CHAPTER 6

グローバル設定の管理

次の各トピックでは、クライアント ライセンス、ポーリング グループ、保護グループなど、Cisco ANA Manage のグローバル設定を定義および管理する方法について説明します。また、「今日のお知らせ」をカスタマイズする方法についても説明します。

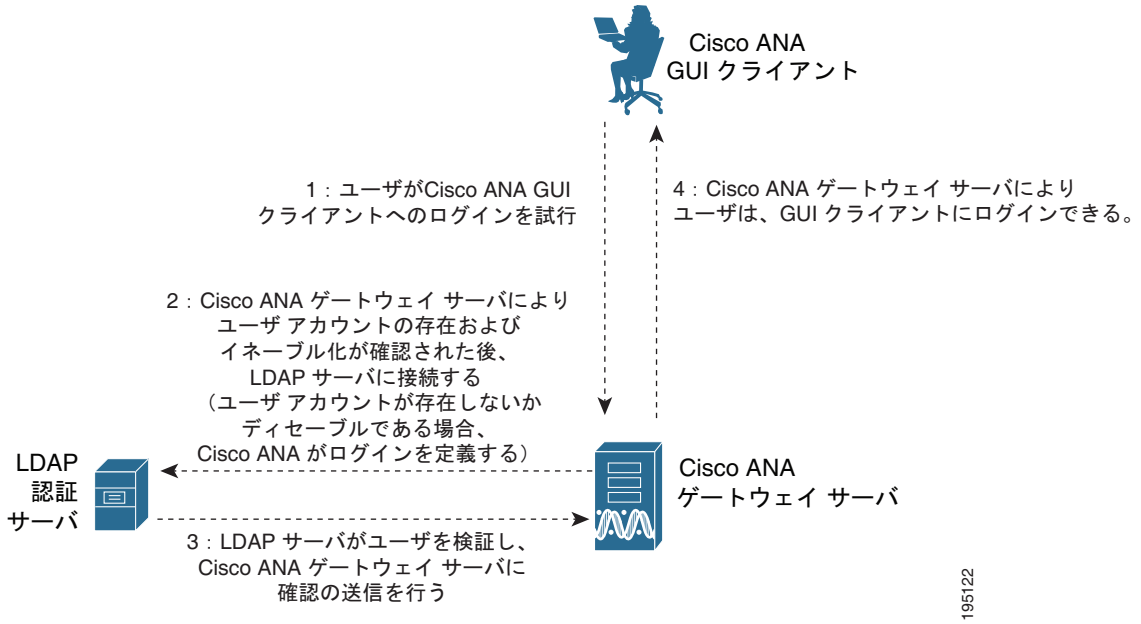
グローバル設定ブランチの詳細については、「[Global Settings] ブランチ」（P.2-16）を参照してください。

外部 LDAP サーバによるパスワード認証

ユーザ認証は、Cisco ANA によりローカルに管理できるほか、Lightweight Directory Access Protocol（LDAP）アプリケーションにより外部で管理することもできます。外部認証を使用する場合、ユーザ情報は（Cisco ANA データベースではなく）外部 LDAP サーバに格納されている情報と照合されます。外部認証サーバには、ログイン情報およびパスワード情報だけが保存され、ユーザのロールおよびスコープに関する情報は Cisco ANA データベースに保存されます。

図 6-1 で説明されているように、ユーザが GUI クライアントにログインすると、ゲートウェイ サーバは LDAP サーバにそのユーザの認証を行うよう要求します。ユーザが認証されると、LDAP サーバからゲートウェイ サーバへ認証確認が送信され、ゲートウェイ サーバにより、そのユーザに対して Cisco ANA へのログインが許可されます。これ以降そのユーザは、ロールおよびスコープにより指定された範囲で、機能を実行したりネットワーク要素にアクセスしたりできます（「ユーザ認証および権限付与の概要」（P.9-1）を参照）。

図 6-1　外部 LDAP サーバによるユーザ認証のプロセス



root ユーザが、LDAP の「緊急時」ユーザです。LDAP の緊急時ユーザは、Cisco ANA の検証のみを受けます。そのため、LDAP サーバがダウンしても、root ユーザは再度 Cisco ANA へログインできます。

次のトピックでは、外部認証サーバの使用方法について説明します。

- 「外部 LDAP サーバとの通信を行うための Cisco ANA の設定」（P.6-2）
- 「外部認証からローカル認証への変更」（P.6-5）

外部 LDAP サーバとの通信を行うための Cisco ANA の設定

ここで説明するのは、Cisco ANA ゲートウェイ サーバが LDAP サーバと通信するための設定手順です。プライマリ LDAP サーバとセカンダリ LDAP サーバを設定できます。手順の説明の中には、Distinguished Name（DN; 認定者名）、Common Name（CN; 通常名）、Domain Component（DC; ドメイン コンポーネント）などの LDAP 用語が使用されています。LDAP の DN は、LDAP データベースにおいてユーザを一意に識別するためのものです。絶対ファイル名と同じようにすべての階層が列記されますが、その順序は絶対ファイル名とは逆になります。CN および DC は、ドメイン名のアトリビュートです。

始める前に

『*Cisco Active Network Abstraction 3.6.7 Installation Guide*』に記載されている次の前提条件が満たされていることを確認します。

- LDAP サーバが適切に設定されていること。
- SSL または簡易暗号化プロトコルに必要なポート番号を把握していること。通常、SSL には 636、簡易暗号化プロトコルには 389 を使用します。
- ANA-LDAP プロトコルに対して SSL を選択すると、Cisco ANA ゲートウェイに SSL 証明書がインストールされます。

Cisco ANA ゲートウェイ サーバが LDAP サーバと通信するための設定手順は次のとおりです。

ステップ 1　[Global Settings] > [Authentication Method] を選択します。

ステップ 2　[LDAP Authentication] をクリックして、[LDAP Settings] 領域をアクティブにします。

ステップ 3　LDAP の設定を行います。この設定の中で、CN や DC などの LDAP スキーマ アトリビュートを指定します。

LDAP の URL	
LDAP サーバの名前およびポート番号を指定します。形式は次のとおりです。 **ldap://***host.company***.com:***port* プライマリ LDAP サーバおよびセカンダリ LDAP サーバは、次の形式で指定します。 **ldap://***host1.company***.com:***port1*　**ldap://***host2.company***.com:***port2* 例 **ldap://ldapsj.acme.com:636　ldap://ldapsfo.acme.com:636**	
*host.company***.com**	LDAP サーバの完全修飾ドメイン名または IP アドレスと、2 つのフィールドからなる DN サフィックス（*company***.com**）を続けて指定します。
port	LDAP サーバのネットワーク ポートを指定します。通常、LDAP サーバのポート番号には、簡易暗号化の場合は 389、SSL 暗号化の場合は 636 を使用します。

DN プレフィクス

LDAP DN の前半部分です。これを基にしてユーザを一意に識別できます。DN プレフィクスは必ず次の形で入力してください。

CN=

実際には **CN=***Value* という形式で、特定ユーザの通常名を指定しますが、ここでは、*Value* は空の状態にしてください。*Value* には Cisco ANA のユーザ名が自動的に設定されます。

DN サフィックス

LDAP DN の後半部分です。ディレクトリ内の場所が指定されます。

,CN=Users,DC=*LDAP_server***,DC=***company***,DC=com**

形式上、次の点に注意が必要です。

- 先頭の文字がカンマ（,）であること。
- 末尾に終了記号や句読記号を一切入力しないこと。

例

,CN=Users,DC=ldapsj,DC=cisco,DC=com

,CN=Users	ユーザのタイプに対する通常名を指定します。**Users** と入力してください。次のように、先頭にはカンマを入力する必要があります。 **,DC=Users**
,DC=*LDAP_server*	Cisco ANA サーバの完全修飾ドメイン名または IP アドレスを表すドメイン コンポーネントを指定します。先頭にはカンマを入力する必要があります。例 **,DC=ldapsj**
,DC=*company*	ドメイン名の前半部分を指定します。先頭にはカンマを入力する必要があります。例 **,DC=acme**
,DC=com	ドメイン名の後半部分を指定します。**com** と入力してください。次のように、末尾には終了記号や句読記号を一切入力しないでください。 **,DC=com**

ANA-LDAP プロトコル

Cisco ANA ゲートウェイ サーバと LDAP サーバとの間の通信に使用する暗号化プロトコルです。

（注） 使用する暗号化プロトコルは、Cisco ANA ゲートウェイ サーバと LDAP サーバの双方で設定する必要があります。

SIMPLE	LDAP を使用して暗号化します。デフォルトではポート 389 を使用します。
SSL	SSL を使用して暗号化します。デフォルトではポート 636 を使用します。SSL 証明書は Cisco ANA ゲートウェイ上にインストールする必要があります（『*Cisco Active Network Abstraction 3.6.7 Installation Guide*』を参照）。

ステップ 4　[Apply] をクリックします。

ステップ 5　ゲートウェイを再起動して、変更内容を有効にします。「Cisco ANA ゲートウェイの再起動（ユーティリティ スクリプト）」（P.C-1）を参照してください。

これによって、外部 LDAP サーバを使用してユーザ パスワードを管理できるようになります。

外部認証からローカル認証への変更

外部認証を使用している Cisco ANA が LDAP サーバと通信できない場合は、root ユーザに限り Cisco ANA に再ログインできます。これは、root ユーザが LDAP の*緊急時ユーザ*であり、その検証を行えるのが Cisco ANA に限られるためです。root ユーザは、Cisco ANA にログインして、認証方式をローカル認証に変更し、その他のユーザがログインできるようにそのユーザ アカウントを編集できます。ユーザ アカウントの編集に関する詳細については、「ユーザ情報の変更とアカウントの無効化（[General] タブ）」（P.9-10）を参照してください。

認証方式を外部認証からローカル認証へ変更する手順は次のとおりです。

ステップ 1　[Global Settings] > [Authentication Method] を選択します。

ステップ 2　[ANA Authentication] をクリックして、ローカル認証をアクティブにします。

ステップ 3　[Apply] をクリックします。

ステップ 4　ゲートウェイを再起動して、変更内容を有効にします。「Cisco ANA ゲートウェイの再起動（ユーティリティ スクリプト）」（P.C-1）を参照してください。

ステップ 5　ユーザ アカウントの設定を適切に変更します（「ユーザ情報の変更とアカウントの無効化（[General] タブ）」（P.9-10）を参照）。

クライアント ライセンスの管理

ここでは、クライアント ライセンスの管理手順について説明します。

インストール時に Cisco ANA で作成されるユーザは、root ユーザだけです。その他のユーザに権限を付与する場合は、ライセンス キーを取得し、それをインストールする必要があります。使用できるライセンス キーのタイプは次のとおりです。

- Fixed（固定）：ユーザに対して Cisco ANA クライアントへアクセスする権限が付与されます。製品に付属するデフォルトのライセンスは固定タイプであり、root ユーザに限って適用されます。
- Floating（フローティング）：特定数のユーザに対して、Cisco ANA クライアントおよび BQL へ同時にアクセスする権限が付与されます。Cisco ANA クライアント（Cisco ANA Manage、Cisco ANA NetworkVision、または Cisco ANA EventVision）または BQL にログインする各ユーザは、ライセンスを使用していると見なされます。Cisco ANA クライアントおよび BQL すべてに対する同時ログインの総数は、ライセンスの数によって制限されます。
- Floating User（フローティング ユーザ）：特定数のユーザに対して、各 Cisco ANA クライアント（Cisco ANA Manage、Cisco ANA NetworkVision、および Cisco ANA EventVision）のインスタンスを同時に 1 つずつ開く権限が付与されます。つまり各ユーザは Cisco ANA Manage、Cisco ANA NetworkVision、および Cisco ANA EventVision の同時セッションにログインして作業を行えます。同一ユーザが同一クライアントのインスタンスを複数開いた場合、インスタンスごとに別々のライセンスを使用していると見なされます。

一般に、Floating ライセンスは BQL へのアクセスに使用され、Floating User ライセンスは、GUI アプリケーションへのアクセスに使用されます。

Cisco ANA のライセンス メカニズムでは、ログインして認証されたユーザに対してライセンス ファイルが検索されます。その際、ライセンスは 1 つずつ検索され、ユーザに適したライセンスが見つかった時点で、そのライセンスにユーザが関連付けられます。

Floating ライセンスまたは Floating User ライセンスに対するユーザ数は、ライセンスの提供時にシスコが設定します。すべてのライセンスが使用中の場合、さらに別のユーザがログインしようとすると、エラー メッセージが表示され、そのユーザはログインできません。

次に示すライセンスの具体例も参考にしてください。

例 1：Floating ライセンス

3 名のユーザに権限を付与する Floating ライセンスがインストールされているとします。次のように、このライセンスにはさまざまな使用方法があります。

- あるユーザが Cisco ANA Manage、Cisco ANA NetworkVision、および Cisco ANA EventVision へ同時にログインする場合。このライセンスでは最大 3 つの同時ログインしか許可されないため、その他のユーザはログインできません。
- Cisco ANA Manage、Cisco ANA NetworkVision、Cisco ANA EventVision にそれぞれユーザが 1 名ずつログインする場合。同様に、このライセンスでは最大 3 つの同時ログインしか許可されないため、これ以上のユーザはログインできません。

例 2：Floating User ライセンス

この例では、3 名のユーザに権限を付与する Floating User ライセンスがインストールされているとします。3 名の各ユーザが、Cisco ANA Manage、Cisco ANA NetworkVision、および Cisco ANA EventVision それぞれのインスタンスを同時に 1 つずつ開くと、3 つのライセンスが使用されることになります。この場合、3 名のうちいずれかのユーザ、またはこの 3 名とは別のユーザが、いずれかの Cisco ANA GUI アプリケーションの別のインスタンスを 1 つ開こうとすると、4 つめのライセンスが使用されると見なされます。しかしこの Floating User ライセンスのユーザ数は 3 名に制限されています。このため、その Cisco ANA GUI アプリケーションは開きません。

詳細については、「[Client Licenses] サブブランチ」（P.2-18）を参照してください。

ライセンス キーを取得する場合、またはライセンス購入後にユーザを追加する場合は、シスコの代理店にお問い合せください。

ライセンスのインストール

ライセンスをインストールする手順は次のとおりです。

ステップ 1　[Global Settings] > [Client Licenses] を選択します。[Client Licenses] テーブルが表示されます。

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

- [Client Licenses] を右クリックし、[New License] を選択する。
- [File] > [New License] を選択する。
- ツールバーにある [New License] をクリックする。

ステップ 3　付与されたファイルからキーをコピーします。

ステップ 4　それを [New Client License] ダイアログボックスに貼り付けます。

ステップ 5　[OK] をクリックします。コンテンツ領域に、新しいライセンス情報が表示されます。

ライセンスのアンインストール

ライセンスは必要に応じてアンインストールできます。アンインストールするのは、たとえばライセンスの有効期限が経過した場合などです。

（注）　デフォルト ライセンスはアンインストールできません。

ライセンスをアンインストールする手順は次のとおりです。

ステップ 1　Cisco ANA Manage で [Global Settings] > [Client Licenses] を選択します。

ステップ 2　コンテンツ領域で、アンインストールするライセンスを選択します。

ステップ 3　選択したライセンスを次のいずれかの方法でアンインストールします。

- ライセンスを右クリックし、[Delete] を選択する。
- ツールバーにある [Delete] をクリックする。

これでライセンスがアンインストールされます。アンインストールされたライセンスはこれ以降、[Cisco ANA Manage] ウィンドウのコンテンツ領域には表示されません。

クライアント ライセンスのプロパティの表示

Cisco ANA Manage では、IP アドレスやアカウント名など、ライセンスのさまざまなプロパティを表示できます。

クライアント ライセンス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 で [Global Settings] > [Client Licenses] を選択します。

ステップ 2　コンテンツ領域から目的のライセンスを選択します。

ステップ 3　次のいずれかの方法で [Client License Properties] ウィンドウを開きます。

- ライセンスを右クリックし、[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。

表 6-1 は、[Client License Properties] ウィンドウに表示されるフィールドとその説明をまとめたものです。

表 6-1　クライアント ライセンスのプロパティ

フィールド	説明
[License Type]	使用できるライセンスのタイプは次のとおりです。 • [Fixed] : ユーザに対して Cisco ANA クライアントへアクセスする権限が付与されます。製品に付属しているデフォルト ライセンスは、固定タイプであり、root ユーザに限って適用されます。 • [Floating] : 特定数のユーザに対して、Cisco ANA クライアントおよび BQL へ同時にアクセスする権限が付与されます。Cisco ANA クライアント（Cisco ANA Manage、Cisco ANA NetworkVision、または Cisco ANA EventVision）または BQL にログインする各ユーザは、ライセンスを使用していると見なされます。Cisco ANA クライアントおよび BQL すべてに対する同時ログインの総数は、ライセンスの数によって制限されます。 • [Floating user] : 特定数のユーザに対して、各 Cisco ANA クライアント（Cisco ANA Manage、Cisco ANA NetworkVision、および Cisco ANA EventVision）のインスタンスを同時に 1 つずつ開く権限が付与されます。つまり各ユーザは Cisco ANA Manage、Cisco ANA NetworkVision、および Cisco ANA EventVision の同時セッションにログインして作業を行えます。
[User Count]	ライセンスによってクライアント アプリケーションの操作を許可されているユーザ数が表示されます。ユーザ数に上限がある場合はその数が表示され、ユーザ数に制限がない場合は 0（ゼロ）が表示されます。
[Client Type]	ユーザに権限が付与されたアプリケーション（BQL や クライアント アプリケーションなど）が表示されます。
[Creation Date]	ライセンスが実装された日付が表示されます。
[Properties Content Area] テーブル 選択したライセンスに割り当てられているユーザのプロパティが表示されます。	
[IP]	このライセンスおよびユーザ名に対して許可されたログイン元の IP アドレスが表示されます。IP アドレスが表示されていない場合、指定されたユーザ名を持つユーザは、任意の IP アドレスからログインできます。
[BQL Enabled]	ライセンスにより許可されている接続先が、クライアント アプリケーションに限定されているか、BQL も含んでいるかが明示されます。
[Account Name]	ログインに使用するユーザ名が表示されます。

ステップ 4　右上隅をクリックして、[Client License Properties] ウィンドウを閉じます。

データベース セグメントの表示

Cisco ANA Manage では、次のような情報を表示し、それらを監視できます。

- データベース セグメントのストレージ割り当て情報
- データベースによるディスクの使用量
- データベースのデータ量増加

これらの情報は、システムにより自動的にチェックされます。

データベース セグメントを表示するには、[Global Settings] > [DB Segments] を選択します。データベース セグメントは、コンテンツ領域に表示されます。

[DB Segments] テーブルに表示されるカラムの詳細については、「[DB Segments] サブブランチ」（P.2-20）を参照してください。

「今日のお知らせ」のカスタマイズ

Cisco ANA Manage では、ユーザがクライアント アプリケーションにログインする際に表示される「今日のお知らせ」（バナー）を定義できます。ユーザは、ログインする前にこのメッセージの内容に同意する必要があります。同意しないユーザはログインできません。このメッセージは、HTML フォーマットをサポートしています。

メッセージの内容は必要に応じて変更できます。ただし、一度に適用できるメッセージは 1 つだけです。

ここでは、「今日のお知らせ」を追加する方法および削除する方法について説明します。

- 「メッセージの追加」（P.6-9）
- 「メッセージの削除」（P.6-10）

メッセージの追加

「今日のお知らせ」をカスタマイズする手順は次のとおりです。

ステップ 1　[Global Settings] > [Message of the Day] を選択します。コンテンツ領域に [Title] フィールドと [Message] フィールドが表示されます。

ステップ 2　[Title] フィールドには、メッセージのタイトルを入力します。

ステップ 3　[Message] フィールドには、ユーザのログイン時に表示するテキストを入力します。

（注）　[Message] ダイアログボックスには、[Abort] ボタンと [Continue] ボタンがデフォルトで表示されます。そのため、メッセージはこれらのボタンのアクションに合せた内容にする必要があります （例：「製品ライセンス契約の利用規約に同意しますか。同意する場合は [Continue] を、同意しない場合は [Abort] をクリックしてください。」）。

ステップ 4　[Save] 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。これで、ユーザがクライアント アプリケーションにログインする際にメッセージが表示されます。

メッセージの削除

「今日のお知らせ」を削除する手順は次のとおりです。

ステップ 1　[Global Settings] > [Message of the Day] を選択します。

ステップ 2　[Message] フィールド内のテキストを削除します。

ステップ 3　[Save] 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 4　[OK] をクリックします。これで、ユーザがクライアント アプリケーションにログインしても、メッセージは表示されません。

ポーリング グループの管理と適応ポーリング

ここでは、ポーリング グループの管理方法と、Cisco ANA における適応ポーリングの動作のしくみについて説明します。

ポーリング グループの概要

ユニット サーバでは、ネットワークの正確な最新情報を検出し、それらを表示するために、NE へのポーリングが行われます。ポーリングは、設定された時間間隔で定期的にトリガーされます。管理者は、ポーリング レートのカスタマイズや最適化を行えます。

Cisco ANA では、管理対象デバイスから情報を取得する周期を微調整できます。そのため、さまざまな VNE により使用されるネットワーク トラフィックの量に対して高度な制御と柔軟な対応が可能です。

表 6-2 は、設定できるさまざまなポーリング間隔とその説明をまとめたものです。

表 6-2　ポーリング間隔のタイプ

タイプ	説明
ステータス	デバイス 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、ステータスに関連する情報のポーリング レート。これらの情報は、NE の動作ステータスおよび管理ステータスに関連するものです。
設定	VC テーブルやスクランブリングなど、設定に関連する情報のポーリング レート。
システム	デバイス名やデバイスの場所など、システムに関連する情報のポーリング レート。

表 6-2　ポーリング間隔のタイプ （続き）

タイプ	説明
トポロジ レイヤ 1 カウンタ	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。
トポロジ レイヤ 2 カウンタ	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。

（注）　ポーリング レートの単位はすべて秒です。

VNE では、定義されたポーリング間隔に加え、ネットワーク要素が過負荷にならないよう適応ポーリングが実装されます。デバイスの CPU のチェック時には、管理対象デバイスへの負荷が増大しないように、特定のポーリングが一時保留される場合があります。「適応ポーリング」（P.6-11）を参照してください。

ユーザは、管理対象デバイスに適用可能なカスタマイズされたポーリング間隔を設定することにより、ポーリング プロファイルを定義できます。VNE では、事前に設定されたその値に従って、ネットワーク要素へのポーリングが行われます。これにより、デバイスに対するさまざまな情報のポーリングが、技術上の要件や業務上の要件に合せて確実に実行されます。

コア デバイスは、ステータスに関連する情報のポーリング間隔を短く、設定に関連する情報のポーリング間隔を長く設定したポーリング グループに割り当てることができます（すべてのデバイスに同じポーリング プロファイルを使用します）。一方、エッジ デバイスおよびアクセス デバイスに対しては、システムおよび設定に関連する情報のポーリング間隔をより短く設定できます。たとえば、管理対象ネットワーク サービス オペレータには、カスタマーとの契約内容を反映したポーリング グループを使用できます。これにより、特別なカスタマーのデバイスに対するポーリング間隔を、通常カスタマーのデバイスより短く設定できます。

便宜上、Cisco ANA には、*デフォルト*および*低レート*という事前設定済みのポーリング グループが用意されています。これらのポーリング グループは削除できません。表 6-3 は、デフォルトおよび低レートの各ポーリング グループに対する設定内容をまとめたものです。

表 6-3　デフォルト ポーリング グループおよび低レート ポーリング グループのポーリング レート

アトリビュート	デフォルト ポーリング グループの設定	低レート ポーリング グループの設定
ステータス ポーリング レート	180 秒（3 分）	360 秒（6 分）
設定ポーリング レート	900 秒（15 分）	1800 秒（30 分）
システム ポーリング レート	86400 秒（24 時間）	172800 秒（48 時間）
レイヤ 1 ポーリング レート	30 秒	30 秒
レイヤ 2 ポーリング レート	30 秒	30 秒

適応ポーリング

VNE では、定義されたポーリング間隔に加え、ネットワーク要素が過負荷にならないよう適応ポーリングが実装されます。デバイスの CPU 使用量をチェックする際は、管理対象デバイスへの負荷が増大しないように、特定のポーリングが一時保留される場合があります。

VNE に対する CPU 使用量が最大しきい値を超過すると、アラームが送信され、その VNE に対するポーリング間隔は通常より長くなり、NE へコマンドが送信されてから次のコマンドが送信されるまでの間に遅延時間が追加されます。

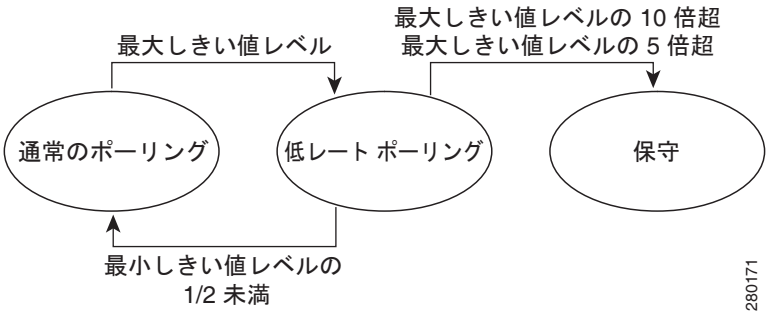
- SNMP の場合は、SNMP パケットがデバイスへ送信される間隔が遅延時間として追加されます。
- Telnet または SSH の場合は、CLI コマンドがデバイスへ送信される間隔が遅延時間として追加されます。

VNE に対する CPU 使用量のしきい値が、基準となるしきい値を下回ると、アラームが送信され、その VNE に対するポーリングは通常に戻ります。

VNE に対するこれらの値は、システム レジストリを介してカスタマイズできます（CPU 使用量の最小しきい値および最大しきい値など）。定義されたしきい値に達した場合はアラームが送信されます。また、基準となるしきい値も定義できます。これにより、CPU 使用量のしきい値が最大値を下回った場合、または最小値を上回った場合には、メッセージが送信され元のアラームはクリアされます。これらの値はレジストリで定義されます。

さらには、最大および最小の許容値レベルも、システム レジストリを使ってカスタマイズできます。通常のポーリングが行われている VNE に対して、CPU 使用量が増加し最大しきい値（上限許容値レベル）を上回った場合、その状態が 5 回（デフォルト）確認された時点で、その VNE へのポーリングは低レート ポーリングに移行します（図 6-2 を参照）。

図 6-2　　ポーリングのしきい値レベル

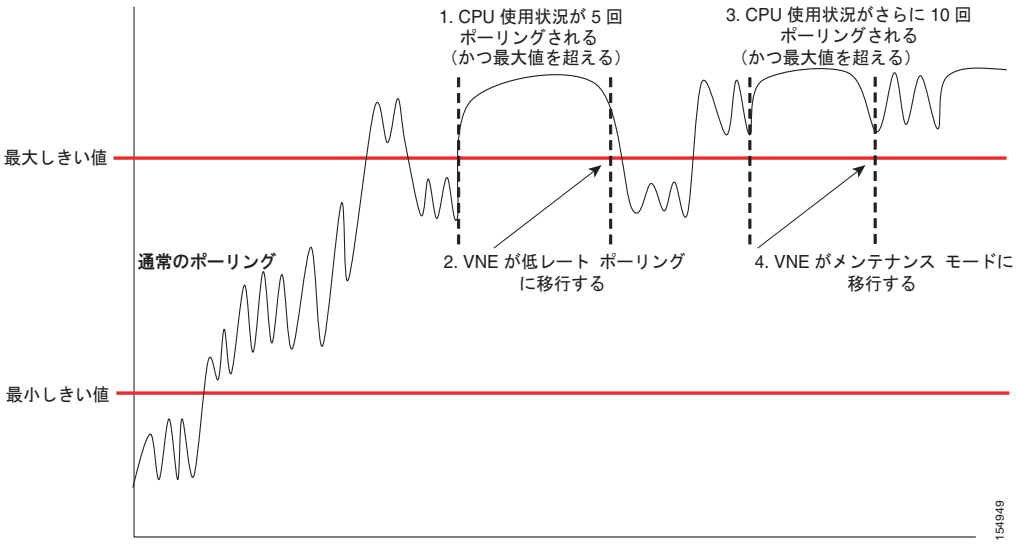


5 回のチェック後に低レート ポーリングへ移行した VNE に対しては、CPU 使用量が依然多い状態にあるかどうかを確認するため、さらに 10 回（デフォルト）のチェックが行われます。CPU 使用量が多ければ、その VNE はメンテナンス モードに移行します。いったんメンテナンス モードに移行した VNE へのポーリングは、自動では通常のポーリングに戻りません。通常のポーリングに戻すには、手動での操作が必要です。VNE がメンテナンス モードの場合、NE に対するポーリングは行われません。

図 6-3 のグラフ変化の説明

1. CPU 使用量は、5 回行われたいずれのポーリングでも、最大しきい値を上回っている。
2. VNE へのポーリングが低レート ポーリングに移行する。
3. CPU 使用量のポーリングがさらに 10 回行われる。
4. CPU 使用量は依然、最大しきい値を上回っているため、VNE がメンテナンス モードへ移行する。

図 6-3　CPU 使用量の例 1

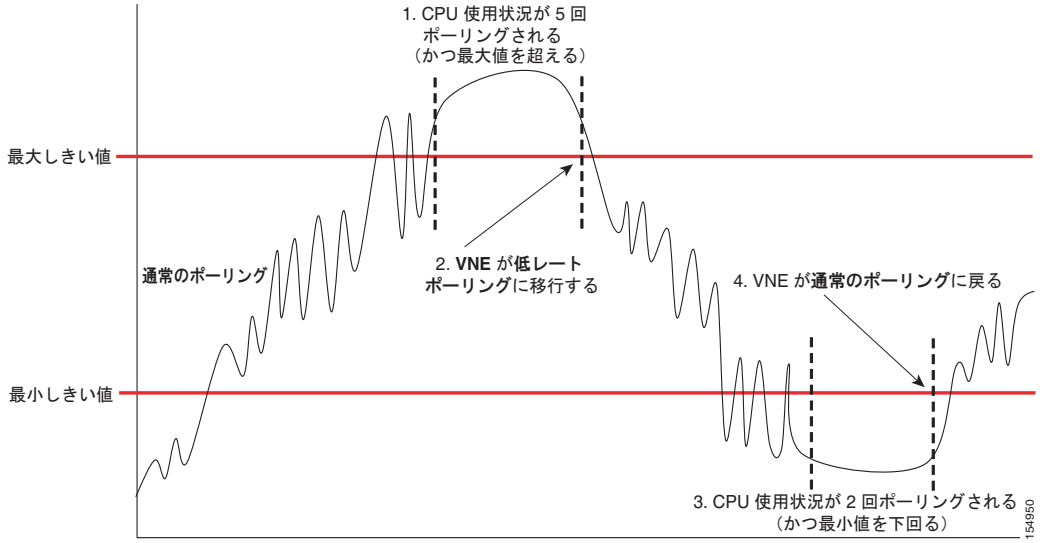


VNE で低レート ポーリングが行われている場合、CPU 使用量が通常レベルにまで低下する（または最小しきい値を下回る）と、Cisco ANA では、その VNE に対する CPU 使用量が最大しきい値を下回った状態が 2 回（デフォルト）確認された時点で、その VNE のポーリングが通常のポーリングに戻されます。

図 6-4 のグラフ変化の説明

1. CPU 使用量は、5 回行われたいずれのポーリングでも、最大しきい値を上回っている。
2. VNE へのポーリングが低レート ポーリングに移行する。CPU 使用量が通常レベルまで低下し、さらに最小しきい値を下回る。
3. CPU 使用量のポーリングがさらに 2 回行われる。
4. CPU 使用量は依然、最大しきい値を超えていないため、VNE のポーリングが通常ポーリングに戻る。

図 6-4　CPU 使用量の例 2



CPU 使用量が多く、低レート ポーリングが適用されている場合、AVM がダウンしたとしても、再起動すれば以前のポーリング間隔はそのまま維持されます。再起動された AVM には、ダウンする前と同じポーリング間隔が適用されます。

ポーリング グループのカスタマイズ

Cisco ANA Manage では、新規ポーリング グループの作成およびカスタマイズを行えます。これらの新規ポーリング グループは、VNE を定義する際に使用できます。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。

注意　ポーリング レートを変更すると、過剰なトラフィックが発生することや、ネットワーク要素がクラッシュすることがあります。導入に関する情報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。

ポーリング グループを作成およびカスタマイズする手順は次のとおりです。

ステップ 1　[Global Settings] > [Polling Groups] を選択します。

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

- [Polling Groups] を右クリックし、[New Polling Group] を選択する。
- [File] > [New Polling Group] を選択する。
- ツールバーにある [New] をクリックする。

ステップ 3　新規のポーリング グループに対して必要な情報を入力します。

フィールド	説明
[Name]	ポーリング グループの名前を入力します。
[Description]	ポーリング グループに関する説明を入力します。
[Status]	ステータスに関連した情報に対するポーリング間隔の秒数を入力します。
[Configuration]	設定に関連した情報に対するポーリング間隔の秒数を入力します。
[System]	システムに関連した情報に対するポーリング間隔の秒数を入力します。
[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間隔を秒単位で入力します。このプロセスは、継続的に実行されます。
[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間隔を秒単位で入力します。このプロセスは、オンデマンドで使用できます。

ステップ 4　[OK] をクリックします。コンテンツ領域に、新しいポーリング グループが表示されます。

ポーリング グループの詳細については、「ポーリング グループの概要」（P.6-10）を参照してください。

新しいポーリング グループは、新規の VNE を定義する際に使用できます。「VNE の作成：前提条件」（P.5-12）を参照してください。

ポーリング グループの編集

Cisco ANA Manage では、ポーリング グループのさまざまなプロパティの編集や表示を行えます。

ポーリング グループのプロパティを表示する手順および必要に応じて編集する手順は次のとおりです。

ステップ 1　[Global Settings] > [Polling Groups] を選択します。

ステップ 2　次のいずれかの方法で、ポーリング グループの [Properties] ダイアログボックスを開きます。

- コンテンツ領域で、表示または編集するポーリング グループを右クリックし、[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。

[Update Polling Group] ダイアログボックスに表示されるフィールドの詳細については、「ポーリング グループのカスタマイズ」（P.6-14）を参照してください。

ステップ 3　必要に応じて、ポーリング グループのプロパティを編集します。

（注）　このポーリング グループがいずれかの VNE で使用されている場合は、警告メッセージが表示されます。

ステップ 4　[Apply] をクリックします。

ステップ 5　[OK] をクリックします。編集した内容に従ってポーリング グループの設定が修正されます。

（注）　編集したポーリング グループの設定は、そのポーリング グループを使用しているすべての VNE およびデバイスに適用されます。

ポーリング グループの削除

Cisco ANA Manage では、ポーリング グループを削除できます。

（注）　ただし、VNE で使用されているポーリング グループは削除できません。

ポーリング グループを削除する手順は次のとおりです。

ステップ 1　[Global Settings] > [Polling Groups] を選択します。

ステップ 2　コンテンツ領域で、削除するポーリング グループを右クリックし、[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 3　[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 4　[OK] をクリックします。[Polling Group] テーブルから目的のポーリング グループが削除されます。

保護グループの管理

デフォルトでは、Cisco ANA ファブリック内のユニットはすべて、default-pg 保護グループという単一のグループ（またはクラスタ）に属します。これらのユニットのデフォルト設定は、保護グループをカスタマイズしそれらのグループにユニットを割り当てることで変更できます。

ユニットのハイ アベイラビリティを設定および管理する手順については、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。

Cisco ANA Manage では、新規の保護グループを作成できます。新規作成した保護グループは、ユニットを定義する際に使用できます。詳細については、「新しい Cisco ANA ユニットの追加」（P.4-5）を参照してください。

保護グループを作成する手順は次のとおりです。

ステップ 1　[Global Settings] > [Protection Groups] を選択します。

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

- [Protection Groups] を右クリックし、[New Protection Group] を選択する。
- [File] > [New Protection Group] を選択する。
- ツールバーにある [New] をクリックする。

ステップ 3　新規の保護グループに対して必要な情報を入力します。

フィールド	説明
[Name]	保護グループに対する一意の名前を入力します。
[Description]	保護グループに関する説明を入力します。

ステップ 4　[OK] をクリックします。[Protection Groups] テーブルのコンテンツ領域に、新規作成された保護グループと、現在定義されているすべての保護グループが表示されます。

（注）　コンテンツ領域に表示されている default-pg 保護グループがデフォルトの保護グループです。デフォルトでは、Cisco ANA ファブリック内のユニットはすべて、この保護グループに属します。

保護グループのプロパティの表示および編集

保護グループのさまざまなプロパティ（説明など）を表示できるほか、必要に応じて編集することもできます。

保護グループのプロパティを表示または編集する手順は次のとおりです。

ステップ 1　[Global Settings] > [Protection Groups] を選択します。

ステップ 2　次のいずれかの方法で、保護グループの [Properties] ダイアログボックスを開きます。

- [Protection Groups] を右クリックし、[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。

ステップ 3　保護グループのプロパティを表示し、必要に応じてその説明を編集します。

ステップ 4　[OK] をクリックします。[Cisco ANA Manage] ウィンドウが表示されます。

保護グループの削除

Cisco ANA Manage では、保護グループを削除できます。

（注）　削除する保護グループが、いずれのユニットでも使用されていないことを確認します。

保護グループを削除する手順は次のとおりです。

ステップ 1　[Global Settings] > [Protection Groups] を選択します。

ステップ 2　コンテンツ領域で、削除する保護グループを選択します。

ステップ 3　次のいずれかの方法で保護グループを削除します。

- 保護グループを右クリックし、[Delete] を選択する。
- ツールバーにある [Delete] をクリックする。

目的の保護グループが削除されます。