォーム」を選択します。



6. 「Cookie ドメイン」リストで、Cookie ドメイン名を次のように変更してください。

   a. デフォルトのドメイン「iplanet.com」を選択して、「削除」をクリックします。

   b. Identity Server インストールのホスト名を入力して「追加」をクリックします。

   例 : server.example.com

   ブラウザに設定された次のような 2 つの Cookie を確認する必要があります。

Cookie	ホスト名
iPlanetDirectoryPro	server.example.com
sunIdentityServerAuthNServer	example.com

再配布可能ファイル

Sun Java System Identity Server 2004Q2 には、再配布可能なファイルはありません。

問題の報告およびフィードバックの提供方法

Sun Java System Identity Server 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/supportraining`

  このサイトには、ナレッジベース、オンラインサポートセンター、ProductTracker へのリンクと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。
- 保守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の説明
- 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://docs.sun.com/coll/entsys_04`

該当の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先頭に記述されている 7 桁または 9 桁の番号です。たとえば、このリソースノートドキュメントの Part No. は 817-7133 です。

Sun が提供しているその他の情報

その他の Sun Java System 情報については、次の Web サイトを参照してください。

- Sun Java System マニュアル
  `http://docs.sun.com/db/prod/entsys?l=ja`
- Sun Java System プロフェッショナルサービス
  `http://www.sun.com/service/products/software/javaenterprisesystem/`
- Sun Java System ソフトウェア製品およびサービス
  `http://wwws.sun.com/software/`
- Sun Java System ソフトウェアサポートサービス
  `http://www.sun.com/supportraining`
- Sun Java System サポートおよびナレッジベース
  `http://sunsolve.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/products/software/javaenterprisesystem`
- Sun Java System 開発者用情報
  `http://developers.sun.com/`
- Sun 開発者サポートサービス
  `http://www.sun.com/developers/support`

Copyright © 2004 Sun Microsystems, Inc. All rights reserved.

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、http://www.sun.com/patents の一覧に示される米国特許、および米国をはじめとする他の国々で取得された、または申請中の特許などが含まれています。

SUN PROPRIETARY/CONFIDENTIAL.

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.

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、米国および他の国々における同社の商標または登録商標です。