Cisco Identity Services Engine アップグレード ガイド リリース 1.2

初版：2013 年 01 月 31 日

最終更新：2013 年 07 月 22 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/

Text Part Number: OL-27087-01-J

【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。

はじめに

目的

このマニュアルは、Cisco ISE アプライアンスおよび VMware 仮想マシンで Cisco Identity Services Engine（ISE）ソフトウェア イメージをアップグレードする方法について説明します。

以前のリリースまたはメンテナンス リリースからリリース 1.2 に Cisco ISE をアップグレードできます。 Cisco Secure Access Control System (ACS)、リリース 5.3 からリリース 1.2 に移行できます。

Cisco Secure ACS 4.*x* 以前のバージョン、Cisco Secure ACS 5.1、または 5.2 Cisco Network Admission Control (NAC) アプライアンスからリリース 1.2 に移行することはできません。

Cisco Secure ACS、リリース 5.3 から Cisco ISE、リリース 1.2 への移行については、『*Cisco Identity Services Engine, Release 1.2 Migration Tool Guide*』を参照してください。

（注） Cisco Secure ACS、リリース 5.3 からのみ、Cisco ISE、リリース 1.2 に直接移行できます。 Cisco Secure ACS、リリース 4.*x*、5.1、および 5.2 では、ACS、リリース 5.3 にアップグレードしてから、Cisco ISE、リリース 1.2 に移行する必要があります。

対象読者

このガイドは、Cisco ISE 3300 シリーズ アプライアンスまたは VMware サーバで Cisco ISE ソフトウェアをアップグレードおよび設定するネットワーク管理者、システム インテグレータ、ネットワーク導入担当者を対象としています。このアップグレードガイドを使用する準備として、ネットワーク設備およびケーブル接続を理解し、電気回路、配線、装置ラックの取り付けに関する基礎知識を得ておく必要があります。

ガイドの構成

章	説明（Description）
Cisco ISE のアップグレード	Cisco Identity Services Engine (ISE) をリリース 1.2 にアップグレードする場合について概要を説明します。
スタンドアロンおよび 2 ノード展開の Cisco ISE、リリース 1.2 へのアップグレード, （19 ページ）	Cisco ISE スタンドアロンおよび 2 ノードの展開をリリース 1.2 にアップグレードする方法について説明します。
分散展開の Cisco ISE、リリース 1.2 へのアップグレード	Cisco ISE 分散展開をリリース 1.2 にアップグレードする方法について説明します。
Cisco ISE アップグレードの障害からの復旧	アップグレードの障害から回復する方法について説明します。

表記法

表記法	説明（Description）
^ 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 キーを押して、D キーを押すことを意味します。（キー ラベルは大文字で表記されていますが、大文字と小文字の区別はありません）。
太字	ユーザが入力する必要があるコマンドおよびキーワードは、**太字** で示しています。
イタリック体	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、イタリック体フォントで示しています。

表記法	説明（Description）
courier フォント	システムが表示するターミナル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。
|	選択肢を示す縦棒は、キーワード セットまたは引数セットのいずれかの選択肢を示します。
[x | y]	いずれか1つを選択できる省略可能な要素は、角カッコで囲み、選択肢を示す縦棒で区切って示しています。
{x | y}	必ずいずれか 1 つを選択しなければならない必須要素は、波カッコで囲み、縦棒で区切って示しています。
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。
< >	山カッコは、ユーザが入力しても画面に表示されないパスワードなどの文字列を示しています。
[ ]	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。
! #	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、このマニュアル以外の参照資料などを紹介しています。

ヒント　この情報が問題の解決などに役立つ情報をであることを示しています。

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。 記述されている操作を実行すると時間を節約できます。

警告　**「警告」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。**

関連資料

リリース固有のドキュメント

次の表に、Cisco ISE リリースで利用可能な製品マニュアルを示します。

表 *1*：*Cisco Identity Services Engine* の製品マニュアル

『*Release Notes for the Cisco Identity Services Engine, Release 1.2*』	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
『*Cisco Identity Services Engine Network Component Compatibility, Release 1.2*』	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
• 『*Cisco Identity Services Engine User Guide, Release 1.2*』 • 『*Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.2*』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』 『*Cisco Identity Services Engine アップグレード ガイド リリース 1.2*』 『*Cisco Identity Services Engine, Release 1.2 Migration Tool Guide*』 『*Regulatory Compliance and Safety Information for Cisco Identity Services Engine 3400 Series Appliance and Cisco 3400 Secure Access Control System*』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2*』 『*Cisco Identity Services Engine API Reference Guide, Release 1.2*』	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
『*Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card*』	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html

プラットフォーム固有のマニュアル

次の表に、その他のプラットフォーム固有のマニュアルのリンクを示します。

表 *2*：プラットフォーム固有のマニュアル

Cisco ISE	http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html
Cisco UCS C シリーズ	http://www.cisco.com/en/US/docs/unified_computing/ucs/overview/guide/UCS_rack_roadmap.html
Cisco Secure Access Control System	http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html
Cisco NAC Appliance	http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html
Cisco NAC Profiler	http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
Cisco NAC Guest Server	http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『What's New in Cisco Product Documentation』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

Cisco ISE のアップグレード

Cisco Identity Services Engine（ISE）は、CLI からのみ（CLI）アプリケーションのアップグレードをサポートしています。 Cisco ISE の古いリリースはすべて、新しいリリースにアップグレードできます。 以前のリリースは、パッチがインストールされているか、メンテナンス リリースである場合があります。

リリース 1.2 にアップグレードする前に確認する必要がある重要事項

（注）

- Cisco ISE、リリース 1.0.4.573 を Cisco ISE、リリースの新しいバージョン（たとえば、Cisco ISE、リリース 1.1、1.1.x、1.2 など）にアップグレードするとき、または Cisco ISE、リリース 1.0.4.573 バックアップから Cisco ISE の以降のバージョンに復元するときに、システムのデフォルトのスポンサー グループとスポンサー グループ ポリシーを削除しないでください。
- 管理、サービス ポリシー、モニタリング ノードのみをアップグレードできます。 アップグレードは、インライン ポスチャ ノード（IPN）ではサポートされません。 IPN では、アプライアンスのイメージを再作成し、新規インストールを実行する必要があります。
- すべてのノードのローカル リポジトリにアップグレード バンドルをコピーすることを強くお勧めします。 ローカル リポジトリでアップグレード バンドルを使用すると、アップグレード プロセス中にネットワークからのダウンロードにかかる時間が大幅に短縮されます。

  1. Cisco ISE UI からディスク :/ のローカル リポジトリを作成します。
  2. Cisco ISE CLI から copy コマンドを使用してローカル ディスクにアップグレード バンドルをコピーします。 **copy***ftp-filepath* **ise-upgradebundle-1.1.x-to-1.2.0.899.i386.tar.gz disk:/**

     再びローカル ディスクにアップグレード バンドルをコピーしたら、ローカル ディスクのアップグレードバンドルのサイズがリポジトリのアップグレードバンドルと同じであることを確認します。 **dir** コマンドを使用して、ローカルディスクのアップグレード バンドルのサイズを確認します。

- アップグレードバンドルの MD5sum を確認します。 FTP、SFTP など、リポジトリにアップグレードバンドルをダウンロードした後、MD5sum が正しいことを確認します。 Linux で **md5sum コマンド**または **MAC OSX で** md5 コマンドを使用できます。
- 仮想マシンで Cisco ISE をアップグレードしている場合は、Cisco ISE、リリース 1.2 用の VMware 仮想マシンの設定, （4 ページ）のセクションを読みます。 これらの推奨事項は、ノードのイメージを再作成する場合、新しい VM またはアプライアンスとノードを交換する場合、または修復が不可能なセカンダリ ノードのアップグレード エラーがある場合にも有用です。

関連トピック

『Cisco Identity Services Engine User Guide, Release 1.2』

『Cisco Identity Services Engine CLI Reference Guide, Release 1.2』

通信用に開く必要があるファイアウォール ポート

レプリケーション ポートは、Cisco ISE、リリース 1.2 で変更されました。プライマリ管理ノードと他のノード間でファイアウォールを導入した場合は、リリース 1.2 にアップグレードする前に次のポートを開く必要があります。

- TCP 1528：プライマリ管理ノードとモニタリング ノード間の通信。
- TCP 443：プライマリ管理ノードとその他すべてのセカンダリ ノード間の通信。
- TCP 12001：グローバル クラスタのレプリケーション用。

Cisco ISE、リリース 1.2 の全リストについては、『*Cisco Identity Services Engine Hardware Installation*』を参照してください。

Preupgrade のその他の考慮事項

アップグレードを開始する前に、次の情報を注意深く読み、そのコンフィギュレーション（バックアップ、エクスポート、スクリーン ショットの取得）を可能な限り記録してください。

- 新しくアップグレードされたノードにデータを復元する前に、『*Cisco Identity Services Engine User Guide, Release 1.2*』のデータの復元に関するガイドラインお読みください。
- Cisco Application Deployment Engine（ADE）の設定データが含まれているプライマリ管理ノードから Cisco ISE 設定データのバックアップを実行します。
- プライマリ モニタリング ノードから Cisco ISE 動作データのバックアップを実行します。
- 秘密キーを含む証明書を、環境内のすべてのノードからエクスポートし、ローカル システムに保存します。 Cisco ISE ノードごとに HTTPS および EAP 証明書の Common Name (CN) または SAN が、該当ノードの完全修飾ドメイン名に一致することを確認します。
- Cisco ISE CLI から **copy running-config** *destination* コマンドを使用して実行コンフィギュレーションのバックアップを作成します。*destination* は、 ftp、sftp、ディスクなどの URL です。
- 外部アイデンティティ ソースとして Active Directory を使用している場合は、Active Directory クレデンシャルがあることを確認します。 アップグレード後に、Active Directory 接続が失われることがあります。 この場合、Cisco ISE を Active Directory に再度参加させます。
- デフォルトのプロファイラのポリシーを編集およびカスタマイズした場合は、デフォルトのプロファイラのポリシーをファイルにエクスポートし、アップグレード後にインポートします。 アップグレード プロセスでは、デフォルトのプロファイラのポリシーが上書きされます。
- ユーザがデフォルトの言語テンプレートに行ったカスタマイゼーションを記録します。アップグレード後に、古い展開でカスタマイズしたデフォルト言語テンプレートを編集する必要があります。

- アラーム、メールの設定、レポートのカスタマイズ、お気に入りレポート、モニタリングデータのバックアップ スケジュール、およびデータ削除の設定を記録します。 そして、アップグレード後に再設定する必要があります。
- アップグレード前に、ゲスト、プロファイラ、オンボード デバイスなどのサービスをディセーブルにし、アップグレード後にこれらをイネーブルにします。 そうしない場合、失われたゲスト ユーザを追加し、デバイスのプロファイルとオンボードを再度行う必要があります。
- SNMP プロファイラのプローブ設定を記録します。 プロファイリングに使用する場合、アップグレード後にプライマリ管理ノードからのプロファイラの SNMP ポーリングを再設定する必要があります。
- リモート アップグレードで Cisco ISE CLI からコンソール タイムアウトを一時的にディセーブルにします。 Cisco ISE CLI から次のコマンドを使用します。**terminal session-timeout 0**。コンソール タイムアウトをディセーブルにした後、Cisco ISE CLI からのログアウトとログインを行います。 アップグレードの完了後、ターミナル セッション タイムアウトが元の値に設定されていることを確認します。 デフォルト値は 30 分です。
- ノード ペルソナの変更、システム同期、ノードの登録または登録解除などの展開設定の変更は、展開内のすべてのノードが完全にアップグレードされるまで遅延することを強く推奨します。 ただし、この推奨事項は、失敗したアップグレードからの復旧時に必要な手順にはあてはまりません。
- ディスク領域の使用率を最適化し、パフォーマンスを向上する Release 1.2 のデータベース設計とスキーマの変更のために、モニタリング ノードのデータベース サイズは Release 1.2 へのアップグレード後に減少します。
- Cisco ISE 1.1.*x* から 1.2 へのアップグレードには、32 ビットから 64 ビット システムへのオペレーティング システムとアプリケーション バイナリのアップグレードが含まれます。 アップグレード中、データベース、オペレーティング システムのアップグレード後に、ノードが 2 回リブートされます。 2 回目のリブートの後、64 ビット アプリケーション バイナリがインストールされ、データベースが 64 ビット システムに移行されます。 このプロセス中に、**show application status ise** コマンドを使用して、CLI からアップグレードの進行状況をモニタできます。 次のメッセージが表示されます。「% NOTICE: Identity Services Engine upgrade is in progress...」

関連トピック

『Cisco Identity Services Engine User Guide, Release 1.2』
『Cisco Identity Services Engine CLI Reference Guide, Release 1.2』

Cisco ISE、リリース 1.2 用の VMware 仮想マシンの設定

仮想マシンでノードをアップグレードしたら、次のステートメントを慎重に確認してください。リリース 1.2 にアップグレードする前に、次の変更を行う必要があります。

（注） 次の変更を行う前に仮想マシンの電源をオフにし、変更後に電源を再投入する必要があります。

- Cisco ISE、リリース 1.2 は、64 ビット システムです。 仮想マシンのハードウェアが 64 ビット システムと互換性を持つことを確認します。 詳細については、『Cisco Identity Services Engine Hardware Installation Guide, Release 1.2』を参照してください。 64 ビット システムに必要な BIOS 設定をイネーブルにします。 64 ビット ゲスト オペレーティング システムのハードウェアおよびファームウェアの要件については、VMware ナレッジ ベースを参照してください。 リリース 1.2 へのアップグレード後に、ゲスト オペレーティング システムとして Linux、バージョンとして Red Hat Enterprise Linux 5（64 ビット）を選択します。 詳細については、VMware ナレッジ ベースを参照してください。
- また、仮想マシンの CPU およびメモリ サイズを増やすこともできます。 SNS 3400 シリーズ アプライアンスの導入のサイジングおよびスケーリングの推奨事項については、『Cisco Identity Services Engine Hardware Installation Guide、リリース 1.2』を参照してください。 仮想マシンのディスク サイズを大きくする場合は、アップグレードできないため、リリース 1.2 の新規インストールを実行します。 リリース 1.2 のインストール後は、Cisco ISE CLI から **show inventory** コマンドを使用して CPU およびメモリ サイズを検査できます。

アップグレード時間の計算

アップグレード時間の計算

次の表に、リリース 1.2 にアップグレードするためにかかる推定時間を示します。 アップグレードにかかる実際の時間は、いくつかの要因によって異なります。 実稼働ネットワークは、アップグレード プロセス中にダウンタイムなしで動作し続けます。 ここに示すデータは、44 個の Cisco ISE ノード（2 個の管理ノード、2 個の監視ノード、および 40 個ポリシー サービス ノード）を含む展開からのものです。 この展開は、100,000 のエンドポイント、12,500 のユーザ。25,000 のゲスト ユーザ。100 のユーザ グループ（ユーザごとに 5 つの属性）から構成されます。 プロファイリング サービスがイネーブルになり、DHCP、HTTP、RADIUS、ネットワーク スキャン（NMAP）、DNS、SNMPQUERY のプローブが有効になりました。

展開のタイプ	ノードのペルソナ	アップグレードにかかる時間
スタンドアロン（2000 エンドポイント）	管理、ポリシー サービス、監視	1 時間 20 分

分散（12,500 のユーザと 25,000 のエンドポイント）	セカンダリ管理	7 時間
	モニタリング（Monitoring）	4 hours（4 時間）
	ポリシー サービス（Policy Service）	1.5 時間
	管理、モニタリング	2 時間

アップグレードにかかる時間に影響する要因

- ネットワークのエンドポイント数
- ネットワークのユーザ数とゲスト ユーザ数
- イネーブルの場合はプロファイリング サービス

（注） 仮想マシンの Cisco ISE ノードでは、リリース 1.2 にアップグレードするためにさらに時間がかかることがあります。

データ損失を回避するために、アップグレードを実行する前にバックアップを行う

データ損失を防ぐために、アップグレード前に Cisco ISE の設定データおよびモニタリング（運用）データを手動でバックアップする必要があります。

Cisco ISE ユーザ インターフェイスからのオンデマンド バックアップの実行

Cisco ISE ユーザ インターフェイスでは、プライマリ管理ノードのオンデマンド バックアップを実行できます。 Cisco ISE アプリケーション、ADE-OS 設定データ、モニタリング（運用）データのバックアップを実行します。 バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、または TFTP。 これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。分散展開では、プライマリ管理およびプライマリ モニタリング ペルソナが同じノード（アプライアンスまたは仮想マシン）で実行する場合、バックアップ用のローカル リポジトリを使用できます。別のノード（アプライアンスまたは仮想マシン）で実行している場合、ローカル リポジトリをバックアップに使用できません。 リポジトリを作成するために CLI および GUI を使用できますが、Cisco ISE リリース 1.2 の場合、次の理由により GUI を使用することを推奨します。

- CLI で作成されたリポジトリはローカルに保存され、他の展開ノードに複製されません。 こうしたリポジトリは、リポジトリの GUI ページに表示されません。
- GUI を通じてプライマリ管理ノードで作成されたリポジトリは、他の展開ノードに複製されます。

はじめる前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- このタスクを実行するには、Cisco ISE でバック アップ可能なデータの種類について基本的な理解が必要です。 Cisco ISE の設定およびモニタリング データのオンデマンド バックアップを実行する必要があります。
- このタスクを実行する前に、リポジトリを設定したことを確認します。 詳細については、『Cisco Identity Services Engine User Guide, Release 1.1.x』を参照してください。
- バックアップを実行する場合、ノードのロールを変更しないでください。また、ノードを昇格させないでください。 バックアップの実行中にノードのロールを変更すると、すべての手順が中断し、データに不一致が生じる場合があります。 ノードのロールを変更する際は、バックアップが完了するまで待機してください。
- 実行コンフィギュレーションをネットワーク サーバなどの安全な場所にコピーするか、Cisco ISE サーバのスタートアップ コンフィギュレーションとして保存します。 このスタートアップ コンフィギュレーションは、バックアップおよびシステム ログから Cisco ISE アプリケーションを復元またはトラブルシューティングする際に使用できます。 実行中の設定をスタートアップ コンフィギュレーションにコピーする詳細な方法については、『Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x』の「**copy**」コマンドを参照してください。

（注） 運用（モニタリング データ）のバックアップは、プライマリおよびセカンダリのモニタリング ノードからのみ取得できます。

手順

ステップ 1 Cisco ISE 管理ユーザ インターフェイスにログインします。

ステップ 2 [管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] を選択します。

ステップ 3 [データ管理（Data Management）] > [管理ノード（Administration Node）] > [オンデマンド フル バックアップ（Full Backup On Demand）]を選択します。
モニタリング データをバック アップする場合は、[モニタリング ノード（Monitoring Node）] を選択します。

ステップ 4 バックアップを実行するために必要な値を入力します。

ステップ 5 [すぐにバックアップ（Backup Now）] をクリックします。

ステップ 6 バックアップが正常に完了したことを確認します。
Cisco ISE は、バックアップ ファイル名にタイムスタンプを追加し、このファイルを特定のリポジトリに保存します。バックアップ ファイルが指定したリポジトリ内に存在するかどうか確認してください。

関連トピック

http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_backup.html#wp1066156
『Cisco Identity Services Engine User Guide, Release 1.1.*x*』

Cisco ISE CLI からのバックアップの実行

Cisco ISE CLI から Cisco ISE の設定または運用データのバックアップを実行し、そのバックアップをリポジトリに保存するには、EXEC モードで **backup** コマンドを入力します。

はじめる前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- このタスクを実行するには、Cisco ISE でバック アップ可能なデータの種類について基本的な理解が必要です。 Cisco ISE の設定およびモニタリング データのオンデマンド バックアップを実行する必要があります。
- このタスクを実行する前に、リポジトリを設定したことを確認します。 詳細については、『Cisco Identity Services Engine User Guide, Release 1.1.x』を参照してください。
- バックアップを実行する場合、ノードのロールを変更しないでください。また、ノードを昇格させないでください。バックアップの実行中にノードのロールを変更すると、すべての手順が中断し、データに不一致が生じる場合があります。 ノードのロールを変更する際は、バックアップが完了するまで待機してください。
- 実行コンフィギュレーションをネットワーク サーバなどの安全な場所にコピーするか、Cisco ISE サーバのスタートアップ コンフィギュレーションとして保存します。 このスタートアップ コンフィギュレーションは、バックアップおよびシステム ログから Cisco ISE を復元またはトラブルシューティングする際に使用できます。 実行中の設定をスタートアップ コンフィギュレーションにコピーする詳細な方法については、『Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x』の「**copy**」コマンドを参照してください。

（注） 運用のバックアップは、プライマリおよびセカンダリのモニタリング ノードからのみ取得できます。

バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、またはTFTP。 これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。

分散展開では、プライマリ管理およびプライマリ モニタリング ペルソナが同じノード（アプライアンスまたは仮想マシン）で実行する場合、バックアップ用のローカル リポジトリを使用できます。 別のノード（アプライアンスまたは仮想マシン）で実行している場合、ローカル リポジトリをバックアップに使用できません。

手順

Cisco ISE コンフィギュレーション データを取得するには、古い展開のプライマリ管理ノードで CLI で ISE **コンフィギュレーション** コマンドの operator パラメータと **backup** コマンドを入力します。 Cisco ISE 運用（モニタリングおよびトラブルシューティング）データを取得するには、古い展開のプライマリまたはセカンダリ モニタリング ノードの CLI で **ise-operational** のコマンドの operator パラメータとともに **backup** コマンドを入力します。
Cisco ISE 設定バックアップを取得する CLI コマンド。

backup *backup-name* **repository** *repository-name* **ise-config encryption-key**{**hash | plain**} *encryption-keyname*

Cisco ISE 運用バックアップを取得する CLI コマンド。

backup *backup-name* **repository** *repository-name* **ise-operational encryption-key**{**hash | plain**} *encryption-keyname*

下の表に構文を説明します。

backup-name	バックアップ ファイルの名前。 最大 100 文字の英数字をサポートします。
repository	バックアップ ファイルを保存するリポジトリを指定します。
repository-name	ファイルのバック アップ先になるリポジトリの名前と場所。 最大 80 文字の英数字をサポートします。
ise-config	（任意）Cisco ISE コンフィギュレーション データをバックアップします（Cisco ISE ADE-OS コンフィギュレーション データが含まれます）。

ise-operational	（任意）Cisco ISE 運用（モニタリングおよびトラブルシューティング）データだけをバックアップします。 プライマリおよびセカンダリ モニタリング ノードでは、このコマンドの operator パラメータのみを指定できます。
encryption-key	暗号キーを指定して、バックアップを保護します。
hash	ハッシュ化された暗号キーを指定して、バックアップを保護します。
plain	プレーンテキストの暗号キーを指定して、バックアップを保護します。 使用する暗号化されたプレーンテキストの暗号化キーを指定します。 最大 15 文字長のサポート。 バックアップ用。
encryption-key name	hash | plain 形式の暗号キーの名前。 ハッシュ暗号化について 40 文字、プレーン テキストの暗号化について最大 15 文字をサポートします。

backup コマンドは Cisco ISE と ADE-OS コンフィギュレーション データとモニタリング データのバックアップを実行し、暗号化（ハッシュ）または暗号化プレーン テキストのパスワードのバックアップをリポジトリに保存します。

ユーザ定義の暗号キーを使用してバックアップを暗号化および復号化できます。

```
ise/admin# backup mybackup repository myrepository ise-config encryption-key plain Lab12345
% Creating backup with timestamped filename: backup-111125-1252.tar.gpg
ise/admin#

ise/admin# backup mybackup repository myrepository ise-operational encryption-key plain
Lab12345
% Creating backup with timestamped filename: backup-111125-1235.tar.gpg
ise/admin#
```

関連トピック

『Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x』

Cisco ISE 1.2 アップグレード プロセス

Cisco ISE Command-Line Interface (CLI) からのみ Cisco ISE、リリース 1.2 にアップグレードできます。 スタンドアロンのアップグレードまたは 2 ノードの導入の手順については、「第 *2* 章、スタンドアロンおよび *2* ノード展開のリリース *1.2* へのアップグレード」を参照してください。 分散

展開のアップグレード手順については、「第 *3* 章、分散展開を *Cisco ISE*、リリース *1.2* にアップグレードする」を参照してください。

スタンドアロン ノードのアップグレードプロセスは、展開のノードをアップグレードするための設定とは異なります。 Cisco ISE CLI から application upgrade コマンドを実行すると、各ノードでバックグラウンドにより次の処理が行われます。

1. アップグレード バンドルをダウンロードし、抽出します。
2. コンフィギュレーションデータベースのバックアップを実行します（リカバリ可能な障害時の自動ロール バックの場合）。
3. 構成データベースをアップグレードするか、アップグレードされた構成データベースのダンプをダウンロードします（スタンドアロン ノードの場合）。
4. モニタリング データベースをアップグレードします。
5. オペレーティング システムとアプリケーション バイナリ ファイルをアップグレードします。
6. 32 ビット システムから 64 ビット システムにデータベースを移行します。
7. 正常なアップグレード後、Cisco ISE、リリース 1.2 にログインするプロンプトがユーザに示されます。

分散展開では、アップグレードプロセスは分散展開モデルに従います。新しいリリースにセカンダリ管理ノードをアップグレードした後、Cisco ISE は新規展開を作成します。 古い展開からのセカンダリ管理ノードが新規展開のプライマリ管理ノードになります。 古い展開の他のノードをアップグレードすると、新しい展開に結合されます。

古い展開からセカンダリ管理ノードをアップグレードすると、古い展開設定が保存され、アップグレードのプライマリ管理ノードに通知されます。 古い展開のプライマリ管理ノードがアップグレードについて他のノードに通知します。 アップグレード後に、古い展開からのノードは、新規配置のプライマリ管理ノードに参加します。アップグレードプロセスでは、ライセンスと証明書が維持されます。 ファイルを再インストールまたは再インポートする必要はありません。 Cisco ISE、リリース 1.2 は、2 ノードの Unique Device Identifier (UDI) が含まれるライセンス ファイルをサポートします。プライマリおよびセカンダリ管理ノードの UDI を含む新しいライセンスを要求できます。 詳細については、『*Cisco Identity Services Engine Hardware Installation Guide*』を参照してください。

（注） 以前のリリースの場合とは異なり、Cisco ISE、リリース 1.2 にアップグレードするときに、展開からノードを登録解除して、新しい展開に登録する必要はありません。 CLI から **application upgrade** コマンドを実行すると、アップグレード ソフトウェアがノードを登録解除し、新しい展開に自動的に登録されます。

アップグレードは、セカンダリ管理ノードのアップグレードを開始した後で古い展開のノードのペルソナの設定を変更すると失敗します。

最初にセカンダリ管理ノードをアップグレードします。 次に、プライマ監視ノードをアップグレードし、続いてポリシー サービス ノードとインライン ポスチャ ノードをそれぞれ個別にアップグレードします。 次に、セカンダリ監視ノードをアップグレードします（古い展開に存在する

場合）。 最後に、古い展開からプライマリ管理ノードをアップグレードします。 ポリシー サービス ノードでは、データベース スキーマはアップグレードされません。その代わりに、ポリシー サービス ノードは、新規の展開のプライマリ管理ノードから新しいデータベースのコピーを取得します。

Cisco ISE 1.2 でサポートされるアップグレード パス

次のリリースはすべて、Cisco ISE、リリース 1.2 にアップグレードできます。

- Cisco ISE、リリース 1.1.0.665（または最新のパッチを適用した 1.1.0）
- Cisco ISE、リリース 1.1.1.268（または最新のパッチを適用した 1.1.1）
- Cisco ISE、リリース 1.1.2（最新のパッチを適用）
- Cisco ISE、リリース 1.1.3（最新のパッチを適用）
- Cisco ISE、リリース 1.1.4（最新のパッチを適用）

次の表に、Cisco ISE バージョンと、そのバージョンから Cisco ISE、リリース 1.2 にアップグレードするために必要な作業を示します。

表 *3*：アップグレードのロードマップ

アップグレード前のバージョン	アップグレード パス
Cisco ISE、リリース 1.0 または 1.0.*x*	**1** Cisco ISE、リリース 1.1.0 にアップグレードします。 **2** Cisco ISE、リリース 1.1.0 の最新のパッチを適用します。 **3** Cisco ISE、リリース 1.2 にアップグレードします。
Cisco ISE リリース 1.1	**1** Cisco ISE、リリース 1.1.0 の最新のパッチを適用します。 **2** Cisco ISE、リリース 1.2 にアップグレードします。
Cisco ISE、リリース 1.1.*x*	**1** Cisco ISE、リリース 1.1.*x* の最新のパッチを適用します。 **2** Cisco ISE、リリース 1.2 にアップグレードします。

アップグレード ソフトウェアのダウンロード

Cisco.com からアップグレード バンドル（**ise-upgradebundle-*x.x.x.x*.i386.tar.gz**）をダウンロードするには、次のことを行います。

手順

	コマンドまたはアクション	目的
ステップ 1	http://www.cisco.com/go/swonly にアクセスします。 このリンクにアクセスするには、有効な Cisco.com ログイン クレデンシャルが事前に必要です。	
ステップ 2	[ソフトウェア ダウンロード（Download Software for this Product）] をクリックします。	
ステップ 3	アップグレード バンドルをダウンロードします。	リリース 1.1.*x* からリリース 1.2 にアップグレードするには、**ise-upgradebundle-1.1.x-to-1.2.0.899.i386.tar.gz** をダウンロードします。 可用性の制限されたリリースからリリース 1.2 にアップグレードするには、**ise-upgradebundle-1.2.0.899.x86_64.tar.gz** をダウンロードします

次の作業

展開内にインライン ポスチャ ノードがある場合は、ISE-IPN 1.2 ISO イメージもダウンロードします。

リリース 1.2 にアップグレードするための CLI コマンド

Cisco ISE CLI から直接アップグレードできます。 このオプションによりアプライアンスの新しい Cisco ISE ソフトウェアをインストールし、同時に情報データベースの設定とモニタリングをアップグレードできます。

application upgrade コマンドを使用するには、Cisco ISE CLI から次を入力します。

application upgrade *application-bundle repository-name*

- *application-bundle* は Cisco ISE アプリケーションをアップグレードするためのアプリケーション バンドルの名前です。
- *repository-name* はリポジトリの名前です。

以前のバージョンの Cisco ISE からリリース 1.2 に Cisco ISE モニタリング ノードがアップグレードまたは復元されると、アクティブ セッションは保持されず、0 にリセットされます。

関連トピック

2 ノード展開の Cisco ISE、リリース 1.2 へのアップグレード, （23 ページ）
アップグレード時のデータ損失を防ぐためのバックアップの実行

さまざまな展開タイプのアップグレード方法

アップグレードを続ける前に、次の展開のタイプに応じて、アップグレードの実行方法の詳細を確認するために、このマニュアルの以降の章をお読みになることをお勧めします。

- スタンドアロンおよび 2 ノードの展開
- 分散型展開

関連トピック

2 ノード展開の Cisco ISE、リリース 1.2 へのアップグレード, （23 ページ）
分散展開のノードのアップグレード, （26 ページ）

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。

- ade.log ファイルでアップグレード プロセスを確認します。 ade.log ファイルを表示するには、Cisco ISE CLI から次のコマンドを入力します。**show logging system ade/ADE.log**
- **show version** コマンドを実行し、ビルド バージョンを検証します。
- すべてのサービスが実行していることを確認するために、**show application status ise** コマンドを入力します。

コンフィギュレーション データベースの問題でアップグレードが失敗すると、変更は自動的にロールバックされます。 詳細については、第 4 章「Cisco ISE アップグレードの障害からの復旧」の章を参照してください。

アップグレード後の作業

次のタスクの詳細については、『Cisco *Identity Services Engine User Guide, Release* 1.2』を参照してください。

- ローカルおよび認証局の証明書（CA）が使用できるかどうかを確認します。 これらは、必要に応じて再インポートします。

- バックアップ スケジュールを再設定します（設定および動作）。 古い展開で設定されたスケジュール バックアップはアップグレード中に失われます。
- Active Directory への外部アイデンティティ ソースと接続が失われたときに Active Directory を使用する場合は、Active Directory と Cisco ISE を再度結合します。
- 外部アイデンティティ ソースとして RSA SecurID サーバを使用する場合は、RSA のノード秘密をリセットします。
- ポスチャ サービスをイネーブルにした場合は、アップグレード後にプライマリ管理ノードからポスチャの更新を実行します。
- カスタム プロファイラのポリシーを調べ、インポートします。 デフォルトのプロファイラのポリシーを変更した場合は、アップグレード プロセスで変更が上書きされます。
- プローブ設定のプロファイルを検査し、必要に応じて再設定します。
- アップグレード後のデフォルト言語テンプレートのカスタマイズ。 古い展開のデフォルト言語テンプレートをカスタマイズした場合は、アップグレードプロセスで変更が上書きされます。
- プロファイラの SNMP ポーリングを再設定します。 この設定は、アップグレード中に失われます。
- Cisco ISE の以前のリリースでは、ゲスト ユーザ レコードは内部ユーザ データベースで利用可能でした。 Cisco ISE、リリース 1.2 では、内部ユーザ データベースとは異なるゲスト ユーザ データベースが導入されています。 アイデンティティ ソースのシーケンスに内部ユーザ データベースを追加した場合は、ゲスト ユーザ データベースがアイデンティティ ソースのシーケンスの一部になります。 ゲスト ユーザ ログインを使用しない場合は、アイデンティティ ソースのシーケンスからゲスト ユーザ データベースを削除します。
- 電子メール設定、お気に入りレポート、データ削除設定を再設定します。
- 必要とする特定のアラームのしきい値またはフィルタを確認します。 すべてのアラームは、アップグレード後にデフォルトでイネーブルになります。
- 必要に応じてレポートをカスタマイズします。 古い展開でレポートをカスタマイズした場合は、アップグレード プロセスでは、加えた変更が上書きされます。
- 運用（モニタリング、トラブルシューティング）データの削除は、Cisco ISE、リリース 1.2 で変更されました。 削除設定のデフォルトは 90 日です。 ログの一部は、新規導入へのアップグレード後、24 時間以内に削除されます。 過去 24 時間のデータを表示しているかどうかダッシュボードを確認します。 また、レポートおよびライブ ログも検査できます。 必要とするすべてのモニタリング（運用）データのバックアップが行われていることを確認します。

アップグレードに関する既知の問題

ここでは、既知のアップグレードの問題とその回避策をいくつか示します。 詳細については、『*Release Notes for Cisco Identity Services Engine, Release 1.2*』の「Open Caveats」セクションを参照してください。

可用性の制限されたリリースからリリース 1.2 にセカンダリ ノードをアップグレードするときに失敗する

問題 この問題は、可用性の制限されたリリースから Cisco ISE、リリース 1.2 にセカンダリ ノードをアップグレードする場合に発生します。

考えられる原因 この問題は、Cisco ISE でバックアップ スケジュールが設定されている場合に確認されます。

解決法 リリース 1.2 にアップグレードする前に、バックアップ スケジュールをディセーブルにするか、またはキャンセルします。

スケジュールされたバックアップの設定が失われる

問題 この問題は、以前のリリースからリリース 1.2 にアップグレードした後に発生します。 アップグレードの前に設定データをバック アップしており、Cisco ISE、リリース 1.2 で復元しても、スケジュール バック アップの設定は失われます。

解決法 Cisco ISE、リリース 1.2 のスケジュール バックアップを再設定します。

ブラウザのキャッシュの問題

問題 この問題は、アップグレードの前後で Cisco ISE へのアクセスに同じブラウザを使用すると発生します。

解決法 アップグレード後に Cisco ISE、リリース 1.2 にアクセスするには、ブラウザ キャッシュをクリアする必要があります。

Active Directory の参加の問題

問題 外部 ID ストアとして Active Directory を使用している場合、リリース 1.2 にアップグレード後、Cisco ISE は Active Directory ドメインに参加しなくなります。

解決法 Cisco ISE ユーザ インターフェイスの [Active Directory] ページから Active Directory ドメインにノードを再度参加させる必要があります。

RSA の接続が失われる

問題 外部アイデンティティ ソースとして RSA SecurID サーバを使用する場合、RSA SecurID サーバ接続は、アップグレード後に失われる可能性があります。

解決法 プライマリ管理ノードから RSA ノードの秘密をリセットします。 詳細については、『*Cisco Identity Services Engine User Guide, Release 1.2*』を参照してください。

アップグレード中に古い展開に追加された新しいユーザまたはエンドポイントが失われる

問題 新しい展開の形成時に古い展開に追加されたエンドポイントまたはゲスト ユーザが失われます。

解決法 アップグレード前に、ゲスト、プロファイラ、オンボードデバイスなどのサービスをディセーブルにし、アップグレード後にこれらをイネーブルにします。 そうしない場合、失われたゲスト ユーザを追加し、デバイスのプロファイルとオンボードを再度行う必要があります。

プロファイラの SNMP ポーリングの設定が失われる

問題 プロファイラの SNMP ポーリングの設定は、アップグレード後に失われます。

解決法 アップグレード後に Cisco ISE、リリース 1.2 プライマリ管理ノードからプロファイラの SNMP ポーリングを再構成します。 詳細については、『*Cisco Identity Services Engine User Guide, Release 1.2*』を参照してください。

デフォルトの言語テンプレートのカスタマイズが失われる

問題 デフォルトの言語テンプレートを編集した場合でも、行った変更は、アップグレード後に失われます。

解決法 アップグレード後、デフォルトの言語テンプレートを再度カスタマイズします。

CLI パスワード ポリシーがアップグレード中に失われる

問題 この問題は、Cisco ISE、リリース 1.2 にアップグレードすると発生します。

考えられる原因 Cisco ISE、リリース 1.2 では、GUI および CLI パスワード ポリシーはすべてのノードに統合され、複製されます。

解決法 リリース 1.2 にアップグレード後、Cisco ISE Admin Portal（[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [パスワード ポリシー（Password Policy）]）からパスワード ポリシーを設定します。

ポスチャの更新が上書きされる

問題 アップグレード中、ポスチャ規則に影響を及ぼす可能性があるポスチャのオペレーティング システムのリストが更新されます。

解決法 アップグレード後、プライマリ管理ユーザ インターフェイスから、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）] を選択します。 Cisco がサポートする OS バージョンを確認します。 これが 0.0.0.0 に設定されている場合、ポスチャの更新を実行します。

アップグレード実行中のマニフェスト エラー

問題 Cisco.com から Apple Safari などの Web ブラウザを使用してダウンロードしたアプリケーション バンドルを使用して ISE をアップグレードしようとすると、「マニフェスト エラー」が表示されることがあります。

考えられる原因 アップグレード ファイルは、ダウンロード後に圧縮解除されます。 デフォルトでは、Apple Safari Web ブラウザで、ダウンロード後に「安全な」ファイルが開きます。 この設定により、ダウンロード後にアップグレード バンドルが圧縮解除され、アップグレード中にマニフェスト エラーが発生します。

解決法 Apple Safari Web ブラウザの [環境設定（Preferences）] の下にある [ダウンロード後、安全なファイルを開く（open safe files after downloading）] オプションをオフにします。

第 2 章

スタンドアロンおよび2ノード展開の Cisco ISE、リリース 1.2 へのアップグレード

アップグレード ソフトウェアでは、Command-Line Interface (CLI) からリリース 1.2 にアップグレードすることができます。

Cisco ISE スタンドアロン ノードのリリース 1.2 へのアップグレード

Administration、Policy Service、Monitoring のペルソナを担当するスタンドアロン ノードの CLI から **application upgrade** コマンドを実行できます。

はじめる前に

- スタンドアロン ノードからコンフィギュレーション データのオンデマンド バックアップを実行します。
- 管理ユーザ インタフェースを使用して、スタンドアロン ノードからモニタリング データのオンデマンド バックアップを実行します。

手順

Cisco ISE CLI から **application upgrade** コマンドを入力します。

このコマンドは、アプリケーション バイナリ、データベース スキーマ、データモデル モジュールを内部でアップグレードします。 また、Cisco Application Deployment Engine オペレーティング システム（ADE-OS）のアップグレードを処理します。

アップグレード プロセスを完了するためにシステムのリロードが必要な場合、アップグレードの成功後にノードは自動的に再起動します。

アップグレードが完了した後、Cisco ISE ノードに古いモニタリング ログが含まれる場合、**application configure ise**コマンドを実行し、11（M&T データベースの統計情報の更新）を選択します。

スタンドアロン ノードでアップグレードを成功させるための CLI トランスクリプトは次のとおりです。

```
ise-vm29/admin# application upgrade ise-upgradebundle-1.1.x-to-1.2.0.899.i386.tar.gz myrepository
Save the current ADE-OS running configuration? (yes/no) [yes] ?
 ################################################################
                    Upgrading ISE to 1.2.0.899
 ################################################################
yes
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
STEP 1: Stopping ISE application...
STEP 2: Taking backup of the configuration data...
STEP 3: Running ISE configuration DB schema upgrade...

ISE Database schema upgrade completed.
STEP 4: Running ISE configuration data upgrade...
- Data upgrade step 1/79, ConfiguratorUpgradeService(1.2.0.155)... Done in 2 seconds.
- Data upgrade step 2/79, NSFUpgradeService(1.2.0.180)... Done in 0 seconds.
- Data upgrade step 3/79, GuestUpgradeService(1.2.0.195)... Done in 1 seconds.
- Data upgrade step 4/79, ProfilerUpgradeService(1.2.0.196)... Done in 9 seconds.
- Data upgrade step 5/79, SystemConfigUpgradeService(1.2.0.201)... Done in 0 seconds.
- Data upgrade step 6/79, NSFUpgradeService(1.2.0.217)... Done in 0 seconds.
- Data upgrade step 7/79, NSFUpgradeService(1.2.0.224)... Done in 3 seconds.
- Data upgrade step 8/79, GuestUpgradeService(1.2.0.225)... Done in 0 seconds.
- Data upgrade step 9/79, NSFUpgradeService(1.2.0.229)... Done in 0 seconds.
- Data upgrade step 10/79, ProfilerUpgradeService(1.2.0.256)... Done in 0 seconds.
- Data upgrade step 11/79, RBACUpgradeService(1.2.0.257)... Done in 34 seconds.
- Data upgrade step 12/79, ProfilerUpgradeService(1.2.0.257)...
.............................Done in 1764 seconds.
- Data upgrade step 13/79, GuestUpgradeService(1.2.0.263)... Done in 2 seconds.
- Data upgrade step 14/79, ProfilerUpgradeService(1.2.0.265)... Done in 0 seconds.
- Data upgrade step 15/79, GuestUpgradeService(1.2.0.268)... Done in 0 seconds.
- Data upgrade step 16/79, NSFUpgradeService(1.2.0.270)... Done in 0 seconds.
- Data upgrade step 17/79, DictionaryUpgradeRegistration(1.2.0.272)... Done in 26 seconds.
- Data upgrade step 18/79, GuestUpgradeService(1.2.0.276)... Done in 0 seconds.
- Data upgrade step 19/79, NSFUpgradeService(1.2.0.281)... Done in 1 seconds.
- Data upgrade step 20/79, GuestUpgradeService(1.2.0.290)... Done in 1 seconds.
- Data upgrade step 21/79, NSFUpgradeService(1.2.0.291)... Done in 2 seconds.
- Data upgrade step 22/79, NSFUpgradeService(1.2.0.298)... Done in 0 seconds.
- Data upgrade step 23/79, PolicySetUpgradeService(1.2.0.310)... Done in 4 seconds.
- Data upgrade step 24/79, GuestUpgradeService(1.2.0.311)... Done in 0 seconds.
- Data upgrade step 25/79, GlobalExceptionUpgradeRegistration(1.2.0.311)... Done in 1
seconds.
- Data upgrade step 26/79, GuestUpgradeService(1.2.0.319)... Done in 0 seconds.
- Data upgrade step 27/79, ProfilerUpgradeService(1.2.0.319)... Done in 1 seconds.
- Data upgrade step 28/79, NetworkAccessUpgrade(1.2.0.326)... Done in 0 seconds.
- Data upgrade step 29/79, GuestUpgradeService(1.2.0.341)... Done in 2 seconds.
- Data upgrade step 30/79, NSFUpgradeService(1.2.0.344)... Done in 0 seconds.
- Data upgrade step 31/79, RBACUpgradeService(1.2.0.344)... .Done in 77 seconds.
- Data upgrade step 32/79, NSFUpgradeService(1.2.0.349)... Done in 0 seconds.
- Data upgrade step 33/79, AuthzUpgradeService(1.2.0.351)... Done in 0 seconds.
- Data upgrade step 34/79, RegisterPostureTypes(1.2.0.363)... ..............Done in 903
seconds.
```

```
- Data upgrade step 35/79, NSFUpgradeService(1.2.0.366)... Done in 2 seconds.
- Data upgrade step 36/79, NetworkAccessUpgrade(1.2.0.366)... Done in 11 seconds.
- Data upgrade step 37/79, GuestUpgradeService(1.2.0.370)... Done in 1 seconds.
- Data upgrade step 38/79, NSFUpgradeService(1.2.0.379)... Done in 0 seconds.
- Data upgrade step 39/79, AuthzUpgradeService(1.2.0.391)... Done in 0 seconds.
- Data upgrade step 40/79, GuestUpgradeService(1.2.0.400)... Done in 0 seconds.
- Data upgrade step 41/79, NSFUpgradeService(1.2.0.420)... Done in 0 seconds.
- Data upgrade step 42/79, NSFUpgradeService(1.2.0.430)... Done in 0 seconds.
- Data upgrade step 43/79, RBACUpgradeService(1.2.0.445)... .Done in 62 seconds.
- Data upgrade step 44/79, GuestUpgradeService(1.2.0.478)... Done in 0 seconds.
- Data upgrade step 45/79, RBACUpgradeService(1.2.0.481)... Done in 3 seconds.
- Data upgrade step 46/79, CertMgmtUpgradeService(1.2.0.485)... Done in 2 seconds.
- Data upgrade step 47/79, ProfilerUpgradeService(1.2.0.495)... Done in 0 seconds.
- Data upgrade step 48/79, RBACUpgradeService(1.2.0.496)... Done in 21 seconds.
- Data upgrade step 49/79, NSFUpgradeService(1.2.0.500)... Done in 0 seconds.
- Data upgrade step 50/79, NetworkAccessUpgrade(1.2.0.585)... Done in 4 seconds.
- Data upgrade step 51/79, GuestUpgradeService(1.2.0.618)... Done in 1 seconds.
- Data upgrade step 52/79, NetworkAccessUpgrade(1.2.0.621)... Done in 2 seconds.
- Data upgrade step 53/79, NSFUpgradeService(1.2.0.624)... Done in 5 seconds.
- Data upgrade step 54/79, NetworkAccessUpgrade(1.2.0.625)... Done in 0 seconds.
- Data upgrade step 55/79, VendorUpgradeRegistration(1.2.0.638)... Done in 0 seconds.
- Data upgrade step 56/79, CertMgmtUpgradeService(1.2.0.665)... Done in 2 seconds.
- Data upgrade step 57/79, ProfilerUpgradeService(1.2.0.700)... Done in 0 seconds.
- Data upgrade step 58/79, RegisterPostureTypes(1.2.0.706)... Done in 1 seconds.
- Data upgrade step 59/79, NetworkAccessUpgrade(1.2.0.708)... Done in 0 seconds.
- Data upgrade step 60/79, GuestUpgradeService(1.2.0.716)... Done in 1 seconds.
- Data upgrade step 61/79, NetworkAccessUpgrade(1.2.0.716)... Done in 0 seconds.
- Data upgrade step 62/79, RegisterPostureTypes(1.2.0.728)... Done in 1 seconds.
- Data upgrade step 63/79, NSFUpgradeService(1.2.0.729)... Done in 0 seconds.
- Data upgrade step 64/79, AuthzUpgradeService(1.2.0.729)... Done in 3 seconds.
- Data upgrade step 65/79, GuestUpgradeService(1.2.0.737)... Done in 0 seconds.
- Data upgrade step 66/79, NetworkAccessUpgrade(1.2.0.738)... Done in 0 seconds.
- Data upgrade step 67/79, GuestUpgradeService(1.2.0.747)... Done in 13 seconds.
- Data upgrade step 68/79, NSFUpgradeService(1.2.0.754)... Done in 1 seconds.
- Data upgrade step 69/79, RBACUpgradeService(1.2.0.757)... .Done in 83 seconds.
- Data upgrade step 70/79, NetworkAccessUpgrade(1.2.0.762)... Done in 0 seconds.
- Data upgrade step 71/79, NetworkAccessUpgrade(1.2.0.764)... Done in 0 seconds.
- Data upgrade step 72/79, NetworkAccessUpgrade(1.2.0.774)... Done in 0 seconds.
- Data upgrade step 73/79, NSFUpgradeService(1.2.0.775)... Done in 0 seconds.
- Data upgrade step 74/79, NSFUpgradeService(1.2.0.826)... Done in 0 seconds.
- Data upgrade step 75/79, GuestUpgradeService(1.2.0.852)... .......Done in 435 seconds.
- Data upgrade step 76/79, ProfilerUpgradeService(1.2.0.866)... Done in 0 seconds.
- Data upgrade step 77/79, CertMgmtUpgradeService(1.2.0.873)... Done in 0 seconds.
- Data upgrade step 78/79, NSFUpgradeService(1.2.0.881)... Done in 0 seconds.
- Data upgrade step 79/79, GuestUpgradeService(1.2.0.882)... Done in 2 seconds.
STEP 5: Running ISE configuration data upgrade for node specific data...
STEP 6: Running ISE MnT DB upgrade...
Upgrading Session Directory...
Completed.
- Mnt Schema Upgrade completed, executing sanity check...
 % Mnt Db Schema Sanity success
Generating Database statistics for optimization ....
- Preparing database for 64 bit migration...
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS to 64 bit. During
 this time progress of the upgrade is visible on console. It could take up to 30 minutes
for this to complete.
Rebooting to do Identity Service Engine upgrade...
```

次の作業

- Cisco ISE、リリース 1.1.1 パッチ 3 または Cisco ISE メンテナンス リリース 1.1.2 を Cisco ISE リリース 1.2 にアップグレードすると、**crypto host_key add host** *sftp-server-name* コマンドを使用してホスト キーを承認するまで SFTP リポジトリを使用できない場合があります。
- Cisco ISE、リリース 1.2 にアップグレードした後、古いジョブが正しく機能しないため、すべてのバックアップ スケジュールを再作成します。

- アプリケーション バイナリと Cisco ADE-OS のアップグレード中に障害が発生した場合、前バージョンのイメージの再作成とインストールを行い、バックアップを復元する必要があります。

関連トピック

『Cisco Identity Services Engine CLI Reference Guide, Release 1.2』

以前のバージョンのスタンドアロンアプライアンスとリリース 1.2 を実行するアプライアンスを交換する

このアップグレードのシナリオは、既存の Cisco ISE アプライアンスを交換するのと同時に、Cisco ISE、リリース 1.1.*x* をリリース 1.2 にアップグレードする場合にのみ必要です。

はじめる前に

古い展開のプライマリ管理ノードから、Cisco ISE 1.1.*x*、設定データとモニタリング データのバックアップを実行します。 新しい SNS-3400 シリーズ アプライアンスの Unique Device Identifier (UDI) に基づいてライセンスを取得します。

（注） アップグレードせずに、Cisco ISE、リリース 1.2 を新規インストールする場合、新しいアプライアンスをインストールおよびセットアップした後、データを復元するか、手動で設定します。

手順

ステップ 1 新しい Cisco ISE、リリース 1.2 アプライアンスをセットアップします。 詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』を参照してください。

ステップ 2 Cisco ISE、リリース 1.2 アプライアンスに新しいライセンスをインストールします。

ステップ 3 Cisco ISE CLI により、作成したバックアップから設定データおよびモニタリング データをリストアします。
データの復元後、すべてのアプリケーション サーバ プロセスが起動および実行するまで待ちます。

ステップ 4 Cisco ISE アプリケーション サーバ プロセスの起動を確認するには、Cisco ISE CLI から次のコマンドを入力します。
show application status ise

関連トピック

『Cisco Identity Services Engine User Guide, Release 1.2』

『Cisco Identity Services Engine CLI Reference Guide, Release 1.2』
『Cisco Identity Services Engine Hardware Installation Guide, Release 1.2』

2 ノード展開の Cisco ISE、リリース 1.2 へのアップグレード

application upgrade コマンドを使用して、リリース 1.2 に 2 ノードの展開をアップグレードします。 手動でノードの登録を解除して、再登録する必要はありません。 アップグレード ソフトウェアは自動的にノードを登録解除し、新しい展開に移行します。 Cisco ISE、リリース 1.2 に 2 ノードの展開をアップグレードすると、最初にセカンダリ管理ノード（ノードB）のみをアップグレードする必要があります。 セカンダリ ノードのアップグレードを完了したら、プライマリ ノード（ノード A）をアップグレードします。 次の図に示すような展開の設定の場合、このアップグレード手順を続けることができます。

図 *1*：*Cisco ISE* リリース *1.1.x* ノード管理展開

はじめる前に

- プライマリ管理ノードから設定および運用データのオンデマンドバックアップを手動で実行します。
- 管理ペルソナがプライマリ管理ノードでのみイネーブルである場合、アップグレードプロセスによりセカンダリ ノードを最初にアップグレードすることが求められるので、アップグレード手順を開始する前にセカンダリ管理ノードの管理ペルソナをイネーブルにします。
- 2 ノード構成で 1 つの管理ノードのみがある場合は、セカンダリ ノードの登録を解除します。 両方のノードがスタンドアロン ノードになります。 両方のノードをスタンドアロン ノードとしてアップグレードし、リリース 1.2 へのアップグレード後に、展開をセット アップします。
- モニタリング ペルソナが 1 つのノードのみでイネーブルの場合、次に進む前に他のノードのモニタリング ペルソナをイネーブルにします。

手順

ステップ 1 CLI から、セカンダリ ノード（ノード B）を Cisco ISE、リリース 1.2 にアップグレードします。
アップグレードプロセスでは、展開からのノードBの除外、そしてリリース1.2へのアップグレードが自動的に行われます。 再起動すると、ノード B はプライマリ ノードになります。

ステップ 2 ノード A をリリース 1.2 にアップグレードします。
アップグレード プロセスで、自動的にノード A が展開に登録され、セカンダリ ノードになります。

ステップ 3 新規の展開で、ノード A をプライマリ ノードに昇格させます。
プライマリ ノードとしてノードB を保持する場合、プライマリ管理ノードとセカンダリ管理ノードの両 UDI を含むライセンスを取得します。 ライセンスを取得する方法については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』を参照してください。

アップグレードが完了した後、リリース 1.2 にアップグレードされたノードに古いモニタリング ログが含まれる場合、**application configure ise** コマンドを実行し、該当するノードで 11（M&T データベースの統計情報の更新）を選択します。

関連トピック

さまざまな展開タイプのアップグレード方法, （14 ページ）
リリース 1.2 にアップグレードするための CLI コマンド, （13 ページ）
『Cisco Identity Services Engine User Guide, Release 1.2』

第 3 章

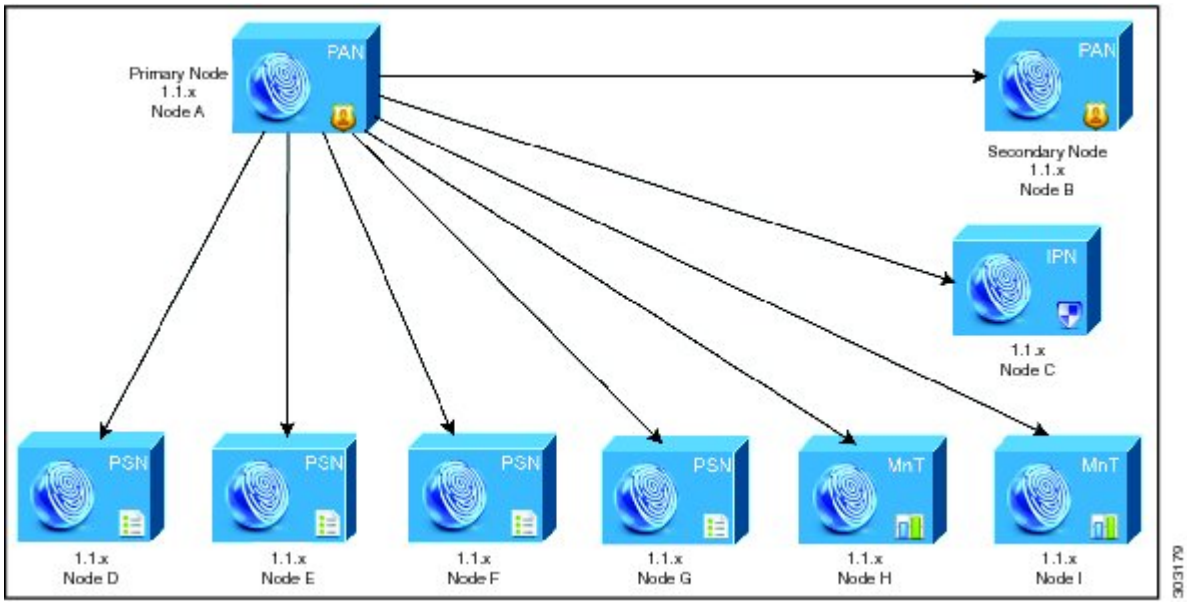
分散展開の Cisco ISE、リリース 1.2 へのアップグレード

この章では、分散展開を Cisco ISE リリース 1.2 にアップグレードする方法について説明します。

分散展開のアップグレード

次の図に示すように、一般的な Cisco ISE 分散展開は、プライマリおよびセカンダリの管理ノードとモニタリング ノード、いくつかのポリシー サービス ノード、IPN ノードから構成されます。

図 *2*：*Cisco ISE* リリース *1.1.x* 管理展開



上の図に示した分散展開をアップグレードするには、次の手順に従います。

分散展開のノードのアップグレード

Cisco ISE、リリース 1.2 へのアップグレード時には、最初にセカンダリ管理ノードをリリース 1.2 にアップグレードします。 たとえば、図 2 に示すように、1 つのプライマリ管理ノード（ノード A）、1 つのセカンダリ管理ノード（ノード B）、1 つのインライン ポスチャ ノード（IPN）（ノード C）、および 4 つのポリシー サービス ノード（PSN）（ノード D、ノード E、ノード F、およびノード G）、1 つのプライマリ モニタリング ノード（ノード H）、および 1 つのセカンダリ モニタリング ノード（ノード I）を含む展開がセットアップされている場合、次のアップグレード手順に進むことができます。

（注） アップグレードの前にノードを手動で登録解除する必要はありません。 **application upgrade** コマンドを使用してノードをリリース 1.2 にアップグレードします。 アップグレード プロセスは自動的にノードを登録解除し、新しい展開に移行します。アップグレードの前に手動でノードの登録をキャンセルする場合は、アップグレードプロセスを開始する前に、プライマリ ノード管理用のライセンス ファイルがあることを確認します。 手元にこのファイルがない場合（たとえば、シスコ パートナー ベンダーによってライセンスはインストールされていない場合）、Cisco TAC に連絡してください。

はじめる前に

- 展開にセカンダリ管理ノードがない場合は、アップグレードプロセスを開始する前に、セカンダリ管理ノードにするポリシー サービス ノードを 1 つ設定します。
- プライマリ管理ノードから設定およびADE-OSデータのオンデマンドバックアップを手動で実行します。
- モニタリング データのオンデマンド バックアップを実行します。
- アップグレード前に IPN 設定を記録し、アップグレード後に IPN を再設定できるようにします。（このために、手動で設定の詳細を確認することや、IPNユーザインターフェイスから既存のコンフィギュレーションのスクリーン ショットを取得できます）。
- 全 Cisco ISE 展開をアップグレードする場合は、ドメイン ネーム システム（DNS）のサーバ解決（順ルックアップおよび逆ルックアップ）が必須です。そうでない場合、アップグレードは失敗します。

手順

ステップ 1 CLI からセカンダリ管理ノード（ノード B）をアップグレードします。
アップグレード プロセスでは、展開からのノード B の登録解除、そしてリリース 1.2 へのアップグレードが自動的に行われます。 再起動すると、ノードBは、新規のプライマリ ノードになります。 各展開でモニタリング ノードが少なくとも 1 つ必要になるため、アップグレード プロセスは古い展開の該当ノードでイネーブルになっていなくても、ノードBのモニタリング ペルソナをイネーブルにします。 ポリシー サービス ペルソナが古い展開のノード B でイネーブルであった場合、この設定は新規導入へのアップグレード後も維持されます。

ステップ 2 モニタリング ノードの 1 つ（ノード H）を新規展開にアップグレードします。
セカンダリ モニタリング ノードの前にプライマリ モニタリング ノードをアップグレードすることをお勧めします（古い展開でプライマリ管理ノードがプライマリモニタリングノードとしても動作している場合にはこれは不可能です）。 プライマリ モニタリング ノードが起動し、新規展開からログを収集します。この詳細は、プライマリ管理ノードのダッシュボードから表示できます。

古い展開でモニタリング ノードが 1 つだけある場合は、アップグレードする前に、古い展開のプライマリ管理ノードであるノード A のモニタリング ペルソナをイネーブルにします。 ノード ペルソナの変更により、Cisco ISE アプリケーションが再起動します。 ノード A が再起動するまで

待ちます。新規展開にモニタリング ノードをアップグレードすると、運用データを新しい展開に移行する必要があるために、他のノードよりも時間がかかります。

新規展開のプライマリ管理ノードであるノード B が、古い展開でイネーブルにされたモニタリング ペルソナを持たない場合、モニタリング ペルソナをディセーブルにします。 ノード ペルソナの変更により、Cisco ISE アプリケーションが再起動します。プライマリ管理ノードが起動するまで待ちます。

ステップ 3 CLI から、ポリシー サービス ノード（ノード D、E、F、および G）を Cisco ISE、リリース 1.2 にアップグレードします。 複数の PSN ノードを同時にアップグレードできますが、すべての PSN を同時にアップグレードした場合、ネットワークでダウン タイムが発生します。
アップグレード後に、新規展開のプライマリ ノード（ノード B）に PSN が登録され、プライマリ ノード（ノード B）からのデータがすべての PSN に複製されます。 PSN ではそのペルソナ、ノード グループ情報、およびプローブのプロファイリング設定が維持されます。

ステップ 4 プライマリ管理ノードから IPN ノード（ノード C）を登録解除します。

ステップ 5 IPN アプライアンス（ノード C）のイメージを再作成します。

ステップ 6 イメージが再作成された IPN ノード（ノード C）で IPN ISO 1.2 をインストールします。

ステップ 7 IPN ノード（ノード C）を新規展開のプライマリ管理ノード（ノード B）に登録します。

ステップ 8 古い展開に 2 番目のモニタリング ノード（ノード I）がある場合、次のことを行う必要があります。

a) 古い展開のプライマリ ノードであるノード A のモニタリング ペルソナをイネーブルにします。展開でモニタリング ノードは少なくとも 1 つ必要です。古い展開から第 2 のモニタリング ノードをアップグレードする前に、プライマリ ノード自身でこのペルソナをイネーブルにします。ノード ペルソナの変更により、Cisco ISE アプリケーションが再起動します。 プライマリ ISE ノードが再起動するまで待ちます。

b) セカンダリ モニタリング ノード（ノード I）を古い展開からの新しい展開にアップグレードします。

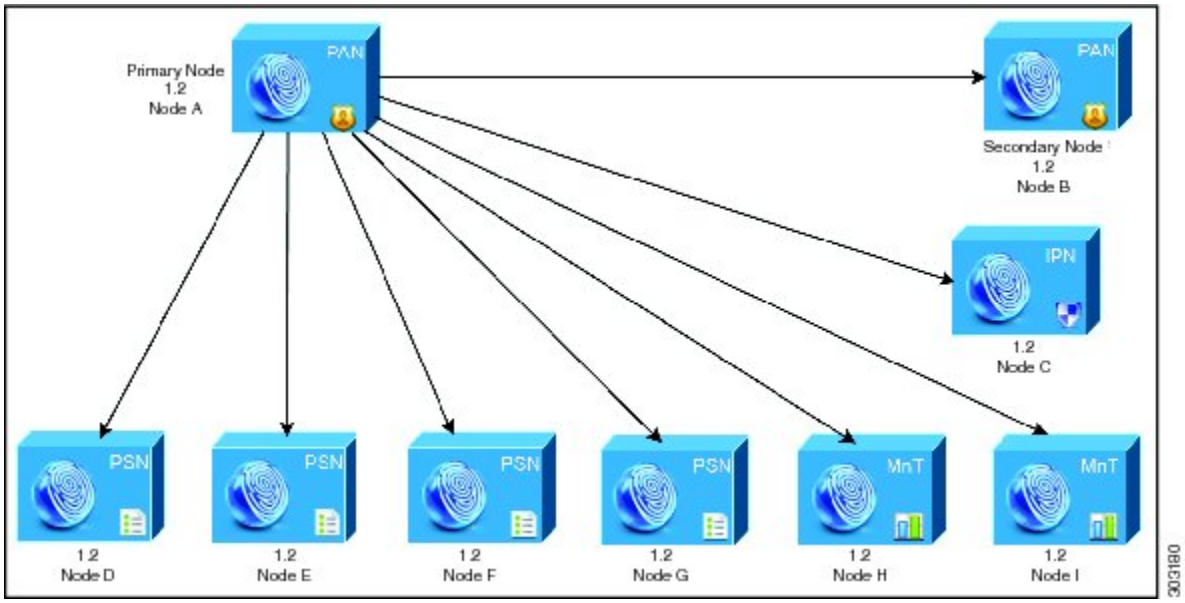
プライマリ管理ノード（ノード A）を除いて、他のすべてのノードについては新規展開にアップグレードする必要はありません。

ステップ 9 最後に、プライマリ管理ノード（ノード A）を Cisco ISE、リリース 1.2 にアップグレードします。このノードは、リリース 1.2 にアップグレードされ、新しい展開にセカンダリ管理ノードとして追加されます。セカンダリ管理ノード（ノード A）を新規展開のプライマリ ノードに昇格させることができます。プライマリ ノードとしてノード B を保持する場合、プライマリ管理ノードとセカンダリ管理ノードの両 UDI を含むライセンスを取得します。

アップグレードが完了した後、リリース 1.2 にアップグレードされたモニタリング ノードに古いログが含まれる場合、**application configure ise** コマンドを実行し、該当するモニタリング ノードで 11（M&T データベースの統計情報の更新）を選択します。

アップグレード後、新規展開は次の図のようになります。

図 *3*：リリース *1.2* にアップグレードされた完全な展開



CLI トランスクリプトの正常なアップグレード

次の例は、正常なセカンダリ管理ノードのアップグレードの CLI トランスクリプトです。

```
ise-vm30/admin# application upgrade ise-upgradebundle-1.1.x-to-1.2.0.899.i386.tar.gz myrepository
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
STEP 1: Stopping ISE application...
STEP 2: De-registering node from current deployment.
STEP 3: Taking backup of the configuration data...
STEP 4: Running ISE configuration DB schema upgrade...

ISE Database schema upgrade completed.
STEP 5: Running ISE configuration data upgrade...
- Data upgrade step 1/79, ConfiguratorUpgradeService(1.2.0.155)... Done in 2 seconds.
- Data upgrade step 2/79, NSFUpgradeService(1.2.0.180)... Done in 0 seconds.
- Data upgrade step 3/79, GuestUpgradeService(1.2.0.195)... Done in 1 seconds.
- Data upgrade step 4/79, ProfilerUpgradeService(1.2.0.196)... Done in 7 seconds.
- Data upgrade step 5/79, SystemConfigUpgradeService(1.2.0.201)... Done in 0 seconds.
- Data upgrade step 6/79, NSFUpgradeService(1.2.0.217)... Done in 9 seconds.
- Data upgrade step 7/79, NSFUpgradeService(1.2.0.224)... Done in 2 seconds.
- Data upgrade step 8/79, GuestUpgradeService(1.2.0.225)... Done in 0 seconds.
- Data upgrade step 9/79, NSFUpgradeService(1.2.0.229)... Done in 0 seconds.
- Data upgrade step 10/79, ProfilerUpgradeService(1.2.0.256)... Done in 0 seconds.
- Data upgrade step 11/79, RBACUpgradeService(1.2.0.257)... Done in 14 seconds.
- Data upgrade step 12/79, ProfilerUpgradeService(1.2.0.257)... ............Done in 816
seconds.
- Data upgrade step 13/79, GuestUpgradeService(1.2.0.263)... Done in 3 seconds.
- Data upgrade step 14/79, ProfilerUpgradeService(1.2.0.265)... Done in 0 seconds.
- Data upgrade step 15/79, GuestUpgradeService(1.2.0.268)... Done in 0 seconds.
- Data upgrade step 16/79, NSFUpgradeService(1.2.0.270)... Done in 0 seconds.
- Data upgrade step 17/79, DictionaryUpgradeRegistration(1.2.0.272)... Done in 26 seconds.
- Data upgrade step 18/79, GuestUpgradeService(1.2.0.276)... Done in 0 seconds.
- Data upgrade step 19/79, NSFUpgradeService(1.2.0.281)... Done in 1 seconds.
```

```
- Data upgrade step 20/79, GuestUpgradeService(1.2.0.290)... Done in 1 seconds.
- Data upgrade step 21/79, NSFUpgradeService(1.2.0.291)... Done in 1 seconds.
- Data upgrade step 22/79, NSFUpgradeService(1.2.0.298)... Done in 0 seconds.
- Data upgrade step 23/79, PolicySetUpgradeService(1.2.0.310)... Done in 3 seconds.
- Data upgrade step 24/79, GuestUpgradeService(1.2.0.311)... Done in 0 seconds.
- Data upgrade step 25/79, GlobalExceptionUpgradeRegistration(1.2.0.311)... Done in 4
seconds.
- Data upgrade step 26/79, GuestUpgradeService(1.2.0.319)... Done in 0 seconds.
- Data upgrade step 27/79, ProfilerUpgradeService(1.2.0.319)... Done in 2 seconds.
- Data upgrade step 28/79, NetworkAccessUpgrade(1.2.0.326)... Done in 0 seconds.
- Data upgrade step 29/79, GuestUpgradeService(1.2.0.341)... Done in 2 seconds.
- Data upgrade step 30/79, NSFUpgradeService(1.2.0.344)... Done in 0 seconds.
- Data upgrade step 31/79, RBACUpgradeService(1.2.0.344)... Done in 38 seconds.
- Data upgrade step 32/79, NSFUpgradeService(1.2.0.349)... Done in 0 seconds.
- Data upgrade step 33/79, AuthzUpgradeService(1.2.0.351)... Done in 0 seconds.
- Data upgrade step 34/79, RegisterPostureTypes(1.2.0.363)... ..Done in 121 seconds.
- Data upgrade step 35/79, NSFUpgradeService(1.2.0.366)... Done in 0 seconds.
- Data upgrade step 36/79, NetworkAccessUpgrade(1.2.0.366)... Done in 2 seconds.
- Data upgrade step 37/79, GuestUpgradeService(1.2.0.370)... Done in 1 seconds.
- Data upgrade step 38/79, NSFUpgradeService(1.2.0.379)... Done in 0 seconds.
- Data upgrade step 39/79, AuthzUpgradeService(1.2.0.391)... Done in 0 seconds.
- Data upgrade step 40/79, GuestUpgradeService(1.2.0.400)... Done in 0 seconds.
- Data upgrade step 41/79, NSFUpgradeService(1.2.0.420)... Done in 0 seconds.
- Data upgrade step 42/79, NSFUpgradeService(1.2.0.430)... Done in 0 seconds.
- Data upgrade step 43/79, RBACUpgradeService(1.2.0.445)... Done in 26 seconds.
- Data upgrade step 44/79, GuestUpgradeService(1.2.0.478)... Done in 0 seconds.
- Data upgrade step 45/79, RBACUpgradeService(1.2.0.481)... Done in 1 seconds.
- Data upgrade step 46/79, CertMgmtUpgradeService(1.2.0.485)... Done in 1 seconds.
- Data upgrade step 47/79, ProfilerUpgradeService(1.2.0.495)... Done in 0 seconds.
- Data upgrade step 48/79, RBACUpgradeService(1.2.0.496)... Done in 9 seconds.
- Data upgrade step 49/79, NSFUpgradeService(1.2.0.500)... Done in 0 seconds.
- Data upgrade step 50/79, NetworkAccessUpgrade(1.2.0.585)... Done in 4 seconds.
- Data upgrade step 51/79, GuestUpgradeService(1.2.0.618)... Done in 1 seconds.
- Data upgrade step 52/79, NetworkAccessUpgrade(1.2.0.621)... Done in 2 seconds.
- Data upgrade step 53/79, NSFUpgradeService(1.2.0.624)... Done in 0 seconds.
- Data upgrade step 54/79, NetworkAccessUpgrade(1.2.0.625)... Done in 0 seconds.
- Data upgrade step 55/79, VendorUpgradeRegistration(1.2.0.638)... Done in 0 seconds.
- Data upgrade step 56/79, CertMgmtUpgradeService(1.2.0.665)... Done in 1 seconds.
- Data upgrade step 57/79, ProfilerUpgradeService(1.2.0.700)... Done in 0 seconds.
- Data upgrade step 58/79, RegisterPostureTypes(1.2.0.706)... Done in 1 seconds.
- Data upgrade step 59/79, NetworkAccessUpgrade(1.2.0.708)... Done in 0 seconds.
- Data upgrade step 60/79, GuestUpgradeService(1.2.0.716)... Done in 1 seconds.
- Data upgrade step 61/79, NetworkAccessUpgrade(1.2.0.716)... Done in 1 seconds.
- Data upgrade step 62/79, RegisterPostureTypes(1.2.0.728)... Done in 1 seconds.
- Data upgrade step 63/79, NSFUpgradeService(1.2.0.729)... Done in 0 seconds.
- Data upgrade step 64/79, AuthzUpgradeService(1.2.0.729)... Done in 1 seconds.
- Data upgrade step 65/79, GuestUpgradeService(1.2.0.737)... Done in 0 seconds.
- Data upgrade step 66/79, NetworkAccessUpgrade(1.2.0.738)... Done in 0 seconds.
- Data upgrade step 67/79, GuestUpgradeService(1.2.0.747)... Done in 10 seconds.
- Data upgrade step 68/79, NSFUpgradeService(1.2.0.754)... Done in 0 seconds.
- Data upgrade step 69/79, RBACUpgradeService(1.2.0.757)... Done in 34 seconds.
- Data upgrade step 70/79, NetworkAccessUpgrade(1.2.0.762)... Done in 0 seconds.
- Data upgrade step 71/79, NetworkAccessUpgrade(1.2.0.764)... Done in 0 seconds.
- Data upgrade step 72/79, NetworkAccessUpgrade(1.2.0.774)... Done in 0 seconds.
- Data upgrade step 73/79, NSFUpgradeService(1.2.0.775)... Done in 0 seconds.
- Data upgrade step 74/79, NSFUpgradeService(1.2.0.826)... Done in 0 seconds.
- Data upgrade step 75/79, GuestUpgradeService(1.2.0.852)... .......Done in 445 seconds.
- Data upgrade step 76/79, ProfilerUpgradeService(1.2.0.866)... Done in 0 seconds.
- Data upgrade step 77/79, CertMgmtUpgradeService(1.2.0.873)... Done in 0 seconds.
- Data upgrade step 78/79, NSFUpgradeService(1.2.0.881)... Done in 0 seconds.
- Data upgrade step 79/79, GuestUpgradeService(1.2.0.882)... Done in 2 seconds.
STEP 6: Running ISE configuration data upgrade for node specific data...
 STEP 7: Making this node PRIMARY of the new deployment. When other nodes are upgraded it
will be added to this deployment.
STEP 8: Running ISE MnT DB upgrade...
Upgrading Session Directory...
Completed.
- Mnt Schema Upgrade completed, executing sanity check...
 % Mnt Db Schema Sanity success
Generating Database statistics for optimization ....
- Preparing database for 64 bit migration...
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS to 64 bit. During
 this time progress of the upgrade is visible on console. It could take up to 30 minutes
```

```
for this to complete.
Rebooting to do Identity Service Engine upgrade...
```

次の例は、正常な PSN（モニタリング）ノードのアップグレードの CLI トランスクリプトです。

```
ise-vm31/admin# application upgrade ise-upgradebundle-1.1.x-to-1.2.0.899.i386.tar.gz myrepository

Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
STEP 1: Stopping ISE application...
STEP 2: De-registering node from current deployment.
STEP 3: Taking backup of the configuration data...
STEP 4: Registering this node to primary  of new deployment...
STEP 5: Downloading configuration data from primary  of new deployment...
STEP 6: Importing configuration data...
STEP 7: Running ISE configuration data upgrade for node specific data...
STEP 8: Running ISE MnT DB upgrade...
Upgrading Session Directory...
Completed.
- Mnt Schema Upgrade completed, executing sanity check...
 % Mnt Db Schema Sanity success
Generating Database statistics for optimization ....
- Preparing database for 64 bit migration...
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS to 64 bit. During
 this time progress of the upgrade is visible on console. It could take up to 30 minutes
for this to complete.
Rebooting to do Identity Service Engine upgrade...
```

関連トピック

さまざまな展開タイプのアップグレード方法, （14 ページ）

分散展開のインライン ポスチャ ノードのアップグレード

Cisco ISE、リリース 1.2 に直接インライン ポスチャ ノードをアップグレードできません。 Cisco ISE 3300 シリーズ アプライアンスのイメージを再作成して、そこに ISE-IPN 1.2 ISO をインストールする必要があります。 このセクションでは、リリース 1.2 に IPN ノードをアップグレードする手順について説明します。

はじめる前に

- ISE-IPN 1.2 ISO イメージがあることを確認します。
- 展開で IPN の高可用性ペアがある場合は、Cisco ISE、リリース 1.1.*x* の展開から IPN ノードを登録解除する前に、高可用性ペアをキャンセルします。
- ノードを登録解除する前に、IPN ノードのすべての設定データを記録します。 また、データを記録するために、（プライマリ管理ユーザ インタフェースから）各 IPN タブのスクリーンショットを保存することもできます。 このデータが手元にあれば、IPN ノードの再登録のプロセスが早く終わります。

手順

ステップ 1 プライマリ管理ノードから IPN ノードを登録解除します。

CLI にアクセスし、コマンド **show application status ise** を入力することによって、IPN ノードが Cisco ISE ノードのステータスに戻ったことを確認します。 ノードが戻っていない場合は、コマンド プロンプトで次のように入力できます。**pep switch outof-pep**。 ただしこれは、最後の手段としてのみを使用することをお勧めします。

ステップ 2 Cisco ISE 3300 シリーズ アプライアンスのイメージを再作成します。 詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』を参照してください。

ステップ 3 アプライアンスに ISE-IPN 1.2 ISO イメージをインストールします。 詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』を参照してください。

ステップ 4 IPN ノード CLI から証明書を設定します。

ステップ 5 ノードを IPN ノードとしてプライマリ管理ノードに登録し、再設定します。

ステップ 6 IPN の設定を確認し、設定を保存します。

関連トピック

アップグレード ソフトウェアのダウンロード, （13 ページ）
インライン ポスチャ ノードの証明書の設定, （33 ページ）
『Cisco Identity Services Engine User Guide, Release 1.2』
『Cisco Identity Services Engine Hardware Installation Guide, Release 1.2』

分散展開の IPN ノードのアクティブ/スタンバイ ペアのアップグレード

インライン ポスチャ ノードのアクティブ/スタンバイ ペアをリリース 1.2 にアップグレードするには、まず高可用性ペアをキャンセルし、ISE-IPN 1.2 ISO イメージを再作成してノードにインストールします。

手順

ステップ 1 プライマリ管理ノードにログインします。

ステップ 2 アクティブ/スタンバイ高可用性ペアをキャンセルします。

a) [管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択します。
b) アクティブな IPEP ノードの隣にあるチェックボックスをオンにして [編集（Edit）] をクリックします。
c) [フェールオーバー（Failover）] タブをクリックします。
d) [HA 有効（HA Enabled）] チェックボックスをオフにします。
e) [保存（Save）] をクリックします。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 プライマリ管理ノードから IPN ノードを登録解除します。
CLI にアクセスし、コマンド **show application status ise** を入力することによって、IPN ノードが Cisco ISE ノードのステータスに戻ったことを確認します。 ノードが戻っていない場合は、コマン

ドプロンプトで次のように入力できます。**pep switch outof-pep**。 ただしこれは、最後の手段としてのみを使用することをお勧めします。

ステップ 5 スタンドアロン IPN ノードのイメージの再作成。 詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』を参照してください。

ステップ 6 IPN ノードに ISE-IPN 1.2 ISO イメージをインストールします。 詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』を参照してください。

ステップ 7 CLI から IPN ノードの証明書を設定します。

ステップ 8 プライマリ管理ノードに IPN ノードを登録します。

ステップ 9 アクティブ/スタンバイ ペアで IPN ノードを再構成します。

ステップ 10 IPN の設定を確認し、設定を保存します。

関連トピック

『Cisco Identity Services Engine User Guide, Release 1.2』
『Cisco Identity Services Engine Hardware Installation Guide, Release 1.2』

インライン ポスチャ ノードの証明書の設定

サポートされるいずれかのアプライアンス プラットフォームで ISE-IPN 1.2 ISO イメージをインストールし、セットアップ プログラムを実行した後、展開に追加する前に、インライン ポスチャ ノードの証明書を設定する必要があります。

はじめる前に

- IPN ノードは、プライマリ管理ノードを認定した同じ CA から認定される必要があります。
- Command-Line Interface (CLI) からのみ、インライン ポスチャ ノードの証明書を設定できます。
- インライン ポスチャ ノードのアクティブ/スタンバイ ペアを展開する場合は、アクティブおよびスタンバイの両インライン ポスチャ ノードで証明書を設定します。

手順

ステップ 1 CLI を使用してインライン ポスチャ ノードにログインします。

ステップ 2 IPN ノードの証明書署名要求（CSR）を生成します。

ステップ 3 DER または Base-64 形式の署名付き証明書をダウンロードし、FTP サーバにコピーします。

ステップ 4 インライン ポスチャ ノードの CLI から次のコマンドを入力します。
pep certificate server add

ステップ 5 再起動するアプリケーションで **y を入力**します。

ステップ 6 最後の CSR に証明書をバインドするために **y** を入力します。

ステップ 7 CA 署名付き証明書の名前を入力します。 IPN のアプリケーションを再起動します。 これで、プライマリ管理ノードにこの IPN ノードを登録できます。

関連トピック

『Cisco Identity Services Engine User Guide, Release 1.2』

インライン ポスチャ ノードの証明書署名要求の生成

Cisco ISE の展開に IPN を追加する前に、IPN はプライマリ管理ノードを認定した同じ CA から認定されることが必要です。

はじめる前に

IPN の CLI にログインする必要があります。

手順

ステップ 1 次のコマンドを入力します。
pep certificate server generatecsr

ステップ 2 **n** を入力して CSR を含む既存の秘密キー ファイルを使用するか、**y** を入力して新しいキー ファイルを生成します。

ステップ 3 必要なキー サイズを入力します。

ステップ 4 証明書に署名するダイジェストのタイプを入力します。

ステップ 5 国番号（2 桁の番号）を入力します。

ステップ 6 都道府県、市町村、構成、組織ユニット値を入力します。

ステップ 7 共通名を入力します。 共通名はホスト名と同じです。 完全修飾名（FQDN）を入力します。 たとえば、ホスト名が IPEP1、DNS ドメイン名が cisco.com である場合、共通名として IPEP1.cisco.com を入力します。

ステップ 8 自分の電子メール アドレスを入力します。

ステップ 9 END CERTIFICATE REQUEST タグの後に、空白行を含むテキスト ブロック全体をコピーします（復帰を含みます）。

ステップ 10 プライマリ管理ノードの証明書に署名した CA に CSR を送信します。

Microsoft の CA を使用している場合は、署名要求の送信中に証明書のテンプレートとして [Web Server] を選択します。

（注） IPN ノードでは、リリース 1.2 でサーバ認証のみがサポートされます。 証明書に署名するために他の CA を使用する場合は、キーの拡張用途でサーバ認証のみが指定されていることを確認します。

CA から署名付き証明書を受信します。

次の作業

DER または Base-64 形式の署名付き証明書をダウンロードし、FTP サーバにコピーします。

FTP サーバへの署名付き証明書のコピー

はじめる前に

インライン ポスチャ ノードで証明書署名要求（CSR）を生成し、CA に送る必要があります。

手順

ステップ 1 インライン ポスチャ ノードの CLI から次のコマンドを入力します。
copy ftp:// *a.b.c.d/ipep1.cer* **disk:**

a.b.c.d は FTP サーバの IP アドレス、*ipep1.cer* は IPN ノードに追加する CA 署名付き証明書です。

ステップ 2 FTP サーバのユーザ名とパスワードを入力します。

次の作業

インライン ポスチャ ノードに署名付き証明書を追加します。

ISE 3400 シリーズ アプライアンスと古いアプライアンスの置き換え

ここでは、古いアプライアンスを Cisco ISE 3400 シリーズ アプライアンスと交換する方法について説明します。

リリース 1.2 を実行するアプライアンスと既存のノードの置き換え

ここでは、Cisco ISE 1.1.*x* ノードを新しい Cisco ISE、リリース 1.2 アプライアンスと交換する場合に、リリース 1.2 にアップグレードするときに、必要な手順を説明します。 管理ノードおよびモニタリング ノードのみをプライマリ ロールおよびセカンダリ ロールでハイ アベイラビリティ用に設定できます。 ロード バランシングとフェールオーバーの目的で、ポリシー サービス ノードをグループ化できます。

はじめる前に

アプライアンスを新しい SNS-3400 シリーズ アプライアンスと交換する場合は、プライマリとセカンダリの管理ノードとして設定する新しい SNS-3400 シリーズのアプライアンスの UDI を使用してライセンスを取得します。

手順

ステップ 1 既存のセカンダリ管理ノードをリリース 1.2 にアップグレードします。
このノードは自動的に、古い展開から自身の登録を解除し、新しいプライマリ管理ノードになります。

ステップ 2 「分散展開」セクションの「ノードのアップグレード」の説明に従って、新規導入の監視、ポリシー、インライン ポスチャ、プライマリ管理のノードをアップグレードします。

ステップ 3 交換する古いアプライアンスのノードを登録解除します。

ステップ 4 新規インストールを実行し、新しい Cisco ISE、リリース 1.2 アプライアンスを、新規のプライマリ管理ノードでを登録します。 詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』および『*Cisco Identity Services Engine User Guide, Release 1.2*』を参照してください。

ステップ 5 新しい SNS-3400 シリーズ アプライアンスの 1 つを新しいプライマリ管理 ISE ノードに昇格させます。 新しいアプライアンスの UDI で取得したライセンスをインストールします。

リリース 1.2 を実行するアプライアンスとすべてのノードの置き換え

ここでは、リリース 1.2 にアップグレードする場合に、すべての Cisco ISE、リリース 1.1.*x* ノードを新しい SNS-3400 シリーズ アプライアンスに交換するために必要な手順について説明しています。 管理ノードおよびモニタリング ノードのみをプライマリ ロールおよびセカンダリ ロールでハイ アベイラビリティ用に設定できます。 ロード バランシングとフェールオーバーの目的で、ポリシー サービス ノードをグループ化できます。

はじめる前に

プライマリおよびセカンダリの管理ノードとして設定する新しい SNS-3400 シリーズ アプライアンスの UDI を使用してライセンスを取得します。

手順

ステップ 1 Cisco ISE の設定データおよびモニタリング データのバックアップを実行します。

ステップ 2 新規インストールを実行し、新規展開でプライマリ管理ノードにする新しい SNS-3400 シリーズのアプライアンスの 1 つを設定します。 詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』を参照してください。

ステップ 3 新しいプライマリおよびセカンダリ管理ノード（SNS-3400 シリーズ アプライアンス）の UDI に基づいて、新規展開のプライマリ管理ノードにライセンスをインストールします。

ステップ 4 新規展開のプライマリ ノードで Cisco ISE 設定を復元します。

ステップ 5 モニタリング ノードとして指定するアプライアンスで、新規インストールを実行し、モニタリングのバックアップを復元して、新規展開のプライマリ管理ノードに登録します。

ステップ 6 新規インストールを実行し、新規展開のプライマリ管理ノードに他の SNS-3400 シリーズ アプライアンスを登録して、プライマリ管理ノードのユーザインターフェイスから設定を行います。 詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』および『*Cisco Identity Services Engine User Guide, Release 1.2*』を参照してください。

第 4 章

Cisco ISE アップグレードの障害からの復旧

この章では、アップグレードの障害からの復旧時に必要な作業について説明します。

アップグレード ソフトウェアは、いくつかの検証を実行します。 アップグレードで障害が発生した場合は、画面に表示される指示に従い、復旧してリリース 1.2 へのアップグレードを成功させます。

また、アップグレードで、セカンダリ管理ノードを最初にアップグレードするなど、ノードのアップグレード順序に従わないために障害が発生することがあります。 このエラーが発生した場合、このガイドに記載されているアップグレード順序に従って展開をアップグレードできます。

まれに、イメージを再作成し、新規インストールを実行して、データを復元することが必要になる場合があります。 アップグレードを開始する前に、Cisco ISE の設定およびモニタリング データのバックアップが存在することが重要です。 構成データベースの障害発生時に自動的に変更のロールバックが試みられますが、コンフィギュレーションおよびモニタリング データをバック アップしておくことが重要です。

（注） モニタリング データベースの問題により発生したアップグレードの障害は、自動的にロールバックされません。 システムのイメージを手動で再作成し、Cisco ISE、リリース 1.2 をインストールしてから、設定データおよびモニタリング データを復元する必要があります。

アップグレードの障害

アップグレード中、コンフィギュレーション データベース スキーマとデータ アップグレードの障害は自動的にロールバックされます。 アプライアンスは、最後の既知の正常な状態に戻ります。 この場合、次のメッセージがコンソールとログに表示されます。

```
% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.2.0-899.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
 Assistance Center for support.
```

アップグレードの障害を修復し、ノードを元の状態に戻すと、コンソールに次のメッセージが表示されます。

```
% Warning: Do the following steps to revert node to its pre-upgrade state."
error: %post(CSCOcpm-os-1.2.0-899.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
 Assistance Center for support.
```

実際のアップグレードの障害ではない認証エラーが発生した場合は、次のメッセージが表示されます。 たとえばセカンダリ PAN のアップグレードの前に PSN をアップグレードしようとすると、このエラーが表示されることがあります。 このエラーが発生した場合は、このドキュメントで説明されているアップグレードを実行できることを確認します。

```
STEP 1: Stopping ISE application...
% Warning: Cannot upgrade this node until the standby PAP node is upgraded and running. If
 standbyPAP is already upgraded
and reachable ensure that this node is in SYNC from current Primary UI.
Starting application after rollback...

% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.2.0-899.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
 Assistance Center for support.
```

ADE-OS またはアプリケーションのバイナリ アップグレードが失敗すると、再起動後に CLI から、**show application status ise** コマンドを実行したときに。次のメッセージが表示されます。

```
% WARNING: An Identity Services Engine upgrade had failed. Please consult logs. You have
to reimage and restore
 to previous version
```

どのような種類の障害でも（アップグレードのキャンセル、コンソール セッションの切断、電源障害など）、ノードで初めてイネーブルにしたペルソナに応じて、コンフィギュレーションとオペレーションのバックアップのイメージを再作成し、復元する必要があります。 ノードのイメージを再作成する場合は、イメージを再作成する前に、失敗の原因を確認するために、**backup-logs** CLI コマンドを実行し、リモート リポジトリ内にサポート バンドルを格納することによって、サポート バンドルを生成します。

アップグレードが失敗する場合、Cisco ISE、リリース 1.2 にアップグレードする前に、次のことを再度行います。

- ログを分析します。 エラーがないかアプリケーション バンドルを検査します。
- 生成したアプリケーション バンドルを Cisco Technical Assistance Center（TAC）に送信して、問題を特定および解決します。

（注） Cisco ISE、リリース 1.1.*x* から 1.2 へのアップグレードは、32 ビットから 64 ビットへのアップグレードです。 このプロセスでは、64 ビットへの ADE-OS およびアプリケーション バイナリのアップグレードを行い、この期間にノードが 2 回リブートされます。 ただし、SSH 経由でログインし、**show application status ise** コマンドを使用することで、アップグレードの進行状況を表示できます。 次のメッセージが表示されます。「% NOTICE: Identity Services Engine upgrade is in progress...」

アップグレードがバイナリのインストール中に失敗する

問題 アプリケーション バイナリのアップグレードはデータベースのアップグレード後に発生する。 バイナリのアップグレードで障害が発生すると、コンソールと ADE.log に次のメッセージが表示されます。

```
% Application install/upgrade failed with system removing the corrupted install
```

解決法 ロールバックまたはリカバリを行う前に、**backup-logs** コマンドを使用してアプリケーション バンドルを生成し、リモート リポジトリにアプリケーション バンドルを配置します。

解決法 ロール バックするには、以前の ISO イメージを使用して Cisco ISE アプライアンスのイメージを再作成し、バックアップ ファイルからデータを復元します。 アップグレードを再試行するには、毎回新しいアップグレード バンドルが必要です。

- **解決法** ログを分析します。 エラーがないかアプリケーション バンドルを検査します。
- **解決法** 生成したアプリケーション バンドルを Cisco Technical Assistance Center（TAC）に送信して、問題を特定および解決します。

SSH セッションがアップ グレード中に終了する

問題 SSH セッションまたはコンソールがアップグレード中に切断される可能性があります。 この場合、reimage、バックアップ ファイルからの以前の ISO イメージを復元し、以前の既知の正常な状態に戻すことによって、Cisco ISE アプライアンスのイメージを再作成します。

解決法 新しい Cisco ISE、リリース 1.2 展開にアップグレードするには、ここでもアップグレード手順を再度開始するか、または新しい Cisco ISE、リリース 1.2 展開でセカンダリ ノードとしてアプライアンスが使用される場合は、イメージを再度作成し、Cisco ISE 1.2 ISO イメージをそこにインストールして、新しいプライマリ管理ノードに登録します。