パスワード暗号化の改善

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.27.4

機能説明

CUPS の構成ファイルには、非機密情報からきわめて機密性の高い情報まで、さまざまなレベルの機密情報に関する多くのコマンドが含まれています。管理者またはユーザーによる不正アクセスから機密情報を保護する必要があります。以下に示すように、機密データを保護するさまざまな方法があります。

- 対称暗号化
- 非対称暗号化
- 一方向ハッシュ

機能の仕組み

対称暗号化は、クライアント認証用のリモート TACACS+ パスワード、LI 設定、パスワード、SSH キー、SNMP コミュニティストリングなど、構成ファイルに存在する機密情報を保護するために使用されます。プレーンテキスト形式の機密情報が CUPS のリモートサーバーに転送される場合があります。1 つの例は、CUPS システムが TACACS+ クライアントとして機能し、

リモートTACACS+サーバーにアクセスするためにパスワード認証が必要な場合です。一方向ハッシュプロセス後に機密情報が保存されると、システムはハッシュ値を復号または反転してプレーンテキストを取得できません。CUPS は対称暗号化を使用して、パスワードをランダムなソルトでハッシュできるようにして、この問題に対処します。

次に示されているように、プレーンテキストパスワードは、**PBKDF2**ハッシュアルゴリズムを使用してシステムによってハッシュされます。

- システムが、/dev/urandom デバイスファイルから 16 バイトのランダムなソルトを生成します。
- **PBKDF2** 内の反復回数は、次のように計算されます。
  - 基本値として 10,000 ラウンド。
  - ランダムなソルトに基づく追加のラウンド。
  - 長さ 64 バイトの結果（ハッシュ値）。

ハッシュされたパスワードは、システム設定プロセス中に保存されます。ユーザーが入力したプレーンテキストパスワードは、認証フェーズと比較するために、同じソルトに基づいてハッシュ値に変換されます。

（注） パスワードハッシュ値は、既存のCLIでのさらなる変更を最小限に抑え、回避するように暗号化されます。

対称暗号化の発生

CUPS では、さまざまなタイプのデータに対する対称暗号化が数多く発生します。

小規模な一般機密データの暗号化（512 バイト未満）

CUPS は、長さが 512 バイト未満の小規模な一般機密データの暗号化を処理します。

フラッシュ上の永続性ファイルに対する P2P ライブラリライセンスの有効期限

P2P ライセンス機能では、有効期限によって P2P ライブラリを制御します。P2P ライセンスには、有効な P2P ライブラリのローディングを制御する有効期限があります。P2P ライセンスのライセンス有効期限は、後で参照できるようにファイルに保存されます。

長いデータの暗号化（512 バイトを超える長さ）

サイズの大きいバイナリテキストは、それぞれ512バイトの小さいチャンクに分割されます。これらの小さなチャンクはそれぞれ個別に暗号化され、文字列として連結されます。

CUPS をクライアントとする SSH キー（mgmt インターフェイス）

CUPS は、一部のトランザクションでは SSH クライアントとしても機能します。クライアント SSH キーが生成されると、設定時に暗号化されて保存されます。その後のシステムのリブートでは、この SSH キーを復号して使用します。

CUPS のサーバー SSH キー（コンテキストごと）

CUPS は、管理者から受信するログイン接続要求に対して、SSH サーバーとして機能します。SSH サーバーの SSH キーは一度生成され、設定時に暗号化されて保存されます。その後のシステムのリブートでは、この SSH キーを復号して使用します。

システムの RSA 秘密キー

CUPS は、設定モードで RSA 証明書と秘密キーの設定をサポートします。これらの秘密キーは、設定時に対称暗号化を使用して暗号化されます。

暗号化パスワードの設定

システムレベルおよび管理者パスワードの暗号化

システムレベルおよび管理者パスワードの暗号化について以下で説明します。

保存された設定の管理者パスワード

システム管理者アカウントのパスワードの値は、**show configuration o/p** コマンドでは「**」と表示されます。一方、パスワードは **save configuration o/p** コマンドを使用して暗号化されます。

テクニカル サポート パスワード

サポートおよびデバッグ用のテクニカルサポートパスワードは、CUPS で使用できます。テクニカル サポート パスワードを設定するには、次のコンフィギュレーション コマンドを使用します。

```
configure
   tech-support test-commands [encrypted] password
   end
```

QvPC-SI システムの接続アプリケーション セッション パスワード

セッションパスワードを設定するには、次のコンフィギュレーション コマンドを使用します。

```
sess-passwd encrypted password
```

ACS 課金情報

RADIUSユーザーのパスワードを設定するには、次のコンフィギュレーション コマンドを使用します。

cca radius user-password encrypted password *password*

IMS CSCF NPBD バインド IP システム ID

IMS CSCF NPBD バインド IP システム ID を設定するには、次のコンフィギュレーション コマンドを使用します。

IMS CSCF NPBD Bind IP System-id *sys_id* **id** *id* **encrypted password** *password*

SNMP コミュニティ文字列

SNMP コミュニティ文字列を設定するには、次のコンフィギュレーション コマンドを使用します。

snmp community encrypted *password*

TACACS+ クライアントパスワード

TACACS+ クライアントパスワードを設定するには、次のコンフィギュレーション コマンドを使用します。

server priority ip-address *ip_address* **password** *password*

BFD マルチホップピア認証

BFD マルチホップピア認証を設定するには、次のコンフィギュレーション コマンドを使用します。

bfd multihop-peer *peer_name* **authentication** *authentication* **encrypted password** *password*

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。