



Cisco EPN Manager 7.1 高可用性インストール

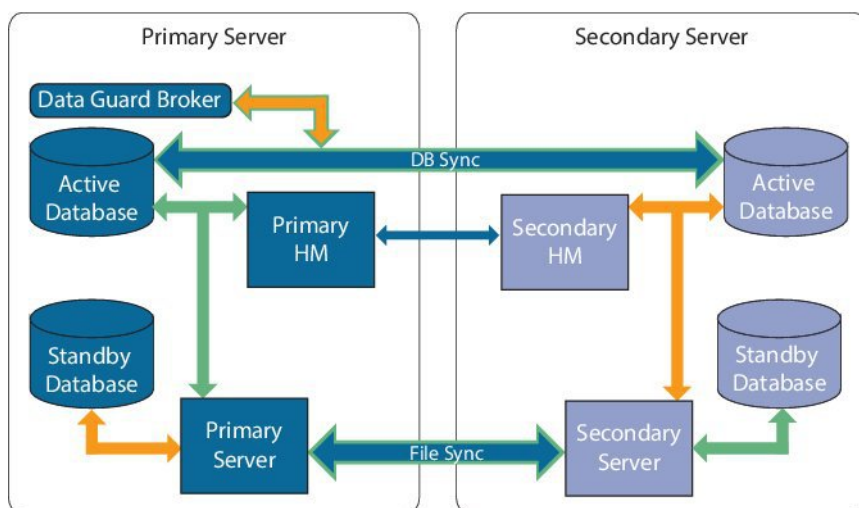
この章では、高可用性環境における Cisco EPN Manager に関する情報を示します。

- [高可用性の概要 \(1 ページ\)](#)
- [高可用性展開の考慮事項 \(2 ページ\)](#)
- [高可用性インストールの前提条件 \(5 ページ\)](#)
- [高可用性展開での Cisco EPN Manager 7.1 のインストール \(6 ページ\)](#)
- [HA 設定の準備状況の確認 \(7 ページ\)](#)

高可用性の概要

Cisco EPN Manager 高可用性 (HA) システムは、障害発生時に継続的なシステム動作を確保します。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抑えるか、あるいは完全に排除します。

次の図に、高可用性展開の主なコンポーネントとプロセス フローを示します。



高可用性展開は、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マニター (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すると (問題が発生したためか、または手動で停止させたため)、プライマリ サーバーへのアクセスを復元する間はセカンダリ サーバーがネットワークの管理を引き継ぎます。自動フェールオーバーするように展開を設定すると、プライマリ サーバーの障害発生後 2~3 分以内にセカンダリ サーバーがアクティブなロールを引き継ぎます。

プライマリ サーバーに関する問題が解決し、サーバーが実行状態になっても、スタンバイモードのままとなり、アクティブなセカンダリ サーバーとのデータの同期が開始されます。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なロールを再度引き継ぎます。プライマリ サーバーとセカンダリ サーバーの間でのこのロールの切り替えは、障害後、プライマリ サーバーが再インストールされていない限り、通常、約 2~3 分かかります。プライマリ サーバーが再インストールされている場合は、(セットアップのサイズに基づき) それよりも長く時間がかかります。

HA の詳細については、『[Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド](#)』の HA に関する項を参照してください。

高可用性展開の考慮事項

- [高可用性展開のモデル](#)
- [高可用性の制限について](#)
- [仮想アドレスを使用できるかどうかの検討](#)

高可用性展開のモデル

Cisco EPN Manager は、次の高可用性 (HA) 展開モデルをサポートしています。

HA 展開モデル	プライマリ サーバーとセカンダリサーバーの場所	例:
ローカル (Local)	同じサブネット上 (レイヤ 2 プロキシミティ)	同じデータ センターにあるサーバー
キャンパス (Campus)	LAN 経由で接続されているさまざまなサブネット	同じキャンパス、市区町村、県などにあるサーバー
リモート (Remote)	WAN 経由で接続されているさまざまなサブネット	サーバーが地理的に分散している

ローカル、キャンパス、またはリモートの HA 展開モデルを使用するかどうかの決定時には、次の要因を考慮してください。

- 災害へのリスク：展開モデルの分散が多いほど、自然災害によるビジネスへのリスクが軽減されます。リモートからの HA 展開は自然災害による影響を最も受けにくく、複雑さとコストが軽減されたビジネス継続性モデルを実現できます。ローカルでの HA 展開は、サーバー コロケーションにより災害に対して最も脆弱になります。
- 仮想 IP アドレスを使用できるかどうか：ローカルでの HA 展開のみが仮想 IP アドレスを使用できます。仮想 IP アドレスは、フェールオーバーやフェールバックの後でも、常にアクティブなサーバーを指す単一の IP アドレスです。また、プライマリ サーバーとセカンダリ サーバーの両方で共通の管理 IP アドレスを共有することもできます。
- 帯域幅/遅延：プライマリ サーバーとセカンダリ サーバーは、帯域幅が高く、遅延が小さい短いネットワークリンクによって接続されているため、ローカル HA 展開において帯域幅は最も高くなり、遅延は最も小さくなります。キャンパス HA 展開では、ローカルでの HA 展開よりも帯域幅が低くなり、遅延が大きくなる場合があります。リモートからの HA 展開では、帯域幅は最も低く、遅延は最も大きくなります。
- 管理：HA 管理は、ローカルでの HA 展開で最も簡単ですが、キャンパスおよびリモートの HA 展開の場合はより複雑になります。リモートでの HA 展開には、管理上の修復が必要になります。
- デバイスイベントの転送の設定：イベント転送の設定は、ローカルでの HA 展開が最も簡単です。これは、仮想 IP アドレスを使用し、その単一の仮想 IP アドレスにイベントを転送するようにデバイスを設定できるためです。仮想 IP アドレスを使用しない場合は、プライマリ サーバーとセカンダリ サーバーの両方にイベントを転送するようにデバイスを設定する必要があります。

HA の詳細については、『[Cisco Evolved Programmable Network Manager ユーザーおよび管理者ガイド](#)』を参照してください。

高可用性の制限について

Cisco EPN Manager の HA システムには、次の制限要因が適用されます（これは、すべての高可用性展開モデルに適用されます）。

- HA システムでは、HA 動作に対応するために、少なくとも 500 Mbps（メガビット/秒）以上のネットワーク帯域幅が必要です。これらの操作には、HA 登録、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）。Cisco EPN Manager は、すべてのネットワーク ニーズに単一の物理ポートを使用するため、帯域幅が不十分になり、HA パフォーマンスに影響を与える可能性があります。
- HA システムでは、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上は低遅延（最大 100 ms、70 ms 未満を推奨）が必要です。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。これは、大規模なデータベースには、より低い遅延とより高い帯域幅を必要とする同期トランザクションが多く必要になるためです。Cisco EPN Manager を使用して比較的小規模なネットワークを管理している場合、データベースは小さいため、HA はネットワーク遅延が長くなり、帯域幅が低くなる可能性があります。

- HA パフォーマンスは、プライマリサーバーとセカンダリサーバーに接続するネットワークが提供するネットワークスループットに大きく影響されます。この制約は、すべての展開モデルに（ある程度まで）適用されます。たとえば、地理的に分散した展開では、低帯域幅と高遅延により、リモート HA 展開に問題が発生する可能性が高くなります。ただし、ローカルおよびキャンパスでの HA 展開が正しく設定されていない場合、使用率の高いネットワークでの帯域幅の制限により、遅延による問題の影響を非常に受けやすくなります。

さまざまな HA のどれにネットワークが適しているかを判断するには、シスコの担当者に問い合わせ、支援を受けてください。

仮想アドレスを使用できるかどうかの検討

ローカル HA は展開のセットアップに仮想 IP アドレスを使用すると、ユーザーは実際にアクティブなサーバーを知らなくても、単一の IP アドレスまたは Web URL を使用してアクティブなサーバーに接続できます。仮想 IP アドレスを使用すると、両方のサーバーが共通の管理 IP アドレスを共有することもできます。通常操作中、仮想 IP アドレスはプライマリサーバーをポイントします。フェールオーバーが発生すると、仮想 IP アドレスはセカンダリサーバーを自動的にポイントします。フェールバックが発生すると、仮想 IP アドレスは自動的にプライマリサーバーに切り替わります。

仮想 IP アドレスを使用するには、次の IP アドレスが同じサブネット上にある必要があります。

- 仮想 IP アドレス
- プライマリサーバーおよびセカンダリサーバーの IP アドレス
- プライマリサーバーとセカンダリサーバーに設定されているゲートウェイの IP アドレス

次に、仮想、プライマリ、およびセカンダリの IP アドレスを相互に割り当てる例を示します。プライマリサーバーとセカンダリサーバーに、特定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は、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 (/32)
- プライマリサーバーの IP アドレス : 10.10.101.1
- セカンダリサーバーの IP アドレス : 10.10.101.2
- 仮想 IP アドレス : 10.10.101.[3-30] 例 : 10.10.101.3。仮想 IP アドレスは、特定のサブネットマスクで有効な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。

仮想 IP アドレスを使用しない場合は、プライマリサーバーとセカンダリサーバーの両方にイベントを転送するように（特定のサブネット、または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 IP アドレスの範囲にイベントを転送するなどによって）デバイスを設定する必要があります。データを損失する可能性を低減する（または排除する）には、フェールオーバーが発生する前にデバイスイベントの転送を設定する必要があります。インストール中にセカンダリサーバーに変更を加える必要はありません。プライマリサーバーとセカンダリサーバーを個別の IP アドレスでプロビジョニングするだけです。

HA 展開で単一の IP アドレスを使用するかどうかにかかわらず、ユーザーはアクティブなサーバー IP アドレス/URL を使用して Cisco EPN Manager Web GUI に常に接続する必要があります。

高可用性インストールの前提条件

次に、高可用性展開で Cisco EPN Manager をインストールする前に満たす必要がある前提条件を示します。

- ハードウェアとソフトウェアが、関連するトピックに示されている前提条件を満たしていることを確認します。
 - [OVA/VM の要件](#)
- セカンダリ サーバーが次のように設定されていることを確認します。
 - セカンダリ サーバーのハードウェアとソフトウェアの仕様は、プライマリ サーバーの仕様と同じである必要があります。たとえば、プライマリ サーバーに Cisco EPN Manager をインストールし、プロフェッショナル システム サイズを指定した場合、セカンダリ サーバーもプロフェッショナル システム サイズを使用してインストールする必要があります。また、「[システム要件](#)」にプロフェッショナル サイズ サーバーの要件すべてを満たす必要があります。
 - セカンダリ サーバーは、プライマリ サーバーと同じソフトウェア レベル（パッチ レベルを含む）を実行している必要があります。
 - ローカル HA 展開に仮想 IP アドレスを使用する場合は、仮想 IP アドレス、プライマリ サーバーおよびセカンダリ サーバーが同じサブネット上にある必要があります。プライマリ サーバーとセカンダリ サーバー上のゲートウェイも同じサブネット上に存在する必要があります。
- プライマリ サーバーとセカンダリ サーバーの間にファイアウォールがある場合は、HA で使用されるポートに対するファイアウォールからのアクセス許可が必要です。ポートは、「[Cisco EPN Manager が使用するポート](#)」に記載されています。
- インストール中に入力する必要がある次の情報を準備します。
 - セカンダリ サーバーの IPv4 IP アドレスまたはホスト名（仮想 IP アドレスを使用していない場合）。プライマリ サーバーで HA を設定する際に必要になります。
 - 両方のサーバーに使用する仮想 IPv4 と IPv6（使用している場合）の IP アドレス（仮想 IP アドレスを使用する予定の場合）。
 - HA 認証キーに使用するパスワード。このパスワードは、セカンダリ サーバーのインストール時にユーザーが指定したものです。プライマリ サーバーとセカンダリ サーバー間の通信の認証に使用されます。HA を設定する際、つまり、プライマリ サーバーにセカンダリサーバーを登録する（サーバーのペアリングともいう）ときに入力

する必要があります。最後に、セカンダリ サーバーの [ヘルス モニター (Health Monitor)] ページへのログインに必要になります。

- プライマリ サーバーの管理権限を持つ Cisco EPN Manager Web GUI のユーザー ID。また、ユーザーのパスワードも必要です。
- HA 通知を送信できる有効な電子メールアドレス。

高可用性展開での Cisco EPN Manager 7.1 のインストール

この項の手順は、高可用性環境で製品を新規にインストールするための手順です。以前のバージョンから Cisco EPN Manager 7.1 にアップグレードする場合は、「[Cisco EPN Manager 7.1 \(高可用性\) へのアップグレード](#)」を参照してください。

はじめる前に

サーバーが「[高可用性インストールの前提条件](#)」に記載されている要件を満たしていることを確認します。

-
- ステップ 1** 「[Cisco EPN Manager 7.1 のインストール \(非 HA\)](#)」に記載されているように、Cisco EPN Manager をプライマリサーバーにインストールします。
- ステップ 2** 「[Cisco EPN Manager 7.1 のインストール \(非 HA\)](#)」に記載されているように、Cisco EPN Manager をセカンダリサーバーにインストールします。
- ステップ 3** 新たにインストールしたサーバーを HA 実装環境でセカンダリ フォールバック サーバーとして機能させるかどうかを選択するよう求めるメッセージが表示されたら、**yes** と入力します。
- ステップ 4** プライマリ サーバーとセカンダリ サーバー間の通信に HA 認証キーとして使用するパスワードを入力します。HA を設定するには、このキーが必要になります。(通常の操作中に、セカンダリ サーバーの [ヘルス モニター (Health Monitor)] ページにログインするには、HA 認証キーを入力する必要があります)。
- ステップ 5** 確認のため、パスワードを再入力します。
- ステップ 6** このサーバーをセカンダリ サーバーとしてインストールすることを確認するには、**Y** と入力します。インストールが完了すると、VM (OVA/VM) がリブートします。
- ステップ 7** インストール時に指定した Cisco EPN Manager CLI 管理者ユーザー名とパスワードを使用してログインします。
- ステップ 8** イベント (syslog、trap、および TL1 メッセージ) を両方のサーバー (または仮想 IP アドレスを使用している場合は仮想 IP アドレス) 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。
- (注) プライマリ サーバーにセカンダリ サーバーを登録する前にこの手順を実行せず、フェールオーバーが発生した場合、一部のデータを損失する場合があります。
- ステップ 9** プライマリ サーバーにセカンダリ サーバーを登録して HA を設定します。登録プロセスはプライマリ サーバーから実行する必要があります。詳細については、『[Cisco Evolved Programmable Network Manager User](#)

and Administrator Guide』のプライマリサーバーへのセカンダリサーバーの登録に関するセクションを参照してください。

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 設定が完了したかが判別されます。

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。

プライマリとセカンダリの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)] フィールドに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 1: 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 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 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)	ヘルスマ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 設定の準備状況の確認

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。