Cisco TelePresence Management Suite

インストレーション/アップグレード ガイド

2015 年 12 月

ソフトウェア バージョン 15.1

はじめに

Cisco Telepresence Management Suite（Cisco TMS）は、単一の構造化されたインターフェイスからビデオ会議ネットワークの管理とモニタリングを行うためのポータルです。Cisco TMS は、オンサイトおよびリモートのビデオ システムに対する集中管理と、ビデオ ネットワーク全体に対する導入およびスケジューリングのシステムを提供します。

Cisco TMS は、基本的なテレプレゼンス ネットワーク用のシステム設定を自動化し、追加設定なしで動作します。Cisco TMS の動作を調整して、組織のニーズを満たし、ユーザ権限とネットワーク モデルを設定することができます。これで、Cisco TMS コール処理機能がすべて使用できるようになります。

このマニュアルでは、新規インストールの情報および既存のバージョンのアップグレードとアンインストールの情報を提供します。また、Cisco TMS の新サーバへの移動についての情報を提供します。

注：Cisco TMS を使用する場合、テレプレゼンス ネットワーク上で Cisco TelePresence Manager などの他のテレプレゼンス管理システムを使用しないでください。

関連資料

次の表に、このドキュメントで参照されているドキュメントと Web サイト、および関連するマニュアルを示します。最新バージョンの Cisco Telepresence Management Suite に関するドキュメントはすべて、http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/tsd-products-support-series-home.html で入手できます。

Cisco TMS 拡張に関するマニュアルは、http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/tsd-products-support-series-home.html でご覧いただけます。

表 1　関連マニュアル

タイトル	リンク
Cisco TelePresence Management Suite Release Notes	http://cisco.com
Installing licenses; release and options keys for the Cisco TelePresence Management Suite	http://cisco.com
Cisco TelePresence Management Suite Administrator Guide	http://cisco.com
Cisco TelePresence Management Suite Provisioning Extension Deployment Guides	http://cisco.com
Cisco TelePresence Video Communication Server Cluster Creation and Maintenance Deployment Guide	http://cisco.com

ヒント：すべての Cisco TMS ページの右上隅にある疑問符アイコン（[?]）をクリックすると、Web ヘルプにアクセスできます。

トレーニング

トレーニングはオンラインおよび当社のトレーニング場所で利用できます。シスコが提供するすべてのトレーニングの詳細およびトレーニング オフィスの場所については、www.cisco.com/go/telepresencetraining [英語] を参照してください。

用語集

TelePresence 関連の用語集は tp-tools-web01.cisco.com/start/glossary/ [英語] で入手できます。

前提条件

この章では、Cisco TelePresence Management Suite をインストールまたはアップグレードする前に確認が必要な、ハードウェアとソフトウェアの要件、およびその他の考慮事項と依存関係について説明します。

導入サイズの見積り

Cisco TMS の要件は導入環境の規模や複雑さに応じて増加します。インストールの複雑さは、主にアクティビティの量と、Cisco TMS によって制御される予約可能なエンドポイントの数によって決まります。

次の表を使用して導入環境の相対的なサイズを特定します。複数の条件と一致する場合は、最も高いレベルを適用します。

前提条件

	通常および Cisco BE6000 環境	大規模環境
Cisco TMS	• 制御対象システム数：200 未満 • 同時参加者が最大 100 人 • 同時進行するスケジュール済み会議が最大 50 個	• システム ライセンスを使用するシステム（制御対象システム、Cisco TMS に追加された Unified CM に登録されるシステム、および管理対象外のルーム）数：5,000 未満。このようなシステムを 5,000 を超えて追加することはサポートされていません。 • 同時参加者が最大 1800 人 • 同時進行するスケジュール済み会議が最大 250 個
Cisco TMSXE	Microsoft Exchange で予約可能なエンドポイントが最大 50 個	オンプレミスの Microsoft Exchange で予約可能なエンドポイント数：1,800 未満 または Office 365（またはオンプレミスの Exchange と Office 365 の組み合わせ）で予約可能なエンドポイント数：1,000 未満 Office 365 では、Exchange に対する遅延がオンプレミス導入に比べて一般に大きくなることに注意してください。その結果、Cisco TMSXE で、関連するイベントがすべて処理される前に予約が保存される場合があります。この場合、同じ予約に対して複数の電子メール通知がユーザに送信されます。
Cisco TMSPE	• Collaboration Meeting Room 数：1,000 未満 • Cisco VCS でプロビジョニングされるユーザ数：2,000 未満（注：Cisco VCS のプロビジョニングは BE6000 ではサポートされていません）	• Collaboration Meeting Room 数：48,000 未満 • Cisco VCS でプロビジョニングされるユーザ数：100,000 未満
共存	3 つのアプリケーションと Microsoft SQL Server はすべて共存可能。	• Cisco TMSXE に専用サーバが必要。 • Cisco TMS と Cisco TMSPE は外部 SQL Server を使用する必要あり。

Cisco TMS のパフォーマンスや規模に影響するその他の要因には次のものがあります。

- Cisco TMS の Web インターフェイスにアクセスするユーザの数。
- スケジュールまたは監視されている会議の同時開催。
- アドホック会議モニタリングの使用。
- 複数の拡張またはカスタム クライアントによる Cisco TMSBA の同時使用。予約のスループットは、Cisco TMS の [新しい会議（New Conference）] ページを含むすべてのスケジューリング インターフェイスで共有されます。

実際の予約スピードは、会議のサイズ、機能、および会議のスケジュールの複雑さによって異なります。

前提条件

ハードウェア要件

導入環境のサイズに応じて該当するハードウェア要件を以下で確認してください。

SQL Server を含むすべてのアプリケーションは、以下のハードウェア要件に対応する仕様の仮想マシンにもインストールできます。

通常の導入環境と Cisco Business Edition 6000

通常の導入環境では、Cisco TMS と拡張を同じサーバに配置できます。

	要件	Cisco BE6000
CPU	2 コア（Xeon 2.4 GHz 以上）、専用	1 vCPU
メモリ	8 GB、専用	4 GB の vRAM、専用
サーバで提供されるディスク容量	60 GB	60 GB

Cisco Business Edition 6000 上の Cisco TMSPE には、エンドポイントまたは FindMe 向けの Cisco VCS ベースのユーザ プロビジョニングが含まれないことに注意してください。

大規模な導入環境

大規模な導入環境では、Cisco TMSXE と SQL Server を外部に配置する必要がありますが、Cisco TMS と Cisco TMSPE は常に共存させることができます。

Cisco TMS および Cisco TMSPE サーバ

	要件
CPU	2 コア（Xeon 2.4 GHz 以上）、専用
メモリ	8 GB、専用
サーバで提供されるディスク容量	80 GB

Microsoft SQL Server

このサーバは、Cisco TMS サーバと同じタイム ゾーンに属している必要があります。

	要件
CPU	4 コア（Xeon 2.4 GHz 以上）、専用
メモリ	16 GB、専用
サーバで提供されるディスク容量	60 GB

前提条件

大規模な導入を計画している場合は、次の点にも注意してください。

- 大規模 tmsng データベースに必要なディスク領域は、通常 20 ～ 30 GB です。
- ほとんどの導入環境では、3 つの Cisco TMSPE データベースのサイズが 6 GB を超えることはありません。
- SQL Server のパフォーマンスに影響する主な要因は RAM とディスク I/O です。最適なパフォーマンスを得るためには、これらの値をできるだけ増やす必要があります。

Cisco TMSXE サーバ

このサーバの要件は、サポートされているオペレーティング システムの推奨ハードウェア要件と同じです。

推奨される Cisco TMS の設定変更

大規模な導入環境では、SQL Server と Cisco TMS サービスの負荷を軽減するために、次の設定を強く推奨します。

- **[管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議設定（Conference Settings）]**：[スケジュール コールのデフォルトの予約タイプ（Default Reservation Type for Scheduled Calls）] を [ワンボタン機能（One Button to Push）] に設定します。
- **[管理ツール（Administrative Tools）] > [設定（Configuration）] > [一般設定（General Settings）]**：[電話帳エントリのルーティング（Route Phone Book Entries）] を [いいえ（No）] に設定します。
- **[管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）]**：[アドホック会議の検出を有効にする（Enable Ad Hoc Conference Discovery）] を [MCU 限定（Only for MCUs）] または [いいえ（No）] に設定します。

大規模な導入で推奨されるハードウェアと仮想化

シスコでは、サポート上限以内の大規模な導入に対して次の仕様を推奨しています。これらはすべてテスト済みです。以下に示す仕様を満たすと、Cisco TMS の導入全体を 1 つのラックマウント型サーバでホストできます。

ハードウェア

サーバ	Cisco UCS C220 M3S ラック サーバ
CPU	Intel Xeon プロセッサ E5-2430 v2（2.50 GHz）X 2
ディスク	146 GB 6G SAS 15K RPM SFF HDD/ホット プラグ/ドライブ スレッド マウント（RAID-6 構成）X 8。製品番号：A03-D146GC2。
ディスク コントローラ	LSI MegaRAID 9265-8i 6 Gbps
メモリ	8 GB/1600 MHz X 4
ハイパーバイザ ソフトウェア	以下に示す仕様の仮想マシンを 3 台ホストする VMware ESXi 5.1

前提条件

Cisco TMS と Cisco TMSPE 仮想マシン

CPU	vCPU X 4
メモリ	8 GB
ディスク	200 GB

Microsoft SQL Server 仮想マシン

CPU	vCPU X 4
メモリ	16 GB
ディスク	250 GB

Cisco TMSXE 仮想マシン

CPU	vCPU X 4
メモリ	8 GB
ディスク	100 GB

サーバ ソフトウェアおよび設定要件

ソフトウェア要件は導入環境のサイズとは無関係です。環境のサイズに適したハードウェア要件については、「導入サイズの見積り」（3 ページ）および「ハードウェア要件」（5 ページ）を参照してください。

オペレーティング システムとソフトウェア

製品	バージョン	追加の注意事項
Windows Server	• Windows Server 2012 R2 64 ビット • Windows Server 2012 64 ビット • Windows Server 2008 R2 Standard 64 ビット Service Pack 1	• サーバのオペレーティング システムは英語、日本語、または中国語でなければなりません。 • 標準/業界/データセンターのバージョンがすべてサポートされます。 • 新規インストールでは Windows Server 2012 を使用することを推奨します。 • すべてのバージョンに、最新のサービス パックを使用することを推奨します。
.NET Framework	4.5 .NET Framework	Cisco TMS インストーラを実行する前にインストールする必要があります。

前提条件

製品	バージョン	追加の注意事項
Microsoft IIS	• Windows Server 2012 R2 の場合：IIS 8.5 • Windows Server 2012 の場合：IIS 8 • Windows Server 2008 R2 の場合：IIS 7.5	Microsoft IIS（Internet Information Services）Web サーバがシステムにまだ存在していなければ、Cisco TMS インストーラによって自動的にインストールされます。
Windows インストーラ	4.5	システムに存在しない場合は、続行する前にインストールが必要であることが Cisco TMS インストーラから通知され、インストール パッケージが提供されます。

Windows アップデート

組織のネットワーク ポリシーに従って Windows Updates をイネーブルにし、適用します。

インストール中のアクセス要件

インストールを実行する管理者は、Windows サーバへの管理者アクセス権を持っている必要があります。

日付と時刻の設定

NTP サーバの推奨

Cisco TMS が正しく機能するためには、Windows サーバの時刻が正しく設定されている必要があります。また、サーバが分離されている場合は、Cisco TMS と SQL Server の日付と時刻が一致している必要があります。

このため、両方のサーバを同じ Active Directory ドメイン内で維持し、それらが同じ NTP（Network Time Protocol）サーバを使用するように設定することを強く推奨します。手順については、Microsoft 社のサポート記事「*How to configure an authoritative time server in Windows Server*」を参照してください。

タイム ゾーン

アプリケーションのインストール後に、Cisco TMS を実行している Windows サーバのタイム ゾーンを変更しないでください。サーバのタイム ゾーンを後で変更した場合は、スケジュールに関連していないすべての日付と時刻が変更前のゾーンに残ります。

前提条件

SQL Server ソフトウェアとアクセス許可要件

Cisco TMS は、tmsng という名前の SQL データベースにカスタマー データをすべて保存します。この完全独立型のストレージにより、顧客情報のバックアップとリカバリが容易になります。

新規インストールの場合、インストーラは SQL Server のデフォルトを使用して tmsng を作成します。アップグレードでは、既存の Cisco TMS データベースが再利用されます。

関連項目：

- メンテナンスのベスト プラクティスについては、「データベースのメンテナンス計画」（19 ページ）
- サイズに適したハードウェア要件については、「導入サイズの見積り」（3 ページ）および「ハードウェア要件」（5 ページ）

ソフトウェア

次のいずれかが必要です。

製品	バージョン	追加の注意事項
Microsoft SQL Server 2012	すべてのバージョン、64 ビットのみ	Cisco TMS をインストールする際にサーバに SQL データベースが存在しない場合は、Microsoft SQL Server をインストールするように求められます。SQL Server の Express エディションは無料でインストールできます。 Microsoft SQL Server 2012 Express および 2008 R2 Express には、10 GB のデータベース サイズの制限があります。 このため、10 GB よりも増大すると予測されるデータベースを伴う導入では、フル エディションを使用する必要があります。 新規インストールの場合は、Microsoft SQL Server 2012 を使用することをお勧めします。
Microsoft SQL Server 2008 R2	すべてのバージョン、64 ビットのみ	
SQL Server Browser		データベースとして別のサーバ上の名前の付いたインスタンスを使用するときは、実行する必要があります。

ネットワーク

Cisco TMS サーバと SQL Server の間の遅延は、20 ミリ秒以下である必要があります。

設定とアクセス許可

デフォルトの SQL 言語は英語に設定されている必要があります。

前提条件

認証モード

インストールおよびアップグレードの場合、データベース サーバで *SQL Server 認証モードと Windows 認証モード*（混合モード）を有効にする必要があります。

インストールが完了すると、以降のアップグレードまでは混合モードを無効にして *Windows 認証*を有効にすることができます。

認証モードの変更手順については、『*Cisco TelePresence Management Suite Administrator Guide*』の「TMS Tools」の章または Web ヘルプを参照してください。

ユーザおよびデータベースの作成

Cisco TMS をインストールまたはアップグレードする際に、既存の SQL Server を使用する場合、インストーラから SQL データベースのユーザとパスワードの入力を求められます。デフォルトは、サーバ sa（システム管理者）ユーザ名とパスワードの入力です。

sa アカウントが使用できない場合は、次のいずれかを使用します。

- 自動設定を使用しますが、セキュリティが制限されている役割を使用します。
  1. SQL Server の管理者に、*dbcreator* と *securityadmin* のサーバの役割を持つ SQL ユーザとログインを作成するように依頼します。

     このアカウントが Cisco TMS のサービス アカウントになります。

  2. インストール中に SQL Server のクレデンシャルを入力するように要求された場合、そのアカウントのユーザ名とパスワードを入力します。

     Cisco TMS がサーバのデフォルト値を使用して tmsng データベースを自動的に作成し、自身を所有者として割り当て、提供されたアカウントを引き続き使用して、インストール後にデータベースにアクセスします。

- SQL Server の管理者に、セキュリティが最大限制限されたユーザの役割を使用して手動でデータベースを作成するように依頼します。
  - tmsng という名前のデータベースを、データベース照合 Latin1_General_CI_AI（大文字と小文字を区別せず、アクセント記号も区別しない）で作成します。
  - Cisco TMS サービス アカウントに使用する SQL ユーザとログインを作成し、このユーザに tmsng データベースの *dbowner* の役割を割り当てます。Cisco TMS を機能させるためには、インストール後もこの権限を維持する必要があります。SQL ユーザはデフォルトのスキーマとして *dbo* を使用する必要があります。

前提条件

スナップショットの分離

インストーラによって、自動的に次のようなスナップショット分離設定が tmsng に対して設定されます。この設定は維持する必要があります。

- ALLOW_SNAPSHOT_ISOLATION を ON に設定
- READ_COMMITTED_SNAPSHOT を OFF に設定

クライアント ソフトウェアの要件

管理者を含むすべてのユーザは、Web インターフェイスを使用して Cisco TMS にアクセスします。

Cisco TMS サーバにアクセスするには、Windows のユーザ名とパスワードが必要です。ローカル マシンのアカウントまたはドメインのアカウント（このサーバがドメインに参加している場合）のいずれかが必要です。

Web ブラウザ	Cisco TMS は次のブラウザでテストされています。 • Microsoft Internet Explorer バージョン 10 および 11 • Firefox バージョン 31 • Google Chrome バージョン 37 その他のブラウザも動作する可能性はありますが、積極的にテストされていないため、サポートされていません。
Java Runtime Environment（JRE）	• バージョン 1.5 が必須 • バージョン 1.6.0 以降が推奨 Cisco TMS で [モニタリング（Monitoring）] ページを使用するには、JRE が必要です。これがインストールされていない場合は、ほとんどのブラウザで、ブラウザ プラグインを自動的にダウンロードし、インストールするように求められます。セキュリティ上の制限により JRE の自動インストールができない場合は、http://www.java.com からダウンロード可能な JRE インストール ファイルを、手動でクライアント コンピュータにインストールしてください。

サーバ ネットワークの依存関係

Cisco TMS をインストールする前に、次のネットワークの依存関係を考慮する必要があります。

- 優先するドメイン メンバーシップ：Cisco TMS にログインしている各ユーザは、Web サイトへの認証のため、Windows ユーザ ログインが必要です。ユーザには、Cisco TMS Windows Server 上のローカル アカウント、またはサーバが Active Directory 経由で信頼するドメイン アカウントが必要です。サーバをドメインのメンバにすることによって、すべての信頼ドメインのユーザは、Cisco TMS へのログインに既存の Windows クレデンシャルを自動的に使用できます。Cisco TMS 権限を使用して Cisco TMS にログインした後も、ユーザの実行内容を制限できます。Active Directory のメンバーシップは、各ユーザにローカルの Windows アカウントを作成する必要がないため、ほとんどのインストールに推奨される導入環境です。

前提条件

- IP およびホスト名でアクセス可能な Cisco TMS Web サイト：すべてのデバイスが DNS ホスト名またはポート番号をサポートするわけではないため、Cisco TMS Web サイトはポート 80 の IP アドレスからアクセスできる必要があります。一部の機能は Cisco TMS にホスト名からアクセスできるようにする必要があるため、Cisco TMS には完全修飾ドメイン名でもアクセスできる必要があります。
- メール サーバ アクセス：Cisco TMS では、電子メールを送信できるようにするため、SMTP サーバへのアクセスが必要です。この用途には、社内の既存のメール サーバが利用できます。Cisco TMS では、必要に応じて認証用に SMTP AUTH ログインをサポートしています。
- 管理対象デバイスへのネットワーク アクセス：Cisco TMS には、デバイスを管理するための固有のプロトコルおよびアクセスが必要です。すべてのネットワーク ファイアウォールまたは NAT ルータは、Cisco TMS との間でのトラフィックの流れを許可する必要があります。
- Microsoft IIS のコンポーネント ASP.NET および ASP をイネーブルにする必要があります。
- Windows ファイアウォール機能はデフォルトで有効になり、着信ポートと発信ポートの両方を制御します。Windows ファイアウォールを有効にするときに開く必要があるポートの情報については、「Cisco TMS で使用されるポート」（12 ページ）を参照してください。
- アンチウイルス プログラムまたはそのほかのセキュリティ対策により、アプリケーションが SMTP ポートを使用してメールを直接送信できないようになっていることを確認します。

Cisco TMS で使用されるポート

次のポートは Cisco TMS によって使用され、Windows ファイアウォールで有効にする必要があります。構成および使用デバイスによっては、すべてのサービスがすべてのインストールで使用されるとは限りません。

サービスまたはシステム	トランスポート プロトコル	ポート	方向（Cisco TMS にとって）	
			受信	送信
FTP	TCP	20、21		X
HTTP	TCP	80	X	X
Cisco TelePresence System（CTS）の HTTP	TCP	8081		X
HTTPS	TCP	443	X	X
Cisco TelePresence System（CTS）の HTTPS	TCP	9501		X
Unified CM の HTTPS	TCP	8443		X
LDAP	TCP	389		X
LDAPS	TCP	636		X
Polycom GAB	TCP	3601	X	
SMTP	TCP	25		X
SNMP	UDP	161		X
SNMP トラップ	UDP	162	X	X
SSH	TCP	22		X
Telnet	TCP	23		X
Telnet Challenge	TCP	57		X
Telnet Polycom	TCP	24		X

前提条件

SQL 接続では、デフォルトの SQL サーバ インスタンスに使用される TCP ポートは構成可能です。名前を付けられた SQL サーバ インスタンスに使用されるポートは動的であり、サービスが再起動されるたびに変更されます。SQL サーバが特定のポートをリッスンするように構成する方法については、TechNet の記事「Configure a Server to Listen on a Specific TCP Port (SQL Server Configuration Manager)」を参照してください。

複数の IP アドレスはサポート対象外

Cisco TMS は、複数の IP アドレスを使用できず、利用可能な最初のネットワーク インターフェイスにのみバインドされます。このため、複数のネットワーク カードや、同じカードの IP エイリアスはサポートされません。

ネットワークでパブリックとプライベートの両方のネットワークがルーティングによって相互接続されている限り、Cisco TMS はこの両方のネットワークを管理することができます。複数のネットワーク インターフェイス カードを使用して両方のネットワークを Cisco TMS に直接接続することはできません。

拡張製品との互換性

製品	バージョン
Cisco TelePresence Management Suite Extension Booking API	API バージョン 4 以降最新のバージョンは 15 です。
Cisco TelePresence Management Suite Extension for Microsoft Exchange	4.1
Cisco TelePresence Management Suite Provisioning Extension	1.4
Cisco TelePresence Management Suite Network Integration Extension	バージョンなし
Cisco TelePresence Management Suite Analytics Extension	1.2.1
Cisco TelePresence Management Suite Extension for IBM Lotus Notes	11.3.3

注：すべての機能と修正を利用できるようにするには、最新バージョンが常に必要です。

アップグレードの要件および推奨事項

ご使用の Cisco TMS のアップグレードを開始する前に、現在稼働している Cisco TMS のバージョンに適用される以下のすべてのセクションを確認してください。

仮想ディレクトリ

Cisco TMS のどのバージョンからアップグレードするときも、すべての仮想ディレクトリは削除され、新しいバージョンのインストール時に再作成されます。これにより、仮想ディレクトリのカスタム設定も削除されることに注意してください。

冗長展開

「バージョン 14.4 より前の Cisco TMS からの冗長展開のアップグレード」（47 ページ）を参照してください。

前提条件

2008 R2 より前のバージョンの SQL Server および 2008 R2 より前のバージョンの Windows Server の使用

14.4 および 14.6 では、SQL および Windows サーバの要件が変更されました。Cisco TMS をアップグレードする場合で、2008 R2 より前のバージョンの SQL Server または 2008 R2 より前のバージョンの Windows Server を実行している場合は、Cisco TMS のアップグレードの前にサーバをアップグレードする必要があります。SQL Server および Windows Server は 2012 にアップグレードすることをお勧めします。

サポートされているバージョンの詳細については、「サーバ ソフトウェアおよび設定要件」（7 ページ）および「SQL Server ソフトウェアとアクセス許可要件」（9 ページ）を参照してください。

Cisco TMSXE を使用するお客様向けの 14.4 または 14.4.1 からのアップグレード手順

このアップグレード手順の要件に関する追加の背景情報については、『Cisco TelePresence Management Suite Software Release Notes (14.4.2)』を参照してください。

Cisco TMSXE と Cisco TMS のアップグレード

Cisco TMSXE を使用し、14.4 または 14.4.1 からアップグレードするお客様は、次のアップグレード手順に順番どおりに従う必要があります。

1. Cisco TMSXE をバージョン 4.1 にアップグレードします。
2. このバージョンの Cisco TMS にアップグレードします。
3. 15 分間待ってから Cisco TMSXE ログを確認します。TMSXE-log-file.txt で、**`INFO ReplicationEngine - No changes on TMS`** と記載されている行を確認します。

   これにより、Cisco TMS が自動的に解決できるすべての問題のある予約が Cisco TMS から Microsoft Exchange に正しく複製されていることが確認できます。

   この行を確認できない場合は、シスコのサポート担当者にお問い合わせください。

Cisco TMS で重複する会議を解決する

この 2 番目の手順はアップグレード後なるべく早く実行する必要がありますが、ただちに実行する必要はなく、メンテナンス時間帯の確保も不要です。

1. Cisco TMS に移動し、「外部プライマリ キーが重複する会議シリーズが見つかりました（Conference series with duplicate external primary keys found）」という重要な TMS チケットがないか確認します。
   - このチケットがない場合、何もする必要はありません。
   - チケットが見つかった場合、手順 2 および 3 に進みます。

前提条件

2. Cisco TMS ツールで [重複キーの解決（Resolve Duplicate Keys）] ツールを実行し、重複のリストから適切な会議を選択します。

   どれが正しい会議か明らかでない場合は、会議に参加するシステムの Exchange リソース カレンダーを確認してください。リソース カレンダーの大部分またはすべてが、重複する会議の 1 つと一致する場合、おそらくそれが適切な会議です。

   それでも正しい会議を特定できない場合は、会議の所有者に問い合わせてください。

3. 15 分間待ってから Cisco TMSXE ログを確認します。TMSXE-log-file.txt で、**`INFO ReplicationEngine - No changes on TMS`** と記載されている行を確認します。これにより、残りすべての問題のある予約が Cisco TMS から Microsoft Exchange に正しく複製されていることが確認できます。この行を確認できない場合は、シスコのサポート担当者にお問い合わせください。

Exchange リソース カレンダーで残りの重複するアポイントメントを手動で解決する

導入の状況によっては、Cisco TMS（このバージョンの Cisco TMS）へのアップグレード時に自動的に特定またはクリーンアップされない重複する Exchange アポイントメントがリソース カレンダーに少数残ることがあります。

重複がよく発生するのは、会議テンプレートを使用するか、14.4 より前のバージョンの Cisco TMS の既存の会議をコピーして会議を作成し、それからその会議を 14.4 または 14.4.1 で（Cisco TMS または Microsoft Exchange で）編集した場合です。

このような重複する Exchange アポイントメントを特定して解決するには、次の手順を実行します。

1. Cisco TMSXE サーバにログオンし、現在からスケジュール範囲の最後までの検索期間で Meeting Analyzer を実行します。

   大規模な導入においては、これを営業時間外に実行するか、Exchange サーバの負荷を減らすために短い検索対象期間で Meeting Analyzer を実行することをお勧めします。

2. Meeting Analyzer レポートで、「Cisco TMS で一致する会議が見つかりません（No matching conferences found in）」というフラグが付けられたアポイントメントを探します。

   このフラグが付けられたアポイントメントがない場合、何もする必要はありません。

   フラグ付きのアポイントメントが見つかった場合は、手順 3 に進みます。

3. Exchange リソース カレンダーに対してフル アクセスできるユーザでログインします。
   1. Microsoft Outlook を開きます。
   2. 手順 2 で特定した重複するアポイントメントの 1 つを探します。

4. 重複するアポイントメントの開始時間、終了時間、または件名が Cisco TMS の対応するアポイントメントと異なる場合は、すべての Exchange リソース カレンダーから削除します。

前提条件

アポイントメントに相違点がない場合は、以下の「適切なアポイントメントを特定するための変更の適用」手順に進みます。

5. 手順 3 に戻り、問題のある別のアポイントメントを処理します。

適切なアポイントメントを特定するための変更の適用

開始時間、終了時間、および件名が同じアポイントメントがリソース カレンダーに 2 つ以上ある場合は、重複するアポイントメントを区別できず、どれを削除すべきか判断できません。差異を確認できるようにする変更を適用し、適切なアポイントメントを特定するには、次の手順に従います。

1. Cisco TMS で、[予約（Booking）] > [会議の一覧（List Conferences）] の順に移動し、会議を見つけます。
2. 会議を編集し、会議時間を 5 分短縮して [会議の保存（Save Conference）] をクリックします。

   Cisco TMSXE では 3 分以下の変更は無視されるため、この時間は重要です。

3. Cisco TMSXE レプリケータが変更を処理し、Exchange リソース カレンダーが新しい終了時間に更新されるのを待ちます。これには数分かかることがあります。
4. 終了時間が新しくなった Exchange のアポイントメントが、Cisco TMS に正しくリンクされているアポイントメントになります。終了時間が変更されなかった、重複する 1 つ以上のアポイントメントを削除します。
5. Cisco TMS で、会議の終了時間を元に戻します。

Cisco TMSXN を使用する 14.4 または 14.4.1 からアップグレードするお客様向けの手順

このアップグレード手順の要件に関する追加の背景情報については、『Cisco TelePresence Management Suite Software Release Notes (14.4.2)』を参照してください。

Cisco TMS のアップグレードと重複する会議の解決

Cisco TMSXN を使用し、14.4 または 14.4.1 からアップグレードするお客様は、最初にこのバージョンの Cisco TMS にアップグレードし、アップグレード後なるべく早くこの手順を実行する必要があります。ただし、ただちに実行する必要はなく、メンテナンス時間帯の確保も不要です。

1. Cisco TMSXN Synchronizer が Cisco TMS からのデータを処理するまで 15 分待ちます。
2. Cisco TMS で、「外部プライマリ キーが重複する会議シリーズが見つかりました（Conference series with duplicate external primary keys found）」という重要な TMS チケットがないか確認します。

   このチケットがない場合、何もする必要はありません。

   チケットが見つかった場合は、手順 4 に進みます。

前提条件

3. TMS ツールで [重複キーの解決（Resolve Duplicate Keys）] ツールを実行し、重複のリストから適切な会議を選択します。

   どの会議が適切かわからない場合は、会議に関係するシステムの Domino カレンダーを確認します。リソース カレンダーの大部分またはすべてが、重複する会議の 1 つと一致する場合、おそらくそれが適切な会議です。

   それでも正しい会議を特定できない場合は、会議の所有者に問い合わせてください。

Cisco TMSXN Synchronizer の再起動

このプロセスによって Cisco TMS から Domino への複製が再開され、Cisco TMS に存在する今後のすべての予約（すでに存在している予約以外）が Domino に書き込まれます。

1. Domino Administrator から、[ファイル（Files）] > [ビデオ会議リソース（Video Conference Resources）] を開きます。
2. [予約（Reservations）] > [日付順（By Date）] の順に移動し、予約を選択します。
3. [操作（Actions）] > [Synchronizer の再起動（Restart Synchronizer）] の順に選択します。
4. Domino ログ ファイルを監視し、「`Agent printing: Synchronizer from zero finished`」というステートメントの表示を待ちます。このステートメントが表示されると、Cisco TMS からのすべての予約が Domino に再度複製されています。

14.2 よりも前のバージョン

Cisco TMS のタイム ゾーンのサポートは 14.2 で改善され、以前のバージョンからのアップグレード後にタイム ゾーン データのずれを修正するタイム ゾーン更新ツールが提供されました。このツールをサポートした最後のバージョンは 14.3.2 でした。

次の場合、最新バージョンにアップグレードする前に、14.3.2 にアップグレードしてタイム ゾーン ツールを実行する必要があります。

- 米国と欧州、または北半球と南半球の両方から、会議のスケジュールを作成するユーザがいる。
- オーストラリアなど、州または地域によって DST ルールが異なる国にいる。

注意：上記いずれかの場合に直接アップグレードすると、データが不正確になるおそれがあります。

Cisco TMS およびテレプレゼンス ネットワークで会議の予約を行うすべてのオーガナイザのタイム ゾーンが同じ場合や、タイム ゾーンで米国（アリゾナ州とハワイ州を除く）のように同じ DST ルールを使用する場合、14.3.2 を経由してアップグレードを行う必要は*ありません*。

タイム ゾーンの更新の詳細および手順については、14.3.2 の 『*Cisco TMS Installation and Upgrade Guide*』を参照してください。

タイム ゾーンの不一致が解決されたら、15.1 にアップグレードすることができます。

前提条件

Cisco TMS Agent のレガシー プロビジョニング

レガシー プロビジョニング機能を使用して 13.2.x 以前のバージョンからアップグレードする場合は、Cisco TMS 15.1 へアップグレードする*前に*、Cisco TelePresence Management Suite Provisioning Extension に移行する必要があります。

現在古いバージョンを使用している場合、この移行には Cisco TMS バージョン 13.2 が必要であることに注意してください。次の手順を実行する必要があります。

1. Cisco TMS を 13.2.x にアップグレードします。

   バージョン 13 よりも前のバージョンからアップグレードする場合、このアップグレードを実行するにはシスコから Cisco TMS 13 のリリース キーを取得する必要があります。

2. Cisco TMSPE をインストールします。Cisco TMS 13.2 の『*Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*』の手順に従ってプロビジョニング データベースを移行します。
3. タイム ゾーンの変更により 14.3.2 を介したアップグレードが必要になるかどうかを確認します（「14.2 よりも前のバージョン」（17 ページ）を参照）。
4. タイム ゾーンのすべての問題を解決します。Cisco TMS 15.1 にアップグレードします。

13.2 よりも前のバージョン

デフォルトの予約の確認用電子メール テンプレートとフレーズ ファイルは 13.2 で更新されました。これらのテンプレートがカスタマイズされたテンプレートである 13.2 よりも前のバージョンからアップグレードする場合は、新しい追加は、カスタマイズされたファイルに自動的に追加されませんが、引き続き使用することができます。

この新しい値のデフォルトの使用法を確認し、これらの値をテンプレートに持たせるには、カスタマイズされた予約の確認テンプレートまたはフレーズを保有するカスタマーは次の手順を実行する必要があります。

1. [管理ツール（Administrative Tools）] > [設定（Configuration）] > [電子メールテンプレートの編集（Edit Email Templates）] の順に移動します。
2. [予約の確認（Booking Confirm）] テンプレートを開きます。
3. [デフォルトに戻す（Revert to Default）] をクリックします。

デフォルトに設定されると、カスタマイズをテンプレートまたはフレーズ ファイルに再度追加できます。

13.0 よりも前のバージョン

13.0 までのバージョンへのダウングレードは、Cisco TMS 15.1 でテストされ、サポートされています。それよりも前のバージョンでは、サーバの要件、データベース、およびバックエンドが大幅に変更されているため、アップグレードではなく新規インストールを実行することを推奨します。

展開のベスト プラクティス

この章では、Cisco TMS のインストールと初期設定のベスト プラクティスについて説明します。

データベースのメンテナンス計画

Cisco TMS と Cisco TMSPE は、両方とも SQL Server のデフォルト設定に従ってデータベースを作成します。データベースには次のものがあります。

- tmsng（Cisco TMS）
- tmspe（Cisco TMSPE メイン）
- mspe_vmr（Cisco TMSPE コラボレーション会議室）
- tmspe_userportal（Cisco TMSPE セルフサービス ポータル）

データベースのメンテナンス計画を作成および維持するためのベスト プラクティスについて以下で説明します。データベースの管理は、Microsoft SQL Server Management Studio Express などの外部ツールを使用して行う必要があります。

復旧モデル

必要な動作に応じて、データベースは単純復旧モデルまたは完全復旧モデルに設定できます。各復旧モデルの特徴についての詳細は、MSDN の記事「Recovery Models (SQL Server)」を参照してください。

単純復旧

一般的な Cisco TMS の導入では、単純復旧モデルの使用をお勧めします。これはバックアップ間の復旧のみをサポートします。

このモデルでは、定期的な間隔でデータベースをバックアップし、トランザクション ログは省略します。データベースではログの領域が再利用されるので、ファイル サイズは限られます。データベース トランザクション ログのサイズは小規模で、データベース バックアップの間に増え続けることはありません。

展開のベスト プラクティス

完全復旧

大規模な Cisco TMS を導入する経験豊富な SQL Server 管理者は、完全復旧モデルによって得られる追加機能と保守ツールを選択する場合があります。この復旧モデルでは、データベース トランザクション ログを使用した任意の時点への復旧がサポートされます。

この復旧モデルでは、データベース トランザクション ログ ファイルはバックアップの間に常に増加するため、メンテナンスを行わずに放置すると、データベースが容量を使い切って停止する原因になる場合があります。

この復旧モデルでは、データベースおよびトランザクション ログの定期的なバックアップは必須です。

復旧モデルの特定または変更

データベースの復旧モデルを特定または変更するには、お使いの SQL Server バージョン向けの Microsoft の手順書を参照してください。

- View or Change the Recovery Model of a Database（SQL Server 2012）
- How to: View or Change the Recovery Model of a Database（SQL Server 2008 R2）

定期的なメンテナンス タスク

ベスト プラクティスとして、バックアップとインデックスのメンテナンスのための定期的なメンテナンス タスクを設定します。データベースのメンテナンスは Cisco TMS の性能に影響することに注意してください。これらのタスクは組織のスケジュールされたメンテナンス時間に実行します。

バックアップ

組織のリカバリ ポリシーに従って、最低でも週に 1 回のサーバのバックアップ タスクを設定します。

- Back Up and Restore of SQL Server Databases（SQL Server 2012）
- Backing Up and Restoring Databases in SQL Server（SQL Server 2008 R2）

インデックスのメンテナンス

過度のフラグメンテーションを避けるために、定期的にデータベース インデックスのメンテナンスを実施します。毎月またはフラグメンテーションが 30% を超えたときに、インデックスの再構築を行うことをお勧めします。

- Reorganize and Rebuild Indexes（SQL Server 2012）
- Reorganizing and Rebuilding Indexes（SQL Server 2008 R2）

展開のベスト プラクティス

SQL Server のメンテナンス計画

（Express ではなく）SQL Server のフル バージョンを使用している場合、組み込みのメンテナンス計画機能およびウィザードを前述のタスクに利用できます。使用方法については、次の Microsoft の記事を参照してください。

- Create a Maintenance Plan（SQL Server 2012）
- How to: Create a Maintenance Plan（SQL Server 2008 R2）

データベース サイズの管理

データベースを縮小する定期的なメンテナンス タスクは*行わない*ことを強くお勧めします。時間とともにデータベース サイズは正常に安定し、30% のバッファを加えた固定サイズとして指定することができます。

いくつかの状況では、アップグレードの最中にデータベース サイズが著しく増加します。このような場合には、データベースを縮小する 1 回だけの操作をお勧めします。

セキュリティ

このセクションでは、Cisco TMS をより安全に使用するために推奨する方法を紹介します。

Web および API 通信

Cisco TMS インストーラは、デフォルトで Web コミュニケーション用に HTTPS を設定します。これにより、管理者によって自己署名証明書が提供されない場合に証明書を作成することができます。セキュリティをさらに強化するために、認証局によって署名された有効な証明書を使用することを強くお勧めします。

セキュリティ向上のための IIS の設定

IIS マネージャで次の手順を実行します。

1. Polycom システムを使用しない場合は、次の手順を実行して Polycom の電話帳コンポーネントを無効にします。
    1. デフォルトの Web サイトのツリー ビューを展開します。
    2. /pwx コンポーネントを右クリックし、[削除（Remove）] を選択します。
2. Web と API トランザクション用の HTTP を無効にします。
    1. /tms コンポーネントをクリックして選択します。
    2. [IIS] セクションで、[SSL 設定（SSL Settings）] をダブルクリックします。
    3. [SSL を使用（Require SSL）] をオンにし、[アクション（Actions）] パネルで [適用（Apply）] をクリックします。
    4. /tms コンポーネントを展開し、/public をクリックして選択します。
    5. [IIS] セクションで、[SSL 設定（SSL Settings）] をダブルクリックします。
    6. [SSL を使用（Require SSL）] をオフにし、[アクション（Actions）] パネルで [適用（Apply）] をクリックします。

3. フラッド攻撃からの保護を設定します。詳細は、「付録 2：フラッド攻撃からの保護のための IIS 要求の設定」（59 ページ）を参照してください。

システムとの通信

Cisco TMS は、デフォルトで HTTP を使用してシステムと通信しますが、一部のレガシー システムとは SNMP を使用します。

レガシー システムを使用する場合は、サーバ上で Windows SNMP Service を有効にすることで、SNMP を使用できます。

システムとのセキュアな通信のための Cisco TMS の設定

[セキュアなデバイスのみの通信（Secure-Only Device Communication）] の設定を有効にすると、Cisco TMS は、HTTPS をサポートするシステムに対して HTTPS のみを使用して通信を行います。

この場合、システムで HTTPS が有効になっている必要があり、そうでない場合は通信に失敗します。HTTPS をサポートしていない環境内のシステムに対しては、HTTP が引き続き使用されます。

通信の安全性をさらに確保するために、Cisco TMS の証明書検証を有効にすることもできます。

[管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）] で、次の手順を実行します。

1. 一番下のセクションまで移動し、[セキュアなデバイスのみの通信（Secure-Only Device Communication）] を [オン（On）] に設定します。
2. [証明書の検証（Validate Certificates）] をオンにします。
3. [保存（Save）] をクリックします。

この設定は、次のインフラストラクチャ システムでサポートされています。

- TelePresence Conductor（すべてのバージョン）
- Cisco VCS（X4 以降）
- Cisco TelePresence Server（2.3 以降）
- Cisco TelePresence MCU シリーズ（2.3 以降）
- Cisco TelePresence ISDN Gateway（2.2 以降）
- Cisco TelePresence MPS（J4.2 以降）

この設定は、次のエンドポイントでサポートされています。

- Cisco TelePresence MXP（F7 以降）
- Cisco TelePresence TC エンドポイント（TC3 以降）
- Cisco TelePresence TE エンドポイント（TE4 以降）

展開のベスト プラクティス

Cisco TMS の初期設定

Cisco TMS の設定は、一般的に導入後および運用中にいつでも変更できます。ただし、メンテナンスおよび運用を簡単にするために、インストールの直後、ユーザにシステムの利用を許可する前に、ユーザ アカウント ポリシー、ゾーン、および基本設定のデフォルトを設定することをお勧めします。

手順については、組み込みの Cisco TMS ヘルプまたは『*Cisco TMS Administrator Guide*』を参照してください。

ユーザ管理

Microsoft Active Directory を使用してすべての Cisco TMS ユーザを管理することを強くお勧めします。

ゾーン

インストールの最中にゾーンの初期設定を行うことができます。インストール後にこの設定を表示または変更するには、[管理ツール（Administrative Tools）] > [ロケーション（Locations）] > [ISDN ゾーン（ISDN Zones）] または > [IP ゾーン（IP Zones）] の順に移動します。

フォルダ階層

Cisco TMS へのシステムの追加を始める前に、[システム（Systems）] > [ナビゲータ（Navigator）] 内のエンドポイントおよびインフラストラクチャ システムについて、よく構造化された拡張性の高いフォルダ階層を計画することを強くお勧めします。

会議のデフォルト設定

ユーザが会議の予約を始める前に、接続タイプ、帯域幅などについてデフォルト設定を見直して調整することをお勧めします。[管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議設定（Conference Settings）] の順に移動します。

Cisco TMS のインストールまたはアップグレード

この章では Cisco TMS の新規インストールまたはアップグレードを行う手順について説明します。

はじめる前に

次の内容について確認してください。

- 使用環境へのインストールに関するすべての「前提条件」（3 ページ）が考慮されている
- 必要な Cisco TMS ソフトウェア バンドルが Cisco.com からダウンロードされている
- Cisco TMS のリリース キーおよびすぐに追加する予定のシステムおよび機能のオプション キーを取得済みである

アップグレードする場合は、必ず「アップグレードの要件および推奨事項」（13 ページ）を見直して、現在の Cisco TMS のバージョンからアップグレードするときに適用される特別な手順または要件についても確認してください。

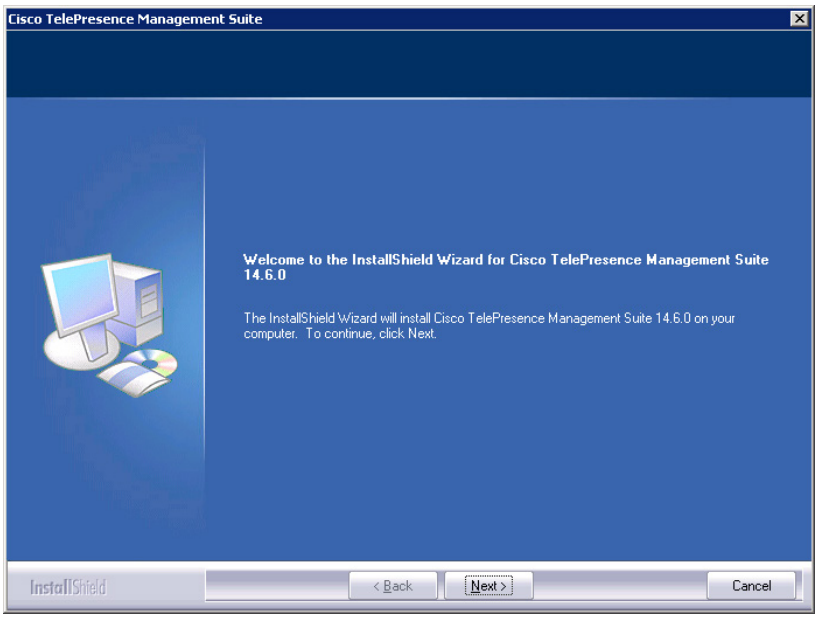
インストール中にサーバをリブートするように複数回要求される場合があります。インストーラは、サーバのリブート後に自動的に再開します。

インストーラの実行

追加する必要がある Windows コンポーネントによって、インストール時にサーバを複数回リブートするように求められる場合があることに注意してください。インストーラは、サーバのリブート後に自動的に再開します。

1. 実行中のすべてのアプリケーションを終了し、ウィルス スキャン ソフトウェアなどのインストールの実行を妨げる恐れのあるソフトウェアを無効にします。
2. フォルダに Cisco TMS .zip アーカイブを展開します。

3. Cisco TMS 実行可能ファイルを管理者として実行します。
4. インストーラは、サーバのハードウェアとソフトウェアの構成をすぐにチェックします。サーバの構成によっては、警告またはエラー メッセージが表示される場合があります。プロンプトの指示に従って、欠落コンポーネントをインストールします。
5. 以前のバージョンの Cisco TMS が現在インストールされている場合は、アップグレードを求めるプロンプトが表示されます。
   - [はい（Yes）] をクリックして続行します。アップグレードにより、古いバージョンが削除され、既存の Cisco TMS データベースがアップグレードされます。
   - [いいえ（No）] をクリックするとインストールが中断され、現在のインストールはそのままの状態になります。
6. [ようこそ（Welcome）] 画面が表示されたら [次へ（Next）] をクリックして続行します。

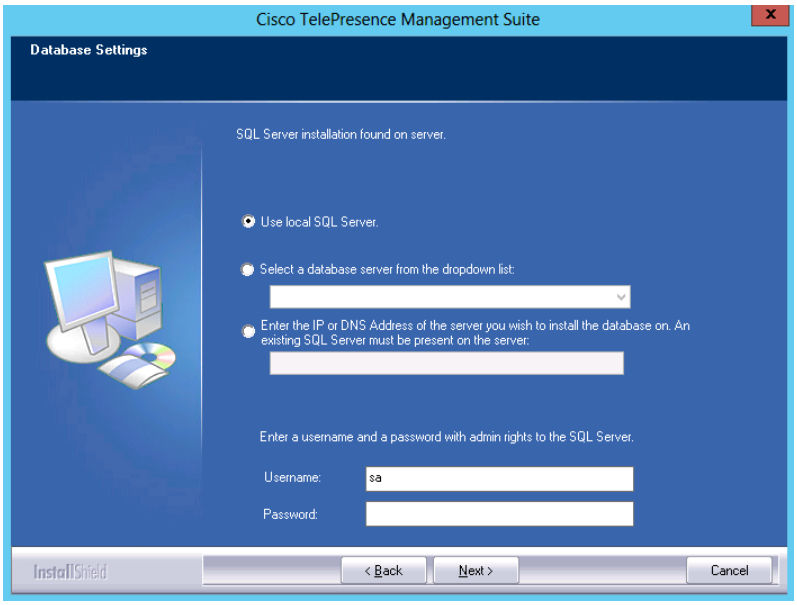


7. ライセンス契約を受け入れるには、[はい（Yes）] をクリックします。

   インストーラは、既存の SQL Server および Cisco TMS データベースを検索します。

Cisco TMS のインストールまたはアップグレード

データベースの作成またはアップグレード



- インストーラによって既存の Cisco TMS データベースが見つからず、ローカルにインストールされた SQL Server が見つかった場合は、ユーザ名とパスワードを入力してインストーラが新しいデータベースを作成できるようにします。[次へ（Next）] をクリックします。
- 大規模導入で必要となる外部 SQL Server を使用している場合は、すべての接続の詳細を入力します。[次へ（Next）] をクリックします。
- インストーラによって既存の Cisco TMS データベースが見つかった場合は、以前指定した SQL Server の情報がダイアログにすでに入力されています。ユーザ名とパスワードの入力を求められたら、入力して [次へ（Next）] をクリックします。
  - 既存のデータベースを最新のバージョンにアップグレードし、既存の情報を保持する場合は [はい（Yes）] をクリックします。

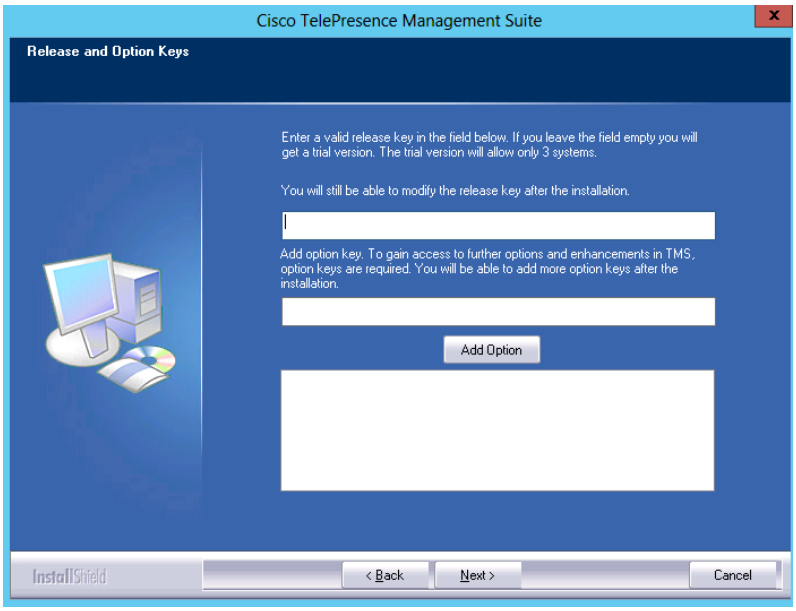
    データベースをアップグレードする前に、適切なツールを使用して、データベースをバックアップすることをお勧めします。「データベースのメンテナンス計画」（19 ページ）も参照してください。

  - [いいえ（No）] をクリックする場合、同じ SQL Server を使用するには、新しい Cisco TMS データベースをインストールする前に、インストーラを停止し、手動でデータベースを削除する必要があります。

リリース キーの追加とネットワーク設定の事前設定

ここで [リリース キーとオプション キー（Release and Option Keys）] ダイアログが表示され、アップグレードの場合はすべての既存のキーが表示されます。

Cisco TMS のインストールまたはアップグレード



新規インストールまたは新しいメジャー リリースへのアップグレードを実行する場合は、新しいリリース キーが必要です。リリース キーが入力されなかった場合は、評価版の Cisco TMS がインストールされます。これには、3 台のシステムのサポートが含まれます。

オプション キーは追加のシステム、拡張、または機能を有効にします。オプション キーは、インストール後に [管理ツール（Administrative Tools）] > [設定（Configuration）] > [一般設定（General Settings）] で追加することもできます。

リリース キーまたはオプション キーに関する質問については、シスコ リセラーまたはシスコ サポートに連絡してください。

1. 必要な場合はリリース キーを入力します。

   リリース キーはオプション キーを追加する前に入力する*必要があります*。

2. オプション キーをそれぞれ入力し、[オプションを追加（Add Option）] をクリックします。

   オプション キーを追加すると検証が行われます。

3. キーの追加が終わったら、[次へ（Next）] をクリックします。

   [ネットワーク設定（Network Settings）] 画面が表示されます。

4. ここで、Cisco TMS が基本ネットワーク設定を使用してただちに動作を開始するように、デフォルト設定を事前に設定できます。この設定はインストール後に変更できます。

   アップグレードする場合、既存のデータベースから値が表示されます。

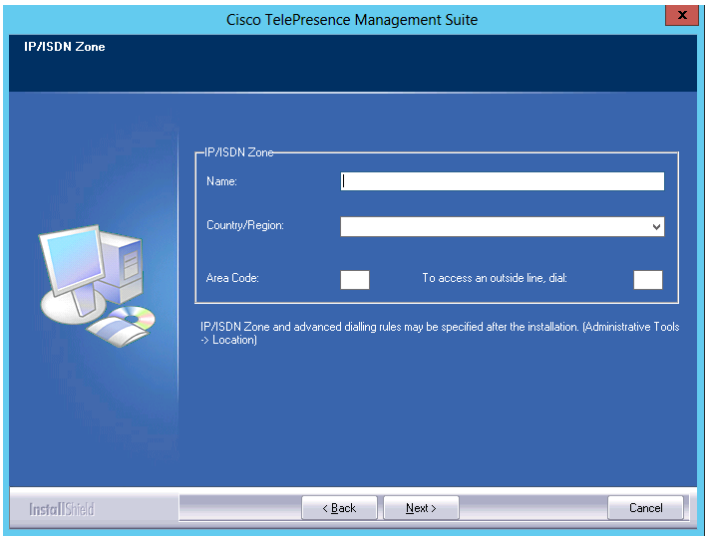
フィールド ラベル	説明
TMS サーバ IPv4 アドレス（TMS Server IPv4 Address）	ローカル サーバの IPv4 アドレス。
TMS サーバ IPv6 アドレス（TMS Server IPv6 Address）	ローカル サーバの IPv6 アドレス。IPv6 が Windows Server でイネーブルでない場合、このフィールドはブランクのままにできます。
IP ブロードキャスト/マルチキャスト アドレス [...]（IP Broadcast/Multicast Addresses [...]）	Cisco TMS で自動的にデバイスを検索するネットワークのブロードキャスト アドレス（Cisco TMS で検出されたシステムは管理設定とともに自動的に Cisco TMS に追加されます）。複数のブロードキャスト アドレスをコンマで区切って入力することもできます。SNMP 探索パケットが指定のアドレスに送信されて、Cisco TMS でネットワークが検索されます。デフォルト値は Cisco TMS サーバのネットワークのブロードキャスト アドレスになります。 新規インストールでは、デフォルトで Windows SNMP Service は無効であることに注意してください。
TMS のシステムの自動登録を有効にする（Enable automatic registration of systems in TMS）	有効な場合は、Cisco TMS によってネットワーク上で検出されたシステムが、自動的に Cisco TMS のフォルダに追加され、管理設定が行われます。デフォルトでは、この設定はディセーブルになっています。
送信者の電子メール アドレス（Sender E-mail Address）	Cisco TMS から送信されるメッセージの [送信者（From）] フィールドに表示される電子メールアドレス。例：`videomanagement@example.com`.
SMTP サーバ アドレス（SMTP Server Address）	Cisco TMS で電子メールの送信に使用する SMTP サーバのネットワーク アドレス。追加の認証構成設定は必要に応じてインストール後に設定することができます。

5. 設定の変更が完了したら、[次へ（Next）] をクリックします。

   Cisco TMS が、指定された SMTP サーバに接続して設定を検証します。サーバに接続できない場合は、警告が表示されます。

   新規インストールの場合、[IP/ISDN ゾーン（IP/ISDN Zone）] 画面が次に表示されます。

ゾーンの事前設定とインストール フォルダの場所の設定



ゾーンは、通話のスケジューリングや電話帳の使用の際に、電話番号およびエイリアスをルーティングするために Cisco TMS で使用される設定概念です。

インストール中に入力する情報によって、Cisco TMS に最初の IP ゾーンおよび ISDN ゾーンが作成されます。これらは基本 IP ネットワークおよび ISDN ネットワークがインストール後に動作するための初期デフォルト値として設定されます。追加のゾーンおよび設定を、複数のロケーションまたはより複雑な要素があるネットワークにはインストール後に追加しなければなりません。

1. 次の説明に従ってゾーン情報を入力します。

フィールド ラベル	説明
名前（Name）	通常、都市または建物を参照するゾーンの識別に役立つ名前。
国/地域（Country/Region）	このゾーンが位置する国。これは、ISDN のダイヤル情報に使用されます。
市外局番（Area Code）	場所の市外局番（該当する場合）。これは、ISDN のダイヤル情報に使用されます
外線にアクセスする場合にダイヤル（To access an outside line, dial）	ISDN 回線の外線に到達するためのプレフィックス（該当する場合）。

2. 設定を変更したら、[次へ（Next）] をクリックします。

   [フォルダ設定（Folder Settings）] 画面が表示されます。

3. Cisco TMS のインストール パスを指定して、[次へ（Next）] をクリックします。

   [暗号化キー（Encryption Key）] 画面が表示されます。

4. Cisco TMS データベース内のシステム ユーザ名とパスワードのデータを暗号化する新しいキーを作成するために、[生成（Generate）] をクリックします。または、必要に応じて、Cisco TMS の以前のインストールから既存のキーを追加します。[次へ（Next）] をクリックします。

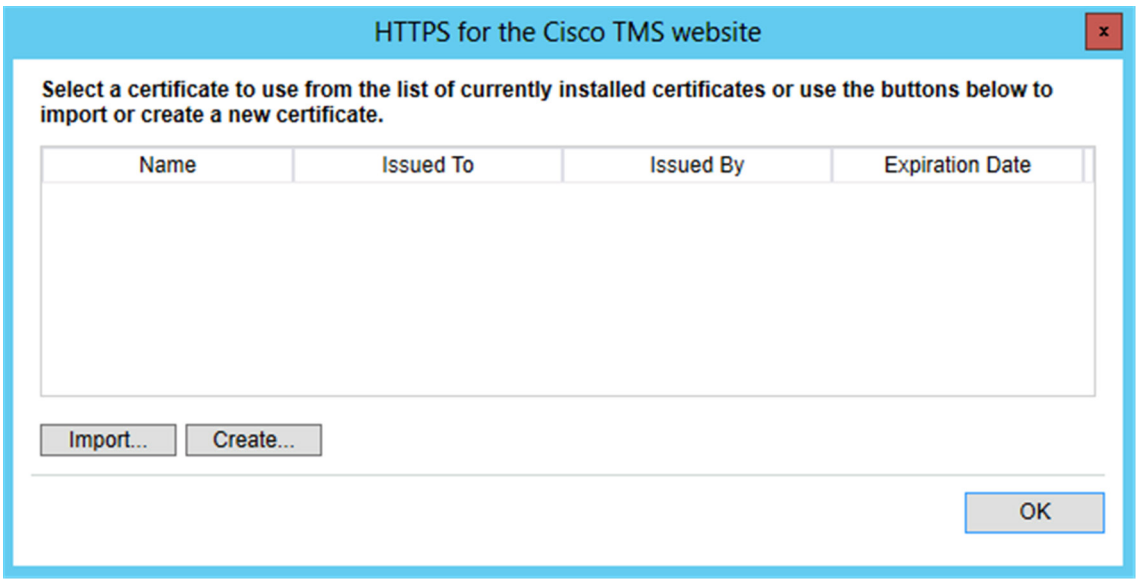
   [ファイルのコピーの開始（Start Copying Files）] 画面が表示されます。

5. 表示された要約のすべての設定を確認し、[次へ（Next）] をクリックします。

   インストール プロセスが始まります。

証明書の追加

インストールが完了したら、Cisco TMS Web サイトへの HTTPS アクセスができるようにするために、TLS 証明書をインポートするか、または作成します。テスト環境にインストールする場合を除いて、信頼できる CA からの正式な証明書を使用することを強くお勧めします。



1. [インポート（Import）] をクリックして .pfx 形式の既存の証明書を追加するか、[作成（Create）] をクリックして自己署名証明書を作成します。
2. インポートが完了したら、[OK] をクリックします。
3. セットアップ ウィザードを終了します。[完了（Finish）] をクリックします。
4. 必要な場合は、サーバをリブートするように求められます。

Windows SNMP Service の有効化

Cisco TMS の新規インストールでは、デフォルトで Windows SNMP Service が無効になっています。SNMP を必要とするレガシー装置を使用している場合は、インストール後にこのサービスを有効にできます。

Cisco TMS への初回アクセス

Cisco TMS をインストールしたら、ブラウザを使用して Web インターフェイスにアクセスします。

1. 次のいずれかを実行します。
   - Windows の [スタート（Start）] メニューの Cisco プログラム グループにあるショートカットを使用します。
   - Web ブラウザの URL フィールドに「`https://<serveraddress>/tms`」と入力します。ここで、<serveraddress> は、サーバのホスト名（推奨）または IP アドレスです。ホスト名を使用すると、Active Directory に統合された認証に対応します。
2. サーバ コンソールから Web サイトにアクセスする場合は、通常、現在ログインしているユーザ名で自動的に認証が行われ、Cisco TMS が開きます。そうでない場合は、認証情報の入力を求められます。

   ほとんどのブラウザでは、ログイン ウィンドウに 2 つの項目が表示されます。つまり、ユーザ名とパスワードのフィールドです。ユーザ名の入力方法は、使用している Windows アカウントによって異なります。

フィールド	説明	例
ドメイン ユーザ	ユーザ名は、「`domain\username`」という形式で入力する必要があります。「`username@<Domain DNS name>`」の形式も使用できますが、あまり使用されていません	**`corp\firstname.lastname`**
ローカルの Windows アカウント	ユーザ名は、「`machinename\username`」という形式で入力する必要があります。	**`tms-2\administrator`**

3. 正常に認証されると、[個人情報の編集（Edit Personal Information）] というウィンドウがポップアップします。

   このウィンドウが表示されない場合は、ブラウザのポップアップ ブロックのアラートを見つけ、Cisco TMS のポップアップ ブロッキングを無効にします。

4. 詳細を入力し、[個人情報を更新する（Update Your Personal Information）] をクリックします。

冗長展開の設定

Cisco TMS は、アプリケーションの可用性を向上させる冗長構成を使用した展開をサポートしています。

この章では、2 つのサポートされている冗長性シナリオでの Cisco TMS の展開に関する要件、設定、および制限について説明します。

この章は、Cisco TMS、Cisco TMS のインストール、および Windows Server オペレーティング システムについて理解しており、コンピュータ ネットワーキングとネットワーク プロトコルに関する高度な知識を持っている方を対象としています。

事前情報

サポートされる構成

自動フェールオーバー プロセスを備えた完全冗長 Cisco TMS 展開では、前面にネットワーク ロード バランサ（NLB）を備えた 2 台の Cisco TMS サーバを設定する必要があります。新しく展開する場合、2 台の Cisco TMS サーバ間における IP トラフィックのロード バランシングを行うには F5 BIG-IP ロード バランサを使用することをお勧めします。このため、このドキュメントでは、Cisco TMS を F5 BIG-IP アプライアンスとともに展開する方法について説明します。Cisco ACE 4710 Application Control Engine アプライアンスの使用もサポートされています。ACE ロード バランサを使用している場合の以前の冗長性モデルからこの拡張モデルへの移行については、「バージョン 14.4 より前の Cisco TMS からの冗長展開のアップグレード」（47 ページ）で説明します。

冗長展開の設定

この章では、ホット スタンバイ モデルを使用して 2 台の Cisco TMS サーバを展開する方法についても説明します。

2 つの冗長性モデルのどちらを展開するかに関係なく、3 台 以上の Cisco TMS サーバを使用することはできません。冗長設定における 3 台以上の Cisco TMS サーバの展開は、シスコではテストされておらず、サポートもされていません。

2 台の Cisco TMS サーバを配置すると、Cisco TMS のアベイラビリティは向上しますが、Cisco TMS のスケーラビリティが増加することはまったくありません。

代替設定を使用したその他のモデルのロード バランサも Cisco TMS で動作する可能性はありますが、シスコによるテストは行われていません。

ライセンシング

冗長 Cisco TMS 実装で使用できるライブ データベースは 1 つだけです。このため、両方のサーバでは同じ Cisco TMS シリアル番号、および同じリリース キーとオプション キーのセットを使用します。

データベースの冗長性

Cisco TMS は SQL データベースに大きく依存しているため、完全な耐障害性 Cisco TMS ソリューションでは、SQL Server 2012 で提供される高可用性テクノロジーのうちの 1 つも使用します。

Cisco TelePresence Management Suite Provisioning Extension

冗長環境における Cisco TMSPE の実装については、『Provisioning Extension Deployment Guides』に記載されています。

ロード バランサを使用した冗長展開の制限

Cisco TMS 環境に冗長性を実装する場合は、次のことに注意してください。

- システムのシステム接続性設定の自動更新（[管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）] > [システムのシステム接続性の更新（Update System Connectivity for Systems）]）は、冗長環境では無効化されます。
- 電話帳と Active Directory の同期などのタスクは、次の場合にフェールオーバーが実行されると失敗する可能性があります。
  - タスクの実行中。
  - タスクの実行がスケジュールされている直前。
- 割り当てと接続の再試行の頻度によって、会議がフェールオーバー中に影響を受けることはありません。
- 独自の予約クライアントまたはサード パーティの予約クライアントを使用している場合、バージョン 13 の Cisco TMSBA で導入されたクライアント セッション メカニズムを使用する必要があります。詳細については、『Cisco TMS Booking API Programming Reference Guide』を参照してください。

冗長展開の設定

ロード バランサを使用した展開

ネットワーク ロード バランサ（NLB）を使用して 2 台の Cisco TMS サーバ（この場合は「ノード」とも呼びます）を構成すると、完全な自動フェールオーバーを備えた、真に冗長性のある Cisco TMS セットアップが実現します。

推奨ハードウェア

新しく展開する場合は、F5 BIG-IP ロード バランサを使用することをお勧めします。現在は Cisco ACE 4710 Application Control Engine アプライアンスの使用もサポートされていますが、このロード バランサは将来のバージョンの Cisco TMS ではサポートされなくなります。

Active Directory およびユーザ認証の要件

- 両方の Cisco TMS サーバは同じ Windows ドメインのメンバーである必要があります。
- すべての Cisco TMS ユーザは Active Directory からインポートされ、Active Directory に対して認証されます。
- ローカル ユーザ アカウントを使用することは、この冗長モデルではサポートされません。

概要

ノード

Cisco TMS は、ネットワーク ロード バランサ（NLB）の内部に展開されると、クラスタ対応アプリケーションになります。2 台の Cisco TMS サーバを同じ tmsng データベースに接続して、[管理ツール（Administrative Tools）] > [設定（Configuration）] > [一般設定（General Settings）] で冗長性を有効にした場合、片方のサーバはただちにアクティブ ノードになり、もう片方はパッシブ ノードになります。アクティブにできるノードは、常に 1 つだけです。

アクティブ ノードの動作は、スタンドアロンの Cisco TMS サーバと完全に同じです。

パッシブ ノードの動作は以下のとおりです。

- Web ページとサービスがロック ダウンされたスタンバイ モードのままになります。
- ユーザおよび管理対象システムからのすべての着信トラフィックを拒否します。

ノードがパッシブである間は、Cisco TMS の全体のパフォーマンスをパッシブ ノードがほとんど変化させないように、tmsng データベースへのトラフィックは最小限に抑えられます。

冗長展開の設定

フェールオーバー

ノードのステータスがパッシブとアクティブ間で切り替わるプロセスは、フェールオーバーと呼ばれます。フェールオーバーは、自動的に起きる場合も、管理者によって手動で開始される場合もあります。

自動フェールオーバーは、以下のいずれかの場合に行われます。

- アクティブ ノードが、自身のサービスの応答がないか、無効化されていることを検出した場合。
- パッシブノードが、アクティブ ノードのサービスの応答がないか、無効化されていることを検出した場合。

フェールオーバーが開始されると、それまでパッシブであったノードはすぐにアクティブに変更され、同時にそれまでアクティブであったノードは、自身のサービスと Web インターフェイスをスタンバイ モードへと後退させます。この変更が NLB に検出されるまでには最大で 1 分かかる可能性があり、この間、Cisco TMS がほとんど利用不可能になります。このため、手動フェールオーバーの開始は、通常の業務時間外に限って行う必要があります。

Cisco TMS は、単純な計数メカニズムを使用して、自動フェールオーバーを開始すべきかどうかを決定します。そのプロセスは次のとおりです。

1. アクティブ ノードとパッシブ ノードの両方の各 Cisco TMS サービス（IIS を含む）は、最後に機能していた時期を示すキープアライブ通知を tmsng データベースに連続的に書き込みます。
2. アクティブ ノードはこのサービスとタイムスタンプのリストを監視し、過去 1 分間に通知を送信したサービスを使用可能であると分類します。アクティブ ノードは、自身よりもパッシブ ノードの方が多くのサービスを使用中であるとみなした場合に、制御を回収してパッシブ ノードに渡します。その後、パッシブ ノードがアクティブになります。
3. フォールバック メカニズムと同様に、パッシブ ノードもタイムスタンプを監視し、アクティブ ノードがキープアライブ通知の書き込みを停止した場合にフェールオーバーを強制的に開始します。

ネットワーク ロード バランサ

NLB は両方のノードのステータスを監視して、すべての着信トラフィックをアクティブ ノードにのみ転送します。フェールオーバーが行われた場合を除いて、着信トラフィックがパッシブ ノードに転送されることはありません（「概要」（34 ページ）を参照してください）。

ノードのステータスを監視するには、（[管理ツール（Administrative Tools）] > [TMS サーバ メンテナンス（TMS Server Maintenance）] に表示される）特定の URL を 5 秒ごとに両方のノードで検出するように、NLB を設定する必要があります。Cisco TMS の両方のノードが自身へのアクセス頻度の記録を保持するため、この URL の精査は別の目的にも役立ちます。ノードは、この URL へのプローブ要求の受信を停止した場合、NLB と自身の間のネットワーク リンクがダウンしたとみなして、その IIS サービスを非アクティブであるとマークします。これがアクティブ ノードで起きた場合、上記のようにフェールオーバーが作動されます。

冗長展開の設定

ネットワーク トポロジおよび管理対象システムとの通信

ユーザおよび管理対象システムからの着信ネットワーク トラフィックは、NLB を経由して Cisco TMS サーバにルーティングされます。仮想 IP アドレス（VIP）を NLB に割り当てるとともに、NLB の VIP を指す DNS レコードを作成する必要があります。その後、VIP（または関連付けられた DNS レコード）を、すべての管理対象システムの管理アドレスとフィードバック アドレスとして使用します。

NLB のホスト名と IP アドレスは、Cisco TMS の [管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）] > [内部 LAN のシステムの高度なネットワーク設定（Advanced Network Settings for Systems on Internal LAN）] および [パブリック インターネット上/ファイアウォールの背後のシステムの高度なネットワーク設定（Advanced Network Settings for Systems on Public Internet/Behind Firewall）] に入力する必要があります。

[ネットワーク設定（Network Settings）] の IP アドレスとホスト名の値が変更されると、データベース スキャナ サービスがこれらの新規ネットワーク設定を管理対象のシステムに適用します。その後、システムは NLB へのトラフィックの転送を開始し、NLB はこれらの要求を Cisco TMS サーバに転送します。

Cisco TMS 自身のサービスからの発信トラフィックは NLB を経由しないため、Cisco TMS のアクティブ ノードは、システムを管理するときに NLB をバイパスします。このため、IP プロトコル ヘッダーに基づいてシステムの接続設定とパラメータを自動更新する Cisco TMS のロジックは、Cisco TMS の冗長性が有効化されると無効になります。Cisco TMS が管理対象システムと通信する方法の詳細については、『Cisco TMS Administrator Guide』の「*System management overview*」の章を参照してください。

冗長性のある Cisco TMS ソリューションの導入後にネットワークに重大な変更を行った場合、Cisco TMS と管理対象システムの間のシステム接続がネットワークの変更後も機能していることを手動で検証する必要があります。接続を検証する必要がある変更の例としては、管理対象システムと Cisco TMS の間への新しいプロキシの導入が挙げられます。

この構成の実施方法については、「ロード バランサを使用した展開」（34 ページ）を参照してください。

アーキテクチャの概要およびネットワーク構成図

設定例

次の例では、次の値が使用されます。

表 2　VLAN200

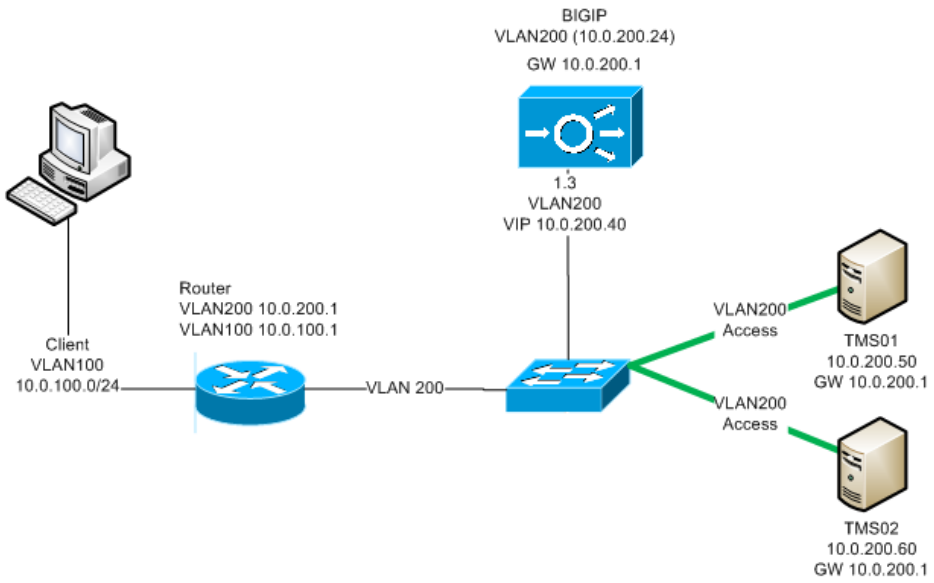
デバイス	IP アドレス	ホストネーム
F5 BIG-IP 仮想 IP アドレス	10.0.200.40	tms.example.com
tms01	10.0.200.50	tms01.example.com
tms02	10.0.200.60	tms02.example.com

冗長展開の設定

表 3　VLAN100

デバイス	IP アドレス	ホストネーム
管理対象システムとユーザ	10.0.100.0/24	

- VLAN200 および VLAN100 という 2 つの仮想 LAN があります。
- F5 BIG-IP は VLAN200 上に設定されています。
- 2 台の Cisco TMS サーバ（10.0.200.50 の tms01 および 10.0.200.60 の tms02）は VLAN200 上に設定されています。
- すべてのクライアント（管理対象システムおよびユーザ）は VLAN100 で設定されています。
- F5 BIG-IP の仮想 IP アドレスへのトラフィックはすべて、2 台の Cisco TMS サーバの 1 つに転送されます。
- すべての管理対象システムとユーザは、Cisco TMS との通信時に F5 BIG-IP の仮想 IP アドレスを使用します。
- 2 台の Cisco TMS サーバは、共通の外部 tmsng データベースを共有しています。



インストールと設定

tms01 への Cisco TMS のインストール

1. Cisco TMS をインストールする前に、外部サーバに SQL サーバ インスタンスを設定します。
2. 「インストーラの実行」（24 ページ）に記載されている手順を使用して、最初のノードに Cisco TMS をインストールします。
3. Cisco TMS に外部データベース サーバを指定します。
4. インストール中に生成された暗号キーを書き留めておきます。

5. インストール時に HTTPS を有効にする場合は、tms.example.com に発行された証明書を使用します。
6. Cisco TMS Web アプリケーションにログインして正しく動作することを確認します。
7. [管理ツール（Administrative Tools）] > [一般設定（General Settings）] > [TMS の冗長性の有効化（Enable TMS Redundancy）] の順に移動して、[はい（Yes）] を選択します。

   この設定を [はい（Yes）] にすると、[管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）] > [システムのシステム接続性の更新（Update System Connectivity for Systems）] の設定が自動的に無効化されることに注意してください。

tms02 への Cisco TMS のインストール

1. tms02 のサービス パック レベルを含むオペレーティング システムが正確に tms01 上のものと同じであることを確認します。
2. 両方のサーバが同じタイム ゾーンに設定されていること、および時計が同期されていることを確認します。
3. tms01 の設定時と同じ外部データベース サーバとインストール ディレクトリを使用して、Cisco TMS をインストールします。同じバージョンの Cisco TMS をインストールします。
4. tms01 のインストール中に生成された暗号キーを入力します。（暗号キーを上記のステップ 4 で書き留めていない場合は、tms01 の [TMS ツール（TMS Tools）] の [セキュリティ設定（Security Settings）] で確認できます）。
5. HTTPS を有効にするときに tms01 で使用した証明書と同じ証明書を使用します。
6. Cisco TMS にログインします。Cisco TMS が利用できないことを示すエラーが表示されれば成功です。

手動フェールオーバーのテスト

1. tms01 の IP/ホスト名にアクセスします。
2. [管理ツール（Administrative tools）] > [TMS サーバ メンテナンス（TMS Server Maintenance）] > [TMS の冗長性（TMS Redundancy）] の順に移動します。
3. どちらのノードがアクティブであるかを記録し、[アクティブ ノードのリタイア（Retire Active Node）] をクリックします。
4. Cisco TMS Web ページをリフレッシュします。
5. 「*Cisco TMS が利用できません（Cisco TMS is unavailable）*」というエラーが表示されれば成功です。
6. tms02 の IP/ホスト名にアクセスします。

   もう片方のノードがアクティブになっていることが表示されれば成功です。Cisco TMS にアクセスできます。

ネットワーク ロード バランサの設定

第 2 ノードが動作可能になったら、ネットワーク ロード バランサを設定します。

1. HTTP 接続と HTTPS 接続、および SNMP トラップをアクティブ ノードに転送するように NLB を設定します。
2. Polycom の電話帳を動作させるために、TCP ポート 3601 をアクティブ ノードに転送するように NLB を設定します。

3. プローブ URL をプローブするように NLB を設定します。
   a. 両方のノードの Cisco TMS で [管理ツール（Administrative Tools）] > [TMS サーバ メンテナンス（TMS Server Maintenance）] > [TMS の冗長性（TMS Redundancy）] > [プローブ URL（Probe URL）] に表示される URL をプローブするように、NLB を設定します。これらの URL は、積極的（可能であれば 5 秒ごと）にプローブする必要があります。
   b. すべてのトラフィックをアクティブ ノード（HTTP 200 に応答する方のノード）にプッシュします。

注：プローブ URL は、その他のモニタリング アプリケーションにモニタされないようにしてください。

F5 BIG-IP の設定については、「F5 BIG-IP の設定例」（49 ページ）を参照してください。

Cisco TMS の設定

アクティブ ノードで次の操作を実行します。

1. Cisco TMS アプリケーションで、[管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）] の順に移動します。
2. 次の IP アドレスとホスト名を、NLB の仮想 IP アドレスとホスト名に変更します。
   - [イベント通知（Event Notification）] > [SNMP トラップホスト IP アドレス（SNMP Traphost IP Address）]
   - [社内 LAN のシステムの詳細ネットワーク設定（Advanced Network Settings for Systems on Internal LAN）]：すべてのフィールド
   - **公共インターネット/ファイアウォール外のシステムの詳細ネットワーク設定（Advanced Network Settings for Systems on Public Internet/Behind Firewall）**

両方のノードにおいて：

Cisco TMS サーバのブラウザを使用していくつかの管理対象システムの Web インターフェイスにアクセスし、Cisco TMS サーバが管理対象システムに到達できること、およびその逆も可能かどうかを確認します。

ローカル ファイルの同期

Cisco TMS によって使用されるカスタマイズ可能なファイルの中には、tmsng データベース内ではなく Windows サーバのローカルのファイル システム内に保存されるものがあります。これらのファイルが保存されるフォルダは、2 つのサーバ間で同期させる必要があります。同期させる必要があるすべてのフォルダのリストについては、「同期するローカル ファイル」（50 ページ）を参照してください。

DFS レプリケーションを使用して、2 つのノード間でフォルダの同期を行います。

冗長展開の設定

オプション：TLS クライアント証明書の使用の有効化

展開で TLS クライアント証明書の使用を選択していない場合は、以下を確認する必要があります。

- 同じオプションが両方のサーバの Cisco TMS Tools で選択されます。
- 両方のサーバにインポートされる TLS 証明書は同じです。
- 両方のサーバが証明書の失効に同じ機能を使用します。

詳細については、『Cisco TMS Administrator Guide』の「Cisco TMS Tools」の章を参照してください。

フェールオーバーの動作のテスト

1. NLB の VIP を使用して Cisco TMS にログインします。
2. 手動フェールオーバーを強制実行します。
3. 1 分間待ってから、ブラウザを更新します。
4. [管理ツール（Administrative Tools）] > [TMS サーバ メンテナンス（TMS Server Maintenance）] > [TMS の冗長性（TMS Redundancy）] の順に移動し、[フェールオーバーのアクティビティ ログ（Failover Activity Log）] を見て、フェールオーバーが実際に行われたことを確認します。

Cisco TMS のアップグレード

アップグレードを行うとユーザが短い間 Cisco TMS を使用できなくなるため、最新のソフトウェア バージョンへの Cisco TMS のアップグレードはメンテナンス時間帯に行う必要があります。

2 台の Cisco TMS ノードは共通のデータベースを共有しているため、常に同じソフトウェア バージョンを実行する必要があります。したがって、一方のノードを一度にアップグレードし、他方のノードがシステムおよびユーザに対して機能できる状態を保つことは不可能です。

1. 両方の Cisco TMS Windows サーバにログインします。
2. ローカル ファイルの同期を一時的に停止するためにファイル複製を無効にします。
3. 両方のノードのすべての TMS サービス、IIS サービスを停止します。
4. 一方のノードを新しいソフトウェア バージョンにアップグレードします。これは tmsng データベースをアップグレードします。
5. このサーバの Cisco TMS Web アプリケーションにログインして、正常に動作していることを確認します。

NLB のプローブが、アップグレードしたサーバがアクティブ ノードであると認識するようになります。これで、ユーザと管理対象システムは再び Cisco TMS を使用できるようになります。

1. 2 番目の Cisco TMS ノードをアップグレードします。
2. インストーラはデータベースがアップグレード済みであることを検出し、更新されたデータベースの使用を継続するよう求めます。[はい（Yes）] を選択します。インストーラは、次にバイナリを更新し、データベースを放置します。

3. アクティブ サーバの Cisco TMS Web アプリケーションにログインし、手動フェールオーバーを強制実行します。2 番目のサーバが 1 分以内にアクティブになることを確認します。
4. ファイル複製を有効にします。

ネットワーク設定がインストール処理中に変更されていないことを確認してください。

1. Cisco TMS アプリケーションで、[管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）] の順に移動します。
2. 次の IP アドレスとホスト名が、NLB の仮想 IP アドレスとホスト名に設定されていることを確認します。
   - [イベント通知（Event Notification）] > [SNMP トラップホスト IP アドレス（SNMP Traphost IP Address）]
   - [社内 LAN のシステムの詳細ネットワーク設定（Advanced Network Settings for Systems on Internal LAN）]：すべてのフィールド
   - **公共インターネット/ファイアウォール外のシステムの詳細ネットワーク設定（Advanced Network Settings for Systems on Public Internet/Behind Firewall）**

ノードに障害が発生した場合のリカバリ

サーバ障害の場合、緊急措置は必要ありません。パッシブ ノードがダウンした場合、アクティブ ノードは通常どおりに動作を続けます。アクティブ ノードがダウンした場合、パッシブ ノードが自動的にアクティブになるとともに、NLB が障害を検出し、すべてのトラフィックを新しくアクティブになったノードに転送します。

フェールオーバーの実行には約 1 分の遅れが予想されます。この間、Web ページには「Cisco TMS に接続できません（Unable to connect to Cisco TMS）」というエラーが表示されます。

通常行うように、失敗したノードのソフトウェアとハードウェアのトラブルシューティングを実行し、動作可能になったらオンラインに戻してください。

冗長展開の管理対象システムのトラブルシューティング

アクティブ Cisco TMS サーバの Wireshark トレースをキャプチャすると、NLB から入ってくるすべての着信トラフィックが表示されます。したがって、Cisco TMS と目的の管理対象システムの間の通信を簡単に特定することはできません。

トラブルシューティングを開始する前に、次の手順を実行します。

1. 調査するすべてのシステムの管理アドレスを、一時的にアクティブ Cisco TMS サーバのアドレスに設定します。
2. Wireshark キャプチャを行います。
3. トレースが完了したら、すべてのシステムの管理アドレスを NLB のアドレスに戻します。

冗長展開の設定

ログ

- ログ ファイルは両方の Cisco TMS サーバから収集する必要があります。
- ログ レベルを変更する場合は、両方のサーバで行うようにしてください。ログ レベルを上げ、問題を再現してからすぐに元のログ レベルに戻すなど、ごくわずかな時間だけログ レベルを変更する場合はこの必要はありません。

ホット スタンバイの展開

障害に備えて追加の Cisco TMS サーバをウォーム スペアとして保持することは、「ホット スタンバイ」冗長性モデルと呼ばれます。これは、プライマリ Cisco TMS サーバに障害が発生した場合に手動による介入が必要になるため、フェールオーバー ソリューションではなくスイッチオーバー ソリューションです。

この冗長性モデルでは、常に 1 台の Cisco TMS サーバがアクティブです。ホット スタンバイ サーバは、プライマリ サーバで障害が発生した場合に数分以内にアクティベーションを行う準備ができているように、セキュリティ パッチおよび他のアップグレードで最新の状態に保つ必要があります。

ホット スタンバイ冗長モデルでは tmsng データベースを外部 SQL サーバに配置する必要があること、および 2 台の Cisco TMS サーバが同じ Windows ドメイン内にある必要があることに注意してください。

この展開では、[一般設定（General Settings）] > [TMS 冗長性の有効化（Enable TMS Redundancy）] を使用して冗長性を有効化することはしないでください。

下の手順では次の例が使用されます。

サーバ	DNS 名	IP アドレス
プライマリ Cisco TMS サーバ（tms01）	tms01.example.com	10.0.0.10
セカンダリ Cisco TMS サーバ（tms02）	tms02.example.com	10.0.0.11

これらの例では、IPv4 を使用することを前提としています。また IPv6 を使用する場合は、IPv6 アドレスを適宜変更します。

プライマリ Cisco TMS サーバの設定

Cisco TMS をインストールする前に次の手順を実行します。

1. 外部サーバ上の SQL サーバ インスタンスを設定します。
2. プライマリ サーバ tms01 の IP アドレス（10.0.0.10）を指すように、DNS レコード tms.example.com を設定します。

Cisco TMS をインストールするには次の操作を実行します。

1. 『Cisco TMS Installation and Getting Started Guide』の手順に従って tms01 に Cisco TMS をインストールし、Cisco TMS が上記のステップ 1 で使用した外部データベース サーバをポイントするようにします。

2. インストール中に生成された暗号キーを書き留めておきます。
3. インストール時に HTTPS を有効にする場合は、tms.example.com に発行された証明書を使用します。
4. Cisco TMS Web アプリケーションにログインして正しく動作することを確認します。

すべてのユーザと管理対象システムは、Cisco TMS への接続時に tms.example.com を使用する必要があります。サーバの独自のホスト名（tms01.example.com）を使用してはいけません。

Cisco TMS のインストールが成功したことを確認してから、次の操作を実行します。

1. Cisco TMS で、[管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）] の順に移動します。
2. [TMS サーバの完全修飾ホスト名（TMS Server Fully Qualified Hostname）] フィールドおよび [TMS サーバ アドレス（完全修飾ホスト名または IPv4 アドレス）（TMS Server Address (Fully Qualified Hostname or IPv4 Address)）] フィールドに、*tms.example.com* と入力します。

Cisco TMS にログインするときに、ローカル ユーザ アカウントは使用しないでください。セカンダリ サーバ tms02 にスワップしなければならない場合に使用可能なように、すべてのユーザ アカウントがドメイン アカウントでなければなりません。

セカンダリ Cisco TMS サーバの設定

1. tms02 のサービス パック レベルを含むオペレーティング システムが正確に tms01 上のものと同じであることを確認します。
2. サーバが同じ時間帯に設定されていることを確認します。同じに設定されていないと、スケジュールされた会議の開始および終了時刻はスイッチオーバー時に不正であることを意味します。
3. tms02 で Cisco TMS インストーラを実行します。
    a. 求められたら、外部 SQL サーバの IP アドレスを入力します。
    b. tms01 上と同じディレクトリにインストールし、tms01 上と同じログ ディレクトリを使用します。これは、ログ ディレクトリのパスが SQL データベースではなく Windows に環境変数として保存されるため重要です。
    c. tms01 のインストール中に生成された暗号キーを入力します。
    d. HTTPS を有効にするときに tms01 で使用した証明書と同じ証明書を使用します。
4. Cisco TMS Web アプリケーションにログインして正しく動作することを確認します。
5. tms02 で、[管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）] > [内部 LAN のシステムの高度なネットワーク設定（Advanced Network Settings for Systems on Internal LAN）] の順に移動します。インストーラがこれらの値を変更した可能性があるため、IP アドレスが tms01（10.0.0.10）で、ホスト名が tms.example.com であることを確認します。
6. tms02 でサービス管理コンソールを開きます。
    - すべての Cisco TMS サービス（名前はすべて TMS から始まります）を停止します。
    - World Wide Web Publishing Service という名前の Internet Information Services（IIS）サービスを停止します。
    - IIS と TMS サービスのスタートアップの種類を [手動（Manual）] に設定します。

これで Tms02 は tms01 で障害が起きた場合にウォーム スペアとして動作するように準備できました。

[管理ツール（Administrative Tools）] > [サーバ メンテナンス（Server Maintenance）] > [TMS サービス ステータス（TMS Service Status）] では、両方のサーバのサービスが表示されることに注意してください。リストから tms02 の停止したサービスを削除するには、[リストのクリア（Clear List）] をクリックします。

ローカル ファイルの同期

Cisco TMS によって使用されるカスタマイズ可能なファイルの中には、tmsng データベース内ではなく Windows サーバのローカルのファイル システム内に保存されるものがあります。これらのファイルが保存されるフォルダは、2 つのサーバ間で同期させる必要があります。同期させる必要があるすべてのフォルダのリストについては、「同期するローカル ファイル」（50 ページ）を参照してください。

DFS レプリケーションを使用して、2 つのノード間でフォルダの同期を行います。

プライマリ サーバに障害が発生した場合に 2 台のサーバをスワップする場合は、tms02 から tms01 に同期化するように、tms01 および tms02 のフォルダを同期するように設定した同期メカニズムを変更します。

オプション：TLS クライアント証明書の有効化

展開で TLS クライアント証明書の使用を選択していない場合は、以下を確認する必要があります。

- 同じオプションが両方のサーバの Cisco TMS Tools で選択されます。
- 両方のサーバにインポートされる TLS 証明書は同じです。
- 両方のサーバが証明書の失効に同じ機能を使用します。

詳細については、『Cisco TMS Administrator Guide』の「Cisco TMS Tools」の章を参照してください。

Cisco TMS のアップグレード

プライマリ サーバとセカンダリ サーバの Cisco TMS のソフトウェア バージョンは一致させる必要があります。プライマリ サーバをアップグレードした後で、セカンダリ サーバをできるだけ早くアップグレードする必要があります。セカンダリ サーバのソフトウェア バージョンが古い状態でプライマリ サーバに障害が発生した場合、セカンダリ サーバを新しい Cisco TMS のソフトウェア バージョンにアップグレードするまで、サーバをスワップできません。

1. ローカル ファイルの同期を一時的に停止するためにファイル複製を無効にします。
2. プライマリ サーバをアップグレードします。
3. セカンダリ サーバをアップグレードします。
4. Cisco TMS Web アプリケーションにログインして正しく動作することを確認します。

5. Cisco TMS アプリケーションで、[管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）] の順に移動します。
6. 次の IP アドレスとホスト名が、IP アドレス 10.0.0.10 とホスト名 tms.example.com に設定されていることを確認します。
   - [イベント通知（Event Notification）] > [SNMP トラップホスト IP アドレス（SNMP Traphost IP Address）]
   - [社内 LAN のシステムの詳細ネットワーク設定（Advanced Network Settings for Systems on Internal LAN）]：すべてのフィールド
   - **公共インターネット/ファイアウォール外のシステムの詳細ネットワーク設定（Advanced Network Settings for Systems on Public Internet/Behind Firewall）**
7. TMS サービスを停止し、手動に再度設定します。
8. ファイル複製を有効にします。

プライマリ サーバで障害が発生した場合のリカバリ

プライマリ サーバ tms01 が故障して使用不能になった場合、セカンダリ サーバ tms02 を動作状態に変更するのに何分もかかりません。

1. ネットワークから tms01 を外します。
2. tms02 の IP アドレスを tms01 の古い IP アドレス、たとえば 10.0.0.10 に変更します。
3. tms02 がその新しい IP アドレスで接続可能であることを確認します。
4. Cisco TMS Tools アプリケーションを開き、[設定（Configuration）] > [データベース接続設定の変更（Change DB Connection Settings）] の順に移動します。
5. 最初に tms02 を設定してからデータベースへのパスワードが変更された可能性があるため、[OK] をクリックして tms02 のパスワードが正しいままであることを確認します。
6. サービス管理コンソールで次の操作を行います。
   a. すべての TMS サービスと World Wide Web 発行サービスの起動タイプを[自動（Automatic）] に設定します。
   b. サービスを開始します。

これで、tms02 がアクティブな Cisco TMS サーバになります。Cisco TMS との通信時に tms.example.com を使用するように管理対象サービスを設定済みのため、管理対象自体の再設定は必要ありません。

tms02 が正しく動作することを確認するには：

1. 短い会議をこの先 2 分にスケジュールします。
2. これが正しく起動し、期待どおりに切断されることを認識します。
3. [会議制御センター（Conference Control Center）] を使用してこの会議を監視できることを確認します。
4. Cisco TMS がこの会議のコール詳細レコード（CDR）を生成することを確認します。

Cisco TMS がシステムと通信していることを確認するために、次の操作を実行します。

1. TMS データベース スキャナ サービスが完全な実行を完了まで約 20 分待機します。
2. Cisco TMS で、[システム（Systems）] > [システム概要（System Overview）] の順に移動します。

3. 左側のツリーにあるすべてのシステムを選択し、右側のツリーで[ネットワーク設定（Network Settings）] > [TMS とシステムの接続性（TMS To System Connectivity）] の順に選択します。
4. [表示（View）] をクリックして、すべてのシステムの [ステータス（Status）] が [応答なし（NoResponse）] に設定されていないことを確認します。

[管理ツール（Administrative Tools）] > [サーバ メンテナンス（Server Maintenance）] > [TMS サービス ステータス（TMS Service Status）] では、両方のサーバのサービスが表示されることに注意してください。リストから tms01 の停止したサービスを削除するには、[リストのクリア（Clear List）] をクリックします。

ネットワークに tms01 を接続する前に：

1. その IP アドレスを tms02 の古い値、たとえば 10.0.0.11 に変更します。
2. すべての TMS サービスおよび IIS をディセーブルにします。

tms01 の問題が解決したら、それは tms02 がダウンするとウォーム スペアになります。

注：IP アドレスを新しい値に変更する前に、tms01 をネットワークに戻さないでください。このようにすると、IP アドレスの競合が発生し、Cisco TMS の予期しない動作の原因となります。

バージョン 14.4 以降からの冗長展開のアップグレード

サーバをアップグレードする前に

両方の Cisco TMS サーバで次の操作を行います。

1. ローカル ファイルの同期を一時的に停止するためにファイル複製を無効にします。
2. すべての TMS サービスおよび IIS サービスを停止します。

プライマリ ノードのアップグレード

1. 通常の方法で、プライマリ Cisco TMS サーバをアップグレードします。
2. [管理ツール（Administrative Tools）] > [TMS サーバ メンテナンス（TMS Server Maintenance）] の順に移動し、[TMS の冗長性（TMS Redundancy）] セクションでサーバが [アクティブ（Active）] とリストされていることを確認します。[パッシブ（Passive）] とリストされている場合は、データが正しく更新されるまで最大で 1 分間、[更新（Refresh）] を繰り返しクリックします。

セカンダリ ノードのアップグレード

1. 通常の方法で、セカンダリ Cisco TMS サーバをアップグレードします。
2. NLB の仮想 IP を介して [管理ツール（Administrative Tools）] > [TMS サーバ メンテナンス（TMS Server Maintenance）] の順に移動し、[TMS の冗長性（TMS Redundancy）] セクションで、2 番目のサーバが [パッシブ（Passive）] と表示されていることを確認します。

3. [TMS サービスのステータス（TMS Services Status）] セクションで、パッシブ ノードのすべての TMS サービス（TMSProbeURL を含む）が [サービスはスタンバイ状態（Service On Standby）] と表示されていることを確認します。
4. 「手動フェールオーバーのテスト」（38 ページ）の手順に従って、手動フェールオーバーをテストします。
5. 2 つの Cisco TMS ノード間のローカル ファイル レプリケーションを再び有効化します。

バージョン 14.4 より前の Cisco TMS からの冗長展開のアップグレード

バージョン 14.4 より前の Cisco TMS から 冗長 Cisco TMS 展開をアップグレードするには、ネットワーク ロード バランサ（NLB）の設定を変更する必要があります。アップグレードをする前に「冗長展開の設定」（32 ページ）を読んで、新しい推奨 NLB 設定をよく理解してください。

サーバをアップグレードする前に

両方の Cisco TMS サーバで次の操作を行います。

1. ローカル ファイルの同期を一時的に停止するためにファイル複製を無効にします。
2. すべての TMS サービスおよび IIS サービスを停止します。
3. サーバがデフォルト ゲートウェイとして NLB を使用しないように、デフォルト ゲートウェイを変更します。
4. 管理対象システムの Web インターフェイスにアクセスするなどして、管理対象システムのネットワークに接続できることを確認します。

プライマリ サーバのアップグレードと設定

1. 通常の方法で、プライマリ Cisco TMS サーバをアップグレードします。
2. アップグレードが完了したら、Cisco TMS Web インターフェイスにログインします。[管理ツール（Administrative Tools）] > [設定（Configuration）] > [一般設定（General Settings）] の順に移動し、[TMS の冗長性の有効化（Enable TMS Redundancy）] を [はい（Yes）] に設定します。
3. [管理ツール（Administrative Tools）] > [TMS サーバ メンテナンス（TMS Server Maintenance）] の順に移動し、[TMS の冗長性（TMS Redundancy）] セクションでサーバが [アクティブ（Active）] とリストされていることを確認します。[パッシブ（Passive）] とリストされている場合は、データが正しく更新されるまで最大で 1 分間、[更新（Refresh）] をクリックします。
4. [プローブ URL（Probe URL）] をメモします。

プライマリ サーバでの NLB 設定の更新と検証

1. 「ACE 設定の移行」（48 ページ）） で説明されているように NLB を移行します。上記ステップ 4 のプローブ URL を使用します。

セカンダリ サーバはまだアップグレードされていないため、セカンダリ サーバのプローブはこの段階では失敗することに注意してください。

2. プライマリ サーバで [管理ツール（Administrative Tools）] > [TMS サーバ メンテナンス（TMS Server Maintenance）] の順に移動し、[TMS サービスのステータス（TMS Services Status）] セクションのリストに [TMSProbeURL] が表示されていることを確認します。[管理ツール（Administrative Tools）] > [TMS サーバ メンテナンス（TMS Server Maintenance）] の順に移動して、[TMS サービスのステータス（TMS Services Status）] セクションのリストに [TMSProbeURL] が表示されていることを確認します。
3. ブラウザで NLB の仮想 IP アドレス（VIP）を入力し、Cisco TMS に転送されることを確認します。

セカンダリ サーバのアップグレードと設定

1. 通常の方法で、セカンダリ Cisco TMS サーバをアップグレードします。
2. NLB の VIP を介して [管理ツール（Administrative Tools）] > [TMS サーバ メンテナンス（TMS Server Maintenance）] の順に移動し、[TMS の冗長性（TMS Redundancy）] セクションで、2 番目のサーバが [パッシブ（Passive）] と表示されていることを確認します。
3. [TMS サービスのステータス（TMS Services Status）] セクションで、パッシブ ノードのすべての TMS サービス（TMSProbeURL を含む）が [サービスはスタンバイ状態（Service On Standby）] と表示されていることを確認します。
4. 「フェールオーバーの動作のテスト」（40 ページ）の手順に従って、手動フェールオーバーをテストします。
5. 2 つの Cisco TMS ノード間のローカル ファイル レプリケーションを再び有効化します。

ACE 設定の移行

Cisco ACE 4710 Appliance Control Engine ロード バランサを『Cisco TelePresence Management Suite Administrator Guide (14.3.2)』の「*ACE 設定例(Example ACE configuration)*」に従って設定し、Cisco TMS とロード バランサのみを併用しているという前提のもとでこの設定を適用することにより、ロード バランサが Cisco TMS 14.4 で新しく導入された冗長性モデルと適切に動作するようになります。

```
!CHANGING AN EXISTING PROBE
 probe http PROBE-HTTP-80
 no expect status 200 499
 description Probing TMS Redundancy URL
 port 80
 interval 2
 faildetect 1
 passdetect interval 2

!THIS IS THE PROBE URL PROVIDED BY CISCO TMS.CHANGE TO THE GUID OF YOUR CISCO TMS.NOTE: IF THE ? IS STRIPPED
OUT, ENTER: CTRL+V BEFORE THE ?
 request method head url /tms/public/IsAlive.aspx?guid=1cd4cd49-1ef5-4319-9bb5-e3ab87345997
 expect status 200 200
 open 1
 serverfarm host SFARM-TMS-WEB-443

!ADD A NEW PROBE FOR HTTP
 probe PROBE-HTTP-80
```

冗長展開の設定

```
!REMOVE UNUSED PROBES FROM THE SERVER FARM
 no probe BOOKING-PROBE-TMS
 no probe TMS-Monitoring-443
 no probe TMS-WEBSERVICES-443
 no probe CITIES-PROBE-TCP-443

!ENABLE NAT ON THE VIRTUAL SERVERS
 policy-map multi-match L4-POLICY-TMS-WEB
 class L4-CLASS-TMS-WEB-162
 nat dynamic 1 vlan 200
 class L4-CLASS-TMS-WEB-161
 nat dynamic 1 vlan 200
 class L4-CLASS-TMS-WEB-80
 nat dynamic 1 vlan 200
 class L4-CLASS-TMS-WEB-443

!SELECT THE CORRECT VLAN
 nat dynamic 1 vlan 200

!DELETE UNUSED PROBES
 no probe https TMS-Monitoring-443
 no probe http TMS-Monitoring-80
 no probe https TMS-WEBSERVICES-443
 no probe https CITIES-PROBE-TCP-443
 no probe https BOOKING-PROBE-TMS

!CONFIGURE A NAT POOL ON THE CORRECT VLAN
 interface vlan 200

!CONFIGURE THE ADDRESS RANGE FOR NAT
 nat-pool 1 10.0.200.30 10.0.200.30 netmask 255.255.255.0 pat
```

F5 BIG-IP の設定例

F5 BIG-IP ロード バランサの初期設定の後で、以下の設定をコピーして貼り付けることで、お使いのロード バランサを設定することができます。すべての IP アドレス、DNS 名、ユーザ名、およびパスワードは、ロード バランサに設定を適用する前に、実際の設定を反映するように改める必要があります。

#CREATE VLAN 200 on BIGIP INTERFACE 1.3 tmsh create net vlan VLAN200 interfaces add {1.3} tag 200

#CREATE BIGIP SELF IP IN VLAN 200 tmsh create net self 10.0.200.24/24 vlan VLAN200 allow-service none

#CREATE TMS NODES tmsh create ltm node nd-TMS-01 address 10.0.200.50 monitor icmp description 'TMS NODE 01' tmsh create ltm node nd-TMS-02 address 10.0.200.60 monitor icmp description 'TMS NODE 02'

#CREATE MONITOR FOR TMS KEEPALIVE THE GUID IS FOUND IN TMS GUI tmsh create ltm monitor https mn-TMS-HTTPS {cipherlist DEFAULT:+SHA:+3DES:+kEDH compatibility enabled defaults-from https destination *:443 interval 5 password flott recv 200 recv-disable 503 send " HEAD /tms/public/IsAlive.aspx?guid=<CHANGE TO THE GUID OF YOUR CISCO TMS>\r\n" time-until-up 0 timeout 16 username 'domain\\username'}

#CREATE POOL USING OUR NEWLY CREATED MONITOR tmsh create ltm pool pl-TMS-HTTPS monitor mn-TMS-HTTPS members add {nd-TMS-01:443 nd-TMS-02:443}

冗長展開の設定

#CREATE VIRTUAL SERVER WITH VIP IP tmsh create ltm virtual vs-TMS-HTTPS {description "TMS Redundancy Virtual Server" destination 10.0.200.40:443 ip-protocol tcp mask 255.255.255.255 pool pl-TMS-HTTPS profiles add {fastL4} source 0.0.0.0/0 source-address-translation {type automap} translate-address enabled translate-port enabled vlans add {VLAN200} vlans-enabled}

#SAVE CONFIG tmsh save sys config

#END

同期用ローカル ファイル

Cisco TMS のインストール中に、冗長展開を使用する場合に 2 台のサーバ間で同期する必要のある、カスタマイズ可能ファイルが追加されます。

このようなファイルには、Cisco TMS にアップロード可能なソフトウェアおよびイメージ、Cisco TMS により作成されたイメージなどが含まれます。

デフォルトのインストールではファイルは次の場所に置かれます。

C:\Program Files (x86)\TANDBERG\TMS\Config\System\

C:\Program Files (x86)\TANDBERG\TMS\Data\GenericEndpoint\

C:\Program Files (x86)\TANDBERG\TMS\Data\SystemTemplate\

C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\CompanyLogo\

C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles\

C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware\

注：ディレクトリは初めて使用するときに作成されるため、これらのディレクトリはノード間のファイル レプリケーションの設定時に存在しない可能性があります。

Cisco TMS の移行またはアンインストール

この章では、Cisco TMS を新サーバに移行する手順と旧サーバからすべてのコンポーネントを削除する手順について説明します。

新しいサーバへの Cisco TMS の移行

サーバの使用を停止する場合でも、導入を拡大してより高いハードウェア機能が必要になる場合でも、Cisco TMS のインストールを別のサーバに移行する際は以下の手順に従ってください。

はじめる前に

- 可能な場合、同じ DNS ホスト名と IP アドレスを使用して、新しいサーバ上でネットワーク設定を同じ状態に保つことを推奨します。これは、移動後に必要な管理タスクを最小限に抑えます。
- 古いサーバと同じポートが新しいサーバのファイアウォールで開いていることを確認します。
- Cisco TMSPE が Cisco TMS サーバにインストールされている場合は、同時に移行する必要があります。

Cisco TelePresence Management Server（アプライアンス）

Cisco TelePresence Management Server（アプライアンス）を新しい Windows サーバに移動している場合、シスコの営業担当者にお問い合わせ頂き、Cisco TMS の新しいソフトウェア専用のコピーを購入してください。その後、ライセンス用ポータル サイトまたはライセンス サポート リクエスト フォームから グローバルライセンスオペレーション部門にお問い合わせいただき、オプション キーの再ホストを要求してください。

アプリケーションおよびデータベースの移行

インストール データのコピー

ローカルまたはリモートのデータベースとともに Cisco TMS を移行する前に、以下の作業を行ってください。

1. インストール プロセスで新サーバに入力する暗号キーの控えを作成します。Cisco TMS サーバで、TMS ツールを開き、[セキュリティ設定（Security Settings）] > [暗号化キー（Encryption Key）] の順に選択します。メモ帳ファイルにコピーします。
2. 同じ IP アドレスを維持し、外部の認証局からの TLS クライアント証明書を使用する場合、新しいサーバで使用するためにコピーを取得します。新サーバのホスト名が変わる場合は、新しい証明書を生成する必要があります。

Cisco TMS の移行またはアンインストール

SQL データベースが Cisco TMS サーバのローカルに保存される場合

両方のサーバで同バージョンの Cisco TMS を使用し、同じタイム ゾーンに設定する必要があります。

1. 元の Cisco TMS サーバですべての TMS サービスと IIS を停止します。
   a. サービス管理コンソールを開きます。
   b. すべての Cisco TMS サービス（名前はすべて TMS から始まります）を停止します。
   c. World Wide Web Publishing Service という名前の Internet Information Services（IIS）サービスを停止します。
2. SQL Server Management Studio Express を使用して SQL データベースのバックアップを作成し、tmsng.bak ファイルを新 Cisco TMS サーバにコピーします。
   a. tmsng データベースを右クリックします。
   b. [タスク（Tasks）] > [バックアップ（Back Up...）] **> [データベース（Database...）] の順に選択します。**
   c. バックアップの保存先のパスをメモし、[OK] をクリックします。
   d. バックアップ先の場所から新サーバ上の場所に tmsng.bak ファイルをコピーします。
3. 同バージョンの Cisco TMS を新サーバにインストールします。
   a. [データベースをこのサーバにインストール（Install the database on this server）] を選択します。
   b. リリースまたはオプション キーを入力しないでください。
   c. 旧サーバの [IP アドレス（IP Address）] を入力します。
   d. 旧サーバの [暗号化キー（Encryption Key）] を入力します。
4. SQL Server Management Studio Express を使用して、SQL データベースを復元します。
   a. tmsng データベースを右クリックします。
   b. [タスク（Tasks）] > [復元（Restore）] > [データベース（Database）] の順に選択します。
   c. [復元するバックアップ セットのソースと場所を指定（Specify the source and location of backup sets to restore）] で [デバイスから（From device）] を選択し、tmsng.bak ファイルを保存した場所を参照します。
   d. [データベースの復元 - tmsng（Restore Database - tmsng）] ウィンドウに戻るまで [OK] をクリックします。
   e. [復元するバックアップ セットを選択（Select the backup sets to restore）] で該当するバックアップ ファイルの横の [復元（Restore）] 列のチェックボックスをオンにします。[OK] をクリックします。
5. Cisco TMS Web アプリケーションを開いて、アプリケーションが動作し、すべてのデータが実装されていることを確認します。
6. 必要に応じて、元のサーバにローカルに保存された次のカスタマイズ可能なフォルダを新しいサーバ上の同じ場所にコピーします。これらのフォルダは最初の使用時に作成されるため、手動で作成しなければならない場合があります。デフォルトのインストールではファイルは次の場所に置かれます。
   - C:\Program Files (x86)\TANDBERG\TMS\Config\System\
   - C:\Program Files (x86)\TANDBERG\TMS\Data\GenericEndpoint\
   - C:\Program Files (x86)\TANDBERG\TMS\Data\SystemTemplate\
   - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\CompanyLogo\
   - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles\
   - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware\

SQL データベースがリモート サーバにある場合

この場合、インストール時にデータベースがアップグレードされるため、同バージョンの Cisco TMS を使用する必要はありません。

1. 元の Cisco TMS サーバですべての TMS サービスと IIS を停止します。
   a. サービス管理コンソールを開きます。
   b. すべての Cisco TMS サービス（名前はすべて TMS から始まります）を停止します。
   c. World Wide Web Publishing Service という名前の Internet Information Services（IIS）サービスを停止します。
2. 新サーバに Cisco TMS をインストールし、インストール時に既存の外部 SQL データベースを指定します。
3. Cisco TMS Web アプリケーションを開いて、アプリケーションが動作し、すべてのデータが実装されていることを確認します。
4. 必要に応じて、元のサーバにローカルに保存された次のカスタマイズ可能なフォルダを新しいサーバ上の同じ場所にコピーします。これらのフォルダは最初の使用時に作成されるため、手動で作成しなければならない場合があります。デフォルトのインストールではファイルは次の場所に置かれます。
   - C:\Program Files (x86)\TANDBERG\TMS\Config\System\
   - C:\Program Files (x86)\TANDBERG\TMS\Data\GenericEndpoint\
   - C:\Program Files (x86)\TANDBERG\TMS\Data\SystemTemplate\
   - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\CompanyLogo\
   - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles\
   - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware\

新しいネットワーク構成での移行

移行の一環として、Cisco TMS サーバの IP アドレスやホスト名まで変更する必要がある場合があります。

その場合は新サーバに Cisco TMS をインストールした後、データベースに接続されていること、すべてのデータが存在することを確認し、次の手順を実行します。

- [管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）] の順に移動し、[内部 LAN のシステムの高度なネットワーク設定（Advanced Network Settings for Systems on Internal LAN）] および [パブリック インターネット上またはファイアウォール内側のシステム向けの高度なネットワーク設定（Advanced Network Settings for Systems on Public Internet/Behind Firewall）] に Cisco TMS サーバの新しい IP アドレスとホスト名を入力します。
- [管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）] > [システム上の管理設定の強制（Enforce Management Settings on Systems）] で、[今すぐ適用（Enforce Now）] をクリックします。
- サーバのホスト名が変わり、Active Directory アカウントではなくローカル ユーザ アカウントを使用する場合は、[TMS ツール（TMS Tools）] > [ユーティリティ（Utilities）] > [ユーザ ドメインの変更（Change User Domain）] を使用してユーザ ドメインを変更します。ローカル ユーザのアカウントを使用している場合は、新しいサーバ上で手動で再作成する必要があることに注意してください。
- Polycom システムの場合は、SNMP の [コンソール IP アドレス（Console IP Address）] を Cisco TMS サーバの新しい IP アドレスやホスト名に手動で変更し、各システムをリブートします。
- Cisco TMSXE を使用している場合は、構成ツールを開き、必要に応じて Cisco TMS 接続の詳細を変更します。

Cisco TMS の移行またはアンインストール

- Cisco TMSXN を使用している場合は、Domino Administrator を開き、必要に応じて Cisco TMS 用に作成したリソース予約データベースで [ホスト名（Host name）] を変更します。
- リモート システムの場合、各システムの [外部マネージャ アドレス（External Manager Address）] を新しい IP アドレスまたはホスト名に手動で変更します。

アプリケーションを移行したら

移行後は、元のサーバで Cisco TMS に関連するサービスを再度アクティブにしないでください。

サーバ自体を使用停止にしない場合は、元のサーバから Cisco TMS を削除することを強くお勧めします（「サーバからのすべての Cisco TMS 情報の削除」を参照）。

Cisco TMSXE の移行

Cisco TMSXE を新サーバに移行する方法については、『*Cisco TMSXE Deployment Guide*』を参照してください。

ごく小規模に導入する場合を除き、Cisco TMSXE は Cisco TMS と同じサーバ上にはインストールしないでください。詳細については、インストレーション ガイドのベスト プラクティスの項を参照してください。

Cisco TMSPE の移行

Cisco TMSPE は、Cisco TMS サーバ上にインストールされるため、Cisco TMS を移行したらすぐに移行する必要があります。

Cisco TMS と同様に、Cisco TMSPE データベースはローカルまたはリモートにすることができます。

ローカル データベース

Cisco TMSPE を移行するには次の手順を実行します。

1. 元のサーバのプロビジョニング拡張機能 Windows サービスを停止します。
2. tmspe データベースをコピーして復元する手順については、Cisco TMS 向けに前述した、「SQL データベースがサーバのローカルに保存される場合」（52 ページ）を参照してください。
3. 新サーバに Cisco TMSPE をインストールし、インストーラに新しい tmspe データベースの場所を指定します。
4. Cisco TMS のネットワーク構成を変更した場合は、[管理ツール（Administrative Tools）] > [設定（Configuration）] > [プロビジョニング拡張機能の設定（Provisioning Extension Settings）] > [Cisco TMS 設定（Cisco TMS Settings）] の順に移動します。

   [ホスト名（Hostname）] が `localhost` でない場合は、新しい Cisco TMS アドレスを反映するように更新する必要があります。

リモート データベース

Cisco TMSPE を移行するには次の手順を実行します。

1. 元のサーバのプロビジョニング拡張機能 Windows サービスを停止します。
2. 新サーバに Cisco TMSPE をインストールし、インストーラに新しいリモート データベースの場所を指定します。

3. Cisco TMS のネットワーク構成を変更した場合は、[管理ツール（Administrative Tools）] > [設定（Configuration）] > [プロビジョニング拡張機能の設定（Provisioning Extension Settings）] > [Cisco TMS 設定（Cisco TMS Settings）] の順に移動します。

   [ホスト名（Hostname）] が `localhost` でない場合は、新しいアドレスを反映するように更新する必要があります。

Cisco TMSAE の移行

Cisco TMSAE は常に Cisco TMS サーバ上にインストールされますが、すべてのプログラム データは外部のデータ ウェアハウス サーバに保存されます。

Cisco TMS の移行後 Cisco TMSAE インストールを移行するには次の手順を実行します。

1. 元のサーバの TANDBERG 分析拡張機能 Windows サービスを停止します。
2. 『Cisco TMSAE Installation Guide』の手順に従って、新サーバに Cisco TMSAE をインストールします。次のことを確実に実行します。
   - 元のサーバと同じ仮想ディレクトリの名前を使用します。

     仮想ディレクトリの名前を変更する場合は、インストール後に Cisco TMS の Cisco TMSAE パスを更新する必要があります。

   - ウェアハウス サーバの既存の Cisco TMSAE データベースにインストーラを指定できるように、[事前設定を使用（Use Preconfigured）] オプションを選択します。
   - 要求された場合に、新 Cisco TMS サーバの詳細（変更した場合の新しいホスト名または IP アドレスなど）を指定します。
3. [管理ツール（Administrative Tools）] > [分析拡張機能（Analytics Extension）] の順に移動して [ETL ジョブを今すぐ実行（Run ETL Job Now）] をクリックすることにより、ETL ジョブを正しく実行できることを確認します。

Cisco TMS のアンインストール

ここでは Cisco TMS アプリケーションを削除する方法について説明します。通常の状態では、古いバージョンの Cisco TMS は Cisco TMS インストーラによって自動的に削除されます。

Cisco TMS をアンインストールすると、Cisco TMS アプリケーション、Web サイト、およびサービスも削除されます。カスタマー データ、ログ、データベースおよびデータベース サーバは、今後のアップグレードに備えて削除されません。

アンインストール ウィザードでは、SQL Server はいっさい変更されません。データベース サーバを含むすべての Cisco TMS 情報をサーバから完全に削除するには、次の項を参照してください。

Cisco TMS アプリケーションを削除するには次の手順を実行します。

1. [スタート（Start）] メニューまたは [スタート（Start）] 画面の Cisco プログラム グループから [Cisco TMS のアンインストール（Uninstall Cisco TMS）] を選択するか、Windows コントロール パネルの [プログラムの追加と削除（Add/Remove Programs）] を使用します。

Cisco TMS の移行またはアンインストール

[ようこそ（Welcome）] ウィンドウに、アンインストール スクリプトで Cisco TMS は削除されるが、データベースとデータベース サーバは個別に削除する必要があるという説明が表示されます。

2. [次へ（Next）] をクリックします。

   ウィザードによって、Cisco TMS のサービス、Web サイト、およびアプリケーション データが削除されます。

Cisco TMS アプリケーションの削除が完了します。

サーバからのすべての Cisco TMS の情報の削除

アンインストール ウィザードでは、将来 Cisco TMS を容易に再インストールまたはアップグレードできるように、Cisco TMS アプリケーションのみをサーバから削除します。

注意：

- 次の手順では、SQL Server は Cisco TMS によってインストールされており、他のアプリケーションから使用されていないため、安全に削除できると想定しています。SQL Server が他のアプリケーションによって使用されている場合、SQL Server またはそのプログラム フォルダを削除しないでください。
- 次のステップに従うと *すべての* Cisco TMS データが削除されます。ご使用の Cisco TMS インストレーションの情報を保持したい場合は、先に進まないでください。

Cisco TMS とそのすべてのデータを完全にサーバから削除するには、次の手順を実行してください。

1. 前のセクションの手順を使用して Cisco TMS アンインストール ウィザードを実行します。
2. Cisco TMSPE がインストールされている場合は、『*Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*』に記載されている手順に従ってアンインストールしてください。
3. Cisco TMS インストレーションによって使用されていたプログラム フォルダを削除します。デフォルトの場所は C:\Program Files (x86)\TANDBERG\TMS です。
4. [スタート（Start）] メニューの [ファイル名を指定して実行（Run）] を選択して「regedit」と入力し、[OK] をクリックして Windows レジストリ エディタを開きます。
5. プラス アイコンを使用して左側のツリーを展開し、ハイブ（フォルダ）HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Tandberg\TANDBERG Management Suite を探します。
6. [TANDBERG Management Suite] フォルダ アイコンを右クリックし、[削除（Delete）] をクリックします。確認のために [はい（Yes）] をクリックします。
7. レジストリ エディタを閉じます。
8. リモートの SQL Server を使用していた場合は、SQL 管理者に tmsng という名前のデータベースをドロップするように依頼します。
9. Cisco TMS によって排他的に使用されている SQL Server のローカル コピーがある場合は、次の手順を実行して削除します。
   a. Windows のコントロール パネルから [プログラムの追加と削除（Add/Remove Programs）] を開きます。
   b. 一覧から 「Microsoft SQL Server」と対応するバージョン番号（インストレーションに応じて 2012 または 2008）を探して [削除（Remove）] をクリックします。

Cisco TMS の移行またはアンインストール

c. SQL インストレーションで使用されたプログラム フォルダを削除します。デフォルトの場所は C:\Program Files\Microsoft SQL Server です。

Cisco TMS、データベース、カスタマーによって保存されたすべてのデータの削除は、これで完了しました。

トラブルシューティング

インストールのタイムアウト

Cisco TMS をアップグレードするときのデフォルトのデータベースのタイムアウト値は 30 分です。この値は、インストーラの内部データベース操作のそれぞれに適用されます。数年分のコール履歴とシステム データの一方または両方を大規模に導入する場合、一部の操作は完了までに 30 分以上かかる場合があります。

このタイムアウト値はコマンドライン オプションを使用して設定できます。60 分のタイムアウト値を使用するには、次のようにコマンドラインからインストーラを実行します。

```
TMS15.1.exe /z"sqltimeout 60"
```

必要であれば、**60** をさらに大きな値に置き換えます。

デフォルト値の 30 分を使用することと、最初のアップグレードの試みが失敗した場合にのみタイムアウト値を増やすことを推奨します。

付録

付録 1：IIS モジュールを必要最低限に制限する

IIS では、セキュリティを最高の状態に保つために、サーバにインストールして有効にするコンポーネントを管理者が微調整できるモジュラ システムが提供されています。サーバをさらに制限したいと考えている管理者のために、Cisco TMS の必須モジュールの一覧を以下に示します。モジュールは、サイト レベルまたはサーバ レベルで制御される場合があります（一部はサーバ レベルだけです）。下記の手順では、サーバ レベルで変更を加えていると想定しています。

モジュールを削除する前に、コマンド `%windir%\system32\inetsrv\appcmd.exe add backup "TMS"` を使用して、IIS の設定をバックアップすることを推奨します。

後でバックアップを復元する必要がある場合は、コマンド `%windir%\system32\inetsrv\appcmd.exe restore backup "TMS"` を使用します。

IIS の有効化モジュールを変更するには、次の手順を実行します。

1. **インターネット インフォメーション サービス（IIS）マネージャ**を開きます。
2. 左側のセクションのツリーから、サーバ名をクリックします。
3. 中央のセクションの [IIS] で [モジュール（Modules）] をダブルクリックします。

   インストール済みの管理対象モジュールとネイティブ モジュールの一覧が表示されます。

4. モジュールを削除するには、そのエントリを右クリックするか、エントリを選択して [操作（Actions）] パネルに移動し、[削除（Remove）] を選択します。

次のモジュールは Cisco TMS に必要なため、*削除しない*でください。

- AnonymousAuthenticationModule
- BasicAuthenticationModule
- DefaultDocumentModule
- DefaultAuthentication
- DigestAuthenticationModule

- HttpCacheModule
- HttpLoggingModule（推奨）
- HttprRedirectionModule
- IsapiFilterModule
- ProtocolSupportModule
- RequestFilteringModule
- セッション（Session）
- StaticCompressionModule
- StaticFileModule
- WindowsAuthentication
- WindowsAuthenticationModule

付録 2：フラッド攻撃からの保護のための IIS 要求の設定

システムからの非常に多くの数の同時着信要求のフラッディングに対する Cisco TMS の安定性と保護のために、サーバ上で IIS のフラッド保護の設定を行うことをお勧めします。

推奨される値での設定手順を次に示します。

IIS 8 および 8.5

お使いのサーバで IIS 8 および 8.5 を実行している場合は、以下の手順を実行します。

IP およびドメイン制限ロールの有効化

1. [サーバー マネージャー（Server Manager）] を開きます。
2. スタート ページで[役割と機能の追加（Add Roles and Features）] をクリックします。**ロールと機能の追加ウィザード**の [はじめる前に（Before you begin）] 画面が表示されます。
3. 説明されているサーバとパスワードの前提条件が満たされていることを確認し、[次へ（Next）] をクリックします。

   [インストールの種類（Installation type）] 画面が表示されます。

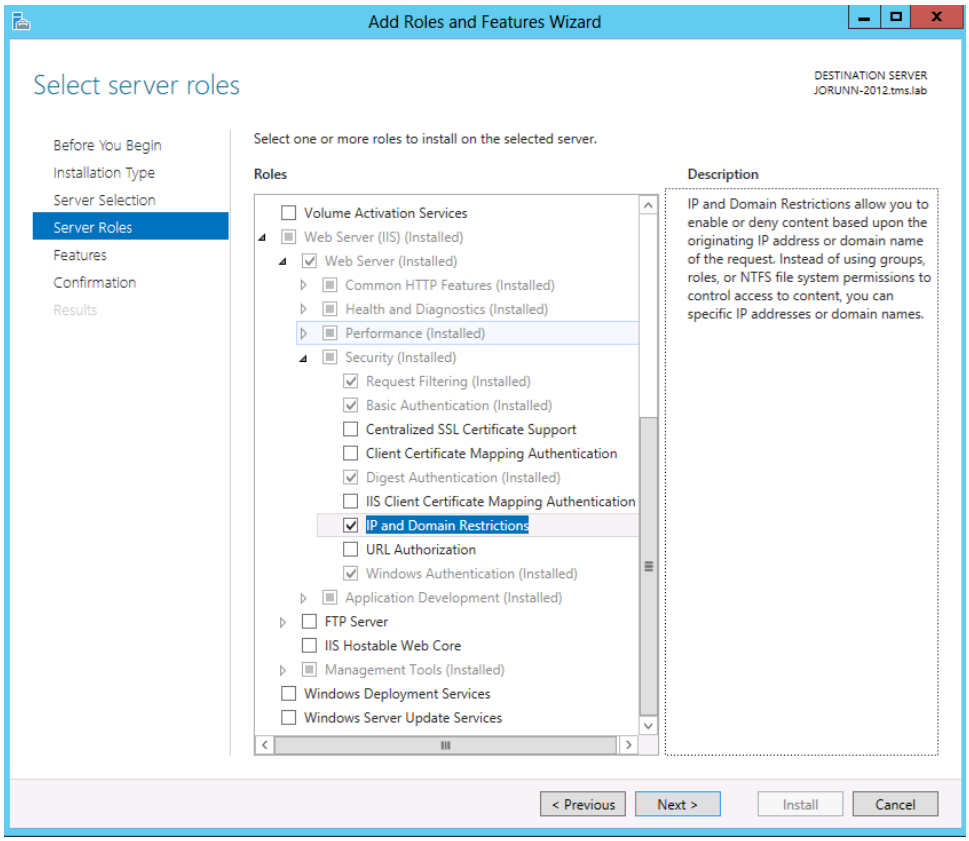
4. [ロールベースまたは機能ベースのインストール（Role-based or feature-based installation）] を選択して [次へ（Next）] をクリックします。

   [サーバーの選択（Server selection）] 画面が表示されます。

5. [サーバー プールからサーバーを選択（Select a server from the server pool）] オプションを選択し、正しいサーバが選択されていることを確認して [次へ（Next）] をクリックします。

   [サーバーのロールの選択（Select server roles）] 画面が表示されます。

付録



6. [ロール（Roles）] ペインで [Web サイト（IIS）（Web Site (IIS)）] > [Web サーバー（Web Server）] > [セキュリティ（Security）] の順に展開して [IP およびドメインの制限（IP and Domain Restrictions）] をオンにし、[次へ（Next）] をクリックします。

   [機能（Features）] 画面が表示されます。

7. [次へ（Next）] をクリックします。

   [確認（Confirmation）] 画面が表示されます。

8. [インストール（Install）] をクリックします。

   インストールが完了したらウィザードを閉じます。

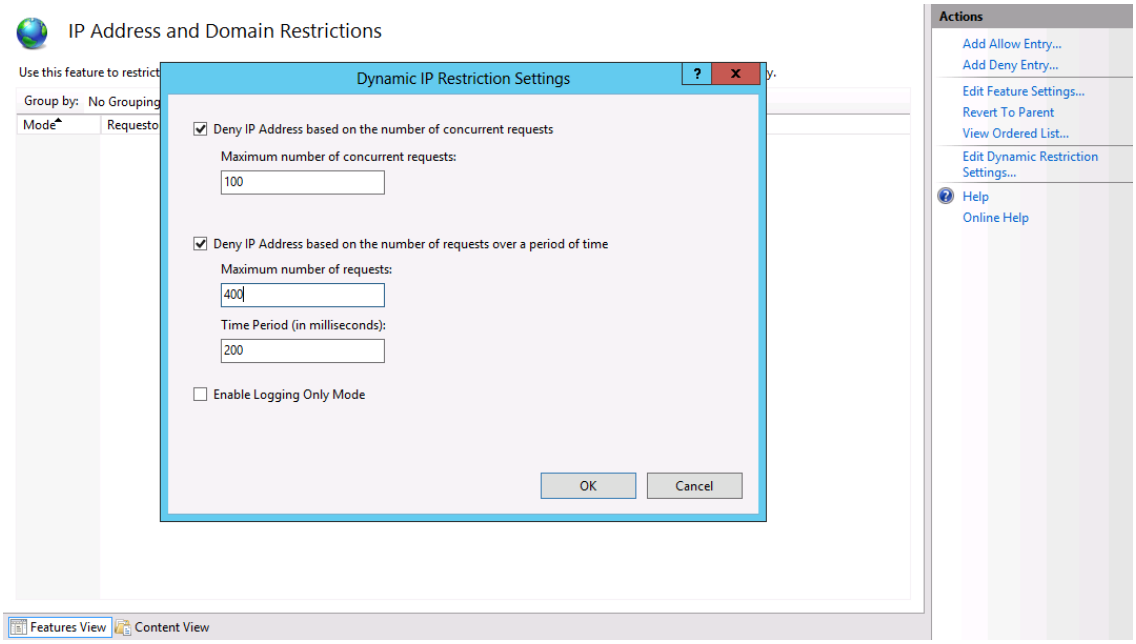
付録

デフォルト サイトへの動的 IP 制限の設定

IIS マネージャで次の手順を実行します。

1. 左側のパネルで、[既定の Web サイト（Default Website）] に移動し、エントリをクリックして [既定の Web サイト ホーム（Default Web Site Home）] を表示します。
2. [IIS] セクションの [IP アドレスおよびドメインの制限（IP Address and Domain Restrictions）] をダブルクリックします。
3. 右の [操作（Actions）] パネルの [動的制限設定の編集（Edit Dynamic Restriction Settings）] をクリックします。

   [動的 IP 制限（Dynamic IP Restrictions）] ダイアログが開きます。



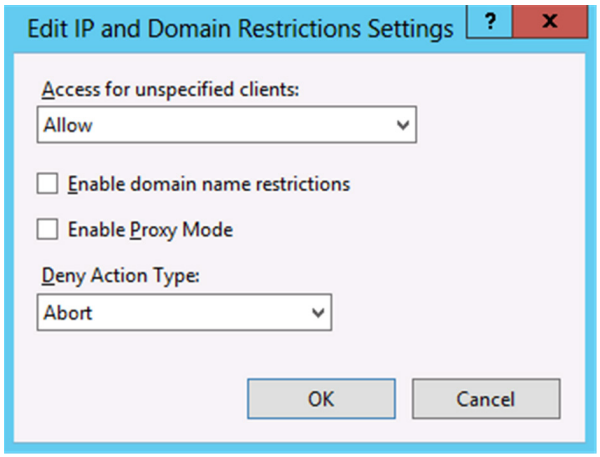
4. このダイアログで以下を行います。
   a. [同時要求の数に基づいて IP アドレスを拒否する（Deny IP Address based on the number of concurrent requests）] をオンにし、最大数を `100` に設定します。
   b. [一定時間の要求数に基づいて IP アドレスを拒否する（Deny IP Address based on the number of requests over a period of time）] をオンにします。

      要求の最大数を `400` に、時間（ミリ秒）を `200` に設定し、[OK] をクリックします。

5. 右の [操作（Actions）] パネルの [機能設定の編集（Edit Feature Settings）] をクリックします。

   [IP およびドメイン制限設定の編集（Edit IP and Domain Restriction Settings）] ダイアログが表示されます。

付録



6. [拒否のアクション タイプ（Deny Action Type）] を [中止（Abort）] に設定します。
7. [OK] をクリックします。

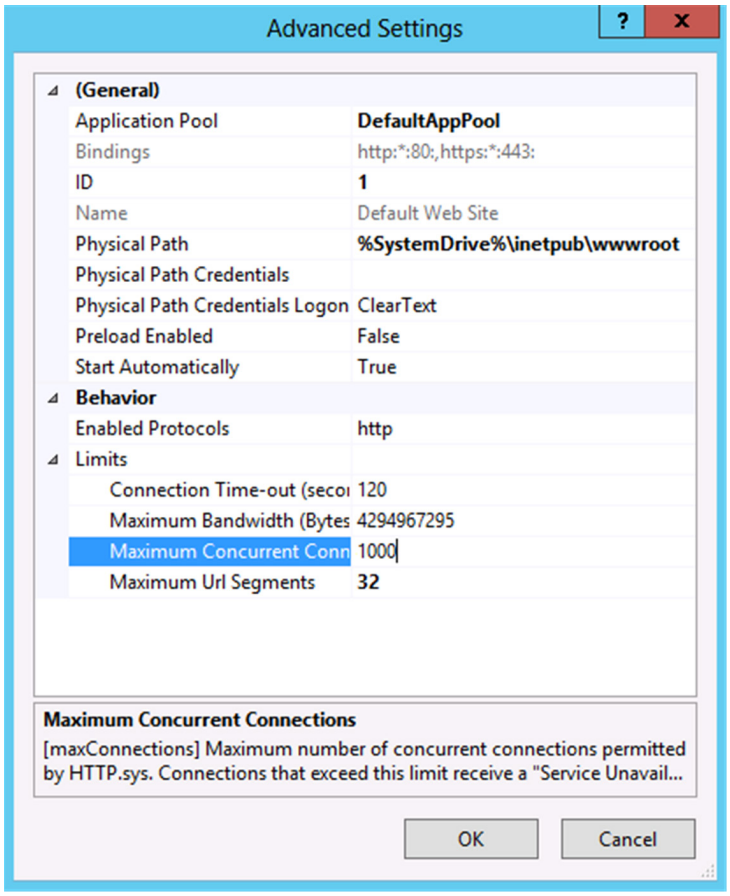
合計接続数の制限

IIS マネージャで次の手順を実行します。

1. 左側のパネルで、[既定の Web サイト（Default Website）] に移動し、エントリをクリックして [既定の Web サイト ホーム（Default Web Site Home）] を表示します。
2. 右側のパネルの [詳細設定（Advanced Settings）] をクリックします。

   [詳細設定（Advanced Settings）] ダイアログが表示されます。

付録



3. [動作（Behavior）] > [制限（Limits）] で [最大同時接続数（Maximum Concurrent Connections）] を `1000` に設定します。
4. [OK] をクリックして保存します。
5. IIS マネージャを閉じます。

IIS 7

お使いのサーバで IIS バージョン 7 を実行している場合は、以下の手順を実行します。

IIS 拡張のインストール

フラッド保護を設定する前に、IIS.NET からサーバに Dynamic IP Restrictions 拡張をダウンロードしてインストールする必要があります：http://www.iis.net/downloads/microsoft/dynamic-ip-restrictions

このダウンロードは Microsoft Web Platform Installer を使用します。

付録

デフォルト サイトへの動的 IP 制限の設定

IIS マネージャで次の手順を実行します。

1. 左側のパネルで、[既定の Web サイト（Default Website）] に移動し、エントリをクリックして [既定の Web サイト ホーム（Default Web Site Home）] を表示します。
2. [動的 IP 制限（Dynamic IP Restrictions）] をダブルクリックします。
3. [同時要求の数に基づいて IP アドレスを拒否する（Deny IP Address based on the number of concurrent requests）] をオンにし、最大数を `100` に設定します。
4. [一定時間の要求数に基づいて IP アドレスを拒否する（Deny IP Address based on the number of requests over a period of time）] をオンにします。

   要求の最大数を `400` に、時間（ミリ秒）を `200` に設定します。

5. [拒否のアクション タイプ（Deny Action Type）] ドロップダウンから [要求を中止（接続の終了）（Abort Request (Close Connection)）] を選択します。
6. [適用（Apply）] をクリックして、変更内容を保存します。

IIS マネージャを開いたままにし、合計同時接続数の制限に移ります。

合計接続数の制限

IIS マネージャで次の手順を実行します。

1. 左側のパネルで、[既定の Web サイト（Default Website）] に移動し、エントリをクリックして [既定の Web サイト ホーム（Default Web Site Home）] を表示します。
2. 右側のパネルの [詳細設定...（Advanced Settings...）] をクリックします。
3. [動作（Behavior）] > [接続制限（Connection Limits）] で [最大同時接続数（Maximum Concurrent Connections）] を `1000` に設定します。
4. [OK] をクリックして保存します。
5. IIS マネージャを閉じます。

詳細については、IIS.NET の記事「*Using Dynamic IP Restrictions*」を参照してください。

通告

アクセシビリティ通知

シスコは、利用しやすい製品およびテクノロジーの設計および提供に取り組んでいます。

Cisco TelePresence Management Suite の Voluntary Product Accessibility Template（VPAT）は、ここで入手可能です。

http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence

アクセシビリティの詳細については、次を参照してください。

www.cisco.com/web/about/responsibility/accessibility/index.html

マニュアルの入手方法およびテクニカル サポート

資料の入手方法、Cisco Bug Search Tool（BST）の使用方法、サービス要求の送信および追加情報の収集方法については、「What's New in Cisco Product Documentation」（www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html）を参照してください。

「What's New in Cisco Product Documentation」は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

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。

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。

シスコの商標または登録商標

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 [英語]）をご覧ください。

シスコの商標または登録商標