ハイ アベイラビリティの設定

- ハイ アベイラビリティに関する情報，1 ページ
- ハイ アベイラビリティの制約事項，7 ページ
- ハイ アベイラビリティの設定（GUI），10 ページ
- ハイ アベイラビリティの設定（CLI），12 ページ

ハイ アベイラビリティに関する情報

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。

1:1（アクティブ：スタンバイホット）のアクセス ポイント ステートフル スイッチオーバー（AP 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。 スイッチオーバーの原因は、手動トリガー、コントローラの障害、またはネットワークの障害のいずれかです。

AP SSO 中に、すべての AP セッションはステートフルにスイッチオーバーして、FlexConnect モードでローカルに切り替えられたクライアントを除くすべてのクライアントは認証解除され、新しいアクティブ コントローラに再アソシエートされます。

スタンバイホットコントローラは、専用のリダンダンシーポートに有線で直接接続したアクティブコントローラの状態を連続してモニタします。 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イーサネット ケーブルを使用して、冗長ポート経由で物理的に接続されていることを確認します。 また、アップリンクがインフラストラクチャスイッチに接続され、ゲートウェイが両方のコントローラから到達可能であることを確認します。

HA アーキテクチャで、リダンダンシー ポートおよびリダンダンシー マネージメント インターフェイスが導入されました。

アクティブ コントローラからスタンバイ コントローラへのクライアントのシームレスな移行もサポートされます。 実行状態にないクライアントはスイッチオーバー後に削除されます。 クライアントのステートフル スイッチオーバー（クライアント SSO）中に、クライアントがスタンバイ コントローラに関連付けられている、または設定されている場合に、クライアントの情報がそのコントローラと同期されます。 完全に認証されたクライアント、つまり、実行状態にあるクライアントはピア コントローラと同期されます。 クライアントのデータ構造は、クライアントの状態に基づいて同期されます。 過渡状態にあるクライアントでは、スイッチオーバー後にアソシエーションが解除されます。

Cisco Wireless LAN Controller 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 しているのか、アクティブ コントローラから同期されているのかに応じ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** コマンドの出力に、アクティブ コントローラとスタンバイ コントローラのペア成立後のアクセスポイントとクライアントの一括同期ステータスが表示されます。 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。 この問題は、ハイ アベイラビリティを有効にする前に NAT IP アドレスと ACL が管理インターフェイス上で設定された場合にのみ発生します。

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。
- 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） 2 つの Cisco Wireless Services Module 2（WiSM2）プラットフォーム間の HA を実現するには、コントローラを単一のシャーシに配置するか、仮想スイッチング システム（VSS）を使用してリダンダンシー VLAN を複数のシャーシ間に拡張することで、複数のシャーシに配置する必要があります。

（注） リダンダンシー VLAN は、ルーティング不能 VLAN にする必要があります。 つまり、この VLAN 用のレイヤ 3 インターフェイスを作成せず、トランク ポート上のインターフェイスで HA セットアップを複数のシャーシ間に拡張できるようにする必要があります。 リダンダンシー VLAN は、他のデータ VLAN 同様に Cisco IOS ベースのスイッチング ソフトウェアで作成する必要があります。 リダンダンシー VLAN は、バックプレーン経由でシスコ WiSM2 の冗長ポートに接続されます。 IP アドレスが自動的に生成されるため、リダンダンシー VLAN の IP アドレスを設定する必要はありません。 また、リダンダンシー VLAN が管理 VLAN と同じではないことを確認します。

（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 が有効になっている場合は、必ず、スタンバイ コントローラが RMI を使用して、他のすべてのインターフェイス（動的と管理）が無効になります。 ping は RMI だけをソースとして受け入れ、他のインターフェイスは受け入れないようにする必要があります。
- 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、バック アップされた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。
  - Cisco WiSM2 については、冗長性をイネーブルにした後、サービス ポートの再設定が必要です。 そうしないと、Cisco WiSM2 はスーパーバイザと通信できない場合があります。 冗長性をイネーブルにする前に、サービス ポートで DHCP を有効にすることを推奨します。
  - スタンバイホット コントローラで **reset** コマンドを直接使用しないことを推奨します。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。
- [Ignore AP] リストでは、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てから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。 これを行うには、HA SKU コントローラ上で **config redundancy unit secondary** コマンドを実行する必要があります。
  - **config redundancy unit secondary** コマンドの実行が成功したら、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、FTP および TFTP サーバと通信するために RMI を使用します。

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。

リダンダンシー 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。

Cisco WiSM2 では、利用可能な物理リダンダンシー ポートがないため、リダンダンシー VLAN を Cisco Catalyst 6000 Supervisor Engine 上で設定する必要があります。

Cisco WiSM2 のリダンダンシー ポートおよびリダンダンシー VLAN には、最後の 2 オクテットが RMI の最後の 2 オクテットから取得され、自動的に生成された IP アドレスが割り当てられます。 最初の 2 オクテットは常に 169.254 です。 たとえば、RMI の IP アドレスが 209.165.200.225 の場合、リダンダンシー ポートの IP アドレスは 169.254.200.225 です。

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。

暗号化のサポート

アクティブおよびスタンバイ コントローラ間の HA 関連メッセージの暗号化は、Data Transport Layer Security（DTLS）の使用でサポートされています。 暗号化は、デフォルトで無効になっています。 暗号化は、設定、AP、およびクライアント同期でサポートされます。

暗号化は、アクティブおよびスタンバイ コントローラが管理ポートのリダンダンシー インターフェイス経由で通信する場合に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。 ただし、リダンダンシー ポートにマッピングされた RMI がデフォルト オプションです。 RMI がリダンダンシー ポートにマッピングされていない場合は、HA 情報がネットワーク経由で送信されるため、暗号化が有効になります。

暗号化が 1 台のコントローラで有効になっており、他方で無効の場合、コントローラはペアになりますが、冗長リンクによるデータ同期は暗号化されません。 暗号化は、設定および AP とクライアントの同期化でサポートされています。 ロール ネゴシエーションとキープアライブ メッセージは暗号化されません。

ハイ アベイラビリティの制約事項

- 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 を有効にしている場合は、サービス インターフェイスを介して Cisco WiSM2 GUI にアクセスすることはできません。 回避策は、HA が確立された後に、サービス ポート インターフェイスを再作成することです。
- 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。
- 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 リリースがある場合、アクティブ コントローラで **config boot backup** コマンドを入力すると、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。
- **debug** コマンドおよび **show** コマンドだけが、スタンバイホット コントローラで許可されます。
- 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。

- HA SSO 設定で LAG が有効になっており、2 つのポートがプライマリおよびセカンダリ コントローラの両方に接続されている場合、アクティブ コントローラで 1 つのスイッチ ポートが動作不能になると、スイッチオーバーが発生します。 リダンダンシー マネジメント インターフェイスが DP にマッピングされている場合に、いずれかのポートの動作不能が 300 ミ

リ秒を超えると、SSO が発生します。これは、LAG のコンバージェンスが約 5 秒かかるためです。

- 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。
- Cisco WiSM2 および Cisco Catalyst 6500 シリーズ Supervisor Engine 2T では、HA が有効になっている場合、スイッチオーバー後に AP は接続を解除して WiSM2 コントローラと再アソシエートする可能性があります。 この問題の発生を防ぐために、HA を設定する前に、ポートチャネルでアクティブおよびスタンバイの両方の Cisco WiSM2 コントローラの詳細（ポートが同じ順序に保たれていて、ポート チャネル ハッシュ分散で固定アルゴリズムが使用されている）を確認することをお勧めします。 これらが適切でない場合、ポート チャネル分散

を訂正し、Cisco Catalyst 6500 シリーズ Supervisor Engine 2T から Cisco WiSM2 をリセットする必要があります。

- 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

（注） SSO が有効な場合、Web UI/Telnet 機能を使用しても、サービス ポートの Cisco Prime Infrastructure/Prime NCS を使用しても、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ことはできません。

- コントローラのスイッチオーバー後に、子メッシュ アクセス ポイント（MAP）とともに、クライアントは接続を解除されて新しいアクティブ コントローラに再 join されます。 メッシュ ツリー全体が再構築されます。 ルート アクセス ポイント（RAP）のクライアントも接続を解除されますが、RAP はコントローラと共にそのまま残ります。
- 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）

はじめる前に

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。

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] ページが表示されます。

ステップ 2 [Redundant Management IP] および [Peer Redundant Management IP] テキスト ボックス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 マスクが設定ページに表示されます。 HA ピアが使用可能で稼働している場合にのみ、サービス ポートのピア IP アドレスとネット マスクがピアにプッシュできます。 HA 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 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にのみ、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 （任意）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ている場合にピア 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 を有効にすると、[Global Configuration] ページで次のパラメータを設定する必要がありません。

- [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。

HA を有効にし、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、コンソールまたはサービス ポートを介してのみ、管理できます。

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 [Apply] をクリックします。

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] ページが表示されます。

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 次の手順に従って、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] ページが表示されます。

このページでは、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 ルートの概要を示します。 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 アドレス、IP ネットマスク、およびゲートウェイ IP アドレスを入力します。
d) [Apply] をクリックします。

ハイ アベイラビリティの設定（CLI）

はじめる前に

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。

コントローラのハイ アベイラビリティを設定するには、次の手順を実行する必要があります。

- 次のコマンドを入力して、ローカル リダンダンシー IP アドレスおよびピア リダンダンシー マネジメント IP アドレスを設定します。
config interface address redundancy-management *ip-addr1* **peer-redundancy-management** *ip-addr2*
- 次のコマンドを入力して、コントローラのロールを設定します。
config redundancy unit {**primary** | **secondary**}
- 次のコマンドを入力して、冗長モードを設定します。
config redundancy mode {**sso** | **none**}

（注） 両方のコントローラはリブートし、次にアクティブおよびスタンバイホット コントローラのロールをネゴシエートします。

- 次のコマンドを入力して、冗長性を設定します。
config redundancy mode {**sso** {**ap** | **client**} | **disable**}

（注） AP SSO とクライアント SSO を選択できます。

- 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。

- 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。

- 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。

- 次のコマンドを入力して、手動スイッチオーバーを開始します。
  redundancy force-switchover

  手動スイッチオーバーが必要な場合のみこのコマンドを実行します。

- 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、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、ハッシュ分散を固定に設定します。

  トラブルシューティングのヒント
  config port-channel hash-distribution fixed

- 次のコマンドを入力して、ポート チャネル メンバーの順序および負荷値を確認します。

  トラブルシューティングのヒント
  show etherchannel port-channel

- 次のコマンドを入力して、冗長ステータスを表示します。
  show redundancy summary
- 次のコマンドを入力して、リダンダンシー マネジメント 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
- 次のコマンドを入力して、リダンダンシー マネージャのコマンドをデバッグします。
  debug rmgr {packet | events | errors | detail}
- 次のコマンドを入力して、リダンダンシー 同期マネージャのコマンドをデバッグします。
  debug rsnyncmgr {packet | events | errors | detail}
- 次のコマンドを入力して、リダンダンシー ファシリテータのコマンドをデバッグします。
  debug rfrac {packet | events | errors | detail}