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、次の項で構成されています。

AES パスワード暗号化およびプライマリ暗号キーについて

強力で、反転可能な 128 ビットの高度暗号化規格（AES）パスワード暗号化を有効にすることができます。タイプ 6 暗号化とも言います。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有効にし、パスワード暗号化および復号化に使用されるプライマリ暗号キーを構成する必要があります。

AES パスワード暗号化を有効にしてプライマリ キーを構成すると、タイプ 6 パスワード暗号化を無効にしない限り、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 を構成することもできます。

関連トピック

プライマリ キーの設定および AES パスワード暗号化機能の有効化 （4 ページ）
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

プライマリ キーの設定および AES パスワード暗号化機能の有効化 （4 ページ）

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、およびプライマリ キーを設定できるのは、管理者権限（network-admin）を持つユーザだけです。
- Cisco NX-OS リリース 10.3(3)F 以降、RPM キーチェーン インフラストラクチャは、Cisco Nexus 9000 シリーズ プラットフォーム スイッチの RPM レガシー キーチェーンの AES パスワード暗号化をサポートします。
- タイプ 6 暗号化パスワードを含む構成は、ロールバックに準拠していません。
- プライマリ キーがなくても AES パスワード暗号化機能を有効にできますが、プライマリ 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。
- TACACS+ および RPM レガシー キーチェーンの場合、AES パスワード暗号化機能をイネーブルにし、プライマリキーを設定した後、**encryption re-encrypt obfuscated** コマンドを実行して、パスワードをタイプ 6 暗号化パスワードに変換する必要があります。
- プライマリ キーを削除するとタイプ 6 暗号化が停止され、同じプライマリ 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。
- 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プライマリ キーを設定します。
- タイプ 6 暗号化は、MACsec キーチェーンおよび RPM レガシーキーチェーンでのみサポートされます。cloudsec キーではサポートされていません。
- Cisco NX-OS リリース 9.3(6) 以降、タイプ 6 暗号化パスワードを元の状態に戻すことは、MACsec キーチェーンではサポートされていません。
- Cisco NX-OS リリース 10.3(3)F 以降、タイプ 6 暗号化パスワードを元の状態に戻すことは、RPM 汎用キーチェーンではサポートされていません。
- タイプ 6 暗号化は、AES パスワード暗号化機能が有効で、プライマリ キーが設定されている場合にのみ設定できます。
- プライマリ キーが構成され、AES パスワード暗号化機能がスイッチで有効になっている場合、キーチェーン infra の下の各 MACsec キー ストリング構成は、タイプ 6 暗号化で自動的に暗号化されます。
- プライマリ キーの設定は、スイッチに対してローカルです。あるスイッチからタイプ 6 に構成された実行データを取得し、別のプライマリ キーが設定されている別のスイッチに適用すると、新しいスイッチでの復号化は失敗します。

- タイプ6暗号化の後にスタートアップ構成を消去し、構成の置換機能を使用すると、プライマリ キーがPSSに保存されないため、構成の置換は失敗します。したがって、MACsecタイプ6暗号化キー文字列の構成が失われます。
- タイプ6のキーを構成すると、SKSDが提供する復号コマンドを適用しないと、既存のタイプ6の暗号化キー文字列をタイプ7の暗号化キー文字列に変更できません。
- タイプ6暗号化がサポートされていない古いイメージでコールドリブートによってシステムをダウングレードする場合は、コールドリブートを続行する前に設定を取り出す必要があります。これを行わないと、設定が失われます。
- システムをダウングレードすると、タイプ6の構成は失われます。
- ISSDによってシステムをダウングレードすると、機能確認チェックが呼び出され、ダウングレードに進む前に設定を削除するように通知されます。**encryption decrypt** コマンドを使用して、タイプ6暗号化キーをタイプ7暗号化キーに変換してから、ダウングレードを続行できます。
- ISSUのアップグレード中に、タイプ7暗号化キーを含む古いイメージからタイプ6暗号化をサポートする新しいイメージに移行する場合、再暗号化が強制されるまで、rpmは既存のキーをタイプ6暗号化キーに変換しません。再暗号化を適用するには、**encryption re-encrypt obfuscated** コマンドを使用します。
- タイプ7暗号化キーを含む古いイメージからタイプ6暗号化をサポートする新しいイメージへのISSUアップグレード後、古いイメージに保存されている構成ファイル、またはアップグレード後にタイプ6に対してパスワードを再暗号化せずに保存された構成ファイルを使用して構成の置換が行われた場合（**encryption re-encrypt obfuscated** コマンドを使用して）、構成の置換は失敗します。
- タイプ6暗号化の後にプライマリ キーを変更すると、既存のタイプ6暗号化キー文字列に対する復号コマンドは失敗します。既存のタイプ6キーストリングを削除し、新しいキーストリングを設定する必要があります。
- RPM レガシー キーチェーンの場合、タイプ6キー ストリングは、AESパスワード暗号化機能を有効にしてプライマリ キーを設定しなくても構成できますが、これらのタイプ6キー ストリングは、AESパスワード暗号化機能が有効になり、タイプ6キー ストリングが生成されたプライマリ キーが設定されるまでは使用できません。
- Cisco NX-OS リリース 10.3(2)F 以降、DMEペイロードおよび非インタラクティブ モードを使用して、プライマリ キーを構成できます。

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	無効
プライマリ鍵	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。

プライマリ キーの設定および **AES** パスワード暗号化機能の有効化

タイプ6暗号化用のプライマリ キーを構成し、高度暗号化規格（AES）パスワード暗号化機能を有効にすることができます。

Cisco NX-OS リリース 10.3(3)F 以降では、RPM レガシー キーチェーンでタイプ 6 暗号化がサポートされています。

Procedure

	Command or Action	Purpose

ステップ 1	[**no**] **key config-key ascii**[<new_key> old <old_master_key>]
	Example:
	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
	`{`
	`"actionLSubj": {`
	`"attributes": {`
	`"dn": "sys/action/lsubj-[sys/passwdenc]"`
	`}`
	`"children": [{`
	`"smartcardPasswdEncryptMasterKeyConfigLTask": {`
	`"attributes": {`
	`"adminSt": "start",`
	`"dn":`
		プライマリ キー（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。プライマリ キーは、16 ～ 32 文字の英数字を使用できます。このコマンドの **no** 形式を使用すると、いつでもプライマリ キーを削除できます。
		プライマリ キーを設定する前に AES パスワード暗号化機能を有効にすると、プライマリ 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。プライマリ キーがすでに設定されている場合は、新しいプライマリ キーを入力する前に現在のプライマリ キーを入力するように求められます。

	Command or Action	Purpose
	"sys/action/lsubj-[sys/passwdenc]/smartcardPasswdEncryptMasterKeyConfigTask", "key": "ciscociscociscocisco", "oldKey": "test1test1test1test1", "delete": "no", "freq": "one-shot" } } }] } }	**Note** Cisco NX-OS リリース 10.3(2)F 以降、DME ペイロードおよび非インタラクティブ モードを使用して、プライマリ キーを構成できます。

ステップ 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 3	[no] **feature password encryption aes tam** **Example:** `switch(config)# feature password encryption aes tam`	AES パスワード暗号化機能を有効化または無効化します。
ステップ 4	**encryption re-encrypt obfuscated** **Example:** `switch(config)# 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。
ステップ 5	(Optional) **show encryption service stat** **Example:** `switch(config)# show encryption service stat`	AES パスワード暗号化機能とプライマリ キーの設定ステータスを表示します。
ステップ 6	**copy running-config startup-config** **Example:** `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。 **Note** 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プライマリ キーを同期するために必要です。

Related Topics

AES パスワード暗号化およびプライマリ暗号キーについて （1 ページ）
AES パスワード暗号化およびプライマリ暗号キーについて （1 ページ）

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。

Before you begin

AESパスワード暗号化機能を有効にし、プライマリ キーを設定したことを確認します。

Procedure

	Command or Action	Purpose
ステップ1	**encryption re-encrypt obfuscated** **Example:** `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。この機能は、macsecキーチェーンではサポートされていません。

Before you begin

プライマリ キーを設定したことを確認します。

Procedure

	Command or Action	Purpose

ステップ1	**encryption decrypt type6**
	Example:
	`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。

MACsecキーでのタイプ6暗号化の有効化

Advanced Encryption Standard（AES）パスワード暗号化機能とも呼ばれるタイプ6暗号化機能を使用すると、タイプ6暗号化形式でMACsecキーを安全に保存できます。

Cisco NX-OSリリース9.3(5)以降では、MACsec機能をサポートするすべてのCisco Nexus 9000シリーズ スイッチに、タイプ6暗号化形式でMACsecキーを保存できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **key config-key ascii**
	例：
	`switch(config)# key config-key ascii`
	`switch(config)# New Master Key:`
	`Switch(config)# Retype Master Key:`
		プライマリ キー（マスター キー）を構成します。

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有効化または無効化します。

ステップ 4	**key chain** *name* **macsec**
	例：
	`switch(config)# key chain 1 macsec`
	`switch(config-macseckeychain)#`
		MACSec キーチェーンを作成して MACSec キーのセットを保持し、MACSec キーチェーン設定モードを開始します。

ステップ 5	**key** *key-id*
	例：
	`switch(config-macseckeychain)# key 1000`
	`switch(config-macseckeychain-macseckey)#`
		MAC secキーを作成し、MACsec キー設定モードを開始します。範囲は 1 ー 32 オクテットで、最大サイズは 64 です。AES_128 は 32 ビットで使用され、AES_256 は 64 ビットで使用されます。

ステップ 6	**key-octet-string** *octet-string* **cryptographic-algorithm** {**AES_128_CMAC** | **AES_256_CMAC**} 例： `switch(config-macseckeychain-macseckey)# key-octet-string abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm AES_256_CMAC`	そのキーの octet ストリングを設定します。*octet-string* 引数には、最大 64 文字の 16 進数文字を含めることができます。オクテット キーは内部でエンコードされるため、**show running-config macsec** コマンドの出力にクリア テキストのキーが現れることはありません。 キーオクテット文字列には、次のものが含まれます。 • 0 暗号化タイプ - 暗号化なし（デフォルト） • 6 Encryption Type-Proprietary（Type-6 encrypted）

	コマンドまたはアクション	目的
		• 7 暗号化タイプ - 最大 64 文字の、独自仕様 WORD キー オクテット文列

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。

Procedure

	Command or Action	Purpose
ステップ1	**encryption delete type6** **Example:** `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プライマリ キーの設定ステータスを表示します。

パスワード暗号化の設定例

次の例は、プライマリ キーを作成し、AES パスワード暗号化機能を有効にして、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構成する方法を示しています。

```
key config-key ascii
  New Master Key:
  Retype Master Key:
configure terminal
feature password encryption aes tam
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=="
```

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。