ハイ アベイラビリティ

ハイ アベイラビリティについて

コントローラのハイ アベイラビリティ（HA）によって、コントローラのフェールオーバーで生じる無線ネットワークのダウン タイムを短縮することができます。

A 1:1（アクティブ：スタンバイホット）アクセス ポイントとクライアントのステートフル スイッチオーバー（HA SSO）がサポートされています。HA アーキテクチャでは、1 台のコントローラはプライマリ コントローラとして、別のコントローラはセカンダリ コントローラとして設定されています。

HA を有効にした後、プライマリおよびセカンダリ コントローラがリブートされます。ブート プロセス中に、プライマリ コントローラのロールはアクティブとして、セカンダリ コントローラのロールはスタンバイ ホットとしてネゴシエートされます。スイッチオーバー後、セカンダリ コントローラは、アクティブ コントローラになり、プライマリ コントローラがスタンバイ ホット コントローラになります。それ以降の切り替えの後、ロールは、プライマリおよびセカンダリ コントローラ間で交換されます。ほとんどのスイッチオーバー イベントの理由や原因は、手動トリガー、コントローラまたはネットワーク障害です。

HA SSO フェールオーバー イベントの間、コントローラ上の RUN 状態になっているすべての AP CAPWAP セッションとクライアント セッションが、中断することなくスタンバイ コントローラにステートフルにスイッチオーバーされます。ただし、PMIPv6 クライアントは除きます。PMIPv6 クライアントは、HA SSO スイッチオーバー後に、コントローラに再接続して、認証される必要があります。その他のクライアントの SSO 動作と制限事項については、次の

URL にあるハイ アベイラビリティ（*SSO*）導入ガイド [英語] の「Client SSO」セクションを参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/HA_SSO_DG/High_Availability_DG.html#pgfId-53637

スタンバイホット コントローラは、専用の冗長ポートを介してアクティブ コントローラの状態を常時モニタします。両方のコントローラは管理インターフェイスの IP アドレスを含め、同じ設定を共有します。

HA を有効にする前に、両方のコントローラが、直接ケーブル接続またはレイヤ 2 のいずれかを経由し、それぞれの専用冗長ポートを介して互いに正常に通信できることを確認してください。詳細については、ハイ アベイラビリティ *(SSO)* 導入ガイド [英語] の「Redundancy Port Connectivity」セクションを参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/HA_SSO_DG/High_Availability_DG.html#pgfId-83028

リリース 8.0 以降では、**show ap join stats summary** コマンドの出力に、アクセス ポイントがコントローラに join しているか、アクティブ コントローラから同期されているかに基いてアクセス ポイントのステータスが表示されます。次のステータスのいずれかが表示されます。

- Synched：アクセス ポイントが SSO 前にコントローラに join しました。
- Connected：アクセス ポイントが SSO 後にコントローラに join しました。
- Joined：アクセス ポイントがコントローラに再 join したか、新しい AP が SSO 後にコントローラに join しました。

リリース 8.0 以降では、**show redundancy summary** コマンドの出力はアクティブおよびスタンバイのコントローラ・ペアの後のアクセス ポイントおよびクライアントのバルク同期の状態が発生します。値は次のとおりです。

- Pending：アクティブ コントローラからスタンバイ コントローラへのアクセス ポイントと対応するクライアント詳細の同期がまだ開始されていないことを示します。
- In-progress：アクティブ コントローラからスタンバイ コントローラへのアクセス ポイントと対応するクライアント詳細の同期が開始され、進行中であることを示します。
- Complete：同期が完了し、スタンバイ コントローラで、アクティブ コントローラのサービスを再開するためのスイッチオーバーの準備ができていることを示します。

リリース 8.0 以降のハイ アベイラビリティ シナリオでは、スリープ タイマーがアクティブとスタンバイの間で同期されます。

ACL と NAT IP の設定は、これらのパラメータが HA ペア成立前に設定されていれば、HA スタンバイ コントローラに同期されます。NAT IP が管理インターフェイス上で設定された場合は、アクセス ポイントが AP マネージャの IP アドレスを NAT IP アドレスとして設定します。

次に、ハイ アベイラビリティに関する注意事項を示します。

- 異なるハードウェア モデルの2台のコントローラを組み合わせないことを推奨します。それらを組み合わせると、上位のコントローラ モデルがアクティブ コントローラになり、下位のコントローラがメンテナンス モードに入ります。
- コントローラ ソフトウェア リリースの異なる 2 台のコントローラを組み合わせないことを推奨します。それらを組み合わせると、下位のリダンダンシー マネージメント アドレスを持つコントローラがアクティブ コントローラになり、上位のコントローラがメンテナンス モードに入ります。
- HA を無効にし、Cisco 55208540 WLC（RTU ベース）にライセンスを追加することをお勧めします。ただし、プライマリ WLC で追加した AP ライセンスはセカンダリ WLC に継承されるため、HA の無効化は必須ではありません。
- イメージ、設定、Web 認証バンドル、シグニチャ ファイルなどのダウンロード ファイル タイプはすべて、アクティブ コントローラにダウンロードされてから、スタンバイホット コントローラにプッシュされます。
- 組み合わせる前に、証明書を各コントローラに個別にダウンロードする必要があります。
- アクティブ コントローラの GUI または CLI を使用して、設定ファイル、イベント ログ、クラッシュ ファイルなどのファイル タイプをスタンバイホット コントローラからアップロードできます。また、ファイル名にアップロードされたファイルを識別するサフィックスを指定できます。
- ピア アップロードを実行するには、サービス ポートを使用します。管理ネットワークでは、リダンダンシー マネージメント インターフェイス（RMI）が管理 VLAN と同じ場合に、リダンダンシー ポートと RMI VLAN のどちらかまたはその両方にマッピングされた RMI を使用することもできます。RMI とリダンダンシー ポートが別々のレイヤ 2 VLAN 上に存在しなければならないことに注意してください。これは必須設定です。
- コントローラが冗長ポートおよび RMI を介して相互に接続できない場合、プライマリ コントローラがアクティブになり、スタンバイホット コントローラはメンテナンス モードになります。

（注） ペアになっており、同じ VLAN にマッピングされ、同じレイヤ 3 スイッチに接続されている 2 つのコントローラの RMI が動作を停止すると、スタンバイ コントローラが再起動されます。

HA セットアップのアクティブ/スタンバイ セカンド スイッチオーバーの間は、「mobilityHaMac は範囲外」XML メッセージが表示されます。このメッセージは、モビリティ HA の MAC フィールドが 128 を超えると表示されます。

- HA が有効な場合、スタンバイ コントローラは常に Remote Method Invocation（RMI）を使用します。他のすべてのインターフェイス（動的と管理）は無効になります。

（注） RMIの使用目的はアクティブ通信とスタンバイ通信だけです。他に目的はありません。

- ハイ アベイラビリティを有効にする前に、RMI ポート上の最大伝送単位（MTU）が 1500 バイト以上であることを確認する必要があります。
- HA が有効な場合は、バックアップ イメージを使用しないでください。このイメージが使用されると、HA 機能が想定どおりに機能しない可能性があります。
  - SSO をイネーブルにすると、設定されているサービス ポートとルート情報が失われます。SSO をイネーブルにした後は、サービス ポートとルート情報を再設定する必要があります。**peer-service-port** および **peer-route** コマンドを使用して、スタンバイ ホット コントローラのサービス ポートとルート情報を設定できます。
  - スタンバイホット コントローラでは **reset** コマンドを直接使用しないでください。これを使用すると、保存されていない設定は失われます。
- インフラストラクチャ スイッチのポート チャネルを有効にする前に、コントローラのリンク集約設定を有効にすることをお勧めします。
- アクティブ コントローラのリブートが必要なすべての設定によって、スタンバイホット コントローラがリブートされることになります。
- [Rogue AP Ignore] リストは、アクティブ コントローラからスタンバイホット コントローラに同期されません。このリストは、スタンバイホット コントローラがアクティブになった後で、Cisco Prime Infrastructure の SNMP メッセージを通して再取得されます。
- クライアント SSO 関連の注意事項
  - スタンバイ コントローラは 2 つのクライアント リストを保持します。実行状態のクライアントのリストおよび他のすべての状態である一時的なクライアントのリストです。
  - 実行状態にあるクライアントのみがフェールオーバー中に維持されます。ローミング、802.1X キーの再生成、Web 認証ログアウトなどの過渡状態にあるクライアントのアソシエーションが解除されます。
  - AP SSO と同様に、クライアント SSO は WLAN 上でのみサポートされます。コントローラは、同じサブネット内にある必要があります。Layer3 接続はサポートされません。
- リリース 7.3.x では AP SSO はサポートされますが、クライアント SSO はサポートされないため、リリース 7.3.x を使用した HA セットアップでスイッチオーバーが発生した場合は、コントローラに関連付けられているすべてのクライアントが認証解除され、強制的に再アソシエーションされます。

- ピア コントローラにリリース 7.2 以前のコントローラ ソフトウェア リリースがある場合、スイッチオーバー後のアクティブ コントローラにモビリティ MAC アドレスを設定する必要があります。
- アクセス ポイントで音声パラメータとビデオ パラメータの制御された Quality of Service（QoS）を維持できるようにするために、スイッチオーバーが発生すると、すべての帯域幅ベースまたは静的コール アドミッション制御（CAC）パラメータがアクティブからスタンバイに同期されます。
- リリース 8.0 以降では、スタンバイ コントローラがリブートしません。代わりに、リダンダンシー ポートを使用してデフォルト ゲートウェイに接続できない場合は、メンテナンス モードに入ります。コントローラがデフォルト ゲートウェイに再接続すると、スタンバイ コントローラがリブートして、アクティブ コントローラとの HA ペアが開始されます。ただし、アクティブ コントローラはメンテナンス モードに入る前にリブートします。
- リリース 8.0 からサポートされたものを以下に示します。
  - 静的 CAC 同期：音声パラメータとビデオ パラメータの制御された Quality-of-Service（QoS）を維持するために、スイッチオーバーが発生すると、すべての帯域幅ベースまたは静的 CAC パラメータ サービスがクライアントですぐに利用できるようになります。
  - 内部 DHCP サーバ：コントローラの無線クライアントを機能させるために、内部 DHCP サーバのデータがアクティブ コントローラからスタンバイ コントローラに同期されます。アクティブからスタンバイへのロール変更が発生しても、割り当てられたすべての IP アドレスは有効なままで、IP アドレス割り当てが継続されます。
  - デバッグとサービスアビリティの強化：すべてのデバッグ サービスとサービスアビリティ サービスがユーザ向けに強化されました。
- スイッチ上のアクセス ポイントの物理接続またはトポロジは、アクティブ コントローラからスタンバイ コントローラに同期されません。スタンバイ コントローラは同期が完了しないと詳細を取得しません。そのため、**show ap cdp neighbors all** コマンドは、同期が完了して、スタンバイ コントローラがアクティブ コントローラになった場合にのみ実行する必要があります。
- アクセス ポイントが、工場出荷時設定にリセットされた HA-SKU セカンダリ コントローラに join できるようにするには、次の手順を実行する必要があります。
  - HA SKU コントローラをセカンダリ コントローラとして設定します。この設定を行うには、HA SKU コントローラで **config redundancy unit secondary** コマンドを実行する必要があります。
  - **config redundancy unit secondary** コマンドを正常に実行してから、HA SKU コントローラをリブートします。

リダンダンシー マネジメント インターフェイス

アクティブおよびスタンバイホット コントローラでは、RMI を使用して、ネットワーク インフラストラクチャを介して管理インターフェイスのピア コントローラおよびデフォルト ゲートウェイのヘルスをチェックします。

また、障害が発生または手動でリセットした場合に、RMI がアクティブ コントローラからスタンバイホット コントローラに通知を送信するために使用されます。スタンバイホット コントローラは、syslog、NTP/SNTP サーバ、FTP サーバおよび TFTP サーバと RMI で通信します。

プライマリ コントローラおよびセカンダリ コントローラの両方で同じサブネット内のリダンダンシー マネジメント インターフェイスおよび管理インターフェイスの IP アドレスを設定する必要があります。

冗長ポート

リダンダンシー ポートは、設定、動作データの同期、プライマリおよびセカンダリ コントローラ間のロール ネゴシエーションに使用されます。

リダンダンシー ポートは、スタンバイホット コントローラからアクティブ コントローラに 100 ミリ秒ごとに（デフォルトの頻度）UDP キープアライブ メッセージを送信することによってピアの到達可能性を確認します。アクティブ コントローラの障害が発生した場合、リダンダンシー ポートがスタンバイホット コントローラを通知するために使用されます。

NTP/SNTP サーバが設定されていない場合、リダンダンシー ポートがアクティブ コントローラからスタンバイホット コントローラに時刻同期を行います。

リダンダンシー ポートは L2 スイッチを介して接続できます。リダンダンシー ポートのラウンドトリップ時間は、キープアライブ タイマーがデフォルトの 100 ミリ秒に設定されている場合は 80 ミリ秒未満、キープアライブ タイマーが 100 ミリ秒～ 400 ミリ秒の範囲に設定されている場合はキープアライブ タイマーの 80% にしてください。たとえば、キープアライブ タイマーが 100 ミリ秒に設定されている場合、障害検出時間は次のように計算されます：3 * 100 = 300 + 60 = 360 + ジッタ（12 ミリ秒）＝～ 400 ミリ秒。リダンダンシー ポート間の帯域幅が 60 Mbps 以上であることを確認します。最大伝送単位（MTU）が 1500 バイト以上であることを確認します。

関連資料

- ハイ アベイラビリティ（*SSO*）導入ガイド [英語]：https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/HA_SSO_DG/High_Availability_DG.html
- *N+1* ハイ アベイラビリティ導入ガイド[英語]：https://www.cisco.com/c/en/us/td/docs/wireless/technology/hi_avail/N1_High_Availability_Deployment_Guide.html

ハイ アベイラビリティの制約事項

- HA SSO が有効になっているときは、LAG 物理ポートを無効にしないことを推奨します。
- ファブリック関連の統計情報の HA の同期はサポートされていません。

- Cisco WLC が HA SSO に設定され、リダンダンシー マネジメントがダイナミック インターフェイスで設定されている場合、SSH のアクセス リストをリダンダンシー インターフェイスに適用する必要があります。そうしないと、SSH クライアントが CPU ACL に関係なくリダンダンシー マネジメント インターフェイス経由で接続できるようになります。
- HA 環境で FlexConnect のローカルにスイッチされるクライアントを使用すると、クライアント情報にユーザ名が表示されない場合があります。クライアントの詳細を取得するには、クライアントの MAC アドレスを使用する必要があります。この制限は、FlexConnect の中央でスイッチされるクライアントまたは中央（ローカル）モードのクライアントには適用されません。
- HA 環境では、LDPE イメージから LDPE 以外のイメージへのアップグレードはサポートされていません。
- 2 台のプライマリ コントローラまたは 2 台のセカンダリ コントローラを組み合わせることはできません。
- スタンバイ コントローラは AP に接続されたスイッチ ポートでは利用できません。
- 評価ライセンスを持つ HA-SKU コントローラをスタンバイ コントローラにすることはできません。ただし、ゼロ ライセンスを持つ HA-SKU コントローラはスタンバイ コントローラにすることができます。
- HA モードから HA 以外のモード、またはその逆に移行すると、サービス VLAN 設定が失われます。再度サービス IP アドレスを手動で設定する必要があります。
- プライマリ コントローラの管理アドレスとリダンダンシー マネジメント アドレスが同じ VLAN 上にあって、プライマリ コントローラと同じ VLAN 上にセカンダリ コントローラの管理アドレスがあり、別の VLAN にそのリダンダンシー マネジメント アドレスがあるというシナリオはサポートされていません。
- 次に、ソフトウェア アップグレードのシナリオの一覧を示します。
  - アクティブ コントローラのソフトウェア アップグレードでは、スタンバイホット コントローラのアップグレードを確認します。
  - インサービス アップグレードはサポートされません。このため、HA 環境でコントローラをアップグレードする前に、ネットワークのダウンタイムを計画する必要があります。
  - ソフトウェア アップグレード後のアクティブ コントローラをリブートすると、スタンバイホット コントローラもリブートします。
  - **config boot backup** コマンドを実行する前に、アクティブとスタンバイの両方のホット コントローラのバックアップに同じソフトウェア イメージを保存することをお勧めします。アクティブおよびスタンバイホット コントローラの両方のバックアップに異なるソフトウェア イメージが含まれている場合、アクティブ コントローラで **config boot backup** コマンドを実行すると、両方のコントローラがそれぞれのバックアップ イメージでリブートされて、ソフトウェアの不一致により HA ペアが切断されます。

- スケジュール リセットがHA環境の両方のコントローラに適用されます。アクティブ コントローラで期限切れになるスケジュール時刻の 1 分前にピア コントローラがリブートします。
- リセットがスケジュールされていない場合、**reset peer-system** コマンドを入力して、アクティブ コントローラからスタンバイホット コントローラをリブートできます。このコマンドでスタンバイホット コントローラのみをリセットすると、スタンバイホットコントローラの未保存の設定はすべて失われます。そのため、スタンバイホット コントローラをリセットする前に、アクティブ コントローラ上で設定を保存する必要があります。
- プリイメージ ダウンロードは、SSO がイメージの転送時にトリガーされると再起動されます。
- スタンバイホット コントローラでは、**debug** コマンドと **show** コマンドのみ許可されます。
- スイッチオーバー後、ピア コントローラにリリース 7.5 以前のコントローラ ソフトウェア リリースがある場合、すべてのモビリティ クライアントが認証解除されます。

- コントローラ GUI、Cisco Prime Infrastructure、または Telnet 経由でスタンバイホット コントローラにアクセスすることはできません。コンソールでのみスタンバイホット コントローラにアクセスできます。
- フェールオーバーが発生した場合、正常なスイッチオーバーのために、SSOでは、スタンバイ コントローラはスタンバイホット状態、冗長ポートはターミナル状態である必要があります。
- LAG を有効または無効にするには、HA を無効にする必要があります。

（注） LAG が無効になっていて、プライマリおよびバックアップ ポートの両方が管理インターフェイスに接続されている場合、プライマリ ポートが動作不能になると、デフォルト ゲートウェイに到達できずにバックアップ ポートのフェールオーバーが 12 秒を超える可能性があるので、スイッチオーバーが発生することがあります。

- フェールオーバーが発生し、スタンバイ コントローラが新しいアクティブ コントローラになる場合、2台のコントローラ間のデータベースの同期（AP、クライアントおよびマルチキャスト）に約 15 ～ 20 分かかります。新たにフェイルオーバーがこの時間内に発生した場合、HAの構造が同期されることはありません。したがって、APおよびクライアントを再アソシエートして、個別に再認証する必要があります。
- Pairwise Master Key（PMK）キャッシュの同期はFlexConnectのローカル認証クライアントではサポートされません。
- クライアント SSO の制限

- 新しいモビリティはサポートされていません。
- ポスチャおよびネットワーク アドミッション コントロール アウトオブバンドは、クライアントが実行状態にないため、サポートされません。
- 次の内容は、アクティブ コントローラとスタンバイ コントローラの間で同期されません。
  - Cisco Compatible Extensions ベースのアプリケーション
  - クライアントの統計
  - プロキシ モバイル IPv6、Application Visibility and Control、セッション開始プロトコル（SIP）、およびスタティック コール アドミッション制御（CAC）ツリー
  - ワークグループ ブリッジおよびその関連クライアント
  - パッシブ クライアント
- 暗号化はサポートされています。

- 暗号化は、アクティブおよびスタンバイのコントローラが管理ポートのリダンダンシーマネジメントインターフェイス経由で通信する場合のみサポートされます。暗号化は、リダンダンシー ポートがアクティブ コントローラとスタンバイ コントローラ間の通信に使用される場合はサポートされません。
- コントローラがリダンダンシー モードの場合、管理インターフェイスの NAT アドレスの設定は変更できません。管理インターフェイスで NAT アドレス設定を有効にするには、最初に冗長構成を削除する必要があります。プライマリ コントローラで必要な変更を行ってから、同じコントローラで冗長構成を再度有効にします。
- SSO を有効にしてから、スタンバイおよびアクティブの両方のコントローラにアクセスするには、次を使用します。
  - コンソール接続
  - サービス ポートの SSH 機能
  - リダンダンシー マネジメント インターフェイスの SSH 機能
- バルク同期設定は、XML に保存されている設定に対してのみサポートされます。スケジュールされたリブートは、XML またはフラッシュに保存されていない設定です。そのため、スケジュールされたリブートの設定は、バルク同期設定には含まれません。
- スイッチオーバーが発生すると、DHCP ダーティ ビットがアクティブ コントローラ上に設定されていても、コントローラは DHCP ダーティ ビットの情報をアクティブからスタンバイ コントローラへ同期しません。スイッチオーバーの後、コントローラは、クライアントの DHCP リトライに基づいて DHCP ダーティ ビットを挿入します。

ハイ アベイラビリティの設定（GUI）

始める前に

両方のコントローラの管理インターフェイスが同じサブネット上にあることを確認します。[Controllers] > [Interfaces] を選択し、管理インターフェイスの IP アドレスを表示して、両方のコントローラの GUI でこれを確認できます。

手順

ステップ 1 両方のコントローラの GUI で、[Controller] > [Redundancy] > [Global Configuration] を選択します。

[Global Configuration] ウィンドウが表示されます。

ステップ 2 [Redundant Management IP] および [Peer Redundant Management IP] フィールドに両方のコントローラのアドレスを入力します。

（注） 1 台のコントローラのリダンダンシー マネジメント インターフェイス IP アドレスがピア コントローラのリダンダンシー マネジメント インターフェイス IP アドレスと同じであることを確認します。

ステップ 3 [Redundant Unit] ドロップダウン リストで、コントローラの 1 つをプライマリとして、他のコントローラをセカンダリとして選択します。

ステップ 4 両方のコントローラの GUI で、[SSO] を [Enabled] 状態に設定します。

（注） SSO を有効にすると、サービス ポートのピア IP アドレス、およびサービス ポートのネットマスクが [Configuration] ウィンドウに表示されます。HA ピアが使用可能で稼働している場合、サービス ポートのピア IP アドレスとネット マスクがピアのみにプッシュできることに注意してください。HA をイネーブルにすると、サービス ポートのピア IP アドレスおよびサービス ポートのネット マスク パラメータを設定する必要はありません。HA ピアが使用可能で稼働している場合、パラメータを設定する必要があります。SSO を有効にした後、両方のコントローラがリブートされます。リブートプロセス中に、コントローラは設定に基づいて冗長ポートを介して冗長ロールをネゴシエートします。プライマリ コントローラは、アクティブ コントローラになり、セカンダリ コントローラがスタンバイ コントローラになります。

ステップ 5 （オプション）HA ペアが使用可能および動作可能になると、サービス ポートがスタティックに設定された後に、ピア サービス ポートの IP アドレスおよびネットマスクを設定できます。サービス ポートの DHCP を有効にした場合、[Global Configuration] ウィンドウで次のパラメータを設定する必要はありません。

- [Service Port Peer IP]：ピア コントローラのサービス ポートの IP アドレス。
- [Service Port Peer Netmask]：ピア コントローラのサービス ポートのネットマスク。

- [Mobility MAC Address]：モビリティ プロトコルで使用されるアクティブ コントローラとスタンバイ コントローラの共通 MAC アドレス。HA ペアをモビリティ グループのモビリティ メンバとして追加する場合は、モビリティ MAC アドレスを（アクティブまたはスタンバイ コントローラのシステム MAC アドレスの代わりに）使用する必要があります。通常、モビリティ MAC アドレスはアクティブ コントローラの MAC アドレスとして選択されるため、手動で設定する必要はありません。
- [Keep Alive Timer]：スタンバイ コントローラがアクティブ コントローラにハートビート キープアライブ メッセージを送信する頻度を制御するタイマー。有効範囲は 100 ～ 1000 ミリ秒です。
- [Peer Search Timer]：アクティブ コントローラがスタンバイ コントローラにピア検索メッセージを送信する頻度を制御するタイマー。有効な範囲は 60 ～ 300 秒です。

（注） HA をイネーブルにし、コントローラを組み合わせると、管理ポートを通じて HA ペアを管理する統合 GUI が 1 種類のみになります。サービス ポートを通過する GUI へのアクセスは、アクティブ コントローラとスタンバイ コントローラのいずれでも実行できません。スタンバイ コントローラは、コンソール ポートまたはサービス ポートを介してのみ管理することができます。

Telnet および SSH セッションだけが、アクティブ コントローラとスタンバイ コントローラのサービス ポート経由で許可されます。

ステップ 6 （オプション）HA ペア間のリンクを暗号化するには、[Global Configuration] ページで、[Link Encryption] ドロップダウンリストから [Enabled] を選択します。

ステップ 7 [Save Configuration] をクリックします。

ステップ 8 [Monitor] > [Redundancy] > [Summary] を選択し、HA ペアの冗長ステータスを表示します。

[Redundancy Summary] ウィンドウが表示されます。

ステップ 9 [Monitor] > [Redundancy] > [Detail] を選択し、HA ペアの冗長ステータスを表示します。

[Redundancy Detail] ページが表示されます。

ステップ 10 [Monitor] > [Redundancy] > [Statistics] を選択し、HA ペアの冗長統計情報を表示します。

[Redundancy Statistics] ページが表示されます。

ステップ 11 （オプション）次の手順を実行して、ピア ネットワーク ルートを設定します。

a) **[Controller]** > **[Redundancy]** > **[Peer Network Route]** を選択します。

[Network Routes Peer] ウィンドウが表示されます。

このウィンドウには、異なるサブネット上のネットワークまたは要素管理システムへの、ピア コントローラの既存のサービス ポート ネットワーク ルートの概要が表示されます。IP アドレス、IP ネットマスク、またはゲートウェイ IP アドレスを表示できます。

b) 新しいピア ネットワーク ルートを作成するには、[New] をクリックします。

c) ルートの [IP address]、[IP netmask]、および [Gateway IP address] を入力します。

d) [Apply] をクリックします。

高可用性の有効化（CLI）

手順

ステップ 1 HA を設定する前に、両方のコントローラの管理インターフェイスを同じサブネットに入れる必要があります。両方のコントローラで次のコマンドを入力して、インターフェイスの要約情報を参照してください。

show interface summary

ステップ 2 HA はデフォルトでディセーブルになっています。HA を有効にする前に、冗長性管理 IP アドレスおよびピア冗長性管理 IP アドレスを設定する必要があります。両方のインターフェイスは、管理インターフェイスと同じサブネットにある必要があります。次のコマンドを入力して、冗長性管理 IP アドレスを設定します。

- WLC1：**config interface redundancy-management** *redundancy-mgmt-ip-addr-wlc1***peer-redundancy-management** *peer-redundancy-mgmt-ip-addr-wlc2*
- WLC2：**config interface redundancy-management** *redundancy-mgmt-ip-addr-wlc2***peer-redundancy-management** *peer-redundancy-mgmt-ip-addr-wlc1*

ステップ 3 1 つのコントローラをプライマリ（デフォルトでは、WLC HA ユニット ID がプライマリで、有効な AP-BASE カウント ライセンスがインストールされている必要あり）として設定し、もう 1 つのコントローラをセカンダリ（プライマリ コントローラからの AP-BASE カウントをこのユニットで継承）として設定します。

- プライマリとしての WLC1：**config redundancy unit primary**
- セカンダリとしての WLC2：**config redundancy unit secondary**

（注） リリース 7.3 以降でオーダーできるファクトリ オーダー HA SKU の場合は、ユニットをセカンダリとして設定する必要はありません。ファクトリ オーダー HA SKU は、デフォルトのセカンダリ ユニットであり、有効な AP カウント ライセンスを持つアクティブなコントローラと初めてペアにされたときに、スタンバイ コントローラの役割を引き受けます。

ステップ 4 コントローラに冗長性管理とピア冗長性管理の IP アドレスを設定し、冗長ユニットを設定したら、SSO を有効にする必要があります。SSO を有効にする前に、両方のコントローラ間の物理接続が動作しており（イーサネット ケーブルを使用し、冗長ポートを介して両方のコントローラをバックツーバック接続している）、アップリンクもインフラストラクチャ スイッチに接続されていて、両方のコントローラからゲートウェイに到達可能なことを確認します。

SSOを有効にすると、両方のコントローラがリブートします。起動プロセス中に、コントローラは設定に基づいて冗長ポートを介してHAの役割をネゴシエートします。コントローラが冗長ポートまたは冗長管理インターフェイスを介して相互に到達できない場合、セカンダリとして設定されているコントローラはメンテナンス モードに移行することがあります。

次のコマンドを入力して、両方のコントローラで SSO を有効にします。

config redundancy mode sso

（注） SSO を有効にすると、コントローラのリブートが開始されます。

ステップ 5 SSOを有効にすると、実施した設定に基いてHAの役割をネゴシエートするためにコントローラがリブートされます。役割が決まると、冗長ポートを介してアクティブ コントローラからスタンバイ コントローラに設定が同期されます。最初にセカンダリとして設定されたコントローラは、XML の不一致を報告し、アクティブなコントローラから設定をダウンロードして、 再度リブートします。コントローラは、役割が決まった後の次回リブート時に設定を再度検証して、 XML の不一致がないことを報告し、スタンバイ コントローラとして機能するための処理を続行します。

（注） SSO を有効にすると、コンソール接続を介して、またはサービス ポートおよび冗長管理インターフェイス上の SSH からスタンバイ コントローラにアクセスできます。

ステップ 6 SSO を有効にして、コントローラがリブートされ、XML 設定が同期されると、WLC1 の状態はアクティブに移行し、WLC2 の状態はスタンバイ ホットに移行します。この時点以降は、すべての設定と管理をアクティブなコントローラから行う必要があるため、管理インターフェイス上の WLC2 用の GUI、Telnet、SSH は機能しません。必要に応じて、スタンバイ コントローラ（WLC2）は、コンソールまたはサービス ポートを介してのみ管理することができます。

また、ピア コントローラがスタンバイ ホット状態に移行すると、*-Standby* キーワードがスタンバイ コントローラのプロンプト名に自動的に追加されます。

ステップ 7 次のコマンドを入力して、両方のコントローラの冗長性の要約情報を確認します。

show redundancy summary

高可用性パラメータの設定

手順

- 次のコマンドを入力して、コントローラ間の通信の暗号化を設定します。

  config redundancy link-encryption {**enable** | **disable**}

- 次のコマンドを入力して、スタンバイピア コントローラのピア サービス ポートの IP アドレスとネットマスクを設定します。

  config redundancy interface address peer-service-port *ip-address netmask*

このコマンドはHAピア コントローラが使用可能であり、正常に動作している場合だけ実行できます。

- （オプション）次のコマンドを入力して、スタンバイ コントローラのルート設定を設定します。

  config redundancy peer-route { **add** *network-ip-addr ip-mask* | **delete** *network-ip-addr*}

（注） このコマンドはHAピア コントローラが使用可能であり、正常に動作している場合だけ実行できます。

- （オプション）次のコマンドを入力して、モビリティの MAC アドレスを設定します。

  config redundancy mobilitymac *mac-addr*

（注）
- このコマンドは、SSO が無効になっている場合にだけ実行できます。
- リリース8.0.110.0からそれ以降リリースにアップグレードすると、このコマンドの設定は削除されます。アップグレード後に手動でモビリティ MAC アドレスを再設定する必要があります。

- 次のコマンドを入力して、冗長タイマーを設定します。

  config redundancy timer { **keep-alive-timer** *time-in-milliseconds* | **peer-search-timer** *time-in-seconds*}

- 次のコマンドを入力して、冗長性のステータスを表示します。

  show redundancy {**summary** | **detail**}

- 次のコマンドを入力して、冗長管理インターフェイスに関する情報を表示します。

  show interface detailed redundancy-management

- 次のコマンドを入力して、リダンダンシー ポートに関する情報を表示します。

  show interface detailed redundancy-port

- 次のコマンドを入力して、ピア コントローラをリブートします。

  reset peer-system

- アクティブ コントローラで次のコマンドを入力して、スタンバイホット コントローラから、設定、イベント ログ、クラッシュ ファイルなどのファイル タイプのアップロードを開始します。

  transfer upload peer-start

- アクティブコントローラで次のコマンドを入力して、スイッチオーバー後のスリープ状態のクライアントの情報を表示します。

show custom-web sleep-client summary

高可用性に対する IPsec 暗号化のトラブルシューティングのヒント

手順

- HA ペアが起動しない場合は、両方のコントローラでリンク暗号化の設定を確認します。
- 両方のコントローラのリンク暗号化の設定は同じである必要があります。
- 両方のコントローラの IPsec ステータスを確認し、RP または RMI が壊れているリンクを確認します。
- 両方のコントローラで **rping** を実行して、ピアが到達可能かどうか確認します。
- 次のコマンドを入力して、リンク暗号化のステータスを確認します。

  show redundancy summary

- 次のコマンドを入力して、HA ペア間の IPsec ステータスを確認します。

  show ipsec status

- 次のコマンドを入力して、IPsec のデバッグ メッセージを有効にし、ピアのセカンダリ コントローラをリブートします。

  debug ipsec events enable

  このコマンドは、IPsec のデバッグ メッセージを有効にします。このコマンドを有効にすると、ピアのセカンダリ コントローラがリブートします。

（注） **debug ipsec events enable** では、次回リブート（ブートアップ）時にログは印刷されません。

vWLC および N+1 高可用性

シスコ ワイヤレス コントローラ（WLC）リリース 8.4 では、Cisco Virtual Wireless Controller（vWLC）プラットフォームでの N+1 高可用性（HA）のサポートが導入されています。HA の設定方法については、以下を参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/technology/hi_avail/N1_High_Availability_Deployment_Guide/N1_HA_Overview.html#pgfId-1054644

Cisco vWLC HA には、次の前提条件があります。

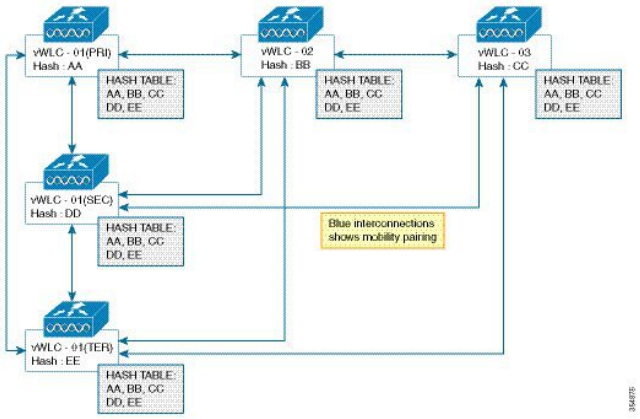
- プライマリ、セカンダリ、およびターシャリ vWLC は、同じモビリティ グループの一部である必要があります。
- モビリティ グループの vWLC には、AP を 1 つの vWLC から別の vWLC にシームレスに移動するための均一のハッシュ キーのセットが必要です。たとえば、モビリティ グループに vWLC、N があるか、または vWLC、M、および通常の WLC（M は N より大きい）

がある場合、すべての vWLC が同じグループ内のその他の vWLC のハッシュを保有している必要があります。

- （N+1 形式の vWLC モビリティ メンバーを含む）モビリティ グループ内のすべての vWLC で AP の効率的な接続を確保するためには、モビリティ ハッシュ テーブルにすべての vWLC ハッシュ キーを含める必要があります。

（注） ハッシュ テーブルは、vWLC がモビリティ メンバーとペアリングされている場合にのみ機能します。

図 *1*：モビリティ グループ内の *vWLC N+1*



Cisco vWLC へのハッシュ キーの追加（GUI）

Cisco vWLC にハッシュ キーを追加するには、次の手順を実行します。

始める前に

ハッシュ キーを Cisco vWLC に追加する前に、モビリティ ピアを作成します。

手順

ステップ 1 [Controller] > [Mobility Management] > [Mobility Groups] の順に選択します。

[Static Mobility Group Members] ウィンドウに、既存のメンバーとそれらのメンバーに設定されているハッシュ キーが表示されます。

ステップ 2 [New] をクリックします。

[Mobility Group Member] > [New] ウィンドウが表示されます。

ステップ 3 [Member IP Address(Ipv4/Ipv6)] フィールドに、メンバーの IP アドレスを入力します。[Member MAC Address] フィールドに、メンバーの MAC アドレスを入力します。[Group Name] フィールドに、グループ名を入力します。[Hash] フィールドに、ハッシュ キーを入力します。

ステップ 4 [Apply] をクリックします。

Cisco vWLC へのハッシュ キーの追加（CLI）

CLI を使用して Cisco vWLC にハッシュ キーを追加するには、次の手順を実行します。

- ハッシュ キーを読み取ります。
- ハッシュ キーをモビリティ グループのその他のメンバーにコピーします。
- モビリティ ハッシュの設定を確認します。

始める前に

- ハッシュ値は各 vWLC で一意である必要があります。
- ハッシュ キーを vWLC に追加する前に、モビリティ ピアを作成します。

手順

ステップ 1 **show mobility group member hash**

例：

```
(Cisco Controller)> show mobility group member hash
```

既存のハッシュ キーを読み取ります。

ステップ 2 **config mobility group member hash** *ipv4-address hash-key*

例：

```
(Cisco Controller)> config mobility group member hash 9.11.34.55
1f81d80082e9d30312d3b4920be22aed34b93b56
```

ハッシュをモビリティ グループのその他のメンバーにコピーします。

ステップ 3 **show mobility group member hash**

例：

```
(Cisco Controller)> show mobility group member hash
Default Mobility Domain..................... default

 IP Address      Hash Key
------------------------------------------------------------
 9.11.34.55     1f81d80082e9d30312d3b4920be22aed34b93b56
```

グループ内のすべてのモビリティ メンバーのモビリティ ハッシュの設定を確認します。

ハイ アベイラビリティ スタンバイ WLC の監視

アクティブ WLC とスタンバイ WLC のステータス情報とヘルス情報を別々に表示できます。ここでは、スタンバイ WLC からヘルス情報とトラップを取得する方法について説明します。

スタンバイ WLC では、Syslog、NTP サーバ、TFTP サーバなどとの通信のように、外部の通信には冗長管理インターフェイスが使用されます。スタンバイ WLC では、冗長管理インターフェイスで管理ユーザの認証とアカウンティングが実行されます。ローカル管理ユーザ アカウントとは別に、ユーザ認証には RADIUS または TACACS+ サーバを使用できます。これをサポートするには、冗長インターフェイスの IP アドレスをネットワーク デバイスとして RADIUS または TACACS+ サーバに追加する必要があります。認証要求は、冗長管理インターフェイスを介して RADIUS または TACACS+ サーバに送信されます。スタンバイ WLC にログオンするたびに、アカウンティング メッセージが RADIUS サーバに送信されます。アカウンティング メッセージの目的は、スタンバイ WLC コンソールでの管理者ログオン イベントをログに記録することです。

この機能は、HA SSO 機能をサポートしているすべての WLC モデルでサポートされます。

- Cisco 8500 シリーズ WLC
- Cisco 3504 WLC
- Cisco 5500 シリーズ WLC

イベントと通知

- WLC がホット スタンバイになったときのトラップ：トラップは HA ピアがホット スタンバイになったときのタイムスタンプ付きで報告され、次のようなトラップが報告されます。

  「RF notification EventType:37 Reason :HA peer is Hot-Standby...At:...」

  新しいトラップ タイプが CISCO-RF-SUPPLEMENTAL-MIB.my に追加されます。

- 一括同期が完了したときのトラップ：HA ペアリングが実行され、一括同期が完了すると、次のトラップが報告されます。

  「RF notification EventType:36 Reason :Bulk Sync Completed...At:..」

  新しいトラップ タイプが CISCO-RF-SUPPLEMENTAL-MIB.my に追加されます。

- スタンバイ WLC がダウンしたときのトラップ：スタンバイ ピアが、手動リセット、クラッシュ、メモリ リーク/ハング、またはメンテナンス モードへの移行が原因でダウンすると、次のトラップが報告されます。

  「RF failure notification ErrorType: 34 Reason :Lost Peer, Moving to Active-No-Peer State!」

CLI では、**show traplog** コマンドを入力してトラップを表示できます。

- スタンバイでの管理者ログイン時の syslog 通知

  1. 管理者がSSH経由でスタンバイにログインすると、msglog/syslogでイベントが生成されます。システム メッセージのサンプルを以下に示します。

     ***emWeb: Mar 06 20:34:42.675: #CLI-3-LOGIN_STANDBY: [SS] cli_lvl7.c:4520 [USER@9 name="admin" from="SSH"] user login success on standby controller.**

     このメッセージは、**show msglog** コマンドを入力して、スタンバイ WLC で表示できます。

  2. 管理者がコンソール経由でスタンバイにログインすると、msglog/syslog でイベントが生成されます。システム メッセージのサンプルを以下に示します。

     ***emWeb: Mar 06 20:34:42.675: #CLI-3-LOGIN_STANDBY: [SS] cli_lvl7.c:4520 [USER@9 name="admin" from="console"] user login success on standby controller.**

     このメッセージは、**show msglog** コマンドを入力して、スタンバイ WLC で表示できます。

- ピア プロセス統計情報：スタンバイ WLC のすべてのスレッドの CPU とメモリの統計情報は、10 秒ごとにアクティブ WLC と同期されます。この情報は、アクティブ WLC 上のピア統計情報を照会したときに表示されます。

  アクティブ WLC で次のコマンドを入力すると、ピア プロセス システム、CPU、およびメモリの統計情報を表示できます。

  - **show redundancy peer-system statistics**
  - **show redundancy peer-process cpu**
  - **show redundancy peer-process memory**

  GUI で、**[Monitor]** > **[Redundancy]** > **[Peer Statistics]** の順に選択すると、ピア プロセス システム、CPU、およびメモリの統計情報が表示されます。

HA セットアップでのプライマリ コントローラの交換

HA セットアップで、プライマリ コントローラが動作せず、交換する必要があるとします。スタンバイ コントローラは関連付けられているすべての AP で動作しており、HA ペアの障害が発生したコントローラのいずれかに追加できる返品許可（RMA）を新しいコントローラが受信したとします。次の手順に従い、アクティブなHAセットアップでプライマリ コントローラを交換します。

手順

ステップ 1 新しいコントローラと交換対象のコントローラで同じバージョンのコントローラ ソフトウェアが実行されていることを確認します。

ステップ 2 交換対象のコントローラと同じサブネット管理 IP アドレスを指定して、新しいコントローラを設定します。

ステップ 3 冗長性の管理、IPアドレス、およびピアプライマリを含む、HA設定で新しいコントローラを設定します。AP SSO を有効にします。

ステップ 4 AP SSO を有効にすると、コントローラがリブートします。コントローラのリブート中に、AP SSO によって現在アクティブなスタンバイ コントローラが検出されて設定が同期され、スタンバイホット状態に移行します。

（注） 現在アクティブなコントローラのHAの設定を中断したり、現在アクティブなコントローラをリブートしたりする必要はありません。設定は現在アクティブなコントローラと同期されます。