Cisco Application Policy Infrastructure Controller エンタープライズ モジュール リリース 1.2.x アップグレード ガイド

初版：2016 年 05 月 25 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

対象読者

このマニュアルは、ネットワーク内の Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（Cisco APIC-EM）をアップグレードする経験豊富なネットワーク管理者を対象としています。このマニュアルを使用して、Cisco APIC-EMの現在のバージョンをアップグレードしてください。

Cisco APIC-EMの展開、セキュリティ、およびアクセスの詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。

コントローラの GUI を初めて使用する場合は、『*Cisco APIC-EM Quick Start Guide*』を参照してください。

（注）

Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（Cisco APIC-EM）は、このアップグレード ガイドでは コントローラ とも呼ばれます。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、^Dまたは Ctrl+Dというキーの組み合わせは、Ctrl キーを押しながらDキーを押すことを意味します（ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
Italic フォント	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
`太字の courier` フォント	**`太字の courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。

表記法	説明
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス 時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。ステートメント 1071

これらの注意事項を保管しておいてください。

関連資料

- Cisco APIC-EMのドキュメンテーション：
  - 『*Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*』
  - 『*Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*』
  - 『*Cisco APIC-EM Quick Start Guide*』（コントローラの GUI から直接アクセス可能）
  - 『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』

- 『*Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール アップグレード ガイド』
- 『*Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*』
- 『*Cisco Application Policy Infrastructure Controller Enterprise Module Hardware Installation Guide*』
- 『*Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*』
- 『*Open Source Used In Cisco APIC-EM*』

• Cisco APIC-EM用 Cisco IWAN のドキュメンテーション：

- 『*Release Notes for Cisco IWAN*』
- 『*Release Notes for Cisco Intelligent Wide Area Network (Cisco IWAN)*』
- 『*Software Configuration Guide for Cisco IWAN on APIC-EM*』
- 『*Open Source Used in Cisco IWAN and Cisco Network Plug and Play*』

• Cisco APIC-EM用シスコ ネットワーク プラグ アンド プレイのドキュメンテーション：

- 『*Release Notes for Cisco Network Plug and Play*』
- 『*Solution Guide for Cisco Network Plug and Play*』
- 『*Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*』
- 『*Cisco Open Plug-n-Play Agent Configuration Guide*』
- 『*Mobile Application User Guide for Cisco Network Plug and Play*』

（注） ノースバウンド REST API によってコントローラと対話する独自のアプリケーションの開発については、developer.cisco.com/site/apic-em の Web サイトを参照してください。

マニュアルの入手方法およびテクニカル サポート

ドキュメントの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元に直接送信するには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

第 1 章

はじめる前に

アップグレードを開始する前に、次の情報をよくお読みください。

サポートされているアップグレード パスの確認

次のリリースはすべて、Cisco APIC-EMリリース 1.2.0.x に直接アップグレードできます。

- 1.1.2.15
- 1.1.1.38
- 1.1.1.34
- 1.1.0.767
- 1.0.3.4
- 1.0.2.8

リリース 1.0.2.8 または 1.0.3.4 からのアップグレードで問題が発生した場合は、回避手順に関するリリース ノートを参照してください。上記の Cisco APIC-EMリリースよりも前のバージョンを使用している場合は、最新のパッチを使用して上記のいずれかのリリースにアップグレードしてから、リリース 1.2.0.x にアップグレードしてください。

アップグレードにかかる時間の確認

Cisco APIC-EMのアップグレード プロセスは、完了するまでに約 60 分かかる場合があります。アップグレードにかかる実際の時間は、ネットワーク展開の規模、関連するエンドポイントの数、

使用中のアプリケーション（EasyQoS、IWAN、Network Plug and Play）など、いくつかの要因に左右されます。

（注） アップグレードプロセスではサービスがそれぞれ異なるタイミングで再起動するので、すべてのアプリケーションが同時に起動することはありません。

使用可能な Cisco APIC-EM ポートの確認

次の表に、着信トラフィックを許可する Cisco APIC-EMポートと、発信トラフィックに使用されるCisco APIC-EM ポートを示します。着信と発信の両方のトラフィック フローに対して、コントローラでこれらのポートが開かれていることを確認してください。

次の表に、コントローラへの着信トラフィックを許可する Cisco APIC-EM ポートを示します。

表 *1*：*Cisco APIC-EM*着信トラフィック ポートのリファレンス

ポート番号	許可されるトラフィック	プロトコル（**TCP** または **UDP**）
22	SSH	TCP
67	bootps	UDP
80	HTTP	TCP
123	NTP	UDP
162	SNMP	UDP
443	HTTPS	TCP
500	ISAKMP 特定の展開でファイアウォールを越えて複数のホストを展開するには、IPSec ISAKMP（Internet Security Association and Key Management Protocol）UDP ポート 500 の通過を許可する必要があります。	UDP
14141	Grapevine コンソール	TCP
16026	SCEP	TCP

次の表に、コントローラからの発信トラフィックに使用される Cisco APIC-EM ポートを示します。

表 *2* : ***Cisco APIC-EM***発信トラフィック ポートのリファレンス

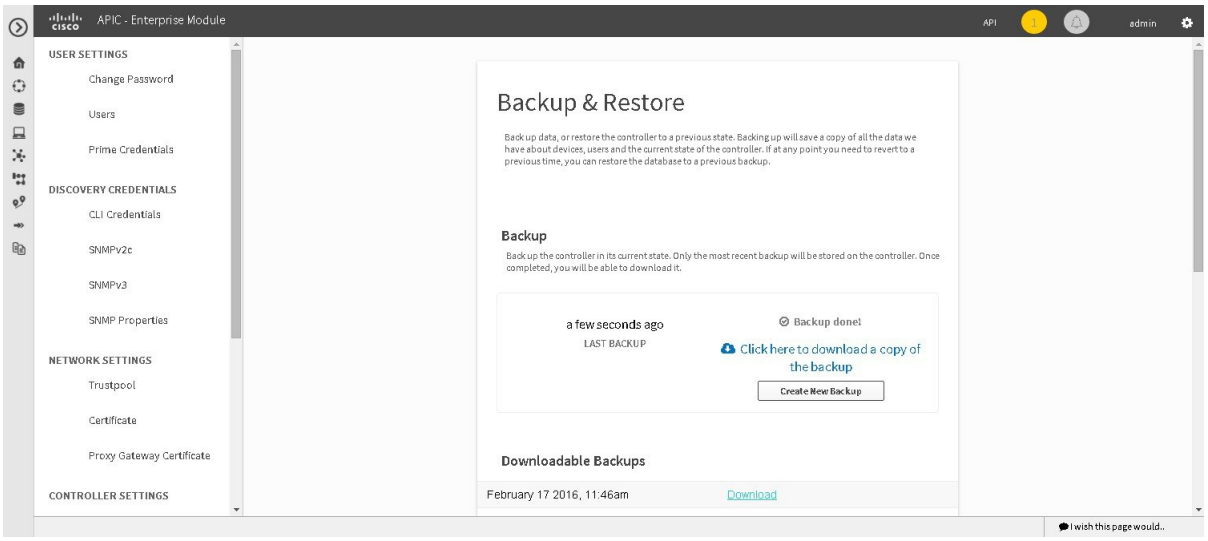
ポート番号	許可されるトラフィック	プロトコル（**TCP** または **UDP**）
22	SSH（ネットワーク デバイスへ）	TCP
23	Telnet（ネットワーク デバイスへ）	TCP
53	DNS	UDP
80	ポート 80 は出力プロキシ設定に使用できます。 さらに、プロキシが Cisco APIC-EM 設定ウィザードで設定されている場合は、8080 など、その他の共通ポートも使用できます（プロキシがすでにネットワークで使用されている場合）。 （注） シスコがサポートしている証明書および trustpool にアクセスするには、コントローラから Cisco アドレス（次の URL を参照）への発信 IP トラフィックを許可するようにネットワークを設定します。 http://www.cisco.com/security/pki/	TCP
123	NTP	UDP
161	SNMP エージェント	UDP
443	HTTPS	TCP

ポート番号	許可されるトラフィック	プロトコル（**TCP** または **UDP**）
500	ISAKMP 特定の展開でファイアウォールを越えて複数のホストを展開するには、IPSec ISAKMP（Internet Security Association and Key Management Protocol）UDP ポート 500 の通過を許可する必要があります。	UDP

コントローラのデータベースとファイルのバックアップ

アップグレードを実行する前に、GUI の [Backup & Restore]ウィンドウ使用して、コントローラのデータベースとファイルをバックアップする必要があります。

図 *1*：*[Backup & Restore]* ウィンドウ



（注） マルチホスト クラスタでは、データベースとファイルは 3 つのホスト間で複製されて共有されます。マルチホスト クラスタでバックアップと復元を実行する場合は、クラスタ内の 3 つのホストのいずれか1つをバックアップする必要があります。バックアップおよび復元の詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。

はじめる前に

この手順を実行するには、管理者（ROLE_ADMIN）権限が必要です。

Cisco APIC-EMを使用してタスクを実行するために必要なユーザ権限については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*』の「*Managing Users and Roles*」の章を参照してください。

ステップ 1 [Home]ウィンドウで、[admin] をクリックするか、画面の右上隅の [Settings] アイコン（歯車）をクリックします。

ステップ 2 ドロップダウン メニューで [Settings]リンクをクリックします。

ステップ 3 [Settings]ナビゲーション ウィンドウで、[Backup & Restore] をクリックして [Backup & Restore] ウィンドウを表示します。

ステップ 4 [Backup & Restore]ウィンドウで、[Create New Backup] ボタンをクリックしてバックアップ ファイルを作成します。

[Create New Backup]ボタンをクリックすると、[Backup in Progress] ウィンドウが GUI に表示されます。

このプロセスで、Cisco APIC-EMはコントローラのデータベースとファイルを圧縮して *.backup* ファイルを作成します。このバックアップ ファイルにはファイル名に反映されるタイムスタンプが付けられます。使用されるファイル命名規則は *yyyy-mm-dd-hh-min-seconds*（年-月-日-時-秒）です。

次に例を示します。

backup_2015_08_14-08-35-10

（注） デフォルトのタイムスタンプ命名規則を使用する代わりに、必要に応じて、バックアップ ファイルの名前を変更できます。

このバックアップ ファイルはコントローラ内のデフォルトの場所に保存されます。バックアップ プロセスが終了すると、[Backup Done!]通知を受け取ります。一度に 1 つのバックアップ ファイルのみがコントローラに保存されます。

（注） バックアップ プロセスが何らかの理由で失敗しても、コントローラやそのデータベースには影響しません。また、バックアップが失敗した理由を示すエラー メッセージが表示されます。バックアップが失敗する最も一般的な原因は、ディスク スペースの不足です。バックアップ プロセスに失敗した場合は、コントローラのディスクに十分な空き容量があることを確認して、再度バックアップを試みてください。

ステップ 5 （任意）別の場所にバックアップ ファイルのコピーを作成します。

バックアップが成功すると、[Download]リンクが GUI に表示されます。そのリンクをクリックして、バックアップ ファイルのコピーをダウンロードし、ネットワーク上の安全な場所に保存します。

（注） コントローラのバックアップ ファイルの復元については『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。

第 2 章

Cisco APIC-EM 展開のアップグレード

最新の Cisco APIC-EM バージョンへのアップグレードおよび検証については、この章の以下のセクションを参照してください。

GUI による Cisco APIC-EMのアップグレード

GUI のアップグレード手順では、次のタスクを実行する必要があります。

1. ソフトウェア ダウンロード リンクのセキュアなシスコ Web サイトからリリース アップグレード パックをダウンロードします。
2. リリース アップグレード パックに対してチェックサムを実行します。
3. GUI を使用して、コントローラにリリース アップグレード パックをアップロードします。
4. GUI を使用して、リリース アップグレード パックでコントローラのソフトウェアを更新します。

（注） マルチホストクラスタでは、1つのホストで更新プロセスを開始すると、クラスタ内の他のすべてのホストで更新プロセスが開始されます。更新プロセスが終了すると、クラスタ内の全ホストの設定が同一になります。最新のソフトウェア リリース（1.2.0.x）が搭載されたマルチホスト クラスタを更新し、ホスト間に IPSec トンネリングも設定する場合は、次の手順を実行します。マルチホスト クラスタでの Cisco APIC-EM リリース 1.2.0.x へのアップグレードおよび IPSec の有効化，（12 ページ）

はじめる前に

Cisco APIC-EMが正常に展開され、動作している必要があります。

Cisco APIC-EMのソフトウェア アップグレードをセキュアなシスコ Web サイトからダウンロードできるという通知を、シスコから受信している必要があります。

この手順を実行するには、管理者（ROLE_ADMIN）権限が必要です。

Cisco APIC-EMを使用してタスクを実行するために必要なユーザ権限については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*』の「*Managing Users and Roles*」の章を参照してください。

重要 リリースのアップグレードについてさらに要件が追加されている可能性があるため、この手順と併せて、Cisco APIC-EMの最新バージョンのリリース ノートもお読みください。Cisco APIC-EMの最新リリースはリリース 1.2.0.x です。このバージョンにアップグレードする場合は、手順を開始する前に、まず『*Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module*, Release 1.2.0.x』を参照してください。

ステップ 1 Cisco APIC-EMのアップグレードに関するシスコからの通知で情報を確認します。
シスコからの通知には、リリース アップグレード パックの場所、および Message Digest 5（MD5）または Secure Hash Algorithm（SHA）512 ビット（SHA512）チェックサムの検証値の場所が指定されています。

（注） Cisco APIC-EMリリース アップグレード パックはビット ファイルになっており、特定のアップグレードの要件に応じてサイズが異なります。リリース アップグレード パックは、数ギガビットの大きさになることもあります。

ステップ 2 ソフトウェア ダウンロード リンクのセキュアなシスコ Web サイトから Cisco APIC-EM のアップグレード パックをダウンロードします。
リリース アップグレード パックは、圧縮された tar ファイルとしてダウンロードできるので、リリース アップグレード パックには .tar.gz 拡張子が付いています。リリース アップグレード パック自体は、次の更新ファイルの一部またはすべてから構成されています。

- サービス ファイル
- Grapevine ファイル
- Linux ファイル

（注） 各リリース アップグレード パックには、セキュリティのために暗号化されたシスコの署名と、パッケージを検証するリリース バージョンのメタデータが含まれています。

ステップ 3 所有しているチェックサム検証ツールまたはユーティリティ（MD5 または SHA512）を使用し、ファイルに対してチェックサムを実行します。

ステップ 4 チェックサム検証ツールまたはユーティリティにより表示されたチェックサム検証値を確認します。
チェックサム検証ツールまたはユーティリティの出力が、シスコ通知またはセキュアなシスコ Web サイトの適切なチェックサム値と一致した場合は、次のステップに進みます。出力がチェックサム値と一致し

ない場合は、リリース アップグレード パックをダウンロードして、別のチェックサムを実行します。チェックサム検証の問題が継続する場合は、シスコ サポートに連絡してください。

ステップ 5 GUI の [Software Update]機能を使用して、コントローラにアップグレード パッケージをアップロードします。
このステップの詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。

ステップ 6 GUI の [Software Update]機能を使用して、アップグレード パッケージでコントローラのソフトウェアを更新します。
このステップの詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。

ステップ 7 GUI の [Home]ウィンドウで、コントローラのソフトウェア バージョン番号を確認します。GUI の [Home] ウィンドウに、新しいソフトウェア バージョンが表示されます。

（注） 以前のリリースから最新の Cisco APIC-EMリリースにアップグレードする場合は、完了まで 1 時間ほどかかることがあります。

次の作業

アップグレード プロセスを確認します（アップグレード プロセスの確認, （15 ページ）を参照）。

CLI による Cisco APIC-EMのアップグレード

CLI のアップグレード手順では、次のタスクを実行する必要があります。

1. ソフトウェア ダウンロード リンクのセキュアなシスコ Web サイトからリリース アップグレード パック（.tar ファイル）をダウンロードします。
2. ファイルに対してチェックサムを実行します。
3. アプライアンス、サーバ、または仮想マシン上の場所にファイルを保存します。
4. ファイルに対して Grapevine アップグレード コマンドを実行します。

（注） マルチホスト クラスタでは、1 つのホストで更新プロセスを開始すると、クラスタ内の他のすべてのホストで更新プロセスが開始されます。更新プロセスが終了すると、クラスタ内の全ホストの設定が同一になります。最新のソフトウェア リリース（1.2.0.x）が搭載されたマルチホスト クラスタを更新し、ホスト間に IPSec トンネリングも設定する場合は、次の手順を実行します。マルチホスト クラスタでの Cisco APIC-EM リリース 1.2.0.x へのアップグレードおよび IPSec の有効化, （12 ページ）

はじめる前に

Cisco APIC-EMが正常に展開され、動作している必要があります。

Cisco APIC-EMのソフトウェア アップグレードをセキュアなシスコ Web サイトからダウンロードできるという通知を、シスコから受信している必要があります。

この手順を実行するには、管理者（ROLE_ADMIN）権限が必要です。

Cisco APIC-EMを使用してタスクを実行するために必要なユーザ権限については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*』の「*Managing Users and Roles*」の章を参照してください。

重要 リリースのアップグレードについてさらに要件が追加されている可能性があるため、この手順と併せて、Cisco APIC-EMの最新バージョンのリリース ノートもお読みください。Cisco APIC-EMの最新リリースはリリース 1.2.0.x です。このバージョンにアップグレードする場合は、手順を開始する前に、まず『*Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module*, Release 1.2.0.x』を参照してください。

ステップ 1 Cisco APIC-EMのアップグレードに関するシスコからの通知で情報を確認します。
シスコからの通知には、リリース アップグレード パックの場所、および Message Digest 5（MD5）または Secure Hash Algorithm（SHA）512 ビット（SHA512）チェックサムの検証値の場所が指定されています。

（注） Cisco APIC-EMリリース アップグレード パックはビット ファイルになっており、特定のアップグレードの要件に応じてサイズが異なります。リリース アップグレード パックは、数ギガビットの大きさになることもあります。

ステップ 2 ソフトウェア ダウンロード リンクのセキュアなシスコ Web サイトから Cisco APIC-EM のアップグレード パックをダウンロードします。
リリース アップグレード パックは、圧縮された tar ファイルとしてダウンロードできるので、リリース アップグレード パックには .tar.gz 拡張子が付いています。リリース アップグレード パック自体は、次の更新ファイルの一部またはすべてから構成されています。

- サービス ファイル
- Grapevine ファイル
- Linux ファイル

（注） 各リリース アップグレード パックには、セキュリティのために暗号化されたシスコの署名と、パッケージを検証するリリース バージョンのメタデータが含まれています。

ステップ 3 所有しているチェックサム検証ツールまたはユーティリティ（MD5 または SHA512）を使用し、ファイルに対してチェックサムを実行します。

ステップ 4 チェックサム検証ツールまたはユーティリティにより表示されたチェックサム検証値を確認します。
チェックサム検証ツールまたはユーティリティの出力が、シスコ通知またはセキュアなシスコ Web サイトの適切なチェックサム値と一致した場合は、次のステップに進みます。出力がチェックサム値と一致し

ない場合は、リリース アップグレード パックをダウンロードして、別のチェックサムを実行します。チェックサム検証の問題が継続する場合は、シスコ サポートに連絡してください。

ステップ 5 ラップトップまたは安全なネットワーク上の場所から、コントローラがあるアプライアンス、サーバ、または仮想マシンにファイルをコピーまたは移動します。

ステップ 6 セキュア シェル（SSH）クライアントを使用し、設定ウィザードで指定したIPアドレスによりホスト（アプライアンス、サーバ、または仮想マシン）にログインします。

ステップ 7 プロンプトが表示されたら、Linux のユーザ名（「grapevine」）と SSH アクセス用のパスワードを入力します。

ステップ 8 ファイルが格納されているフォルダに移動し、次のコマンドを実行します。

```
$ grape update upload [path-to-upgrade-package]
```

grape update upload コマンドでは、そのファイルを使ってコントローラのアップグレード（アップロードと更新）へと進みます。

アップグレード プロセス全体にわたってコントローラの使用を控える必要があります。アップグレード プロセス中に、コントローラがシャットダウンして再起動する可能性があります。シャットダウンプロセスには数分かかることがあります。パーセント バーにアップロードの進捗状況が表示されます。アップロード プロセスが完了すると、アップロードの完了および更新プロセスの開始についての通知が届きます。

```
Release upgrade package uploaded successfully, Update process started.
task_id: 8507f3f6-1de2-11e6-bf7e-00505695af10
```

（注） 更新プロセスの開始時に、コントローラはリリース アップグレード パックの 2 番目の検証テストを実行します。リリース アップグレード パック自体には暗号化されたセキュリティ値（署名）が含まれており、この値がコントローラで復号化されてレビューされます。この 2 番目の検証テストでは、リリース アップグレード パックがシスコからアップロードされたものであることが確認されます。アップグレードプロセスを続行するには、リリースアップグレードパックがこの 2 番目の検証テストに合格する必要があります。

ヒント **grape task display***task_id* コマンドを使用して、更新タスクの進捗状況をモニタします。通知に示されている更新タスク ID を使用します。

ステップ 9 アップグレードプロセス（アップロードと更新）が完了すると、成功または失敗を示す通知が届きます。アップグレードに成功した場合は、アップグレードの成功を示す通知が届き、コントローラの使用を続行できます。アップグレードに失敗した場合は、アップグレードの失敗と推奨是正措置に関する通知が届きます。

次の作業

アップグレード プロセスを確認します（アップグレード プロセスの確認, （15 ページ）を参照）。

マルチホストクラスタでの Cisco APIC-EM リリース 1.2.0.x へのアップグレードおよび IPSec の有効化

コントローラの GUI の [Software Update]機能を使用して、Cisco APIC-EM リリース 1.2.0.x にアップグレードできます。既存のマルチホスト クラスタを Cisco APIC-EM リリース 1.2.0.x にアップグレードして、ホスト間の通信に IP Security（IPSec）を設定する場合は、追加の手順を実行する必要があります。

既存のマルチホスト クラスタをアップグレードし、IPSec トンネリングを設定するには、下記の手順を実行します。手順は以下の順序で実行する必要があります。

1. いずかのホストにコントローラ ソフトウェアをダウンロードして、更新する（ステップ 1 ～ 5）。
2. マルチホスト クラスタを分割または分解する（ステップ 6 ～ 10）。
3. 分解したマルチホスト クラスタ内のすべてのホストを再起動する（ステップ 11）。
4. クラスタに含まれていた最後のホストに IPSec トンネリングを設定する（ステップ 12 ～ 16）。
5. IPSec トンネリングを設定した最後のホストを中心にして、マルチホスト クラスタを再構成する（ステップ 17 ～ 26）。

（注） （既存のマルチホスト クラスタではなく）シングル ホストからマルチホスト クラスタへのアップグレードを予定しており、そのシングル ホストをリリース 1.2.0.x に更新済みの場合は、最初にシングル ホストを再起動してから、設定ウィザードで IPSec トンネリングを設定する必要があります。そのシングル ホストでこの手順を実行した後、新しいホストを結合してクラスタを構成する際には、結合する前にそれらのホストを再起動する必要があります（Cisco APIC-EM ISO を新規にインストールするのではなく、それらの新しいホストがリリース 1.2.0.x に更新済みの場合）。ホストを結合してクラスタを構成すると、各ホストに IPSec トンネリングが設定されます。

はじめる前に

Cisco APIC-EMが正常に展開され、動作している必要があります。

Cisco APIC-EMのソフトウェア アップグレードをセキュアなシスコ Web サイトからダウンロードできるという通知を、シスコから受信している必要があります。

この手順を実行するには、管理者（ROLE_ADMIN）権限が必要です。

Cisco APIC-EMを使用してタスクを実行するために必要なユーザ権限については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*』の「*Managing Users and Roles*」の章を参照してください。

重要 リリースのアップグレードについてさらに要件が追加されている可能性があるため、この手順と併せて、Cisco APIC-EMの最新バージョンのリリース ノートもお読みください。Cisco APIC-EM の最新リリースはリリース 1.2.0.x です。この手順を開始する前に、まず『*Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module*, Release 1.2.0.x』を参照してください。

ステップ 1 ソフトウェア ダウンロード リンクのセキュアなシスコ Web サイトから、リリース 1.2.0.x 用の Cisco APIC-EM アップグレード パックをダウンロードします。

ステップ 2 GUI の [Software Update]機能を使用して、コントローラ（クラスタ内のいずれかのホスト）にアップグレード パッケージをアップロードします。
このステップの詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。

ステップ 3 GUI の [Software Update]機能を使用して、アップグレード パッケージでコントローラのソフトウェアを更新します。
このステップの詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。

ステップ 4 GUI の [Home]ウィンドウで、コントローラのソフトウェア バージョン番号を確認します。GUI の [Home] ウィンドウに、新しいソフトウェア バージョン（1.2.0.x）が表示されます。
（注） 以前のリリースから Cisco APIC-EMリリース 1.2.0.x にアップグレードする場合は、完了まで 1 時間ほどかかることがあります。

ステップ 5 次に進んで、クラスタ内の他のホストのソフトウェア バージョンを確認します。
（注） クラスタ内のいずれかのホストでソフトウェアを更新すると、同じアップグレード パッケージによってクラスタ内の他のホストも更新されます。

ステップ 6 セキュア シェル（SSH）クライアントを使用して、クラスタ内のいずれかのホストにログインします。プロンプトが表示されたら、Linux のユーザ名（「grapevine」）と SSH アクセス用のパスワードを入力します。

ステップ 7 次のコマンドを入力して設定ウィザードにアクセスします。

```
$ config_wizard
```

ステップ 8 [Welcome to the APIC-EM Configuration Wizard!]画面を確認し、クラスタからホストを削除する次のオプションを選択します。

- [Remove this host from its APIC-EM cluster]

ステップ 9 [proceed]を実行してクラスタからこのホストを削除するためのオプションがメッセージとともに表示されます。
[proceed>>]を選択して開始します。[proceed>>]を選択すると、クラスタからこのホストを削除する処理が設定ウィザードで開始されます。

このプロセスの最後に、クラスタからこのホストが削除されます。

ステップ 10 クラスタの 2 番目のホストに対して上記の手順（ステップ 6 ～ 9）を繰り返します。

（注） マルチホスト クラスタが分割されるまで、クラスタ内の各ホストに対して上記のステップを繰り返す必要があります。

重要 最後に削除したクラスタ内の最後のホストをメモします。そのホストに対して次のステップ（IPSec のイネーブル化）を実行する必要があります。たとえば、クラスタ内に3つのホスト（A、B、C）があり、最初にホスト A を削除し、次にホスト B を削除する場合は、ホスト C で IPSec トンネリングを有効にする必要があります。

ステップ 11 IPSec を有効にする前に、sudo reboot コマンドを使用して、上記で分解したマルチホスト クラスタ内の各ホストを再起動します。

```
$ sudo reboot
```

ステップ 12 Secure Shell（SSH）クライアントを使用して、クラスタ内の最後のホストにログインし、config_wizard コマンドを実行します。

```
$ config_wizard
```

ステップ 13 [INTER-HOST COMMUNICATION]画面が表示されるまで、設定ウィザードの現在の設定値を確認して [next>>] をクリックします。

ステップ 14 [yes]を選択して、マルチホスト クラスタ内のホスト間の通信に IPSec スプリット トンネリングを設定します。
マルチホスト クラスタ内のホスト間の通信に使用されるデフォルトのトンネリング プロトコルは、総称ルーティング カプセル化（GRE）です。「yes」と入力すると、このステップで IPSec トンネリングが設定されます。

ステップ 15 設定ウィザード プロセスの最後のステップに達するまで [next>>]をクリックします。

ステップ 16 [proceed>>]をクリックして、設定ウィザードによって Cisco APIC-EM の導入に対する設定変更を保存および適用します。
設定プロセスの最後に、「CONFIGURATIONSUCCEEDED」というメッセージが表示されます。

次に、マルチホストクラスタに含まれていた他のホストにログインし、設定ウィザードを使用して、（ホスト間のセキュアな通信が設定されている）クラスタを再構成します。

ステップ 17 セキュア シェル（SSH）クライアントを使用して、クラスタ内の他のホストのいずれかにログインします。
プロンプトが表示されたら、Linux のユーザ名（「grapevine」）と SSH アクセス用のパスワードを入力します。

ステップ 18 次のコマンドを入力して設定ウィザードにアクセスします。

```
$ config_wizard
```

ステップ 19 [Welcome to the APIC-EM Configuration Wizard!]画面を確認し、[Create a new APIC-EM cluster] オプションを選択します。

（注）　この（2 番目の）ホストを IPSec トンネリングが設定されているホストに結合すると、この（2 番目の）ホストに自動的に IPSec トンネリングが設定されます。

ステップ 20 設定ウィザードによるクラスタの再作成に進みます。
このステップおよびプロセスの詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。

ステップ 21 設定プロセスの最後に、[proceed>>]をクリックし、設定ウィザードにより設定の変更を保存して適用します。
「CONFIGURATIONSUCCEEDED!」というメッセージが表示されます。

ステップ 22 Secure Shell（SSH）クライアントを使用して、3 番目のホストにログインし、設定ウィザードを使って新しいマルチホスト クラスタに参加します。
プロンプトが表示されたら、Linux のユーザ名（「grapevine」）と SSH アクセス用のパスワードを入力します。

ステップ 23 次のコマンドを入力して設定ウィザードにアクセスします。

```
$ config_wizard
```

ステップ 24 [Welcome to the APIC-EM Configuration Wizard!]画面を確認し、[Add this host to an existing APIC-EM cluster]オプションを選択します。

（注）　（IPSec トンネリングが設定されている）マルチホスト クラスタにこのホストを追加すると、このホストに自動的に IPSec トンネリングが設定されます。

ステップ 25 次に進み、設定ウィザードを使用してこのホストをクラスタに追加します。
このステップおよびプロセスの詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。

ステップ 26 設定プロセスの最後に、[proceed>>]をクリックし、設定ウィザードにより設定の変更を保存して適用します。
「CONFIGURATIONSUCCEEDED!」というメッセージが表示されます。

このステップが終了すると、マルチホスト クラスタが更新され、IPSec トンネリングが設定されます。上記のステップを繰り返して、マルチホスト クラスタにホストを追加します。

次の作業

アップグレード プロセスを確認します（アップグレード プロセスの確認, （15 ページ）を参照）。

アップグレード プロセスの確認

アップグレードが正常に行われたかどうかを確認するには、次のいずれかを実行します。

- コントローラの GUI を確認します。

更新すると、更新に関する情報が [Software Update]ウィンドウの [Update History]フィールドにも表示されます。このフィールドには次の更新データが表示されます。

- [Date]：ローカルな更新日時
- [User]：更新を開始した人物のユーザ名
- [UpdateVersion]：リリース アップグレード パックのバージョンの更新パスが矢印で示されます。
- [UpdateStatus]：更新のステータス（成功または失敗）。

（注） このフィールドの失敗ステータスの上にカーソルを置くと（マウスオーバー）、その失敗に関する詳細が表示されます。

- セキュア シェル（SSH）クライアントを使用し、設定ウィザードで指定した IP アドレスでホスト（物理または仮想）にログインして、次の CLI コマンドを実行します。
  - **grape update history**：個々のタスク ID など、コントローラの更新履歴を表示します。
  - **grape release display current**：現在実行されている Cisco APIC-EM ソフトウェア リリースをサービスおよびバージョンと共に表示します。
  - **grape instance display**：サービス インスタンスとバージョンを表示します。
  - **grape instance status**：サービス インスタンスのステータスとバージョンを表示します。

また、ネットワーク テスト（ディスカバリやパス トレースなど）を実行して、コントローラが期待どおりに機能しているかどうか、およびユーザがネットワークで認証されてリソースにアクセスできるかどうかを確認することを推奨します。

第 3 章

アップグレードの失敗からの回復

アップグレードの失敗

次の表は、既知のアップグレード エラーとその回復方法の一部を示しています。

表 *3*：アップグレードの失敗

症状	考えられる原因	推奨処置
ベアメタル サーバでアップグレードに失敗。	このリリースのシステム要件を満たしていない状態で、コントローラのアップグレードを試みた。	最新の Cisco APIC-EM リリース ノートにアクセスし、システム要件を確認します。ベアメタルのアップグレードに適した特定のシステム要件を確認してください。 コントローラのアップグレードを再試行します。 引き続き失敗する場合は、シスコのサポートに連絡してください。 Cisco TAC の連絡先情報については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x*』を参照してください。

症状	考えられる原因	推奨処置
仮想マシンでアップグレードに失敗。	このリリースのシステム要件を満たしていない状態で、コントローラのアップグレードを試みた。	最新の Cisco APIC-EM リリースノートにアクセスし、システム要件を確認します。VMware リソースプールの要件を含めて、仮想マシンのアップグレードに適した特定のシステム要件を確認してください。 コントローラのアップグレードを再試行します。 引き続き失敗する場合は、シスコのサポートに連絡してください。 Cisco TAC の連絡先情報については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x*』を参照してください。
仮想マシンでアップグレードに失敗。	コントローラのエラーメッセージが、NTP サーバに問題があることを示している。	VMware vSphere 環境内の仮想マシンで Cisco APIC-EM をアップグレードする場合は、ESXi ホストの時刻設定が NTP サーバと同期していることも確認する必要があります。同期を確保できないと、アップグレードに失敗します。 NTP サーバの設定が同期していない場合は、SSH を使用してコントローラにログインし、**reset_grapevine** コマンドを実行して NTP サーバの設定を更新します。 コントローラのアップグレードを再試行します。 **reset_grapevine** コマンドの使用方法および Cisco TAC の連絡先情報については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x*』を参照してください。

症状	考えられる原因	推奨処置
ベア メタル サーバまたは仮想マシンでアップグレードに失敗。	コントローラ GUI のエラー メッセージが、アップグレード後に Cisco APIC-EM でコア サービスの起動に失敗したことを示している。	コントローラのアップグレードを再試行します。 引き続き失敗する場合は、次のアクションを実行します。 • 開発者コンソールにログインします。 • 開発者コンソールでサービスのステータスを確認します。 • rca ファイルを作成してサポートに送信し、支援を求めます。 上記の手順および Cisco TAC の連絡先情報については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x*』を参照してください。

アップグレード失敗時のシステムログの確認とサポートファイルの作成

システム ログを確認してサポート ファイルを作成することにより、Cisco APIC-EMのアップグレードの失敗をトラブルシューティングできます。このサポート ファイルは、ログ、コンフィギュレーションファイル、およびコマンド出力から構成されます。サポートファイルを作成した後、それをシスコ サポートに電子メールで送信してサポートを得ることができます。

ステップ 1 セキュア シェル（SSH）クライアントを使用し、設定ウィザードで指定したIPアドレスによりホスト（物理または仮想）にログインします。

（注） SSH クライアントで入力する IP アドレスは、ネットワーク アダプタ用に設定した IP アドレスです。この IP アドレスによって、ホストが外部ネットワークに接続されます。

ステップ 2 プロンプトが表示されたら、Linux のユーザ名（「grapevine」）と SSH アクセス用のパスワードを入力します。

ステップ 3 ホストの /var/log ディレクトリに移動します。log ディレクトリには、コントローラのシステム ログが格納されています。

ステップ 4 次のログ ファイルを開いて表示し、アップグレードが失敗した原因を特定します。

- grapevine_manager_activity.log
- grapevine_manager.log

アップグレードの失敗原因を特定して修正できない場合は、次の手順に進みます。

ステップ 5 ホストのbinディレクトリに移動します。binディレクトリにはgrapevineスクリプトが含まれています。

ステップ 6 サポート ファイルを作成するには、このディレクトリで rca コマンドを入力します。

```
$ rca
mkdir: created directory '/tmp grapevine-rca-2016-04-05_16-22-20-PM_PDT-0700'

----------------------------------------------------------------------
RCA package created On Tues April 5 16:22:20 PDT 2016
----------------------------------------------------------------------
```

rca コマンドにより根本原因分析スクリプトが実行され、ログ ファイル、コンフィギュレーション ファイル、およびコマンド出力を含む tar ファイルが作成されます。

次の作業

この手順で作成した tar をシスコ サポートに送信して、問題を解決するためのサポートを受けてください。

索 引