NAC アプライアンス（CCA）： Clean Access Manager（CAM）のハイ アベイラビリティ（HA）の設定

目次

概要

このドキュメントでは、ハイ アベイラビリティ（HA）で 2 つの Clean Access Manager（CAM）マシンを設定する方法について説明します。 Clean Access Manager がハイ アベイラビリティ モードで導入されると、想定外のシャットダウンというイベントが発生しても、ユーザは、重要な監視、認証、およびレポートの作業を継続できます。

注: CAS で HA 機能を設定する方法については、『Cisco NAC アプライアンス：Clean Access Server（CAS）インストールおよびアドミニストレーション ガイド』の「ハイ アベイラビリティ（HA）の設定」セクションを参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Network Admission Control（NAC; ネットワーク アドミッション制御）アプライアンスの CAM バージョン 4.1.x に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

概要

次のキー ポイントでは、HA-CAM の運用に関する概要について説明します。

1. Clean Access Manager のハイ アベイラビリティ モードは、アクティブ/パッシブの 2 サーバの構成で、スタンバイ用の CAM マシンがアクティブな CAM マシンのバックアップの役割を担います。
2. アクティブな Clean Access Manager で、システムのすべての作業が実行されます。 スタンバイ CAM では、アクティブな CAM が監視され、スタンバイのデータベースとアクティブな CAM のデータベースの同期がとられます。
3. 両方の CAM では、信頼済みインターフェイス eth0 の仮想サービス IP が共有されます。 ドメイン名は、SSL 証明書に使用する必要があります。
4. プライマリ CAM マシンとセカンダリ CAM マシンでは、2 秒ごとに UDP ハートビート パケットがやり取りされます。 ハートビート タイマーの期限が切れると、ステートフル フェールオーバーが発生します。
5. CAM の eth1 インターフェイスとシリアル インターフェイスのいずれか一方または両方は、ハートビート パケットおよびデータベースの同期に使用できます。 eth1 インターフェイスとシリアル インターフェイスの両方がハートビートに設定されると、両方のインターフェイスでフェールオーバーが発生します。

Clean Access Manager のハイ アベイラビリティ モードは、アクティブ/パッシブの 2 サーバの構成で、スタンバイ用の Clean Access Manager マシンがアクティブな Clean Access Manager マシンのバックアップの役割を担います。 アクティブな CAM で、ほとんどの作業が通常の状態で実行されます。また、スタンバイでは、アクティブな CAM が監視され、スタンバイのデータベースとアクティブな CAM のデータベースの同期がとられます。

アクティブな CAM がシャットダウンし、ピアの「ハートビート」信号に応答しないなどの、フェールオーバー イベントが発生すると、スタンバイがアクティブな CAM の役割を担います。

最初に HA ピアを設定するときに、HA プライマリ CAM および HA セカンダリ CAM を指定する必要があります。 まず、HA プライマリがアクティブな CAM で、HA セカンダリがスタンバイ（パッシブ）CAM ですが、アクティブ/パッシブの役割は永続的には割り当てられません。 プライマリ CAM がダウンすると、セカンダリ（スタンバイ）がアクティブな CAM になります。 元のプライマリ CAM が再起動されると、バックアップの役割を担います。

Clean Access Manager の起動時に、ピアがアクティブかどうかが確認されます。 アクティブではない場合、起動される CAM が、アクティブの役割を担います。 一方、ピアがアクティブな場合、起動される CAM は、スタンバイになります。

同時に 2 台の Clean Access Manager を HA ペアとして設定できます。または、新しい Clean Access Manager を既存のスタンドアロン CAM に追加し、ハイ アベイラビリティのペアを作成することもできます。 ネットワークと Clean Access Server に対してペアが 1 つのエンティティとして示されるようにするには、HA ペアの信頼済みインターフェイス（eth0）としてサービス IP アドレスを指定する必要があります。

ハイ アベイラビリティ情報がやり取りされるクロスオーバー ネットワークを作成するためには、両方の CAM の eth1 ポートを接続し、組織内で現在ルーティングされていないプライベート ネットワーク アドレスを指定します（デフォルトの HA クロスオーバー ネットワークは 192.168.0.252 です）。 次に、Clean Access Manager によって、各 CAM の eth1 ポートのプライベートでセキュアな 2 ノード ネットワークが作成され、UDP ハートビート トラフィックがやり取りされて、データベースが同期されます。 CAM では、eth1 が常に UDP ハートビート インターフェイスとして使用されることに注意してください。

追加のセキュリティとして、各 Clean Access Manager のシリアル ポートも、ハートビートのやり取りのために接続できます。 この場合、UDP ハートビートとシリアル ハートビートの両方のインターフェイスに障害が発生すると、スタンバイ システムに制御が渡されます。

注: HA のシリアル ケーブル接続（HA-CAM または HA-CAS のいずれか）では、シリアル ケーブルは「ヌル モデル」ケーブルである必要があります。

基本的な要件

警告： データベースの同期の際にデータが損失する可能性を防ぐためには、アクティブな（プライマリの）Clean Access Manager がフェールオーバーする前に、スタンバイの（セカンダリの）Clean Access Manager が常に実稼働状態である必要があります。

ハイ アベイラビリティの設定を開始する前に、次の要件が満たされていることを確認してください。

1. ハイ アベイラビリティ（フェールオーバー）用ライセンスを取得済みであること。**注:** CAM フェールオーバー（HA）ライセンスをインストールするときには、まず、プライマリ CAM にフェールオーバー ライセンスをインストールし、次に他のすべてのライセンスをロードしてください。 スタンドアロン ライセンスも、ハイ アベイラビリティで使用できます。
2. 両方の CAM がインストールされ、設定されていること。
3. ハートビートには、各 CAM が、固有のホスト名（またはノード名）を有していること。 HA CAM ペアでは、このホスト名がピアに示され、DNS を介して解決されるか、ピアの /etc/hosts ファイルに追加される必要があります。
4. HA CAM ペアのドメイン名の CA 署名済み証明書があること。
5. HA プライマリ CAM が、実行時の操作のために、完全に設定されること。 これは、認証ソース、ポリシー、ユーザ ロール、アクセス ポイントなどへの接続が、すべて指定されるこ

とを意味します。 この設定は、HA セカンダリ（スタンバイ）CAM で自動的に複製されます。
6. 両方の Clean Access Manager が、ネットワーク上でアクセス可能であること（両方に ping を送信し、接続をテストします）。
7. CAM ソフトウェアがインストールされているマシンに、イーサネットの空きポート（eth1）および 1 つの空きシリアル ポートがあること。 サーバ ハードウェアの仕様マニュアルを使用して、各マシンのシリアル ポート（ttyS0 または ttyS1）を識別します。
8. アウトオブバンドの導入では、CAS および CAM が接続されるスイッチ インターフェイスでは、ポート セキュリティがイネーブルではないこと。 これは、CAS HA および DHCP の配信と干渉する場合があります。

これらの手順では、Clean Access Manager のリブートが必要になります。 その時点で、サービスが一時的に使用できなくなります。 ダウンタイムによって影響を受けるユーザがほとんどいないタイミングで、オンライン CAM を設定します。

注: Cisco NAC アプライアンス Web 管理コンソールでは、Internet Explorer 6.0 またはそれ以上のブラウザがサポートされます。

Clean Access Manager マシンの接続

HA-CAM ピア間には、次の 2 つのタイプの接続があります。 1 つでは、Clean Access Manager アクティビティに関連する実行時データがやり取りされ、1 つでは、ハートビート信号がやり取りされます。 ハイ アベイラビリティでは、Clean Access Manager によって、データのやり取りとハートビート UDP のやり取りの両方で、常に eth1 インターフェイスが使用されます。 一定の時間内に送受信する UDP ハートビート信号に障害が発生すると、スタンバイ システムに制御が渡されます。 さらにセキュリティを追加するには、Clean Access Manager ピア間でシリアル ハートビート接続を追加することを強く推奨します。 シリアル接続によって、追加の専用ハートビートをやり取りする方法に障害が発生してから、スタンバイ システムに制御を渡すことができます。 CAM ピア間の eth1 接続は、必須であることに注意してください。

ピア Clean Access Manager を次のように接続します。

- クロス ケーブルを使用して、Clean Access Manager マシンの eth1 イーサネット ポートを接続します。 この接続は、フェールオーバー ピア間での、ハートビート UDP インターフェイスとデータのやり取り（データベース ミラー機能）に使用されます。
- ヌル モデム シリアル ケーブルを使用して、シリアル ポートを接続します（強く推奨）。 この接続は、フェールオーバー ピア間の追加のハートビート シリアルのやり取り（キープアライブ）に使用されます。

注: HA のシリアル ケーブル接続（HA-CAM または HA-CAS のいずれか）では、シリアル ケーブルは「ヌル モデル」ケーブルである必要があります。

シリアル接続

Clean Access Manager ソフトウェアが実行されるマシンに、2 つのシリアル ポートがある場合、追加のシリアル ハートビート接続に追加のポートを使用できます。 デフォルトでは、CAM サーバで検出される最初のシリアル ポートは、コンソールの入出力に設定されます（インストールやその他のタイプの管理アクセスに活用）。

マシンに 1 つのシリアル ポートのみ（COM1 または ttyS0）がある場合、ハイ アベイラビリティ ハートビート接続の役割を果たすよう、ポートを再設定できます。 これは、CAM ソフトウェア

のインストール後に、SSH または KVM コンソールを常に使用して、CAM のコマンド ライン インターフェイスにアクセスできるためです。

HA CAM 設定の [Disable Serial Login] チェックボックスでシリアル ポートをイネーブルまたはディセーブルにできます（ [Administration] > [Clean Access Manager] > [Network & Failover | **Failover Settings** | Disable Serial Login] ）。 CAM マシンにシリアル ポートが 1 つのみの場合、管理者は、このチェックボックスを使用して、HA-Clean Access Manager のペアのハートビート シリアル インターフェイスとして使用できるよう、COM1 のシリアル ログインをディセーブルにできます。

注: CAM では、シリアル ログインは、デフォルトで**イネーブル**にされています。 CAM のハートビート シリアル インターフェイスとして COM1 を使用する場合、[Disable Serial Login] チェックボックスをクリックし、COM1 へのシリアル ログインをディセーブルにする必要があります。

HA プライマリ CAM の設定

前提条件を確認したら、次の手順を実行し、ハイ アベイラビリティ ペアの HA プライマリとして Clean Access Manager を設定します。 設定例については、図を参照してください。

1. HA プライマリとして指定するために、Clean Access Manager の Web 管理コンソールを開き、[Administration] > [CCA Manager] > [SSL Certificate] にアクセスして、プライマリ CAM の SSL 証明書を設定します。 [Generate Temporary Certificate] フォームが表示されます。 **注:** このドキュメントの HA 設定手順では、HA プライマリ CAM から HA セカンダリ CAM へ一時証明書がエクスポートされることを前提としています。*HA ペアの一時証明書を使用する場合は、次の手順を実行します。*[Generate Temporary Certificate] フォームに入力し、[Generate] をクリックします。 証明書は、HA ペアのドメイン名に対して、生成する必要があります。一時証明書の生成後、[Choose an action] メニューから [Export CSR/Private Key/Certificate] を選択します。[Currently Installed Private Key] の [Export] ボタンをクリックし、SSL プライベート キーをエクスポートします。 キー ファイルをディスクに保存します。 後ほど、このキーを HA セカンダリ CAM にインポートする必要があります。 [Currently Installed Certificate] の [Export] ボタンをクリックし、現在の SSL 証明書をエクスポートします。 証明書ファイルをディスクに保存します。 後ほど、この証明書を HA セカンダリ CAM にインポートする必要があります。*HA ペアの CA 署名付き証明書を使用する場合は、次の手順を実行します。***注:** CA 署名付きの証明書は、DNS を介してサービス IP に解決可能なドメイン名に基づく必要があります。 詳細については、『Cisco NAC アプライアンス：CAM インストレーション アドミニスト レーション ガイド』の「管理」セクションにある「CAM SSL 証明書の管理」を参照してください。[Choose an action] メニューから [Import Certificate] を選択します。[Certificate File] フィールドの横にある [Browse] ボタンを使用して、CA 署名付きの証明書に移動します。[File Type] ドロップダウン メニューから [CA-signed PEM-encoded X.509 Cert] を選択します。[Upload] をクリックし、証明書をインポートします。 後ほど、この証明書を HA セカンダリ CAM にインポートする必要があることに注意してください。[Verify and Install Uploaded Certificates] をクリックします。 [Choose an action] ドロップダウン リストから [Export CSR/Private Key/Certificate] を選択します。[Currently Installed Private Key] の [Export] ボタンをクリックし、CA 署名付き証明書に関連付けられている SSL プライベート キーをエクスポートします。 キー ファイルをディスクに保存します。 後ほど、このファイルを HA セカンダリ CAM にインポートする必要があります。
2. [Administration] > [CCA Manager] に進み、[Network & Failover] タブをクリックします。 [High-Availability Mode] ドロップダウン メニューから [HA-Primary] オプションを選択しま

す。 ハイ アベイラビリティの設定が表示されます。
3. [Network Settings] にある [IP Address] フィールドから値をコピーし、[Service IP Address] フィールドに入力します。 ネットワーク設定 IP アドレスは、現在の Clean Access Manager に存在する IP アドレスです。 Clean Access Server ですでに認識されているこの IP アドレスが、Clean Access Manager の仮想 IP アドレスに変換されます。
4. [Network Settings] の IP アドレスを、たとえば n.152 などの使用可能なアドレスに変更します。
5. 各 Clean Access Manager には、camanager1 や camanager2 などの固有のホスト名が必要です。 [Network Settings] の [Host Name] フィールドに、HA プライマリ CAM のホスト名を入力し、[Failover Settings] の [Peer Host Name] フィールドに、HA セカンダリ CAM のホスト名を入力します。ハイ アベイラビリティを設定するときには、[Host Name] の値は必須で、[Host Domain] の名前はオプションです。[Host Name] フィールドと [Peer Host Name] フィールドでは、大文字と小文字が区別されます。 ここに入力する値が、後ほど HA セカンダリ CAM に入力する値に一致するようにしてください。
6. [Heartbeat Serial Interface] ドロップダウン メニューから、HA プライマリ CAM のシリアル ケーブルに接続したシリアル ポートを選択するか、または、シリアル接続を使用しない場合は、[n/a] のままにします。
7. 使用しているマシンにあるシリアル ポートが 1 つのみで、ハートビート シリアル インターフェイスとして COM1 を使用する場合、[Disable Serial Login] チェックボックスをオンにし、COM1 でシリアル ログインをディセーブルにする必要があります。 詳細は、「シリアル接続」を参照してください。
8. 同期を管理するために、Clean Access Manager ピアでは、クロスオーバー ネットワークによってデータをやり取りします。 [Crossover Network] フィールドに、10.10.10 などの、組織内で現在ルーティングされていないプライベート ネットワーク領域を指定する必要があります。 提示されるデフォルト クロスオーバー ネットワークは 192.168.0.252 です。 このアドレスが使用しているネットワークで矛盾を生じさせる場合には、異なるプライベート アドレス領域を指定するようにしてください。 たとえば、組織内でプライベート ネットワーク 192.168.151.0 を使用している場合は、クロスオーバー ネットワークとして 10.1.1.x を使用します。 サブネット マスクと IP アドレスの最後のオクテットは固定ですので、IP アドレスのネットワーク部分のみを [Crossover Network] フィールドに入力します。
9. [Update] をクリックし、次に [Reboot] をクリックして、Clean Access Manager を再起動します。Clean Access Manager の再起動後、CAM マシンが適切に動作していることを確認してください。 Clean Access Server が接続され、新規ユーザが認証されているかどうかを確認します。

HA セカンダリ CAM の設定

HA セカンダリ CAM を設定するには、次の手順を実行します。

1. HA プライマリとして指定するために、Clean Access Manager の Web 管理コンソールを開き、[Administration] > [CCA Manager] > [SSL Certificate] にアクセスします。
2. 次に進む前に、次の手順を実行します。セカンダリ CAM のプライベート キーをバックアップします。サービス IP/HA プライマリ CAM に関連付けられているプライベート キーおよび SSL 証明書ファイルが使用可能であることを確認してください（「HA プライマリ CAM の設定」で説明したように、前にエクスポート済み）。
3. 次の手順で、HA プライマリ CAM のプライベート キー ファイルおよび証明書をインポートします。[SSL Certificate] タブで、[Choose an action] メニューから [Import Certificate] を選

択します。[Certificate File] フィールドの横にある [Browse] をクリックし、HA ペアで使用されている証明書で生成されたプライベート キー ファイルのバックアップ コピーを表示します。[File Type] として [Private Key] を選択します。[Upload] をクリックし、プライベート キーをアップロードします。[Choose an action] メニューから選択した [Import Certificate] で、プライベート キーに関連付けられている（一時または CA 署名済みの）証明書を表示します。[File Type] として [CA-signed PEM-encoded X.509 Cert] を選択します。[Upload] をクリックし、一時証明書または CA 署名付き証明書をアップロードします。[Verify and Install Uploaded Certificates] をクリックします。詳細については、『Cisco NAC アプライアンス：CAM インストレーション アドミニスト レーション ガイド』の「管理」セクションにある「CAM SSL 証明書の管理」を参照してください。

4. [Administration] > [CCA Manager] > [Network & Failover] | [Network Settings] に進み、セカンダリ CAM の IP アドレスを、HA プライマリ CA IP アドレスともサービス IP アドレスとも異なるアドレスに変更します。
5. [Network Settings] にある [Host Name] の値を、HA プライマリ CAM 設定の [Peer Host Name] に設定されている値と同じ値に設定します。 HA プライマリ セクションの図を参照してください。**注:** [Host Name] フィールドと [Peer Host Name] フィールドでは、大文字と小文字が区別されます。 ここに入力する値が、後ほど HA プライマリ CAM に入力した値に一致するようにしてください。
6. [High-Availability Mode] ドロップダウン メニューから [HA-Secondary] を選択します。 ハイアベイラビリティの設定が表示されます。
7. [Failover Settings] にある [Service IP Address] の値を、HA プライマリ CAM 設定の [Service IP Address] に設定されている値と同じ値に設定します。
8. [Failover Settings] にある [Peer Host Name] の値を、HA プライマリ CAM のホスト名に設定します。
9. [Heartbeat Serial Interface] ドロップダウン メニューから、HA プライマリ CAM のシリアル ケーブルに接続したシリアル ポートを選択するか、または、シリアル接続を使用しない場合は、[n/a] のままにします。
10. 使用しているマシンにあるシリアル ポートが 1 つのみで、ハートビート シリアル インターフェイスとして COM1 を使用する場合、[Disable Serial Login] チェックボックスをオンにし、COM1 でシリアル ログインをディセーブルにする必要があります。 詳細は、「シリアル接続」を参照してください。
11. HA プライマリ CA に入力した設定と同じ設定を、[Crossover Network Interface Setting] に入力します。
12. [Update] をクリックし、次に [Reboot] をクリックします。

スタンバイ CAM の起動時に、スタンバイのデータベースとアクティブな CAM とが自動的に同期されます。

最後に、スタンバイの管理コンソールを再度開き、設定を完了します。 スタンバイの管理コンソールには、1 つの管理モジュールのみがあることに、注意してください。

設定の完了

スタンバイ CAM の [Network & Failover] ページの設定を確認します。

ハイ アベイラビリティの設定は以上で完了です。

HA-CAM ペアのフェールオーバー

警告： データベースの同期の際にデータが損失する可能性を防ぐためには、アクティブな CAM がフェールオーバーする前に、スタンバイ CAM が常に実稼働状態である必要があります。

HA-CAM ペアをフェールオーバーするためには、ペアのアクティブ マシンへの SSH で、次のコマンドのいずれかを実行します。

- **shutdown** または
- **reboot** または
- **service perfigo stop**これによって、アクティブ マシン上のすべてのサービスが停止されます。 ハートビートに障害が発生した場合には、スタンバイ マシンがアクティブの役割を担います。 **service perfigo start** を実行し、停止されたマシンのサービスを再起動します。 これにより、停止されたマシンがスタンバイの役割を担うことになります。**注: service perfigo restart** は、ハイ アベイラビリティ（フェースオーバー）のテストには使用しないでください。 代わりに、シスコでは、マシン上で **shutdown** または **reboot** を使用するか、CLI コマンド **service perfigo stop** および **service perfigo start** を使用して、フェールオーバーをテストすることを推奨します。

HA で役に立つ CLI コマンド

CAM で HA を使用する場合に役に立つディレクトリは、次のとおりです。

- `/etc/ha.d/perfigo/conf`
- `/etc/ha.d/ha.cf`

次に、HA デバッグ/ログ ファイルの場所、および、HA ペアの各 CAM（ノード）の名前を示します。

```
[root@cam1  ha.d]#more ha.cf # Generated by make-hacf.pl udpport 694 bcast eth1 auto_failback
off apiauth default uid=root log_badpack false debug 0 debugfile /var/log/ha-debug logfile
/var/log/ha-log #logfacility local0 watchdog /dev/watchdog keepalive 2 warntime 10 deadtime 15
node cam1 node cam2
```

HA CAM でアクティブ/スタンバイの実行時ステータスを確認する方法

次に、CLI を使用して、HA ペアの各 CAM の実行時ステータス（アクティブまたはスタンバイ）を特定する方法を示します。 通常は、最後のアップグレードの /store ディレクトリから、/store/cca_upgrade-4.x.x. などの **fostate.sh** コマンドを見つけることができます。

1. 最初の CAM で **fostate.sh** スクリプトを実行します。`[root@cam1  cca_upgrade-4.x.x]# ./fostate.sh`
   My node is active, peer node is standby `[root@cam1 cca_upgrade-4.x.x]#` *`!--- This CAM is the active CAM in the HA-pair`*
2. 2 番目の CAM で **fostate.sh** スクリプトを実行します。`root@cam2  cca_upgrade-4.x.x]# ./fostate.sh`
   My node is standby, peer node is active `[root@cam2 cca_upgrade-4.x.x]#` *`!--- This CAM is the standby CAM in the HA-pair`*

HA CAM でプライマリ/セカンダリの設定ステータスを確認する方法

次に、CLI を使用して、HA ペアで最初に設定された各 CAM の HA モード（プライマリ/セカンダリ）を特定する方法を示します。

1. /etc/ha.d/ha.cf. で、CAM（ノード）の名前を見つけます。

2. たとえば次のように、各 CAM のステータスを確認します。`[root@cam1 ~]# /perfigo/control/bin/check-ha cam1`
   ```
   active
   [root@cam1 ~]# /perfigo/control/bin/check-ha cam2
   active
   ```
3. /perfigo/control/tomcat and perform ls -la に進みます。webapps が **normal-webapps** を指している場合、それがプライマリ CAM です。webapps が **admin-webapps** を指している場合、それがセカンダリ CAM です。たとえば、次の CAM は、プライマリ CAM です。
   ```
   [root@cam1 tomcat]# cd /perfigo/control/tomcat
   [root@cam1 tomcat]# ls -la
   total 216
   drwxr-xr-x12 root root4096 Sep 14 23:28 .
   drwxr-xr-x8 root root4096 Aug 28 22:12 ..
   drwxr-xr-x4 root root4096 Aug 28 22:12 admin-webapps
   <output cut…..>
   drwxr-xr-x2 root root4096 Aug 28 22:12 temp
   lrwxrwxrwx1 root root38 Sep 14 23:28 webapps -> /perfigo/control/tomcat/normal-
   webapps drwxr-xr-x 3 root root 4096 Aug 28 15:15 work
   ```
   次の CAM は、セカンダリ CAM です。
   ```
   [root@cam2 tomcat]# ls -la
   total 216
   drwxr-xr-x12 root root4096 Sep 14 23:33 .
   drwxr-xr-x8 root root4096 Sep 152006 ..
   drwxr-xr-x4 root root4096 Sep 152006 admin-webapps
   <output cut …>
   drwxr-xr-x2 root root4096 Sep 152006 temp
   lrwxrwxrwx1 root root37 Sep 14 23:33 webapps -> /perfigo/control/tomcat/admin-webapps
   drwxr-xr-x 3 root root 4096 Sep 14 23:25 work
   ```

トラブルシューティング

問題 1

HA ペアのセカンダリ CAS がアクティブになるときに、CAM の「**SSKEY on server doesn't match the value in database**」エラーが発生する。

解決策

プライマリ CAS SSKEY を手動でセカンダリにプッシュして、この問題を解決します（SSKEY ボタンをリセットするか、CAS で /etc/.GUSSK ファイルを手動で上書きします）。 この問題は、通常、アプライアンスを置き換えるときに、CAM から削除しなかった場合か、CAM に再追加しなかった場合に発生します。 この場合、CAS には、その MAC アドレスに基づいた SSKEY があるか、または、CAM に前に設定されていたものと一致しなかった可能性があります。 セカンダリ CAS には、その MAC アドレスに基づいた SSKEY があるため、これは、セカンダリ CAS の場合に発生することがあります。 HA の設定で、セカンダリでも、プライマリ CAS MAC に基づいたプライマリ CAS SSKEY を使用する必要があります。

問題 2

フェールオーバー CAM ペアで、プライマリ CAM によって、「WARNING! `Closed connections to peer [x.x.x.x](standby IP Address) database! !!` というエラー メッセージが表示されます。

解決策

プライマリ eth1 リンクの接続が解除され、シリアル リンクのみが残っているときに、対応する HA と同期がとれないことを示すデータベース エラーが、CAM によって返され、管理者は、このエラーを CAM Web コンソールで確認できます。 を探します。

```
WARNING! Closed connections to peer [standby
 IP] database! Please restart peer node to bring databases in
 sync!!
```

この問題を解決するには、自己署名証明書またはサード パーティ証明書を CAM で使用します。

問題 3

CAM でハイ アベイラビリティの IP アドレスを変更するには、どのようにするか。

解決策

service perfigo stop で、セカンダリ CAM をダウンさせます。 この方法では、perfigo サービスは実行されませんが、依然、SSH によってアクセスできます。 プライマリ CAM 上で、[Administration] > [CCA Manager] > [Network] を使用して、IP を変更します。 ここでは、まだ、リブートしないでください。 [Failover] タブを表示し、サービス IP アドレスを変更します。 この手順の後で、リブートします。

完全にアップされたら、到達可能であることを確認します。 次に、セカンダリ CAM で **service perfigo start** を実行し、プライマリで行った変更と同じ変更を行います。 ここでリブートすると、セカンダリとしてアップされます。 SSL 証明書が名前に対して発行された場合、名前が新しいサービス IP に解決されるよう、DNS エントリを変更します。 IP に対して発行された場合、新しい一時証明書が再生成されます。 ここで、テスト ユーザでログインしてみます。 正常にログインしたら、セカンダリにフェールオーバーし、ユーザがログインできるようにします。

関連情報

- Cisco NAC アプライアンスに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems