パスワード暗号化の設定

この章では、Cisco NX-OS デバイスにパスワード暗号化を設定する手順について説明します。

この章は、次の内容で構成されています。

- パスワード暗号化の概要，1 ページ
- パスワード暗号化のライセンス要件，2 ページ
- パスワード暗号化の注意事項と制約事項，2 ページ
- パスワード暗号化のデフォルト設定，3 ページ
- パスワード暗号化の設定，3 ページ
- パスワード暗号化の設定の確認，6 ページ
- パスワード暗号化の設定例，7 ページ
- パスワード暗号化に関する追加情報，7 ページ
- パスワード暗号化の機能の履歴，7 ページ

パスワード暗号化の概要

ここでは、Cisco NX-OS デバイスでのパスワード暗号化について説明します。

AES パスワード暗号化およびマスター暗号キー

強力で、反転可能な 128 ビットの高度暗号化規格（AES）パスワード暗号化（タイプ 6 暗号化ともいう）をイネーブルにすることができます。 タイプ 6 暗号化の使用を開始するには、AES パスワード暗号化機能をイネーブルにし、パスワード暗号化および復号化に使用されるマスター暗号キーを設定する必要があります。

AES パスワード暗号化をイネーブルにしてマスター キーを設定すると、タイプ 6 パスワード暗号化をディセーブルにしない限り、サポートされているアプリケーション（現在は RADIUS と TACACS+）の既存および新規作成されたクリア テキスト パスワードがすべて、タイプ 6 暗号化

の形式で保存されます。 また、既存の弱いすべての暗号化パスワードをタイプ 6 暗号化パスワードに変換するように Cisco NX-OS を設定することもできます。

関連トピック

マスター キーの設定および AES パスワード暗号化機能のイネーブル化
グローバル RADIUS キーの設定
特定の RADIUS サーバ用のキーの設定
グローバル TACACS+ キーの設定
特定の TACACS+ サーバ用のキーの設定

パスワード暗号化の仮想化サポート

AES パスワード暗号化機能で使用するマスター キーは VDC ごとに一意です。

（注） VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

パスワード暗号化のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	パスワード暗号化にはライセンスは必要ありません。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

パスワード暗号化の注意事項と制約事項

パスワード暗号化設定時の注意事項と制約事項は次のとおりです。

- AES パスワード暗号化機能、関連付けられた暗号化と復号化のコマンド、およびマスター キーを設定できるのは、管理者権限（network-admin または vdc-admin）を持つユーザだけです。

- AES パスワード暗号化機能を使用できるアプリケーションは RADIUS と TACACS+ だけです。
- タイプ 6 暗号化パスワードを含む設定は、ロールバックに従いません。
- マスター キーがなくても AES パスワード暗号化機能をイネーブルにできますが、マスター キーがシステムに存在する場合だけ暗号化が開始されます。
- マスター キーを削除するとタイプ 6 暗号化が停止され、同じマスター キーが再構成されない限り、既存のすべてのタイプ 6 暗号化パスワードが使用できなくなります。
- Cisco NX-OS Release 5.2 から以前のリリースにダウングレードする前に、すべてのタイプ 6 パスワードを復号化し、AES パスワード暗号化機能をディセーブルにして、マスター キーを削除してください。
- デバイス設定を別のデバイスに移行するには、他のデバイスに移植する前に設定を復号化するか、または設定が適用されるデバイス上に同じマスター キーを設定します。

パスワード暗号化のデフォルト設定

次の表に、パスワード暗号化パラメータのデフォルト設定を示します。

表 *1*： パスワード暗号化パラメータのデフォルト設定

パラメータ	デフォルト
AES パスワード暗号化機能	ディセーブル
マスター キー	未設定

パスワード暗号化の設定

ここでは、Cisco NX-OS デバイスでパスワード暗号化を設定する手順について説明します。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

マスターキーの設定および**AES**パスワード暗号化機能のイネーブル化

タイプ 6 暗号化用のマスター キーを設定し、高度暗号化規格（AES）パスワード暗号化機能をイネーブルにすることができます。

手順の概要

1. **[no] key config-key ascii**
2. **configure terminal**
3. **[no] feature password encryption aes**
4. （任意） **show encryption service stat**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**[no] key config-key ascii**
	
	例：
	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
		マスター キーを、AES パスワード暗号化機能で使用するように設定します。 マスター キーは、16 ～ 32 文字の英数字を使用できます。 マスター キーを削除するために、いつでもこのコマンドの **no** 形式を使用できます。
		
		マスター キーを設定する前に AES パスワード暗号化機能をイネーブルにすると、マスター キーが設定されていない限りパスワード暗号化が実行されないことを示すメッセージが表示されます。 マスター キーがすでに設定されている場合、新しいマスター キーを入力する前に現在のマスター キーを入力するように求められます。

ステップ 2	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	**[no] feature password encryption aes** 例： `switch(config)# feature password encryption aes`	AES パスワード暗号化機能をイネーブルまたはディセーブルにします。
ステップ 4	**show encryption service stat** 例： `switch(config)# show encryption service stat`	（任意） AES パスワード暗号化機能とマスター キーの設定ステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 （注） このコマンドは、実行コンフィギュレーションとスタートアップ コンフィギュレーションのマスター キーを同期するために必要です。

関連トピック

AES パスワード暗号化およびマスター暗号キー
キーのテキストの設定
キーの受け入れライフタイムおよび送信ライフタイムの設定

既存のパスワードのタイプ 6 暗号化パスワードへの変換

既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換できます。

はじめる前に

AES パスワード暗号化機能をイネーブルにし、マスター キーを設定したことを確認します。

手順の概要

1. **encryption re-encrypt obfuscated**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**encryption re-encrypt obfuscated** 例： `switch# encryption re-encrypt obfuscated`	既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換します。

タイプ 6 暗号化パスワードの元の状態への変換

タイプ 6 暗号化パスワードを元の状態に変換できます。

はじめる前に

マスター キーを設定したことを確認します。

手順の概要

1. **encryption decrypt type6**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**encryption decrypt type6**
	
	例：
	`switch# encryption decrypt type6`
	`Please enter current Master Key:`
		タイプ 6 暗号化パスワードを元の状態に変換します。

タイプ 6 暗号化パスワードの削除

Cisco NX-OS デバイスからすべてのタイプ 6 暗号化パスワードを削除できます。

手順の概要

1. **encryption delete type6**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**encryption delete type6** 例： `switch# encryption delete type6`	すべてのタイプ 6 暗号化パスワードを削除します。

パスワード暗号化の設定の確認

パスワード暗号化の設定情報を表示するには、次の作業を行います。

コマンド	目的
show encryption service stat	AES パスワード暗号化機能とマスター キーの設定ステータスを表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

パスワード暗号化の設定例

次に、マスター キーを作成し、AES パスワード暗号化機能をイネーブルにして、TACACS+ アプリケーションのためのタイプ 6 暗号化パスワードを設定する例を示します。

```
key config-key ascii
  New Master Key:
  Retype Master Key:
configure terminal
feature password encryption aes
show encryption service stat
  Encryption service is enabled.
  Master Encryption Key is configured.
  Type-6 encryption is being used.
feature tacacs+
tacacs-server key Cisco123
show running-config tacacs+
  feature tacacs+
  logging level tacacs 5
  tacacs-server key 6
"JDYkqyIFWeBvzpljSfWmRZrmRSRE8syxKlOSjP9RCCkFinZbJI3GD5c6rckJR/Qju2PKLmOewbheAA=="
```

パスワード暗号化に関する追加情報

ここでは、パスワード暗号化の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

Standards

Standards	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

パスワード暗号化の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *2*：パスワード暗号化の機能の履歴

機能名	リリース	機能情報
パスワードの暗号化	6.0(1)	Release 5.2 以降、変更はありません。
パスワードの暗号化	5.2(1)	この機能が導入されました。