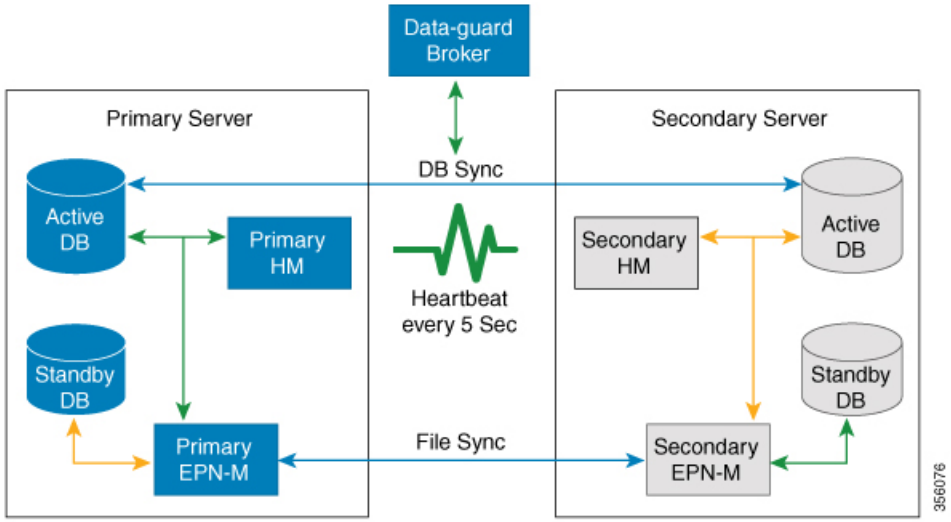
ハイ アベイラビリティの設定と管理

ハイ アベイラビリティの仕組み

Cisco EPN Manager ハイ アベイラビリティ（HA）フレームワークでは、障害が発生してもシステム動作が継続されます。HA では、リンクされて同期された Cisco EPN Manager サーバーのペアを使用して、いずれかのサーバーで発生する可能性のあるアプリケーション障害またはハードウェア障害による影響を最小限に、あるいは完全に排除します。サーバーの障害は、以下の 1 つ以上の領域での問題が原因で発生する可能性があります。

- アプリケーション プロセス：サーバー、TFTP、FTP などのプロセスの失敗。CLI **ncs status** コマンドを使用して、これらのプロセスのステータスを確認できます。
- データベース サーバー：データベース関連のプロセスの失敗（データベース サーバーは Cisco EPN Manager でサービスとして実行されます）。
- ネットワーク：ネットワーク アクセスまたは到達可能性に関連する問題。
- システム：サーバーの物理ハードウェアまたはオペレーティング システムに関連する問題。
- 仮想マシン（HA が VM 環境で稼動している場合）：プライマリ サーバーとセカンダリ サーバーがインストールされている VM 環境に関する問題。

次の図は、HA セットアップの主なコンポーネントとプロセス フローを示しています。



HA展開は、プライマリ サーバーとセカンダリ サーバーで構成され、両方のサーバー上にヘルス モニター（HM）インスタンス（アプリケーション プロセスとして実行）が存在します。プライマリ サーバーに障害が発生（自動的に発生、または手動で停止したために発生）すると、プライマリ サーバーへのアクセスが復元されるまでの間はセカンダリ サーバーがネットワークの管理を引き継ぎます。展開で自動フェールオーバーを設定すると、セカンダリ サーバーはフェールオーバー後 2 ～ 3 分以内にアクティブ ロールを引き継ぎます。この HA は、アクティブ/パッシブまたはコールド スタンバイの動作モデルに基づいています。クラスタ化されたシステムではないため、プライマリ サーバーに障害が発生した場合、セッションはセカンダリ サーバーに保持されません。

プライマリ サーバーの問題が解決してサーバーが実行状態になっても、アクティブなセカンダリ サーバーとのデータの同期を開始する間はスタンバイ モードのままになります。プライマリ サーバーが再び使用可能になった時点で、フェールバック操作を開始できます。フェールバックがトリガーされると、プライマリ サーバーがアクティブ ロールを再度引き継ぎます。このようなプライマリ サーバーとセカンダリ サーバー間でのロールの切り替えは、2 ～ 3 分以内に実行されます。

HA 設定によってプライマリ サーバーでの変更が確認されると、変更内容がセカンダリ サーバーと同期されます。これらの変更には、次の 2 種類があります。

- ファイルの変更。HTTPS プロトコルを使用して同期されます。対象となる項目には、レポート設定、設定テンプレート、TFTP ルート ディレクトリ、管理設定、ライセンス ファイル、キー ストアなどがあります。ファイルの同期は、以下のいずれかで行われます。
  - 頻繁に更新されないファイル（ライセンス ファイルなど）の同期は、一括で行われます。これらのファイルは、500 秒間隔で同期されます。
  - 頻繁に更新されるファイルの同期は、ほぼリアルタイムで行われます。これらのファイルは、11 秒間隔で同期されます。

- データベースの変更（設定、パフォーマンス、およびモニターリングデータに関連する更新など）。Oracle Recovery Manager（RMAN）が最初のスタンバイ データベースを作成し、変更が発生すると、Oracle Active Data Guard がデータベースを同期します。

プライマリ HA サーバーとセカンダリ HA サーバーは、次のメッセージを交換して 2 つのサーバー間の同期を維持します。

- データベース同期：プライマリ サーバーとセカンダリ サーバー上のデータベースが稼働および同期するために必要なすべての情報が含まれます。
- ファイル同期：頻繁に更新されるコンフィギュレーション ファイルが含まれます。これらのファイルは 11 秒間隔で同期され、他の頻繁に更新されないコンフィギュレーション ファイルは 500 秒間隔で同期されます

Note プライマリで手動で更新されたコンフィギュレーション ファイルは、セカンダリに同期されません。プライマリでコンフィギュレーション ファイルを手動で更新する場合は、セカンダリ上のファイルも更新する必要があります。

- プロセス同期：アプリケーションおよびデータベースに関連するプロセスの実行が継続されるようにします。これらのメッセージは、ハートビート カテゴリに分類されます。
- ヘルス モニター同期：これらのメッセージは、ネットワーク、システム、およびヘルス モニターの障害状態の有無を確認します。

プライマリ サーバーとセカンダリ サーバーについて

どの EPN Manager HA 実装でも、プライマリサーバーのある特定のインスタンスに対して専用のセカンダリサーバーが 1 台のみ必要です。

通常、HA サーバーごとに独自の IP アドレスまたはホスト名が設定されています。同一サブネット上に配置されているサーバーは、仮想 IP を使用して同じ IP を共有できます。これにより、デバイスの設定が容易になります。

HA をセットアップした後は、HA サーバーの IP アドレスやホスト名を変更しないください。変更すると、HA のセットアップが失われます。

詳細については、サーバーの IP アドレスまたはホスト名のリセット （46 ページ）を参照してください。

（注） HA 構成サーバーの場合、EPNM タイトルバーには、接続しているサーバーのタイプ、つまり、プライマリサーバーに接続しているかセカンダリサーバーに接続しているかが表示されます。

HA の導入計画

HA 機能は、以下の導入モデルをサポートしています。

- **ローカル**：HA サーバーの両方を同じサブネットに配置します（サーバーにレイヤ 2 近接性を与えます）。通常は、両方のサーバーが同じデータ センター内に配置されます。
- **キャンパス**：HA サーバーのそれぞれを、LAN で接続された異なるサブネットに配置します。通常、これらのサーバーは同じ 1 つのキャンパスに導入されますが、キャンパス内で配置される場所は異なります。
- **リモート**：HA サーバーのそれぞれを、WAN で接続された異なるリモート サブネットに配置します。各サーバーが、異なる施設に配置されます。これらの施設は、国や大陸間にまたがり、地理的に分散されています。

以降の項で、各モデルの利点および欠点と、すべての導入モデルに影響する基本的な制約事項について説明します。

HA は、サポートされているいずれの導入モデルでも機能します。主な制約事項は、HA のパフォーマンスと信頼性に関して存在し、これらは帯域幅と遅延の基準によって異なります（「HA のネットワーク スループットに関する制限事項」参照）。これらのパラメータを正常に管理できる限り、使用可能な導入モデルのどれを選んで実装するかは、（コスト、企業の規模、地理、コンプライアンス標準などのビジネスパラメータに基づく）ビジネス上の意思決定です。

HA のネットワーク スループットに関する制限事項

Cisco EPN Manager の HA パフォーマンスは、常に以下の制限要因の影響を受けます。

- すべての操作を処理するために Cisco EPN Manager で利用できる正味の帯域幅。これらの操作には、HA 設定、データベース同期、ファイル同期、フェールバックのトリガーが含まれます（ただし、これらに限定されません）。
- プライマリ サーバーとセカンダリ サーバー間のリンク全体における正味のネットワーク遅延。この 2 台のサーバーの物理的な近接性に関わらず、サーバー間のリンクで発生する遅延が大きい場合、Cisco EPN Manager によるプライマリ サーバーとセカンダリ サーバー間のセッション維持状態に影響が及ぶ可能性があります。
- プライマリ サーバーとセカンダリ サーバーを接続するネットワークが提供できる正味のスループット。正味のスループットは正味の帯域幅と遅延によって異なり、これら 2 つの要因の関数と見なすことができます。

モデルによって問題の大きさが異なりますが、これらの制限は、少なくとも何らかのレベルであらゆる導入モデルに当てはまります。たとえば、リモート導入モデルは、地理的な分散が大きいため、帯域幅と遅延の両方で問題が発生しがちです。一方、ローカル モデルとキャンパス モデルの場合も、正しく構成されていなければ、帯域幅の問題が発生する可能性が高くなります。これは、低帯域幅、高遅延、高ネットワーク使用率によって制限を受ける可能性があるためです。

スループットの問題がフェールバックやフェールオーバーに影響することはほとんどありません。2 つの HA サーバーがほとんど常に通信して、データベースの変更内容が即座に複製されるためです。ほとんどのフェールオーバーおよびフェールバックは、約 2 ～ 3 分を要します。

この原則の最大の例外は、データベースのフル コピー動作における遅延です。この種類のアクションは、プライマリ サーバーがデータ保持期間を超えてダウンした後、これを再度稼働させる場合にトリガーされます。Express、Express-Plus、Standard の各構成サーバーのデータ保持期間は 6 時間で、Professional および Gen 2 アプライアンス サーバーでは 12 時間です。

Cisco EPN Manager はセカンダリ サーバーからプライマリ サーバーへのデータベースのフル コピー動作をトリガーします。この期間中のフェールバックはできませんが、[ヘルス モニター（Health Monitor）] ページには、データベースのコピー進行中に発生したすべてのイベントが表示されます。コピーが完了するとすぐに、プライマリ サーバーが「プライマリ同期中（Primary Synching）」状態に移行し、フェールバックのトリガーが可能になります。データベースのフル コピーが行われている間は、プライマリ サーバーの再起動やネットワーク接続切断を行わないでください。

データベースのフル コピー動作中の正味スループットの変動は、データベースのサイズやその他の要因とは無関係に、データベースのフル コピー動作が 1 時間未満で正常に完了するケースと、まったく完了できないケースという違いを生じるぐらいの意味を持ちます。次のことを推奨します。

- ネットワーク スループット：最小 500 Mbps（メガビット毎秒）。可能であればこれ以上を推奨。
- ネットワーク遅延：最大 100 ミリ秒。可能であれば 70 ミリ秒を推奨。

パフォーマンスが低いとシステムの安定性が低下し、ハイアベイラビリティのシナリオ（主に登録とフェールバック）を完了できなくなる可能性があります。

ローカル モデルの使用

ローカル導入モデルの主要なメリットは、仮想 IP アドレスをシステムの単一管理ドレスとして使用することが許可される点です。ユーザーはこの仮想 IP アドレスを使用して Cisco EPN Manager に接続でき、デバイスでは SNMP トラップおよびその他の通知の宛先としてこの仮想 IP アドレスを使用できます。

仮想 IP アドレスを割り当てる際の唯一の制約は、仮想 IP アドレスが、プライマリ サーバーの IP アドレスおよびセカンダリ サーバーの IP アドレスと同じサブネット上のアドレスでなければならない点です。例：プライマリ サーバーとセカンダリ サーバーに対し、1 つのサブネット内の次の IP アドレスが割り当てられている場合、この両方のサーバーの仮想 IP アドレスは次のように割り当てることができます。

- サブネット マスク：255.255.255.224 (/27)
- プライマリ サーバーの IP アドレス：10.10.101.2
- セカンダリ サーバーの IP アドレス：10.10.101.3

- 仮想 IP アドレス：10.10.101.[4-30]（例：10.10.101.4）仮想 IP アドレスは、特定のサブネットマスクで有効かつ未使用のアドレス範囲内の任意のアドレスになることに注意してください。

この主な利点に加え、ローカル モデルには以下の利点もあります。

- 通常、高帯域幅と低遅延を実現します。
- 管理が簡素化されます。
- syslog および SNMP 通知を転送するようにデバイスを設定するのが、大幅に簡単になります。

ローカル モデルには、以下の欠点があります。

- 同じデータ センター内に配置されることから、停電や自然災害など、サイト全体の障害の危険にさらされます。
- 破壊的なサイト障害の危険が高くなることから、ビジネス継続性の計画が複雑になります。また、損害保険のコストも高くなる可能性があります。

キャンパス モデルの使用

キャンパス モデルでは、HA を導入する組織が、同じ都道府県の同じ市区町村内の 1 つ以上のロケーションを拠点にしていて、これらの複数ロケーションによって「キャンパス」を形成していることが前提となります。このモデルには、以下の利点があります。

- 通常、ローカル モデルに匹敵するか、それ以上の帯域幅と遅延を提供します。
- リモート モデルより簡単に管理できます。

キャンパス モデルには、以下の欠点があります。

- ローカル モデルより、管理が複雑になります。
- 仮想 IP アドレスをシステムの単一管理アドレスとして使用することを許可しないでください。このため、多くのデバイス設定が必要となります（仮想 IP アドレッシングを使用できない場合の対処 （11 ページ）を参照）。
- ローカル モデルと比べると、帯域幅が小さくなり、遅延が大きくなる可能性があります。これは HA の信頼性に影響を与える可能性があり、是正するには管理者の介入が必要になる場合もあります（「HA のネットワーク スループットに関する制限事項 （4 ページ）」を参照）。
- 同じサイトに配置されてはいませんが、それでも都道府県全体、または市区町村全体の災害の危険にさらされます。そのため、ビジネス継続性の計画が複雑になり、災害復旧のコストが高くなる可能性があります。

リモート モデルの使用

リモートモデルでは、導入する組織に複数のサイトまたはキャンパスがあること、そしてこれらのロケーション間では、地理的な境界を超えて WAN リンクで通信することが前提となります。このモデルには、以下の利点があります。

- 自然災害による影響を受ける可能性が最小限になります。ビジネス継続性および災害復旧という点では、通常、これが最も複雑でなく、コストのかからないモデルになります。
- 事業保険のコストを節約できる可能性があります。

リモート モデルには、以下の欠点があります。

- ローカルまたはキャンパス モデルより、管理が複雑です。
- 仮想 IP アドレスをシステムの単一管理アドレスとして使用できないため、多くのデバイス設定が必要となります（仮想 IP アドレッシングを使用できない場合の対処 （11 ページ）を参照）。
- 通常、他の 2 つのモデルよりも提供される帯域幅が低く、遅延が大きくなります。これは HA の信頼性に影響を与える可能性があり、是正するには管理者の介入が必要になる場合もあります（「HA のネットワーク スループットに関する制限事項 （4 ページ）」を参照）。

自動フェールオーバーと手動フェールオーバーの違い

自動フェールオーバーを行うように HA を設定すると、ネットワーク管理者による HA の管理の必要性が減少します。また、セカンダリ サーバーが自動的に起動されるため、フェールオーバーの発生原因となった状況への対応に要する時間が削減されます。

ただし、ほとんどの場合は、システムで手動フェールオーバーを設定することが推奨されます。この推奨に従うことで、断続的なネットワークの停止を理由に Cisco EPN Manager がセカンダリ サーバーに頻繁にフェールオーバーすることがなくなります。この状況が発生する可能性が最も高いのは、リモートモデルを使用して HA を導入する場合です。このモデルは、特に帯域幅と遅延の急激な変化による影響を受けます（HA の導入計画 （4 ページ）および HA のネットワーク スループットに関する制限事項 （4 ページ）を参照）。

フェールオーバー タイプが [自動（Automatic）] に設定されている場合に、ネットワーク接続がダウンするか、またはプライマリ サーバーとセカンダリ サーバー間のネットワーク リンクが到達不能になると、プライマリ サーバーとセカンダリ サーバーの両方が同時にアクティブになる可能性がわずかながらあります。これは「スプリット ブレーン状況」と呼ばれます。

この状況を防ぐため、プライマリ サーバーはセカンダリ サーバーがアクティブかどうかを常に確認します。ネットワーク接続またはリンクが復元され、プライマリ サーバーからセカンダリ サーバーに再び到達可能になると、プライマリ サーバーはセカンダリ サーバーの状態を確認します。セカンダリ サーバーの状態がアクティブな場合、プライマリ サーバーは自らダウンします。続いてユーザーがプライマリ サーバーへの標準の手動フェールバックを実行できます。

この状況が発生するのは、プライマリ HA サーバーで自動フェールオーバーが設定されている場合だけであることに注意してください。プライマリ サーバーで手動フェールオーバーを設定することで、この状況が発生する可能性が排除されます。これが、手動フェールオーバー設定を推奨するもう 1 つの理由です。

大企業では特に、自動フェールオーバーは不適切です。特定の HA 導入環境で自動フェールオーバーを実行することになった場合、管理者はプライマリ サーバーまたはセカンダリ サーバーに新規に追加されたデータのいずれかを選択しなければならないことがあります。つまり、スプリットブレーンの状況が発生するたびにデータが失われる可能性があります。この問題に対処する際のヘルプについては、を参照してください。 スプリット ブレイン シナリオからの回復方法 （38 ページ）

HA を適切に管理するために、Cisco EPN Manager 管理者は、フェールオーバーまたはフェールバックを開始する前に、以下を含む HA 導入の全体的な状態を必ず確認することが推奨されます。

- プライマリ サーバーの現在の状態。
- セカンダリ サーバーの現在の状態。
- 2 台のサーバー間の現在の接続状態。

ハイ アベイラビリティのセットアップ

ハイ アベイラビリティ導入環境にプライマリ サーバーとセカンダリ サーバーをインストールする方法については、『Cisco Evolved Programmable Network Manager Installation Guide』で説明しています。インストールの一環として、管理者は HA 導入環境で手動または自動フェールオーバーが使用されるように設定します。現在のフェールオーバー設定は、**ncs ha status** コマンドを使用して確認するか、[ヘルスモニター（Health Monitor）] Web ページで確認できます（ヘルス モニター Web ページの使用 （20 ページ）を参照）。

プライマリ サーバーとセカンダリ サーバーをインストールしたら、プライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （11 ページ）で説明する HA 設定手順を実行する必要があります。

次のトピックで、HA の導入に関する追加情報を提供します。

- HA での仮想 IP アドレッシングの使用 （9 ページ）
- 仮想 IP アドレッシングを使用できない場合の対処 （11 ページ）
- プライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （11 ページ）
- HA 環境での SSO サーバーの設定 （13 ページ）

HA での仮想 IP アドレッシングの使用

仮想IPアドレスは、アクティブHAサーバーの管理IPアドレスを表します。フェールオーバーまたはフェールバック中は、仮想 IP アドレスが 2 つの HA サーバー間で自動的に切り替えられます。これには次の 2 つのメリットがあります。

- Cisco EPN Manager Web GUI に接続するために、どのサーバーがアクティブかを把握する必要がありません。仮想 IP を使用すれば、要求がアクティブな HA サーバーに自動的に転送されます。
- プライマリ サーバーとセカンダリ サーバーの両方に通知を転送するように管理対象デバイスを設定する必要がありません。通知を仮想 IP アドレスに転送するだけで済みます。

プライマリ サーバーと一緒にセカンダリ サーバーを設定するときに、仮想 IP アドレッシングを有効にすることができます。両方のサーバーで共有する仮想アドレス（IPv4 は必須で IPv6 はオプション）を入力する必要があります。プライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （11 ページ）を参照してください。

仮想IPアドレスを使用しても、フェールオーバーまたはフェールバックの発生時に、アクティブなクライアント/サーバー セッションが終了するという事実は変わりません。仮想 IP アドレスが使用可能な状態であっても、新しいサーバーが新しい要求の処理を開始すると、アクティブなクライアント/サーバー セッション（Web GUI または NBI）が終了します。Web GUI ユーザーは、ログアウトしてログインし直す必要があります。中断したNBIセッションの処理方法については、Cisco Evolved Programmable Network Manager MTOSI API ガイド（OSS 統合） を参照してください。

（注） 仮想 IP を使用するには、プライマリ サーバーとセカンダリ サーバーの IP アドレスが同じサブネット上に存在する必要があります。

HA での複数の仮想 IP アドレッシング

Cisco EPN Manager では、独自の仮想 IP アドレスを持つように最大 3 つのインターフェイスを設定できます。さらに、仮想 IP アドレスを使用して、複数のインターフェイスのチーム（論理バインディング）を設定できます。これを行うには 2 つの方法があります。

- （**推奨**）CLI からすべての仮想 IP アドレスを設定します。

  この場合は Cisco EPN Manager UI で [仮想 IPの有効化（Enable Virtual IP）] チェックボックスをオンにしないでください。このフィールドのチェックボックスには、CLI から設定した最初の仮想 IP アドレスが自動的に入力されます。

- Cisco EPN Manager UI から最初の仮想IPアドレスを設定し、残りの仮想 IP アドレスは CLI から設定します。

(注) HA 登録時の問題を回避するには、CLI から設定する最初の仮想 IP が UI で設定したものと一致していることを確認します。不一致がある場合は HA 登録がブロックされ、エラーメッセージが表示されます。

このプロセスは HA 登録を実行するための前提条件です。

CLI から複数の仮想 IP を有効にするには、次の手順を実行します。

ステップ 1 Cisco EPN Manager の CLI 管理者ユーザーとしてサーバーにログインします。

ステップ 2 コンフィギュレーション モードを入力します。

```
configure terminal
```

ステップ 3 仮想 IP を設定するインターフェイスを選択します。

```
interface <name of interface>
```

ステップ 4 プロンプトで次のコマンドを入力します。

```
virtual-ip
```

ステップ 5 プライマリおよびセカンダリの HA サーバーで共有する IPv4 仮想 IP アドレスを指定します。必要に応じて、IPv6 仮想 IP アドレスを指定します（IPv4 アドレスは必須ですが、IPv6 アドレスはオプションです）。

- （必須）IPv4 アドレスを設定するには、次の手順を実行します。

  ```
  ip-address IPv4 address
  ```

- （オプション）IPv6 アドレスを設定するには、次の手順を実行します。

  ```
  ipv6-address IPv6 address
  ```

ステップ 6 サブメニューを終了します。

```
exit
```

ステップ 7 インターフェイス コンフィギュレーションを終了します。

```
exit
```

ステップ 8 コンフィギュレーション モードを終了します。

```
exit
```

ステップ 9 （オプション）インターフェイスで次のコマンドを実行して設定を確認します。

```
show running-config
```

HA 登録が正常に完了すると、仮想 IP アドレスがプライマリサーバーで有効になります。仮想 IP アドレスは HA 登録時にセカンダリサーバーにコピーされますが、フェールオーバーの場合にのみ有効になります。

（注）

- Cisco EPN Manager UI には、最初のインターフェイスである GigabitEthernet 0（または Ethernet 0）に設定された仮想 IP のみが表示されます。残りのインターフェイスに設定された仮想 IP アドレスは、Web UI に表示されません。
- インターフェイスに設定されているすべての仮想IPアドレスを表示するには、CLI で `show running config` コマンドを実行します。

仮想 IP アドレッシングを使用できない場合の対処

選択する導入モデルによっては、仮想IPアドレスを設定しないでおくと、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーが発生した場合に syslog と SNMP 通知がセカンダリ サーバーに転送されるようにするために、管理者が追加の作業を行わなければならない状況になることがあります。一般的な方法は、両方のサーバーにすべてのsyslogとトラップを転送するようにデバイスを設定することです。このためには通常、転送先をプライマリ サーバーとセカンダリ サーバーの両方を含む特定のサブネットまたは IP アドレス範囲に設定します。

この設定作業は、HA のセットアップと同時に行う必要があります。つまりセカンダリ サーバーをインストールした後、プライマリ サーバーでHAを登録する前に行います。これはフェールオーバーが発生する前に完了しておく必要があります。これにより、データが失われる可能性を解消または削減できます。仮想 IP アドレスを使用しない場合、セカンダリ サーバーのインストール手順は変更されません。ただし通常どおり、個別の IP アドレスを使用してプライマリ サーバーとセカンダリ サーバーをプロビジョニングする必要があります。

プライマリ サーバーとセカンダリ サーバー間の HA の設定方法

HA を有効にするには、プライマリ サーバーで HA を設定する必要があります。プライマリ サーバーがHAコンフィギュレーションに参加するために、サーバーのインストール中に必要となる設定はありません。プライマリ サーバーで必要な情報は次の情報のみです。

- すでにインストールおよび設定済みのセカンダリ HA サーバーの IP アドレスまたはホスト名（セカンダリサーバーのインストールについては、『*Cisco Evolved Programmable Network Manager Installation Guide*』を参照してください）。
- セカンダリ サーバーのインストール時に設定した認証キー。
- （オプション）通知の送信先となる 1 つ以上の電子メール アドレス。
- フェールオーバー タイプ（自動フェールオーバーと手動フェールオーバーの違い （7 ページ）を参照してください）。

仮想 IP アドレッシングを使用する場合は、HA での仮想 IP アドレッシングの使用 （9 ページ）を参照してください。

次の手順では、プライマリ サーバーで HA を設定する方法について説明します。HA を再設定する場合も、同じ手順を実行します。

始める前に

複数の仮想 IP アドレスを使用する場合は、この手順の前に必ず CLI からそれらのアドレスを設定してください。詳細については、HA での複数の仮想 IP アドレッシング （9 ページ）を参照してください。

（注） 1 つの仮想 IP アドレスのみを使用する場合は、HA 登録時に Cisco EPN Manager UI から設定できます。CLI から設定する必要はありません。

ステップ 1 管理者権限を持つユーザー ID とパスワードを使用して Cisco EPN Manager にログインします。

ステップ 2 メニューから、**[管理（Administration）]>[設定（Settings）]>[ハイ アベイラビリティ（High Availability）]** の順に選択します。Cisco EPN Manager によって HA ステータス ページが表示されます。

ステップ 3 [HA 設定（HA Configuration）] を選択し、次のフィールドに入力します。

1. [セカンダリ サーバー（Secondary Server）]：セカンダリ サーバーの IP アドレスまたはホスト名を入力します。

   （注） ホスト名を IP アドレスに解決するには、DNS サーバーを使用することをお勧めします。DNS サーバーの代わりに「/etc/hosts」ファイルを使用している場合は、ホスト名の代わりにセカンダリ IP アドレスを入力します。

2. [認証キー（Authentication Key）]：セカンダリ サーバーのインストール中に設定したパスワードを認証キーとして入力します。

3. [電子メールアドレス（Email Address）]：（任意）HA の状態変更に関する通知の送信先アドレス（またはコンマで区切ったアドレスのリスト）を入力します。[メールサーバー設定（Mail Server Configuration）] ページで電子メール通知をすでに設定している場合、ここに入力した電子メールアドレスは、メールサーバーですでに設定されているアドレスのリストに追加されます。

4. [フェールオーバー タイプ（Failover Type）]：[手動（Manual）] または [自動（Automatic）] を選択します。[手動（Manual）] を選択することが推奨されます。

ステップ 4 （仮想 IP アドレスを CLI からすでに設定している場合は、このステップを無視してステップ 5 に進んでください。）仮想 IP 機能を使用する場合：[仮想 IP の有効化（Enable Virtual IP）] チェックボックスをオンにし、追加フィールドに次のように入力します。

1. [IPV4 仮想 IP（IPV4 Virtual IP）]：両方の HA サーバーに使用する仮想 IPv4 アドレスを入力します。

2. [IPV6 仮想 IP（IPV6 Virtual IP）]：（オプション）両方の HA サーバーに使用する仮想 IPv6 アドレスを入力します。

両方のサーバーが同一サブネット上にない場合は、仮想 IP アドレッシングは機能しないことに注意してください。

ステップ 5 [準備状況の確認（Check Readiness）] をクリックし、HA 関連の環境パラメータが設定を行える状態になっているかを確認します。

詳細については、HA 設定の準備状況の確認 （14 ページ）を参照してください。

（注） 準備状況チェックによって HA 設定がブロックされることはありません。すべてのテストに合格しなくも、HA を設定できます。

ステップ 6 [保存（Save）] をクリックして変更を保存します。Cisco EPN Manager によって HA 設定プロセスが開始されます。設定が正常に完了すると、**[コンフィギュレーションモード（Configuration Mode）]** に、**[HA対応（HA Enabled）]** という値が表示されます。

（注） FTP または TFTP サービスがプライマリサーバーで実行されている場合は、フェールオーバーが失敗しないようにするために、設定の完了後にセカンダリサーバーを再起動する必要があります。

注意すべき重要点：

- 高可用性機能は、HA 登録後に追加された仮想 IP アドレスを管理しません。HA 登録後に仮想 IP アドレスを追加しないことをお勧めします。
- HA 登録に失敗すると、設定されているすべての仮想 IP アドレスが削除されます。HA 登録の前に、これらを再設定する必要があります。
- 高可用性を有効にした後で仮想 IP アドレスを削除すると、高可用性は失敗します。
- 設定した仮想 IP アドレスを変更するには、次の手順を実行します。
  1. 既存の HA 設定を削除します。
  2. 仮想 IP アドレスを設定します。
  3. HA 登録を再度実行します。

HA 環境での SSO サーバーの設定

シングルサインオン（SSO）認証は、マルチユーザー、マルチリポジトリ環境でのユーザーの認証および管理に使用されます。SSO は、さまざまなシステムにログインするために使用されるクレデンシャルを格納および取得します。Cisco EPN Manager の他のインスタンス用の SSO サーバーとして Cisco EPN Manager をセットアップできます。

ハイ アベイラビリティ環境で SSO サーバーを設定するには、表 1 : HA 展開における SSO の設定に記載されているいずれかの手順を選択します。詳細については、次のトピックを参照してください。

- SSO サーバーを設定するには、「Cisco EPN Manager への RADIUS または TACACS+ サーバーの追加」を参照してください。
- HA サーバーを設定するには、『Cisco Evolved Programmable Network Manager Installation Guide』を参照してください。

表 *1: HA* 展開における *SSO* の設定

SSO の設定	SSO サーバーのセットアップ	サーバーのフェールオーバー シナリオ	SSOサーバーの障害シナリオ
スタンドアロン サーバーとして SSO を設定	1. スタンドアロンのSSOサーバーを設定します。 2. プライマリおよびセカンダリ HA サーバーを設定します。	プライマリ サーバーに障害が発生すると、セカンダリ サーバーが有効化されます。プライマリ サーバーに接続されているすべてのマシンが、セカンダリ サーバーにリダイレクトされます。	SSOサーバーで障害が発生すると、SSO機能が無効になります。Cisco EPN Manager ではローカル認証が使用されます。
セカンダリ サーバーで SSO を設定	1. 1 台のサーバーをSSOサーバーとプライマリ サーバーに設定します（つまり、プライマリ サーバーは SSO サーバーでもあります）。 2. セカンダリ HA サーバーを設定します。	プライマリ サーバーに障害が発生すると、セカンダリ サーバーが有効化されます。プライマリ サーバーに接続されているすべてのマシンは、セカンダリ サーバーにリダイレクトされません（これは、プライマリ サーバーで SSO が設定されているためです）。	SSO（プライマリ）サーバーで障害が発生した場合は、セカンダリ サーバーを SSO のフェールバック オプションとして設定できます。これにより、すべてのインスタンスをセカンダリ サーバーに接続できます。 セカンダリ サーバーが SSO サーバーのフェールバック オプションとして設定されていない場合、Cisco EPN Manager はローカル認証を使用します。

HA 設定の準備状況の確認

HA 設定時に、HA に関連する他の環境パラメータ（システム仕様、ネットワーク構成、サーバー間の帯域幅など）によって HA 設定が決定されます。

15のチェックがシステムで実行され、エラーや障害なくHA設定が完了したことが確認されます。準備状況の確認機能を実行すると、チェックリストの名前および対応するステータスが、該当する場合は推奨事項とともに表示されます。

（注） **準備状況の確認**によってHA設定がブロックされることはありません。すべてのチェックに合格しなくても、HA を設定できます。

プライマリ認証キーとセカンダリ認証キーが異なる場合、準備状況チェックは続行されません。HA 登録を続行できます。

HA 設定の準備状況を確認するには、次の手順に従います。

ステップ 1 管理者権限を持つユーザー ID とパスワードを使用して Cisco EPN Manager にログインします。

ステップ 2 メニューから、**[管理（Administration）]**>**[設定（Settings）]**>**[ハイ アベイラビリティ（High Availability）]** の順に選択します。Cisco EPN Manager によって HA ステータス ページが表示されます。

ステップ 3 [HA 設定（HA Configuration）] を選択します。

ステップ 4 [セカンダリ サーバー（Secondary Server）] フィールドにセカンダリ サーバーの IP アドレスを入力し、[認証キー（Authentication Key）] フィールドのセカンダリの認証キーを入力します。

ステップ 5 [準備状況の確認（Check Readiness）] をクリックします。

ポップアップ ウィンドウが開き、システム仕様およびその他のパラメータが表示されます。画面には、チェックリスト項目の名前、ステータス、影響、推奨事項の詳細が示されます。

その下に、準備状況の確認に使用されたチェックリストのテスト名と説明のリストが表示されます。

表 *2:* チェックリストの名前と説明

チェックリストのテスト名	テストの説明
システム - CPU数の確認（SYSTEM - CHECK CPU COUNT）	プライマリ サーバーとセカンダリ サーバーの両方の CPU 数を確認します。 両方のサーバーのCPU数が要件を満たしている必要があります。
システム - ディスク IOPS の確認（SYSTEM - CHECK DISK IOPS）	プライマリ サーバーとセカンダリ サーバーの両方のディスク速度を確認します。 必要な最小ディスク速度は 200 Mbps です。
システム - RAM サイズの確認（SYSTEM - CHECK RAM SIZE）	プライマリ サーバーとセカンダリ サーバーの両方の RAM サイズを確認します。 両方のサーバーの RAM サイズが要件を満たしている必要があります。
システム - ディスクサイズの確認（SYSTEM - CHECK DISK SIZE）	プライマリ サーバーとセカンダリ サーバーの両方のディスク サイズを確認します。 両方のサーバーのディスク サイズが要件を満たしている必要があります。
システム - サーバーへの ping 確認（SYSTEM - CHECK SERVER PING REACHABILITY）	プライマリ サーバーが ping を介してセカンダリ サーバーに到達できることを確認します。
システム - OS互換性の確認（SYSTEM - CHECK OS COMPATABILITY）	プライマリ サーバーとセカンダリ サーバーの OS バージョンが同じであることを確認します。

システム - ヘルス モニターのステータス（SYSTEM - HEALTH MONITOR STATUS）	ヘルス モニター プロセスがプライマリ サーバーとセカンダリ サーバーの両方で実行されているかどうかを確認します。
ネットワーク - ネットワーク インターフェイスの帯域幅確認（NETWORK - CHECK NETWORK INTERFACE BANDWIDTH）	インターフェイス eth0 の速度がプライマリサーバーとセカンダリサーバーで推奨されている 100 Mbps に一致しているかどうかを確認します。 このテストでは、プライマリサーバーとセカンダリサーバー間でのデータ送信によるネットワーク帯域幅の測定は行いません。
ネットワーク - データベース ポートの開閉についてファイアウォールの確認（NETWORK - CHECK FIREWALL FOR DATABASE PORT ACCESSIBILITY）	データベース ポート 1522 がシステム ファイアウォールで開いているかどうかを確認します。 このポートが無効になっていると、テストは IP テーブルリストで 1522 の権限を付与します。
データベース - オンラインステータスの確認（DATABASE - CHECK ONLINE STATUS）	データベース ファイルのステータスがオンラインになっており、プライマリ サーバーとセカンダリ サーバーの両方でアクセス可能であるかどうかを確認します。
データベース - メモリターゲットの確認（DATABASE - CHECK MEMORY TARGET）	HA セットアップの「/dev/shm」データベース メモリ ターゲット サイズを確認します。
データベース - リスナーのステータス（DATABASE - LISTENER STATUS）	プライマリ サーバーとセカンダリ サーバーの両方でデータベース リスナーが稼働中であるかどうかを確認します。 障害が発生した場合、テストによってリスナーの起動とステータスの報告が試行されます。
データベース - リスナー設定ファイルの破損確認（DATABASE - CHECK LISTENER CONFIG CORRUPTION）	すべてのデータベース インスタンスがデータベース リスナー設定ファイル「listener.ora」に存在するかどうかを確認します。
データベース - TNS 設定ファイルの破損確認（DATABASE - CHECK TNS CONFIG CORRUPTION）	すべての「WCS」インスタンスがデータベース TNS リスナー設定ファイル「tnsnames.ora」に存在するかどうかを確認します。
データベース - TNS 到達可能性のステータス（DATABASE - TNS REACHABILITY STATUS）	プライマリ サーバーとセカンダリ サーバーの両方で TNSPING が成功しているかどうかを確認します。

ステップ 6 すべてのパラメータのチェックが完了したら、パラメータのステータスを確認し、[クリア（Clear）] をクリックしてウィンドウを閉じます。

（注） **準備状況の確認**中のフェールバック イベントとフェールオーバー イベントは、[アラームおよびイベント（Alarms and Events）] ページに転送されます。設定障害イベントは [アラームおよびイベント（Alarms and Events）] リストに表示されません。

HA サーバーにパッチを適用する方法

次のいずれかの方法で HA サーバーの UBF パッチをダウンロードおよびインストールできます。

- 現在ペアリングされていない HA サーバーにパッチをインストールします。Cisco EPN Manager 用に HA が設定されていない場合は、この方法をお勧めします。
- 手動フェールオーバーを使用して、ペアリングされている既存の HA サーバーにパッチをインストールします。HA がすでに設定されている場合はこの方法が推奨されます。
- 自動フェールオーバーを使用して、ペアリングされている既存の HA サーバーにパッチをインストールします。

それぞれの方法について詳しくは、以下を参照してください。

新しい HA サーバーへのパッチ適用方法

新しい Cisco EPN Manager ハイ アベイラビリティ（HA）実装のセットアップで、新しいサーバーのパッチ レベルが異なる場合は、次の手順に従って両方のサーバーにパッチをインストールし、同じパッチ レベルにします。

ステップ 1 パッチをダウンロードして、プライマリ サーバーにインストールします。

a) ブラウザで Cisco EPN Manager のソフトウェア パッチ リストにアクセスします（「Software patches listing for Cisco Evolved Programmable Network Manager」参照してください）。

b) インストールする必要があるパッチ ファイル（UBF ファイル拡張子で終わるファイル）に対応する [ダウンロード（Download）] ボタンをクリックし、そのファイルをローカルに保存します。

c) 管理者特権を持つ ID を使用してプライマリ サーバーにログインし、[管理（Administration）]>[ライセンスおよびソフトウェア アップデート（Licenses and Software Updates）]>[ソフトウェア アップデート（Software Update）] を選択します。

d) ページ上部の [アップロード（Upload）] リンクをクリックし、パッチ ファイルの保存場所に移動します。

e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。

f) 次のオプションのいずれかを使用して、UBF ファイルをアップロードします。

1. ローカル コンピュータからアップロード

   - [アップデートのアップロード（Upload Update）] ウィンドウの [ローカルコンピュータからアップロード（Upload from local computer）] ラジオ ボタンをクリックします。

- [参照（Browse）] をクリックし、ファイルまで移動して [OK] をクリックします。アップロードが成功すると、[ファイル（Files）] タブの下にソフトウェアが表示されます。

2. サーバーのローカル ディスクからコピー

- [アップデートのアップロード（Upload Update）] ウィンドウの [サーバーのローカルディスクからコピー（Copy from server's local disk）] ラジオ ボタンをクリックします。
- [選択（Select ）] をクリックして、[ローカルディスクからファイルを選択（Select file from local disk）] ポップアップから UBF ファイルを選択し、[選択（Select）] をクリックします。アップロードが成功すると、[ファイル（Files）] タブの下にソフトウェアが表示されます。

g) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。

h) パッチ ファイルを選択し、[インストール（Install）] をクリックします。

i) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。

j) プライマリ サーバーでのインストールが完了したら、[ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、このパッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 2 セカンダリ サーバーに同じパッチをインストールします。

a) ブラウザで以下の URL にアクセスして、セカンダリ サーバーの Health Monitor（HM）Web ページを表示します。

https://*ServerIP***:8082**

ここで、*ServerIP* はセカンダリ サーバーの IP アドレスまたはホスト名です。

b) セカンダリ サーバーの認証キーの入力を求めるプロンプトが出されます。パスワードを入力してから、[ログイン（Login）] をクリックします。

c) HM Web ページの [ソフトウェア アップデート（Software Update）] リンクをクリックします。再び、認証キーの入力を求めるプロンプトが出されます。パスワードを入力し、[ログイン（Login）] を再びクリックします。

d) [アップデート ファイルのアップロード（Upload Update File）] をクリックし、パッチ ファイルを保存した場所を参照します。

e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。

f) ページ上部の [アップロード（Upload）] リンクをクリックします。

g) 次のオプションのいずれかを使用して、UBF ファイルをアップロードします。

1. ローカル コンピュータからアップロード

- [アップデートのアップロード（Upload Update）] ウィンドウの [ローカルコンピュータからアップロード（Upload from local computer）] ラジオ ボタンをクリックします。
- [参照（Browse）] をクリックし、ファイルまで移動して [OK] をクリックします。アップロードが成功すると、[ファイル（Files）] タブの下にソフトウェアが表示されます。

2. サーバーのローカル ディスクからコピー
   - [アップデートのアップロード（Upload Update）] ウィンドウの [サーバーのローカルディスクからコピー（Copy from server's local disk）] ラジオ ボタンをクリックします。
   - [選択（Select ）] をクリックして、[ローカルディスクからファイルを選択（Select file from local disk）] ポップアップから UBF ファイルを選択し、[選択（Select）] をクリックします。アップロードが成功すると、[ファイル（Files）] タブの下にソフトウェアが表示されます。

h) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。

i) パッチ ファイルを選択し、[インストール（Install）] をクリックします。

j) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。

k) セカンダリ サーバーでのインストールが完了したら、[ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、このパッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 3 両方のサーバーのパッチ ステータスが同一であることを次のように確認します。

a) 上記のステップ 1 と同じ方法でプライマリ サーバーにログインし、[ソフトウェア アップデート（Software Update）] ページにアクセスします。インストールされているすべてのパッチの [ステータス（Status）] 列で [インストール済み（Installed）] と表示されていることを確認します。

b) 上記のステップ 2 と同じ方法でセカンダリ サーバーのヘルス モニター Web ページにアクセスします。インストールされているすべてのパッチの [ステータス（Status）] 列で [インストール済み（Installed）] と表示されていることを確認します。

ステップ 4 サーバーを登録します。

詳細については、「Software patches listing for Cisco Evolved Programmable Network Manager」および Cisco EPN Manager の停止と再起動を参照してください。

ペアリング済み HA サーバーへのパッチ適用方法

現在の Cisco EPN Manager 実装に含まれているハイ アベイラビリティ サーバーのパッチ レベルが同一ではない場合、または両方の HA サーバーに新しいパッチを適用する必要がある場合は、次の手順を実行します。

ペアリング済み HA サーバーへのパッチの適用はサポートされていません。HA が設定されている状態では Cisco EPN Manager サーバーのアップデートが実行できないことを示すポップアップ エラー メッセージが表示されます。そのため、パッチを適用する前に、まずプライマリおよびセカンダリ サーバーを接続解除しなければなりません。

1. GUI での HA の削除 （44 ページ）の手順に従って、プライマリ サーバーとセカンダリ サーバーの接続を解除します。

2. 新しい HA サーバーへのパッチ適用方法 （17 ページ）の手順に従ってパッチを適用します。
3. ハイ アベイラビリティのセットアップ （8 ページ）の手順に従って HA の設定を復元します。

HA ステータスとイベントのモニター

次のトピックでは、HA 環境の全体的な正常性をモニターリングする方法を説明します。

ヘルス モニター Web ページの使用

ヘルス モニターは、HA 操作を管理する主要コンポーネントの 1 つです。ヘルス モニター インスタンスはアプリケーション プロセスとして両方のサーバーで実行され、各サーバーにそれぞれの Web ページが表示されます。LMP は、次の機能を実行します。

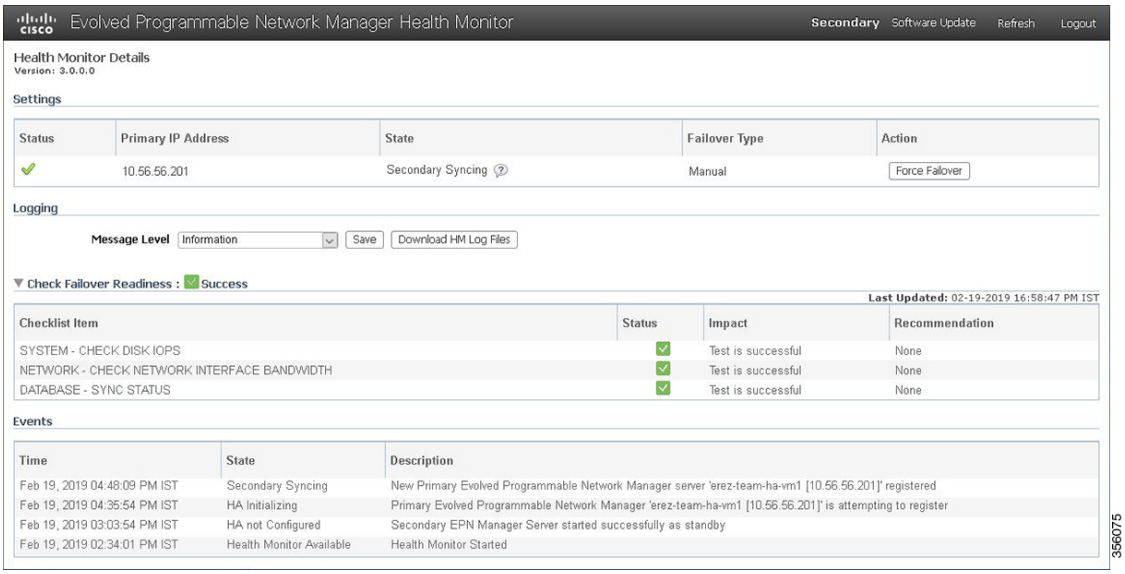
- HA に関連するデータベースおよびコンフィギュレーション データを同期します（Oracle Data Guard を使用して別途同期されるデータベースは除きます）。
- プライマリ サーバーとセカンダリ サーバーの間で 5 秒間隔でハートビート メッセージを交換し、サーバー間の通信が維持されていることを確認します。正常なサーバーは、もう一方の冗長サーバーからのハートビートを 3 回連続して受信できなかった場合、10 秒間待機します。その後、正常なサーバーは冗長サーバーで Web URL を開こうとします。この試行が失敗すると、正常なサーバーがアクティブ サーバーになります。
- 両方のサーバー上で使用可能なディスク容量を定期的に確認し、ストレージ容量が不足するとイベントを生成します。
- リンクされた HA サーバーの全体的な健全性を管理、制御、モニターします。プライマリ サーバーで障害が発生すると、ヘルス モニターによってセカンダリ サーバーがアクティブ化されます。

HA 設定が正常に完了した後は、ブラウザで以下の URL を指定することにより、プライマリ サーバーまたはセカンダリ サーバーのヘルス モニター Web ページにアクセスできます。

https://*ServerIP*:8082

ServerIP はプライマリ サーバーまたはセカンダリ サーバーの IP アドレスかホスト名です。

次の例は、**[セカンダリ同期中（Secondary Syncing）]** 状態のセカンダリ サーバーのヘルス モニター Web ページを示しています。



1	[設定（Settings）]：ヘルス モニターの状態と設定の詳細が 5 つのセクションに表示されます。	2	[ステータス（Status）]：HA セットアップの現在の機能ステータスを示します（緑色のチェック マークは、HA が有効化されていて機能していることを示します）。
3	[イベント（Events）]：現在の HA 関連イベントが最新のイベントを先頭に時系列順に表示されます。	4	[プライマリ IP アドレス（Primary IP address）]/[セカンダリ IP アドレス（Secondary IP address）]：ペアリングされたサーバーの IP アドレスが表示されます。このヘルス モニター インスタンスはセカンダリ サーバーで実行されているため、プライマリ サーバーの IP アドレスが表示されています。
5	[ダウンロード（Download）]：ヘルス モニター ログ ファイルをダウンロードできます。	6	[状態（State）]：このヘルス モニター インスタンスが実行されているサーバー（この例ではセカンダリ サーバー）の現在の状態が示されます。
7	[メッセージレベル（Message Level）]：現在のログ レベル（[エラー（Error）]、[情報（Informational）]、および [トレース（Trace）]）を示します。変更可能です。ログ レベルを変更するには、[保存（Save）] をクリックする必要があります。	8	タイトル バー：表示しているヘルス モニター Web ページの対象 HA サーバーと、[更新（Refresh）] および [ログアウト（Logout）] ボタンが表示されます。[ソフトウェアアップデート（Software Updates）] はセカンダリ サーバーに対してのみ表示されます。

9	[フェールオーバータイプ（Failover Type）]：設定されているフェールオーバー タイプ（[手動（Manual）] または [自動（Automatic）]）を示します。	10	[アクション（Actions）]：実行できるアクション（フェールオーバーやフェールバックなど）を示します。使用可能なアクションのみがここに表示されます。
11	[フェールオーバーの準備状況の確認（Check Failover Readiness）]：HA 設定を有効にした後のディスク速度、ネットワーク インターフェイス帯域幅、および DB 同期ステータスのチェック結果が表示されます。		

Note **準備状況の確認**によってセカンダリへのフェールオーバー（自動または手動）がブロックされることはありません。

HA ステータスと全体的な健全性の確認

Cisco EPN Manager の Web GUI または CLI を使用して、HA ステータスを確認できます。どちらの方法でも、サーバーの状態が一覧表示されます。状態については、HA の状態と遷移（40 ページ）で説明します。

Web GUI を使用して HA ステータスを確認するには、次のいずれかを実行します。

- Cisco EPN Manager の Web GUI で **[管理（Administration）]** > **[設定（Settings）]** > **[ハイアベイラビリティ（High Availability）]** の順に選択し、[HAステータス（HA Status）] を選択します。現在の HA ステータスとイベントの状態が表示されます。
- ヘルス モニターを使用します。「ヘルス モニター Web ページの使用 （20 ページ）」を参照してください。

CLI を使用して HA ステータスを確認するには、CLI 管理ユーザーとしていずれかのサーバーにログインします（Cisco EPN Manager サーバーとの SSH セッションの確立を参照）。**ncs ha status** コマンドは、次の例のような HA 固有の出力を提供します。

```
ncs ha status
[Role] Secondary [Primary Server] cisco-ha1(192.0.2.133) [State] Secondary Active [Failover
 Type] Manual
```

ncs status コマンドを使用して、ヘルス モニターとその他のサーバー プロセスを確認します。次の例のような出力が表示されます。

```
ncs status
Health Monitor Server is running. ( [Role] Primary [State] Primary Active )
Database server is running
FTP Service is disabled
TFTP Service is disabled
NMS Server is running.
```

```
SAM Daemon is running ...
DA Daemon is running ...
```

HA イベントの表示とカスタマイズ

HA 関連のアラームは、[アラームおよびイベント（Alarms and Events）] テーブルに一覧表示されます。これらのアラームのリストについては、『Cisco Evolved Programmable Network Manager のサポート対象アラーム』を参照してください。次の手順では、Web GUI でこれらのアラームを表示する方法について説明します。

必要に応じて、次の操作を行うこともできます。

- アラームの重大度を調整する
- アラームの通知を設定する

詳細については、システムの問題を示すサーバー内部 SNMP トラップの使用を参照してください。

HA 関連アラームを表示する手順は次のとおりです。

ステップ 1 **[モニター（Monitor）]>[モニターリング ツール（Monitoring Tools）]>[アラームおよびイベント（Alarms and Events）]** を選択し、[アラーム（Alarms）] タブをクリックします

ステップ 2 テーブルの右上にある [表示（Show）] ドロップダウンリストから [クイックフィルタ（Quick Filter）] を選択します。

ステップ 3 [メッセージ（Message）] フィールドに、**High Availability** と入力します。

HA エラー ロギングの使用

ディスク容量を節約して最大限のパフォーマンスを達成するために、HA エラー ロギングはデフォルトで無効になっています。HA に問題がある場合は、次の手順に従ってエラー ロギングを有効化してログ ファイルを確認します。

ステップ 1 問題のあるサーバーのヘルス モニターを起動します（ヘルス モニター Web ページの使用, on page 20を参照）。

ステップ 2 [ロギング（Logging）] 領域で、[メッセージレベル（Message Level）] ドロップダウンリストからエラー ロギング レベルを選択し、[保存（Save）] をクリックします。

ステップ 3 確認するログ ファイルをダウンロードします。

a. [ダウンロード（Download）] をクリックします。

.zip ファイルがデフォルトのダウンロード場所にコピーされます。

b. ログ ファイルを抽出し、ASCII テキスト エディタを使用して表示します。

フェールオーバーのトリガー

フェールオーバーでは、プライマリ サーバーで検出された障害への対応として、セカンダリ サーバーがアクティブ化されます。

ヘルス モニターは、2 台の HA サーバー間で交換されるハートビート メッセージを使用して障害状態を検出します。ハートビート メッセージが 5 秒ごとに送信され、セカンダリ サーバーからのハートビート メッセージにプライマリ サーバーが 3 回連続して応答しないと、ヘルス モニターはプライマリ サーバーに障害が発生したと見なします。ヘルス チェック中に、ヘルス モニターはアプリケーション プロセスのステータスとデータベースの健全性もチェックします。これらのチェックに対して適切な応答がない場合は、障害が発生したものと見なされます。

セカンダリ サーバーの HA システムがプライマリ サーバーのプロセス障害を検出するのに約 15 秒かかります。ネットワークの問題によってセカンダリ サーバーがプライマリ サーバーに接続できない場合、障害を検出してフェールオーバーを開始するまでにさらに時間がかかることがあります。また、セカンダリ サーバーでのアプリケーション プロセスが完全に機能するようになるまでにも時間がかかることがあります。

ヘルス モニターは障害を検出するとすぐに電子メール通知を送信します。この電子メールには、障害ステータスに加え、セカンダリ サーバーのヘルス モニター Web ページへのリンクも記載されます。HA に自動フェールオーバーが設定されている場合、セカンダリ サーバーは自動的にアクティブ化されます。

手動フェールオーバーを実行する手順は次のとおりです。

Before you begin

- プライマリ サーバーとセカンダリ サーバーの状態を確認します。
- 2 台のサーバー間の接続を検証します。
- 仮想 IP アドレスを使用していない場合は、トラップと syslog を両方のサーバーに転送するようにすべてのデバイスが設定されていることを確認します。

ステップ 1 電子メール通知に記載されている Web リンクを使用するか、ブラウザで次の URL を入力して、セカンダリ サーバーのヘルス モニター Web ページにアクセスします。

https://*ServerIP*:8082

ステップ 2 [フェールオーバー（Failover）] をクリックします。

フェールバックのトリガー

フェールバックとは、オンライン状態に戻ったプライマリ サーバーをアクティブ化するプロセスのことです。また、アクティブ ステータスをセカンダリ サーバーからプライマリ サーバーに移して、セカンダリ サーバーでのアクティブなネットワーク モニターリング プロセスを停止します。

フェールバックがトリガーされると、セカンダリ サーバーはその現行のデータベース情報と更新済みファイルをプライマリ サーバーに複製します。セカンダリ サーバーからプライマリ サーバーへのフェールバックを完了するまでの所要時間は、複製する必要のあるデータの量と使用可能なネットワーク帯域幅によって異なります。

データが正常に複製されると、HA はプライマリ サーバーの状態を [プライマリアクティブ（Primary Active）] に変更し、セカンダリ サーバーの状態を [セカンダリ同期中（Secondary Syncing）] に変更します。

フェールバック中のセカンダリ サーバーの可用性は、フェールオーバー後に Cisco EPN Manager がプライマリ サーバーに再インストールされたかどうかによって次のように異なります。

- フェールオーバー後に Cisco EPN Manager がプライマリ サーバーに再インストールされた場合は、完全なデータベース コピーが必要になり、フェールバック プロセス中はセカンダリ サーバーを使用できません。
- Cisco EPN Manager がプライマリ サーバーに再インストールされていない場合は、プライマリ サーバーでプロセスが開始されてセカンダリ サーバーで停止されるまでの期間を除き、セカンダリ サーバーを使用できます。両方のサーバーの Health Monitor Web ページにアクセスして、フェールバックの進行状態をモニターすることができます。さらに、ユーザーはセカンダリ サーバーに接続して、通常のすべての機能を使用することもできます。

以下の手順で説明するように、常に手動でフェールバックをトリガーする必要があります。（注）

- フェールバックの進行中は、設定またはプロビジョニングのアクティビティを開始しないでください。
- フェールバックが正常に完了すると、セカンダリ サーバーがダウンして、制御がプライマリ サーバーに切り替わります。このプロセス中は、しばらくの間、ユーザーが Cisco EPN Manager にアクセスできなくなります。

Before you begin

- プライマリ サーバーとセカンダリ サーバーの状態を確認します。
- 2 台のサーバー間の接続を検証します。
- 仮想 IP アドレスを使用していない場合は、トラップと syslog を両方のサーバーに転送するようにすべてのデバイスが設定されていることを確認します。
- プライマリ サーバーに Cisco EPN Manager を再インストールしてオフライン Geo マップを使用する場合は、フェールバックをトリガーする前に、プライマリ サーバーに Geo マッ

プリソースを再インストールする必要があります。『Cisco Evolved Programmable Network Manager Installation Guide』を参照してください。

ステップ 1 電子メール通知に記載されているリンクを使用するか、ブラウザで次の URL を入力して、セカンダリ サーバーのヘルス モニター Web ページにアクセスします。

https://*ServerIP*:8082

ステップ 2 [フェールバック（Failback）] をクリックします。

フェールオーバーの強制実行

強制フェールオーバーは、プライマリ サーバーが稼働している間に、セカンダリ サーバーをアクティブにするプロセスです。このオプションは、たとえば、HA セットアップは完全に機能しているかどうかをテストする場合に使用します。

強制フェールオーバーを使用できるのは、プライマリがアクティブで、セカンダリが「セカンダリ同期中（Secondary Syncing）」状態であり、すべてのプロセスが両方のサーバーで実行中の場合に限られます。プライマリ サーバーがダウンしている場合、強制フェールオーバーは無効になります。この状況では、通常のフェールオーバーのみが有効です。

強制フェールオーバーが完了すると、セカンダリ サーバーがアクティブになり、プライマリ サーバーは自動的にスタンバイ状態で再起動します。通常のフェイルバックをトリガーすると、元の通りプライマリ サーバーがアクティブになり、セカンダリ サーバーがスタンバイ状態になります。

ステップ 1 「ヘルス モニター Web ページの使用」の手順に従って、セカンダリサーバーのヘルスモニター Web ページにアクセスします。

ステップ 2 [強制フェールオーバー（Force Failover）] ボタンをクリックして強制フェールオーバーをトリガーします。強制フェールオーバーは 2 ～ 3 分で完了します。

その他の HA イベントに対する応答

HA 関連のすべてのイベントは、[HA ステータス（HA Status）] ページ、Health Monitor Web ページ、および Cisco EPN Manager の [アラームおよびイベント（Alarms and Events）] ページに表示されます。ほとんどのイベントには、オペレータの応答は不要ですが、フェールオーバーおよびフェールバックのトリガーは例外です。次のトピックで説明するように、複雑なイベントもいくつかあります。

- HA 登録が失敗した場合 （27 ページ）
- ネットワークがダウンしている場合（自動フェールオーバー） （28 ページ）

HA 登録が失敗した場合

HA 登録が失敗すると、各サーバーの HA 状態が以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[HA 初期化中（HA Initializing）]	元の状態：[HA 初期化中（HA Initializing）]
次の状態：[HA 未設定（HA not Configured）]	次の状態：[HA 未設定（HA not Configured）]

HA 登録の失敗から回復するには、次の手順に従います。

ステップ 1 ping または他のツールを使用して、2 台の Cisco EPN Manager サーバー間のネットワーク接続を確認します。プライマリ サーバーからセカンダリ サーバーに接続できること、その逆も可能であることを確認します。

ステップ 2 ゲートウェイ、サブネットマスク、仮想IPアドレス（設定されている場合）、サーバーのホスト名、DNS、NTP 設定がすべて正しいことを確認します。

ステップ 3 設定された DNS および NTP サーバーにプライマリ サーバーとセカンダリ サーバーから接続可能であること、そして DNS および NTP サーバーの両方が遅延や他のネットワーク固有の問題を伴うことなく応答していることを確認します。

ステップ 4 すべての Cisco EPN Manager ライセンスが正しく設定されていることを確認します。

ステップ 5 接続または設定の問題を解決したら、プライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （11 ページ）の手順を再試行します。

ネットワークがダウンしている場合（自動フェールオーバー）

フェールオーバー タイプが [自動（Automatic）] に設定されている場合、2 台の Cisco EPN Manager サーバー間のネットワーク接続が失われると、それぞれのサーバーの HA 状態が以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリのフェールオーバー（Secondary Failover）]
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

セカンダリ サーバーがアクティブであることを示す電子メール通知を受信します。

ステップ 1 2台のサーバー間のネットワーク接続を確認し、復元します。ネットワーク接続が復旧し、セカンダリ サーバーがアクティブなことをプライマリ サーバーが検出できるようになったら、プライマリ サーバー上のすべてのサービスが自動的に再開し、パッシブ状態になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ同期中（Primary Syncing）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

ステップ 2 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ同期中（Primary Syncing）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ フェールバック（Secondary Failback）]

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ ポスト フェールバック（Secondary Post Failback）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

ネットワークがダウンしている場合（手動フェールオーバー）

フェールオーバー タイプが [手動（Manual）] に設定されている場合、2 台の Cisco EPN Manager サーバー間のネットワーク接続が失われると、それぞれのサーバーの HA 状態が以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]

各サーバーがもう一方のサーバーを失ったことを通知する電子メールを受信します。

ステップ 1 2 台のサーバー間のネットワーク接続を確認し、必要に応じて復元します。

ネットワーク接続が復元されると、次ように状態が遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	元の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

管理者による応答は不要です。

ステップ 2 何らかの理由でネットワーク接続を復元できない場合は、セカンダリ サーバーの HM Web ページを使用して、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	元の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリのフェールオーバー（Secondary Failover）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

セカンダリ サーバーがアクティブになったことを通知する電子メールを受信します。

ステップ 3 2台のサーバー間のネットワーク接続を確認し、復元します。ネットワーク接続が復旧し、セカンダリ サーバーがアクティブなことをプライマリ サーバーが検出したら、プライマリ サーバー上のすべてのサービスが自動的に再開し、パッシブ状態になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ同期中（Primary Syncing）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

ステップ 4 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。

以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ同期中（Primary Syncing）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ フェールバック（Secondary Failback）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ ポスト フェールバック（Secondary Post Failback）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

プロセスを再開できない場合（自動フェールオーバー）

Cisco EPN Manager Health Monitor プロセスは、失敗した Cisco EPN Manager サーバー プロセスの再開を試行します。通常、そのような障害が発生した時点でのプライマリ サーバーとセカン

ダリ サーバーの状態は、[プライマリ アクティブ（Primary Active）] および [セカンダリ同期中（Secondary Syncing）] となっているはずです。

HM がプライマリ サーバーで重要なプロセスを再開できない場合は、プライマリ サーバーは障害が発生したものとみなされます。現在設定されているフェールオーバー タイプが [自動（automatic）] の場合、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリが状態を確認できません（Primary Uncertain）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリのフェールオーバー（Secondary Failover）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

このプロセスが完了すると、セカンダリ サーバーがアクティブになったことを通知する電子メールでの通知を受信します。

ステップ 1 プライマリ サーバーを再起動し、稼働していることを確認します。プライマリ サーバーが再起動すると、その状態は [プライマリ同期中（Primary Syncing）] になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ フェールオーバー（Primary Failover）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリがフェールバックの準備中（Primary Preparing for Failback）]	次の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ同期中（Primary Syncing）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

ステップ 2 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ同期中（Primary Syncing）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ フェールバック（Secondary Failback）]

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ ポスト フェールバック（Secondary Post Failback）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

プロセスをリスタートできない場合（手動フェールオーバー）

Cisco EPN Manager Health Monitor プロセスは、失敗した Cisco EPN Manager サーバー プロセスの再開を試行します。通常、そのような障害が発生した時点でのプライマリ サーバーとセカンダリ サーバーの状態は、[プライマリ アクティブ（Primary Active）] および [セカンダリ同期中（Secondary Syncing）] となっているはずです。HM がプライマリ サーバーで重要なプロセスを再開できない場合は、プライマリ サーバーは障害が発生したものとみなされます。その場合、障害を通知する電子メールを受信します。現在設定されているフェールオーバー タイプが [手動（Manual）] の場合、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリが状態を確認できません（Primary Uncertain）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]

ステップ 1 セカンダリ サーバーで、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリが状態を確認できません（Primary Uncertain）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリのフェールオーバー（Secondary Failover）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

ステップ 2 プライマリ サーバーを再起動し、稼働していることを確認します。プライマリ サーバーが再起動すると、プライマリ サーバーの HA 状態は [プライマリ同期中（Primary Syncing）] になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ フェールオーバー（Primary Failover）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリがフェールバックの準備中（Primary Preparing for Failback）]	次の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ同期中（Primary Syncing）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

ステップ 3 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ同期中（Primary Syncing）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ フェールバック（Secondary Failback）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ ポスト フェールバック（Secondary Post Failback）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

同期中にプライマリ サーバーが再起動した場合（手動フェールオーバー）

セカンダリ サーバーとの同期中にプライマリ Cisco EPN Manager サーバーが再起動された場合は、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリ単独（Primary Alone）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

[プライマリ単独（Primary Alone）] および [プライマリ アクティブ（Primary Active）] 状態への遷移は、プライマリ サーバーがオンライン状態に戻った直後に行われます。管理者による応答は必要ありません。

同期中にセカンダリ サーバーが再起動した場合

プライマリ サーバーとの同期中にセカンダリ Cisco EPN Manager サーバーが再起動された場合は、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	元の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

管理者による応答は必要ありません。

HA サーバーが両方ともダウンしている場合

プライマリ サーバーおよびセカンダリ サーバーが同時にダウンした場合、次の手順で説明するように正しい順序で稼働中の状態に戻すことで復旧できます。

ステップ 1 セカンダリ サーバーと、セカンダリ サーバー上で稼働する Cisco EPN Manager インスタンスを再起動します。何らかの理由でセカンダリ サーバーを再起動できない場合は、HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合 （36 ページ）を参照してください。

ステップ 2 セカンダリ サーバーで Cisco EPN Manager が稼働中になったら、セカンダリ サーバーの Health Monitor Web ページにアクセスします。セカンダリ サーバーの状態が [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] に遷移します。

ステップ 3 プライマリ サーバーと、プライマリ サーバー上で稼働する Cisco EPN Manager インスタンスを再起動します。Cisco EPN Manager がプライマリ サーバー上で稼働している場合、プライマリ サーバーは自動的にセカンダリ サーバーと同期します。これを確認するには、プライマリ サーバーの Health Monitor Web ページにアクセスします。2 台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

両方の HA サーバーの電源がダウンしている場合

プライマリ サーバーおよびセカンダリ サーバーの電源が同時にダウンした場合、次の手順で説明するように正しい順序で稼働中の状態に戻すことで復旧できます。

ステップ 1 セカンダリ サーバーと、セカンダリ サーバー上で稼働する Cisco EPN Manager インスタンスの電源をオンにします。この状態ではプライマリ サーバーに到達できないため、セカンダリ HA の再起動は失敗します。ただし、セカンダリ サーバーの HM プロセスは実行され、エラーが表示されます。

ステップ 2 セカンダリ サーバーで Cisco EPN Manager が稼働中になったら、セカンダリ サーバーの HM Web ページにアクセスします（ヘルス モニター Web ページの使用 （20 ページ）を参照）。セカンダリ サーバーが [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] 状態に遷移します。

ステップ 3 プライマリ サーバーと、プライマリ サーバー上で稼働する Cisco EPN Manager インスタンスの電源をオンにします。

ステップ 4 Cisco EPN Manager がプライマリ サーバー上で稼働している場合、プライマリ サーバーは自動的にセカンダリ サーバーとの同期を開始します。これを確認するには、プライマリ サーバーの HM Web ページにアクセスします。2 台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

ステップ 5 セカンダリ サーバーと、セカンダリ サーバー上で稼働する Cisco EPN Manager インスタンスを再起動します。この時点では、プロセスのすべてがセカンダリ サーバーで実行されているわけではないため、この操作が必要です。

何らかの理由でセカンダリ サーバーを再起動できない場合は、HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合 （36 ページ）を参照してください。

ステップ 6 Cisco EPN Manager がセカンダリ サーバーでの再起動を完了したときには、すべてのプロセスが実行されています。これを確認するには、**ncs ha status** コマンドを実行します。

HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合

両方の HA サーバーが同時にダウンし、セカンダリサーバーが再起動しない場合は、セカンダリサーバーが交換できるまで、プライマリサーバーをスタンドアロンサーバーとして使用するために、プライマリサーバーから HA 設定を削除する必要があります。

以下の手順では、すでにセカンダリ サーバーの再起動を試み、再起動に失敗したものとしています。

ステップ 1 Cisco EPN Manager のプライマリ インスタンスの再起動を試みます。プライマリ サーバーの再起動が可能である場合は、HA 設定の削除が必要であることを示すエラー メッセージが表示されて再起動が中断されます。

ステップ 2 プライマリ サーバーとの CLI セッションを開きます（Cisco EPN Manager サーバーとの SSH セッションの確立を参照）。

ステップ 3 次のコマンドを入力して、プライマリ サーバーの HA 設定を削除します。

```
ncs ha remove
```

（注） HA 設定を削除すると、プライマリサーバーは以前のセカンダリサーバーに登録できなくなるため、セカンダリサーバーを再インストールする必要があります。

ステップ 4 HA 設定を削除することを確認します。

エラー メッセージが表示されることなく Cisco EPN Manager のプライマリ インスタンスの再起動が可能になり、スタンドアロン サーバーとして使用できるようになります。セカンダリサーバーを交換できる場合は、プライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （11 ページ）の説明に従って続行します。

プライマリ サーバーの交換方法

通常の状況下では、プライマリ サーバーの状態は[プライマリアクティブ（Primary Active）]、セカンダリ サーバーの状態は[セカンダリ同期中（Secondary Syncing）]になります。何らかの理由でプライマリ サーバーに障害が発生した場合、セカンダリ サーバーへのフェールオーバーが自動または手動で行われます。

HA への完全なアクセスを復旧するには、新しいハードウェアを使用してプライマリ サーバーをインストールする必要があることがあります。この場合、次の手順に従うことで、データを失うことなく新しいプライマリ サーバーを起動できます。

始める前に

セカンダリ サーバーでHAを設定したときに指定したパスワード（認証キー）があることを確認します。以下の手順では、これが必要となります。

ステップ 1 セカンダリ サーバーが [セカンダリアクティブ（Secondary Active）] 状態であることを確認します。プライマリ サーバーで手動フェールオーバーが設定されている場合は、セカンダリ サーバーへのフェールオーバーをトリガーする必要があります（フェールオーバーのトリガー （24 ページ）を参照）。

ステップ 2 交換する古いプライマリ サーバーがネットワークから切断していることを確認します。

ステップ 3 新しいプライマリ サーバーが使用可能な状態であることを確認します。これには、新しいサーバーをネットワークに接続し、古いプライマリ サーバーと同様に設定する（IP アドレス、サブネット マスクなど）ことが含まれます。セカンダリ サーバーに HA をインストールするときに使用した同じ認証キーを入力する必要があります。

ステップ 4 プライマリサーバーとセカンダリサーバーが同じパッチレベルであることを確認します。プライマリサーバーを置換する場合は、次の手順を実行する必要があります。

a) セカンダリサーバーの CLI で次のコマンドを実行して、プライマリサーバーとセカンダリサーバーが TOFU モードになっていることを確認します。

```
admin# ncs certvalidation certificate-check trust-on-first-use trustzone
system
```

b) セカンダリサーバー管理 CLI にログインします。

c) セカンダリサーバーの CLI で次のコマンドを実行します。

```
admin# ncs certvalidation tofu-certs deletecert host
<primaryserver's-IP-address appended with "_8082">
```

例：**ncs certvalidation tofu-certs deletecert host 10.56.58.91_8082**

これは、プライマリサーバーとセカンダリサーバー間の通信を再確立するために必要です。

ステップ 5 次に示すように、IP テーブルのエントリを更新します。

- プライマリの場合：1522 ポートの iptables にセカンダリ IP アドレスと仮想 IP アドレスを追加します（設定されている場合）。
- セカンダリの場合：1522 ポートの iptables にプライマリ IP アドレスと仮想 IP アドレスを追加します（設定されている場合）。

例:

```
iptables -A INPUT -s IP address -p tcp --dport 1522 -j ACCEPT
iptables -A INPUT -s IP address -j ACCEPT
```

ステップ 6 セカンダリ サーバーから新たにインストールしたプライマリ サーバーへのフェールバックをトリガーします。新しいプライマリ HA サーバーへのフェールバック中にはデータベースのフル コピーが実行されるため、使用可能な帯域幅とネットワーク遅延によってはこの処理の完了に時間がかかります。2 台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[HA 未設定（HA not configured）]	元の状態：[セカンダリ アクティブ（Secondary Active）]

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ フェールバック（Secondary Failback）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ ポスト フェールバック（Secondary Post Failback）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

スプリット ブレイン シナリオからの回復方法

スプリット ブレインのシナリオでは、プライマリ サーバーとセカンダリ サーバーの両方が同時にアクティブになります。これは、ネットワークの停止または一時的にダウンしたリンクが原因となっている可能性があります。ただし、プライマリ サーバーはセカンダリ サーバーを継続的にチェックするため、接続が再確立されてセカンダリ サーバーがアクティブになると、プライマリ サーバーはダウンします。

「スプリットブレーン状況」が発生するまれな状況では、データが失われる可能性が常にあります。この場合、以下の手順に従い、新しく追加されたデータをセカンダリに保存し、追加されたデータをプライマリには保存しないようにすることができます。

ステップ 1 ネットワークが起動し、セカンダリ サーバーが起動すると、プライマリ サーバーはスタンバイ データベースを使用して自動的に再起動します。プライマリ サーバーの HA ステータスはまず「プライマリフェールオーバー（Primary Failover）」になり、その後「プライマリ同期中（Primary Syncing）」に遷移します。これを確認するには、プライマリ サーバーの Health Monitor Web ページにログオンします。

ステップ 2 プライマリ サーバーのステータスが「プライマリ同期中（Primary Syncing）」になったら、ユーザーが Web ブラウザを使用してセカンダリ サーバーの Cisco EPN Manager ページ（たとえば、https://server-ip-address:443）にログインできることを確認します。確認が済むまで、手順を進めないでください。

ステップ 3 セカンダリ サーバーにアクセスできることが確認できたら、セカンダリ サーバーのヘルス モニター Web ページから、フェールバックを開始します（フェールバックのトリガー （25 ページ）を参照）。プライマリ サーバーへのスイッチオーバーが完了するまで、セカンダリ サーバーでモニターリング アクティビティを続行できます。

セカンダリ サーバーがダウンした場合

このシナリオでは、スタンバイ サーバーとして機能しているセカンダリ サーバーがダウンします。

セカンダリ サーバーを再び稼働させる手順は次のとおりです。

ステップ 1 セカンダリ サーバーの電源を入れます。

ステップ 2 セカンダリ サーバーで Cisco EPN Manager を起動します。

ステップ 3 プライマリ サーバーで、プライマリ サーバーの HA ステータスが「プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）」から「プライマリアクティブ（Primary Active）」に変わっていることを確認します。[管理（Administration）] > [設定（Settings）] > [ハイアベイラビリティ（High Availability）] > [HA設定（HA Configuration）] に移動します。

ステップ 4 ブラウザに URL **https://*serverIP*:8082** を入力して、セカンダリ サーバーのヘルス モニター ページにログインします。

ステップ 5 セカンダリ サーバーの HA ステータスが「セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）」から「セカンダリ同期中（Secondary Syncing）」に変わっていることを確認します。
上記のステータスが表示されたら、それ以上の操作は必要ありません。ただし、HA ステータスが変わらない場合、セカンダリ サーバーは自動的に回復できません。この場合は、次の手順に進みます。

ステップ 6 プライマリ サーバーで HA 設定を削除します。[管理（Administration）] > [設定（Settings）] > [ハイアベイラビリティ（High Availability）] > [HA設定（HA Configuration）] に移動して、[削除（Remove）] をクリックします。

ステップ 7 セカンダリ サーバーをプライマリ サーバーに登録します。を参照してくださいプライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （11 ページ）。
HA 登録が成功した場合、それ以上の操作は必要ありません。ただし、HA 登録が失敗した場合は、セカンダリ サーバーでハードウェアまたはソフトウェアの損失が発生している可能性があります。この場合は、次の手順に進みます。

ステップ 8 プライマリ サーバーで HA 設定を削除します。

ステップ 9 プライマリ サーバーと同じリリースおよびパッチ（該当する場合）を使用してセカンダリ サーバーを再インストールします。

ステップ 10 セカンダリ サーバーをプライマリ サーバーに登録します。を参照してくださいプライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （11 ページ）。

データベースの同期の問題を解決する方法

データベースの同期の問題を解決するには、プライマリ サーバーが「プライマリ アクティブ」状態で、セカンダリ サーバーが「セカンダリ同期」状態になっているときに、次の手順に従います。

ステップ 1 HA を削除します（CLI での HA の削除 （45 ページ）およびGUI での HA の削除 （44 ページ）を参照）。

ステップ 2 プライマリ サーバーとセカンダリ サーバーの両方が「HA未設定（HA Not Configured）」状態になったら、HA の設定を実行します。ハイ アベイラビリティのセットアップ （8 ページ） を参照してください。

ハイ アベイラビリティの参照情報

次のトピックでは、HA の参考情報を提供します。

HA コンフィギュレーション モード

HA コンフィギュレーション モードは、完全な HA 設定の全体的なステータスを表します（サーバー固有の HA 状態とは異なります）。

モード	説明
HA未設定（HA Not Configured）	このサーバーでは HA が設定されていません。
HA 初期化中（HA Initializing）	プライマリ サーバーとセカンダリ サーバー間の HA 設定プロセスが開始されました。
HA対応（HA Enabled）	プライマリ サーバーとセカンダリ サーバー間で HA が有効になっています。
HA単独（HA Alone）	1 台のサーバーがダウンしているか、同期していないか、到達不能であるため、サーバーが単独で稼働しています。

HA の状態と遷移

次の表に、HA の状態を示します（ユーザーによる応答が不要なものも含む）。これらの状態は、[HAステータス（HA Status）] ページ（**[管理（Administration）] > [設定（Settings）] > [ハイアベイラビリティ（High Availability）] > [HAステータス（HA Status）]**）またはヘルス モニターで確認できます。HA イベントの一覧と、イベントの有効化、無効化、および調整の手順については、サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送を参照してください。

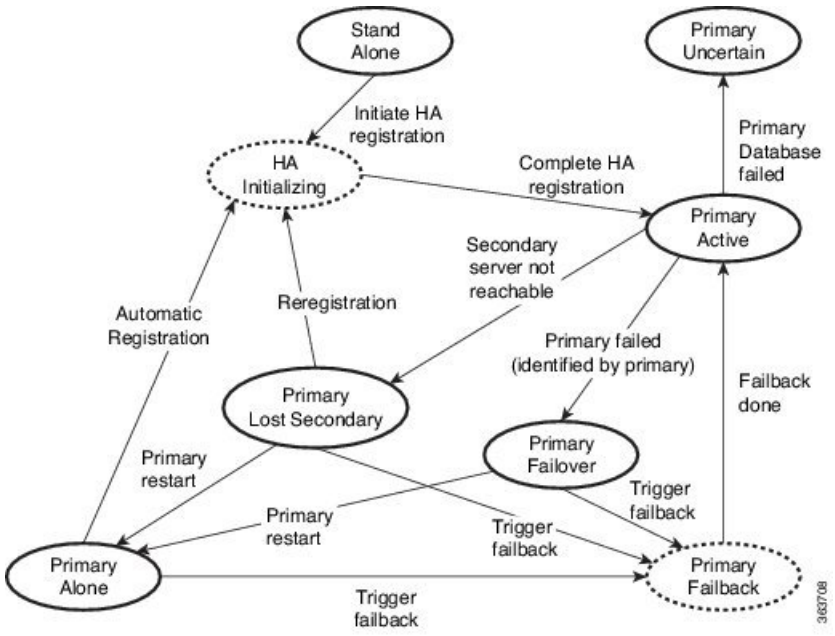
状態	**[サーバー（Server）]**	説明
スタンドアロン（Stand Alone）	両方	このサーバーでは HA が設定されていません。
プライマリ単独（Primary Alone）	プライマリ（Primary）	プライマリ サーバーは、セカンダリ サーバーとの接続を失った後に再起動しました（この状態で実行されるのはヘルス モニターのみです）。
HA 初期化中（HA Initializing）	両方	プライマリ サーバーとセカンダリ サーバー間の HA 設定プロセスが開始されました。

プライマリ アクティブ（Primary Active）	プライマリ（Primary）	プライマリ サーバーは現在アクティブであり、セカンダリ サーバーと同期中です。
プライマリ データベースのコピーに失敗しました（Primary Database Copy Failed）	プライマリ（Primary）	再起動したプライマリ サーバーがデータ ギャップを検出してアクティブなセカンダリ サーバーからのデータ コピーをトリガーし、データベースのコピーに失敗しました。プライマリ サーバーは再起動すると必ず、自身が 24 時間以上ダウンしていたためにデータ ギャップが生じていないかを確認します。このコピーが失敗することはほとんどありませんが、まれに失敗した場合は、データベース コピーが正常に終了するまで、プライマリへのフェールバックの試行はすべてブロックされます。データベース コピーが正常に終了するとすぐに、プライマリ サーバーの状態が [プライマリ同期中（Primary Syncing）] に設定されます。
プライマリ フェールオーバー（Primary Failover）	プライマリ（Primary）	プライマリ サーバーで障害が検出されました。
プライマリ フェールバック（Primary Failback）	プライマリ（Primary）	ユーザーによってトリガーされたフェールバックが進行中です。
プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）	プライマリ（Primary）	プライマリ サーバーは、セカンダリ サーバーと通信できません。
プライマリがフェールバックの準備中（Primary Preparing for Failback）	プライマリ（Primary）	フェールオーバー後にプライマリ サーバーがスタンバイ モードで起動しました（セカンダリ サーバーがまだアクティブであるため）。プライマリ サーバーでフェールバックの準備ができると、その状態が [プライマリ同期中（Primary Syncing）] に設定されます。
プライマリ同期中（Primary Syncing）	プライマリ（Primary）	プライマリ サーバーは、データベースおよびコンフィギュレーション ファイルを、アクティブなセカンダリ サーバーと同期しています。フェールオーバー後にプライマリ プロセスが起動すると（かつセカンダリ サーバーがアクティブ ロールを果たしている場合）、この状態になります。

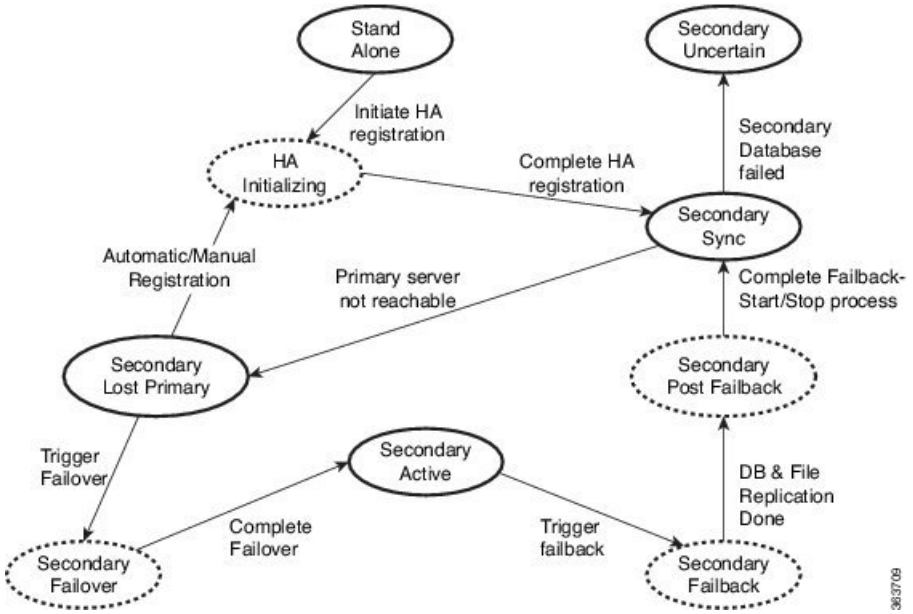
プライマリが状態を確認できません（Primary Uncertain）	プライマリ（Primary）	プライマリ サーバーのアプリケーション プロセスがデータベースに接続できません。
セカンダリ単独（Secondary Alone）	セカンダリ（Secondary）	プライマリ サーバーの再起動後、セカンダリ サーバーからプライマリ サーバーに到達できません。
セカンダリ同期中（Secondary Syncing）	セカンダリ（Secondary）	セカンダリ サーバーは、データベースおよびコンフィギュレーション ファイルをプライマリ サーバーと同期しています。
セカンダリ アクティブ（Secondary Active）	セカンダリ（Secondary）	プライマリ サーバーからセカンダリ サーバーへのフェールオーバーが正常に完了しました。
セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）	セカンダリ（Secondary）	セカンダリ サーバーがプライマリ サーバーに接続できません（この状態は、プライマリ サーバーで障害が発生した場合、またはネットワーク接続が失われた場合に発生します）。 自動フェールオーバーの場合、セカンダリ サーバーは自動的に [セカンダリアクティブ（Secondary Active）] 状態に移ります。手動フェールオーバーの場合は、フェールオーバーをトリガーしてセカンダリ サーバーをアクティブにする必要があります（フェールオーバーのトリガー（24 ページ）を参照）。
セカンダリのフェールオーバー（Secondary Failover）	セカンダリ（Secondary）	フェールオーバーがトリガーされて進行中です。
セカンダリ フェールバック（Secondary Failback）	セカンダリ（Secondary）	フェールバックがトリガーされ、データベースおよびファイルの複製が進行中です。
セカンダリ ポスト フェールバック（Secondary Post Failback）	セカンダリ（Secondary）	フェールバックがトリガーされ、関連するプロセスの停止と再起動が進行中です。データベースおよびコンフィギュレーション ファイルがセカンダリ サーバーからプライマリ サーバーに複製されました。プライマリ サーバーのステータスが [プライマリアクティブ（Primary Active）] に変わり、セカンダリ サーバーの HA ステータスが [セカンダリ同期中（Secondary Syncing）] に変わります。

セカンダリが状態を確認できません（Secondary Uncertain）	セカンダリ（Secondary）	セカンダリ サーバーのアプリケーション プロセスが、サーバーのデータベースに接続できません。

次の図は、プライマリ サーバーの HA 状態の変化を示しています。



次の図は、セカンダリ サーバーの HA 状態の変化を示しています。



ハイ アベイラビリティ CLI コマンド リファレンス

次の表に、HA 管理に使用できる CLI コマンドをリストします。これらのコマンドを使用するには、管理 CLI ユーザーとしてログインする必要があります。出力には、使用しているサーバーのステータスが反映されます。つまり、プライマリ サーバーから **ncs ha status** を実行すると、Cisco EPN Manager によってプライマリ サーバーのステータスが報告されます。

Table 3: ハイ アベイラビリティ コマンド

コマンド	説明
ncs ha ?	コマンドの使用方法に関するメッセージを表示します。
ncs ha authkey *newAuthkey*	認証キーを *newAuthKey* に更新します。
ncs ha remove	HA 設定を削除します。
ncs ha status	HA の現在のステータスを表示します。

HA 認証キーのリセット

管理者権限を持つユーザーは、**ha authkey** コマンドを使用して HA 認証キーを変更できます。新しい認証キーがパスワード標準を満たすようにする必要があります。

ステップ 1 Cisco EPN Manager CLI 管理ユーザーとしてプライマリ サーバーにログインします（Cisco EPN Manager サーバーとの SSH セッションの確立を参照）。

ステップ 2 コマンドラインに次のように入力します。

```
ha authkey newAuthKey
```

newAuthKey は新しい認証キーです。

GUI での HA の削除

既存の HA 実装を削除するには、以下の手順で説明するように、GUI を使用するのが最も簡単な方法です。また、コマンド ラインから HA 設定を削除することもできます。

この方法を使用するには、プライマリ Cisco EPN Manager サーバーの現在の状態が「プライマリアクティブ（Primary Active）」であることを確認する必要があります。何らかの理由でセカンダリ サーバーが現在アクティブである場合、フェールバックが完了してセカンダリ サーバーが自動的に再起動してから、フェールバックを実行して HA 設定を削除します。

ステップ 1 管理者権限を持つユーザー ID を使用してプライマリ Cisco EPN Manager サーバーにログインします。

ステップ 2 [管理（Administration）]>[設定（Settings）]>[ハイ アベイラビリティ（High Availability）]>[HA 設定（HA Configuration）] の順に選択します。

ステップ 3 [削除（Remove）] を選択します。HA 設定の削除には 3 ～ 4 分かかります。

削除が完了したら、ページに表示されている HA 設定モードが「HA 未設定（HA not Configured）」になっていることを確認します。

CLI での HA の削除

何らかの理由でプライマリ サーバー上の Cisco EPN Manager GUI にアクセスできない場合、管理者は以下の手順に従い、コマンド ラインから HA 設定を削除することができます。

この方法を使用するには、プライマリ Cisco EPN Manager サーバーの現在の状態が「プライマリアクティブ（Primary Active）」であることを確認する必要があります。何らかの理由でセカンダリ サーバーが現在アクティブである場合、フェールバックが完了してセカンダリ サーバーが自動的に再起動してから、フェールバックを実行して HA 設定を削除します。

ステップ 1 CLI を使用してプライマリ サーバーに接続します。「configure terminal」モードにしないでください。

ステップ 2 コマンドラインに次のように入力します。

admin# **ncs ha remove**。

アップグレード中の HA の削除

HA を使用した Cisco EPN Manager 実装をアップグレードするには、以下の手順に従います。

ステップ 1 GUI を使用して、プライマリ サーバーから HA 設定を削除します。「GUI での HA の削除 （44 ページ）」を参照してください。

ステップ 2 必要に応じてプライマリ サーバーをアップグレードします。

ステップ 3 現在のイメージを使用してセカンダリ サーバーを再インストールします。

セカンダリ サーバーを以前のバージョンやベータ版からアップグレードすることはできません。セカンダリ サーバーは常に新規インストールでなければなりません。

ステップ 4 アップグレードが完了したら、HA 設定プロセスを再度実行します。

復元中の HA の削除

Cisco EPN Manager は、ハイ アベイラビリティ関連の構成時の設定をバックアップしません。HA を使用した実装を復元する場合は、データをプライマリ サーバーのみに復元する必要があります。復元されたプライマリ サーバーは、そのデータを自動的にセカンダリ サーバーに複製します。セカンダリ サーバーで復元を実行しようとすると、Cisco EPN Manager によってエラー メッセージが生成されます。

HA を使用している実装を復元する場合は、次の手順を実行してください。

1. GUI を使用して、プライマリ サーバーから HA 設定を削除します。「GUI での HA の削除（44 ページ）」を参照してください。
2. プライマリ サーバーでデータを復元します。「Cisco EPN Manager データの復元」を参照してください。
3. 復元プロセスが完了したら、HA 設定プロセスを再度実行します。プライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （11 ページ） を参照してください。

サーバーの IP アドレスまたはホスト名のリセット

プライマリ サーバーまたはセカンダリ サーバーの IP アドレスまたはホスト名は、できるだけ変更しないようにしてください。IP アドレスまたはホスト名を変更しなければならない場合は、変更を行う前に、プライマリ サーバーから HA 設定を削除します。変更が終わったら、HA を再登録します。

任意の状態の TOFU エラーの解決

プライマリサーバーとセカンダリサーバーが通信する場合、次の TOFU エラーが発生する可能性があります。

続行する前に、次のエラーを修正する必要があります。「この接続には、ゼロトラスト（*TOFU*）ベースの証明書が設定されています。リモートホストの現在の証明書は、以前に使用されていたものとは異なります。（*A Trust-on-first-use (TOFU) based Certificate is configured for this connection. The current certificate on the remote host is different than what was used earlier.*）」

この問題を解決する手順は、次のとおりです。

- プライマリサーバーとセカンダリサーバーの両方で NCS CLI コマンドを使用して既存の証明書をクリアします。

```
ncs certvalidation tofu-certs deletecert host <server-hostname>
```