

# Cisco TelePresence VCS クラスターの作成およびメンテナンス導入ガイド

導入ガイド

初版：2009年12月

最終更新日：2015年11月

Cisco VCS X8.7

Cisco TMS 13.2 以降

## はじめに

Cisco TelePresence Video Communication Server (VCS) クラスタは、Cisco VCS インストールの復元力および容量を拡張するように設計されています。クラスタ内の VCS ピアは、帯域幅およびルーティング、ゾーン、FindMe™ などのその他の設定を共有します。エンドポイントは、クラスタの任意のペアに登録できます。エンドポイントは、初期ピアとの接続を失っても、クラスタの別のピアに再登録できます。

コールのライセンスは、クラスタごとに実行されます。クラスタ ピアにインストールされたコールのライセンスは、クラスタ内の任意のピアで使用できます。クラスタ ピアが使用できなくなった場合は、そのピアにインストールされたコールのライセンスは、ピアへの接続をクラスタが失った時から 2 週間の期間中、残りのクラスタ ピアにそのまま使用できます。これにより、クラスタの全体的なライセンス キャパシティが維持されます。ただし、各ピアはその物理キャパシティによって制限されることに注意してください。

クラスタのすべての VCS ピアのルーティング キャパシティは同じである必要があります。VCS がコールを宛先にルーティングできる場合、そのクラスタのすべての VCS ピアが、コールをその宛先にルーティングできると見なされます。ルーティングが VCS ピア間で異なる場合、個別の VCS/VCS クラスタを使用する必要があります。

このガイドでは、VCS クラスタを作成および保守する方法について説明します。次の情報を提供します。

- [X7.1 \(またはそれ以降の\) クラスタの X8.7 へのアップグレード \(6 ページ\)](#)
- [VCS ピアの新規クラスタの作成 \(11 ページ\)](#)
- [クラスタへのピアの追加 \(16 ページ\)](#)
- [ピア固有の項目 \(23 ページ\)](#)
- [クラスタからのライブ ピアの完全な削除 \(27 ページ\)](#)
- [クラスタからのデッド ピアの完全な削除 \(29 ページ\)](#)
- [クラスタの解体 \(31 ページ\)](#)
- [プライマリ ピアの変更 \(34 ページ\)](#)
- [ピアの IP アドレスの変更 \(36 ページ\)](#)
- [ピアの置換 \(37 ページ\)](#)

Cisco TMS は、FindMe 設定が Cisco TMS から行われる場合、およびエンドポイントがプロビジョニングされる場合に必要です。クラスタの設定には Cisco TMS は不要で、FindMe は必要に応じ VCS クラスタを使ってローカルで設定できます (FindMe を VCS クラスタ上にローカルで保存し、ソースとして Cisco TMS を使用しない場合、後にその FindMe 情報を Cisco TMS に移動することはできません)。

プロビジョニングの有効化とクラスタの作成は、それぞれ異なるプロセスです。クラスタでプロビジョニングを有効にする場合、次のいずれかの手順を実行します。

- 本ガイドの手順に従い（プロビジョニングを有効化せずに）VCS のクラスタを作成し、続いて『*Cisco TMS Provisioning Extension Deployment Guide*』の手順に従ってクラスタ全体のプロビジョニングを有効化します、または
- 『*Cisco TMS Provisioning Extension Deployment Guide*』の手順に従ってプライマリ VCS となるアイテムのプロビジョニングを有効化し、続いて本ガイドの手順に従って VSC のクラスタを作成します

X8 以降の VCS は、Cisco TMS Provisioning Extension モードのみをサポートしています。

TMS Agent レガシー モード プロビジョニングの詳細、またはこれ以前のバージョンのソフトウェア上で実行可能なクラスタの作成、変更、トラブルシューティングについては、本導入ガイドの旧バージョンを参照してください。また、これらのクラスタの X8.7 へのアップグレードに関する詳細は、「[付録 8：VCS の旧バージョンから X8.7 へのアップグレード \(60 ページ\)](#)」を参照してください。

## 前提条件

X8.7 VCS ピアのクラスタを設定する前、または X8.7 VCS をクラスタに追加する前に、次のことを確認します。

### プラットフォームとソフトウェアバージョンが一致している

- すべてのクラスタのピアが同じバージョンのコードを実行している。異なるピアが異なるバージョンのコードを実行できる唯一の機会、クラスタが分割された方法で動作する間に、クラスタが 1 つのバージョンのコードから他のバージョンのコードへアップグレードされる間です。
- 各ピアは、同等の機能のハードウェア プラットフォーム（アプライアンスまたは仮想マシン）を使用している。たとえば、2 コア ミディアム VM で実行されているピアを使用する標準のアプライアンスで実行されているピアをクラスタ化することはできますが、8 コアの大型 VM で実行されているピアを使用する標準のアプライアンスで実行されているピアをクラスタ化することはできません。

### ネットワーク条件を満たしている

- 異なる LAN 設定（有効な異なる IPv4 アドレスと異なる IPv6 アドレス）が各ピアで設定されている。
- クラスタの各ピアは、クラスタ内またはクラスタに追加されるすべての VCS から 15 ms ホップ（ラウンドトリップ遅延 30 ms）以内にある。
- クラスタの各ピアはクラスタ内またはクラスタに追加されるすべての VCS に直接ルーティングできる。（クラスタ ピア間の NAT は許可されず、ファイアウォールがある場合、必須ポートがオープンであることを確認します）

### 基本設定が済んでいる

- 各ピアで異なるシステム名を使用している。
- すべてのピアに、同じオプション キーのセットがインストールされている。
  - コール ライセンス キーの数はピアごとに異なる場合があります。この場合、他のすべてのライセンス キーは各ピアで同じでなければなりません。
  - オプション キーをインストールした場合、これらをアクティブにするには、VCS を再起動する必要があります。
- 各ピアで H.323 モードが有効になっている（**[設定 (Configuration)] > [プロトコル (Protocols)] > [H.323]** の順に選択し、**H.323 モード**で **[オン (On)]** を選択）。

クラスタは、ピア間の H.323 シグナリングを使って発信に最も適したルートを決めます。これは、すべてのエンドポイントが SIP でも同様です。

### DNS 設定が済んでいる

- VCS のピアが使用する DNS サーバは、Cisco TMS およびすべての VCS のピア アドレスの DNS フォワード ルックアップ（正引き）と DNS リバース ルックアップ（逆引き）の両方をサポートする必要があり、DNS サーバが、次に示すような、その他の必要とされる DNS の機能にもアドレス ルックアップを提供する必要があります。

- DNS 名を使用して設定した場合の NTP サーバまたは外部マネージャ
- Microsoft Lync サーバの FQDN ルックアップ
- LDAP サーバのフォワード ルックアップとリバース ルックアップ（リバース ルックアップは PRT レコードを介して提供されます）

**注：** DNS サーバの構成は複製されないため、ユーザはそれぞれのピアにおいて DNS サーバのアドレスを構成する必要があります。

- DNS SRV レコードはクラスタの各ピアの A または AAAA レコードを含むクラスタで使用できる。

この構成はビデオの相互運用性と企業間（B2B）ビデオ通話を行う場合推奨されますが、**モバイルおよびリモート アクセスに関しては必須ではありません。**

- （MRA）VSC Expressway クラスタ内の各ピアに対し、`collab-edge` SRV レコードを作成する
- （B2Bのみ）VCS Expressway クラスタに、すべてのクラスタ ピアを定義する DNS SRV レコードがある

#### TMS の（必要に応じた）設定が完了している

- Cisco TMSを使用している場合、13.2 以降のバージョンが実行されている（プロビジョニングまたは FindMe に Cisco TMS を使用していない場合は 12.6 以降を使用することも可能）。
- FindMe の複製および/またはデータのプロビジョニングに Cisco TMS を使用している場合は、Provisioning Extension モード機能（詳細は『[Cisco TMS Provisioning Extension Deployment Guide](#)』を参照）が有効化されていることを確認する。

## X7.1（またはそれ以降の）クラスタの X8.7 へのアップグレード

ここでは、既存の X7.1 以降のクラスタを X8.7 クラスタにアップグレードする方法について説明します。

アップグレード ウィンドウを選択し、以下を行います。

- ロー アクティビティ期間を選択する。
- 同じウィンドウ内にあるすべてのピアがアップグレードするまで待つ。クラスタは、ソフトウェア バージョンがすべてのピアで一致するまで正しく再形成されることはありません

### 前提条件

デバイスのプロビジョニングまたは FindMe 用に Cisco TMS を使用している場合、この手順は以下を前提としています。

- Cisco TMS がバージョン 13.2 以降のソフトウェアを実行しており、X7.1 以降のクラスタで稼働する。
- VCS クラスタおよび Cisco TMS が、Cisco TMS Provisioning Extension モードを使用して設定され、また稼働している。Provisioning Extension モードで稼働していない場合、このアップグレード手順を実行する前に、『Cisco TelePresence Management Suite Provisioning Extension Deployment Guide』の手順に従い、Provisioning Extension モードにアップグレードする必要があります。

各 VCS ピアで（プライマリを含む）、**[アラーム (Alarms)]** ページ (**[ステータス (Status)]** > **[アラーム (Alarms)]**) を確認し、すべてのアラームが機能し、クリアされていることを確認します。

## VCS クラスタ ピアの X8.7 へのアップグレード

**注：**サービスの継続性を保持することに加えて、設定データ消失のリスクを回避するために、ここで指定された順序でアップグレード手順に従うことが重要です。推奨事項を次にまとめます。

1. 初めにプライマリ ピアをアップグレードし再起動します。
2. 他の下位のピアをアップグレードしてから、ピアを 1 つずつ再起動します。

詳細な手順は、次のとおりです。

### プライマリ ピアのアップグレード

1. Web インターフェイスで管理者としてプライマリ ピアにログインします。
2. VCS をバックアップします (**[メンテナンス (Maintenance)]** > **[バックアップおよびリストア (Backup and restore)]**) 。

アップグレードする前に、システムをバックアップする必要があります。アップグレード後、前のバージョンにダウングレードする場合、設定を復元するには、過去のリリースに対し行ったバックアップを復元する必要があります。

### 3. メンテナンス モードを有効にします。

1. 管理者として VCS にログインします (SSH またはシリアル)。

2. コマンド プロンプトで、次のように入力します。xConfiguration SystemUnit Maintenance Mode: On

X8.1 以降のバージョンでは、Web インターフェイスを通じてメンテナンス モードを有効化できます ([メンテナンス (Maintenance)] > [メンテナンス モード (Maintenance mode)])。

これにより、プライマリ ピアで、新規コールが処理されなくなります (既存のコールは、再起動する場合のみドロップされ、他のクラスタ ピアでは引き続きコールが処理されます)。

### 4. このピアですべてのコールがクリアされ、登録がタイムアウトになるまで待機します。

- 必要な場合、自動的にクリアされないコールをこのピアから手動で削除します (Web ブラウザを使用し、[ステータス (Status)] > [コール (Calls)] に移動して、終了するコールの横のチェックボックスをオンにして、[切断 (Disconnect)] をクリックします)。

- 必要な場合、自動的にクリアされない登録をこのピアから手動で削除します (Web ブラウザを使用し、[ステータス (Status)] > [登録 (Registrations)] > [デバイスごと (By device)] に移動して、削除するデバイスの横のチェックボックスをオンにして、[登録解除 (Unregister)] をクリックします)。

Conference Factory の登録はそのままにしておいて構いません。これはコールのソースではなく、また他のピアが各自の Conference Factory 登録を所有しているため (有効化されている場合)、これを削除しても別のピアにロールオーバーされることはありません。

### 5. プライマリ VCS をアップグレードして再起動します ([メンテナンス (Maintenance)] > [アップグレード (Upgrade)])。

詳細については、『VCS Administrator Guide』の「Upgrading Software」のセクションを参照してください。

経過表示バーが終了を示した後に、Web ブラウザ インターフェイスが再起動プロセス中にタイムアウトする可能性があることに注意してください。これは VCS が約 30 回の再起動ごとに実行されるディスクのファイル システム チェックを行う場合、または過去 6 カ月にディスクのファイル システム チェックが実行されていない場合に発生する可能性があります。

これで、プライマリ VCS でのソフトウェアのアップグレードは完了しました。

## クラスタ関連のアラーム

アップグレード プロセス中に発生するクラスタ関連のアラームを無視できます。たとえば、

- プライマリまたは任意の下位ピアでの「クラスタ通信障害 (Cluster communication failure)」アラーム (これは予期されるアラームです)。
- 「クラスタ複製エラー: マスターまたはこのスレーブのピアの設定ファイルが見つかりません。設定を手動で同期化する必要があります (Cluster replication error: cannot find master or this slave's peer configuration file, manual synchronization of configuration is required)」

同様に、このアップグレード中にクラスタ問題に関して作成される Cisco TMS の警告および電子メールも無視できます。これらのアラームおよび警告は予期されているもので、すべてのクラスタ ピアがアップグレードされ、クラスタ データの同期が発生するとクリアされます（アップグレード完了後 10 分以内にクリアされます）。

**プライマリ VCS ピアで、次の手順を実行します。**

1. 正しい構成データがあることを確認します。
  - FindMe を使用している場合は、正しい FindMe エントリが存在することを確認します（[ステータス (Status) ] > [アプリケーション (Applications) ] > [TMS Provisioning Extension サービス (TMS Provisioning Extension Services) ] > [FindMe] > [アカウント (Accounts) ] ）。
  - [システム (System) ] および [設定 (Configuration) ]、[アプリケーション (Application) ] メニューで、各項目の構成を確認します。
2. VCS をバックアップします（[メンテナンス (Maintenance) ] > [バックアップおよびリストア (Backup and restore) ] ）。

**注：**VCS ピアが別のバージョンのコードで実行している場合は、アップグレードに必要な箇所以外は変更を加えないください。クラスタは、プライマリ VCS とは異なるバージョンの VCS 上にあるピアに対しては、変更を複製しません。

## 下位ピアのアップグレード

アップグレード プロセス中に発生するクラスタの関連アラームを無視できます（これらは予期されています）。

1. Web インターフェイスで管理者として下位ピアにログインします。
2. VCS をバックアップします（[メンテナンス (Maintenance) ] > [バックアップおよびリストア (Backup and restore) ] ）。

アップグレードする前に、システムをバックアップする必要があります。アップグレード後、前のバージョンにダウングレードする場合、設定を復元するには、過去のリリースに対し行ったバックアップを復元する必要があります。

3. メンテナンス モードを有効にします。
  1. 管理者として VCS にログインします（SSH またはシリアル）。
  2. コマンド プロンプトで、次のように入力します。 `xConfiguration SystemUnit Maintenance Mode: On`

X8.1 以降のバージョンでは、Web インターフェイスを通じてメンテナンス モードを有効化できます（[メンテナンス (Maintenance) ] > [メンテナンス モード (Maintenance mode) ] ）。
4. このピアですべてのコールがクリアされ、登録がタイムアウトになるまで待機します。
  - 必要な場合、自動的にクリアされないコールをこのピアから手で削除します（Web ブラウザを使用し、[ステータス (Status) ] > [コール (Calls) ] に移動して、終了するコールの横のチェックボックスをオンにして、[切断 (Disconnect) ] をクリックします）。



- 必要な場合、自動的にクリアされない登録をこのピアから手動で削除します（Web ブラウザを使用し、**[ステータス (Status)] > [登録 (Registrations)] > [デバイスごと (By device)]** に移動して、削除するデバイスの横のチェックボックスをオンにして、**[登録解除 (Unregister)]** をクリックします）。

Conference Factory の登録はそのままにしておいて構いません。これはコールのソースではなく、また他のピアが各自の Conference Factory 登録を所有しているため（有効化されている場合）、これを削除しても別のピアにロールオーバーされることはありません。

5. VCS をアップグレードして再起動します（**[メンテナンス (Maintenance)] > [アップグレード (Upgrade)]**）。

複数のピアを再起動する必要がある場合、次のピアを再起動する前に Web インターフェイスからピアにアクセスできることを確認してから、各ピアを再起動します。

詳細については、『*VCS Administrator Guide*』の「Upgrading Software」のセクションを参照してください。

経過表示バーが終了を示した後に、Web ブラウザ インターフェイスが再起動プロセス中にタイムアウトする可能性があることに注意してください。これは VCS が約 30 回の再起動ごとに実行されるディスクのファイル システム チェックを行う場合、または過去 6 ヶ月にディスクのファイル システム チェックが実行されていない場合に発生する可能性があります。

これで、下位の VCS ピアでのソフトウェアのアップグレードは完了しました。

### クラスタ関連のアラーム

アップグレード プロセス中に発生するクラスタ関連のアラームを無視できます。たとえば、

- プライマリまたは任意の下位ピアでの「クラスタ通信障害 (Cluster communication failure)」アラーム（これは予期されるアラームです）。
- 「クラスタ複製エラー：マスターまたはこのスレーブのピアの設定ファイルが見つかりません。設定を手動で同期化する必要があります (Cluster replication error: cannot find master or this slave's peer configuration file, manual synchronization of configuration is required)」

同様に、このアップグレード中にクラスタ問題に関して作成される Cisco TMS の警告および電子メールも無視できます。これらのアラームおよび警告は予期されているもので、すべてのクラスタ ピアがアップグレードされ、クラスタ データの同期が発生するとクリアされます（アップグレード完了後 10 分以内にクリアされます）。

下位の VCS ピアで、次の手順を実行します。

1. **[ステータス (Status)] > [アラーム (Alarms)]** に移動し、すべてのアラームが機能し、クリアされていることを確認します。
2. 正しい構成データがあることを確認します。
  - FindMe を使用している場合は、正しい FindMe エントリが存在することを確認します（**[ステータス (Status)] > [アプリケーション (Applications)] > [TMS Provisioning Extension サービス (TMS Provisioning Extension Services)] > [FindMe] > [アカウント (Accounts)]**）。

- [システム (System) ] および [設定 (Configuration) ]、[アプリケーション (Application) ]メニューで、各項目の構成を確認します。
3. 各下位ピアでこの手順を繰り返します。

## クラスター ステータスの確認

この手順は、すべてのピアのアップグレードが完了した後に行ってください。

各 VCS (プライマリを含む) で、[システム (System) ]>[クラスタリング (Clustering) ]に移動し、クラスター データベースのステータス レポートが [アクティブ (Active) ]であることを確認します。

これで、X7.1 以降のクラスターから X8.7 クラスターへのアップグレードは完了しました。

## VCS ピアの新規クラスタの作成

**注：**この手順では VCS サービスのダウンタイム期間が必要です。これらの手順は、計画されているメンテナンス期間中に実行してください。

デバイス プロビジョニングを X8.7 VCS クラスタで使用する場合、Cisco TMS を使用する必要があります。また、FindMe を Cisco TMS で管理する場合も、Cisco TMS を使用する必要があります。デバイス プロビジョニングも FindMe も Cisco TMS で管理しない場合、Cisco TMS を使用する必要はありませんが、使用することをお勧めします。

### プロセスの概要

このプロセスでは、1 つの VCS のクラスタを開始します。クラスタがすでにある場合は、このプロセスを使用しないでください。

複数の VCS を含むクラスタを終了するには、このセクションが完了した際、「[クラスタへのピアの追加 \(16 ページ\)](#)」の手順に従ってクラスタに下位ピアを追加してください。

### 前提条件

- Cisco TMSを使用している場合、13.2 以降のバージョンが実行されている（プロビジョニングまたは FindMe に Cisco TMS を使用していない場合は 12.6 以降を使用することも可能）。
- デバイス プロビジョニングまたは FindMe を Cisco TMS で管理する場合、この VCS および Cisco TMS は、Provisioning Extension モードで稼働する必要があります。このモードは、稼働することが証明されています。
- ファイアウォールがクラスタ ピア間に設定されている場合は、「[付録 2：IP ポートおよびプロトコル \(43 ページ\)](#)」に記載されているトラフィックを許可するよう設定する必要があります。
- クラスタに含まれるすべての VCS では、同じバージョン (X8.7) の VCS ソフトウェアを実行する必要があります。

### プライマリ ピアの設定

このプロセスでは、この新しいクラスタの最初の（プライマリ）ピアをセットアップします。後に追加される追加ピアについては「[クラスタへのピアの追加 \(16 ページ\)](#)」の手順を使用してください。

手順を実行する前に、プライマリ ピアに使用する VCS を決定する必要があります。プライマリ VCS は、クラスタのすべての VCS ピアの設定情報のソースとして使用されます。下位 VCS ピアの設定は、削除され、そのプライマリ VCS ピアの設定で置換されます。

**他の VCS で、次の手順を実行します。**

構成内の他の VCS に、クラスタリング ピアのリスト内にある VCS の IP アドレスが設定されていないことを確認します。

このプライマリ VCS で、次の手順を実行します。

1. VCS が X8.7 ソフトウェアを実行していることを確認します。
2. VCS をバックアップします ([メンテナンス (Maintenance)] > [バックアップおよびリストア (Backup and restore)] )。
3. Web インターフェイスを使用して、VCS が次の条件を満たしているかどうか、設定を確認してください。
  - 有効なイーサネット速度 ([システム (System)] > [ネットワーク インターフェイス (Network interfaces)] > [イーサネット (Ethernet)] ) が設定されている。
  - 有効な IP アドレスおよび IP ゲートウェイ ([システム (System)] > [ネットワーク インターフェイス (Network interfaces)] > [IP]) が設定されている。
  - クラスタのその他のすべてのピアにインストールされるオプション キーと同じオプション キー のセットがインストールされている ([メンテナンス (Maintenance)] > [オプション キー (Option keys)] )。  
コール ライセンス キーの数はピアごとに異なる場合があります。この場合、他のすべてのライセンス キーは各ピアで同じでなければならないことに注意してください。
  - 少なくとも 1 つの有効な DNS サーバが設定されている。また、非修飾 DNS 名が (NTP サーバなどで) 使用されている場合は、ドメイン名が正しく設定されている必要がある (非修飾の DNS 名には、これを FQDN にするため、サフィックスとしてドメイン名が追加されます ([システム (System)] > [DNS]) )。
  - 有効かつ稼働している NTP サーバが設定されている ([システム (System)] > [時間 (Time)] : [ステータス (Status)] セクションの [状態 (State)] が「同期 (Synchronized)」でなければなりません)。
  - ピアが設定されていない ([システム (System)] > [クラスタリング (Clustering)] : このページのすべてのピアおよび IP アドレスのフィールドが空白でなければなりません。入力されている場合、エントリを削除して、[保存 (Save)] をクリックします)。
  - H.323 モードが [オン (On)] に設定されている ([設定 (Configuration)] > [プロトコル (Protocols)] > [H.323]) 。
4. この VCS のリストに、ネイバー ゾーンまたはトラバーサル ゾーンの新しいクラスタのピアとする VCS が表示されていないことを確認します ([設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] で、各ネイバーおよびトラバーサル ゾーンを確認します) 。
5. [H.323 生存時間 (Time to live)] を、導入のサイズに適した値に設定します。60 (秒) といった低数値を割り当てると、VCS がアクセス不可能になった場合、エンドポイントが別のピアに迅速に登録されます ([設定 (Configuration)] > [プロトコル (Protocols)] > [H.323]) 。

**注：**登録生存時間を大きく削減すると、登録要求によりパフォーマンスに大きな影響を及ぼす VCS のフラッディングが発生するリスクが高まります。この影響の程度はエンドポイントの数に比例するため、発生頻度の低い迅速なフェイルオーバーの必要性和、良好なパフォーマンスの継続の必要性の間で均衡を図る必要があります。

6. [システム (System) ] > [DNS] に移動し、[システムのホスト名 (System host name) ] がこの VCS の DNS ホスト名であることを確認します (通常は、スペースを除き、[システム (System) ] > [管理 (Administration) ] の [システム名 (System name) ] と同じであり、クラスタの各 VCS に固有です)。正しく設定されていない場合は、適切に設定し、[保存 (Save) ] をクリックします。

注： <System host name>.<DNS domain name> = この VCS の FQDN であることに注意してください

7. [設定 (Configuration) ] > [コールルーティング (Call routing) ] に移動し、[コールシグナリングの最適化 (Call signaling optimization) ] を [オン (On) ] にします。
8. [保存 (Save) ] をクリックします。
9. メンテナンス モードを有効にします。
- 1.[メンテナンス (Maintenance) ] > [メンテナンスモード (Maintenance mode) ] に移動します。
  - 2.[メンテナンスモード (Maintenance mode) ] を [オン (On) ] に設定します。
  - 3.確認ダイアログ ボックスで [保存 (Save) ] をクリックし、[OK] をクリックします。
10. このピアですべてのコールがクリアされ、登録がタイムアウトになるまで待機します。
- 必要な場合、自動的にクリアされないコールをこのピアから手動で削除します (Web ブラウザを使用し、[ステータス (Status) ] > [コール (Calls) ] に移動して、終了するコールの横のチェックボックスをオンにして、[切断 (Disconnect) ] をクリックします)。
  - 必要な場合、自動的にクリアされない登録をこのピアから手動で削除します (Web ブラウザを使用し、[ステータス (Status) ] > [登録 (Registrations) ] > [デバイスごと (By device) ] に移動して、削除するデバイスの横のチェックボックスをオンにして、[登録解除 (Unregister) ] をクリックします)。
- Conference Factory の登録はそのままにしておいて構いません。これはコールのソースではなく、また他のピアが各自の Conference Factory 登録を所有しているため (有効化されている場合)、これを削除しても別のピアにロールオーバーされることはありません。
11. (MRA には該当しません)[システム (System) ] > [クラスタリング (Clustering) ] に移動し、[クラスタ名 (Cluster name) ] がこの VCS クラスタに対応する SRV レコードで使用されるルーティング可能な完全修飾ドメイン名であることを確認します。たとえば、cluster1.example.com などです (「[付録 3: クラスタ名と DNS SRV レコード \(45 ページ\)](#)」を参照してください)。
- [クラスタ名 (Cluster name) ] を必要に応じて変更します。
12. [保存 (Save) ] をクリックします。
13. 次のように、[クラスタリング (Clustering) ] ページでフィールドを設定します。

設定マスター (Configuration master)	1
クラスタ事前共有キー (Cluster pre-shared key)	パスワード (任意の文字) を入力します。
ピア 1 IP アドレス (Peer 1 IP address)	この (プライマリ ピア) VCS の IP アドレスに設定します。

注：VCS が高度なネットワークを使用する場合は、**[ピア IP アドレス (Peer IP address)]** に LAN 1 インターフェイスアドレスを指定する必要があります。また、このインターフェイスで NAT が無効にされている必要があります。

14. **[保存 (Save)]** をクリックします。  
**[ピア 1 IP アドレス (Peer 1 IP address)]** フィールドの右側に「このシステム (This system)」という文字が表示されます（ページ更新後に表示される場合もあります）。
15. VCS を再起動します (**[メンテナンス (Maintenance)]** ) > **[再起動オプション (Restart options)]** に移動し、**[再起動 (Restart)]** をクリックし、**[OK]** をクリックします）。

再起動後、プライマリ VCS Web インターフェイスで、次の手順を実行します。

1. 正しい構成データがあることを確認します。
  - FindMe を使用している場合は、正しい FindMe エントリが存在することを確認します (**[ステータス (Status)]** ) > **[アプリケーション (Applications)]** ) > **[TMS Provisioning Extension サービス (TMS Provisioning Extension Services)]** ) > **[FindMe]** > **[アカウント (Accounts)]** ) 。
  - **[システム (System)]** ) および **[設定 (Configuration)]** 、 **[アプリケーション (Application)]** ) メニューで、各項目の構成を確認します。
2. VCS をバックアップします (**[メンテナンス (Maintenance)]** ) > **[バックアップおよびリストア (Backup and restore)]** ) 。

他のデバイスで、次の手順を実行します。

他の VCS が、このプライマリ VCS ピアに隣接している場合（またはトラバーサルゾーン経由で接続されている場合）、このクラスタのゾーン設定が更新され、このプライマリ VCS のアドレスのみが含まれていることを確認します。

プライマリ VCS ピアで、次の手順を実行します。

1. VCS の Web ブラウザにログインします。
2. **[ステータス (Status)]** ) > **[アラーム (Alarms)]** ) に移動します。  
VCS を再起動する必要があることを知らせるアラームがある場合は、**[メンテナンス (Maintenance)]** ) > **[再起動オプション (Restart options)]** ) に移動し、**[再起動 (Restart)]** をクリックします。
3. VCS を再起動する必要がない場合、メンテナンスモードが無効になっていることを確認します。
  1. **[メンテナンス (Maintenance)]** ) > **[メンテナンスモード (Maintenance mode)]** ) に移動します。
  2. **[メンテナンスモード (Maintenance mode)]** ) を **[オフ (Off)]** ) にします。
  3. **[保存 (Save)]** をクリックします。

## 次の手順

[ステータス (Status) ] > [アラーム (Alarms) ] に移動し、すべてのアラームが機能し、クリアされていることを確認します。

(1 点の VCS の) 新規クラスタの設定が完了しました。クラスタに他の VCS を追加する方法については、「[クラスタへのピアの追加 \(16ページ\)](#)」を参照してください。

Microsoft Lync をこのクラスタに接続する場合は、「[付録 5：クラスタリングによる他の VCS アプリケーションへの影響 \(52 ページ\)](#)」を参照してください。

## クラスタへのピアの追加

既存の X8.7 クラスタ（1 つ以上のピアを含む）に別の VCS ピアを追加する場合は、次の手順を実行します。既存のクラスタがない場合は、「[VCS ピアの新規クラスタの作成（11 ページ）](#)」の手順に従ってください。

次のプロセスでは、X8.7 VCS をクラスタに追加して、クラスタ プライマリの設定を VCS に複製します。次の点に注意してください。

- VCS は、プライマリ VCS を含め最大で 6 つまでクラスタに追加できます。
- 一度にクラスタに追加する必要がある VCS は 1 つだけです。

設定を変更する必要があるのはプライマリ VCS のみです。

**注意：**実行中のすべてのピアでクラスタが安定するまで、クラスタ全体の設定を変更しないでください。いずれかのピアがアップグレード中または再起動中である、あるいはサービスを使用できない状態でクラスタ設定の変更を行った場合、クラスタ データベースの複製により悪影響が及ぶ恐れがあります。

他のピアに対する変更がクラスタ全体に反映されることはなく、次にプライマリの設定がピア全体に複製された場合に上書きされます。ただし、[ピア固有の設定項目](#)のみは例外となります。

変更がクラスタ内のすべてのピアで更新されるのに、1 分間ほどかかる場合があります。

## 前提条件

一般的な前提条件：

- デバイス プロビジョニングが有効な場合、または Cisco TMS で FindMe を管理する場合、1 つ以上のピアを含む既存のクラスタが、Provisioning Extension モードで稼働している必要があります。
- クラスタに含まれるすべての VCS では、同じバージョン（X8.7）の VCS ソフトウェアを実行する必要があります。

## 新しいピアの追加

**プライマリ VCS で、次の手順を実行します。**

プライマリ VCS のネイバー ゾーンまたはトラバーサル ゾーンのリストに、この新しい VCS ピアが含まれていないことを確認します（[\[設定 \(Configuration\)\] > \[ゾーン \(Zones\)\] > \[ゾーン \(Zones\)\]](#)）。

**注：**プライマリ VCS は、この新しい VCS ピアおよびクラスタの他のすべての VCS ピアの設定情報のソースとして使用されます。VCS がクラスタに追加されると、その設定は削除され、プライマリの設定で置換されます。



クラスタに追加する VCS で、次の手順を実行します。

1. 構成内の他の VCS に、クラスタリング ピアのリスト内にある VCS の IP アドレスが設定されていないことを確認します。
2. VCS をバックアップします ([メンテナンス (Maintenance)] > [バックアップおよびリストア (Backup and restore)] )。
3. Web インターフェイスを使用して、VCS が次の条件を満たしているかどうか、設定を確認してください。
  - 有効なイーサネット速度 ([システム (System)] > [ネットワーク インターフェイス (Network interfaces)] > [イーサネット (Ethernet)] ) が設定されている。
  - 有効な IP アドレスおよび IP ゲートウェイ ([システム (System)] > [ネットワーク インターフェイス (Network interfaces)] > [IP]) が設定されている。
  - クラスタのその他のすべてのピアにインストールされるオプション キーと同じオプション キー のセットがインストールされている ([メンテナンス (Maintenance)] > [オプション キー (Option keys)] )。  
コール ライセンス キーの数はピアごとに異なる場合があります。この場合、他のすべてのライセンス キーは各ピアで同じでなければならないことに注意してください。
  - 少なくとも 1 つの有効な DNS サーバが設定されている。また、非修飾 DNS 名が (NTP サーバなどで) 使用されている場合は、ドメイン名が正しく設定されている必要がある (非修飾の DNS 名には、これを FQDN にするため、サフィックスとしてドメイン名が追加されます ([システム (System)] > [DNS]) )。
  - 有効かつ稼働している NTP サーバが設定されている ([システム (System)] > [時間 (Time)] : [ステータス (Status)] セクションの [状態 (State)] が「同期 (Synchronized)」でなければなりません)。
  - ピアが設定されていない ([システム (System)] > [クラスタリング (Clustering)] : このページのすべてのピアおよび IP アドレスのフィールドが空白でなければなりません。入力されている場合、エントリを削除して、[保存 (Save)] をクリックします)。
  - H.323 モードが [オン (On)] に設定されている ([設定 (Configuration)] > [プロトコル (Protocols)] > [H.323]) 。

クラスタを Cisco TMS で管理する場合、そのクラスタに追加する VCS も Cisco TMS で管理する必要があります。

Cisco TMS を使用する場合、クラスタに追加する VCS で、次の手順を実行します。

1. VCS が Cisco TMS を認識できることを確認します。  
これを実行するには、[システム (System)] > [外部マネージャ (External Manager)] の順に選択し、[ステータス (Status)] セクションで [状態 (State)] が [アクティブ (Active)] になっていることを確認します。  
これがアクティブになっていない場合は、「付録 6 : Cisco TMS への VCS の追加 (53 ページ)」の手順に従います。
2. Cisco TMS がこの VCS と通信できることを確認します。  
これを実行するには、Cisco TMS で [システム (System)] > [ナビゲータ (Navigator)] (および必須サブ フォルダ) の順に選択し、VCS の名前をクリックして以下のメッセージが表示されることを確認します。

「システムには開かれたチケットまたは承認済みのチケットはありません (System has no open or acknowledged tickets)」

このメッセージが表示されない場合は、「[付録 6 : Cisco TMS への VCS の追加 \(53 ページ\)](#)」の手順に従います。

クラスタに追加する VCS で、次の手順を実行します。

[ステータス (Status)] > [アラーム (Alarms)] に移動します。VCS を再起動する必要があることを知らせるアラームがある場合は、[メンテナンス (Maintenance)] > [再起動オプション (Restart options)] に移動し、[再起動 (Restart)] をクリックします。

複数のピアを再起動する必要がある場合、次のピアを再起動する前に Web インターフェイスからピアにアクセスできることを確認してから、各ピアを再起動します。

### Cisco TMS を使用している場合

1. クラスタに追加する VCS で、VCS のホスト名が VCS TMS で設定されていることを確認します。

1. [システム (Systems)] > [ナビゲータ (Navigator)] (および必須サブ フォルダ) の順に選択します。

2. この VCS を選択します。

3. [接続 (Connection)] タブを選択します。

4. [ホスト名 (Host Name)] をこの下位ピアの FQDN に設定します (例: vcs3.uk.company.com)。

5. [保存/試行 (Save/Try)] をクリックします。

「DNS config failure resolving <DNS name>: Did not find system IP address () in DNS: <Server IP>」  
のようなメッセージは無視します。

6. Cisco TMS がその DNS を更新することを確認します。

1. [設定 (Settings)] タブを選択します。

2. [強制的に更新 (Force Refresh)] をクリックします。

2. FindMe アカウントを確認します (該当する場合)。

クラスタに追加される VCS で FindMe 情報が複製されるように Cisco TMS を設定している場合 (Cisco TMS で [システム (Systems)] > [ナビゲータ (Navigator)] (および必須サブ フォルダ) に移動し、この VCS を選択し、[プロビジョニング (Provisioning)] タブを選択して、[FindMe サービス (FindMe services)] チェックボックスがオンになっているか確認します)、VCS に存在するユーザ アカウントを削除します。

- FindMe 複製が有効でない場合、FindMe データは Cisco TMS に保存されないため、FindMe エントリを削除する必要はありません。
- FindMe データが Cisco TMS からプロビジョニングされた場合は、既存のユーザ アカウントをすべて削除します。クラスタに追加する VCS で、次の手順を実行します。

1. [ユーザ (Users)] > [FindMe アカウント (FindMe accounts)] に移動します。

2. 表示されるすべてのアカウントを選択して、[削除 (Delete)] をクリックします。

クラスタに追加する VCS で、次の手順を実行します。

1. メンテナンス モードを有効にします。
  - 1.[メンテナンス (Maintenance) ] > [メンテナンス モード (Maintenance mode) ] に移動します。
  - 2.[メンテナンス モード (Maintenance mode) ] を [オン (On) ] に設定します。
  - 3.確認ダイアログ ボックスで [保存 (Save) ] をクリックし、[OK] をクリックします。
2. このピアですべてのコールがクリアされ、登録がタイムアウトになるまで待機します。
  - 必要な場合、自動的にクリアされないコールをこのピアから手で削除します (Web ブラウザを使用し、[ステータス (Status) ] > [コール (Calls) ] に移動して、終了するコールの横のチェックボックスをオンにして、[切断 (Disconnect) ] をクリックします) 。
  - 必要な場合、自動的にクリアされない登録をこのピアから手で削除します (Web ブラウザを使用し、[ステータス (Status) ] > [登録 (Registrations) ] > [デバイスごと (By device) ] に移動して、削除するデバイスの横のチェックボックスをオンにして、[登録解除 (Unregister) ] をクリックします) 。

Conference Factory の登録はそのままにしておいて構いません。これはコールのソースではなく、また他のピアが各自の Conference Factory 登録を所有しているため (有効化されている場合)、これを削除しても別のピアにロールオーバーされることはありません。

プライマリ VCS で、次の手順を実行します。

1. [システム (System) ] > [クラスタリング (Clustering) ] に移動します。

1 つ以上の [ピア X IP アドレス (Peer x IP address) ] フィールドが空白になっています。
2. 最初の空白のフィールドに、新しい VCS ピアの IP アドレスを入力します。

**注：**

  - 一度にクラスタに追加する必要がある VCS は 1 つだけです (複数の VCS ピアを追加する場合、プロセス全体を繰り返します) 。
  - VCS が高度なネットワークを使用する場合は、ピア IP アドレスは、LAN 1 インターフェイス アドレスを指定する必要があります。また、このインターフェイスでは、NAT が無効にされている必要があります。
3. [保存 (Save) ] をクリックします。

ピア 1 は、「このシステム (This system) 」を示します。新しいピアは、「不明 (Unknown) 」を示す場合があります。リフレッシュすると、クラスタへの VCS の追加が完了していないので「失敗 (Failed) 」を示します。

**注：**

- この新しい VCS ピアが通信していないことを示すクラスタ障害アラームが、プライマリおよびクラスタの他の下位ピアで発生します。このアラームは後でクリアされます。
- 新しい VCS の追加が完了するまで、クラスタ設定の複製は中断します。クラスタ設定の変更は、この VCS の追加が完了するまで、複製されません。

クラスタのすべての下位 VCS (追加する VCS 以外) で、次の手順を実行します。

1. 次のように、[システム (System) ] > [クラスタリング (Clustering) ] に移動し、フィールドを設定します。

クラスタ名 (Cluster name)	マスター VCS で設定される [クラスタ名 (Cluster name) ] と同じ
クラスタ事前共有キー (Cluster pre-shared key)	プライマリ VCS の設定と同じ
設定マスター (Configuration master)	プライマリ VCS の設定と同じ
ピア 1 IP アドレス～ピア 6 IP アドレス (Peer 1 IP address ...Peer 6 IP address)	プライマリ VCS の設定と同じ

2. [保存 (Save) ] をクリックします。

クラスタに追加する別の下位 VCS で、次の手順を実行します。

1. 管理者として SSH または他の CLI インターフェイスでログインします。VCS コマンド プロンプトで、次のように入力します。

```
xcommand DefaultValueSet Level: 2
xcommand DefaultLinksAdd
```

**注：**このコマンドは、LDAP 認証設定を削除します。このコマンドを実行するには、Web 管理者パスワードが必要です。

2. [ユーザ (Users) ] > [管理者アカウント (Administrator accounts) ] に移動します。
3. デフォルトの管理者アカウント以外のすべてのエントリを削除します。
4. [システム (System) ] > [DNS] に移動し、[システムのホスト名 (System host name) ] がこの VCS の DNS ホスト名であることを確認します (通常は、スペースを除き、[システム (System) ] > [管理 (Administration) ] の [システム名 (System name) ] と同じであり、クラスタの各 VCS に固有です)。正しく設定されていない場合は、適切に設定し、[保存 (Save) ] をクリックします。

**注：**<System host name>.<DNS domain name> = この VCS の FQDN であることに注意してください

5. 次のように、[システム (System) ] > [クラスタリング (Clustering) ] に移動し、フィールドを設定します。

クラスタ名 (Cluster name)	マスター VCS で設定される [クラスタ名 (Cluster name)] と同じ
クラスタ事前共有キー (Cluster pre-shared key)	プライマリ VCS の設定と同じ
設定マスター (Configuration master)	プライマリ VCS の設定と同じ
ピア 1 IP アドレス～ピア 6 IP アドレス (Peer 1 IP address ...Peer 6 IP address)	プライマリ VCS の設定と同じ

6. **[保存 (Save)]** をクリックします。

この新しい VCS が通信していないことを示すクラスタ通信障害アラームが、この VCS ピアで発生します。これは、再起動後にクリアされることに注意してください。

7. VCS を再起動します ([メンテナンス (Maintenance)] > [再起動オプション (Restart options)] に移動し、[再起動 (Restart)] をクリックし、[OK] をクリックします)。

複数のピアを再起動する必要がある場合、次のピアを再起動する前に Web インターフェイスからピアにアクセスできることを確認してから、各ピアを再起動します。

8. 再起動後、約 2 分間待ちます。この間に、プライマリから設定がコピーされます。

9. [ステータス (Status)] > [アラーム (Alarms)] に移動します。VCS を再起動する必要があることを知らせるアラームがある場合は、[メンテナンス (Maintenance)] > [再起動オプション (Restart options)] に移動し、[再起動 (Restart)] をクリックします。

複数のピアを再起動する必要がある場合、次のピアを再起動する前に Web インターフェイスからピアにアクセスできることを確認してから、各ピアを再起動します。

10. 正しい構成データがあることを確認します。

- FindMe を使用している場合は、正しい FindMe エントリが存在することを確認します ([ステータス (Status)] > [アプリケーション (Applications)] > [TMS Provisioning Extension サービス (TMS Provisioning Extension Services)] > [FindMe] > [アカウント (Accounts)] )。
- [システム (System)] および [設定 (Configuration)]、[アプリケーション (Application)] メニューで、各項目の構成を確認します。

他のデバイスで、次の手順を実行します。

他の VCS が、この VCS ピアのクラスタに隣接している場合 (またはトラバーサル ゾーン経由で接続されている場合)、このクラスタのゾーン設定が更新され、この新しいピアのアドレスが含まれていることを確認します。

各 VCS ピア (プライマリおよび新しい VCS ピアを含む) で、次の手順を実行します。

[ステータス (Status)] > [アラーム (Alarms)] に移動します。VCS を再起動する必要があることを知らせるアラームがある場合は、[メンテナンス (Maintenance)] > [再起動オプション (Restart options)] に移動し、[再起動 (Restart)] をクリックします。

複数のピアを再起動する必要がある場合、次のピアを再起動する前に Web インターフェイスからピアにアクセスできることを確認してから、各ピアを再起動します。

## 複製ステータスの確認

VCS から成功ステータスが報告されるまで、5 分以上かかる場合があります。問題が発生した場合、5 分待ってから画面をリフレッシュしてください。

**VCS で次の手順を実行します。**

1. **[システム (System) ] > [クラスタリング (Clustering) ]** に移動し、クラスタ データベースのステータスが **[アクティブ (Active) ]** であることを確認します。
2. Cisco TMS を使用している場合、Cisco TMS のリフレッシュを強制実行して、このアップグレードされた Cisco VCS のすべての設定が正しいことを確認します。

**Cisco TMS で次の手順を実行します。**

1. クラスタのすべての VCS (プライマリ VCS を含む) で、次の手順を実行します。
  1. **[システム (Systems) ] > [ナビゲータ (Navigator) ]** (および必須サブ フォルダ) を選択し、VCS の名前をクリックします。
  2. **[設定 (Settings) ]** タブを選択します。
  3. **[強制的に更新 (Force Refresh) ]** をクリックします。
2. この手順をクラスタのすべての VCS ピアで繰り返します。

## 次の手順

Conference Factory (Multiway™) を使用する場合は、「[付録 5：クラスタリングによる他の VCS アプリケーションへの影響 \(52 ページ\)](#)」を参照してください。

デフォルト以外の信頼できる CA 証明書またはデフォルト以外のサーバ証明書、あるいはこれらの両方をクラスタで使用する場合、必要な信頼できる CA 証明書および適切なサーバ証明書が追加されるピアで設定されていることを確認します。

これで、X8.7 VCS の VCS X8.7 クラスタへの追加は完了しました。

## ピア固有の項目

設定のほとんどの項目は、プライマリ ピアを介してクラスタ内のすべてのピアに適用されます。ただし、次の項目（Web インターフェイスで、+ でマークされている）は各クラスタ ピアで個別に指定する必要があります。

**注：**プライマリ ピア以外のすべてのピアに適用された設定データは変更しないでください。変更してもマスターから上書きされるか、プライマリの複製に失敗する場合があります。

### クラスタ構成 ([システム (System)] > [クラスタリング (Clustering)])

クラスタを構成する**ピア IP アドレス**のリスト（ピアそれ自体の IP アドレスを含む）は各ピアで指定される必要があり、ピア IP アドレスは各ピアで一致する必要があります。

**クラスタ名**、および**クラスタの事前共有キー**は、各ピアで指定する必要があり、すべてのピアで同じにする必要があります。

### イーサネット速度 ([システム (System)] > [ネットワーク インターフェイス (Network interfaces)] > [イーサネット (Ethernet)])

**イーサネット速度**は、各ピアに固有です。各ピアでは、イーサネット スイッチに接続するために多少異なる要件がある場合があります。

### IP 設定 ([システム (System)] > [ネットワーク インターフェイス (Network interfaces)] > [IP])

LAN の設定は、各ピアで固有です。

- 各ピアで異なる **IPv4 アドレス**と異なる **IPv6 アドレス**が設定されている必要があります。
- **IP ゲートウェイ**の設定はピアに固有です。各ピアでは、異なるゲートウェイが使用できます。

各ピアが同じプロトコルをサポートする必要があるため、IP プロトコルがすべてのピアに適用されることに注意してください。

### IP スタティック ルート ([システム (System)] > [ネットワーク インターフェイス (Network interfaces)] > [スタティック ルート (Static routes)])

追加するスタティック ルートはピアに固有なので、必要に応じて、異なるルートを異なるピアで作成できます。クラスタ内のすべてのピアが同じスタティック ルートを使用できるようにする場合は、各ピアでルートを作成する必要があります。

### システム名 ([システム (System)] > [管理 (Administration)])

**システム名**はクラスタの各ピアで異なる必要があります。

### DNS サーバと DNS ホスト名 ([システム (System)] > [DNS])

DNS サーバは、各ピアに固有です。各ピアでは、異なる DNS サーバのセットを使用できます。

**システムのホスト名とドメイン名**は各ピアに固有です。



## NTP サーバとタイムゾーン ([システム (System) ]>[時間 (Time) ])

NTP サーバは各ピアに固有です。各ピアは、1 つ以上の異なる NTP サーバを使用できます。

タイムゾーンは各ピアに固有です。各ピアで異なる現地時間を設定できます。

## SNMP ([システム (System) ]>[SNMP])

SNMP 設定は、各ピアに固有です。また、各ピアで異なることができます。

## ロギング ([メンテナンス (Maintenance) ]>[ロギング (Logging) ])

各ピアのイベント ログおよびコンフィギュレーション ログは、特定の VCS のアクティビティのみを報告します。ログレベルとリモート Syslog サーバのリストは、各ピアに固有です。すべてのピアのログを送信できるリモート Syslog サーバを設定することを推奨します。これにより、クラスタ内のすべてのピア間でアクティビティの全体像を把握できます。

## セキュリティ証明書 ([メンテナンス (Maintenance) ]>[セキュリティ証明書 (Security certificates) ])

VCS が使用する信頼できる CA 証明書とサーバ証明書および証明書失効リスト (CRL) は、ピアごとに個別にアップロードする必要があります。

## 管理アクセス ([システム (System) ]>[管理 (Administration) ])

次のシステム管理アクセス設定は各ピアに固有です。

- シリアル ポート/コンソール
- SSH サービス
- Web インターフェイス (HTTPS 経由)
- HTTP リクエストを HTTPS にリダイレクト
- 自動保護サービス

## オプションキー ([メンテナンス (Maintenance) ]>[オプションキー (Option keys) ])

オプションキーは各ピアに固有です。各ピアでは、インストールされている同じオプションキーのセットが設定されている必要がありますが、クラスタの各ピアで個別にこれらを購入する必要があります。ただし、これはトラバーサル コール ライセンスおよび非トラバーサル コール、TURN リレー ライセンスには適用されず、これらのライセンスはすべてのクラスタピアにインストールでき、クラスタのすべてのピアで使用することができます。

## アクティブディレクトリサービス ([設定 (Configuration) ]>[認証 (Authentication) ]>[デバイス (Devices) ]>[Active Directory サービス (Active Directory Service) ])

デバイス認証のためアクティブディレクトリサービスへの接続を設定する場合、NetBIOS マシン名 (上書き) およびドメイン管理者のユーザ名とパスワードは各ピアに固有です。



### **Conference Factory テンプレート ([アプリケーション (Applications) ] > [Conference Factory])**

MCU へのコールをルートする目的で Conference Factory アプリケーションが用いるテンプレートは、ピア固有です。これは、このテンプレートがクラスター内の各ピアに対し固有である必要があるためです。

### **VCS フロントパネル ディスプレイ モード (CLIのみを通じて設定可能)**

**xConfiguration Administration LCDPanel Mode CLI** 設定は各ピアに固有です。

## VCS クラスタ間のネイバー化

ローカル VCS（または VCS クラスタ）をリモートの VCS クラスタのネイバーにすることができます。このリモート クラスタはローカル VCS へのネイバー、トラバーサル クライアント、またはトラバーサル サーバにできます。この場合、コールがローカル VCS で受信され、関連するゾーン経由でリモート クラスタに渡されると、そのコールはそのネイバー クラスタ内のリソース使用率が最も低いピアにルーティングされます。そのピアは必要に応じてコールを次のいずれかに適宜転送します。

- ローカルに登録されたエンドポイント（エンドポイントがそのピアに登録されている場合）
- ピア（エンドポイントがクラスタ内の別のピアに登録されている場合）
- 外部ゾーン（エンドポイントが他の場所に配置されている場合）

最も低いリソース使用率は、ピア上の使用可能なトラバーサル コール数（最大 - 現在の使用率）を比較して、最大数を持つピアを選択することで決定されます。メンテナンス モードにあるピアは考慮されません。

リモート クラスタへの接続を設定するときは、1 つのゾーンを作成し、クラスタ内のすべてのピアの詳細をそれに設定します。ゾーンにこの情報を追加することで、個別のピアの状態に関係なく、コールがそのクラスタに確実に渡ります。

また、**ネイバー**または**トラバーサル クライアント** ゾーン経由で接続される場合は、リモート クラスタにあるすべてのピアの IP アドレスを入力する必要があります。**トラバーサル サーバ** ゾーンの場合は、これらの接続はリモート システムの IP アドレスを指定して設定されていないため、アドレスを入力することはありません。

**注：**ピアとして設定されるシステムを、互いにネイバーとして設定することも**できません**。

### クラスタの隣接化

ローカル VCS（または VCS クラスタ）をリモート VCS クラスタのネイバーにするには、クラスタを示す 1 つのゾーンを作成し、そのクラスタにあるすべてのピアの詳細をそこに設定します。

1. ローカル VCS で（またはローカル VCS がクラスタの場合は、プライマリ ピアで）、適切なタイプのゾーンを作成します。このゾーンは、クラスタへの接続を表します。
2. [ロケーション (Location) ] セクションで、[ピア 1 (Peer 1) ] から [ピア 6 (Peer 6) ] のアドレス フィールドにリモート クラスタ内の各ピアの IP アドレスまたは FQDN を入力します。

次の点に注意してください。

- 可能であればこれらのフィールドには IP アドレスを使用します。FQDN を使用する場合は、各 FQDN が異なっていて、各ピアに対して単一の IP アドレスに解決される必要があります。
- リモート VCS クラスタ内のピアがここでリストされる順序は重要ではありません。
- クラスタにさらに VCS を追加するときは（たとえば容量を増やすためや冗長性を増す目的で）、そのクラスタのネイバーである VCS が新しいクラスタ ピアを認識できるように変更する必要があります。

## クラスタからのライブ ピアの完全な削除

このプロセスでは既存のクラスタから 1 つの VCS ピアを削除します。この VCS への FindMe および設定の複製は停止し、VCS は、クラスタのピアのリストから削除されます。プロビジョニングは、削除された VCS で無効になります。

- クラスタ全体を解体する場合は、代わりに「[クラスタの解体 \(31 ページ\)](#)」を使用します。
- 削除するクラスタ ピアにアクセスできない場合は、「[クラスタからのデッド ピアの完全な削除 \(29 ページ\)](#)」の手順に従います。

### 準備：

1. クラスタから削除する VCS がプライマリ ピアとして表示されていないことを確認します。  
これがプライマリである場合は、「[プライマリ ピアの変更 \(34 ページ\)](#)」の手順に従います。

### 削除する VCS で、次の手順を実行します。

1. Web インターフェイスにログインします。
2. **[システム (System)]** > **[クラスタリング (Clustering)]** に移動します。
  - 1.**[クラスタ名 (Cluster name)]** をこの VCS に固有の ID に変更します (可能な場合、たとえば、「vcse1.example.com」など、この個々の VCS に対応する SRV レコードで使用されるルーティング可能な完全修飾ドメイン名に変更します。「[付録 3：クラスタ名と DNS SRV レコード \(45 ページ\)](#)」を参照してください)。
  - 2.**[クラスタ事前共有キー (Cluster pre-shared key)]** を削除します。
  - 3.**[ピア x IP アドレス (Peer x IP address)]** フィールドのすべてのエントリを削除します。
3. **[保存 (Save)]** をクリックします。

次の点に注意してください。

- 過去の FindMe ユーザは、削除されたこの VCS 上でも利用可能となっています。必要に応じ、これらのユーザを削除します (**[ユーザ (Users)]** > **[FindMe アカウント (FindMe accounts)]**) 。
- 次のようなアラームが、Web インターフェイスおよび削除する VCS の CLI に表示される場合があります。これはエラーではありません。このアラームは、VCS を再起動するとクリアされます。



4. クラスタで Microsoft Lync B2BUA を使用した場合は、次の手順を実行します。
  - 1.**[アプリケーション (Applications)]** > **[B2BUA]** > **[Microsoft Lync]** > **[設定 (Configuration)]** に移動します。
  - 2.**[Microsoft Lync B2BUA]** が **[有効 (Enabled)]** の場合は **[無効 (Disabled)]** に変更し、**[保存 (Save)]** をクリックします。

5. VCS を再起動します ([メンテナンス (Maintenance)] > [再起動オプション (Restart options)] に移動し、[再起動 (Restart)] をクリックし、[OK] をクリックします)。

プライマリ VCS で、次の手順を実行します。

1. [システム (System)] > [クラスタリング (Clustering)] に移動します。
2. 削除された VCS の IP アドレスを削除します。
3. 削除する VCS が、リストの最後のフィールドでない場合、エントリ間に空のフィールドができないように、リスト上の他の IP アドレスが上に移動します。
4. 前述の手順で、プライマリ VCS ピアの IP アドレスがリスト上で上に移動した場合、その新しい位置に合わせて [設定マスター (Configuration master)] の値を変更します。
5. [保存 (Save)] をクリックします。

残りのすべての下位 VCS ピアで、次の手順を実行します。

1. [システム (System)] > [クラスタリング (Clustering)] に移動します。
2. プライマリ VCS での設定と同じになるように、[ピア X IP アドレス (Peer x IP address)] および [設定マスター (Configuration master)] フィールドを編集します。
3. [保存 (Save)] をクリックします。
4. 他のすべての下位 VCS ピアで、クラスタリング設定が同じになるまで、この手順を繰り返します。

他のデバイスで、次の手順を実行します。

1. 他のシステムが、この VCS ピアのクラスタに隣接している場合 (またはトラバーサル ゾーンを介して接続されている場合)、このクラスタのゾーン設定が更新され、削除されたピアのアドレスが除外されることを確認してください。
2. 削除された VCS に登録しているエンドポイントがある場合、クラスタの他の VCS ピアのいずれかに登録されるように、エンドポイントの設定 (または、クラスタ ピアを示す DNS サーバ エントリの設定) を変更します。

**注意：** 削除された VCS は、クラスタから削除された時点では、その設定が保持され、非クラスタ化 VCS として機能します。クラスタから削除した後は、サービスを停止するか (たとえば、ネットワークにアウトオブサービス VCS を再接続する前に、「[クラスタからのデッドピアの完全な削除 \(29 ページ\)](#)」に記載されている出荷時の状態へのリセットを実行します)、または他のデバイスがクラスタ ピアとして VCS を使用しないように、代替設定を適用することを推奨します。

これで、ライブ VCS のクラスタからの削除は、完了です。

## クラスタからのデッド ピアの完全な削除

この手順は、次の場合に実行します。

- VCS が使用できなくなり、返品する必要がある
- 何らかの理由で VCS にアクセスできない

クラスタ全体を削除する場合は、「[クラスタの解体 \(31 ページ\)](#)」の手順を使用します。

削除されるクラスタ ピアにアクセスできる場合は、「[クラスタからのライブ ピアの完全な削除 \(27 ページ\)](#)」に定義されている手順を使用します。これにより、削除された VCS ならびにその以前のピアがクリアされます。

**注：**この手順では、削除される VCS のクラスタリング設定は削除されません。削除後は、必ず VCS のすべてのピアを削除し、FindMe と設定の複製（以下の「[このピアからの設定のクリア \(30 ページ\)](#)」を参照）を停止した上で、アウトオブサービス VCS の再接続を行ってください。

### 準備：

クラスタから削除する VCS が Cisco TMS 上でプライマリ VCS として表示されていないことを確認します。

これがプライマリ VCS として表示されている場合は、「[プライマリ ピアの変更 \(34 ページ\)](#)」で別のピアをプライマリに設定する方法を確認してください。

**プライマリ VCS で、次の手順を実行します。**

1. **[システム (System)] > [クラスタリング (Clustering)]** に移動します。
2. 削除された VCS の IP アドレスを削除します。
3. 削除する VCS が、リストの最後のフィールドでない場合、エントリ間に空のフィールドができないように、リスト上の他の IP アドレスが上に移動します。
4. 前述の手順で、プライマリ VCS ピアの IP アドレスがリスト上で上に移動した場合、その新しい位置に合わせて **[設定マスター (Configuration master)]** の値を変更します。
5. **[保存 (Save)]** をクリックします。

**残りのすべての下位 VCS ピアで、次の手順を実行します。**

1. **[システム (System)] > [クラスタリング (Clustering)]** に移動します。
2. プライマリ VCS での設定と同じになるように、**[ピア X IP アドレス (Peer x IP address)]** および **[設定マスター (Configuration master)]** フィールドを編集します。
3. **[保存 (Save)]** をクリックします。
4. 他のすべての下位 VCS ピアで、クラスタリング設定が同じになるまで、この手順を繰り返します。

他のデバイスで、次の手順を実行します。

1. 他のシステムが、この VCS ピアのクラスタに隣接している場合（またはトラバーサルゾーンを介して接続されている場合）、このクラスタのゾーン設定が更新され、削除されたピアのアドレスが除外されることを確認してください。
2. 削除された VCS に登録しているエンドポイントがある場合、クラスタの他の VCS ピアのいずれかに登録されるように、エンドポイントの設定（または、クラスタ ピアを示す DNS サーバエントリの設定）を変更します。

これで、クラスタのアウトオブサービス VCS の削除が完了しました。

## このピアからの設定のクリア

削除したピアを復元するには、これをネットワークに再接続する前にその設定をクリアする必要があります。最も簡単な方法は次のとおりです。

1. VCS に root としてログインします（シリアルまたは SSH を使用します。シリアル接続の場合、工場出荷時のリセットの実行中、詳細が示されます）。
2. `factory-reset` と入力します。
3. 次のようにプロンプトに応答します。
  1. オプション キーを保持しますか（Keep option Keys） = はい（YES）
  2. IP 設定を保持しますか（Keep IP configuration） = はい/いいえ（YES or NO）（VCS を同じ IP アドレスの別の VCS で置換したかどうかにより異なります）
  3. SSH キーを保持しますか（Keep SSH keys） = いいえ（NO）
  4. root および管理パスワードを保持（Keep root and admin passwords） = はい/いいえ（YES or NO）（必要に応じて設定します）
  5. ログ ファイルを保持（Save log files） = いいえ（NO）（分析などのために特に必要がない限りこのように設定します）
  6. ハード ディスクを置換（Replace hard disk） = いいえ（NO）
  7. 続行しますか（Are you sure you want to continue） = はい（YES）

メッセージが表示され、次に、シリアルまたは SSH 経由の接続が失われます。

VCS が再びアクセス可能になるまで、約 20 分以上かかる場合があります。

4. SSH を介して VCS に管理者としてログインします。
5. 次のように入力します：`xcommand DefaultLinksAdd`

これにより、回復した VCS の設定がデフォルトに戻り、以前のピアとの関連がなくなります。

## クラスタの解体

このプロセスは既存のクラスタからすべての VCS ピアを削除します。FindMe および設定の複製が停止します。また、プロビジョニングも停止し、クラスタが Cisco TMS から削除されます。

各 VCS は、クラスタの削除された時点で設定を保持し、スタンドアロン VCS として機能します。

**注意：**クラスタから削除された後で、任意の VCS が稼働していても、同じクラスタの一部であった別の VCS に登録されているエンドポイント間のコールは失敗します。これは、クラスタが削除されると、クラスタ サブゾーンも削除され、コールをルーティングできる 2 つの VCS 間のリンクがなくなるためです。これを解決するには、VCS 間にネイバー関係を確立して、リンクを作成する必要があります。

**準備：**

どの VCS にもアクセスできない場合は、まず「[クラスタからのデッド ピアの完全な削除 \(29 ページ\)](#)」の手順を使用して VCS を削除します。

**Cisco TMS を (Provisioning Extension モードで) 使用している場合は、次の手順を実行します。**

1. **[システム (Systems) ] > [ナビゲータ (Navigator) ]** (および必須サブ フォルダ) を選択して、クラスタの VCS をクリックします。
2. **[プロビジョニング (Provisioning) ]** タブを選択します。
3. すべての 4 つのサービスを無効にします (チェックボックスをオフにします)。
4. **[保存 (Save) ]** をクリックします。

**各下位 VCS ピアで、次の手順を実行します。**

1. Web インターフェイスにログインします。
2. **[システム (System) ] > [クラスタリング (Clustering) ]** に移動します。
  1. **[クラスタ名 (Cluster name) ]** をこの VCS に固有の ID に変更します (可能な場合、たとえば、「vcse1.example.com」など、この個々の VCS に対応する SRV レコードで使用されるルーティング可能な完全修飾ドメイン名に変更します。「[付録 3：クラスタ名と DNS SRV レコード \(45 ページ\)](#)」を参照してください)。
  2. **[クラスタ事前共有キー (Cluster pre-shared key) ]** を削除します。
  3. **[ピア x IP アドレス (Peer x IP address) ]** フィールドのすべてのエントリを削除します。
3. **[保存 (Save) ]** をクリックします。

次の点に注意してください。

- 過去の FindMe ユーザは、削除されたこの VCS 上でも利用可能となっています。必要に応じ、これらのユーザを削除します (**[ユーザ (Users) ] > [FindMe アカウント (FindMe accounts) ]**) 。

- 次のようなアラームが、Web インターフェイスおよび削除する VCS の CLI に表示される場合があります。これはエラーではありません。このアラームは、VCS を再起動するとクリアされます。



4. クラスタで Microsoft Lync B2BUA を使用した場合は、次の手順を実行します。
  1. **[アプリケーション (Applications)] > [B2BUA] > [Microsoft Lync] > [設定 (Configuration)]** に移動します。
  2. **[Microsoft Lync B2BUA]** が **[有効 (Enabled)]** の場合は **[無効 (Disabled)]** に変更し、**[保存 (Save)]** をクリックします。
5. VCS を再起動します (**[メンテナンス (Maintenance)] > [再起動オプション (Restart options)]** に移動し、**[再起動 (Restart)]** をクリックし、**[OK]** をクリックします)。
 

複数のピアを再起動する必要がある場合、次のピアを再起動する前に Web インターフェイスからピアにアクセスできることを確認してから、各ピアを再起動します。
6. それぞれの下位 VCS に対し、同じ手順を繰り返します。

プライマリ VCS で、次の手順を実行します。

1. Web インターフェイスにログインします。
2. **[システム (System)] > [クラスタリング (Clustering)]** に移動します。
  1. (オプション) **[クラスタ名 (Cluster name)]** をこの VCS に固有の ID に変更します (可能な場合、たとえば、「vcse1.example.com」など、この個々の VCS に対応する SRV レコードで使用されるルーティング可能な完全修飾ドメイン名に変更します。(「[付録 3: クラスタ名と DNS SRV レコード \(45 ページ\)](#)」を参照してください) )。
  2. **[クラスタ事前共有キー (Cluster pre-shared key)]** を削除します。
  3. **[ピア x IP アドレス (Peer x IP address)]** フィールドのすべてのエントリを削除します。
3. **[保存 (Save)]** をクリックします。

次の点に注意してください。

- 過去の FindMe ユーザは、削除されたこの VCS 上でも利用可能となっています。
- 次のようなアラームが、Web インターフェイスおよび削除する VCS の CLI に表示される場合があります。これはエラーではありません。このアラームは、VCS を再起動するとクリアされます。



4. VCS を再起動します (**[メンテナンス (Maintenance)] > [再起動オプション (Restart options)]** に移動し、**[再起動 (Restart)]** をクリックし、**[OK]** をクリックします)。



他のデバイスで、次の手順を実行します。

1. 他のシステムがこの VCS ピアのこのクラスタに隣接している場合（またはトラバーサルゾーン経由で接続されている場合）、これらのゾーンが削除または適切に変更されていることを確認します。
2. この VCS クラスタに登録しているエンドポイントがある場合、適切な VCS に登録されるように、エンドポイントの設定（または、クラスタ ピアを示す DNS サーバエントリの設定）を変更します。

これで、VCS のクラスタの削除が完了しました。

## プライマリ ピアの変更

この手順は、現在のプライマリ ピアにアクセスできなくても実行可能です。

**注：**複数のピア間でプライマリをめぐる競合が発生するのを避けるため、記載されたとおりの順序に従ってプロセスを実行してください。

**「新しい」プライマリ VCS で、次の手順を実行します。**

1. **[システム (System) ] > [クラスタリング (Clustering) ]** に移動します。
2. **[設定マスター (Configuration master) ]** ドロップダウン メニューから「このシステム (This system) 」というピア エントリの ID 番号を選択します。
3. **[保存 (Save) ]** をクリックします。

このプライマリ ピアを変更する場合、「クラスタ マスター不一致 (Cluster master mismatch) 」または「クラスタ複製エラー (Cluster replication error) 」というアラームが VCS で発生しますが、この手順の実行中に修正されるので無視してください。

**「古い」マスター ピア (依然アクセス可能な場合) から順番に、他のすべての VCS ピアで次の手順を実行します。**

1. **[システム (System) ] > [クラスタリング (Clustering) ]** に移動します。
2. **[設定マスター (Configuration master) ]** ドロップダウン メニューから「新しい」プライマリ VCS の ID 番号を選択します。
3. **[保存 (Save) ]** をクリックします。

**クラスタの各 VCS (プライマリを含む) で、次の手順を実行します。**

1. **[システム (System) ] > [クラスタリング (Clustering) ]** に移動し、ページをリフレッシュして、**[設定マスター (Configuration master) ]** の変更が適用されていることを確認します。
2. VCS で変更が適用されていない場合、上記の手順を繰り返します。
3. クラスタ データベースのステータスがアクティブであることを確認します。

VCS で発生した「クラスタ マスター不一致 (Cluster master mismatch) 」および「クラスタ複製エラー (Cluster replication error) 」に関するアラームは、約 2 分後に自動的にクリアされます。

### Cisco TMS

変更の必要はありません。Cisco TMS は、VCS クラスタでのプライマリの変更を確認し、適切に報告します。

### 以前のプライマリが使用できない場合

「古い」プライマリにアクセスできないため、プライマリ ピアを変更する場合は、「[クラスタからのデッド ピアの完全な削除 \(29 ページ\)](#)」の手順に従ってください。

クラスタのプライマリ ピアを変更した際は「古い」プライマリ ピアがアクセス不可能であったが、その後 VCS が使用可能になった場合は、その設定をクリアし、「[クラスタへのピアの追加 \(16 ページ\)](#)」の手順を用いてこれをクラスタに戻す必要があります。

これで、VCS クラスタのプライマリ ピアの変更は完了です。

## ピアの IP アドレスの変更

VCS ピアの IP アドレスを変更するには、その VCS をクラスタから削除し、IP アドレスを変更して、VCS を再びクラスタに追加する必要があります。

そのプロセスは次のとおりです。

1. IP アドレスを変更する VCS がプライマリ VCS でないことを確認します。  
これがプライマリ VCS として表示されている場合は、「[プライマリ ピアの変更 \(34 ページ\)](#)」の手順に従って、別のピアをプライマリに設定してください。
2. 「[クラスタからのライブ ピアの完全な削除 \(27 ページ\)](#)」に記載された手順を実行します。
3. VCS の IP アドレスを変更します。
4. 「[クラスタへのピアの追加 \(16 ページ\)](#)」に記載された手順を実行します。

これで、VCS ピアの IP アドレスの変更は完了です。

## ピアの置換

このセクションでは、異なるユニットでクラスタ ピア VCS を交換するための手順の概要を示します。

1. 置換する VCS がプライマリ VCS でないことを確認します。  
これがプライマリ VCS として表示されている場合は、「[プライマリ ピアの変更 \(34 ページ\)](#)」の手順に従って、別のピアをプライマリに設定してください。
2. 次のように、クラスタから既存のピアを削除します。
  1. 置換するクラスタ ピアにアクセスできない場合は、「[クラスタからのデッド ピアの完全な削除 \(29 ページ\)](#)」の手順に従います。
  2. 置換するクラスタ ピアにアクセスできる場合は、「[クラスタからのライブ ピアの完全な削除 \(27 ページ\)](#)」の手順に従います。
3. 「[クラスタへのピアの追加 \(16 ページ\)](#)」で定義された手順を用いて、クラスタに代替ピアを追加します。

## 設定を保持したままピアを置換

この手順では、アクセス可能な VCS を別の VCS で置換すると仮定します。

1. 置換する VCS がプライマリ VCS でないことを確認します。  
これがプライマリ VCS として表示されている場合は、「[プライマリ ピアの変更 \(34 ページ\)](#)」の手順に従って、別のピアをプライマリに設定してください。
2. 「[クラスタからのライブ ピアの完全な削除 \(27 ページ\)](#)」の説明に従って、ピアを安全に削除します。  
**バックアップを行う前に、ピアからクラスタリング設定をクリアし、その他すべてのピアのクラスタリング設定を更新する必要があります (プライマリ ピアから開始すること)。**
3. 削除したピアの設定をバックアップします。
4. 新しい VCS のオプション キーを作成し、これを適用します。他のピアに適用するものと同じキーのセットを適用する必要があります。
5. 新しい VCS にバックアップを復元します。
6. 新しい VCS の DNS 設定が他のピアと同一であることを確認し、これを同じ NTP サーバと同期化します。
7. 「[クラスタへのピアの追加 \(16 ページ\)](#)」で定義された手順を用いて、クラスタに代替ピアを追加します。  
リンク先の手順に記載された設定のほとんどは、すでに設定済みです。ここに記載された手順のうち、最も重要なものは以下のとおりです。
  1. 新しいピアのアドレスをプライマリのクラスタリング設定に追加します
  2. 新しいピアのアドレスを他の既存のピアのクラスタリング設定に追加します
  3. 新しいピアにクラスタリング設定を入力します (クラスタ名、共有秘密、順序付きピア リスト)

8. 新しいピアを再起動します
9. 約 5 分待ってから、クラスタの状態をチェックし、アラームがある場合はこれを解決します

**注：**VCS コントロールのクラスタ内のピアを置換し、かつそのクラスタが MRA クライアントの SSO 用に設定されていた場合、クラスタの新しい SAML メタデータで IDP を更新するまで、SSO が失敗することがあります。

これは、いずれかのピアが新たなシリアル番号を持ち、このシリアル番号がクラスタのメタデータ生成に使用されるためです。

クラスタの SAML メタデータをエクスポートし、これを IDP にコピーする必要があります。[Cisco VCS 構成ガイドページ](#)にある『*Mobile and Remote Access via Cisco VCS*』を参照してください。

## 付録 1：トラブルシューティング

### VCS アラームおよび警告

「クラスタ名が設定されていません：FindMe またはクラスタリングが使用中の場合は、クラスタ名を定義する必要があります（Cluster name not configured: if FindMe or clustering are in use a cluster name must be defined）」

同じクラス名が、クラスタの各 VCS で設定されていることを確認します。

**[クラスタ名 (Cluster name)]** は、この VCS クラスタに対応する SRV レコードで使用されるルーティング可能な完全修飾ドメイン名にする必要があります。たとえば、「cluster1.example.com」などです（「[付録 3：クラスタ名と DNS SRV レコード \(45 ページ\)](#)」を参照してください）。

「クラスタ複製エラー：<エラーの詳細> 設定を手動で同期化する必要があります（Cluster replication error: <details> manual synchronization of configuration is required）」

次の場合もあります。

- 「クラスタ複製エラー：設定を手動で同期化する必要があります（Cluster replication error: manual synchronization of configuration is required）」
- 「クラスタ複製エラー：マスターまたはこのスレーブのピアの設定ファイルが見つかりません。設定を手動で同期化する必要があります（Cluster replication error: cannot find master or this slave's peer configuration file, manual synchronization of configuration is required）」
- 「クラスタ複製エラー：設定マスター ID に一貫がありません：設定を手動で同期化する必要があります（Cluster replication error: configuration master ID is inconsistent, manual synchronization of configuration is required）」
- 「クラスタ複製エラー：このピアの設定がマスターの設定と競合しています。設定を手動で同期化する必要があります（Cluster replication error: this peer's configuration conflicts with the master's configuration, manual synchronization of configuration is required）」

下位 VCS でアラーム「クラスタ複製エラー：<エラーの詳細> 設定の同期化（Cluster replication error - <details> synchronization of configuration）」が報告された場合：

当該の下位 VCS で次の手順を実行します。

- 管理者として SSH または他の CLI インターフェイスでログインします。
- コマンド プロンプトで、次のように入力します。

```
xcommand ForceConfigUpdate
```

これにより、下位 VCS 設定が削除され、プライマリ VCS の設定が強制的に更新されます。

注意：このコマンドは、プライマリ VCS の設定が正常な状態である場合にのみ使用します。このコマンドを実行する前にバックアップすることを推奨します。

「クラスタ複製エラー：NTP サーバに到達できません (Cluster replication error: the NTP server is unreachable) 」

VCS の **[システム (System) ] > [時間 (Time) ]** ページでアクセス可能な NTP サーバを設定します。

「クラスタ複製エラー：ローカル VCS がピアのリストにありません (Cluster replication error: the local VCS does not appear in the list of peers) 」

プライマリ VCS でこの VCS のピアのリストを確認および修正して、他のすべての VCS ピアをコピーします (**[システム (System) ] > [クラスタリング (Clustering) ]**) 。

「クラスタ複製エラー：アップグレードが進行中のため、設定の自動複製が一時的に無効にされています (Cluster replication error: automatic replication of configuration has been temporarily disabled because an upgrade is in progress) 」

アップグレードが完了するまで待ちます。

「無効なクラスタリング設定：H.323 モードを有効にする必要があります。クラスタリングはピア間で H.323 通信を使用します (Invalid clustering configuration: H.323 mode must be turned On - clustering uses H.323 communications between peers) 」

H.323 モードがオンになっていることを確認します (**[設定 (Configuration) ] > [プロトコル (Protocols) ] > [H.323]** を参照してください) 。

「VCS データベース障害：シスコのサポート担当者に連絡してください (VCS database failure: Please contact your Cisco support representative) 」

サポート担当者は以下のステップを通じてサポートします。

1. システムのスナップショットを作成し、サポート担当者に提供します。
2. 「[クラスタからのライブ ピアの完全な削除 \(27 ページ\)](#)」に従いクラスタから VCS を削除します。
3. その VCS で以前作成したバックアップを復元して、VCS のデータベースを復元します。
4. 「[クラスタへのピアの追加 \(16 ページ\)](#)」に従いクラスタに VCS を戻します。



データベースが復元しない場合、次の 2 番目の方式を使用できます。

1. システム スナップショットを作成し、TAC に提供します。
2. 「[クラスタからのライブ ピアの完全な削除 \(27 ページ\)](#)」に従いクラスタから VCS を削除します。
3. root としてログインして、「`clusterdb_destroy_and_purge_data.sh`」を実行します。
4. その VCS で以前作成したバックアップを復元して、VCS のデータベースを復元します。
5. 「[クラスタへのピアの追加 \(16 ページ\)](#)」に従いクラスタに VCS を戻します。

**注**：`clusterdb_destroy_and_purge_data.sh` は危険ですので、このコマンドは、サポート担当者の指示に従って使用してください。

## Cisco TMS 警告

### Cisco TMS クラスタ診断

Cisco TMS クラスタ診断レポートで、VCS ピアの設定が異なる場合、各 VCS の `https://<ip address>/alternatesconfiguration.xml` の出力を比較します。

これらの違いを手動で確認するには、Unix/Linux システムで、次のコマンドを実行します。

```
wget --user=admin --password=<password> --no-check-certificate https://<IP or FQDN of VCS>/alternatesconfiguration.xml
```

これを各 VCS ピアで実行し、`diff` を使用して、違いを確認します。

### Conference Factory テンプレートが複製されない

これは意図された結果です。Conference Factory %% 値は、クラスタ ピア間で共有されません。Conference Factory アプリケーション設定は、クラスタ間で複製されません。

「[付録 5：クラスタリングによる他の VCS アプリケーションへの影響 \(52 ページ\)](#)」を参照してください。

### VCS の外部マネージャ プロトコルが強制的に HTTPS に設定される

Cisco TMS は、接続システムに特定の管理設定を強制するよう設定できます。たとえば、VCS はフィードバックに HTTPS を使用できます。これを有効にすると、Cisco TMS は (Cisco TMS により指定された期間にわたり) VCS の **[システム (System)]** > **[外部マネージャ (External Manager)]** の **[プロトコル (Protocol)]** を **[HTTPS]** に再設定します。

Cisco TMS にフィードバックを供給するため VCS に HTTPS を使用する必要がある場合は、「[付録 6：Cisco TMS への VCS の追加 \(53 ページ\)](#)」で証明書のセットアップ方法を確認してください。

次の場合、Cisco TMS は、VCS に HTTPS を強制設定します。

- **[TMS サービス (TMS Services)] > [システム上の管理設定の強制 (Enforce Management Settings on Systems)]** が **[オン (On)]** になっている (**[管理ツール (Administrative Tools)] > [設定 (Configuration)] > [ネットワーク設定 (Network settings)]**)

かつ

- **[機密保護機能付き専用装置通信 (Secure-Only Device Communication)] > [機密保護機能付き専用装置通信 (Secure-Only Device Communication)]** が **[オン (On)]** になっている (**[管理ツール (Administrative Tools)] > [設定 (Configuration)] > [ネットワーク設定 (Network settings)]**)

Cisco TMS で管理設定を強制設定する必要がない場合、**[システム上の管理設定の強制 (Enforce Management Settings on Systems)]** を **[オフ (Off)]** に設定します。

Cisco VCS で TMS へのフィードバックの提供に HTTPS を使用する必要がない場合 (HTTP で十分な場合)、**[機密保護機能付き専用装置通信 (Secure-Only Device Communication)]** を **[オフ (Off)]** に設定します。

## 高度なネットワークを使用したクラスタが正しく複製されない

高度なネットワーキングを使用した VCS Expressway は、LAN 1 インターフェイス経由のみで複製するようにに設計されています。**[システム (System)] > [クラスタリング (Clustering)]** で指定される **[ピア X IP アドレス (Peer x IP Address)]** エントリがすべて、LAN 1 インターフェイスを示していることを確認します。

また、複製されるインターフェイス (LAN 1) で NAT が無効にされている必要があります。

## スタティック NAT を設定したクラスタが正しく複製されない

スタティック NAT を設定した VCS Expressway を使用する場合、クラスタ複製は、NAT デバイスよりも前にある LAN インターフェイスで発生する必要があります。そのため、LAN インターフェイス 1 は、非 NAT インターフェイスでなければならず、**[システム (System)] > [クラスタリング (Clustering)]** で指定される **[ピア X IP アドレス (Peer x IP Address)]** エントリはすべて、LAN 1 インターフェイスを示している必要があります。LAN インターフェイス 2 は、スタティック NAT で設定する必要があります。

## 付録 2：IP ポートおよびプロトコル

### ピア間の外部ファイアウォール

通常、クラスタ ピア間で外部ファイアウォールを使用することはありませんが、使用する場合、次に一覧表示されている IP プロトコルおよび IP ポートが、クラスタの各 VCS ピアおよびすべての VCS ピア間でオープンである必要があります。

VCS ピア間のクラスタ通信：

- PKI（公開キー インフラストラクチャ）キー交換で使用される UDP ポート 500（ISAKMP）
- データベース同期化に使用される IP プロトコル 51（IPSec AH）

VCS ピア間のコール：

- コールに使用される標準 SIP および H.323 シグナリング ポート
- VCS ピア間の待機幅更新に使用される UDP ポート 1719

### ピアのファイアウォール ルール

（このセクションは、外部ファイアウォールには適用されません）

VCS に内蔵されたファイアウォール ルール機能を使用している場合は、このルールが次の接続をブロックしないよう設定されていることを確認してください。

**表 1 クラスタリング接続**

目的	プロトコル	ソース	ポート	接続先	ポート
クラスタ通信	TCP	その他のピア	エフェメラル	このピア	4369-4380
クラスタ リカバリ	UDP	その他のピア	エフェメラル	このピア	4371

## Cisco TelePresence Management Suite Provisioning Extension

Provisioning Extension モードでの VCS ピアおよび Cisco TMS 間のクラスタ通信：

- Cisco TMS（セキュア）の VCS エフェメラル ポートからポート 443、または
- Cisco TMS の VCS エフェメラル ポートからポート 80

**注：**ポート 443 および 80 はデフォルトの値です。別のポートを使用する場合は、Cisco TMS IIS および VCS で設定できます。

## IPSec 通信

VCS クラスタ ピア間での IPSec :

- AES256 は暗号化に使用されます。SHA256 (4096 ビットのキー長) が認証に使用されます。ピアは IP アドレスで識別され、事前共有キーを使用して認証されます。
- メイン モードは IKE 交換中に使用されます。
- Diffie-Hellman グループ「modp4096」が使用されます

## MTU サイズ

VCS でのデフォルトの MTU サイズは 1500 バイトです。通常の状態では、クラスタに対する影響はありません。ただし、クラスタ ピア間にネットワーク要素がある場合 (これは推奨されません)、パス全体で一貫性のある MTU サイズを確保する必要があります。同期パケットのフラグメント化は許可されていないため、ピア間のパスで MTU が小さい場合、クラスタの複製が失敗することがあります。

ピア間のパスでどのネットワーク要素の MTU 値が一番小さいかを判断し、各ピアのクラスタ インターフェイスでその値を使用するように調整します。

## 付録 3：クラスタ名と DNS SRV レコード

DNS SRV を使用してドメインを IP アドレスに変換する場合、次のような多くの利点があります。

- ルックアップの構造に、サービス タイプとプロトコルおよびドメインが含まれます。これにより、共通するドメインを使用して、異なるマシンでホストされる複数の異なるサービスを参照できます（たとえば、HTTP、SIP、H.323）。
- DNS SRV 応答に優先順位とウェイト値が含まれます。これにより、サーバのプライマリ、セカンダリ、ターシャリなどのグループを指定できます。また、各優先順位グループ内で、ウェイトは、各サーバを使用するアクセスの比率を定義します。
- DNS SRV の応答に複数のサーバのプライオリティとウェイトに関する詳細が含まれているため、受信デバイスは、DNS サーバに繰り返し問い合わせる必要なく、インサービス サーバ（サーバがアクセスできない場合）の検索に単一のルックアップを使用できます。（これは、最初のサーバがアクセスできないことが判明している場合に、DNS サーバへの繰り返しルックアップを必要とするラウンド ロビン DNS を使用する場合と対照的です）。

次に、DNS SRV クエリの通常のフォーマットを示します。

- `_service._protocol.<fully.qualified.domain>`

DNS SRV 応答は、次のフォーマットのレコードのセットです。

- `_service._protocol.<fully.qualified.domain>TTL Class SRV Priority Weight Port Target`  
ここで、Target は、宛先を定義する A レコードです。

DNS SRV の詳細は、『*VCS Administrator Guide*』および『*RFC 2782*』を参照してください。

## モバイルおよびリモート アクセスのための DNS SRV 設定

ここでは、パブリック（外部）とローカル（内部）DNS の要件について説明します。詳細については、[Jabber のインストールとアップグレード ガイド ページ](#)の『*Cisco Jabber Planning Guide*』（該当するバージョン）を参照してください。

### パブリック DNS

エンドポイントが Mobile & Remote Access に使用する VCS Expressway を検出できるように、パブリック（外部）DNS は `_collab-edge._tls.<domain>` SRV レコードで設定する必要があります。SIP サービス レコードも必要です（Mobile & Remote Access だけでなく一般的な導入にも必要です）。たとえば、2 つの VCS Expressway システムのクラスタの場合は、次のようになります。

ドメイン	サービス	プロトコル	プライオリティ	ウェイト	ポート	ターゲット ホスト
example.com	collab-edge	tls	10	10	8443	vcse1.example.com
example.com	collab-edge	tls	10	10	8443	vcse2.example.com
example.com	sips	tcp	10	10	5061	vcse1.example.com
example.com	sips	tcp	10	10	5061	vcse2.example.com

## ローカル DNS

ローカル（内部）DNS には `_cisco-uds._tcp.<domain>` SRV レコードが必要です。次に例を示します。

ドメイン	サービス	プロトコル	プライオリティ	ウェイト	ポート	ターゲット ホスト
example.com	cisco-uds	tcp	10	10	8443	cucmserver1.example.com
example.com	cisco-uds	tcp	10	10	8443	cucmserver2.example.com

`cisco-uds` SRV レコードが内部ネットワークの外側で解決できないことを確認します。解決できてしまうと、Jabber クライアントは、VCS Expressway で Mobile & Remote Access のネゴシエーションを開始しません。

**注：** Mobile & Remote Access で使用されるすべてのユニファイド コミュニケーション ノードで、前方ルックアップと逆ルックアップの両方の内部 DNS レコードを作成することを強く推奨します。これにより、IP アドレスが FQDN の代わりに使用されている場合、VCS Control がノードを検出することができます。

## 従来のビデオ会議の導入のための DNS SRV 設定

次に、VCS で使用される sip (RFC 3263) および H.323 の DNS SRV クエリのフォーマットを示します。

- `_sips._tcp.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`
- `_sip._udp.<fully.qualified.domain>`：ビデオ コールには推奨されません。オーディオ専用コールのみに使用してください。
- `_h323ls._udp.<fully.qualified.domain>`：LRQ などの UDP の場所（RAS）シグナリングに使用します。
- `_h323cs._tcp.<fully.qualified.domain>`：H.323 コール シグナリングに使用します。

次に、エンドポイントにより通常使用される sip (RFC 3263) および H.323 の DNS SRV クエリのフォーマットを示します。

- `_sips._tcp.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`
- `_sip._udp.<fully.qualified.domain>`：ビデオ コールには推奨されません。オーディオ専用コールのみに使用してください。
- `_h323ls._udp.<fully.qualified.domain>`：LRQ などの UDP の場所（RAS）シグナリングに使用します。
- `_h323cs._tcp.<fully.qualified.domain>`：H.323 コール シグナリングに使用します。
- `_h323rs._udp.<fully.qualified.domain>`：H.323 登録に使用します。

UDP がビデオ シグナリング向けに推奨されたトランスポート メディアではないことに注意してください。ビデオ システムの SIP メッセージングはデータグラム ベース（ストリーム ベースではなく）のトランスポートを信頼できる形で続行するには大きすぎます。

VCS のクラスタ名 ([システム (System) ] > [クラスタリング (Clustering) ] ページで設定) は、VCS クラスタを指す DNS SRV レコードで指定された `<fully.qualified.domain>` のようになります。

## 例

example.com の VCS-E クラスタ（2 ピア）の DNS SRV レコード

引数の説明

- VCS Expressway ピア 1 の FQDN : vcse1.example.com
- VCS Expressway ピア 2 の FQDN : vcse2.example.com
- VCS Expressway クラスタの FQDN : example.com

```
_sips._tcp.example.com.86400 IN SRV 1 1 5061 vcse1.example.com.
_sips._tcp.example.com.86400 IN SRV 1 1 5061 vcse2.example.com.

_sip._tcp.example.com.86400 IN SRV 1 1 5060 vcse1.example.com.
_sip._tcp.example.com.86400 IN SRV 1 1 5060 vcse2.example.com.

_h323ls._udp.example.com.86400 IN SRV 1 1 1719 vcse1.example.com.
_h323ls._udp.example.com.86400 IN SRV 1 1 1719 vcse2.example.com.

_h323cs._tcp.example.com.86400 IN SRV 1 1 1720 vcse1.example.com.
_h323cs._tcp.example.com.86400 IN SRV 1 1 1720 vcse2.example.com.

_h323rs._udp.example.com.86400 IN SRV 1 1 1719 vcse1.example.com.
_h323rs._udp.example.com.86400 IN SRV 1 1 1719 vcse2.example.com.
```

次の点に注意してください。

- プライオリティはすべて同じです。1 つのプライマリ クラスタから別のクラスタ（セカンダリ）へのフェールオーバーを許可する異なるクラスタが設定されている場合は、異なるプライオリティのみを使用します。この場合は、プライマリ クラスタのピアに 1 つの値が必要であり、その他（セカンダリ）クラスタのピアに、より大きい値が必要です。
- 各ピアが均等に使用されるように、ウェイトは同じである必要があります。

## SIP DNS SRV をサポートするエンドポイント

バージョン 4.0 より前の Jabber ビデオでのサポート :

- \_sip.\_tls.<fully.qualified.domain>
- \_sip.\_tcp.<fully.qualified.domain>

バージョン 4.0 以降の Jabber ビデオでのサポート :

- \_sips.\_tcp.<fully.qualified.domain>
- \_sip.\_tcp.<fully.qualified.domain>

E20 バージョン TE2.1 でのサポート :

- \_sips.\_tls.<fully.qualified.domain>
- \_sip.\_tcp.<fully.qualified.domain>

MXP バージョン F8.2 でのサポート :

- `_sip._tls.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`

T150 バージョン L6.0 でのサポート：

- `_sip._tls.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`

TC4.0 よりも前の C-Series バージョンでのサポート：

- `_sip._tls.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`

C-Series バージョン TC4.0 以降でのサポート：

- `_sips._tcp.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`

Cisco TelePresence MCU でのサポート：

- `_sips._tcp.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`

必要な SIP DNS SRV レコード：

- `_sips._tcp.<fully.qualified.domain>` Jabber ビデオ（4.0 以降）、C-Series（TC4.0 以降）、VCS、MCU
- `_sips._tls.<fully.qualified.domain>` E20 から TE2.1
- `_sip._tls.<fully.qualified.domain>` MXP から F8.2、T150 から L6.0、4.0 より前の Jabber ビデオ、TC4.0 より前の CSeries
- `_sip._tcp.<fully.qualified.domain>` TCP のすべての製品

## DNS SRV の設定の確認

### Web インターフェイスを使用した DNS SRV 設定の確認

1. [メンテナンス (Maintenance)] > [ツール (Tools)] > [ネットワーク ユーティリティ (Network utilities)] > [DNS ルックアップ (DNS lookup)] に移動します。
2. [ホスト (Host)] フィールドに SRV のパスを入力します。
3. [ルックアップ (Lookup)] をクリックします。



**DNS lookup** You are here: [Maintenance](#) > [Tools](#) > [Network utilities](#) > [DNS lookup](#)

DNS lookup

Host

Query type

Check against the following DNS servers

## nslookup

```
nslookup -query=SRV _sip._tcp.example.com
```

## Dig

```
dig _sip._tcp.example.com SRV
```

```
; <<>> DiG 9.4.1 <<>> _sip._tcp.example.com SRV
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44952
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
;_sip._tcp.example.com.IN      SRV

;; ANSWER SECTION:
_sip._tcp.example.com.1183    IN      SRV     1 0 5060 vcse1.example.com.
_sip._tcp.example.com.1183    IN      SRV     1 0 5060 vcse2.example.com.

;; AUTHORITY SECTION:
example.com.87450      IN      NS      ns1.mydyndns.org.
example.com.87450      IN      NS      ns2.mydyndns.org.

;; ADDITIONAL SECTION:
vcse1.example.com.1536    IN      A       194.73.59.53
vcse2.example.com.1376    IN      A       194.73.59.54
ns1.mydyndns.org.75      IN      A       204.13.248.76
ns2.mydyndns.org.10037   IN      A       204.13.249.76

;; Query time: 0 msec
~ #
```

## 付録 4：NAPTR レコード

NAPTR レコードは、通常、電子メール、SIP、H.323 など、宛先 URI へのさまざまな接続方式を指定するときに使用されます。また、たとえば、SIP TCP または SIP UDP より SIP TLS の使用を優先するなど、接続タイプに使用する優先順位を指定するときにも使用されます。

NAPTR レコードは、電話番号をダイヤル可能 URI に変換するときに、ENUM で使用されます（ENUM の詳細については、『[ENUM Dialing on VCS Deployment Guide](#)』を参照してください）。

### NAPTR レコード フォーマット

例：example.com への SIP アクセス、および 557120、557121、557122 の ENUM ルックアップ

\$ORIGIN example.com.

```
IN  NAPTR  10  100  "s"  "SIPS+D2T"  ""  _sips._tcp.example.com.
IN  NAPTR  12  100  "s"  "SIP+D2T"   ""  _sip._tcp.example.com.
IN  NAPTR  14  100  "s"  "SIP+D2U"   ""  _sip._udp.example.com.
```

\$ORIGIN www.example.com.

```
IN  NAPTR  10  100  "s"  "http+I2R"  ""  _http._tcp.example.com.
IN  NAPTR  10  100  "s"  "ftp+I2R"   ""  _ftp._tcp.example.com.
```

\$ORIGIN 0.2.1.7.5.5.enum.lookup.com.

```
IN  NAPTR  10  100  "u"  "E2U+sip"   "!^.*$!john.smith@tandberg.com!".
IN  NAPTR  12  100  "u"  "E2U+h323"  "!^.*$!john.smith@tandberg.com!".
IN  NAPTR  10  100  "u"  "mailto+E2U" "!^.*$!mailto:john.smith@tandberg.com!".
```

\$ORIGIN 1.2.1.7.5.5.enum.lookup.com.

```
IN  NAPTR  10  100  "u"  "E2U+sip"   "!^.*$!mary.jones@tandberg.com!".
```

\$ORIGIN 2.2.1.7.5.5.enum.lookup.com.

```
IN  NAPTR  10  100  "u"  "E2U+h323"  "!^.*$!peter.archibald@myco.com!".
```

```
IN = Internet routing
  NAPTR = record type
    10 = order value (use lowest order value first)
    100 = preference value if multiple entries have the same order value
    "u" = the result is a routable URI
    "s" = the result is a DNS SRV record
    "a" = the result is an 'A' or 'AAAA' record
    "E2U+sip" to make SIP call
    "E2U+h323" to make h.323 call
    Regular expression:
    ! = delimiter
    "" = no expression used
    ... usual Regex expressions can be used
    Replace field; .= not used
```

## ENUM NAPTR レコードの検索

```
dig 4.3.7.8.enum4.example.com.NAPTR

; <<>> ;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38428
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;4.3.7.8.enum4.example.com.IN    NAPTR

;; ANSWER SECTION:
4.3.7.8.enum4.example.com.60 IN NAPTR 10 100 "u" "E2U+sip" "!^.*$!bob@example.com!".
4.3.7.8.enum4.example.com.60 IN NAPTR 10 100 "u" "E2U+h323" "!^.*$!bob@example.com!".

;; AUTHORITY SECTION:
enum4.example.com.60      IN      NS      int-server1.example.com.

;; ADDITIONAL SECTION:
int-server1.example.com.3600 IN A      10.44.9.144
int-server1.example.com.3600 IN AAAA   3ffe:80ee:3706::9:144

;; Query time: 0 msec
```

## ドメイン NAPTR レコードの検索

例：エンドポイントがパブリック（外部）ネットワークにあることを検出できるようにする NAPTR レコードフラグ「s」は、「外部」であることを示す「se」に拡張されます。

```
~ # dig -t NAPTR example.com

; <<>> DiG 9.4.1 <<>> -t NAPTR example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1895
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 6, ADDITIONAL: 4

;; QUESTION SECTION:
;example.com.IN    NAPTR

;; ANSWER SECTION:
example.com.2      IN    NAPTR  50 50 "se" "SIPS+D2T" "" _sips_tcp.example.com.
example.com.2      IN    NAPTR  90 50 "se" "SIP+D2T" "" _sip_tcp.example.com.
example.com.2      IN    NAPTR  100 50 "se" "SIP+D2U" "" _sip_udp.example.com.

;; AUTHORITY SECTION:
example.com.320069 IN     NS     nserver2.example.com.
example.com.320069 IN     NS     nserver.euro.example.com.
example.com.320069 IN     NS     nserver.example.com.
example.com.320069 IN     NS     nserver3.example.com.
example.com.320069 IN     NS     nserver4.example.com.
example.com.320069 IN     NS     nserver.asia.example.com.

;; ADDITIONAL SECTION:
nserver.example.com.56190 IN  A      17.111.10.50
nserver2.example.com.57247 IN  A      17.111.10.59
nserver3.example.com.57581 IN  A      17.22.14.50
nserver4.example.com.57452 IN  A      17.22.14.59

;; Query time: 11 msec
```

## 付録 5：クラスタリングによる他の VCS アプリケーションへの影響

### Conference Factory (Multiway™)

Conference Factory (Multiway) をクラスタで使用する場合は、以下の点に注意してください。

- Conference Factory アプリケーション設定はクラスタ間で複製されません。
- Conference Factory テンプレートは、各 VCS ピアで異なる必要があります。

Multiway をサポートするようにクラスタを設定するには、次の手順を実行します。

1. 各ピアで**同じ** Conference Factory エイリアスを設定します（エイリアスは、Multiway 会議を開始するときにエンドポイントによりコールされます）。
2. 各ピアで**異なる** Conference Factory テンプレートを設定します（これにより、各ピアで独自の Multiway 会議 ID が生成されます）。

たとえば、アドホック会議の MCU サービス プレフィックスが 775 の場合、プライマリ VCS は `775001%%@domain` のテンプレート、ピア 2 は `775002%%@domain` のテンプレート、ピア 3 は `775003%%@domain` のテンプレートを使用する必要があります。これにより、どの VCS が会議 ID を提供しても、この VCS には他の VCS が提供する可能性がある会議 ID を提供することはできなくなります。

これは、ネットワーク間でも同様です。ネットワークで Conference Factory 機能を提供する複数の VCS または VCS クラスタがある場合、各 VCS およびすべての VCS は、同じ会議 ID が使用されないように、独自の範囲の値を提供する必要があります。

詳細については、『[Cisco TelePresence Multiway Deployment Guide](#)』を参照してください。

### Microsoft Lync

Lync Server が VCS クラスタで稼働するように設定されている場合は、『[Microsoft Lync and VCS Deployment Guide](#)』を参照してください。

## 付録 6：Cisco TMS への VCS の追加

VCS で、次の手順を実行します。

1. **[システム (System)] > [SNMP]** の順に選択し、以下を確認します。
  1. **[SNMP モード (SNMP mode)]** が *[v3 プラス Cisco TMS サポート (v3 plus Cisco TMS support)]* または *[v2c]* に設定されている。
  2. **[コミュニティ名 (Community name)]** が *[パブリック (public)]* に設定されている。  
 (SNMP が無効にされていた場合、再起動が必要なことを示すアラームが表示される場合があります。この場合は、**[メンテナンス (Maintenance)] > [再起動オプション (Restart options)]** を使ってシステムを再起動してください。)
 

複数のピアを再起動する必要がある場合、次のピアを再起動する前に Web インターフェイスからピアにアクセスできることを確認してから、各ピアを再起動します。
2. **[システム (System)] > [外部マネージャ (External Manager)]** の順に選択し、以下を確認します。
  1. **[アドレス (Address)]** が Cisco TMS の IP アドレスまたは FQDN に設定されている。
  2. **[パス (Path)]** が *tms/public/external/management/SystemManagementService.asmx* に設定されている
  3. **[プロトコル (Protocol)]** が *[HTTPS]* で **[証明書検証モード (Certificate verification mode)]** が *[オン (On)]* の場合は、関連する証明書をロードしないと接続が「アクティブ (Active)」になりません。詳細については『*Implementing Secure Management*』(文書参照番号 D50520) を参照してください。  
**[プロトコル (Protocol)]** が *[HTTP]*、または **[証明書検証モード (Certificate verification mode)]** が *[オフ (Off)]* の場合、証明書をロードする必要はありません。
3. **[保存 (Save)]** をクリックします。

**[外部マネージャ (External Manager)]** ページの **[ステータス (Status)]** セクションの **[状態 (State)]** が **[アクティブ (Active)]** または **[初期化中 (Initialising)]** になります。<sup>1</sup>

Cisco TMS で次の手順を実行します。

1. **[システム (Systems)] > [ナビゲータ (Navigator)]** を選択します。
2. VCS を含める適切なフォルダを選択 (または作成) します (次の例の場合、フォルダの名前は「Cluster」です)。

<sup>1</sup> Cisco TMS で、プロトコルが HTTPS に強制設定されることがあります。この設定は、**[管理ツール (Administrative Tools)] > [設定 (Configuration)] > [ネットワーク設定 (Network settings)]** で確認できます。**[TMS サービス (TMS Services)]** セクションで、**[システム上の管理設定の強制 (Enforce Management Settings on Systems)]** が *[オン (On)]* に設定され、**[機密保護機能付き専用装置通信 (Secure-Only Device Communication)]** セクションで **[機密保護機能付き専用装置通信 (Secure-Only Device Communication)]** が *[オン (On)]* の場合、プロトコルは HTTPS に強制設定されます。



3. **[システムの追加 (Add Systems)]** をクリックします。
4. セクション **[1. IP アドレスまたは DNS 名でシステムを指定してください (1. Specify Systems by IP addresses or DNS names)]** で、VCS の IP アドレスまたは DNS 名を入力します。
5. **[次へ (Next)]** をクリックします。
6. **[✓システムが追加されました (System added)]** を確認します。  
「間違ったパスワード (Wrong Password)」などのエラーが発生した場合、**[システムの編集 (Edit System)]** リンクをクリックして、問題を修正します (VCS の root パスワードを入力します)。
7. **[システム追加の終了 (Finish Adding Systems)]** または **[警告を無視してシステムを追加 (Add System despite warnings)]**、**[システムをさらに追加 (Add More Systems)]** のうち、適切なオプションをクリックします。
8. 「Could not connect to system.Details: No SNMP response」が報告された場合、**[接続 (Connection)]** タブに移動して、**[SNMP コミュニティ名の取得 (SNMP Get Community Name)]** に「public」と入力し、**[保存/試行 (Save/Try)]** をクリックします。
9. VCS パスワードがデフォルト以外の場合、**[接続 (Connection)]** タブまたは **[設定 (Settings)]** > **[設定の編集 (Edit Settings)]** で設定します。

VCS が Cisco TMS で設定されている場合、IP アドレスが正しいか確認します (Cisco TMS で **[システム (Systems)]** > **[ナビゲータ (Navigator)]** (および必須サブフォルダ) に移動し、VCS を選択して、**[接続 (Connection)]** タブから、**[IP アドレス (IP Address)]** フィールドを確認します)。

**VCS で次の手順を実行します。**

**[システム (System)]** > **[外部マネージャ (External manager)]** に進み、**[状態 (State)]** が **[アクティブ (Active)]** になっていることを確認します。

## 付録 7：クラスタを使用するためのエンドポイントの設定

エンドポイントを設定するときに、クラスタのすべての VCS ピアを認識するように設定することをお勧めします。このように設定することで、初期登録以降で、VCS ピアとの接続が失われた場合、クラスタの別のピアに登録して、使用することができます。

SIP および H.323 エンドポイントは異なります。ここでは、使用できる方式およびこれらの優先順位について説明します。

DNS SRV およびラウンドロビン DNS の詳細については、『*VCS Administrator Guide*』の URI ダイヤリングに関するセクションを参照してください。

また、「[付録 3：クラスタ名と DNS SRV レコード \(45 ページ\)](#)」も参照してください。

### SIP エンドポイント

次に、1 つ以上の VCS クラスタ ピアがアクセスできなくなった場合に VCS のクラスタとのエンドポイントの接続のレジリエンスを提供するオプションを推奨順にリストします。選択するオプションは、使用するエンドポイントがサポートする機能により異なります。

#### オプション 1：SIP アウトバウンド (推奨)

SIP アウトバウンドでは、エンドポイントを複数の VCS ピアに同時に登録できるように設定できます。この利点は、エンドポイントとピア間の接続が失われた場合でも、エンドポイントと他のピア間の接続が残ります。両方のピアに同時に登録しているエンドポイントでは、登録の失敗を別のピアに登録する前に認識するので、サービスは中断しません。そのため、エンドポイントは到達不能になりません。

SIP アウトバウンドの設定は、エンドポイントにより異なりますが、通常、次のように設定します。

- プロキシ 1
  - [サーバ検出 (Server discovery)] = [手動 (Manual)]
  - [サーバアドレス (Server Address)] =  
[クラスタ ピアの DNS 名 (DNS name of cluster peer)] または  
[クラスタ ピアの IP アドレス (IP address of cluster peer)]
- プロキシ 2
  - [サーバ検出 (Server discovery)] = [手動 (Manual)]
  - [サーバアドレス (Server Address)] =  
[異なるクラスタ ピアの DNS 名 (DNS name of a different cluster peer)] または  
[異なるクラスタ ピアの IP アドレス (IP address of a different cluster peer)]
- [アウトバウンド (Outbound)] = [オン (On)]

## オプション 2 : DNS SRV (優先順位第 2 位)

このオプションを使用するには、各クラスタ ピアで同じウェイトと優先順位を定義する VCS クラスタの DNS 名で利用できる DNS SRV レコードが必要です。

各 SIP エンドポイントで、[SIP 設定 (SIP Settings)] を次のように設定します。

- [サーバ検出 (Server discovery)] = [手動 (Manual)]
- [サーバアドレス (Server Address)] = VCS クラスタの DNS 名

エンドポイントが DNS SRV をサポートする場合、エンドポイントは起動時に DNS SRV 要求を送信して、各クラスタ ピアで同じウェイトと優先順位を定義する DNS SRV レコードを受け取ります。

次に、エンドポイントは、関連するクラスタ ピアへの登録を試行します (優先順位とウェイトが考慮されます)。このピアが使用できない場合、エンドポイントは、同じ優先順位の別のピアへの登録を試行します。同じ優先順位のすべてのピアで登録を試行すると、次に優先順位の低いピアへの登録を試行します。

これは、エンドポイントが VCS に登録できるまで繰り返されます。

エンドポイントは、最初に登録した VCS を再登録およびコールに使用します。エンドポイントは、その VCS との接続を失った場合、DNS SRV エントリを使用して、優先順位の高い VCS から、登録先の新しい VCS を探します。

DNS SRV キャッシュ タイムアウトは、DNS トラフィックを最小化するために、比較的長時間 (たとえば 24 時間) に設定する必要があります。

## オプション 3 : DNS ラウンドロビン (優先順位第 3 位)

このオプションを使用するには、IP アドレスのラウンドロビン リストを提供する VCS クラスタの DNS 名で利用できる DNS A レコードが必要です。

各 SIP エンドポイントで、[SIP 設定 (SIP Settings)] を次のように設定します。

- [サーバ検出 (Server discovery)] = [手動 (Manual)]
- [サーバアドレス (Server Address)] = VCS クラスタの DNS 名

エンドポイントが DNS SRV をサポートしない場合、エンドポイントは起動時に、DNS A レコード ルックアップを実行します。DNS サーバは、各クラスタ ピア メンバーをラウンドロビン リストに定義し、ラウンドロビン DNS をサポートするように設定されます。

エンドポイントは、DNS ルックアップにより提供されたアドレスを使用し、関連するクラスタ ピアへの登録を試行します。そのアドレスが使用できない場合、エンドポイントは、もう一度 DNS ルックアップを実行して、提供される新しい VCS ピアへの接続を試行します (DNS サーバは、次のクラスタ ピアの IP アドレスを提供します)。

これは、エンドポイントが VCS に登録できるまで繰り返されます。



エンドポイントは、最初に登録した VCS を再登録およびコールに使用します。エンドポイントは、その VCS との接続を失うと、もう一度 DNS ルックアップを実行して、登録先の新しい VCS を探します（DNS サーバは、VCS をラウンドロビン方式で提供します）。

DNS キャッシュ タイムアウトは、比較的短時間（たとえば 1 分以内）に設定する必要があります。これにより、エンドポイントは、VCS にアクセスできない場合、すぐに別の VCS を使用します。

#### オプション 4：スタティック IP（優先順位最下位）

このオプションは、VCS クラスタに DNS 名がない場合に使用します。

各 SIP エンドポイントで、[SIP 設定（SIP Settings）] を次のように設定します。

- [サーバ検出（Server discovery）] = [手動（Manual）]
- [サーバアドレス（Server Address）] = VCS ピアの IP アドレス

エンドポイントは起動時に、指定された IP アドレスの VCS への登録を試行します。この VCS が使用できない場合、エンドポイントは、一定の間隔で試行を続けます。

これは、エンドポイントが VCS に登録できるまで繰り返されます。

エンドポイントは、最初に登録した VCS を再登録およびコールに使用します。エンドポイントは、接続を失った場合でも、再びアクセスできるようになるまで、その VCS への登録を試行します。

## H.323 エンドポイント

次に、1 つ以上の VCS クラスタ ピアがアクセスできなくなった場合に VCS のクラスタとのエンドポイントの接続のレジリエンスを提供するオプションを推奨順にリストします。選択するオプションは、使用するエンドポイントがサポートする機能により異なります。

#### オプション 1：DNS SRV（推奨）

このオプションを使用するには、各クラスタ ピアで同じウェイトと優先順位を定義する VCS クラスタの DNS 名で使用できる DNS SRV レコードが必要です。

各 H.323 エンドポイントで、[ゲートキーパー設定（Gatekeeper Settings）] を次のように設定します。

- [検出（Discovery）] = [手動（Manual）]
- [IP アドレス（IP Address）] = VCS クラスタの DNS 名

エンドポイントが DNS SRV をサポートする場合、エンドポイントは起動時に DNS SRV 要求を送信して、各クラスタ ピアで同じウェイトと優先順位を定義する DNS SRV レコードを受け取ります。

次に、エンドポイントは、関連するクラスタ ピアへの登録を試行します（優先順位とウェイトが考慮されます）。このピアが使用できない場合、エンドポイントは、同じ優先順位の別のピアへの登録を試行します。同じ優先順位のすべてのピアで登録を試行すると、次に優先順位の低い（大きい数字の）ピアへの登録を試行します。

これは、エンドポイントが VCS に登録できるまで繰り返されます。VCS に登録すると、VCS は、VCS クラスタ ピア メンバーのリストを含む H.323 [代替ゲートキーパー (Alternate Gatekeepers) ] リストに応答します。

エンドポイントは、最初に登録した VCS を再登録およびコールに使用します。エンドポイントは、その VCS との接続を失うと、提供されたリストから [代替ゲートキーパー (Alternate Gatekeepers) ] を選択します。

DNS SRV キャッシュ タイムアウトは、DNS トラフィックを最小化するために、比較的長時間（たとえば 24 時間）に設定する必要があります。

## オプション 2 : DNS ラウンドロビン (優先順位第 2 位)

このオプションを使用するには、IP アドレスのラウンドロビン リストを提供する VCS クラスタの DNS 名で使用できる DNS A レコードが必要です。

各 H.323 エンドポイントで、[ゲートキーパー設定 (Gatekeeper Settings) ] を次のように設定します。

- [検出 (Discovery) ] = [手動 (Manual) ]
- [IP アドレス (IP Address) ] = VCS クラスタの DNS 名

エンドポイントが DNS SRV をサポートしない場合、エンドポイントは起動時に、DNS A レコード ルックアップを実行します。DNS サーバは、各クラスタ ピア メンバーをラウンドロビン リストに定義し、ラウンドロビン DNS をサポートするように設定されます。

エンドポイントは、DNS ルックアップにより提供されたアドレスを使用し、関連するクラスタ ピアへの登録を試行します。そのピアが使用できない場合、エンドポイントは、もう一度 DNS ルックアップを実行して、提供される新しい VCS ピアへの接続を試行します（DNS サーバは、次のクラスタ ピアの IP アドレスを提供します）。

これは、エンドポイントが VCS に登録できるまで繰り返されます。VCS に登録すると、Cisco は、VCS クラスタ ピア メンバーのリストを含む H.323 [代替ゲートキーパー (Alternate Gatekeepers) ] リストに応答します。

エンドポイントは、最初に登録した VCS を再登録およびコールに使用します。エンドポイントは、接続を失うと、提供されたリストから [代替ゲートキーパー (Alternate Gatekeepers) ] を選択します。

DNS キャッシュ タイムアウトは、比較的短時間（たとえば 1 分未満）に設定する必要があります。これにより、エンドポイントは、起動時に VCS に到達できない場合、すぐに別の VCS を使用します。

### オプション 3：スタティック IP（優先順位最下位）

このオプションは、VCS クラスタに DNS 名がない場合に使用します。

各 H.323 エンドポイントで、[ゲートキーパー設定（Gatekeeper Settings）] を次のように設定します。

- [検出（Discovery）] = [手動（Manual）]
- [IP アドレス（IP Address）] = VCS ピアの IP アドレス

エンドポイントは起動時に、指定された IP アドレスの VCS への登録を試行します。この VCS が使用できない場合、エンドポイントは、一定の間隔で試行を続けます。

これは、エンドポイントが VCS に登録できるまで繰り返されます。VCS に登録すると、VCS は、VCS クラスタ ピア メンバーのリストを含む H.323 [代替ゲートキーパー（Alternate Gatekeepers）] リストに応答します。

エンドポイントは、最初に登録した VCS を再登録およびコールに使用します。エンドポイントは、接続を失うと、提供されたリストから [代替ゲートキーパー（Alternate Gatekeepers）] を選択します。

## 付録 8 : VCS の旧バージョンから X8.7 へのアップグレード

このセクションでは、VCS の旧バージョンから X8.7 へのアップグレード方法を説明します。

### TMS Agent レガシー モードにある X7.1 または X7.2 クラスタの X8.7 へのアップグレード

X8 以降のバージョンでは、TMS Agent レガシー モードはサポートされていません。TMS Agent レガシー モードで実行するクラスタから X8 以降のクラスタに直接アップグレードすることはできません。

X8.7 にアップグレードするには、次の手順を実行する必要があります。

1. 『Cisco TelePresence Management Suite Provisioning Extension Deployment Guide』の手順に従い、X7.1 または X7.2 クラスタを Provisioning Extension モードにアップグレードします。
2. 「[X7.1 \(またはそれ以降の\) クラスタの X8.7 へのアップグレード \(6 ページ\)](#)」の手順に従い X8.7 へのアップグレードを行います。

### X6.0 または X6.1、X7.0、X7.0.n クラスタの X8.7 へのアップグレード

デバイスのプロビジョニングまたは FindMe に Cisco TMS を使用している場合は、次の手順を実行します。

- X8 以降のバージョンでは、TMS Agent レガシー モードはサポートされていません。
- TMS Agent レガシー モードで実行するクラスタから X8 以降のクラスタに直接アップグレードすることはできません。

X8.7 にアップグレードするには、次の手順を実行する必要があります。

1. 『VCS Cluster Creation and Maintenance Deployment Guide (X7.2)』の手順に従い、クラスタを X7.2 にアップグレードします。
2. デバイスのプロビジョニングまたは FindMe 用に Cisco TMS を使用している場合は、『Cisco TelePresence Management Suite Provisioning Extension Deployment Guide』に従って Provisioning Extension モードへのアップグレードを行います。
3. 「[X7.1 \(またはそれ以降の\) クラスタの X8.7 へのアップグレード \(6 ページ\)](#)」の手順に従い X8.7 へのアップグレードを行います。

### X5.1 または X5.1.1、X5.2 クラスタの X8.7 へのアップグレード

X5.1/X5.1.1/X5.2 クラスタから X8.7 クラスタに直接アップグレードすることはできません。過去の VCS バージョンを通じて段階的にアップグレードする必要があります。

X8.7 にアップグレードするには、次の手順を実行する必要があります。

1. 『*VCS Cluster Creation and Maintenance Deployment Guide (X6.1)*』の手順に従い、クラスタを X6.1 にアップグレードします。
2. 『*VCS Cluster Creation and Maintenance Deployment Guide (X7.2)*』の手順に従い、クラスタを X7.2 にアップグレードします。
3. デバイスのプロビジョニングまたは FindMe 用に Cisco TMS を使用している場合は、『*Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*』に従って Provisioning Extension モードへのアップグレードを行います。
4. 「[X7.1 \(またはそれ以降の\) クラスタの X8.7 へのアップグレード \(6 ページ\)](#)」の手順に従い X8.7 へのアップグレードを行います。

## X1/X2 代替または X3/X4/X5.0 クラスタから X8.7 へのアップグレード

X1/X2 代替または X3/X4/X5.0 クラスタから X8.7 クラスタに直接アップグレードすることはできません。過去の VCS バージョンを通じて段階的にアップグレードする必要があります。

X8.7 にアップグレードするには、次の手順を実行する必要があります。

1. 『*VCS Cluster Creation and Maintenance Deployment Guide (X5)*』の手順に従い、クラスタを X5.2 にアップグレードします。
2. 『*VCS Cluster Creation and Maintenance Deployment Guide (X6.1)*』の手順に従い、クラスタを X6.1 にアップグレードします。
3. 『*VCS Cluster Creation and Maintenance Deployment Guide (X7.2)*』の手順に従い、クラスタを X7.2 にアップグレードします。
4. デバイスのプロビジョニングまたは FindMe 用に Cisco TMS を使用している場合は、『*Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*』に従って Provisioning Extension モードへのアップグレードを行います。
5. 「[X7.1 \(またはそれ以降の\) クラスタの X8.7 へのアップグレード \(6 ページ\)](#)」の手順に従い X8.7 へのアップグレードを行います。

## マニュアルの変更履歴

次の表に、このマニュアルの変更履歴の要約を示します。

**表 2：本書に対する変更の概要**

日付	説明
2015 年 11 月	X8.7 に関する内容を更新。
2015 年 7 月	X8.6 に関する内容を更新。ピアの置換に関する新たな手順を追加。
2015 年 4 月	X8.5 以降用にメニュー パスを変更。X8.5.2 に合わせて再発行。
2014 年 12 月	X8.5 に関する内容を更新。
2014 年 6 月	X8.2 に合わせて再発行。
2014 年 4 月	VCS X8.1.1 に関する内容を更新： <ul style="list-style-type: none"> <li>「VCS ピアの置換」セクションを追加</li> <li>「IP ポートとプロトコル」の付録を更新</li> </ul>
2013 年 12 月	VCS X8.1 に関する内容を更新、TMS Agent レガシー モード プロビジョニングのサポートの削除を含む。
2012 年 11 月	エンドポイント SIP アウトバウンド設定に VCS クラスタの DNS 名を使用する旨の推奨を削除。
2012 年 8 月	VCS X7.2 に関する内容を更新。
2012 年 3 月	VCS X7.1 に関する内容を更新。
2012 年 1 月	さまざまなマイナー リビジョンおよび説明の適用。
2011 年 10 月	VCS X7.0.n に関する内容を更新。
2011 年 9 月	付録 3 の更新：IP ポートおよびプロトコル番号。
2011 年 8 月	VCS X7.0 に関する内容を更新。
2011 年 5 月	VCS X6.1 に関する内容を更新。
2011 年 2 月	本書が VCS X6.0 のみ、および Cisco TMS 12.6 以降用であることを明記。
2010 年 12 月	VCS X6 に関する内容を更新。
2010 年 10 月	新しいドキュメント スタイルを適用。

---

日付	説明
2010 年 8 月	VCS X5.2 に関する内容を更新。  以前の付録 12 (debian パッケージのアップグレード: X5.1.1 で必要な場合のみ) を新しい付録 12 : NAPTR レコードの概要に変更。
2010 年 5 月	VCS X5.1.1 および Cisco TMS 12.6 に関する内容を更新。
2009 年 12 月	VCS X5 の更新。
2009 年 12 月まで	旧バージョンの VCS のリリース。

## シスコの法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校 (UCB) により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト ([www.cisco.com/go/offices](http://www.cisco.com/go/offices) [英語]) をご覧ください。

© 2015 Cisco Systems, Inc. All rights reserved.

## シスコの商標または登録商標

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.シスコの商標の一覧は [www.cisco.com/web/JP/trademark\\_statement.html](http://www.cisco.com/web/JP/trademark_statement.html) に掲載されています。Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)