



ハイ アベイラビリティの使用

次の各トピックでは、ハイ アベイラビリティ（冗長性）およびユニットとゲートウェイで利用可能な保護オプションについて説明します。

- 「ハイ アベイラビリティの概要」(P.E-1)
- 「Cisco ANA ユニットのハイ アベイラビリティ設定」(P.E-8)
- 「ウォッチドッグ プロトコルの管理」(P.E-12)
- 「ハイ アベイラビリティ イベント パラメータ」(P.E-14)



(注)

ハイ アベイラビリティは、Cisco ANA で使用可能なオプション機能です。Cisco ANA は、Cisco ANA ゲートウェイにハイ アベイラビリティを設定するためのソリューションではありません。Veritas を使用する Cisco ANA ゲートウェイにハイ アベイラビリティを設定する際の情報については、シスコの代理店にお問い合わせください。

ハイ アベイラビリティの概要

ハイ アベイラビリティ アーキテクチャは、広範囲のハードウェアおよびソフトウェア障害を検出し、障害から回復することにより、Cisco ANA 機能の継続的な可用性を確保します。システムを分散設計することで、1つの障害で発生した影響の範囲を制限できます。これにより、すべての管理サービスのクラッシュにつながる可能性がある、あらゆるタイプの障害が「ドミノ」効果で発生するのを防ぎます。

サーババックボーンのハイ アベイラビリティは、いくつかの補足的なレベルで達成されます。次の例を参考にしてください。

- NEBS 3 に準拠したキャリア クラス サーバのハードウェア
- 障害の発生したプロセスを監視し、必要に応じて、自動的にリロードする役割を担う各ユニット内の内部ウォッチドッグ
- ユニットグループの N + m のウォーム スタンバイ保護



(注)

Cisco ANA は、Cisco ANA ゲートウェイにハイ アベイラビリティを設定するためのソリューションではありません。Veritas を使用する Cisco ANA ゲートウェイにハイ アベイラビリティを設定する際の情報については、シスコの代理店にお問い合わせください。

詳細については、次のトピックを参照してください。

- 「ウォッチドッグ プロトコル」 (P.E-2)
- 「ユニット N+m ハイアベイラビリティ」 (P.E-2)
- 「障害時のダウンタイムの予測」 (P.E-4)

ウォッチドッグ プロトコル

ウォッチドッグ プロトコルは、AVM プロセスを監視して、障害の発生した AVM が再起動したことを確認します。ウォッチドッグ プロトコルは通常、GUI に「AVM Protection」と表示されます。ユニットはそれぞれ、複数のプロセスを実行します。これらのプロセスには、1 つの制御プロセスと、VNE を実行するいくつかの AVM プロセスがあります。ユニット内の各プロセスは完全に独立しています。1 つのプロセスの障害が同じマシンの他のプロセスに影響を与えないように、設計全体で分離概念が採用されています。各ユニットの正確なプロセス数は、ユニットの容量および計算能力によって異なります。

制御プロセスはウォッチドッグ プロトコルを実行し、このプロトコルにより、ユニット上のその他すべてのプロセスが絶えず監視されます。このウォッチドッグ プロトコルでは、各 AVM プロセスが制御プロセスと絶えずハンドシェイクする必要があります。制御プロセスとのハンドシェイクに特定の回数失敗したプロセスは、自動的にキャンセルされ、リロードされます。

制御プロセスの動的設計により、ランタイムのアダプテーションとエスカレーションが実装されます。エスカレーション プロシージャでは、AVM はサスペンド モードになります。つまり、プロセスは停止します。エスカレーション プロシージャの一例として、ソフトウェア問題が再発していることが疑われるため、所定の期間内に n 回を超えるクラッシュが発生したプロセスのリロードを停止することが挙げられます。

リロード プロセスはそのユニットに限定されるため、非常に迅速で、ダウンタイムが最小限に抑えられます。このプロセスは、その直前のキャッシュ情報（パフォーマンスを改善するために使用される一時的な永続性）を使用できるので、スタック プロセスが検出されると、プロセスのリロードに数秒しかかからず、データも失われません。

ウォッチドッグがプロセスをリロードすると、すべてのウォッチドッグ アクティビティがログに記録され、アラームが生成されて送信されます。



(注)

アラーム永続性メカニズムにより、システムは、VNE、AVM、ユニット、またはシステム全体がダウンしているときに発生したイベントに関連するアラームを消去できるため、システムの整合性が維持されます。アラーム永続性の詳細については、付録 F 「VNE 永続性メカニズム」を参照してください。

pulse interval や *retry times* などの、すべてのウォッチドッグ プロトコル パラメータをレジストリに設定できます。これらのパラメータ値が高くなるほど、AVM またはユニットの障害が持続する時間は長くなりますが、障害が実際に発生したかどうかの確実性は増します。これらのパラメータを低い値に設定すると、AVM またはユニットが回復するまでの時間を短縮できますが、これによって、「フォールス ポジティブ」が発生する可能性があり、AVM がビジー状態のとき、あるいはユニットが高負荷のデータを処理しているときに、不必要に AVM を再起動したり、AVM がスタンバイ ユニットに戻ったりすることがあります。

ユニット N+m ハイアベイラビリティ

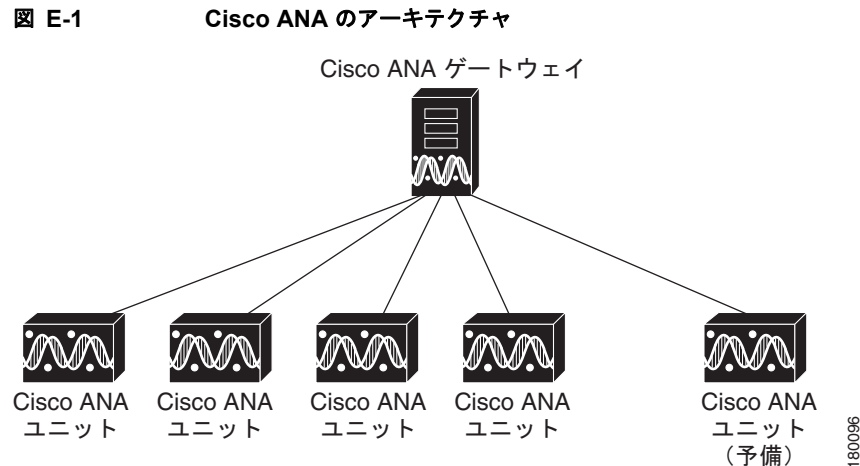
クラスタ化された N+m ハイアベイラビリティ メカニズムで使用される Cisco ANA ファブリックは、ユニットの障害に対処するように設計されています。このような障害には、ハードウェア障害、オペレーティングシステムの障害、電源障害、ネットワーク障害などがあり、これらの障害によって、ユニットの接続が Cisco ANA ファブリックから切断されます。

ユニットの可用性はゲートウェイに確立され、ネットワーク内のすべてのユニットを監視する保護マネージャプロセスを実行します。保護マネージャは、誤作動しているユニットを検出すると、そのユニットのクラスタ内のスタンバイサーバの 1 台に信号を自動的に送信して、障害の発生したユニットの設定を（システムレジストリから）ロードし、その管理対象ネットワーク要素のすべてを引き継ぎます。この設計では、保護とリソースが犠牲になる可能性が高くなります。このような可能性に対する対策は、余分のマシンを追加せずにネットワークをクラスタにセグメント化することから、設定時に各ユニットにウォームスワップ可能な空きユニットを備えることまでに及びます。地理的条件に応じてユニットをクラスタ化したり、負荷の高いクラスタに空きユニットを追加したりすることを推奨します。

冗長スタンバイユニットのスイッチオーバーが発生しても、システムの情報失われません。これは、すべての情報がネットワークから自動検出され、ストレージを永続的に同期化する必要がないからです。結果的に、冗長スタンバイユニットは、ネットワーク要素から情報が永続的に破壊される危険を伴わずにすべての情報を再学習します。さらに、クラスタが飽和状態（クラスタ内の 2 台以上のユニットに障害が同時に発生し、予備のマシンがない場合）になると、残りのユニットが自身のネットワーク範囲を引き続き正常に動作させ、管理します。

ユニットが 1 台設定されている場合、そのユニットをアクティブユニットまたはスタンバイユニットとして指定できます。ゲートウェイに接続されているアクティブユニット（スタンバイユニットを除く）は、保護グループとして認識されます。ゲートウェイに対して設定されているスタンバイユニットは、その保護グループにリンクされます。2 つ以上の保護グループを定義できます。定義する各保護グループには、保護される側のユニットの一群と、保護する側のスタンバイユニット 1 台が含まれます。

図 E-1 に、ユニットの保護グループ（クラスタ）を示します。この保護グループでは、スタンバイとして設定された 1 台のユニットを使用するゲートウェイによってコントロールされています。



この設定例では、ゲートウェイが保護グループ内のユニットの 1 台に障害が発生したと判断すると、保護グループのスタンバイユニットに対して、障害が発生したユニットの設定をただちにロードするよう通知します。スタンバイユニットは、すべての AVM および VNE を含めて障害が発生したユニットの設定をロードし、障害が発生したユニットと同様に機能します。

すべてのイベントが Cisco ANA EventVision システム ログに記録され、このログを使用して、障害が発生したユニットを再度アップにするために必要なアクションを実施できます。障害が発生したユニットが動作可能になると、そのユニットを新しいスタンバイユニットとして設定するか、そのユニットを保護グループに復帰させて別のユニットをスタンバイユニットとして設定するかを決定できます。

障害時のダウンタイムの予測

ユニットまたは AVM に障害が発生したときに、システムがダウンする時間の長さは、障害のタイプ、コンポーネントが機能していないことを検知するまでにかかる時間、および回復時間の長さ（ユニットまたは AVM がリロードし、システムが再び正常に機能し始めるまで）によって異なります。

次のトピックで説明するように、3 つのタイプ障害が発生する可能性があります。

- 「壊滅的なプロセス障害」(P.E-4)
- 「タイムアウト プロセス障害」(P.E-5)
- 「タイムアウト マシン障害」(P.E-7)

壊滅的なプロセス障害

各 AVM には、ログ ファイルが格納されており、このファイルでは、AVM プロセスがメモリを使い果たすなどの壊滅的な障害に関するログ メッセージを Perl プロセスによって常に監視します。Mean Time To Repair (MTTR; 平均修理時間) は AVM をロードするライフ サイクルに基づいているため、このような障害が発生すると、Perl プロセスはただちに AVM を再起動します。

表 E-1 では、このような障害が発生したときの、さまざまな AVM の影響について説明します。

表 E-1 AVM の壊滅的なプロセス障害の影響

プロセス	影響	MTTR	障害が発生する確率
AVM 0 (スイッチ AVM)	マシンへのメッセージまたはマシンからのメッセージの喪失。	ブートストラップに到達するまで 1 分。	システムでメッセージが常に送受信されているため、高い確率で障害が発生します。
AVM 99 (管理 AVM)	Golden Source に加えられた変更に関するレジストリ通知の喪失。	ブートストラップに到達するまで 1 分。	VNE が初めてシステムにロードされたときにだけレジストリ変更が行われるので、この障害は低い確率で発生します。 システムの動作中には、変更はめったに行われません。
AVM 100 (トラップ管理 AVM)	デバイスからのトラップおよび syslog の喪失。	ブートストラップに到達するまでの 1 分に加え、すべての VNE がトラップおよび syslog に再登録されるまでの時間。	トラップおよび syslog がライブの、スケールされたシステムで絶えず受信されるため、リロード期間中にトラップおよび syslog が高い確率で失われます。

プロセス	影響	MTTR	障害が発生する確率
AVM 11 (ゲートウェイ)	あらゆる種類の永続性の喪失。	ブートストラップに到達するまでスケールで 6 ~ 10 分。	AVM 11 は、Oracle 通信およびアラーム処理などのさまざまなゲートウェイ機能を処理するので、この期間にイベント永続性が高い確率で失われます。
AVM 101 ~ 999	AVM が管理するデバイスのセクションに対する管理の喪失。	ブートストラップに到達するまでの 1 分に加え、VNE をロードする時間。この時間は、VNE の数とタイプによって異なる。	AVM がダウン状態のとき、アラーム処理は発生しないため、VNE に送信されたトラップおよび syslog は失われます。 1 分間のうちに高い確率でトラップおよび syslog が失われます。

タイムアウト プロセス障害

各 AVM は、管理 AVM (AVM 99) が、事前設定された間隔で AVM に送信されたウォッチドッグプロトコルパルスメッセージを使用して常時監視します。AVM が、事前設定された試行回数後にパルスメッセージに応答しなかった場合、管理 AVM はプロセスを再開します。

また、管理プロセスは、AVM を再起動した回数の履歴も保持します。管理プロセスが事前設定された再起動回数の最大数に達した場合、これは AVM に重大な問題が発生したことを示すことから、管理 AVM は AVM を再起動して停止します。各再起動がシステム イベントとしてログに記録されます (この AVM がすべての永続性を処理するので、AVM 11 が再起動されるのを除く)。

システム内の AVM の障害は、壊滅的なプロセス障害の計測に使用される方法と同様の方法で計測されます (表 E-1 を参照)。この場合、ウォッチドッグプロトコルのオーバーヘッドが加算されます。これは、パルス間隔に再起動の試行回数を乗算することによって計測されます。

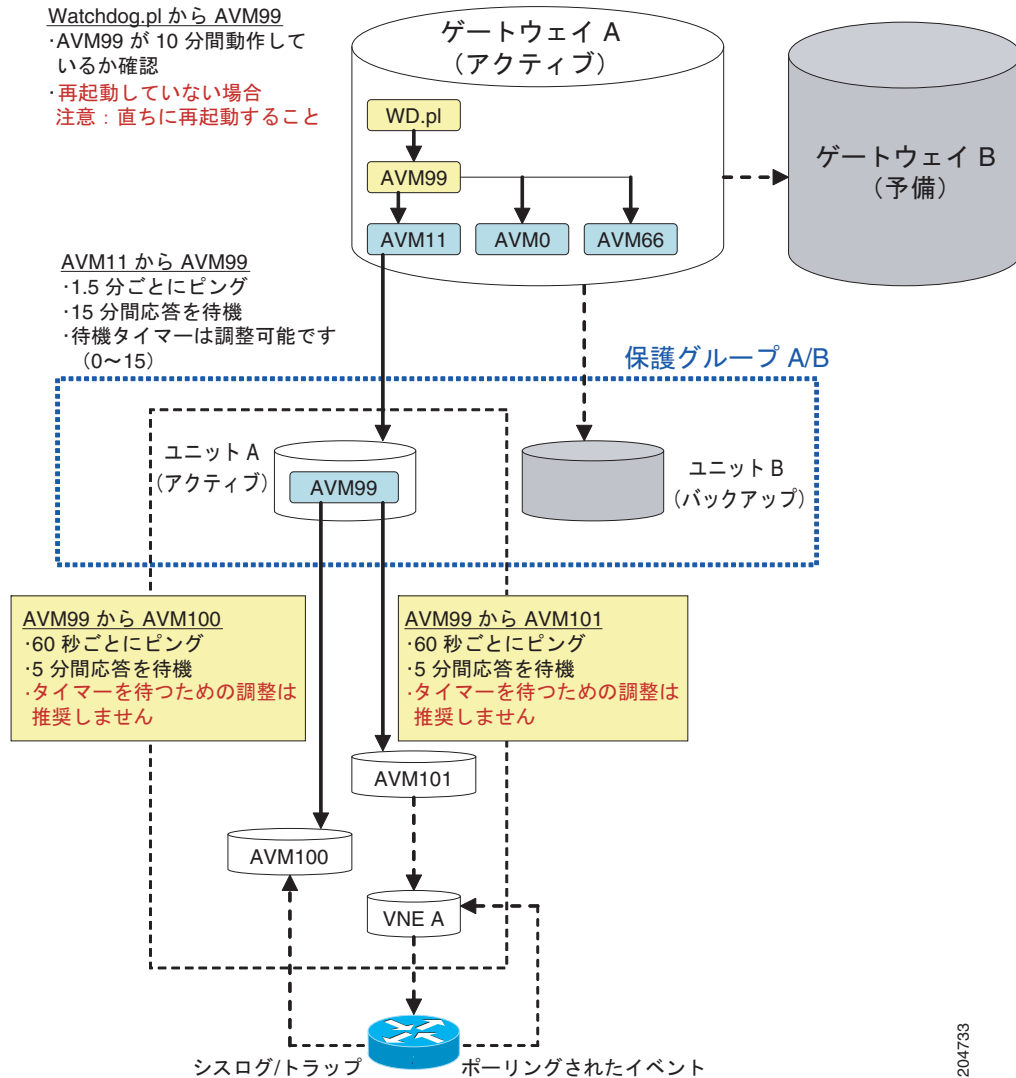


(注)

- 事前設定された再起動の最大回数は、管理プロセスが AVM のリロードを試行しなくなってから 5 回です。
- システムが、AVM (AVM 100 を含む) が機能していないことを検出するまで約 1 分かかります。
- AVM (AVM 100 を含む) がリロードし、システムが再び正常に機能し始めるまでの回復時間は、約 5 分です (AVM ごとの VNE の数および各 VNE の複雑度によって異なります)。

図 E-2 に、ハイアベイラビリティ タイマー パラメータが、AVM の監視中にどのように機能するかの標準的な例を示します。

図 E-2 HA パラメータ タイマーおよび AVM の監視例



AVM のチケット処理ダウンタイムの測定

AVM で障害が発生したときに、チケット処理がダウンする時間は次の係数の合計として測定されます。

- ・ AVM に障害が発生したことを判別するまでにかかる時間。
- ・ AVM がリロードするまでにかかる時間。この時間は VNE の数によって異なります。
- ・ VNE に syslog またはトラップを渡す (AVM 100 の場合)、あるいはゲートウェイにイベントを渡す (AVM 101 ~ 999 の場合) までにかかる時間。



(注) AVM 99 (管理 AVM) が起動してから最初の 30 分間、システムはハイアベイラビリティの問題を検出するための監視を行いません。これにより、システムが動作するのに十分な時間を確保します。

タイムアウト マシン障害

Cisco ANA ゲートウェイは、ユニットの管理 AVM にウォッチドッグ プロトコル パルス メッセージを事前設定された間隔で送信して、絶えずユニットを監視します。ユニットの管理 AVM が、事前設定された再試行回数後にパルス メッセージに 응답しない場合、ゲートウェイはスタンバイ ユニートをロードして置き換えます。

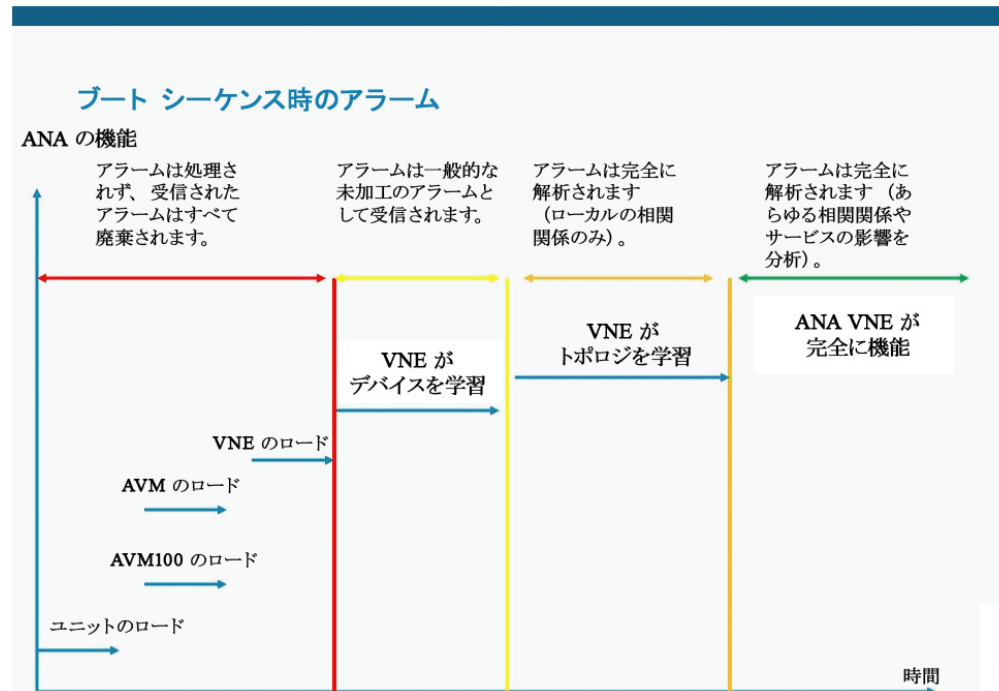
システム上でこのような障害が発生した際の影響とは、応答しないユニットが一定の時間デバイスを管理しないということです。この管理されない時間は、パルス間隔に再試行回数を乗算し、これにユニットのロード時間を加算することによって測定されます。



(注) ユニートのロード時間は、表 E-1 に示すように、AVM および、VNE がモデル化を完了するために必要なロード時間によって異なります。

図 E-3 に、ロード時間中にユニットがイベントをどのように処理するかを示します。

図 E-3 イベント処理からシステム再起動までの段階



ユニットのチケット処理ダウンタイムの測定

ユニットに障害が発生したときに、チケット処理がダウンする時間は次の係数の合計として測定されます。

- ユニートに障害が発生したと判断するまでにかかる時間 (PING 間隔によって異なる)。
- ユニートがリロードするのにかかる時間 (ユニットの AVM および VNE の数によって異なる)。
- 相互に関係するイベントをゲートウェイに渡すのにかかる時間 (デバイス履歴を取得するのにかかる最低 5 分に加え、AVM あたりの VNE の数によって異なる可変時間)。

Cisco ANA ユニットのハイ アベイラビリティ設定

次のトピックでは、保護グループのカスタマイズ、ユニットのハイ アベイラビリティ設定、スタンバイユニットの設定について説明します。

- 「保護グループを使用したユニットのハイ アベイラビリティ設定」(P.E-8)
- 「スタンバイ ユニットの設定」(P.E-9)
- 「保護グループへのユニットの割り当ての確認」(P.E-10)
- 「ユニットの保護グループの変更」(P.E-11)
- 「スタンバイ ユニットへの切り替え」(P.E-11)

保護グループを使用したユニットのハイ アベイラビリティ設定

ユニットのデフォルト設定を変更し、その設定をカスタマイズされた保護グループに割り当てることができます。保護グループの作成、表示、および削除の詳細については、「[保護グループの管理](#)」(P.6-16) を参照してください。

さらに、ユニットのハイ アベイラビリティをイネーブルまたはディセーブルにできます。つまり、これらの設定により、ユニットをどの保護グループに割り当てるか、およびユニットをハイ アベイラビリティに対してイネーブルにするかどうかを定義できます。

スタンバイ ユニットに切り替わる時にユニットまたは AVM がダウンする時間については、「[障害時のダウンタイムの予測](#)」(P.E-4) を参照してください。



(注)

デフォルトでは、Cisco ANA ファブリック内のすべてのユニットは、デフォルト pg 保護グループに属し、ハイ アベイラビリティはイネーブルになります。

次のことを行うための詳細設定は、レジストリ内で見つけることができます。

- プロセスがダウンしているときに検出するためのタイムアウトを含め、各プロセスのウォッチドッグプロトコルをイネーブルにする、またはディセーブルにする。
- ユニットがダウンしているときに検出するための、タイムアウトをコントロールする。

詳細については、シスコの代理店にお問い合わせください。

ユニットをハイ アベイラビリティ用に設定し、保護グループに割り当てる手順は、次のとおりです。

- ステップ 1** [Cisco ANA Manage] ウィンドウで、[ANA Servers] ブランチを選択します。[ANA Servers] ブランチが表示されます。
- ステップ 2** 次のいずれかの方法で [New ANA Unit] ダイアログボックスを開きます。
 - [ANA Servers] ブランチを右クリックし、[New ANA Unit] を選択する。
 - ツールバーにある [New ANA Unit] をクリックする。
 - [File] > [ANA Unit] を選択する。

ステップ 3 新規ユニットの情報を入力します。

フィールド	説明
[IP Address]	ユニットの IP アドレスを入力します。IP アドレスは一意でなくてはなりません。 (注) 同じ IP アドレスを持つユニットがすでに設定されている場合は、エラーメッセージが表示されます。
[Enable Unit Protection]	このチェックボックスがオンになっていることを確認してください。このオプションがオンのとき、ユニットでハイアベイラビリティがイネーブルになります。
[Standby Unit]	このチェックボックスがオンになっていないことを確認してください。
[Protection Group]	新たに作成されたユニットがスタンバイ ユニットとして機能する保護グループを選択します。 保護グループの詳細については、次を参照してください。 <ul style="list-style-type: none"> 「保護グループの管理」(P.6-16) 「ユニットの保護グループの変更」(P.E-11)
[Gateway IP]	ゲートウェイの IP アドレスが表示されていることを確認してください。

ステップ 4 [OK] をクリックします。新しいユニットが [Cisco ANA Manage] ウィンドウに表示されます。

新しいユニットが取り付けられ、到達可能な場合は、次のイベントが発生します。

- そのユニットは自動的に起動します。
- そのユニットはゲートウェイに登録されます。
- 新しいユニットの設定レジストリが Golden Source に作成されます。Golden Source レジストリの詳細については、付録 D 「Golden Source レジストリ」を参照してください。

スタンバイ ユニットの設定

Cisco ANA Manage を使用すると、スタンバイ ユニットを設定して、スタンバイ ユニットを保護グループに割り当てることができます。

スタンバイ ユニットに切り替わる時にユニットまたは AVM がダウンする時間については、「障害時のダウンタイムの予測」(P.E-4) を参照してください。

始める前に

アクティブ ユニットをスタンバイ ユニットに変更する場合は、「Cisco ANA ユニットの削除」(P.4-9) で説明するように、最初にアクティブ ユニットを削除する必要があります。

スタンバイ ユニットを設定するには、次の手順を実行します。

ステップ 1 [Cisco ANA Manage] ウィンドウで、[ANA Servers] ブランチを選択します。[ANA Servers] ブランチが表示されます。

ステップ 2 次のいずれかの方法で [New ANA Unit] ダイアログボックスを開きます。

- [ANA Servers] ブランチを右クリックし、[New ANA Unit] を選択する。
- ツールバーにある [New ANA Unit] をクリックする。

- [File] > [New ANA Unit] を選択する。



(注) ユニットの設定の詳細については、第 4 章「Cisco ANA ゲートウェイとユニットの管理」を参照してください。

ステップ 3 スタンバイ ユニットの情報を入力します。

フィールド	説明
[IP Address]	<p>ユニットの IP アドレスを入力します。IP アドレスは一意でなくてはなりません。</p> <p>(注) 同じ IP アドレスを持つユニットがすでに設定されている場合は、エラー メッセージが表示されます。</p>
[Enable Unit Protection]	<p>このチェックボックスがオンになっていることを確認してください。このオプションがオンのとき、ユニットでハイ アベイラビリティがイネーブルになります。</p> <p>(注) [Enable Unit Protection] チェックボックスは、デフォルトで選択されています。このオプションをディセーブルにしないことを強く推奨します。</p>
[Standby Unit]	<p>ユニットをスタンバイ ユニットとして定義するには、このチェックボックスをオンにします。</p>
[Protection Group]	<p>新たに作成されたユニットがスタンバイ ユニットとして機能する保護グループを選択します。</p> <p>保護グループの詳細については、次を参照してください。</p> <ul style="list-style-type: none"> • 「保護グループの管理」(P.6-16) • 「ユニットの保護グループの変更」(P.E-11)
[Gateway IP]	<p>ゲートウェイの IP アドレスが表示されていることを確認してください。</p>

ステップ 4 [OK] をクリックします。



(注) スタンバイ ユニットは、ナビゲーション ツリーの [ANA Servers] ブランチに表示されません。

ユニットが割り当てられている保護グループの変更についての詳細は、「[ユニットの保護グループの変更](#)」(P.E-11) を参照してください。

保護グループへのユニットの割り当ての確認

ユニットが現在割り当てられている保護グループを表示できます。これにより、設定または割り当てが初期の展開計画と一致しているかを一目で確認できます。

ユニットおよび保護グループの割り当てを表示するには、[Cisco ANA Manage] ナビゲーション ペインで [ANA Servers] ブランチを選択します。[ANA Servers] ブランチのプロパティは、各ユニットおよびスタンバイ ユニットが現在所属する保護グループの詳細を含め、[Content] 領域に表示されます。

ユニットの保護グループの変更

ユニットが割り当てられている保護グループを簡単かつ迅速に変更できます。

ユニットの保護グループを変更する手順は、次のとおりです。

ステップ 1 [Cisco ANA Manage] ウィンドウで、[ANA Servers] ブランチを選択します。[ANA Servers] ブランチが表示されます。

ステップ 2 [ANA Servers] ブランチを展開し、目的の [ANA Unit] サブブランチを選択します。

ステップ 3 次のいずれかの方法で [ANA Unit Properties] ダイアログボックスを開きます。

- [ANA Servers] ブランチを右クリックし、[Properties] を選択する。
- ツールバーにある [Properties] をクリックする。
- [File] > [Properties] を選択する。



(注) ユニットの設定の詳細については、第 4 章「Cisco ANA ゲートウェイとユニットの管理」を参照してください。

ステップ 4 [Protection Group] ドロップダウンリストで、ユニットを割り当てる保護グループを選択します。

ステップ 5 [OK] をクリックして、選択したユニットの更新された保護グループ設定を保存します。[Cisco ANA Manage] ウィンドウが表示されます。

スタンバイ ユニットへの切り替え

Cisco ANA Manage では、スタンバイ ユニットに手動で、または自動的に切り替えることができます。

- ゲートウェイがアクティブユニットの 1 台に障害が発生したことを検出すると、スタンバイユニットへの自動スイッチオーバーが発生します。このような障害には、ハードウェア障害、オペレーティングシステムの障害、電源障害、ネットワーク障害などがあり、これらの障害によって、ユニットの接続が Cisco ANA ファブリックから切断されます。自動スイッチオーバーの詳細は、「[ユニット N+m ハイアベイラビリティ \(P.E-2\)](#)」を参照してください。
- 手動によるスタンバイユニットへの切り替えは、メンテナンスのためにユニットを一時的にシャットダウンする必要がある場合に役立ちます。

スイッチオーバーが発生すると、Cisco ANA は、障害が発生したユニットからすべてのデータを同じ保護グループ内のスタンバイユニットに自動的に転送します。元のユニットはスタンバイ設定から削除され、[Cisco ANA Manage] ウィンドウの [ANA Servers] ブランチに表示されなくなります。

スタンバイユニットに手動で切り替える手順は、次のとおりです。

ステップ 1 [Cisco ANA Manage] ウィンドウで、[ANA Servers] ブランチを選択します。[ANA Servers] ブランチが表示されます。

ステップ 2 [ANA Servers] ブランチを展開し、目的の [ANA Unit] サブブランチを選択します。

ステップ 3 目的のユニットを右クリックし、[Switch] を選択します。確認用のメッセージが表示されます。

ステップ 4 [Yes] をクリックします。スタンバイ ユニットがアクティブ ユニットになり、[ANA Servers] ブランチに表示されます。元のユニットは設定から削除され、安全にシャットダウンできます。そのユニットは、[Cisco ANA Manage] ウィンドウの [ANA Servers] ブランチに表示されなくなります。



(注) ユニットのフェールオーバーが発生した場合、2 台以上のスタンバイ ユニットが利用可能であれば、Cisco ANA ゲートウェイは冗長ユニットをランダムに選択します。

ウォッチドッグ プロトコルの管理

次のトピックでは、ユニットに AVM を定義し、AVM でウォッチドッグ プロトコルをイネーブルまたはディセーブルにする方法について説明します。

- 「AVM のハイ アベイラビリティ設定」(P.E-12)
- 「ウォッチドッグ プロトコル設定の表示および変更」(P.E-13)

AVM のハイ アベイラビリティ設定

デフォルトでは、Cisco ANA ファブリック内のすべての AVM がウォッチドッグ プロトコルによって管理されます。Cisco ANA Manage を使用すると、ユニットに AVM を定義し、各 AVM でウォッチドッグ プロトコルをイネーブルまたはディセーブルにすることができます。

AVM を定義する手順は、次のとおりです。

- ユニットを取り付ける必要があります。
- ユニートを転送ネットワークに接続する必要があります。
- 次のデフォルト AVM が動作している必要があります。
 - AVM 0 : スイッチ AVM
 - AVM 99 : 管理 AVM
 - AVM 100 : トラップ管理 AVM
- 新しい AVM は、ユニット内で一意の識別番号を持っている必要があります。



(注) AVM の定義に関する詳細については、第 5 章「AVM および VNE の管理」を参照してください。

AVM をハイ アベイラビリティ用に定義する手順は、次のとおりです。

ステップ 1 [Cisco ANA Manage] ウィンドウで、[ANA Servers] ブランチを選択します。[ANA Servers] ブランチが表示されます。

ステップ 2 [ANA Servers] ブランチを展開し、目的の [ANA Servers Entity] サブブランチを選択します。

- ステップ 3** 次のいずれかの方法で [New AVM] ダイアログボックスを開きます。
- 目的のユニットを右クリックし、[New AVM] を選択する。
 - ツールバーにある [New AVM] をクリックする。
 - [File] > [New AVM] を選択する。
- ステップ 4** AVM のプロパティを定義します。詳細については、第 5 章「AVM および VNE の管理」を参照してください。
- ステップ 5** [Enable AVM Protection] チェックボックスをオンにして、AVM のウォッチドッグ プロトコルをイネーブルします。



(注) [Enable AVM Protection] チェックボックスは、オフにしないことを強く推奨します。

- ステップ 6** [OK] をクリックします。ウォッチドッグ プロトコルがイネーブルになった新しい AVM は、選択されたユニットに追加され、コンテンツ領域に表示されます。
- 新しい AVM を追加すると、指定したユニットに新しい AVM のレジストリ情報が作成されます。この時点で AVM は、VNE のホストとして機能できます。

ウォッチドッグ プロトコル設定の表示および変更

AVM のステータスやロケーションなどの AVM のプロパティを表示できます。また、ウォッチドッグ プロトコルをイネーブルにしたり、ディセーブルにしたりするなど、AVM のプロパティの一部を編集できます。



(注) AVM の定義と編集に関する詳細については、第 5 章「AVM および VNE の管理」を参照してください。

AVM 設定を表示および編集する手順は、次のとおりです。

- ステップ 1** [Cisco ANA Manage] ウィンドウで、[ANA Servers] ブランチを選択します。[ANA Servers] ブランチが表示されます。
- ステップ 2** ナビゲーション ツリーで [ANA Servers] ブランチを展開し、目的の AVM サブブランチを選択します。
- ステップ 3** 次のいずれかの方法で [AVM Properties] ダイアログボックスを開きます。
- 目的の AVM を右クリックして、[Properties] を選択する。
 - ツールバーにある [Properties] をクリックする。
 - [File] > [Properties] を選択する。
- ステップ 4** 必要に応じて、AVM の詳細を編集します。



(注) [Enable AVM Protection] チェックボックスは、オフにしないことを強く推奨します。

- ステップ 5** [OK] をクリックします。AVM の新しいプロパティがコンテンツ領域に表示されます。

ハイ アベイラビリティ イベント パラメータ

表 E-2 に、Cisco ANA EventVision に表示されるハイ アベイラビリティ イベントをトリガーできるフェールオーバー パラメータのデフォルト設定値を示します。具体的なイベントの情報については、『Cisco Active Network Abstraction 3.6.7 User Guide』のエラー リファレンスを参照してください。

表 E-2 フェールオーバーのデフォルト設定

#	説明	デフォルト値	レジストリのエントリ名
1	猶予期間（イベントが発生しなかったシステム起動時からの時間） ¹	1800000 ミリ秒（30 分）	Delay
2	AVM のタイムアウト	300000 ミリ秒（5 分）	Timeout
3	ユニットのタイムアウト	300000 ミリ秒（5 分） (注) これは初期の回復時間で、分単位で定義されます。この時間には、デバイスのポーリングとインベントリの作成が含まれます。RCA やトポロジなどのエンドツーエンドサービスでは、これらのサービスが利用可能になるまでにかかる時間が長くなる可能性があります。	Timeout
4	AVM が繰り返し応答しない	10800000 ミリ秒（180 分）以内に AVM の再起動を最大 5 回を試行します。再起動の回数が指定値を超えると、AVM は停止します。	maxTimeoutReloadTime maxTimeoutReloadTries

1. 設定されたターゲット（AVM またはユニット）で、システムがハイ アベイラビリティ動作を一切実行しない時間が猶予期間によって定義されます。これには例外が 1 つあります。その例外とは、設定されたターゲットが初めて PING に応答したときに、猶予期間が終了するという点です。