Sun Java System Access Manager 7.1 リリースノート

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

Part No: 820–0363
2007 年 7 月

070828@18135

目次

Sun Java System Access Manager 7.1 リリースノート

2007 年 7 月

Part No. 820-0363

Sun Java™ System Access Manager 7.1 リリースノートには、Access Manager の新機能や既知の問題点 (適用できるものがある場合は回避策も含む) など、Sun Java Enterprise System (Java ES) リリースの重要な情報が含まれています。このリリースのインストールおよび使用を始める前に、このリリースノートをお読みください。

Access Manager コレクションを含む Java ES 製品のマニュアルを確認するには、`http://docs.sun.com/prod/entsys.05q4` を参照してください。

ソフトウェアをインストールおよび設定する前だけでなく、それ以降も定期的にこのサイトをチェックして、最新の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。

改訂履歴

次の表に、Access Manager 7.1 リリースノートの改訂履歴を示します。

表1 改訂履歴

日付	変更の説明
2006 年 7 月	ベータリリース。
2007 年 3 月	Java Enterprise System 5 リリース
2007 年 5 月	既知の問題 6555040、6550261、6554379、6554372、6480354 を新たに追加
2007 年 6 月	既知の問題 6562076、6490150 を新たに追加
2007 年 7 月	既知の問題 6485695 を新たに追加

Sun Java System Access Manager 7.1 について

Sun Java System Access Manager は、企業内および企業間 (B2B) のバリューチェーンで、組織が Web アプリケーションおよびその他のリソースにセキュリティー保護されたアクセスを行うことができるようにする Sun のアイデンティティー管理インフラストラクチャーの一部です。

Access Manager は、以下の主要な機能を提供します。

- ロールに基づくアクセス制御およびルールに基づくアクセス制御の両方を使用した、集中認証および承認サービス
- 組織の Web ベースアプリケーションに対するシングルサインオン (SSO) アクセス
- Liberty Alliance Project および Security Assertions Markup Language (SAML) による連携アイデンティティーのサポート
- Access Manager コンポーネントによるその後の分析、報告、および監査のための、管理者およびユーザーのアクティビティーを含む重要な情報のログ作成

このリリースでの新機能

このリリースには、次の新機能が含まれています。

- 7 ページの「Java ES Monitoring Framework の統合」
- 7 ページの「Web サービスセキュリティー」
- 7 ページの「単一の Access Manager WAR ファイルによる配備」
- 7 ページの「コアサービスの拡張機能」
- 10 ページの「非推奨に関する通知および発表」

Java ES Monitoring Framework の統合

Access Manager 7.1 は、Java Management Extensions (JMX) により Java Enterprise System Monitoring Framework に統合されています。JMX テクノロジは、デバイス、アプリケーション、およびサービス駆動型ネットワークの管理と監視のための分散ソリューション、Web ベースソリューション、モジュール化ソリューション、および動的ソリューションを構築するツールを提供します。JMX テクノロジの一般的な用途には、次のものがあります。アプリケーション設定の調査と変更、アプリケーション動作に関する統計の蓄積、状態の変化と誤動作の通知。データは集中監視コンソールに送信されます。

Access Manager 7.1 は Java ES Monitoring Framework を使用して、次のような統計情報やサービス関連のデータを収集します。

- 認証の試行数、成功数、失敗数
- ポリシーキャッシュの統計情報
- ポリシー評価のトランザクション回数

Web サービスセキュリティー

Access Manager 7.1 は、次の方法で Web サービスに対する認証機能を拡張しています。

- 送信メッセージにトークンを挿入する
- 着信メッセージのセキュリティートークンを評価する
- 新規アプリケーションに対して認証プロバイダのポイントアンドクリック選択を有効にする

単一の Access Manager WAR ファイルによる配備

Access Manager には、サポート対象のプラットフォームにあるどのコンテナに Access Manager サービスを配備するときにも使用できる、単一の WAR ファイルが組み込まれています。Access Manager WAR ファイルは、JAR、XML、JSP、HTML、GIF ファイルや各種プロパティーファイルといった複数のファイルを配備する Java Enterprise System インストーラと共存します。

コアサービスの拡張機能

サポートされる **Web** コンテナ

- Sun Java System Web Server 7.0
- Sun Java System Application Server 8.2

- BEA WL 8.1 SP4
- IBM WebSphere 5.1.1.6

Monitoring Framework の統合

Access Manager は JES Monitoring Framework を使用して、次の情報を監視できます。

1. 認証
   - 認証の試行数
   - リモート認証の試行数 (オプション)
   - 認証の成功数
   - 認証の失敗数
   - ログアウト操作の成功数
   - ログアウト操作の失敗数
   - 実行状態および待機状態の各モジュールのトランザクション時間 (可能な場合)
2. セッション
   - セッションテーブルのサイズ (セッションの最大数)
   - アクティブなセッションの数 (増分カウンタ)
3. プロファイルサービス
   - 最大キャッシュサイズ
   - 実行操作および待機操作でのトランザクション時間
4. ポリシー
   - 受信リクエストや送信リクエストのポリシー評価
   - 対象のプラグインの LDAP サーバーに関するポリシー接続プール統計

認証モジュール

- 負荷分散配備では、分散認証サービスを 1 つのサーバーに固定する必要はありません
- 負荷分散配備では、認証サービスおよび認証サーバーを 1 つのサーバーに固定する必要はありません
- 認証サービス、ポリシーエージェント、およびポリシーサービス間の複合アドバイスのサポート。`AuthenticateToRealm` 条件、 AuthenticateToService 条件、およびすべての条件に対するレルム修飾が含まれます。
- アドバイス組織 (認証条件によって資格を与えられたレルム)
- 認証設定/ 認証連鎖 (`AuthServiceCondition`)
- 認証連鎖を実施する場合に、モジュールベースの認証を却下できるようになりました
- 分散認証サービスは証明書認証モジュールをサポートします
- 分散認証 UI に `CertAuth` が追加され、完全な機能を備えた資格エクストラクタ表示になりました

- 指定のレルム用に設定されたデータストアに対する認証をすぐに行える、新しいデータストア認証モジュール
- アカウントロックアウト設定が、複数の AM サーバーインスタンスにわたって持続的に使用できるようになりました
- 事後処理 SPI クラスのチェーン

ポリシーモジュール

- 新規ポリシー条件 `AuthenticateToServiceCondition` が追加され、特定の認証サービス連鎖に対してユーザー認証ができるようになりました。
- 新規ポリシー条件 `AuthenticateToRealmCondition` が追加され、特定のレルムに対してユーザー認証ができるようになりました。
- 新規ポリシー条件 `LDAPFilterCondition` が追加され、指定した LDAP フィルタでユーザーの照合ができるようになりました。
- サブディレクトリを除いたディレクトリの内容を保護する 1 レベルワイルドカード比較のサポート。
- 組織エイリアス参照がグローバルポリシー設定で有効になっている場合は、親レルムからの明示的な参照ポリシーを持たないサブレルムにポリシーを作成できます。
- `AuthLevelCondition` では、認証レベルに加えてレルム名を指定できます。
- `AuthSchemeCondition` では、認証モジュール名に加えてレルム名を指定できます。

サービス管理モジュール

- サービス管理/ポリシー設定の Active Directory への格納のサポート

Access Manager SDK

- ユーザーをデフォルトのアイデンティティーリポジトリフレームワークのデータベースに対して認証する API のサポート

Web サービスサポート

- Liberty ID-WSF SOAP プロバイダ: Liberty ID-WSF SOAP バインディングを Access Manager による実装としてカプセル化する認証プロバイダ。クライアントおよびサービスプロバイダで構成されます。
- HTTP 層 SSO プロバイダ: サーバー側の Access Manager ベース SSO をカプセル化する HttpServlet 層認証プロバイダ

インストールモジュール

- Access Manager を 1 つの WAR ファイルに再パッケージ化し、J2EE アプリケーションとして Web 配備可能にします
- 64 ビット SJSWeb Server 7.0 のサポート - 64 ビット JVM をサポート

委任モジュール

- 委任特権のグループ化のサポート

アップグレード

- 次のバージョンから Access Manager 7.1 へのアップグレードをサポートします。Access Manager 7.0 2005Q4、Access Manager 6.3 2005Q1、および Identity Server 6.2 2004Q2。

ロギング

- ロギングモジュールでの委任のサポート - ログファイルを読み書きする権限をどのアイデンティティーに付与するかを制御します。
- JCE ベースの `SecureLogHelper` のサポート - JSS に加えて JCE がセキュリティー保護された ロギング実装のセキュリティープロバイダとして使用可能になります。

非推奨に関する通知および発表

Sun Java(TM) System Access Manager 7.1 アイデンティティー管理 API および XML テンプレートを使用することにより、システム管理者は Sun Java System Directory Server でアイデンティティーエントリを作成、削除、および管理することができます。Access Manager ではアイデンティティー管理用の API も用意しています。開発者は `com.iplanet.am.sdk` パッケージに定義されている公開インタフェースおよびクラスを使用し、管理機能を外部アプリケーションまたはサービスに統合して、Access Manager によって管理されるようにします。Access Manager API を使用することで、アイデンティティー関連のオブジェクトを作成または削除するだけでなく、Directory Server との間でオブジェクトの属性の取得、変更、追加、または削除を行うこともできます。

Access Manager の `com.iplanet.am.sdk` パッケージ (通称 AMSDK) は、今後の Access Manager リリースには組み込まれません。この中には、関連するすべての API および XML テンプレートが含まれます。現在利用可能な移行オプションはなく、今後も利用可能になる予定はありません。Sun Java System Identity Manager によって提供されるユーザープロビジョニングソリューションは、今すぐ使用を開始できる代替手段です。Sun Java System Identity Manager の詳細については、`http://www.sun.com/software/products/identity_mgr/index.xml` を参照してください。

ハードウェアおよびソフトウェアの要件

次の表に、このリリースに必要なハードウェアとソフトウェアを示します。

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	要件
オペレーティングシステム (OS)	■ SPARC、x86、および x64 ベースシステム上の Solaris™10。全体ルートローカルゾーンと疎ルートゾーンのサポートを含みます。 ■ SPARC および x86 ベースシステム上の Solaris 9。 ■ Red Hat™ Enterprise Linux 3 および 4、すべてのアップデートリリース Advanced Server (32 および 64 ビットバージョン) および Enterprise Server (32 および 64 ビットバージョン) ■ Windows x86 上の Windows 2000 Advanced Server、Data Center Server バージョン SP4 x86 および x64 ベースシステム上の Windows 2003 Standard (32 および 64 ビットバージョン)、Enterprise (32 および 64 ビットバージョン)、Data Center Server (32 ビットバージョン) x86 ベースシステム上の Windows XP Professional SP2 PA-RISC 2.0 上の 64 ビット HP-UX 11i v1 (uname -r = 11.11) サポートされているオペレーティングシステムについての更新された最新のリストは、『Sun Java Enterprise System 5 リリースノート (UNIX 版)』の『Sun Java Enterprise System 5 リリースノート (UNIX 版)』の「プラットフォームの要件と問題点」、または『Sun Java Enterprise System 5 リリースノート (Windows 版)』の『Sun Java Enterprise System 5 リリースノート (Windows 版)』の「ハードウェアとソフトウェアのプラットフォーム情報」を参照してください。
Java 2 Standard Edition (J2SE)	J2SE プラットフォーム 6.0、5.0 Update 9 (HP-UX: 1.5.0.03)、および 1.4.2 Update 11

表 2 ハードウェアおよびソフトウェアの要件 (続き)

コンポーネント	要件
ディレクトリサーバー	Access Manager 情報ツリー: Sun Java System Directory Server 6.0 または Sun Java System Directory Server 5.2 2005Q4
	Access Manager アイデンティティーリポジトリ: Sun Java System Directory Server 5.2、6.0、および Microsoft Active Directory
Web コンテナ	Sun Java SystemWeb Server 7.0。サポートされるプラットフォーム/OS の組み合わせであれば、Web Server インスタンスを 64 ビット JVM 内で実行することもできます。サポートされるプラットフォーム: Solaris 9/SPARC、Solaris 10/SPARC、Solaris 10/AMD64、Red Hat AS または ES 3.0/AMD64、Red Hat AS または ES 4.0/AMD64
	Sun Java System Application Server Enterprise Edition 8.2
	BEA WebLogic 8.1 SP4
	IBM WebSphere Application Server 5.1.1.6
RAM	基本テスト: 512M バイト
	実際の配備: スレッド、Access Manager SDK、HTTP サーバー、およびその他の内部用に 1G バイト
ディスク容量	Access Manager および関連するアプリケーション用に 512M バイト

コンポーネントのその他のバージョンのサポートについての質問は、Sun Microsystems の技術担当者にご連絡ください。

サポートされているブラウザ

次の表に、Sun Java Enterprise System 5 リリースでサポートされているブラウザを示します。

表3 サポートされているブラウザ

ブラウザ	プラットフォーム
Firefox 1.0.7	Windows XP
	Windows 2000
	Solaris OS、バージョン 9 および 10
	Red Hat Linux 3 および 4
	Mac OS X
Microsoft Internet Explorer™ 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows™ 2000
Mozilla™ 1.7.12	Solaris OS、バージョン 9 および 10
	Windows XP
	Windows 2000
	Red Hat Linux 3 および 4
	Mac OS X
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000
Netscape Communicator 7.1	Solaris OS、バージョン 9 および 10

互換性に関する一般情報

AMSDK と Access Manager サーバーとのシステム間非互換性

次の Java Enterprise System リリースでは、次に示す組み合わせには AMSDK と Access Manager サーバー間での互換性がありません。

- Java Enterprise System 2004Q2 AMSDK は、Java Enterprise System 5 Access Manager サーバー (このリリース) と互換性がありません。

- Java Enterprise System 5 AMSDK (このリリース) は、Java Enterprise System Access Manger 2004Q2 (以前の Identity Server) サーバーと互換性がありません。

Access Manager HPUX バージョンのアップグレードは、サポートされていない

HPUX バージョンには、Access Manager 7 2005Q4 から Access Manger 7.1 (このリリース) へのアップグレードパスのサポートがありません。

Access Manager 旧バージョンモード

Access Manager を次の製品とともにインストールする場合は、Access Manager 旧バージョン (6.x) モードを選択する必要があります。

- Sun Java System Portal Server
- Messaging Server、Calendar Server、Instant Messaging、または Delegated Administrator を含む、Sun Java System Communications Services サーバー

Java ES インストーラの実行方法によっては、Access Manager 旧バージョン (6.x) モードを選択します。

- 14 ページの「状態ファイルを使用した Java ES サイレントインストール」
- 15 ページの「グラフィカルモードでの「今すぐ設定」インストールオプション」
- 15 ページの「テキストベースモードでの「今すぐ設定」インストールオプション」
- 15 ページの「「後で設定」インストールオプション」

Access Manager 7.1 のインストールに関する決定については、15 ページの「Access Manager モードの確認」を参照してください。

状態ファイルを使用した Java ES サイレントインストール

Java ES インストーラのサイレントインストールは、非対話モードで、同じような設定の複数のホストサーバーに Java ES コンポーネントをインストールできます。最初にインストーラを実行して状態ファイルを生成し (実際にはコンポーネントをインストールせずに)、Access Manager およびほかのコンポーネントをインストールする予定の各ホストサーバー用に、状態ファイルのコピーを編集します。

Access Manager の旧バージョン (6.x) モードを選択するには、インストーラをサイレントモードで実行する前に、状態ファイルで (ほかのパラメータと一緒に) 次のパラメータを設定します。

```
...
AM_REALM = disabled
...
```

状態ファイルを使用した Java ES インストーラのサイレントモードでの実行方法の詳細については、『Sun Java Enterprise System 5 インストールガイド (UNIX 版)』の第 5 章「サイレントモードでのインストール」を参照してください。

グラフィカルモードでの「今すぐ設定」インストールオプション

Java ES インストーラをグラフィカルモードで実行し、「今すぐ設定」オプションを選択した場合、「Access Manager: 管理 (1 / 6)」パネルでデフォルトの値である「旧バージョンモード (バージョン 6.x スタイル)」を選択します。

テキストベースモードでの「今すぐ設定」インストールオプション

Java ES インストーラをテキストベースモードで実行しており、「今すぐ設定」オプションを選択した場合、インストールタイプ (レルム - Realm/旧バージョン - Legacy) [Legacy] でデフォルトの値である Legacy を選択します。

「後で設定」インストールオプション

Java ES インストーラを「後で設定」オプションで実行した場合、インストール後に amconfig スクリプトを実行して Access Manager を設定する必要があります。旧バージョン (6.x) モードを選択するには、設定スクリプト入力ファイル (amsamplesilent) で次のパラメータを設定します。

```
...
AM_REALM=disabled
...
```

amconfig スクリプトを実行した Access Manager の設定については、『Sun Java System Access Manager 7.1 管理ガイド』を参照してください。

Access Manager モードの確認

Access Manager 7.1 のインストールが、レルムモードまたは旧バージョンモードのどちらの設定で実行されたかを確認するには、次のように指定します。

```
http(s)://host:port/amserver/SMSServlet?method=isRealmEnabled
```

結果は次のとおりです。

- true: レルムモード
- false: 旧バージョンモード

Access Manager ポリシーエージェント

次の表に、ポリシーエージェントと Access Manager 7.1 モードとの互換性を示します。

表 4　ポリシーエージェントと Access Manager 7.1 モードとの互換性

エージェントとバージョン	互換モード
Web および J2EE エージェント、バージョン 2.2	旧バージョンモードおよびレルムモード
Web および J2EE エージェント、バージョン 2.1 は、Access Manager 7.1 ではサポートされていません。	

既知の問題点と制限事項

この節では、Access Manager 7.1 release 時点での既知の問題点について (適用可能な回避策がある場合はそれとともに) 説明します。

インストールに関する問題

インストールに関する問題については、JES 5 リリースノートで説明しています。『Sun Java Enterprise System 5 リリースノート (UNIX 版)』の「Access Manager のインストールに関する問題点」の節を参照してください。

ここでは、次の既知の問題について説明します。

WebLogic に単一の Access Manager WAR を配備した場合は、Access Manager がクライアント SDK と通信するために JAX-RPC 1.0 JAR ファイルが必要である (6555040)

Weblogic 8.1 に単一の WAR を配備した場合は、JAX-RPC の初期化に関して既知の問題があります。Access Manager がクライアント SDK と通信するには、JAX-RCP 1.1 の jar ファイルを JAX-RPC 1.0 の jar ファイルに置き換える必要があります。

回避策:

WAR ファイルを入手するには、2 つの方法があります。1 つは Java Enterprise System 5 インストーラで Access Manager に対して「後で設定」オプションを設定する方法、もう 1 つは Sun のダウンロードサイトから入手する方法です。

JES 5 インストーラで「後で設定」オプションを設定して WAR ファイルを生成した場合は、次の手順に従います。

1. *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib` から次の JAXRPC 1.1 `.jar` ファイルを削除します。
   - `jaxrpc-api.jar`
   - `jaxrpc-spi.jar`
   - `jaxrpc-impl.jar`
2. 次の `.jar` ファイルをそれぞれの場所から *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib` にコピーします。
   - `/opt/SUNWam/lib/jaxrpc 1.0` の `jaxrpc-api.jar`
   - `/opt/SUNWam/lib/jaxrpc 1.0` の `jaxrpc_ri.jar`
   - `/opt/SUNWmfwk/lib` の `commons-logging.jar`

3. *AccessManager-base*/SUNWam/bin/ に移動して、次のコマンドを実行します。

   amconfig –s *samplesilent*

   amconfig スクリプトを使用して Access Manager を設定する方法の詳細については、『Access Manager Post Installation Guide』の「Running the Access Manager amconfig Script」を参照してください。

Sun ダウンロードサイト (http://www.sun.com/download/index.jsp) から WAR ファイルを入手した場合は、次の手順に従います。

1. *ZIP_ROOT*/applications/jdk14/amserver.war ファイルを入手し、/tmp/am-staging などのステージング領域に展開します。
2. /tmp/am-staging/WEB-INF/lib から次の JAXRPC 1.1 .jar ファイルを削除します。
   - jaxrpc-api.jar
   - jaxrpc-spi.jar
   - jaxrpc-impl.jar
3. *ZIP_ROOT*/applications/jdk14/jarFix ディレクトリにある次の JAXRPC 1.0 .jar ファイルおよび commons logging .jar ファイルを /tmp/am-staging/WEB-INF/lib にコピーします。
   - jaxrpc-api.jar
   - jaxrpc-ri.jar
   - commons-logging.jar
4. Access Manager WAR を再作成して配備します。詳細については、『Access Manager Post Installation Guide』の「Deploying Access Manager as a Single WAR File」を参照してください。

JES 5 インストーラで Websphere 5.1 用に単一の WAR を生成した場合は、追加の .jar ファイルが必要である (6550261)

JES 5 インストーラで「後で設定」オプションを使用して Access Manager の単一の WAR を生成した場合は、Websphere 5.1 を配備する前に追加の .jar ファイルが必要です。

回避策:

1. /usr/share/lib にある jsr173_api.jar を *AcessManager-base*/opt/SUNWam/web-src/WEB-INF/lib ディレクトリにコピーします。
2. *AccessManager-base*/SUNWam/bin/ に移動して、次のコマンドを実行します。

   amconfig –s *samplesilent*

   amconfig スクリプトを使用して Access Manager を設定する方法の詳細については、『Access Manager Post Installation Guid』の「Running the Access Manager amconfig Script」を参照してください。

Webshpere に単一の WAR を配備した場合は、クライアント SDK と通信するために server.xml に変更を加える必要がある (6554379)

Websphere 5.1 に単一の WAR を配備した場合、Access Manager がクライアント SDK と正常に通信するには、`server.xml` ファイルに変更を加える必要があります。

回避策:

`server.xml` ファイルを正しく変更するには、次の手順を参照してください。

1. `amserver.war` ファイルを入手します。単一の WAR ファイルを入手するには、2 つの方法があります。1 つは JES 5 インストーラで「後で設定」オプションを使用する方法、もう 1 つは Sun ダウンロードサイトから入手する方法です。

   注 – JES 5 インストーラで WAR ファイルを生成した場合は、既知の問題 6550261 に示した手順を完了していることを確認します。

   ---

2. Access Manager WAR を `/tmp/am-staging` などのステージング領域に展開します。
3. 次の共有 `.jar` ファイルを `/tmp/am-staging/WEB-INF/lib` から `/export/jars` などの共有の場所にコピーします。

jaxrpc-api.jar	jaxrpc-spi.jar	jaxrpc-impl.jar	saaj-api.jar
saaj-impl.jar	xercesImpl.jar	namespace.jar	xalan.jar
dom.jar	jax-qname.jar	jaxb-api.jar	jaxb-impl.jar
jaxb-libs.jar	jaxb-xjc.jar	jaxr-api.jar	jaxr-impl.jar
xmlsec.jar	swec.jar	acmecrypt.jar	iaik_ssl.jar
iaik_jce_full.jar	mail.jar	activation.jar	relaxngDatatype.jar
xsdlib.jar	mfwk_instrum_tk.jar	FastInfoset.jar	jsr173_api.jar

4. ステージング領域の `/tmp/am-staging/WEB-INF/lib` からこれらの `.jar` ファイルを削除します。
5. Webshpere インスタンスの `server.xml` を更新します。インスタンスのデフォルトの場所が `/opt/WebSphere/AppServer/config/cells/`*node-name*`/nodes/`*node-name*`/servers/server1` である場合は、`server.xml` の *jvmEntries* に次のような変更を加えます。

   ```
   <classpath>/export/jars/jaxrpc-api.jar:/export/jars/jaxrpc-spi.jar:
       /export/jars/jaxrpc-impl.jar:/export/jars/saaj-api.jar:
       /export/jars/saaj-impl.jar:/export/jars/xercesImpl.jar:
       /export/jars/namespace.jar:/export/jars/xalan.jar:/export/jars/dom.jar:
       /export/jars/jax-qname.jar:/export/jars/jaxb-api.jar:/export/jars/jaxb-impl.jar:
       /export/jars/jaxb-libs.jar:/export/jars/jaxb-xjc.jar:/export/jars/jaxr-api.jar:
       /export/jars/jaxr-impl.jar:/export/jars/xmlsec.jar:/export/jars/swec.jar:
       /export/jars/acmecrypt.jar:/export/jars/iaik_ssl.jar:
       /export/jars/iaik_jce_full.jar:/export/jars/mail.jar:
   ```

```
/export/jars/activation.jar::/export/jars/relaxngDatatype.jar:
/export/jars/xsdlib.jar:/export/jars/mfwk_instrum_tk.jar:
/export/jars/FastInfoset.jar:/export/jars/jsr173_api.jar</classpath>
```

6. コンテナを再起動します。
7. /tmp/am-staging にある Access Manager WAR を再作成して配備します。詳細については、『Access Manager Postinstallation Guide』の「Deploying Access Manager as a Single WAR File」を参照してください。

Weblogic および Webshpere で単一の Access Manager WAR の分散認証を機能させるには、変更が必要である (6554372)

Weblogic 8.1 と Websphere 5.1 のどちらでも、コンテナのバージョンが JDK14 であるため、分散認証 WAR には構文解析用の追加の jar ファイルが必要です。JDK14 の `.jar` ファイルは、`.zip` ファイルの次のディレクトリにあります。

ZIP-ROOT`/applications/jdk14/jarFix`

回避策**:**

Weblogic 8.1 の場合:

1. 設定スクリプトを使用して分散認証を設定します。『Access Manager Post Installation Guide』の「Deploying a Distributed Authentication UI Server」を参照してください。
2. 更新された分散認証 WAR を `/tmp/dist-auth` などの一時的な場所に展開します。
3. *ZIP-ROOT*`/applications/jdk14/jarFix` にある `xercesImpl.jar`、`dom.jar` と `xalan.jar` を `/tmp/dist_auth/WEB-INF/lib` ディレクトリにコピーします。
4. 一時的な場所にある分散認証 WAR を再生成し、配備します。詳細については、『Access Manager Post Installation Guide』の「Deploying a Distributed Authentication UI Server WAR File」を参照してください。

Websphere 5.1 の場合:

1. 設定スクリプトを使用して分散認証を設定します。『Access Manager Post Installation Guide』の「Deploying a Distributed Authentication UI Server」を参照してください。
2. 更新された分散認証 WAR を `/tmp/dist_auth/` などの一時的な場所に展開します。
3. *ZIP-ROOT*`/applications/jdk14/jarFix` にある `xercesImpl.jar`、`dom.jar` と `xalan.jar` を `/tmp/dist_auth/WEB-INF/lib` ディレクトリにコピーします。
4. `WEB-INF/web.xml` ファイルを編集して、`jar://web-app_2_3.dtd` を `http://java.sun.com/dtd/web-app_2_3.dtd` に置き換えます。
5. 一時的な場所にある分散認証 WAR を再生成し、配備します。詳細については、『Access Manager Post Installation Guide』の「Deploying a Distributed Authentication UI Server WAR File」を参照してください。

Directory Server に対して単一の WAR の設定ツールを実行できない (6562076)

たとえば、dc=example のように単一コンポーネントから成るルートサフィックスを持つ Directory Server 6 に対して、単一の WAR ファイルとして配備された Access Manager を設定できません。しかし、dc=example,dc=com のような複数コンポーネントのルートサフィックスの場合は設定できます。

回避策: dc=example,dc=com のような複数コンポーネントのルートサフィックスを使用します。

単一の Access Manager WAR を同じホスト上に複数設定すると、例外がスローされる (6490150)

単一の Access Manager WAR の 2 つ目のインスタンスを同じホスト上の Directory Server に対して設定すると、組織エイリアスの更新時に例外がスローされます。この問題は、2 つ目のインスタンスが異なるホスト上で設定された場合は発生しません。

アップグレードに関する問題

アップグレードに関する問題については、『Sun Java Enterprise System 5 リリースノート (UNIX 版)』の「アップグレードの問題」の節で説明しています。

互換性の問題

- 21 ページの「Access Manager のシングルサインオンが汎用 Web クライアントで失敗する (6367058、6429573)」
- 22 ページの「64 ビットモードで実行されている Web Server 7.0 で StackOverflowError が発生する (6449977)」
- 22 ページの「旧バージョンモードでコア認証モジュールに非互換性が存在する (6305840)」
- 23 ページの「Delegated Administrator commadmin ユーティリティーがユーザーを作成しない (6294603)」
- 23 ページの「Delegated Administrator commadmin ユーティリティーが組織を作成しない (6292104)」

Access Manager のシングルサインオンが汎用 Web クライアントで失敗する (6367058、6429573)

Access Manager、Messaging Server、および Calendar Server をインストールし、連動するように設定したあとで、JES5 120955-01 パッチをインストールすると、この問題が発生します。ログインエラーが発生します。Policy Agent 2.1 プロパティーと AMSDK の間に互換性がないことが、このエラーの原因です。現時点では、回避方法はありません。

64 ビットモードで実行されている Web Server 7.0 で StackOverflowError が発生する (6449977)

Access Manager が 64 ビット JVM を使用する Web Server 7.0 インスタンス上に設定されている場合、ユーザーがコンソールログインページにアクセスすると、「サーバーエラー」メッセージが返されます。Web Server エラーログには `StackOverflowError` 例外が含まれます。

回避策: 次の手順で Web Server 設定を変更します。

1. Web Server 管理コンソールに Web Server 管理者としてログインします。
2. 「構成を編集」をクリックします。

   「プラットフォーム」フィールドで「64」を選択してから、「保存」をクリックします。
3. 「Java」タブをクリックしてから、「JVM 設定」タブをクリックします。
   - 「オプション」で、最小ヒープサイズエントリ (-Xms など) を探します。最小ヒープサイズ値は少なくとも 512m である必要があります。たとえば、ヒープサイズ値が -Xms512m 以上ではない場合、値を少なくとも -Xms512m に変更します。
   - 最大ヒープサイズ値は少なくとも 768m である必要があります。最大ヒープサイズが -Xmx768m 以上ではない場合、値を少なくとも -Xmx768m に変更します。
   - Java スタックサイズを `-Xss512k` または `-Xss768k` を使用して、512k または 768k に設定します。この設定を空白にしておくことで、Solaris SPARC 上の 64 ビット JVM のデフォルトサイズ (1024k) のままにすることもできます。
4. 「パフォーマンス」タブをクリックしてから、「スレッドプール設定」リンクをクリックします。

   スタックサイズ値を少なくとも 261144 に変更してから、「保存」をクリックします。
5. 画面右上隅にある「配備保留中」リンクをクリックします。

   「構成の配備」ページで、「配備」ボタンをクリックします。
6. 「結果」ウィンドウで、「了解」をクリックして Web Server インスタンスを再起動します。

   Web Server が再起動したら、「結果」ウィンドウの「閉じる」をクリックします。

旧バージョンモードでコア認証モジュールに非互換性が存在する (6305840)

Access Manager 7 .1 旧バージョンモードでは、Access Manager 6 2005Q1 からのコア認証モジュールに次の非互換性があります。

- 組織認証モジュールが旧バージョンモードで削除されています。
- 「管理者認証設定」および「組織認証設定」の表示方法が変更されました。Access Manager 7.1 コンソールでは、ドロップダウンリストで `ldapService` がデフォルトで選択されています。Access Manager 6 2005Q1 コンソールでは、「編集」ボタンが表示され、LDAP モジュールはデフォルトで選択されませんでした。

回避策: なし。

Delegated Administrator `commadmin` ユーティリティーがユーザーを作成しない (6294603)

Delegated Administrator `commadmin` ユーティリティーを `-S mail,cal` オプションで使用すると、デフォルトドメインにユーザーが作成されません。

回避策: この問題は、Access Manager をバージョン 7.1 にアップブレードして Delegated Administrator をアップグレードしなかった場合に発生します。

Delegated Administrator をアップグレードする予定がない場合は、次の手順を実行します。

1. `UserCalendarService.xml` ファイルで、 `mail`、`icssubcribed`、および `icsfirstday` 属性を必須ではなく省略可能としてマークします。このファイルはデフォルトで、Solaris システム上の `/opt/SUNWcomm/lib/services/` ディレクトリにあります。
2. Access Manager で次のように `amadmin` コマンドを実行して、既存の XML ファイルを削除します。

   ```
   # ./amadmin -u amadmin -w password -r UserCalendarService
   ```

3. Access Manager で、更新した XML ファイルを次のように追加します。

   ```
   # ./amadmin -u amadmin -w password
   -s /opt/SUNWcomm/lib/services/UserCalendarService.xml
   ```

4. Access Manager Web コンテナを再起動します。

Delegated Administrator `commadmin` ユーティリティーが組織を作成しない (6292104)

Delegated Administrator `commadmin` ユーティリティーを `-S mail,cal` オプションで使用すると、組織が作成されません。

回避策: 前の問題の回避策を参照してください。

設定に関する問題

ロードバランサを使用した環境でコンソールのリダイレクションが正しく行われない (6480354)

Access Manager インスタンスがロードバランサとともに配備されている場合、Access Manager コンソールにログインすると、ロードバランサではなく Access Manager インスタンスのいずれかにリダイレクトされる場合があります。ブラウザの URL も Access Manager インスタンスに変更されます。この問題は、たとえば、次の URL を使用してコンソールにログインした場合に発生します。

```
http://loadbalancer.example.com/amserver/realm
```

このリダイレクションは、レルムモードと旧バージョンモードのどちらの配備でも発生する可能性があります。

この問題の回避策は 2 つあります。次のいずれかを使用できます。

1. 次のいずれかの URL でログインします。

   `http://`*loadbalancer*`/amserver/UI/Login`

   `http://`*loadbalancer*`/amserver`

2. `AMConfig.properties` で、`com.sun.identity.loginurl` プロパティーをロードバランサの名前に設定します。これは、ロードバランサとともに配備されている各 Access Manager インスタンスごとに実行する必要があります。

Web コンテナなしで Access Manager SDK をインストールする場合は、通知 URL を更新する必要がある (6491977)

「今すぐ設定」オプションを指定して Java ES 5 インストーラを実行し、Web コンテナなしで Access Manager SDK をインストールすると、AMConfig.properties ファイルの

com.iplanet.am.notification.url プロパティーは NOTIFICATION_URL に設定されます。Web コンテナ設定を特に何もしなければ、ユーザーにリモート Access Manager サーバーからの通知は届きません。

回避策: このプロパティーを次のようにリセットします:
com.iplanet.am.notification.url=""

パスワードが変更されたときに、パスワードリセットサービスが通知エラーを報告する (6455079)

パスワードが変更されると、Access Manager は資格を取得していない送信者名 Identity-Server を使用して電子メール通知を送信します。その結果、amPasswordReset ログにエラーが書き込まれます。次に例を示します。

```
07/19/2006 10:26:04:010 AM PDT: Thread[service-j2ee,5,main]
ERROR: Could not send email to user [Ljava.lang.String;@999262
com.sun.mail.smtp.SMTPSendFailedException: 553 5.5.4 <Identity-Server>...
Domain name required for sender address Identity-Server
```

回避策: /opt/SUNWam/locale/amPasswordResetModuleMsgs.properties の設定を変更します。

- from アドレスを変更します。fromAddress.label=<Identity-Server> を fromAddress.label=<IdentityServer@myhost.company.com> に変更します。
- lockOutEmailFrom プロパティーを変更して、ロックアウト通知が正しい from アドレスを確実に使用するようにします。

プラットフォームサーバーリストおよび FQDN エイリアス属性が更新されない (6309259、6308649)

複数のサーバー配備では、Access Manager を 2 番目 (およびそれ以降) のサーバーにインストールした場合、プラットフォームサーバーリストおよび FQDN エイリアス属性が更新されません。

回避策: レルム/DNS エイリアスおよびプラットフォームサーバーリストエントリを手動で追加します。手順については、『Sun Java System Access Manager 7.1 Postinstallation Guide』の「Adding Additional Instances to the Platform Server List and Realm/DNS Aliases」の節を参照してください。

サービス内の必須属性のデータ妥当性検査 (6308653)

Access Manager 7.1 では、サービス XML ファイルの必須属性には、デフォルト値が割り当てられていなければなりません。

回避策: 値のない必須属性のあるサービスが存在する場合、属性に値を追加してからサービスを再読み込みします。

セキュリティー保護された **WebLogic 8.1** インスタンス上に配備する際の問題に対する回避方法 **(6295863)**

Access Manager 7.1 をセキュリティー保護された (SSL が有効な) BEA WebLogic 8.1 SP4 インスタンスに配備する場合、それぞれの Access Manager Web アプリケーションの配備中に例外が発生します。

回避策**:** 次の手順に従います。

1. BEA から入手可能な WebLogic 8.1 SP4 パッチ JAR `CR210310_81sp4.jar` を適用します。
2. `/opt/SUNWam/bin/amwl81config` スクリプト (Solaris システム) または `/opt/sun/identity/bin/amwl81config` スクリプト (Linux システム) で、`doDeploy` 関数および `undeploy_it` 関数を更新してパッチ JAR のパスを `wl8_classpath` の先頭に追加します。これは Access Manager Web アプリケーションの配備および配備取消しに使用される `classpath` を含む変数です。

   `wl8_classpath` を含む次の行を検索します。

   ```
   wl8_classpath= ...
   ```
3. 手順 2 で検索した行のすぐあとに、次の行を追加します。

   ```
   wl8_classpath=path-to-CR210310_81sp4.jar:$wl8_classpath
   ```

`amconfig` スクリプトが、レルム**/DNS** エイリアスおよびプラットフォームサーバーリストのエントリを更新しない **(6284161)**

複数サーバーの配備では、`amconfig` は追加の Access Manager インスタンスに対してレルム/DNS エイリアスおよびプラットフォームサーバーリストのエントリを更新しません。

回避策**:** レルム/DNS エイリアスおよびプラットフォームサーバーリストエントリを手動で追加します。手順については、『Sun Java System Access Manager 7.1 Postinstallation Guide』の「Adding Additional Instances to the Platform Server List and Realm/DNS Aliases」の節を参照してください。

デフォルトの **Access Manager** モードが設定状態ファイルテンプレートでレルムに設定されている **(6280844)**

デフォルトでは、Access Manager モード (`AM_REALM` 変数) は設定状態ファイルテンプレートで enable に設定されています。

回避策**:** Access Manager を旧バージョンモードでインストールして設定するには、状態ファイルの変数を次のようにセットし直します。

```
AM_REALM = disabled
```

パフォーマンスに関する問題

レルムモードで新しいグループを作成すると、使用されない **ACI** を持つグループ管理者が生成される **(6485695)**

Access Manager がレルムモードでインストールされている場合、新しいグループを作成すると、Access Manager はそのグループを管理するのに必要な ACI を持つグループ管理者を動的に作成します。レルムモードでは、これらのグループ管理者 ACI は使用されません。しかし、Directory Server はサフィックスの下にあるエントリの処理中にこれらの ACI を評価するため、特に配備によって数多くのグループが作成されている場合は、Access Manager のパフォーマンスが低下することがあります。

回避策**:** この問題の回避策は、次の 2 つの部分から成ります。

- 新しいグループが作成されたときに、Access Manager がグループ管理者とそれに対応する ACI を作成しないようにします
- 既存のグループ管理者 ACI を Directory Server から削除します

グループ管理者 **ACI** が作成されないようにする

次の手順を実行すると、新しいグループが作成されたときに、Access Manager がグループ管理者とそれに対応する ACI を作成しないようになります。

注 – この手順により、新しいグループの作成時にグループ管理者とそれに対応する ACI が永続的に作成されなくなります。この手順を使用するのは、この動作が特定の配備に適している場合だけにしてください。

---

1. `amAdminConsole.xml` ファイルをバックアップします。このファイルは、プラットフォーム別に次のディレクトリにあります。
   - Solaris システム: `/etc/opt/SUNWam/config/xml`
   - Linux および HP-UX システム: `/etc/opt/sun/identity/config/xml`
   - Windows システム: *javaes-install-dir*`\identity\config\xml`

     javaes-install-dir は、Java ES 5 のインストールディレクトリを表します。デフォルト値は `C:\Program Files\Sun\JavaES5` です。
2. `amAdminConsole.xml` ファイルで、次のコメント行の間にあるグループ管理者エントリを削除します。

```
<AttributeSchema name="iplanet-am-admin-console-dynamic-aci-list"
    type="list"
    syntax="string"
    i18nKey="g111">
    <DefaultValues>
...
```

```
# Beginning of entry to delete
                <Value>Group Admin|Group Admin Description|ORGANIZATION:aci:
(target="ldap:///GROUPNAME")(targetattr = "*")
(version 3.0; acl "Group and people container admin role";
allow (all) roledn = "ldap:///ROLENAME";)##ORGANIZATION:aci:
(target="ldap:///ORGANIZATION")
(targetfilter=(&amp;FILTER(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Policy Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Organization Admin Role,ORGANIZATION)
(nsroledn=cn=Container Admin Role,ORGANIZATION)
(nsroledn=cn=Organization Policy Admin Role,ORGANIZATION)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members"; allow (read,write,search)
roledn = "ldap:///ROLENAME";)</Value>
# End of entry to delete
...
    </DefaultValues>
</AttributeSchema>
```

3. amadmin を使用して、Access Manager から管理コンソールサービスを削除します。たとえば、Solaris システムでは次のコマンドを実行します。

```
# cd /opt/SUNWam/bin
# ./amadmin -u amadmin -w amadmin_password
--deleteService iPlanetAMAdminConsoleService
```

4. amadmin を使用して、手順 2 で編集した amAdminConsole.xml ファイルから Access Manager に管理コンソールサービスを再読み込みします。

```
# ./amadmin -u amadmin -w amadmin_password
-t /etc/opt/SUNWam/config/xml/amAdminConsole.xml
```

5. Access Manager Web コンテナを再起動します。次の手順に従って Directory Server から ACI を削除する場合は、次の手順の完了後、しばらく待ってから Web コンテナを再起動します。

既存のグループ管理者 **ACI** を削除する

注 – 次の手順では、ldapsearch ユーティリティーと ldapmodify ユーティリティーを使用して、グループ管理者 ACI の検索と削除を行います。配備に Directory Server 6.0 を使用している場合は、Directory Server Control Center (DSCC) または dsconf コマンドを使用して、これらの機能を実行することもできます。詳細については、次の場所にある Directory Server 6.0 のマニュアルを参照してください。

http://docs.sun.com/app/docs/coll/1660.1

次の手順を実行すると、Directory Server にすでに存在するグループ管理者 ACI が削除されます。

1. ldapmodify でグループ管理者 ACI の削除に使用する LDIF ファイルを作成します。これらの ACI を見つけるには、ldapsearch (または、好みに応じてほかのディレクトリ検索ツール) を使用します。

   たとえば、Remove_Group_ACIs.ldif というサンプル LDIF ファイルの次のエントリは、「New Group」というグループの ACI を削除します。

```
dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///cn=New Group,ou=Groups,o=isp")(targetattr = "*")
(version 3.0; acl "Group and people container admin role"; allow (all)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///ou=People,o=isp")(targetattr="nsroledn")
(targattrfilters="add=nsroledn:(!(nsroledn=*)),
del=nsroledn:(!(nsroledn=*))") (version 3.0;
acl "Group admin's right to add user to people container"; allow (add)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///o=isp")
(targetfilter=(&(|(memberof=*cn=New Group,ou=Groups,o=isp)
(iplanet-am-static-group-dn=*cn=New Group,ou=Groups,o=isp))
(!(|(nsroledn=cn=Top-level Admin Role,o=isp)
(nsroledn=cn=Top-level Help Desk Admin Role,o=isp)
(nsroledn=cn=Top-level Policy Admin Role,o=isp)
(nsroledn=cn=Organization Admin Role,o=isp)(
nsroledn=cn=Container Admin Role,o=isp)
(nsroledn=cn=Organization Policy Admin Role,o=isp)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list ||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members";
allow (read,write,search)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)
aci: (target="ldap:///o=isp")(targetattr="*")
```

```
(version 3.0; acl "S1IS special dsame user rights for all under the root suffix";
allow (all) userdn = "ldap: ///cn=dsameuser,ou=DSAME Users,o=isp"; )
```

2. 前の手順で示した LDIF ファイルを指定した `ldapmodify` を使用して、Directory Server からグループ ACI を削除します。たとえば、次のように指定します。

```
# ldapmodify -h ds-host -p 389 -D "cn=Directory Manager"
-w ds-bind-password -f Remove_Group_ACIs.ldif
```

3. Access Manager Web コンテナを再起動します。

Access Manager コンソールに関する問題

新しい Access Manager コンソールは CoS テンプレート優先度を設定できない (6309262)

新しい Access Manager 7.1 コンソールでは、サービスクラス (CoS) のテンプレート優先度を設定または変更できません。

回避策: Access Manager 6 2005Q1 コンソールにログインし、CoS テンプレート優先度を設定または変更します。

Portal Server 関連のサービスを追加すると、古いコンソールが表示される (6293299)

Portal Server および Access Manager は同じサーバーにインストールされます。旧バージョンモードでインストールされた Access Manager で、 `/amserver` を使用して新しい Access Manager コンソールにログインします。既存のユーザーを選択して NetFile または Netlet などのサービスを追加しようとすると、古い Access Manager コンソール (`/amconsle`) が突然表示されます。

回避策: なし。Portal Server の現在のバージョンには、Access Manager 6 2005Q1 コンソールが必要です。

リソース制限に達すると、コンソールは **Directory Server** から設定した結果を返さない **(6239724)**

Directory Server をインストールしてから Access Manager を既存の DIT オプションでインストールします。Access Manager コンソールにログインし、グループを作成します。グループ内のユーザーを編集します。たとえば、フィルタ `uid=*999*` でユーザーを追加します。その結果表示されるリストボックスは空で、コンソールはエラー、情報または警告のメッセージをまったく表示しません。

回避策: グループのメンバーシップは、Directory Server 検索サイズの上限よりも多くすることはできません。グループのメンバーシップが多い場合、それに応じて検索サイズの上限を変更します。

データ移行後に `ContainerDefaultTemplateRole` 属性を追加する必要がある **(4677779)**

旧バージョンモードでは、Access Manager で作成されていないユーザーのロールは組織の下に表示されません。デバッグモードで、次のメッセージが表示されます。

```
ERROR: DesktopServlet.handleException()
com.iplanet.portalserver.desktop.DesktopException:
DesktopServlet.doGetPost(): no privilige to execute desktop
```

このエラーは Java ES インストーラ移行スクリプトを実行すると、明らかになります。組織を既存のディレクトリ情報ツリー (DIT) またはほかのソースから移行した場合に、`ContainerDefaultTemplateRole` 属性は自動的に組織に追加されません。

回避策: Directory Server コンソールを使用して、別の Access Manager の組織から `ContainerDefaultTemplateRole` 属性をコピーし、影響を受ける組織に追加します。

コマンド行に関する問題

Organization Admin role のみを割り当てられた管理者は、**amadmin** コマンド行ユーティリティーを用いて新規ユーザーを作成できない **(6480776)**

Organization Admin role のみが割り当てられている管理者は、ロギング特権が十分でないため、amadmin コマンド行ユーティリティーを使用して新規ユーザーを作成することができません。

回避策: Organization Admin role と Top-Level Admin Role の両方が割り当てられていると、ユーザーを作成できます。そのためには、管理コンソールで次のことを行います。

1. 組織管理者が属する組織に移動します。

2. 「権限」タブをクリックします。
3. 「Organization Admin Role」リンクをクリックします。
4. 「すべてのログファイルに対する読み取りおよび書き込みのアクセス」または「すべてのログファイルに対する書き込みのアクセス」を選択します。
5. 「保存」をクリックします。

SDK およびクライアントに関する問題

サーバーを再起動したあと、クライアントが通知を受け取れない (6309161)

クライアント SDK (`amclientsdk.jar`) を使用して書かれたアプリケーションは、サーバーを再起動しても通知を受け取れません。

回避策: なし。

サービススキーマの変更後、SDK クライアントを再起動する必要がある (6292616)

任意のサービススキーマを変更した場合、`ServiceSchema.getGlobalSchema` は新しいスキーマではなく古いスキーマを返します。

回避策: サービススキーマを変更したあと、クライアントを再起動します。

この問題はパッチ 1 で修正されています。

認証に関する問題

アプリケーションユーザーに十分な特権がないと、分散認証 UI サーバーのパフォーマンスが落ちる (6470055)

デフォルトアプリケーションユーザー (anonymous など) を使用して分散認証 UI サーバーを配備すると、デフォルトアプリケーションユーザーの特権が制限されているため、パフォーマンスが著しく落ちます。

回避策: 適切な特権を持つ新規ユーザーを作成します。

適切な ACI を持つ新規ユーザーを作成するには、次の手順に従います。

1. Access Manager コンソールで、新規ユーザーを作成します。たとえば、`AuthUIuser` という名前のユーザーを作成します。
2. Directory Server コンソールで、次の ACI を追加します。

```
dn:ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>
changetype:modifyadd:aci
aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>")
(targetattr = "*"(version 3.0; acl "SunAM client data anonymous access";
allow (read, search, compare) userdn = "ldap:///<AuthUIuser's DN>";)
```

   `userdn` が `"ldap:///<AuthUIuser's DN>"` に設定されていることに注意してください。

3. `amsilent` ファイルの編集および `amadmin` コマンドの実行については、『Sun Java System Access Manager 7.1 Postinstallation Guide』の「To Install and Configure a Distributed Authentication UI Server」で説明している手順を参照してください。
4. `amsilent` ファイルで、次のプロパティーを設定します。

   APPLICATION_USER　`AuthUIuser` と入力します。

   APPLICATION_PASSWD　`AuthUIuser` のパスワードを入力します。

5. ファイルを保存します。
6. 新しい設定ファイルを使用して、`amconfig` スクリプトを実行します。たとえば、Access Manager がデフォルトディレクトリにインストールされた Solaris システムでは、次のように入力します。

```
# cd /opt/SUNWam/bin
# ./amconfig -s ./DistAuth_config
```

7. 分散認証 UI サーバー上の Web コンテナを再起動します。

旧バージョン (互換) モードの統計サービスの Access Manager デフォルト設定に互換性がない (6286628)

Access Manager を旧バージョンモードでインストールしたあと、統計サービスのデフォルト設定が変更されています。

- サービスがデフォルトでオンになっています (com.iplanet.services.stats.state=file)。以前はオフでした。
- デフォルトの間隔 (com.iplanet.am.stats.interval) が 3600 から 60 に変更されています。
- デフォルトの統計ディレクトリ (com.iplanet.services.stats.directory) が /var/opt/SUNWam/debug から /var/opt/SUNWam/stats に変更されています。

回避策: なし。

最上位の組織で、ネーミング属性の一意性が壊れる (6204537)

Access Manager をインストールしたあと、amadmin としてログインし、o、sunPreferredDomain、associatedDomain、sunOrganizationAlias、uid、および mail 属性を「一意の属性リスト」に追加します。2 つの組織を同じ名前で作成した場合、操作は失敗しますが、予期した「属性の一意性に違反しています」のメッセージではなく「その組織はすでに存在します」のメッセージが表示されます。

回避策: なし。正しくないメッセージを無視してください。Access Manager は正常に動作しています。

セッションおよび SSO に関する問題

- 34 ページの「ロードバランサに SSL 終了を設定した場合に、システムが無効なサービスホスト名を作成する (6245660)」
- 35 ページの「サードパーティー Web コンテナでの HttpSession の使用」

ロードバランサに SSL 終了を設定した場合に、システムが無効なサービスホスト名を作成する (6245660)

ロードバランサに SSL 終了を設定した Web コンテナとしての Web Server に Access Manager が配備されている場合、クライアントは正しい Web Server ページにダイレクトされません。Access Manager コンソールで「セッション」タブをクリックしても、ホストが無効なためエラーが返されます。

回避策: 次の例では、Web Server はポート 3030 で待機します。ロードバランサはポート 80 で待機し、要求を Web Server にリダイレクトします。

web-server-instance-name/config/server.xml ファイルで、使用している Web Server のリリースに従って servername 属性をロードバランサを示すように変更します。

Web Server 6.1 Service Pack (SP) リリースでは、servername 属性を次のように編集します。

```
<LS id="ls1" port="3030" servername="loadbalancer.example.com:80"
defaultvs="https-sample" security="false" ip="any" blocking="false"
acceptorthreads="1"/>
```

Web Server 6.1 SP2 (または以降) では、プロトコルを `http` から `https` または `https` から `http` へと切り替えることができます。つまり、`servername` を次のように編集します。

```
<LS id="ls1" port="3030"
servername="https://loadbalancer.example.com:443" defaultvs="https-sample"
security="false" ip="any" blocking="false" acceptorthreads="1"/>
```

サードパーティー Web コンテナでの HttpSession の使用

認証用にセッションを維持するデフォルトの方法は、`HttpSession` ではなく、「内部セッション」です。無効なセッションの最大時間値は、デフォルトの 3 分で十分です。`amtune` スクリプトは、Web Server または Application Server の場合に、この値を 1 分に設定します。ただし、サードパーティー Web コンテナ (IBM WebSphere または BEA WebLogic Server) とオプションの `HttpSession` を使用する場合は、Web コンテナの最大 `HttpSession` 時間を制限して、パフォーマンスの問題を避ける必要がある可能性があります。

ポリシーに関する問題

- 35 ページの「ポリシー設定サービスで動的属性を削除すると、ポリシーの編集で問題が発生する (6299074)」

ポリシー設定サービスで動的属性を削除すると、ポリシーの編集で問題が発生する (6299074)

ポリシー設定サービスで動的属性を削除すると、次のシナリオのポリシーの編集で問題が発生します。

1. ポリシー設定サービスで 2 つの動的属性を作成します。
2. ポリシーを作成し、(手順 1 からの) 動的属性を応答プロバイダで選択します。
3. ポリシー設定サービスで動的属性を削除し、属性をさらに 2 つ作成します。
4. 手順 2 で作成したポリシーを編集します。

結果は次のとおりです。「エラー 無効な動的プロパティーが設定されています」デフォルトでは、表示されるポリシーはありません。検索が終了したあと、ポリシーが表示されますが、既存のポリシーを編集または削除したり、新しいポリシーを作成したりすることはできません。

回避策: ポリシー設定サービスから動的属性を削除する前に、ポリシーからこれらの属性への参照を削除します。

サーバーの起動に関する問題

Access Manager の起動時に、デバッグエラーが発生する (6309274, 6308646)

Access Manager 7.1 の起動時に、`amDelegation` および `amProfile` デバッグファイルにデバッグエラーが返されます。

- `amDelegation`: 委譲のためのプラグインのインスタンスを取得できません
- `amProfile`: 委譲の例外を取得します

回避策: なし。このメッセージは無視できます。

AMSDK に関する問題

AMIdentity.modifyService を実行するとエラーが表示される (6506448)

`AMIdentity.modifyService` を使用してレルム上にデスクトップサービス動的属性を設定すると、null ポインタ例外が返されます。

回避策: 次のプロパティーを `AMConfig.properties` に追加して、サーバーを再起動します。:

```
com.sun.am.ldap.connnection.idle.seconds=7200
```

選択したリストにグループメンバーが表示されない (6459598)

この問題は次の条件で発生します。

1. 次のレルム設定でレルムを定義します。
   - 最上位レベルレルムは amroot です。サブレルムは example.com です。
   - サブレルム example.com には 2 つのデータストア、exampleDB と exampledminDB があります。
   - データストア exampleDB には、dc=example,dc=com で始まるすべてのユーザーが格納されています。サポートされる LDAPv3 操作は user=read,write,create,delete,service に設定されています。
   - データストア exampleadminDB にはレルムの管理者グループが格納されています。管理者グループは DN: cn=example.com Realm Administrators,ou=Groups,dc=example,dc=com です。このグループに含まれるのは、単一のメンバー scarter です。サポートされる LDAPv3 操作は group=read,write,create,delete に設定されています。
2. 「対象」タブをクリックしてから、「グループ」、ついで example.com Realm Administrators のエントリをクリックします。
3. 「ユーザー」タブをクリックします。

exampleDB データストアのすべてのユーザーが使用可能として表示されますが、scarter は「選択」フィールドに表示されません。

回避策: 操作 user=read を exampleadminDB データストアでサポートされる LDAPv3 操作に追加します。

Access Manager ログイン URL がメッセージ「そのような組織は見つかりません」を返す (6430874)

この問題は、完全修飾ドメイン名 (FQDN) に大文字と小文字の両方が混在して使用されていることが原因である可能性があります。

次に例を示します。HostName.PRC.Example.COM

回避策 :インストール後は、デフォルトの Access Manager ログイン URL を使用しないでください。その代わりに、ログイン URL にデフォルト組織の LDAP の場所を含めます。たとえば、次のように指定します。

```
http://HostName.PRC.Example.COM/amserver/UI/Login?org=dc=PRC,dc=Example,dc=COM
```

Access Manager へのログインに成功したら、Access Manager にログインするたびにユーザーの組織へのフルパスを入力しなくてすむようにできます。次の手順に従います。

1. レルムモードで「レルム」タブに移動するか、旧バージョンモードで「組織」タブに移動します。
2. デフォルトレルムまたは組織名をクリックします。

   この例では、prc をクリックします。
3. 「レルムまたは DNS のエイリアス」値のすべての大文字を小文字に変更します。

   この例では、すべてが小文字の値 hostname.prc.example.com をリストに追加してから、大文字と小文字が混在した HostName.PRC.Example.COM 値をリストから削除します。
4. 「保存」をクリックして、Access Manager コンソールをログアウトします。

これで、次の URL のどれを使用してもログインできます。

- http://hostname.PRC.Example.COM/amserver/UI/Login
- http://hostname.PRC.Example.COM/amserver
- http://hostname.PRC.Example.COM/amserver/console

amadmin を使用して Access Manager からサブ組織を作成することができない (5001850)

2 つの Directory Server の間でマルチマスターレプリケーションが有効になっているときに、amadmin ユーティリティーを使用してサブ組織を作成しようとすると、この問題が発生します。

回避策: 両方の Directory Server で、nsslapd-lookthroughlimit プロパティーを -1 に設定します。

SSL に関する問題

- 38 ページの「SSL 証明書が期限切れになっていると、amconfig スクリプトが失敗する (6488777)」

SSL 証明書が期限切れになっていると、amconfig スクリプトが失敗する (6488777)

Access Manager コンテナを SSL モードで実行しており、コンテナの SSL 証明書の期限が切れている場合、amconfig が失敗し、クラスパスの値が破壊されることがあります。

回避策: amconfig を期限切れの証明書ですでに実行していて、クラスパスの値が破壊されている場合は、まず有効な SSL 証明書を取得してください。ファイル内のクラスパスの値が破壊されていない元の domain.xml ファイルまたはそのコピーに戻します。それから、次のように amconfig コマンドを実行します。

```
/opt/SUNWam/bin/amconfig -s $PWD/amsamplesilent
```

サンプルに関する問題

Clientsdk サンプルディレクトリに不要な makefile が含まれている (6490071)

クライアント SDK にはサンプルファイルが含まれています。これらは、スタンドアロンプログラムや Web アプリケーションの記述方法を示します。サンプルは `Makefile.clientsdk` を生成したディレクトリの下にあり、次のサブディレクトリに分かれています。

```
.../clientsdk-samples/

.../clientsdk-webapps/
```

Clientsdk-samples には、認証、ロギング、ポリシー、および SAML スタンドアロンのプログラムサンプルが収められています。Clientsdk-webapps には、ユーザー管理、サービス管理、およびポリシーのプログラムサンプルが収められています。各サンプルには Readme.html ファイルがあり、サンプルプログラムをコンパイルして実行する手順が示されています。

サンプルをコンパイルするには、対応するサブディレクトリ内で makefile を実行する必要があります。最上位の makefile では、サブディレクトリ内のサンプルはコンパイルされません。

Linux OS に関する問題

Application Server で Access Manager を実行すると、JVM の問題が発生する (6223676)

Red Hat Linux で Application Server 8.1 を実行している場合、Application Server 用に Red Hat OS が作成するスレッドのスタックサイズは 10M バイトですが、Access Manager ユーザーセッション数が 200 に達すると、JVM リソースの問題が発生する可能性があります。

回避策: Application Server を起動する前に、ulimit コマンドを実行して、Red Hat OS が操作するスタックサイズを 2048K バイトまたは 256K バイトなどの小さな値に設定します。ulimit コマンドは、Application Server の起動に使用する同じコンソールで実行します。たとえば、次のように指定します。

```
# ulimit -s 256;
```

Windows および HP-UX に関する問題

- 40 ページの「zh_TW および es ロケールでのインストール時に、Access Manager の自動設定が失敗する (6515043)」
- 40 ページの「HP-UX 上で JES フルスタックのインストールを行う場合、Access Manager のインストール用に gettext バイナリが必要となる (6497926)」

zh_TW および es ロケールでのインストール時に、Access Manager の自動設定が失敗する (6515043)

回避策: HP-UX プラットフォームの zh_TW と es ロケールでは、Access Manager を「後で設定」モードでのみ設定する必要があります。JavaES インストーラを起動して Access Manager 製品をインストールし、JavaES インストーラを終了します。それから、次に示す方法で Access Manager 設定ツールを実行します。

1. LANG=C
2. export LANG
3. *accessmanager-base*/bin/amsamplesilent ファイルを編集します。
4. *accessmanager-base*/bin/amconfig -s amsamplesilent を実行します。

HP-UX 上で JES フルスタックのインストールを行う場合、Access Manager のインストール用に gettext バイナリが必要となる (6497926)

現時点では、この問題の回避策はありません。

連携および SAML に関する問題

- 40 ページの「連携でログアウトエラーが発生する (6291744)」

連携でログアウトエラーが発生する (6291744)

レルムモードで、アイデンティティープロバイダ (IDP) およびサービスプロバイダ (SP) でユーザーアカウントを連携し、連携を終了してログアウトすると、次のエラーが発生します。「エラー: サブ組織が見つかりません。」

回避策: なし。

国際化に関する問題

zh ロケールでの管理コンソールコンポーネントが英語で表示される (6470543)

ブラウザのロケールを zh に設定すると、「Version」、「Help」、「Logout」ボタンなど、管理コンソールコンポーネントが英語で表示されます。

回避策: ブラウザのロケールを、zh ではなく zh-cn に設定します。

コンソールの「現在の値」と「新しい値」が正しく表示されない (6476672)

ローカライズ版の管理コンソールでは、「現在の値」属性と「新しい値」属性のラベルがそれぞれ「label.current.value」および「label.new.value」と誤って表示されます。

ポリシー条件の日付は英語の形式で指定する必要がある (6390856)

中国語ロケールで、ポリシー条件の日付形式ラベルは、中国語の形式では表示されません。ラベルには英語の日付形式が想定されています。関連するフィールドも、英語の日付形式値を受け入れます。

回避策: フィールドごとに、フィールドラベルに示されている日付形式の例に従ってください。

クライアントディテクションで UTF-8 の削除が動作しない (5028779)

「クライアントディテクション」機能は正常に動作しません。Access Manager 7.1 コンソールに加えられた変更は、自動的にブラウザに送られません。

回避策: 2 つの回避策があります。

- 「クライアントディテクション」セクションに変更を加えたあとで、Access Manager Web コンテナを再起動します。

  または

- Access Manager コンソールで、次の手順を実行します。
  1. 「設定」タブの下にある「クライアントディテクション」をクリックします。
  2. 「genericHTML」の「編集」リンクをクリックします。
  3. 「HTML」タブの下の、「genericHTML」リンクをクリックします。
  4. 文字セットのリストで、次のエントリを入力します。UTF-8;q=0.5 (UTF-8 q 係数がロケールのその他の文字セットよりも小さくなるようにする)
  5. 保存してログアウトし、もう一度ログインします。

マルチバイト文字がログファイルで疑問符として表示される (5014120)

/var/opt/SUNWam/logs ディレクトリ内のログファイルにあるマルチバイトのメッセージが疑問符 (?) として表示されます。ログファイルはネイティブなエンコーディングで、常に UTF-8 ではありません。Web コンテナインスタンスを特定のロケールで起動すると、ログファイルはそのロケールのネイティブなエンコーディングになります。別のロケールに切り替えて Web コンテナインスタンスを再起動すると、それ以降のメッセージは現在のロケールのネイティブなエンコーディングになりますが、それ以前のエンコーディングのメッセージは疑問符として表示されます。

回避策: 常に同じネイティブなエンコーディングを使用して Web コンテナインスタンスを起動するようにします。

マニュアルに関する問題

- 43 ページの「LDAPv3 プラグインのロールおよびフィルタを適用したロールのサポートについて (6365196)」
- 43 ページの「AMConfig.properties ファイルの未使用のプロパティーについて (6344530)」
- 43 ページの「XML 暗号化を有効にする方法について (6275563)」

LDAPv3 プラグインのロールおよびフィルタを適用したロールのサポートについて (6365196)

各パッチを適用後、データを Sun Java System Directory Server に保存する場合に、LDAPv3 プラグインにロールおよびフィルタを適用したロールを設定できます (問題 ID 6349959 を修正)。Access Manager 7.1 管理コンソールで、「LDAPv3 プラグインでサポートされるタイプと操作」フィールドの LDAPv3 の設定に、次のような値を入力します。

```
role: read,edit,create,delete
filteredrole: read,edit,create,delete
```

LDAPv3 の設定で使用するロールやフィルタを適用したロールに応じて、上のエントリのいずれかまたは両方を入力できます。

AMConfig.properties ファイルの未使用のプロパティーについて (6344530)

`AMConfig.properties` ファイルの次のプロパティーは使用されていません。

```
com.iplanet.am.directory.host
com.iplanet.am.directory.port
```

XML 暗号化を有効にする方法について (6275563)

Bouncy Castle JAR ファイルを使用して、Access Manager または Federation Manager で XML 暗号化を有効にしてトランスポートキーを生成するには、次の手順に従います。

1. JDK 1.5 より前の JDK バージョンを使用している場合は、Bouncy Castle サイト (`http://www.bouncycastle.org/`) から Bouncy Castle JCE プロバイダをダウンロードします。たとえば、JDK 1.4 の場合、`bcprov-jdk14-131.jar` ファイルをダウンロードします。
2. 前の手順で JAR ファイルをダウンロードした場合は、ファイルを *jdk_root*`/jre/lib/ext` ディレクトリにコピーします。
3. JDK の国内版の場合、Sun サイト (`http://java.sun.com`) から、お使いの JDK のバージョンに対応する JCE Unlimited Strength Jurisdiction Policy Files をダウンロードします。IBM WebSphere の場合は、対応する IBM サイトに移動し、必要なファイルをダウンロードします。
4. ダウンロードした `US_export_policy.jar` および `local_policy.jar` ファイルを *jdk_root*`/jre/lib/security` ディレクトリにコピーします。
5. JDK 1.5 より前の JDK のバージョンを使用している場合は、*jdk_root*`/jre/lib/security/java.security` ファイルを編集し、プロバイダの 1 つとして Bouncy Castle を追加します。たとえば、次のように指定します。

```
security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider
```

6. AMConfig.properties ファイルで、次のプロパティーを true に設定します。

```
com.sun.identity.jss.donotInstallAtHighestPriority=true
```

7. Access Manager Web コンテナを再起動します。

詳細については、問題 ID 5110285 (XML 暗号化には Bouncy Castle JAR ファイルが必要) を参照してください。

マニュアルの更新

これらのマニュアルにアクセスするには、Access Manager 7.1 コレクションを参照してください。

http://docs.sun.com/coll/1292.1

『Technical Note: Deploying Access Manager to an Application Server Cluster』の第 1 章「Technical Note: Deploying Access Manager Instances to an Application Server Cluster」というタイトルの新規マニュアルが、Access Manager 7 2005Q4 コレクションに追加されました。

Sun Java System Access Manager Policy Agent 2.2 コレクションも、新規エージェントを説明する内容に改訂されました。

http://docs.sun.com/coll/1322.1

再配布可能ファイル

Sun Java System Access Manager 7.1 には、製品のライセンスを取得していないユーザーに再配布できるファイルは含まれていません。

問題の報告およびフィードバックの提供方法

Access Manager または Sun Java Enterprise System で問題が生じた場合、次のいずれかの方法で Sun の担当者にご連絡ください。

- http://sunsolve.sun.com/ にある Sun サポートリソース (SunSolve)。

  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。http://docs.sun.com/ に移動し、「コメントの送信」をクリックします。

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、Access Manager リリースノート の Part No. は 820-0363 です。

Sun が提供しているその他の情報

次の場所から Access Manager に関する情報とリソースを入手できます。

- Sun Java Enterprise System のマニュアル: http://docs.sun.com/prod/entsys.05q4
- Sun サービス: http://www.sun.com/service/consulting/
- ソフトウェア製品およびサービス: http://wwws.sun.com/software/
- サポートリソース: http://sunsolve.sun.com/
- 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/

障害を持つ方々向けのアクセシビリティー機能

このメディアの発行以来リリースされているアクセシビリティー機能を入手する場合は、申し込みにより Sun から入手可能な 508 条に関する製品評価資料を参照し、アクセシビリティーのソリューションの配備に最適なバージョンを決定してください。アプリケーションの最新バージョンは
http://sun.com/software/javaenterprisesystem/get.html から入手できます。

アクセシビリティーに関する Sun の方針については、http://sun.com/access を参照してください。

関連するサードパーティーの Web サイト

このリリースノートに紹介されているサードパーティーの URL では、追加情報や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ーの 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、ほかの資料に関し、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。
