CHAPTER 4

認証、認可、アカウンティング（AAA）のサポート

４３０，２００７ OL-12437-01-J

この章では、Cisco BTS 10200 ソフトスイッチの Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）拡張機能について説明します。これらの拡張機能には、システム上での現在のユーザ アカウント管理方式に対する変更が反映されています。次の 2 つのプロトコルのサポートが含まれています。これらのプロトコルは、互いに包含的である必要はありません。

- RADIUS プロトコル
- Lightweight Directory Access Protocol（LDAP）

4.4 より前のリリースの Cisco BTS 10200 ソフトスイッチのユーザ アカウント管理では、Authentication Dial-In User Service の Network Information Service（NIS; ネットワーク情報サービス）を使用せずに、標準の Solaris パスワード管理機能を使用していました。すべてのアカウントがローカルに格納され、ローカルに参照されていました。このセキュリティ機能から、ユーザ アカウント管理の完全な AAA モデルがサポートされ始めました。このモデルは、Cisco BTS 10200 ソフトスイッチ Element Management System（EMS）アプリケーションのいくつかの内部サブシステムに影響します。また、Cisco BTS 10200 ソフトスイッチのその他のノードのコア ログイン サポートにも影響を及ぼします。

プラグイン可能な認証モジュール（PAM）のサポート

Cisco BTS 10200 ソフトスイッチは、Pluggable Authentication Module（PAM; プラグイン可能な認証モジュール）のサポート機能とともに、Secure Shell（SSH）パッケージを配置します。パッケージには、RADIUS サーバおよび LDAP サーバを使用するために必要な PAM サポートが組み込まれています。

RADIUS サーバおよび LDAP サーバを使用できない場合は、サポートされている構成でも、ローカル アカウントが認証に失敗することがあります。Cisco BTS 10200 ソフトスイッチの場合、これに該当するデフォルトのローカル アカウントは、btsuser、btsadmin、secadmin の各アカウントです。これらは、基本製品で提供されている標準のデフォルト アカウントであり、製品固有のパスワード管理を使用します。

UNIX ベースのユーザは、すべてのノード上のオペレーティング システムにアクセスします。oamp ユーザは、パッケージ管理を目的として定義されています。アカウントは、ロックされ、パスワードは使用できません。ただし、Cisco BTS 10200 ソフトスイッチのすべてのノードへの UNIX アクセスを許可すると、デフォルト パスワードが提供されます。

PAM サポートが使用されている場合、SSH は認証の制御を PAM ライブラリに受け渡します。その後、PAM ライブラリは、PAM コンフィギュレーション ファイルに指定されているモジュールをロードします。最後に、PAM ライブラリは、認証が成功したかどうかを SSH に通知します。SSH は、PAM が使用した実際の認証方式の詳細を認識することはありません。関係があるのは、最終結果だけです。

ユーザ セキュリティ アカウント管理

Cisco BTS 10200 ソフトスイッチ EMS には、User Security Management（USM; ユーザ セキュリティ管理）として知られるアプリケーション プログラムが含まれています。このプログラムは、アカウントがローカルであるか、またはそれ以外であるかを判断します。AAA の展開が設定されている場合、Cisco BTS 10200 ソフトスイッチ上のすべてのアカウントについて、パスワード管理機能はディセーブルになっています。AAA を展開すると、これらの既存の機能を管理する責任は、エンドユーザ AAA サーバに受け渡されます。これらの機能には、次の属性が含まれます。

- パスワードのエージング、警告、および期限切れ
- パスワードのリセットおよび自動アカウント ロック
- 新規アカウントのローカル アカウント管理（パスワード ファイルおよびシャドウ ファイル）