Sun Java System Access Manager 7.1 リリースノート (Windows 版)

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

Part No: 820–1795
2007 年 2 月

070614@17466

目次

◆ ◆ ◆ 第 1 章

Sun Java System Access Manager 7.1 リリースノート (Microsoft Windows 版)

『Sun Java™ System Access Manager 7.1 リリースノート』には、Access Manager の新機能、既知の問題点、適用できるものがある場合は回避策など、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。

Access Manager 7.1 リリースノートは、次の節で構成されています。

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 ベースの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
- 後続の分析、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 Access Manager コンポーネントによるログ作成。

このリリースの新機能

このリリースには、次の新機能が含まれています。

- 6 ページの「Java ES Monitoring Framework の統合」
- 7 ページの「Web サービスのセキュリティー」
- 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」

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、サービス駆動型ネットワークを管理および監視するための、分散型で Web ベースのモジュール化された動的ソリューションを構築するツールを提供します。JMX テクノロジは通常、アプリケーション設定の確認と変更、アプリケーションの動作に関する統計情報の蓄積、および状態変化とエラー動作に関する通知に利用されます。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
- アクティブなセッションの数、およびセッションフェイルオーバーデータベースからの統計情報
- セッションフェイルオーバーデータベースの統計情報
- 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
- SAML/連携配備での特定のプロバイダに対する表明の数

Web サービスのセキュリティー

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 には単一の WAR ファイルが含まれています。このファイルを使用することで、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も Access Manager サービスを持続的に配備できます。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。

- 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 (オプション)
  - 実行状態と待機状態の両方に関する各モジュールのトランザクション時間 (可能な場合)
  - バックエンドサーバーの接続失敗数
- 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を示す)

    - 増分カウンタを使用するアクティブなセッションの数
    - セッションのフェイルオーバー (増分カウンタを使用してカウントされるセッションストアに入れられているセッションの数、およびフェイルオーバーデータベース上で実行された読み取り、書き込み、削除などの操作の数)
- ユーザー管理 / アイデンティティーリポジトリ / セッション管理サービス
    - 最大キャッシュサイズ
    - ヒット数、使用率、最大使用率、現在のサイズなどキャッシュ関連の統計情報
    - 実行操作と待機操作の両方に関するトランザクション時間
- ポリシー
    - キャッシュ内のポリシーの数
    - キャッシュ内の `policyManager` の数
    - `policyListeners` キャッシュ内のサービス名の数
    - `resultsCache` 内のサービスの数
    - `sessionListernerRgistry` 内の `tokenID` の数
    - `policyListenerRegistry` 内のサービス名の数
    - `role` キャッシュ内の `tokenID` の数
    - `resourceNames` キャッシュ内のサービス名の数
    - `SubjectEvaluationCache` のエントリの数
    - キャッシュ内の `PolicyEvaluator` の数
    - キャッシュ内のポリシー変更リスナーの数
    - ポリシー評価処理のトランザクション時間
- 連携
    - 指定されたプロバイダのテーブル内のアーティファクト数
    - 指定されたプロバイダのテーブル内の表明数
    - 指定されたプロバイダ ID の、指定されたテーブル内にあるセッションのエントリ数
- SAML
    - アーティファクトマップのサイズ
    - 表明マップのサイズ

認証モジュール

- 負荷が分散された配備で 1 つのサーバーだけを使用する場合、分散認証サービスは必要ない。
- 負荷が分散された配備で 1 つのサーバーだけを使用する場合、認証サービスおよびサーバーは必要ない。
- 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。このサポートには、`AuthenticateToRealm` 条件、AuthenticateToService 条件、およびすべての条件に対するレルム認証が含まれます。
- レルムで資格を与えられた認証条件を使用するアドバイス組織。

- 認証設定/ 認証連鎖 (AuthServiceCondition)。
- 認証連鎖を実施する場合は、モジュールベースの認証を無効にできる。
- 分散認証サービスは証明書認証モジュールをサポートする。
- 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った。
- 新しいデータストア認証モジュールは、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。
- 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った。
- 事後処理 SPI クラスの連鎖。

ポリシーモジュール

- サービスベースの認証に基づいたポリシー定義のサポート。
- 追加された新しいポリシー条件: AuthenticateToRealmCondition
- サブディレクトリを保護せずにディレクトリの内容を容易に保護できるようにする 1 レベルでのワイルドカード比較のサポート。
- LDAP フィルタ条件のサポート。ポリシーの定義時に、ポリシー管理で条件内の LDAP フィルタを指定できます。
- 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る。
- AuthLevelCondition では、認証レベルに加えてレルム名を指定できる。
- AuthSchemeCondition では、認証モジュール名に加えてレルム名を指定できる。

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。このプロバイダは、クライアントおよびサーバー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

- Web に配備できるように、Access Manager を J2EE アプリケーションとして 1 つの WAR ファイルに再パッケージ化

委任モジュール

- 委任特権のグループ化のサポート

ロギング

- ロギングモジュールでの委任のサポート - 委任は、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する。
- JCE ベースの SecureLogHelper のサポート- この追加により、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る。

ハードウェアと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 1–1 ハードウェアと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)	■ Windows 2000 Advanced Server SP4 ■ Windows XP SP2 ■ Windows 2003 Enterprise Server SP1 (32 ビット) ■ Windows 2003 Enterprise Server SP1 (64 ビット)
Java 2 Standard Edition (J2SE™ プラットフォーム)	J2SE プラットフォーム 6.0、5.0 Update 7、および 1.4.2 Update 11
ディレクトリサーバー	Access Manager 情報ツリー: Sun Java System Directory Server 5.2 Access Manager アイデンティティーリポジトリ: Sun Java System Directory Server 6.0 または Microsoft Active Directory
Web コンテナ	Sun Java System Web Server7.0 Sun Java System Application Server Enterprise Edition 8.2

表 1–1 ハードウェアとソフトウェアの要件 *(続き)*

コンポーネント	要件
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 release でサポートされているブラウザを示します。

表 1–2 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
Microsoft Internet Explorer™ 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows 2000
Mozilla 1.7.12	Windows XP
	Windows 2000
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000

互換性に関する一般情報

- 12 ページの「Access Manager 旧バージョンモード」
- 12 ページの「Access Manager ポリシーエージェント」

Access Manager 旧バージョンモード

Access Manager を Sun Java System Portal Server 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。Access Manager 7.1 のインストールに関する決定については、12 ページの「Access Manager モードの確認」を参照してください。

「インストール中に自動的に設定」オプション

グラフィカルモードで「インストール中に自動的に設定」オプションを指定して Java ES Installer を実行している場合、Access Manager は「旧バージョン (バージョン 6.x スタイル)」モードで設定されます。

「インストール後に手動で設定」オプション

「インストール後に手動で設定」オプションを指定して Java ES Installer を実行した場合は、インストール後に `install-dir\identity\setup\amconfig.bat` ファイルを実行して、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、設定ファイル内に次のパラメータを設定します。

```
AM_REALM = disabled

...
install-dir\identity\setup\AMConfigurator.properties
...
```

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
```

戻り値が `true` の場合はレルムモードであることを示します。戻り値が `false` の場合は旧バージョンモードであることを示します。

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 1–3　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 エージェント、バージョン 2.1	旧バージョンモードおよびレルムモード
J2EE エージェント、バージョン 2.1	旧バージョンモードのみ

その他の既知の問題点と制限事項

この節では、7.0 release 時点での既知の問題点について、適用できるものがある場合には回避方法とともに説明します。

インストールに関する情報

Access Manager を既存の DIT にインストールすると、Directory Server のインデックスの再作成が必要になる (6268096)

検索のパフォーマンスを改善するために、Directory Server にはいくつかの新しいインデックスが用意されています。

回避方法:Access Manager を既存のディレクトリ情報ツリー (DIT) とともにインストールした後、Directory Server のインデックスを `db2index.pl` スクリプトを実行して再作成します。次に例を示します。

```
# ./db2index.pl -D "cn=Directory Manager" -w password -n userRoot
```

db2index.pl スクリプトは *DS-install-directory*/*slapd-hostname*/ ディレクトリから利用可能です。

Access Manager と Directory Server を別のマシンにインストールすると、認証サービスが初期化されない (6229897)

インストール時に classpath およびその他の Access Manager Web コンテナ環境変数は更新されますが、インストールプロセスでは Web コンテナが再起動されません。インストール後、Web コンテナが再起動する前に、Access Manager にログインしようとすると、次のエラーが返されます。

```
Authentication Service is not initialized. Contact your system administrator.
```

回避方法:Access Manager にログインする前に、Web コンテナを再起動します。ログインする前に、Directory Server も実行している必要があります。

アップグレードの問題

- 14 ページの「Java ES 4 Access Manager を Java ES 5 Access Manager にアップグレードしたあと Portal Server と Web コンソールが動作しない (6515054)」

Java ES 4 Access Manager を Java ES 5 Access Manager にアップグレードしたあと Portal Server と Web コンソールが動作しない (6515054)

Java ES 5 Access Manager を Java ES 5 Access Manager にアップグレードしたあと、配備されていたアプリケーション、Portal Server と Web コンソールが動作しません。

回避方法:config.properties ファイルを Java ES 5 のインストール場所から Java ES 4 のインストール場所にコピーします。

```
copy install-Dir\share\MobileAccess\config\config.properties
JavaES4–install-dir\PortalServer\https-host-name\portal\web-apps\WEB-INF\classes\
```

設定に関する問題

- 15 ページの「一部の Access Manager モジュールを設定するには Active Perl 5.8 以降が必要」
- 15 ページの「インストーラが分散認証およびクライアント SDK コンポーネントを設定できない」
- 15 ページの「am2bak.bat および bak2am.bat ファイルが正しく生成されない (6491091)」
- 15 ページの「連続してログインに失敗してもユーザーアカウントが 非アクティブにならない (6469200)」

一部の Access Manager モジュールを設定するには Active Perl 5.8 以降が必要

次のコンポーネントを Access Manager とともに設定するには、Active Perl 5.8 以降をインストールする必要があります。

- MFWK
- セッションフェイルオーバー
- 一括連携
- パフォーマンスチューニング

Active Perl は `http://www.activestate.com/Products/ActivePerl/` からダウンロード可能です。

インストーラが分散認証およびクライアント SDK コンポーネントを設定できない

「インストール中に自動的に設定」では、分散認証およびクライアント SDK コンポーネントが設定されません。エラーメッセージは表示されません。

回避方法:「インストール後に手動で設定」オプションをインストール時に使用して、インストール後に分散認証とクライアント SDK コンポーネントを手動で設定します。

`am2bak.bat` および `bak2am.bat` ファイルが正しく生成されない (6491091)

Access manager 7.1 は、バックアップユーティリティー (`am2bak.bat`) および復元ユーティリティー (`bak2am.bat`) をサポートしません。

回避方法:ありません。

連続してログインに失敗してもユーザーアカウントが非アクティブにならない (6469200)

Access Manager へのログインに連続して失敗してもユーザーアカウントが非アクティブになりません。

回避方法:レルム管理コンソール (`\amserver\console`) を使用して、ロックアウトユーティリティーを有効または無効にします。「ログイン失敗時のロックアウトモード」属性を設定するには、次の手順に従います。

1. Access Manager の GUI を開きます。
2. ロックアウトを有効にするレルムを選択します。
3. 「認証」タブを選択します。
4. 「拡張プロパティー」ボタンをクリックします。

5. 「ログイン失敗時のロックアウトモード」属性を選択します。
6. 「保存」ボタンをクリックして、プロパティーを保存します。

Access Manager コンソールに関する問題

新しい Access Manager コンソールでは CoS テンプレートの優先順位を設定できない (6309262)

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

回避方法:Access Manager 6 2005Q1 コンソールにログインし、CoS テンプレートの優先順位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 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。

回避方法:ありません。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)

次の状況では、コンソールは正確な情報を表示しません。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、`uid=*999*` というフィルタを使ってユーザーを追加します。その結果として表示されるリストボックスは空で、コンソールにはエラー、情報、または警告のメッセージがまったく表示されません。

回避方法: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。

SDK およびクライアントに関する問題

削除済みのユーザーと同じユーザーをポータルから作成できない (6479611)

削除済みのユーザーと同じユーザープロファイルをポータルから作成できません。次のエラーメッセージが表示されます。

ユーザープロファイルの格納時にエラーが発生しました。

回避方法:ありません。

サーバーを再起動した後、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。

回避方法:ありません。

サービススキーマの変更の後、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。

回避方法:サービススキーマを変更した後、クライアントを再起動します。

セッションおよび SSO に関する問題

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。デフォルトでは、認証用にセッションを維持する時間は、3 分に設定されており、その時間が過ぎると、セッションは無効となります。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、IBM WebSphere または BEA WebLogic Server などのサードパーティー Web コンテナと、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

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)

次のような場合に、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 で新しく作成した動的属性を選択します。
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。

次のエラーメッセージが表示されます。「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。検索が終了した後、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。

回避方法: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次のデバッグエラーが返されます。

- amDelegation: Unable to get an instance of plugin for delegation

- `amProfile`: GotDelegation Exception

回避方法:ありません。これらのメッセージは無視してかまいません。

連携および SAML に関する問題

- 19 ページの「アーティファクトプロファイルを使用したときに連携が失敗する (6324056)」
- 19 ページの「連携でログアウトエラーが発生する (6291744)」

アーティファクトプロファイルを使用したときに連携が失敗する (6324056)

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) を設定し、ブラウザのアーティファクトプロファイルを使用するように通信プロトコルを変更してから、IDP と SP の間でユーザーを連携しようとすると、連携が失敗します。

回避方法:ありません。

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、次のエラーメッセージが表示されます。「エラー: サブ組織が見つかりません。」

回避方法:ありません。

国際化に関する問題

- 19 ページの「レルムコンソールで、オンラインヘルプの左側のパネルにアプリケーションエラーが表示される (6508103)」
- 20 ページの「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)」
- 20 ページの「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)」

レルムコンソールで、オンラインヘルプの左側のパネルにアプリケーションエラーが表示される (6508103)

Access Manager を Application Server に配備すると、レルムコンソールでオンラインヘルプの左側のパネルにアプリケーションエラーが表示されます。

回避方法:次の手順に従います。

1. `jhall.jar` ファイルをコピーします。

   `copy` *install-dir*`\share\lib\jhall.jar %JAVA_HOME%\jre\lib\ext`

2. Application Server を再起動します。

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。

回避方法:次の回避方法を試してください。

1. 「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後で、Access Manager Web コンテナを再起動します。
2. Access Manager コンソールで次の手順を実行します。
   a. 「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。
   b. 「クライアントタイプ」の「編集」リンクをクリックします。
   c. 「HTML」タブの下の、「`genericHTML`」リンクをクリックします。
   d. 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 の `q` 係数がその他の日本語文字セットよりも小さくなるようにする)
   e. 「保存 (Save)」をクリックします。
   f. ログアウトし、ログインし直します。

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)

`install_dir\identity\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、必ずしも UTF-8 であるとは限りません。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。

回避方法:Web コンテナインスタンスの起動時には、常に同じネイティブなエンコーディングを使用します。

マニュアルに関する問題

- 21 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)」

- 21 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)」
- 21 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。次の手順に従います。

1. Access Manager 7.1 管理者コンソールを開きます。
2. LDAPv3 設定を選択します。
3. LDAPv3 設定で使用するロールおよびフィルタを適用したロールに基づいて、「LDAPv3 プラグインでサポートされるタイプと操作」フィールドに次の値を入力します。

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

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)

XML 暗号化を有効にするには、次の手順を実行します。

1. (省略可能) JDK バージョン 1.5 よりも前の JDK バージョンを使用している場合は、次の手順に従います。
   a. Bouncy Castle のサイト (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 バージョン 1.4 の場合、bcprov-jdk14-131.jar ファイルをダウンロードします。

   b. ファイルを *jdk_root*\jre\lib\ext ディレクトリにコピーします。
2. JCE Unlimited Strength Jurisdiction Policy Files をダウンロードします。使用する JDK のバージョンに対応したものをダウンロードします。
   - Sun Systems の場合は、Sun のサイト (http://java.sun.com) から JDK のバージョンに対応したファイル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。

3. 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。
4. 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。次に例を示します。

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

5. `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
   ```

6. 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は、Access Manager 7.1 コレクション `http://docs.sun.com/coll/1292.1` で参照できます。

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` で参照できます。

再配布可能なファイル

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。

問題の報告とフィードバックの方法

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。
- 保守契約先に電話連絡してください。

問題の解決にあたって最善のサポートを提供させていただくために、サポートにご連絡いただく際には次の情報をお手元にご用意ください。

- 問題が発生する状況と、実行処理への影響を含む問題の説明。
- マシン機種、OS バージョン、および製品のバージョン (問題に関係するパッチおよびその他のソフトウェアを含む)
- 問題を再現するための具体的な手順の説明
- エラーログまたはコアダンプ

このマニュアルに関するコメント

Sun では、マニュアルの改善のために、皆様からのコメントおよび提案をお待ちしております。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 820-1795 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/

障害を持つユーザー向けのアクセシビリティー機能

このメディアの出版以降にリリースされたアクセシビリティー機能を入手するには、米国リハビリテーション法 508 条に関する製品評価資料を Sun に請求し、その内容を確認して、どのバージョンが、アクセシビリティーに対応したソリューションを配備するためにもっとも適しているかを特定してください。最新バージョンのアプリケーションは、http://sun.com/software/javaenterprisesystem/get.html にあります。

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

このマニュアル内で参照している第三者の URL は、追加の関連情報を提供します。

注 – このマニュアル内で引用する第三者の Web サイトの可用性について Sun は責任を負いません。こうしたサイトやリソース上の、またはこれらを通じて利用可能な、コンテンツ、広告、製品、その他の素材について、Sun は推奨しているわけではなく、Sun はいかなる責任も負いません。こうしたサイトやリソース上の、またはこれらを経由して利用可能な、コンテンツ、製品、サービスを利用または信頼したことに伴って発生した (あるいは発生したと主張される) いかなる損害や損失についても、Sun は一切の責任を負いません。
