CHAPTER 5

AVM および VNE の管理

次の各トピックでは、AVM と VNE を定義および管理する方法について説明します。

AVM の管理

ここでは、ネットワークのモデルを作成するために、Cisco ANA が AVM をどのように使用するかについて説明します。また、次のトピックでは、AVM を管理する方法についても説明します。

AVM の概要

AVM とは、専用のメモリを内蔵する Java プロセス（独立 JVM）です。「Cisco ANA のアーキテクチャとコンポーネント」（P.1-3）で説明するように、AVM は、主に複数の VNE を実行および監視するために必要な分散サポート プラットフォームを実現する場合に使用されます。次の AVM は常にゲートウェイ上に作成されますが、その一部はユニット上にも作成されます （Cisco ANA AVM の全リストは、『*Cisco Active Network Abstraction 3.6.7 Installation Guide*』に記載されています）。

予約済み AVM

次の Cisco ANA AVM は予約されているため、編集も削除もできません。GUI クライアントで表示されるのは、AVM 66 と AVM 100 だけです。

表 5-1　予約済み AVM

AVM 番号	目的	インストール先	チェック可能な内容と使用するもの。
AVM 0	ハイアベイラビリティ / スイッチ AVM：ユニットと、その他のユニットおよびゲートウェイ間の通信を可能にします。	ゲートウェイおよびユニット	**cmpctl ステータス**
AVM 11	ゲートウェイ AVM：ゲートウェイ サーバと、ユニットおよびそのユニットで実行されているその他のプロセスを管理します。	ゲートウェイ	**cmpctl ステータス**
AVM 44	Mediator デバッガ AVM：アプリケーションによって Sheer DNA ゲートウェイに送信されたコマンド、結果（生データ）、通知、および結果の現在の状態を監視します （プログラマが使用）。	ゲートウェイ	**cmpctl ステータス**
AVM 66	ワークフロー エンジン AVM：ビジネス プロセスおよびネットワーク プロセスをアクティブにするための規則と依存関係を定義します。	ゲートウェイ	GUI クライアントと **cmpctl ステータス**
AVM 80	Cisco Video Assurance Management Solution（インストールされている場合）が使用するために予約されています。	ゲートウェイ	**cmpctl ステータス**
AVM 99	管理 AVM：ユニットおよび、ユニット上で動作しているその他の AVM（または、別個のユニットがない場合はゲートウェイ）を管理します。	ゲートウェイおよびユニット	**cmpctl ステータス**
AVM 100	トラップ管理 AVM：syslog およびトラップを処理します。 **（注）** AVM 100 が 1 つだけ動作している必要があります。また、すべてのトラップおよび syslog は、ゲートウェイまたは作動中の AVM を含んでいるユニット（およびスタンバイ ユニット。このユニットがハイアベイラビリティ用に設定されている場合）に転送する必要があります。	ゲートウェイ（通常）	GUI クライアントと **cmpctl ステータス**

AVM をユニットに追加するか、直接ゲートウェイに追加できます。これらの各 AVM は、専用のログを *ANAHOME*/sheer4/Main/logs に格納しています。

Cisco ANA ウォッチドッグ プロトコルは、AVM プロセスを監視して、停止した AVM が再起動したことを確認します。ウォッチドッグ プロトコルの詳細については、「ウォッチドッグ プロトコルの管理」（P.E-12）を参照してください。

AVM の基本システム ヘルスを確認するには、「システム ヘルスと診断」（P.10-1）を参照してください。

AVM ステータスの概要

AVM *ステータス*は、ユニットまたはゲートウェイ上の AVM プロセスの状態を示します。AVM ステータスは、次に説明する AVM の管理モードと動作モードの組み合せによって決まります。

- AVM *管理モード*は、AVM に送られた管理指示を Cisco ANA が認識するか、無視するかどうかを示します。このモードは完全にユーザによって指示されます。[ANA Servers] ブランチからこのモードをコントロールできます（「AVM ステータス（Start または Stop）の変更」（P.5-6）を参照）。
- AVM *動作モード*は、ゲートウェイ上の AVM プロセスの健常性および状態（たとえば、ゲートウェイが AVM に到達可能かどうか）を示します。

（注）　AVM 管理モードと動作モードは、Cisco ANA Manage に表示されません。これらのモードは全体のステータスで暗黙的に示されます。全体の AVM ステータスだけが GUI に表示されます。

表 5-2 に、AVM の管理モードと動作モードの組み合せによって、全体の AVM ステータスがどのように決まるかについて説明します。

表 5-2　AVM ステータス

全体の AVM ステータス	管理モード	動作モード	AVM ステータスの説明
Starting Up	Up	Down	**Start** または **Upload**（コマンド）オプションが発行されており、サーバがビジー状態または過負荷状態などの理由でこのオプションを実行できない場合、AVM のステータスは Starting Up になります。
Up	Up	Up	AVM プロセスが到達可能であり、ロード済みで、開始されています。これは、AVM が作成されており（かつ Activate Upon Creation が選択されている）、問題が発生していないときのステータスです。
Shutting Down	Down	Up	**Stop**（コマンド）オプションが発行され、このコマンドの実行中に一部のプロセスがまだ実行されている場合、AVM のステータスは Shutting Down です。
Down	Down	Down	AVM プロセスは到達可能ですが、停止しました。これは、Disable コマンドが発行されているときのステータスです。
Unreachable	Up	Unreachable	AVM プロセスが適切にロードされなかったため、AVM プロセスが動作していません。

AVM を移動するときに、そのステータスはプロセスが自動的にリロードされるかどうかに影響します。AVM のステータスが Up の場合、プロセスはリロードされ、AVM のステータスが Down の場合は、プロセスはリロードされません。AVM の移動の詳細については、「AVM の移動」（P.5-7）を参照してください。

AVM の作成

Cisco ANA では、Cisco ANA ユニットの AVM を定義できます。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 により、管理者はユニットの AVM を定義でき、AVM のウォッチドッグ 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できます。

始める前に

- 導入に関する情報および、AVM のメモリ要件などの推奨事項が必要な場合は、シスコの代理店にお問い合せください。
- AVM の設置に使用するユニットを決定してください。ユニットを設置し、転送ネットワークに接続する必要があります。
- AVM 0、AVM 99、AVM 100 が動作していることを確認してください。AVM のステータスの詳細については、「AVM ステータスの概要」（P.5-3）を参照してください。

（注）　AVM 番号 0 ～ 100 は予約されているため、使用できません。それ以外に、予約されている AVM 番号があります。

AVM を作成する手順は、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。

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　次の情報を入力します。[ANA Unit] フィールドに、親ユニットの IP アドレスが入力されます。AVM を作成する場合、ユニットがアップになっている必要はありません。

フィールド	説明
[ID]	Cisco ANA で定義した AVM の名前。これは、ユニットに一意の名前（たとえば、AVM 18）です。AVM 0 ～ 100 は予約されているため、使用できません。
[Key]	システム（すべてのユニット）の AVM を一意に識別する文字列。これにより、システムで透過的なフェールオーバー シナリオが可能になります。キーを入力しない場合、デフォルト キー（*ID+time_stamp*）が使用されます。
[Allocated Memory]	AVM に割り当てられる最大メモリ容量（MB 単位）。デフォルトは 256 です。導入に関する情報および、AVM のメモリ要件などの推奨事項が必要な場合は、シスコの代理店にお問い合せください。
[Activate on Creation]	AVM をユニットのブートストラップにロードします。これにより、AVM の管理ステータスが Up に変更され、それ以後ユニットを再起動したときに AVM が確実にロードされるようになります。このオプションは、デフォルトでオフになっており、新規作成された AVM の管理ステータスは Down になっています。
[Enable AVM Protection]	デフォルトでは、このチェックボックスはオンになっており、ハイアベイラビリティがイネーブルのときは AVM のウォッチドッグ プロトコルがイネーブルになります（1 台がスタンバイ ユニットになります）。詳細については、「ウォッチドッグ プロトコルの管理」（P.E-12）を参照してください。 **（注）**　ハイアベイラビリティがイネーブルになっている場合は、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。AVM がアップのときにオプションを変更する場合、変更を有効にするために、AVM をディセーブルにしてから、再度イネーブルにする必要があります。

ステップ 5　新規 AVM の情報を入力します。

ステップ 6　[OK] をクリックします。選択したユニットに新しい AVM が追加されると、[Content] 領域に表示され、アクティブになります。

新しい AVM を作成すると、Cisco ANA が、指定されたユニットに新しい AVM のレジストリ情報を提供します。この時点で AVM は、VNE のホストとして機能できます。詳細については、「VNE の作成：前提条件」（P.5-12）を参照してください。

AVM プロパティの表示および編集

Cisco ANA Manage を使用すると、キーまたは割り当てられているメモリなど、AVM の特定のプロパティを表示したり、編集したりできます。

AVM プロパティを表示または編集するための手順は、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。

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 [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。

- [File] > [Properties] を選択する。
- ツールバーにある [Properties] をクリックする。

[AVM Properties] ダイアログボックスが表示され、ここにユニットの IP アドレスまたはキーなど、選択した AVM の詳細情報が表示されます。

ステップ 4　必要に応じて、AVM プロパティを次の手順で表示または編集します。

フィールド	説明
[Key]	システム（すべてのユニット）の AVM を一意に識別する文字列。これにより、システムで透過的なフェールオーバー シナリオが可能になります。デフォルト キー（*ID+time_stamp*）が使用されます。
[Status]	ユニットまたはゲートウェイの AVM の状態（Starting Up、Up、Shutting Down、または Down）（「AVM ステータスの概要」（P.5-3）を参照）。
[Location]	選択したゲートウェイまたはユニットの IP アドレス。
[Max.Memory]	AVM に割り当てられる最大メモリ容量。デフォルト値は 256MB です。導入に関する情報および、AVM のメモリ要件などの推奨事項が必要な場合は、シスコの代理店にお問い合せください。
[Enable AVM Protection]	これをオンにすると、AVM 上でウォッチドッグ プロトコルがイネーブルになります。詳細については、付録 E「ハイ アベイラビリティの使用」を参照してください。 **（注）**　ハイアベイラビリティがイネーブルになっている場合は、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。AVM がアップのときにこのオプションをオンまたはオフにする場合、変更を有効にするために、AVM を再起動する必要があります。

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 [Content] 領域に表示されます。

AVM ステータス（Start または Stop）の変更

Cisco ANA Manage により、AVM を起動または停止できます。

（注）　AVM を停止すると、AVM のすべての VNE が停止します。AVM のステータスになんらかの変化があっても、適用されるまでしばらく時間がかかることに注意してください。たとえば、**Stop** コマンドを実行すると、ステータスが Shutting Down から Down に変化するまでに数分かかることがあります。

AVM を起動または停止するための手順は、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。

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

ステップ 3　次のいずれかの方法で AVM を起動または停止します。

- AVM を右クリックし、[Actions] > [Start] または [Actions] > [Stop] を選択する。
- ツールバーにある [Start] または [Stop] をクリックする。

AVM が起動または停止し、該当するステータスが [Content] 領域に次のように表示されます。

- [Starting Up]：AVM は起動中。
- [Up]：AVM は起動済み。
- [Shutting Down]：AVM は停止中。
- [Down]：AVM が停止。

（注）　AVM ステータスが Down と表示されているときには、ステータスは Down のままになり、リロードは発生しません。

AVM の移動

ユニット間で AVM 全体を移動させることができます。また、1 つの操作で AVM のグループを同じユニットに移動させることができます。AVM 0 ～ 100 は予約されているため、移動できません。

AVM がアップの場合は、AVM は停止し、ターゲット ユニットに移動されます。移動が完了すると、AVM は、移動前のステータスを維持しながら、リロードされます。

（注）　AVM を別のユニットに移動させると、機器およびアラーム永続性情報は失われます。詳細については、「永続性の概要」（P.F-1）を参照してください。

AVM を移動する手順は、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。

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

ステップ 3　AVM を右クリックし、[Move AVM] を選択します。

[Move To] ダイアログボックスが表示され、選択した Cisco ANA サーバとそのユニット（AVM が現在存在するユニットを除く）を表すツリーとブランチが表示されます。ナビゲーション ツリーの最上位に、Cisco ANA サーバが表示されます。これらのブランチを展開したり折りたたんだりすることにより、情報を表示したり非表示にしたりできます。

ステップ 4　AVM の移動先のユニット（ブランチ）を参照して選択します。

ステップ 5　[OK] をクリックします。AVM が移動され、選択したユニットの下に表示されます。

（注）　システムは非同期であるため、変更がただちに GUI に表示されないことがあります。GUI クライアントがサーバから通知を受信して更新されるまで、数分かかる場合があります。

VNE の移動については、「VNE の別の AVM への移動」（P.5-37）を参照してください。

AVM の削除

削除しようとする AVM が動作している場合は、削除する前に、その AVM は停止します。この手順を実行すると、指定したユニットの AVM のレジストリ情報が削除されます。AVM で動作している VNE がある場合、エラー メッセージが表示され、その AVM を削除できません。

詳細については、「VNE の削除」（P.5-38）を参照してください。

（注）　AVM 0 ～ 100 は予約されているため、削除できません。

始める前に

AVM からすべての VNE を削除してください。削除しないと、AVM の削除は失敗します。「VNE の削除」（P.5-38）を参照してください。

AVM を削除する手順は、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。

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。複数の行を選択できます。

ステップ 3　右クリックしてメニューを表示し、[Delete] を選択します。警告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。確認用のメッセージが表示されます。

ステップ 5　[OK] をクリックします。選択した AVM が、選択したユニットから削除されます。

（注）　システムは非同期であるため、変更がただちに GUI に表示されないことがあります。GUI クライアントがサーバから通知を受信して更新されるまで、数分かかる場合があります。

AVM または VNE の検索

Cisco ANA Manage で単一検索を実行すると、具体的に定義した検索条件に一致するすべての Cisco ANA サーバから AVM および VNE を見つけることができます。

AVM または VNE を検索する手順は、次のとおりです。

ステップ 1　[Cisco ANA Manage] ウィンドウで、ゲートウェイのサブブランチ、ユニットのサブブランチ、または AVM のサブブランチを選択します。

ステップ 2　[Find] をクリックします。[Find] ダイアログボックスが表示されます。

ステップ 3　検索項目の条件を次のように入力します。

フィールド	説明
[Find]	必要な AVM または VNE を検索するために具体的な検索条件を入力します。たとえば、AVM を検索するには ID 番号を使用し、VNE を検索するには IP アドレスを使用します。
[Types]	ドロップダウン リストで、検索する項目のタイプを次から選択します。 • [Any]：検索条件に一致する AVM または VNE を検索します。 • [AVM]：検索条件に一致する AVM を検索します。 • [VNE]：検索条件に一致する VNE を検索します。
[Property]	検索条件を含むプロパティを選択するか、[Any] を選択してすべてのプロパティから検索条件を検索します。 表示されるプロパティは、[Types] フィールドで選択した項目によって次のように異なります。 • [Types] フィールドで [Any] を選択すると、[Property] フィールドはディセーブルになります。 • [Types] フィールドで [AVM] を選択すると、[Property] フィールドに次のプロパティが表示されます。 – [ID] – [Status] – [Key] – [Loaded Patches] • [Types] フィールドで VNE を選択すると、[Property] フィールドに次のプロパティが表示されます。 – [Key] – [IP Address] – [Status] – [Maintenance] – [Element Type] – [Polling Group]
[Direction]	検索方向（[Down] または [Up]）を選択します。検索方向は、Cisco ANA ナビゲーション ツリーで現在選択されている項目に関連します。

ステップ 4　[Find] をクリックします。検索条件に一致する AVM または VNE は、Cisco ANA Manage で強調表示されます。

（注）　検索条件に一致する次の AVM または VNE を表示するには、F3 キーを押します。

VNE の管理

ここでは、ネットワークのモデルを作成するために、Cisco ANA が VNE をどのように使用するかについて説明します。また、次のトピックでは、VNE を管理する方法についても説明します。

VNE の概要

各 Virtual Network Element（VNE; バーチャルネットワーク要素）は、1 つのネットワーク要素のインスタンスを管理するために割り当てられます。この VNE には、そのネットワーク要素のレプリカが収容されています。VNE は、各ネットワーク要素およびネットワーク全体のライブ モデルを維持します。VNE のロードとともに、Cisco ANA がネットワーク要素の調査を開始し、ネットワーク要素のライブ モデルが自動的に構成されます。これには、その物理的および論理的インベントリ、設定、ステータスが含まれます。また、Cisco ANA は、ユニットに新しい VNE のレジストリ情報を作成します。新たに作成された VNE は、デフォルトのコミュニティ ストリングとポーリング レートを使用します。VNE は、そのネットワーク要素タイプに対応する設定レコードからこれらのプロパティを継承します。

（注） 必要な前提条件を実行してから VNE を追加した場合にだけ、Cisco ANA は適切にネットワーク要素をモデル化します。詳細については、「VNE の作成：前提条件」（P.5-12）を参照してください。

VNE はその主 IP アドレスによって指定され、1 つの NE に対応します。通常、network element（NE; ネットワーク要素）には、管理に使用する IP アドレスが 1 つだけあります。このようなデバイスの場合、主 IP アドレスは、このデバイスに設定されている単一の IP アドレスです。

NE に複数の IP アドレスがある場合は、IP アドレスのいずれかを選択して、主 IP アドレスとして使用する必要があります。主 IP アドレスは、NE に対応する VNE の ID としての役割を果たし、NE の IP アドレスが要求されると必ず表示されます。

（注） 2 つの VNE が同じ NE を監視するということは、できません。各 VNE は、システムに一度しか追加できません。

VNE によって収集される情報は、VNE のタイプおよびスキームによって異なります。VNE は、ネットワーク要素に実装されているサウスバウンド管理インターフェイス（SNMP や Telnet など）をどれでも使用します。

（注）　デフォルトでは、ネットワーク要素をモデル化し、監視するために、VNE がネットワーク要素との Telnet セッションを開くと、VNE がアイドル状態（そのセッションの間にデバイスを照会しなかった）であっても、Telnet セッションは 5 分間開いたままになります。5 分後、VNE はセッションを閉じ、デバイスを照会する必要があるときにセッションを再度開きます。この設定を変更する場合は、シスコの代理店にお問い合せください。

基礎となるネットワーク要素の監視が開始される前に、VNE をユニットのブートストラップにロードする必要があります。これにより、VNE の管理ステータスが Up に変更され、それ以後、ユニットが再起動したときに VNE が確実にロードされるようになります。VNE をロードすると、ユニットがただちに起動します。VNE のステータスの詳細については、「VNE ステータスの概要」（P.5-11）を参照してください。

VNE ステータスの概要

*VNE ステータス*により、AVM 上の VNE プロセスの状態が示され、Cisco ANA Manage GUI によって報告されます（例については、図 2-4（P.2-13）を参照してください）。全体の VNE ステータスは、次の VNE の管理モードと動作モードの組み合せによって決まります。

- *VNE 管理モード*は、Cisco ANA が VNE を識別するか、無視するかどうかを示します。このモードは完全にユーザによって指示されます。[ANA Servers] ブランチからこのモードをコントロールできます（「AVM ステータス（Start または Stop）の変更」（P.5-6）を参照）。
- *VNE 動作モード*は、AVM 上の VNE プロセス、ユニット、またはゲートウェイのヘルスおよび状態（たとえば、ゲートウェイが VNE に到達可能かどうか）を示します。

表 5-3 に、VNE の管理モードと動作モードの組み合せによって、全体の VNE 状態がどのように決まるかについて説明します。

（注）　VNE 管理モードと動作モードは Cisco ANA Manage に表示されません。これらのモードは全体のステータスで暗黙的です。全体の VNE ステータスだけが GUI に表示されます。

表 5-3　VNE ステータス

全体の VNE ステータス	管理モード	動作モード	説明
Starting Up	Up	Down	Start または Upload（コマンド）オプションが発行されており、サーバがビジー状態または過負荷状態などの理由でこのオプションを実行できない場合、VNE のステータスは Starting Up になります。
Up	Up	Up	VNE プロセスが到達可能であり、ロード済みで、開始されています。これは、**Start** コマンドが発行されているとき（あるいは VNE を作成して、その初期のステータスとして **Start** を選択したとき）に、問題（サーバが過負荷になるなど）が発生しなかった場合のステータスです。
Shutting Down	Down	Up	**Stop**（コマンド）オプションが発行され、このコマンドの実行中に一部のプロセスがまだ実行されている場合、VNE のステータスは Shutting Down です。

表 5-3　VNE ステータス （続き）

全体の VNE ステータス	管理モード	動作モード	説明
Down	Down	Down	VNE プロセスは到達可能ですが、停止しました。これは、**Stop** コマンドが発行されているときのステータスです。
Unreachable	Up	Unreachable	VNE はゲートウェイから到達不能であるため、この VNE を管理できません。

VNE を手動で、または自動的にメンテナンス モードにすることもできます。VNE ステータスは Up のままですが、メンテナンス モードは True に変化します（UI に表示されます）。ソフトウェア アップグレードなどのメンテナンス アクティビティを実行する必要がある場合は、この操作を手動で行うことがあります。そのため、メンテナンス アクティビティの間、Cisco ANA はアラームを無視します。ネットワーク要素の CPU 使用率が一定の設定レベルに達すると、Cisco ANA は、ネットワーク要素をメンテナンス モードに自動的に変更します。この動作により、VNE がネットワーク要素の CPU リソースを過剰に消費するのを防ぎます。ネットワーク要素が以前の状態に戻る準備が完了すると、Cisco ANA は、VNE ネットワーク モデルとエレメントを同期化します。

これにより、アクティブ ネットワークの全体的な機能に影響を与えずに、メンテナンス操作を実行できます。メンテナンス モード（一時的な状態）の間、VNE は次のように動作します。

- VNE を明示的に（手動で）アクティブ状態に切り替えない限り、VNE 自体の状態を変更しません。
- デバイスをポーリングしません。
- 相関関係フロー問題に関するイベントを処理しますが、デバイスをポーリングしません。
- 新しいサービス アラームを開始しませんが、Link Down アラームの場合のように、隣接 VNE からイベントを受信します。
- フローがアクティブであっても、syslog およびトラップを処理しません。
- 既存のリンクのステータスを維持します。
- 検証要求では失敗しません。

メンテナンス モードの詳細については、「VNE ステータス（Start、Stop または Maintenance）の変更」（P.5-36）を参照してください。

VNE の作成：前提条件

新しい VNE を追加して定義する場合、VNE は NE に対応するので、システムに追加できるのは一度だけです。VNE のロードとともに、Cisco ANA がネットワーク要素の調査を開始し、ネットワーク要素のライブ モデルが自動的に構成されます。これには、その物理的および論理的インベントリ、設定、ステータスが含まれます。

新しい VNE を追加すると、Cisco ANA はデバイスに新しい VNE のレジストリ情報を作成します。新たに作成された VNE の管理ステータスは Down になっており、この VNE はデフォルトのコミュニティ ストリングおよびポーリング レートを使用します。VNE は、そのデバイス タイプに対応する設定レコードからこれらのプロパティを継承します。

基礎となるネットワーク要素の監視が開始される前に、VNE をユニットのブートストラップにロードする必要があります。これにより、VNE の管理ステータスが Up に変更され、それ以後、ユニットが再起動したときに VNE が確実にロードされるようになります。VNE をロードすると、VNE もただちに起動します。VNE のステータスの詳細については、「VNE ステータスの概要」（P.5-11）を参照してください。

表 5-4　AVM に VNE を追加するステップ

	このタスクを実行するには	参照先
ステップ 1	追加するネットワーク要素に関するすべての前提条件の情報（IP アドレス、クレデンシャル、およびプロトコルの詳細など）を収集します。	「VNE を追加する前に必要なデバイス情報」（P.5-13）
ステップ 2	Cisco ANA がネットワーク要素を適切に管理できるように、ネットワーク要素に必須の設定をすべて行います。 • Cisco IOS、Cisco IOS XE、CatOS デバイス： • Cisco IOS XR デバイス： • SSH を使用して追加するデバイス： • SNMP トラップ設定： • syslog 設定：	「VNE を追加する前に必要なデバイス設定」（P.5-14） • 「Cisco IOS、Cisco IOS XE、CatOS デバイス：必須設定」（P.5-14） • 「Cisco IOS XR デバイス：必須設定および推奨設定」（P.5-14） • 「SSH を使用して追加されるすべての Cisco デバイス：必須設定、推奨設定、ロールバック デバイス設定」（P.5-15） • 「SNMP トラップ：必須のデバイス設定」（P.5-16） • 「syslog：必須のデバイス設定」（P.5-17）
ステップ 3	VNE を追加するときに指定するスキームを決定します。VNE によって収集され、そのモデルに入力される情報は、スキームによって決まります。スキームは、管理するデバイス タイプおよびデバイス テクノロジーによって異なります。	「VNE スキームの選択」（P.5-17）
ステップ 4	（任意）展開情報および、VNE を AVM に割り当てるためのベスト プラクティスなどの推奨事項を取得します。	シスコの代理店にお問い合せください。

VNE を追加する前に必要なデバイス情報

表 5-5 に、VNE を Cisco ANA に 追加するために必要なデバイス情報を示します。

表 5-5　新しい VNE に必要な情報

必要な情報	次を確認します。
IP アドレス	デバイスの IP アドレス。
名前	デバイス名。
プロトコルとクレデンシャル	
SNMP	• SNMP がデバイスで実行されている。 • サポートされるバージョン（V1、V2、V3）。 • SNMPV1 または V2 の場合：SNMP がコミュニティ ストリングの読み取りおよび書き込みを行う。 • SNMPV3 の場合：ユーザ名と、オプションで認証またはプライバシ設定。

表 5-5　新しい VNE に必要な情報 （続き）

必要な情報	次を確認します。
Telnet	• Telnet がデバイスでサポートされている。 • ポート番号。 • Telnet ログイン シーケンス：ユーザ名、パスワード、およびプロンプト。 （注）　Cisco IOS、Cisco IOS XE、および Cisco IOS XR デバイスでは、Telnet ログイン シーケンスが必要です。
SSH	• SSH がデバイスでサポートされている。 • サポートされるバージョン（V1 または V2）。 • SSH ユーザ名とパスワードおよびその他の任意の設定情報（暗号文、認証、鍵交換（V2）、MAC（V2））。 （注）　最初に任意の SSH クライアント アプリケーション（UNIX SSH や OpenSSH など）を使用して、デバイスの SSH ログイン シーケンスを判別することをお勧めします。また、「SSH を使用して追加されるすべての Cisco デバイス：必須設定、推奨設定、ロールバック デバイス設定」（P.5-15）で説明する必要なデバイス設定を必ず実行してください。

VNE を追加する前に必要なデバイス設定

Cisco ANA がデバイスを正確にモデル化できるように、デバイスに必要な設定を実行し、syslog、トラップ、ロギングの処理などの管理タスクを実行します。詳細については、次のトピックを参照してください。

- 「Cisco IOS、Cisco IOS XE、CatOS デバイス：必須設定」（P.5-14）
- 「Cisco IOS XR デバイス：必須設定および推奨設定」（P.5-14）
- 「SSH を使用して追加されるすべての Cisco デバイス：必須設定、推奨設定、ロールバック デバイス設定」（P.5-15）
- 「SNMP トラップ：必須のデバイス設定」（P.5-16）
- 「syslog：必須のデバイス設定」（P.5-17）

Cisco IOS、Cisco IOS XE、CatOS デバイス：必須設定

Cisco IOS、Cisco IOS XE、および CatOS ネットワーク要素では、次の設定が*必須*です。

```
snmp-server community public RO
snmp-server community private RW
```

Cisco IOS XR デバイス：必須設定および推奨設定

Cisco IOS XR ネットワーク要素では、次の設定が*必須*です。

（注）　該当する場合は、必ず **snmp-server** *host* の前に **snmp-server** *community* をコミットしてください。

```
domain ipv4 host gateway_name gateway_IP
telnet ipv4 server max-servers no-limit
snmp-server community community_name SystemOwner
snmp-server community community_name RO
```

```
snmp-server community public RO
snmp-server community private RW
vty-pool default 0 99
xml agent tty
```

必須の設定以外に、次のガイドラインに従う必要があります。

- Cisco IOS XR バージョン以外に Cisco IOS XR Manageability Package をインストールしてください。この実装に関する情報は、Cisco IOS XR バージョンのリリース ノートから入手できます。
- Cisco ANA は、デバイスのログイン ユーザ、つまり、グループ **root-system** および **cisco-support** のメンバーを使用する必要があります。
- 論理ルータを適切にモデル化するには、Cisco ANA ユーザは一意のログイン *user*@**admin**（グループ **root-system** および **cisco-support** のメンバーでもある）を使用する必要があります。
- Cisco IOS XR VNE は、SystemOwner コミュニティに追加してください。

Cisco IOS XR ネットワーク要素には、次の設定が*推奨*されます。

```
hostname gateway_name
snmp-server location location
snmp-server contact contact
line default exec-timeout 0 0
```

SSH を使用して追加されるすべての Cisco デバイス：必須設定、推奨設定、ロールバック デバイス設定

この SSH 情報は、すべてのデバイス タイプおよびオペレーティング システムに適用されます（SSH を実行するためのデバイス設定方法については、ご使用のデバイスのマニュアルを参照してください）。次の例は、SSH を使用して、Cisco デバイスを Cisco ANA に追加する必要がある場合、Cisco デバイスで SSH をイネーブルにする方法を示しています。

```
(config) ip domain-name DOMAIN
(config) crypto key generate rsa
```

（注） モジュラス長を入力するよう求められたら、デフォルト値のままにしてください。モジュラス長が長いほど安全ですが、生成および使用の際にかかる時間が長くなります。

ローカル パスワード チェックを受け入れるように、vty を次のように設定します。

```
line vty 0 4
login local
```

次の設定は、*推奨*の SSH 設定です。

```
(config)ip ssh time-out 120
(config)ip ssh authentication-retries 2
(config)ip ssh version 1(2)
```

元のデバイス設定にロールバックするには、次の設定を使用します。

```
no ip ssh {timeout | authentication-retries}
crypto key zeroize rsa
```

SNMP トラップ：必須のデバイス設定

次の表に、SNMP トラップを適切に受信するために、設定する必要がある設定を示します。

（注）　すべてのトラップをイネーブルにする場合は、**snmp-server enable traps** を使用してください。

SNMP タイプ	必須の設定
すべて	`snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart` `snmp-server enable traps chassis` `snmp-server enable traps module` `snmp-server enable traps bgp` `snmp-server enable traps ospf state-change` `snmp-server enable traps ospf errors` `snmp-server enable traps ospf retransmit` `snmp-server enable traps ospf lsa` `snmp-server enable traps ospf cisco-specific state-change` `snmp-server enable traps ospf cisco-specific errors` `snmp-server enable traps ospf cisco-specific retransmit` `snmp-server enable traps ospf cisco-specific lsa` `snmp-server enable traps config` `snmp-server enable traps ipmulticast` `snmp-server enable traps syslog` `snmp-server enable traps entity` `snmp-server enable traps flash insertion removal` `snmp-server enable traps envmon fan shutdown supply temperature status` `snmp-server enable traps rtr` `snmp-server enable traps mpls ldp` `snmp-server trap-source` *`interface_name`*[1] **（注）**　*`interface_name`* は、アクティブな管理 IP アドレスです。
SNMPv1	`snmp-server host` *`gateway_IP`* `traps version 1 community`
SNMPv2	`snmp-server host` *`gateway_IP`* `traps version 2c community`
SNMPv3（認証あり）	**（注）**　*MyUsr*、*MyGrp*、*MyPswd*、および *MyView* は、VNE を Cisco ANA に作成するときに入力する情報と一致する必要があります。 すべてのデバイスの場合： `snmp-server view` *`MyView`* `internet included` `snmp-server group` *`MyGrp`* `v3 auth [notify` *`MyView`*`]` Cisco IOS、Cisco IOS XE、CatOS デバイスの場合： `snmp-server user` *`MyUsr MyGrp`* `v3 auth {md5|sha}` *`MyPswd`* Cisco IOS XR デバイスの場合： `snmp-server user` *`MyUsr MyGrp`* `v3 auth {md5|sha} {WORD,CLEAR,encrypted}` *`MyPswd`* `SystemOwner` すべてのデバイスで、デバイスに SNMPv3 を設定したら、次の設定を行います。 `snmp-server host` *`gateway_IP`* `traps version 3 auth` *`MyUser`*

SNMP タイプ	必須の設定
SNMPv3（認証なし）	**（注）** *MyNoAuthUsr* と *MyNoAuthGrp* は、Cisco ANA に VNE を作成するときに入力する情報と一致する必要があります。 Cisco IOS、Cisco IOS XE、CatOS デバイスの場合： `snmp-server group MyNoAuthGrp v3 noauth` `snmp-server user MyNoAuthUsr MyNoAuthGrp v3` Cisco IOS XR デバイスの場合： `snmp-server user MyNoAuthUsr MyNoAuthGrp v3 SystemOwner` すべてのデバイスで、デバイスに SNMPv3 を設定したら、次の設定を行います。 `snmp-server host gateway_IP traps version 3 noauth MyNoAuthUr`

1. デバイスが管理 IP アドレスを保持している場合は必須。

syslog：必須のデバイス設定

次の表に、syslog に対して設定する必要がある設定内容を示します。

必須の設定	
すべて	`logging source-interface interface_name`[1]
Cisco CatOS、Cisco IOS、および Cisco IOS XE	`logging on` `logging buffered 64000 informational` `logging trap informational` `logging gateway_IP` `logging event link-status default`
Cisco IOS XR	`logging on` `logging events level informational` `logging buffered 10000` `logging trap informational` `logging events link-status software-interfaces`

1. デバイスが管理 IP アドレスを保持している場合は必須。*interface_name* は、アクティブな管理 IP アドレスです。

VNE スキームの選択

VNE スキームは、VNE によって収集され、VNE のモデルに入力されるネットワーク要素情報を決定します。つまり、VNE スキームは、検出プロセスの間に調査された VNE モデリング コンポーネントを定義します。VNE を作成する際には、Cisco ANA で管理するデバイス ファミリおよびテクノロジーに基づいてスキームを選択してください。こうすることで、異なるデバイスに異なる動作を定義できます。たとえば、一部のデバイスは SNMP だけでポーリングし、その他デバイスは Telnet でポーリングするなどです。特定のスキームには、ソフト プロパティとアクティベーション スクリプトも接続されています。

（注） VNE を作成する際には、Cisco ANA は使用可能なスキームのドロップダウン リストを表示します。リストには「デフォルト」選択項目が含まれています。デフォルトを選択すると、Cisco ANA はスキームを Product に設定します。

Cisco ANA は次のスキームを使用します。

- Product：このスキームは、このリリースのすべてのデバイス タイプ（Cisco CRS-1、Cisco XR 12000 シリーズ、Cisco 3750ME、Juniper M-Series の各デバイスを除く）に使用されます。
- ipcore：このスキームは、Provider（P; プロバイダー）または Provider Edge（PE; プロバイダー エッジ）デバイスとして機能するルータにだけ使用されます。

2 つのスキームの違いは、ipcore では、P デバイスと PE デバイスを含む MPLS VPN ネットワークの一部としてデバイスが使用されることを想定している点です。したがって、Cisco ANA はこれらの VNE を若干異なる方法でモデル化します。customer edge（CE; カスタマー エッジ）デバイスを含め、その他すべてのインスタンスには Product を使用してください。Product スキームは、MPLS または VRF 設定が存在しないことを前提しているため、これらの設定を取得しません。

これらのスキームでは、ユーザは、VNE がルータのモデル化に使用する登録方式（ライブ デバイスの情報を照会するために、VNE が使用する方式）を柔軟に指定できます。VNE を ipcore スキームで機能するように設定することによって VNE をコア ルータとして指定したり、VNE を Product スキームで機能するように設定することによって VNE をエッジ ルータとして指定したりできます。

表 5-6 に、使用されるスキームをデバイス タイプ別に示します。

表 5-6　デバイス タイプ別に使用されるスキーム

デバイス タイプ	Product スキーム	ipcore スキーム
サポートされる Alcatel-Lucent デバイス		
Alcatel-Lucent 7450 イーサネット サービス スイッチ	X	—
Alcatel-Lucent Intelligent Services Access Manager	X	—
Alcatel-Lucent Riverstone	X	—
Alcatel-Lucent CBX、GX、B-STDX の各スイッチ	X	—
サポートされる Cisco セキュリティ アプライアンス		
Cisco 適応型セキュリティ アプライアンス 5550 シリーズ	X	—
サポートされる Cisco ゲートウェイ		
Cisco AS5300 シリーズ Universal Gateways	X	—
サポートされる Cisco ルータ		
Cisco 800 シリーズ ルータ	X	—
Cisco 1000 シリーズ ルータ	X	—
Cisco 1600 シリーズ ルータ	X	—
Cisco 1700 シリーズ モジュラ アクセス ルータ	X	—
Cisco 1800 シリーズ サービス統合型ルータ	X	—
Cisco 2500 シリーズ ルータ	X	—
Cisco 2600 シリーズ マルチサービス プラットフォーム ルータ	X	—
Cisco 2800 シリーズ サービス統合型ルータ	X	—
Cisco 3600 シリーズ マルチサービス プラットフォーム ルータ	X	X
Cisco 3700 シリーズ マルチサービス アクセス ルータ	X	X
Cisco 3800 シリーズ サービス統合型ルータ	X	X

表 5-6　デバイス タイプ別に使用されるスキーム （続き）

デバイス タイプ	Product スキーム	ipcore スキーム
Cisco 7200 シリーズ ルータ	—	X
Cisco 7400 シリーズ ルータ	—	X
Cisco 7600 シリーズ ルータ	X	X
Cisco 10000 シリーズ ルータ	X	X
Cisco 12000 シリーズ ルータ	X	X
Cisco XR 12000 シリーズ ルータ	—	X
Cisco CRS-1 キャリア ルーティング システム	—	X
Cisco ASR 1000 シリーズ ルータ	—	X
Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ	—	X
Cisco MWR 2900 シリーズ モバイル ワイヤレス ルータ	X	X
サポートされる Cisco スイッチ		
Cisco Catalyst 2900 シリーズ スイッチ	X	—
Cisco ME 3400 シリーズ イーサネット アクセス スイッチ	X	—
Cisco Catalyst 3500 XL シリーズ スイッチ	X	—
Cisco Catalyst 3550 シリーズ スイッチ	X	—
Cisco Catalyst 3560 シリーズ スイッチ	X	—
Cisco Catalyst 3750 シリーズ スイッチ	X	—
Cisco Catalyst 3750 Metro シリーズ スイッチ	—	X
Cisco Catalyst 4000 シリーズ スイッチ	X	—
Cisco Catalyst 4500 シリーズ スイッチ	X	—
Cisco Catalyst 4900 シリーズ スイッチ	X	—
Cisco ME 4900 シリーズ イーサネット スイッチ	X	—
Cisco Catalyst 6500 シリーズ（CatOS）スイッチ	X	—
Cisco Catalyst 6500 シリーズ（IOS）スイッチ	X	—
Cisco ME 6500 シリーズ イーサネット スイッチ（6524）	—	X
サポートされる Juniper デバイス		
Juniper M シリーズ マルチサービス エッジルータ	X	X
Juniper T シリーズ コア プラットフォーム	X	X
サポートされる Redback デバイス		
SmartEdge 800 マルチサービス エッジルータ	X	—
Redback SMS ファミリ	X	—
サポートされる汎用デバイス		
汎用デバイス	X	—

VNE の追加

表 5-5 の情報を確認したら、新しい VNE の追加先となるユニットおよび AVM を決定します。

（注）　展開情報および、VNE を AVM に割り当てる際のベスト プラクティスなどの推奨事項については、シスコの代理店にお問い合せください。

VNE を一括して追加する場合は、「複数の VNE の追加（ユーティリティ スクリプト）」（P.C-3）を参照してください。

[New VNE] ダイアログボックスで、該当する VNE の SNMP、Telnet、SSH、ICMP、およびポーリング情報を定義および管理できます。各 VNE タブで VNE プロパティを定義する際の情報については、次を参照してください。

- 「VNE 全般設定」（P.5-22）
- 「VNE SNMP の設定」（P.5-24）
- 「VNE Telnet/SSH 設定」（P.5-25）
- 「VNE ICMP 設定」（P.5-34）
- 「VNE ポーリング設定」（P.5-34）

到達可能性テストを実行する VNE は、ICMP によってだけ作成できます。これは、VNE を作成し、タイプ ICMP を選択してから、[ICMP] タブで詳細を定義することによって行うことができます。「VNE ICMP 設定」（P.5-34）を参照してください。

（注）　デフォルトでは、ネットワーク要素をモデル化し、監視するために、VNE がネットワーク要素との Telnet セッションを開くと、VNE がアイドル状態（そのセッションの間にデバイスを照会しなかった）であっても、Telnet セッションは 5 分間開いたままになります。5 分後、VNE はセッションを閉じ、デバイスを照会する必要があるときにセッションを再度開きます。この設定を変更する場合は、シスコの代理店にお問い合せください。

始める前に

「VNE の作成：前提条件」（P.5-12）に示す必須情報が収集されていることを確認してください。

ステップ 1　Cisco ANA Manage で、[ANA Servers] ブランチを選択します。

ステップ 2　ナビゲーション ツリーで、必要なゲートウェイまたはユニットおよび AVM を選択します。

ステップ 3　AVM サブブランチを右クリックして、[New VNE] を選択します。[New VNE] ダイアログボックスが表示され、[General] タブに対して開きます。

ステップ 4　VNE の一般情報を入力します。このフィールドについては、表 5-8（P.5-22）で説明します。少なくとも、VNE 名と IP アドレスを入力する必要があります。

ステップ 5　Telnet コマンド シーケンスを定義するため、および SSH をネットワーク要素アクセス（到達可能性）とモデル化に対してイネーブルにするために、[Telnet/SSH] タブをクリックし、VNE Telnet/SSH 情報を入力します。このフィールドについては、表 5-9（P.5-24）で説明します。ダイアログボックスに表示されるフィールドは、選択したプロトコルによって異なります。

VNE を追加するときに誤ったクレデンシャル情報を入力すると、VNE は正常に追加および管理されません。このような場合、クレデンシャルを訂正し、VNE を再起動する必要があります（「VNE ステータス（Start、Stop または Maintenance）の変更」（P.5-36）を参照）。ただし、Telnet クレデンシャルは、VNE を再起動せずに、実行時に変更できます。

（注）　デバイスに一意の SNMP エンジン ID がない場合、Cisco ANA は、対応する SNMP タイムアウト メッセージとともにデバイス到達不能イベントを AVM ログ ファイルに生成します。通常この ID はデバイスの一意の MAC アドレスから取得されて自動的に割り当てられますが、ユーザがこの ID を指定することもできます。カスタム SNMP エンジン ID を使用しないことを推奨します。このようなカスタム ID を使用する場合は、その ID が一意であることを確認してください。

ステップ 6　[ICMP] タブをクリックし、Cisco ANA が到達可能性を確認する際に使用する ICMP ポーリング レートを入力します。このフィールドについては、表 5-7 で説明します。VNE には、ポーリング レートを秒単位で定義できます。

表 5-7　[New VNE] の [ICMP] タブ

フィールド	説明
[Enable]	ICMP 通信プロトコルを使用してネットワーク要素が到達可能であることを確認するように Cisco ANA に指示するには、このチェックボックスをオンにします。ICMP ポーリングは、いつでもイネーブルにしたり、ディセーブルにしたりできます。
[Polling Rate]	ポーリング レートを秒単位で入力します。ICMP がイネーブルの場合、これは必須フィールドです。

ステップ 7　[Polling] タブをクリックし、以前作成したポーリング グループに VNE を関連付けるための VNE ポーリング情報を入力するか、VNE 情報のタイプに応じてさまざまなポーリング設定（ステータス、設定など）をカスタマイズします。このフィールドについては、表 5-12（P.5-34）で説明します。

デフォルトおよび低レート ポーリング グループの設定に関する情報については、表 6-3（P.6-11）を参照してください。

ステップ 8　[OK] をクリックして、VNE を作成します。

VNE はそのユニットのブートストラップにロードされ、Cisco ANA はネットワーク要素の調査を開始します。Cisco ANA は、ネットワーク要素のライブ モデルを構築し、このモデルには、ネットワーク要素の物理的インベントリと論理的インベントリ、設定、およびステータスが含まれます。また、Cisco ANA は、ユニットに新しい VNE のレジストリ情報を作成します。数分経過したら、VNE ステータスが Up であることを確認します。

VNE およびデバイスのソフトウェア アップデート

デバイスのソフトウェアをアップグレードした後で、VNE を手動で再起動する必要はありません。VNE が設定情報をポーリングしたときに、VNE はこの種の変更の検出し、自動的に再起動します。VNE がリロードすると、VNE レジストリ パスなどの必須のレジストリ情報が更新されます。

ポーリング サイクルの設定については、「VNE ポーリング設定」（P.5-34）を参照してください。

VNE プロパティの表示

Cisco ANA Manage では、ステータスや Telnet 設定などの、ユニットの VNE のプロパティを表示したり、編集したりできます。VNE のプロパティを表示する手順は、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。

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　[VNE Properties] テーブルで目的の VNE を右クリックして [VNE Properties] ダイアログボックスを開き、[Properties] を選択します。

ステップ 4　必要に応じて、プロパティを編集または確認します。グレーアウトされている情報は、編集できません。[VNE properties] タブのフィールドに関する詳細は、次のトピックで説明します。

- 「VNE 全般設定」（P.5-22）
- 「VNE SNMP の設定」（P.5-24）
- 「VNE Telnet/SSH 設定」（P.5-25）
- 「VNE ICMP 設定」（P.5-34）
- 「VNE ポーリング設定」（P.5-34）

VNE のプロパティを編集するには、「VNE プロパティの編集」（P.5-35）を参照してください。

VNE 全般設定

次の表では、[VNE General] タブに表示されるフィールドについて説明します。汎用 SNMP VNE の詳細については、「汎用 SNMP VNE に関する注意事項」（P.5-24）を参照してください。

表 5-8　[VNE General] タブのフィールド

フィールド	説明
[Identification] 領域	
[Name]	Cisco ANA の一意キーとして使用される VNE の名前。この名前は、VNE を操作するコマンドにも使用されます。
[IP Address]	ネットワーク要素の IP アドレス。

表 5-8　[VNE General] タブのフィールド （続き）

フィールド	説明
[Type]	Cisco ANA がエレメントをモデル化するために使用するプロトコル、およびエレメントをモデル化する程度を定義します （ネットワーク開発を使用している場合は、ネットワーク開発プロセスはタイプを自動的に認識します）。ドロップダウン リストで、次のいずれかの VNE デバイス タイプを選択します。 • [Auto Detect] : エレメント上で SNMP がイネーブルになっている場合は、このタイプを使用してください。Cisco ANA は、SNMP を使用して、利用可能なインベントリ情報をすべて収集します。 • [Generic SNMP] : SNMP がエレメント上でイネーブルになっており、Cisco ANA がエレメントをサポートしない場合、あるいは Cisco ANA はエレメントをサポートするものの、基本情報だけをモデル化する場合は、このタイプを使用します。Cisco ANA は、SNMP を使用して、通常すべてのネットワーク要素によって提供される最も基本的なインベントリ情報を収集します。「汎用 SNMP VNE に関する注意事項」（P.5-24）を参照してください。 • [Cloud] : 管理対象外のネットワーク セグメントには、このタイプを使用します。具体的なクラウド設定は、プロジェクトごとに指定されます。 • [ICMP] : ICMP がエレメント上でイネーブルになっており、Cisco ANA がエレメントをサポートしない場合、あるいは Cisco ANA はエレメントをサポートするものの、基本情報だけをモデル化する場合は、このタイプを使用します。Cisco ANA は ICMP を使用して、通常すべてのネットワーク要素によって提供される最も基本的なインベントリ情報を収集し、到達可能性テストだけを実行します。
[Scheme]	検出プロセスの間に調査され、VNE モデルに入力される VNE モデリングデル コンポーネントを定義します。これにより、管理者は複数のネットワーク要素にさまざまな動作を定義できます。たとえば、一部のネットワーク要素が Telnet だけでポーリングし、その他のネットワーク要素が SNMP でポーリングするなどです。特定のスキームには、ソフト プロパティとアクティベーション スクリプトも接続されています。デフォルトでは、VNE はデフォルト スキームから VNE スキームを継承します。ネットワーク内に複数のスキームが存在する場合、VNE は選択されたスキームをロードします。 • Default : スキームを [Product] に設定します。 • Product : このスキームは、このリリースのすべてのデバイス タイプ（Cisco CRS-1、Cisco XR 12000 シリーズ、Cisco 3750ME、Juniper M シリーズの各デバイスを除く）に使用されます。 • ipcore : このスキームは、プロバイダー（P）またはプロバイダー エッジ（PE）デバイスとして機能するルータにだけ使用されます。 詳細については、「VNE スキームの選択」（P.5-17）を参照してください。
[Initial State] 領域	
[State]	VNE の初期ディスポジションを設定します。通常、このフィールドは、[Stop] に設定します。特に VNE 設定を確認する場合、あるいは VNE が非常に複雑であり、ロード手順を完了するために余分な処理が必要となることがわかっている場合には、[Stop] に設定してください。 • [Stop] : VNE はロードされません。これがデフォルトの状態です。 • [Start] : VNE はロードされ、データ収集を開始します。 • [Maintenance] : VNE が起動し、メンテナンス モードに移行します。「VNE ステータスの概要」（P.5-11）を参照してください。
[Location] 領域	

表 5-8　[VNE General] タブのフィールド （続き）

フィールド	説明
[ANA Unit]	VNE の AVM のホストとして機能するユニットの IP アドレスを表示します。
[AVM]	この VNE に関連付けられた AVM ID を表示します。

汎用 SNMP VNE に関する注意事項

汎用 SNMP VNE は、どのベンダーにも関連しない VNE であり、（特定の制約条件を持つ）任意のベンダーを代表し、ネットワーク デバイスの Lightweight Management（軽量負荷管理方式）のサポートを提供します。汎用 SNMP VNE は、次のことを実行します。

- デバイスの基本的な管理機能に次のテクノロジーを提供します。
  - IP（基本 IP に限定され、IPsec、MPLS、またはルーティング プロトコルのモデリングを含まない）
  - イーサネット スイッチング
  - 802.q
- 次のインベントリ項目をサポートします。
  - 物理的インベントリ（特定のポート タイプだけ）
  - ルーティング テーブル
  - ARP テーブル
  - デフォルト ブリッジ
  - IP インターフェイス

VNE が未サポートと識別された場合（そのタイプが認識されなかったため）、Cisco ANA は、VNE に Unsupported のステータスを示します。VNE を Unsupported のままにするか、汎用 SNMP VNE としてロードできます。

agentdefaults/da のすべての VNE には、「load generic agent for unsupported device type」というエントリがあります。このエントリでは、値を True または False（デフォルト）として設定できます。値が True の場合、1.3.999.3 がプロパティとして設定されます。このエントリは、agentdefaults/da/deviceTypes 内でこのプロパティを探し、sheer/genericda を見つけます。このエントリは、デバイスのソフトウェア バージョンの検査をスキップし、デフォルト バージョンから VNE（汎用 SNMP）を構築します。

VNE SNMP の設定

次の表では、[VNE SNMP] タブに表示されるフィールドについて説明します。

表 5-9　[VNE SNMP] タブのフィールド

フィールド	説明
[SNMP Version] 領域	
[Enable SNMP]	このフィールドがオンの場合、SNMP 通信プロトコルを使用できるように、SNMP 通信プロトコルをイネーブルにします。VNE では、いつでも SNMP をイネーブルまたはディセーブルにできます。ただし、（[General] タブの）[Auto Detect] チェックボックスがオンになっているときには、ディセーブルにできません。
SNMP V1/V2 設定（SNMP V1 または SNMP V2 を使用してアクティブ化）	
SNMP V1 および V2 フィールドは、SNMP がイネーブルのときにだけ使用可能です。	

表 5-9　[VNE SNMP] タブのフィールド （続き）

フィールド	説明	
[Read]	SNMP リード（read）コミュニティ ステータス（ユーザが Public（デフォルト）または Private を定義）。	
[Write]	SNMP ライト（write）コミュニティ ステータス（ユーザが Public または Private（デフォルト）を定義）。	
SNMP V3 設定（SNMP V3 を使用する場合にアクティブ化）		
SNMP V3 フィールドは、SNMP V3 を選択したときにだけ使用できます。「SNMP トラップ：必須のデバイス設定」（P.5-16）に示す必須の SNMPv3 デバイス設定タスクを実行していることを確認してください。		
[Authentication]	使用される認証のタイプ： • No：認証は不要です（デフォルト）。 • md5：認証メカニズムにメッセージ ダイジェスト 5（MD5）を使用します。 • sha：認証メカニズムに Secure Hash Algorithm（SHA）を使用します。	
	[User]	認証ユーザ名。このフィールドは、No 認証以外の方式を選択した場合にイネーブルになります。
	[Password]	認証パスワード。このフィールドは、No 認証以外の方式を選択した場合にイネーブルになります。
[Encryption]	使用される暗号化方式のタイプ： • No：暗号化は不要です（デフォルト）。 • des：暗号化に Data Encryption Standard（DES; データ暗号規格）を使用します。 • aes128：認証に 128 ビット Advanced Encryption Standard（AES; 高度暗号化規格）を使用します。 • aes192：認証に 192 ビット AES を使用します。 • aes256：認証に 256 ビット AES を使用します。	
	[Password]	このフィールドは、No 暗号化以外の方式を選択した場合にイネーブルになります。暗号化パスワードを入力してください。

VNE Telnet/SSH 設定

次の表では、[VNE SSH/Telnet] タブ内のフィールドについて説明します。Telnet または SSH プロンプト情報の入力例については、「Telnet シーケンス：注意事項と例」（P.5-29）を参照してください。SSHv2 ホスト キー アルゴリズムの詳細については、「SSHV2 公開鍵および秘密鍵のファイル形式に関する注意事項」（P.5-33）も参照してください。

表 5-10　[SSH/Telnet] タブのフィールド

フィールド	説明
[Enable]	Cisco ANA がネットワーク要素を調査できるように、通信プロトコルをイネーブルにします。このチェックボックスをオンにすると、[Login Sequence] 領域がアクティブになります。この通信プロトコルは、いつでもイネーブルまたはディセーブルにできます。

表 5-10　[SSH/Telnet] タブのフィールド （続き）

フィールド	説明	
[Protocol]	使用されるプロトコルのタイプ： • Telnet（デフォルト） • SSHv1 • SSHv2 （注）　デフォルトでは、ネットワーク要素をモデル化し、監視するために、VNE がネットワーク要素との Telnet セッションを開くと、VNE がアイドル状態（そのセッションの間にデバイスを照会しなかった）であっても、Telnet セッションは 5 分間開いたままになります。5 分後、VNE はセッションを閉じ、デバイスを照会する必要があるときにセッションを再度開きます。この設定を変更する場合は、シスコの代理店にお問い合せください。	
[Port]	プロトコルが使用するポート。このフィールドの入力内容は、選択したプロトコルによって異なります。デフォルト ポートを使用しない場合は、該当するポート番号を入力してください。 • 23：Telnet のデフォルト ポート。 • 22：SSHv1 または SSHv2 のデフォルト ポート。	
[Login Sequence] 領域		
[Prompt] および [Run]	ネットワーク要素の予測されるプロンプトと、Cisco ANA がネットワーク要素に送信するストリング（予測されたプロンプトが検出されるとき）。テーブルには現在の設定が表示され、この設定はテーブルの下にあるコントロール ボタンを使って変更できます。[Prompt] フィールドにストリングを入力すると、[Run] フィールドがアクティブになります。パスワードをクリア テキストとして入力したくない場合は、[Prompt] フィールドおよび [Run] フィールドに入力した後で、[Mask] をクリックします。最後に [Add] をクリックして、ログイン シーケンスにプロンプトとストリングを追加します。任意の行を削除するには、[Remove] をクリックします。順序を変更するには、テーブルの右側にある上下ボタンを使用してください。 （注）　VNE とデバイスの間に SSH セッションが確立されると、VNE はログイン シーケンスを開始します。通常、このシーケンスは対応する Telnet ログイン シーケンスより短くなります。これは、ユーザ名またはパスワードが SSH セッションを確立するステップとして送られることがあるからです。	
	Telnet を選択した場合：	Telnet プロンプト情報。シーケンス（コマンドの順序）は、プロンプト フィールドだけを含む行で終了する必要があります。この情報の入力例については、「Telnet シーケンス：注意事項と例」（P.5-29）を参照してください。 [Prompt] フィールドには、デバイスから予測されるプロンプトが含まれており、[Run] フィールドには、予測されるプロンプトに対する応答が含まれている必要があります。Run 情報を入力する際には、[Confirm] フィールドへの入力内容を確認する必要があります。[Hide the Run value] をチェックしていないと、チェックボックスに入力するときに、[Run] および [Confirm] の値がクリア テキストとして表示されます。
	SSH V1 または V2 を選択した場合：	SSH プロンプト情報。通常このシーケンスは、対応する Telnet ログイン シーケンスよりも短くなります。これは、SSH セッション確立プロセス時に、ユーザ名またはパスワードがすでに送信されていることがあるからです。任意の SSH クライアント アプリケーション（UNIX SSH や OpenSSH など）を使用して、デバイスの SSH ログイン シーケンスを判別してから、情報を入力することをお勧めします。

表 5-10　[SSH/Telnet] タブのフィールド（続き）

フィールド	説明	
[Mask]	パスワードがクリア テキストとして表示されないように、パスワードをマスクします（[Prompt] および [Run] フィールドへの入力完了後）。パスワードを入力したら、再度入力するよう求められます。[OK] をクリックすると、情報が追加されます。	
[Add] と [Remove]	プロンプトの順序を操作し、ストリングを実行するために使用します。	
[SSHv1] 領域（SSHv1 を使用している場合にアクティブ化）		
[Username]	デバイス名。	
[Password]	デバイス パスワード。	
[Cipher]	使用する暗号化アルゴリズム。デフォルトでは、すべての方式が使用されます。 • DES：DES アルゴリズムを使用します。 • 3DES：Triple Data Encryption Standard（3DES; トリプル データ暗号規格）アルゴリズムを使用します。 • Blowfish：Blowfish アルゴリズムを使用します。	
[Authentication]	認証方式。パスワードは、現在サポートされている唯一の方式です。	
[SSHv2] 領域（SSHv2 を使用している場合にアクティブ化）		
[Username]	SSHv2 ユーザ名。	
[Client Authentication]	使用するクライアントドリブン認証方式。	
	[Password]	パスワードを使用してクライアントを認証します。[Password] フィールドにパスワードを入力します。
	[Public Key]	必要に応じて、鍵ペア システムを使用する公開鍵認証を使用します。この鍵ペア システムでは、クライアント アプリケーションが秘密鍵で設定され、デバイスが（このペアの）公開鍵で設定されます。 • Private Key：秘密鍵。[Import] をクリックして秘密鍵をインポートするか、[Generate] をクリックして秘密鍵を生成します。 • Public Key：公開鍵。公開鍵をインポートするには、[Import] をクリックします。アプリケーションは、公開鍵と秘密鍵がペアの一部であるかを確認します。

表 5-10　[SSH/Telnet] タブのフィールド （続き）

フィールド	説明	
[Server Authentication]	サーバ認証方式が使用されます。	
	none	サーバ認証なし （この方式では認証を一切実行せず、中間者攻撃「man-in-the-middle」に晒される危険性があるため、この方式は推奨しません）。
	save-first-auth	サーバへの最初の接続試行に使用された公開鍵を使用します。この方式は、最初の接続が正当な接続であったことを前提とします （接続が危険に晒された場合、セキュリティ上の危険性が存在します）。 最初の接続後に、サーバ認証方式は preconfigured に変更され、公開鍵データは事前設定されたデータとして挿入されます。
	pre-configured	最初の接続が試みられる前に、アプリケーション イベントに設定されたサーバの公開鍵またはフィンガープリントを使用します。これがデフォルトであり、推奨方式です。この方式を選択すると、[Finger Print] フィールドまたは [Public Key] フィールドがアクティブになります。 次のいずれかを選択してください（また、この表の最後に記載されている [Host Key Algorithm] フィールドの説明を必ずお読みください）。 • Finger Print：サーバ公開鍵の短いチェックサムを使用します（これは同じ目的を果たしますが、はるかに短くなります）。 • Public Key：許可されたいずれかの形式の公開鍵を使用します（「SSHV2 公開鍵および秘密鍵のファイル形式に関する注意事項」（P.5-33）を参照）。公開鍵を入力するか、[Generate] をクリックし、秘密鍵情報を使用して一致する公開鍵を生成します。
[Key Exchange][1]	使用する鍵交換アルゴリズム。デフォルトは none です。 • DH-group1-sha1：Diffie Hellman Group 1 と、鍵交換アルゴリズムに Secure Hash Algorithm（SHA）1 を使用します。 • DH-group1-exchange-sha1 : Diffie Hellman Group および Key Exchange と、鍵交換アルゴリズムに SHA 1 を使用します。	
[MAC][1]	鍵生成に使用される MAC アルゴリズム。デフォルトは none です。 • SHA1：メッセージ認証に HMAC-SHA-1 を使用します。 • MD5：メッセージ認証に Message Digest algorithm 5（HMAC MD5; メッセージ ダイジェスト アルゴリズム 5）を使用します。 • SHA1-96：メッセージ認証に 96 ビット HMAC-SHA1-96 を使用します。 • MD5-96：メッセージ認証に 96 ビット MDS（HMAC-MD5-96）を使用します。	
[Cipher][1]	使用される暗号文。 • 3DES：3DES ブロック アルゴリズム（3DES-CBC）を使用します。 • AES-128：128 ビット AES アルゴリズム（AES128-CBC）を使用します。 • AES-192：196 ビット AES アルゴリズム（AES192-CBC）を使用します。 • AES-256：256 ビット AES アルゴリズム（AES256-CBC）を使用します。	

表 5-10　[SSH/Telnet] タブのフィールド （続き）

フィールド	説明
[Host Key Algorithm][1,2]	ホスト鍵アルゴリズム（最大 2048 ビット鍵が公式にサポートされます）。有効なファイル形式については、「SSHV2 公開鍵および秘密鍵のファイル形式に関する注意事項」（P.5-33）を参照してください。 • DSA：Digital Signature Authority（DSA; デジタル署名認証局）公開鍵アルゴリズムを使用します。 • RSA：Rivest-Shamir-Adleman（RSA）公開鍵アルゴリズムを使用します。

1. 1 つの方式を選択しながら Ctrl キーを押すと、複数のアルゴリズムを選択できます。複数のアルゴリズムが選択されると、1 つのアルゴリズムがサーバによって受け入れられるまで、アプリケーションはすべてのアルゴリズムの使用を試みます。アルゴリズムの試行方法に優先順位はありません。また、暗号化アルゴリズムに複数の既知のバージョンが存在することがあります（たとえば、3DES には 3des-cbc、3des-ecb、3des-cfb、3des-ofb、3des-ctr がある）。
2. 公開 RSA 鍵と DSA 鍵および秘密 RSA 鍵と DSA 鍵には、いくつかのファイル形式があります。Cisco ANA は公式に OpenSSH 形式をサポートしています（http://www.openssh.com/manual.html を参照）。

Telnet シーケンス：注意事項と例

VNE を追加するとき、Cisco ANA は、指定された通信プロトコルを使用してネットワーク要素に接続し、モデリングおよびステータス情報を収集します。Cisco ANA が必要とする情報を提供する必要があります。その情報とは、完全なシーケンスおよびネットワーク要素の予測されるプロンプトの順序、および Cisco ANA が応答でネットワーク要素に送信するストリング（Cisco IOS および Cisco IOS XE デバイスのモード、および Cisco IOS XR デバイスの XML モードをイネーブルにできるようにする）です。

このトピックでは、次の Telnet シーケンスを入力するための 2 つの例を示します。

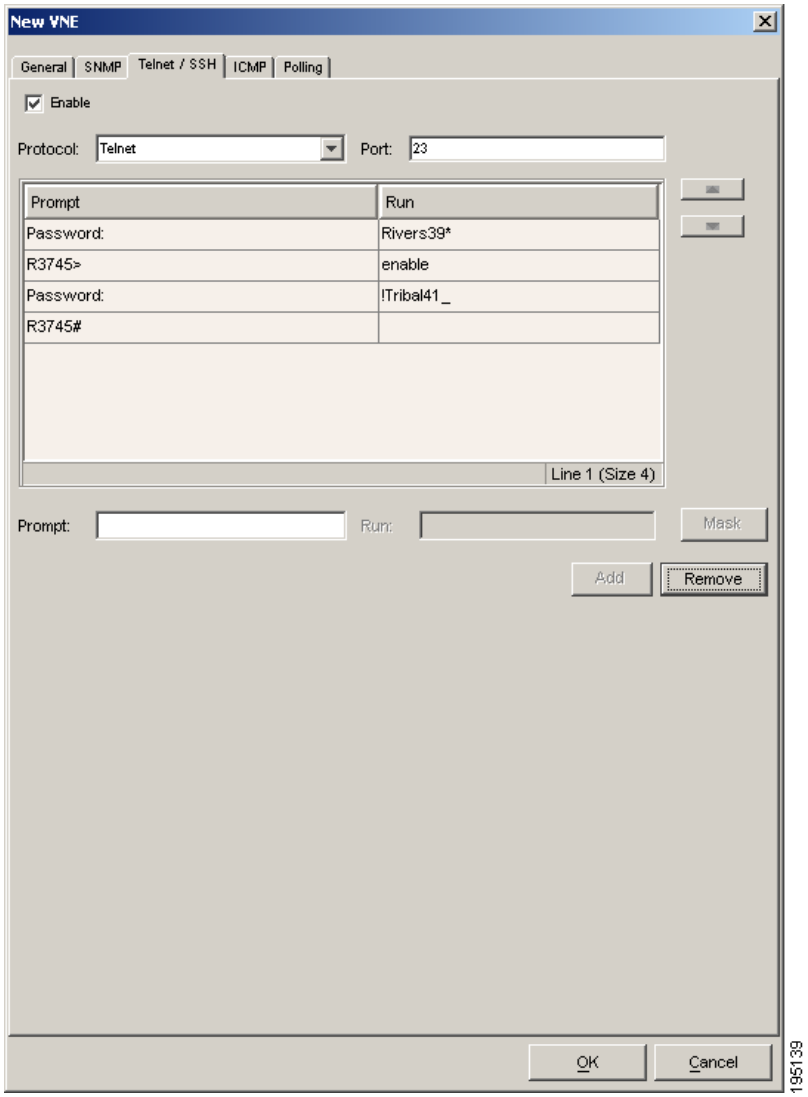
- 「Cisco IOS デバイスの Telnet シーケンス例」（P.5-30）
- 「Cisco IOS XR デバイスの Telnet シーケンス例」（P.5-31）

Telnet シーケンス（コマンドの順序）は、イネーブル プロンプト（Cisco IOS および Cisco IOS XE デバイスの場合）またはルータ CLI プロンプト（Cisco IOS XR デバイスの場合）だけを含む行で終了する必要があります。すべてのデバイス ファミリの Telnet シーケンスが同じとは限りません。このことは、特に Cisco IOS デバイスに当てはまります。RAD ACE-2300 デバイスの場合、SNMP がデバイスのモデリングに使用されるので、不要な照会を避けるために Telnet をディセーブルにすることを推奨します。

Cisco IOS デバイスの Telnet シーケンス例

図 5-1 に、Cisco IOS デバイスの Telnet シーケンスの例を示します（この例は、Cisco IOS XE デバイスにも適用されます）。図に続く手順では、デバイスに VNE を作成するときに、このシーケンスを入力する方法を説明します。

図 5-1　　例：Cisco IOS の Telnet シーケンス



次の手順では、図 5-1 に示すように、Cisco IOS デバイスのサンプル Telnet シーケンスを入力する方法について説明します。

ステップ 1　[Enable] チェックボックスをオンにして、Telnet の [Prompt] フィールドをアクティブにします。

ステップ 2　予測されるデバイスのプロンプトと応答を次のように入力します。

（注）　デバイスの Telnet シーケンスを確認するには、デバイスへの Telnet セッションを開き、情報をコピーしてください。次に、例を示します。

a. [Prompt] フィールドに「Password:」と入力します。

（注）　パスワードをクリア テキストで表示したくない場合は、[Mask] をクリックします。

b. [Run] フィールドと [Confirm] フィールドに「Rivers39*」と入力します。

c. [Add] をクリックします。

ステップ 3　デバイスをイネーブル モードにするために必要なデバイス プロンプトとコマンドを次の手順で入力します。

a. [Prompt] フィールドに「R3745>」と入力します。

b. [Run] フィールドと [Confirm] フィールドに「enable」と入力します。

c. [Add] をクリックします。

ステップ 4　イネーブル モード パスワード情報を次の手順で入力します。

a. [Prompt] フィールドに「Password:」と入力します。

（注）　パスワードをクリア テキストで表示したくない場合は、[Mask] をクリックします。

b. [Run] フィールドと [Confirm] フィールドに「!Tribal41_」と入力します。

c. [Add] をクリックします。

ステップ 5　イネーブル プロンプト情報を次の手順で入力します。

a. [Prompt] フィールドに「R3745#」と入力します。

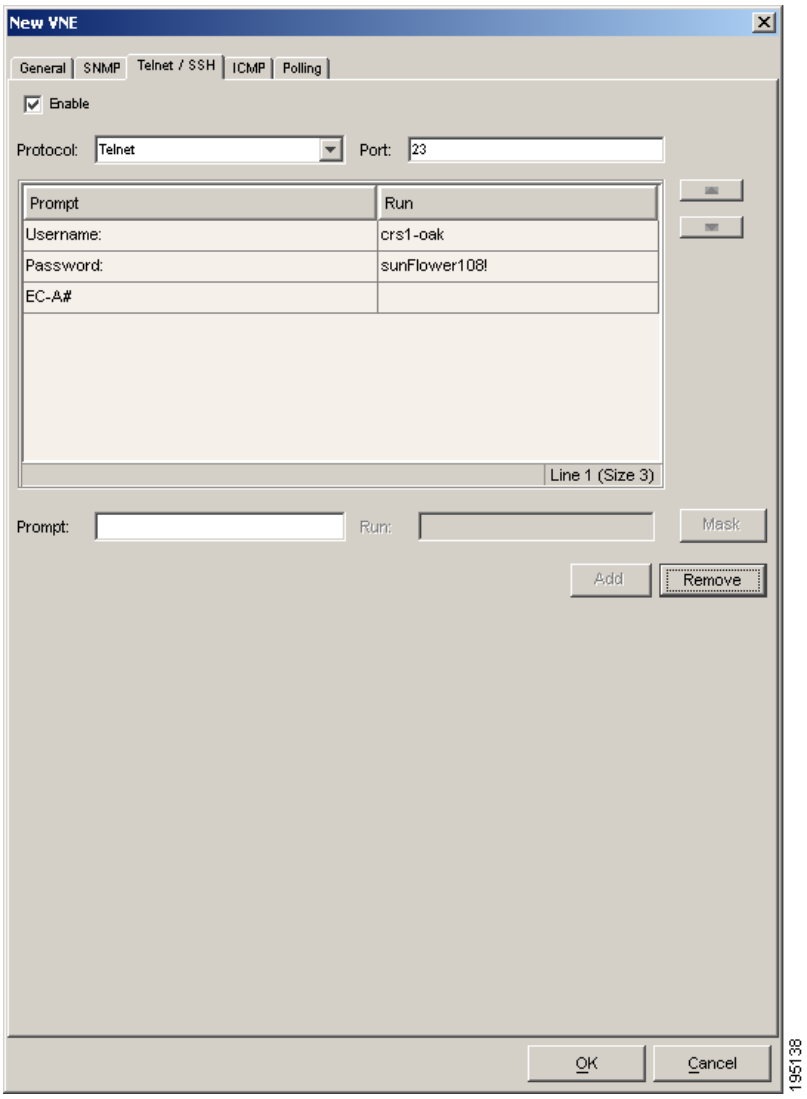
b. [Run] フィールドが空白であることを確認します。

c. [Add] をクリックします。

Cisco IOS XR デバイスの Telnet シーケンス例

図 5-2 に、Cisco IOS XR デバイスの Telnet シーケンスの例を示します。図に続く手順では、デバイスに VNE を作成するときに、このシーケンスを入力する方法を説明します。

図 5-2　例：Cisco IOS XR の Telnet シーケンス



次の手順では、図 5-2 に示すように、Cisco IOS XR デバイスのサンプル Telnet シーケンスを入力する方法について説明します。

ステップ 1　[Enable] チェックボックスをオンにして、Telnet の [Prompt] フィールドをアクティブにします。

ステップ 2　予測されるデバイスのプロンプトと応答を次のように入力します。

（注）　デバイスの Telnet シーケンスを確認するには、デバイスへの Telnet セッションを開き、情報をコピーしてください。次に、例を示します。

a.　[Prompt] フィールドに「Username:」と入力します。

b.　[Run] フィールドと [Confirm] フィールドに「crs1-oak」と入力します。

c.　[Add] をクリックします。

ステップ 3　デバイス パスワード情報を次の手順で入力します。

a. [Prompt] フィールドに「Password:」と入力します。

（注） パスワードをクリア テキストで表示したくない場合は、[Mask] をクリックします。

b. [Run] フィールドと [Confirm] フィールドに「sunFlower108!」と入力します。

c. [Add] をクリックします。

ステップ 4　デバイス プロンプトを次の手順で入力します。

a. [Prompt] フィールドに「EC-A#」と入力します。

（注） マルチプロセッサ搭載のデバイス（Cisco CRS-1 など）の場合、プロンプトはアクティブ CPU + デバイス名（たとえば、**RP/0/RSP0/CPU0:EC-A#**）で構成されます。CPU フェールオーバーによって、プロンプトが変更され、別の CPU がレポートされることがあります。この場合、デバイス名だけを指定するプロンプト（たとえば、**EC-A#**）を挿入する必要があります。

b. [Run] フィールドが空白であることを確認します。

c. [Add] をクリックします。

SSHV2 公開鍵および秘密鍵のファイル形式に関する注意事項

公開 RSA 鍵と DSA 鍵および秘密 RSA 鍵と DSA 鍵には、いくつかのファイル形式があります。同じ鍵を、使用形式に応じて異なる方法で書き込むことができます。

このアプリケーションは公式に OpenSSH 形式をサポートします。詳細については、http://www.openssh.com/manual.html を参照してください。

入力パラメータとして指定した鍵がこの形式であることを確認してください。鍵が OpenSSH 形式でない場合は、鍵を適用する前に、鍵を OpenSSH 形式に変換する必要があります。

使用例 : Cisco IOS で処理するとき、公開鍵は **show crypto key mypubkey** コマンドを使用して取得されます。この形式は OpenSSH 形式と互換性がなく、サポートされていません。ファイル形式を変換する方法は、いくつかあります。

最も簡単な解決策は、公開鍵スキャン（無償）を使用して、OpenSSH アプリケーションでサポートされる形式の公開鍵を取得することです。詳細については、http://www.openssh.com/manual.html を参照してください。

もう 1 つの選択肢として、ファイルを目的の形式に手動で変換するか、スクリプトを使って変換する方法があります。

次の例は、有効なファイル形式の例です。

```
RSA- private key
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDvdpW8ItfbSp/hTbWZJqCPmjRyh9S+EpTJ0Aq3fnGpFPTR+
……..
TiOfhiuX5+M1cTaE/if8sScj6jE9A0MpShBrnDU/0A==
-----END RSA PRIVATE KEY-----

DSA private key
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQDNGO+l2XW+W+YtVnWSYbKXr6qkrH9nOl+
……..
```

```
7wO4+FR9afoRjDusrQrL
-----END DSA PRIVATE KEY-----

DSA public key
ssh-dss AAAAB3……HfuNYu+ DdGY7njEYrN++iWs= aslehr@aslehr-wxp01

RSA - public key
ssh-rsa AAAAB3…lot more…qc8Hc= aslehr@aslehr-wxp01
```

VNE ICMP 設定

次の表では、[VNE ICMP] タブ内のフィールドについて説明します。

表 5-11　[VNE ICMP] タブのフィールド

フィールド	説明
[Enable]	ICMP 通信プロトコルを使用して、ネットワーク要素が到達可能であることを確認するよう Cisco ANA に指示します。このチェックボックスをオンまたはオフにすることで、いつでも ICMP ポーリングをイネーブルまたはディセーブルにできます。
[Polling Rate]	ポーリング レート（秒単位）。ICMP がイネーブルの場合、これは必須フィールドです。

VNE ポーリング設定

次の表では、[VNE Polling] タブ内のフィールドについて説明します。システム設定のポーリングに関する詳細については、「システムのポーリング設定に関する注意事項」（P.5-35）を参照してください。

（注） サポートされている設定やシステム サイジングなど、導入に関する詳細や推奨事項については、シスコの代理店にお問い合せください。

表 5-12　[VNE Polling] タブのフィールド

フィールド	説明
[Polling Group] 領域	
[Group]	ドロップダウン リストに表示されるいずれかのポーリング グループからポーリング レートを使用します。リスト内のグループを選択しない場合、Cisco ANA はデフォルトのポーリング グループを使用します。「ポーリング グループの管理と適応ポーリング」（P.6-10）を参照してください。
[Instance]	ダイアログボックスに表示される組み込みのポーリング間隔のいずれかのポーリング レートを変更して作成されたユーザ指定のポーリング レートを使用します。 [Instance] を選択すると、[Polling Intervals] 領域と [Topology] 領域がアクティブになります。 **（注）** 変更されていないポーリング レートは、[Group] ドロップダウン リストで指定されたグループから設定値を継承します。

表 5-12　[VNE Polling] タブのフィールド （続き）

フィールド	説明
[Polling Intervals] 領域（Instance を使用している場合にアクティブ化）	
（注）　ポーリング間隔には、デフォルト値を使用することを推奨します。これらのフィールドをデフォルト値未満に設定すると、Cisco ANA ユニットまたはポーリング対象のデバイスが過負荷状態になる可能性があります。	
[Status]	ネットワーク要素ステータス（アップまたはダウン）、ポート ステータス、管理ステータスなどのステータス関連の情報についてのポーリング レート。これは、通常最も頻繁にポーリングされる情報で、エレメントとコンポーネントの現在の動作状態と管理状態を反映します。デフォルト設定は 180 秒です。
[Configuration]	VC テーブル、スクランブルなどの設定関連情報のポーリング レート。これらの情報は、フォワーディング テーブル、ルーティング テーブル、およびスイッチング テーブルなどのエレメント設定をより動的に反映します。デフォルト設定は 900 秒です。
[System]	ネットワーク要素名、ネットワーク要素のロケーションなどのシステム関連情報のポーリング レート。これらの情報は、特性上、それほど動的でないエレメント設定を反映します。デフォルト設定は 86400 秒です （「システムのポーリング設定に関する注意事項」（P.5-35）も参照してください）。
[Topology] 領域（Instance を使用している場合にアクティブ化）	
[Layer 1]	レイヤ 1 カウンタに対するトポロジ プロセスのポーリング レート（間隔）。このプロセスは、継続的に実行されます。デフォルト設定は 30 秒です。
[Layer 2]	レイヤ 2 カウンタに対するトポロジ プロセスのポーリング レート（間隔）。このプロセスは、オンデマンドで使用できます。デフォルト設定は 30 秒です。

システムのポーリング設定に関する注意事項

sysoid コマンドと **software version** コマンドは、システム設定をポーリングするために使用します。次のパラメータを使用できます。

- interval：このパラメータは、各ポーリングまで待機する時間をミリ秒単位で指定します。デフォルト値は 180 秒です。
- retries：このパラメータは、ポーリングを中止するまでに実行する再試行回数を指定します。デフォルト値の -1 は、再試行が無制限（常時）であることを意味します。10 などの正の値を定義した場合、この値は VNE が再試行を停止するまでに発生する再試行の回数を表します。

必要に応じて、デフォルト設定値を上書きできます。これらデフォルト設定値の変更は、シスコのサポートを受けながら行ってください。詳細については、シスコの代理店にお問い合せください。

VNE プロパティの編集

スキームを除くすべての VNE 設定を編集できます。設定を変更した場合、変更を有効にするには、VNE を再起動する必要があります。

（注）　展開情報および、VNE を AVM に割り当てる際のベスト プラクティスなどの推奨事項については、シスコの代理店にお問い合せください。

VNE を編集する手順は、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。

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　[VNE Properties] テーブルで目的の VNE を右クリックして [VNE Properties] ダイアログボックスを開き、[Properties] を選択します。

ステップ 4　必要に応じて、プロパティを編集または確認します。グレーアウトされている情報は、編集できません。[VNE properties] タブのフィールドに関する詳細は、次のトピックで説明します。

- 「VNE 全般設定」（P.5-22）
- 「VNE SNMP の設定」（P.5-24）
- 「VNE Telnet/SSH 設定」（P.5-25）
- 「VNE ICMP 設定」（P.5-34）
- 「VNE ポーリング設定」（P.5-34）

ステップ 5　必要な変更を行ったら、[Apply] をクリックし、[OK] をクリックします。VNE プロパティは、入力内容で更新されます。

ステップ 6　「VNE ステータス（Start、Stop または Maintenance）の変更」（P.5-36）の説明に従って、VNE を停止し、再起動します。

VNE ステータス（Start、Stop または Maintenance）の変更

Cisco ANA Manage では、VNE を起動または停止したり、あるいは VNE をメンテナンス モードにすることができます。VNE を起動すると、VNE がサーバ ブートストラップに追加されます。VNE を停止すると、VNE がサーバ ブートストラップから削除されます。

（注）　VNE のステータスを変更しても、VNE 永続性情報は保持されます。永続性情報は、後で使用する場合に備えて保管されるデータです。VNE 永続性メカニズムに関する情報については、「永続性の概要」（P.F-1）を参照してください。

NE では、通常の動作時に、ソフトウェアのアップグレード、ハードウェア変更、またはコールド リブートなどのメンテナンス作業および計画停止が発生することがあります。Cisco ANA プラットフォームでは、アクティブ ネットワークの全体的な機能に影響を与えることなく、このようなメンテナンス作業を実行できます。隣接 VNE は、メンテナンス対象の VNE へのリンクまたはこの VNE からのリンクに関連するアラームを生成しません。

メンテナンス モード（一時的な状態）の間、VNE は次のように動作します。

- VNE を明示的に（手動で）アクティブ状態に切り替えない限り、VNE 自体の状態は変更されません。
- デバイスをポーリングしません。
- 相関関係フロー問題に関するイベントを処理しますが、デバイスをポーリングしません。
- 新しいサービス アラームを開始しませんが、Link Down アラームの場合のように、隣接 VNE からイベントを受信することがあります。
- フローがアクティブであっても、syslog およびトラップを処理しません。
- 既存のリンクのステータスを維持します。
- 検証要求では失敗しません。

ただし、デバイス ソフトウェアをアップグレードする場合は、手動で VNE を再起動する必要はありません。VNE は自動的に再起動し、必要なすべての情報を更新します。詳細については、「VNE およびデバイスのソフトウェア アップデート」（P.5-21）を参照してください。

VNE は、VNE を通過するすべてのプロビジョニング フローをブロックします。メンテナンス モードのデバイスは、接続を切り離して再起動できますが、この操作を行っても Link Down アラームは発生しません。VNE は、再起動時に永続的な情報だけを受信し、VNE の認識された最新の設定に戻ります。トポロジ リンクは自動的に更新されます。

表 5-13 に、VNE がメンテナンス モードであることを表すために使用されるアイコンを示します。

表 5-13　VNE メンテナンス アイコン

アイコン	説明
	VNE が Cisco ANA NetworkVision のメンテナンス モードであることを示します。

VNE の状態を変更する、あるいは VNE をメンテナンス モードにするには、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。

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　[VNEs Properties] テーブルで、目的の VNE を選択します。

ステップ 4　次のアクションのいずれかを実行します。

- VNE を起動するには、右クリックして [Actions] > [Start] を選択するか、ツールバーの [Start] をクリックします。確認用のメッセージが表示されます。[OK] をクリックします。[VNEs Properties] テーブルに Up ステータスが表示されます。ゲートウェイが過負荷の場合、あるいは VNE がまだロード中の場合は、Starting Up ステータスが表示されることがあります。VNE のホストとして機能する AVM が Down ステータスの場合は、AVM がアップになるまで、VNE ステータスは Starting Up のままになります。
- VNE を停止するには、右クリックして [Actions] > [Stop] を選択するか、ツールバーの [Stop] をクリックします。確認用のメッセージが表示されます。[OK] をクリックします。[VNEs Properties] テーブルに Down ステータスが表示されます。プロセスのシャットダウン中に、Shutting Down ステータスが表示されることあります。
- VNE をメンテナンス モードにするには、右クリックして [Actions] > [Maintenance] を選択するか、ツールバーの [Maintenance] をクリックします。確認用のメッセージが表示されます。[OK] をクリックします。[VNEs Properties] テーブルに Maintenance ステータスが表示されます。

VNE の別の AVM への移動

Cisco ANA Manage により、AVM 間で 1 つまたは複数の VNE を移動することができます。移動対象の VNE はアンロードされます。VNE のステータスは、VNE のリロード後も維持されます。

（注）　VNE を別の AVM に移動すると、VNE 永続性情報は失われます。永続性情報は、後で使用する場合に備えて保管されるデータです。VNE 永続性メカニズムに関する情報については、「永続性の概要」（P.F-1）を参照してください。

1 つ以上の VNE を移動するには、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。

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。NE が [Content] 領域に表示されます。

ステップ 3　マウスまたはキーボードを使用して 1 つまたは複数の VNE を選択し、選択された VNE のいずれかを右クリックします。

ステップ 4　ショートカット メニューから [Move VNEs] を選択します。[Move To] ダイアログボックスが表示されます。

[Move To] ダイアログボックスには、VNE が現在存在する AVM を除いて、選択した Cisco ANA サーバ、そのユニット、および AVM を表すツリーとブランチが表示されます。ナビゲーション ツリーの最上位に、Cisco ANA サーバが表示されます。これらのブランチを展開したり折りたたんだりすることにより、情報を表示したり非表示にしたりできます。

ステップ 5　[Move To] ダイアログボックスで、VNE の移動先となる AVM を参照して選択します。

ステップ 6　[OK] をクリックします。VNE は新しい場所に移動され、[VNEs Properties] テーブルで選択した AVM の下に表示されます。

（注）　ナビゲーション ツリーで該当する AVM を選択し、移動した VNE を [VNEs Properties] テーブルに表示することにより、VNE が移動したことを確認できます。

（注）　移動対象の VNE は自動的にアンロードされてリロードされ、そのステータスは維持されます。

VNE の削除

Cisco ANA Manage を使用すると、ユニットおよび AVM から VNE を削除できます。このプロセスが実行されており、システムおよび Golden Source からすべての VNE リファレンスを削除すると、このプロセスは VNE を停止します。これには、指定されたユニットの VNE のレジストリ情報が含まれます。削除された VNE は、これ以降システム レポートに表示されなくなります。

Cisco ANA 3.6.6 からは、VNE を削除すると、すべてのレイヤ 3 VPN サイトと、VNE に関連付けられた仮想ルータ ビジネス エレメント データも削除できます。この手順の間にすべてのサイトおよび仮想ルータ ビジネス エレメント データを保持することを選択した場合、Cisco ANA NetworkVision を使用すると、これらのサイトおよびデータを手動で削除できます。Cisco ANA NetworkVision を使用したビジネス エレメントの削除の詳細については、『*Cisco Active Network Abstraction 3.6.7 User Guide*』を参照してください。

すべての VNE 情報が削除されるため、VNE を再度追加する際には、すべての VNE 情報を再入力する必要があります。

（注）　VNE に対して設定されている静的リンクをすべて削除しないと、静的リンクが設定されている VNE を削除できません。動的リンクは自動的に削除されます。

VNE を削除する手順は、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。

ステップ 2　[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　[VNEs Properties] テーブルで目的の VNE を右クリックし、[Delete] を選択します。確認用のプロンプトが表示されます。

ステップ 4　VNE を削除する場合は [Yes] を、VNE を保持する場合は [No] をクリックします。[Yes] をクリックすると、ダイアログボックスが表示され、Cisco ANA から VNE のレイヤ 3 VPN ビジネス エレメント データをすべて削除するかどうかを尋ねられます。

ステップ 5　次のどちらかを実行します。

- Cisco ANA からすべてのレイヤ 3 VPN サイトと仮想ルータ ビジネス エレメント データを削除するには、[Yes] をクリックします。このオプションを選択すると、選択した VNE に関連付けられたすべての VPN ビジネス エレメントが Cisco ANA から削除されます。Cisco ANA は、削除されたビジネス エレメントを削除することにより、Cisco ANA NetworkVision の VPN トポロジ ビューを適宜更新します。
- Cisco ANA のレイヤ 3 VPN サイトと仮想ルータ ビジネス エレメント データを保持するには、[No] をクリックします。このオプションを選択すると、Cisco ANA の選択された VNE に関連付けられた VPN ビジネス エレメントが保持されます。Cisco ANA は、Cisco ANA NetworkVision の VPN トポロジ ビューを更新します。孤立したビジネス エレメントは、赤の背景に白の X（  ）で示されます。これらの孤立したビジネス エレメントを削除するには、Cisco ANA NetworkVision でこれらのエレメントを手動で削除してください。
- VNE とそのレイヤ 3 VPN サイト、および仮想ルータ ビジネス エレメント データを削除せずにこの手順を終了するには、[Cancel] をクリックします。

レイヤ 3 VPN および Cisco ANA NetworkVision の詳細については、『*Cisco Active Network Abstraction 3.6.7 User Guide*』を参照してください。