Cisco Meeting Server

Cisco Meeting Server 3.10

Cisco Meeting Server 1000 および仮想化導入のための設置ガイド

2024 年 9 月 27 日

Cisco Systems, Inc. www.cisco.com

目次

変更履歴

日付	変更の概要
2024 年 9 月 27 日	バージョン 3.10 で更新。
2024 年 3 月 5 日	バージョン 3.9 で更新。
2023 年 9 月 7 日	バージョン 3.8 で更新。 ESXi バージョンに関するメモと OVA アップグレードに関する情報を更新しました。
2023 年 3 月 16 日	バージョン 3.7 で更新。
2022 年 8 月 23 日	バージョン 3.6 で更新。
2022 年 4 月 20 日	バージョン 3.5 で更新。
2022 年 1 月 10 日	データベース VMでサポートされている vCPU の数を更新
2021 年 12 月 15 日	バージョン 3.4 で更新。
2021 年 9 月 03 日	付録 E にマイナー編集。
2021 年 8 月 24 日	バージョン 3.3 で更新。
2021 年 5 月 19 日	Medium OVA Expressway のウェブアプリのコールキャパシティと推奨事項に関するドキュメントを更新。
2021 年 4 月 22 日	「Smart Licensing について開始する前に」についてのメモを追加。 表 2 を更新。
2021 年 4 月 14 日	バージョン 3.2 で更新。 Cisco Meeting Server プラットフォーム、ESXi サポート、増加した coSpaces の RAM 要件によるコールキャパシティを更新。
2020 年 12 月 9 日	軽微な修正。
2020 年 11 月 30 日	バージョン 3.1 で更新。
2020 年 10 月 30 日	ESXi 情報が更新されました。
2020 年 10 月 6 日	軽微な修正。
2020 年 9 月 9 日	軽微な修正。
2020 年 9 月 2 日	レコーダー/ストリーマの VM の最小要件を 4 vCPU コアに明確化するためのマイナー編集。
2020 年 8 月 10 日	バージョン 3.0 で更新。 X シリーズ サーバへの参照を削除しました。
2020 年 4 月 01 日	リンク切れを修正しました。
2019 年 11 月 27 日	400v/410v への言及を削除。
2019 年 11 月 13 日	バージョン 2.8 の ESXi サポートの変更に対する更新。

日付	変更の概要
2019 年 7 月 16 日	ドキュメントの誤りを修正し、「インストール」の章を挿入し直しました
2019 年 5 月 30 日	ドキュメントの軽微な修正
2019 年 4 月 26 日	VMware ESXi のサポート対象バージョンの更新
2019 年 4 月 9 日	その他の修正。
2019 年 4 月 2 日	ESXi 6.5 ウェブクライアントで OVA ファイルから Meeting Server を導入するための情報が追加。 その他の修正。
2019 年 1 月 28 日	Cisco UCS C220 M5 ラックサーバーを使用する Cisco Meeting Server 1000 は、M4 バリアントに優先。 (2018 年 11 月より)。
2018 年 11 月 29 日	その他の修正。
2018 年 9 月 24 日	「Hyper-V」の項と参照先を削除。
2017 年 12 月 20 日	Cisco Meeting Server バージョン 2.3 からの ESXi 6.5 および ESXi 6.0 Update 3 のサポートを追加しました。
2017 年 11 月 27 日	Cisco Meeting Server 1000 のインストールの詳細を追加。 AWS 参照を削除しました。

1 はじめに

Cisco Meeting Server は、音声、ビデオ、ウェブコンテンツ向けのスケーラブルなソフトウェア プラットフォームであり、Microsoft、Avaya、その他のベンダーのさまざまなサードパーティキットと統合できます。 Cisco Meeting Server があれば、場所、デバイス、テクノロジーに関係なく、ユーザーは接続できます。

Cisco Meeting Server は、VMware ESXi 7.x と仮想ハードウェア vmx-1x を以下のプラットフォームにロードすることで、仮想化導入として実行されます。

- Cisco Meeting Server 1000（事前設定済み Cisco UCS C220 ラックサーバー。（2019 年初頭から、M5 バリアントが M4 バリアントに優先）
- 仕様ベースの VM プラットフォーム。

下の表は Cisco Meeting Server ソフトウェアの現行バージョンがサポートする ESXi バージョンを示しています。

表 1: サポートしている ESXi バージョン

Cisco Meeting Server のバージョン	ESXi バージョン
3.10	ESXi 8.0 U3 ESXi 7.0 Update 3q
3.9	ESXi 7.0 Update 3o
3.8	ESXi 7.0 Update 3n
3.7	ESXi 6.5 P09 ESXi 6.7 P08 ESXi 7.0 Update 3j
3.6	ESXi 6.5 EP26 ESXi 6.7 EP 23 ESXi 7.0 更新 3d
3.5	ESXi 6.5 P07 ESXi 6.7 EP 23 ESXi 7.0 更新 3d
3.4	ESXi 6.5 P07 ESXi 6.7 P05 ESXi 7.0 Update 2a

顧客は多くの場合、Cisco Meeting Server の仮想化された展開を、分割展開およびスケーラブルな展開でのエッジ サーバとして使用します。

参加者の機能性およびユーザ エクスペリエンスは、同じソフトウェアのバージョンを実行しているすべてのプラットフォームで同一です。 ただし、導入は 仮想化導入と物理的導入とは交換できません（Cisco Meeting Server 2000）。 例えば、仮想化導入からバックアップを作成し、それを Cisco Meeting Server 2000 で復元することはできません。逆も同様です。

メモ: Meeting Server 3.0 では Cisco Meeting Management 3.0 (またはそれ以降) が必須です。ミーティング管理は、Smart Licensing サポートのための製品の登録とスマートアカウント（セットアップされている場合）との対話を処理します。

1.1 仮想化プラットフォームの概要

警告：Cisco Meeting Server ソフトウェアを実行している仮想プラットフォームに関係なく、プラットフォームが最新の状態でパッチが適用されていることを確認してください。 プラットフォームのメンテナンスを怠ると、Cisco Meeting Server のセキュリティが損なわれる可能性があります。

Cisco Meeting Server 1000: VMWare ESXi バージョン 7.x および Cisco Meeting Server がプリインストールされた状態で出荷されます。 しかし、これは利用可能な Cisco Meeting Server ソフトウェアの最新バージョンではない可能性があります。 このガイドの指示に従って、Cisco Meeting Server 1000 を設定し、ライセンスを適用してください。 Cisco Meeting Server が起動したら、MMP コマンド **`version`** を使用して、インストールされているソフトウェアのバージョンを確認します。 最新版は ここから入手できます。 Cisco Meeting Server 1000 にインストールされているソフトウェアをアップグレードするには、そのソフトウェアバージョンのリリースノートの指示に従ってください。

注：

Meeting Server に ESXi 7.x が同梱されている場合：Cisco Meeting Server 1000 用のデフォルトの Cisco UCS ESXi 7.x 資格情報は、ログインユーザー名：**`root`**、パスワード：**`c!SCo123`** です。

このログイン管理者アカウントの変更が推奨されています。 パスワードを変更すると、Cisco UCS ESXi が複雑なパスワードを要求することに注意してください。

仕様ベースの VM プラットフォーム：以前に仮想化された Cisco Meeting Server インストールからサーバーをアップグレードする場合は、Cisco Meeting Server リリースノートの指示に従ってください。 新規のインストールの場合、このガイドに従って VM を作成し、Cisco Meeting Server ソフトウェアをインストールします。

1.2 このガイドの使い方

このガイドでは、Cisco Meeting Server 1000 のインストールと仕様ベースの VM の導入について記載しています。

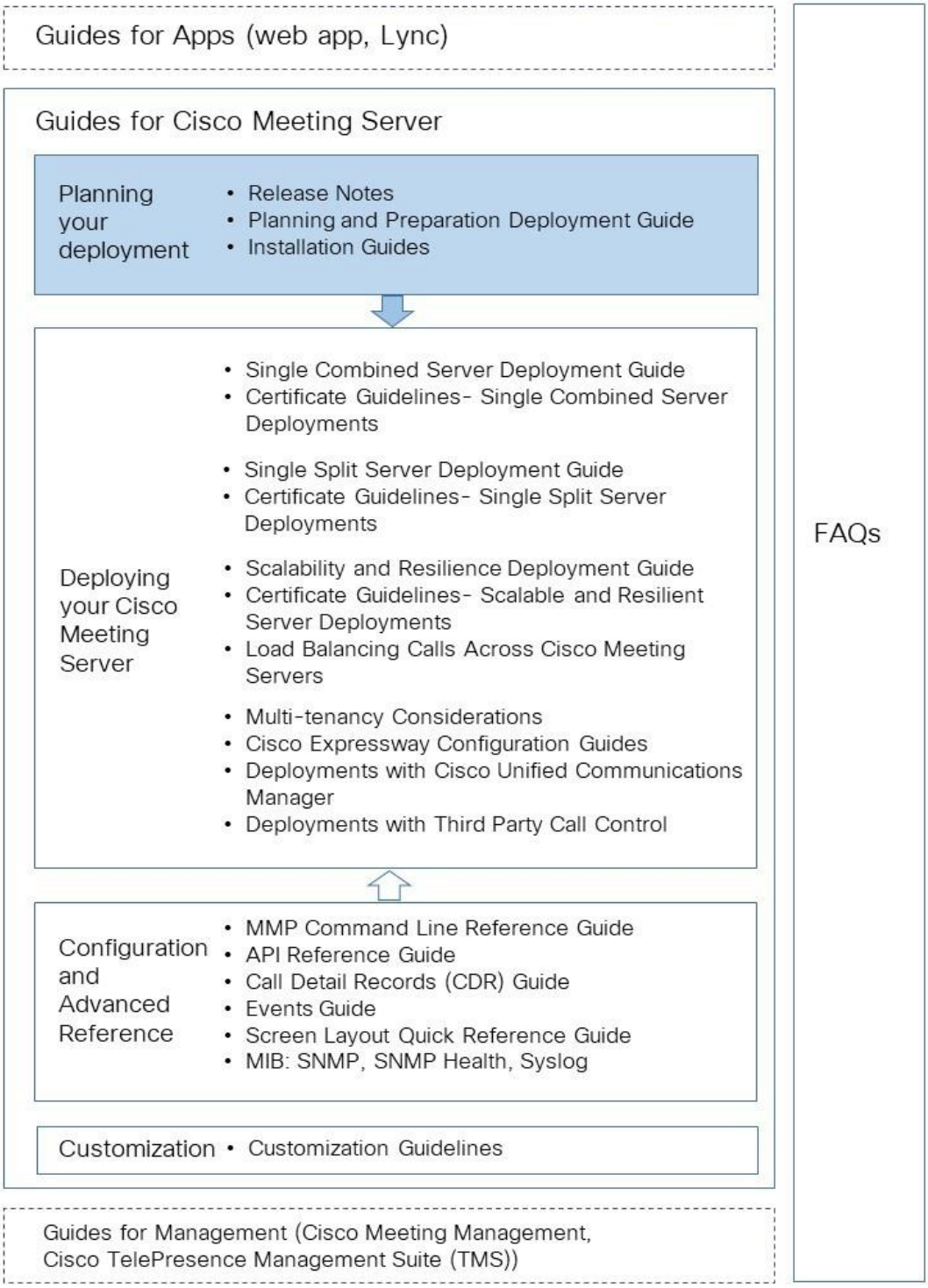
Cisco Meeting Server 1000 は、ソフトウェアがプリインストールされた状態で出荷されます。 このガイドのセクション 2.4 を読んだ後、第 3 章に進んで、Cisco Meeting Server 1000 の設定を開始してください。

注：Cisco Meeting Server 1000 は、仕様ベースの VM サーバーとは異なる設定があります。設定は事前に構成されています。設定を変更しないでください。

仕様ベースの VM 導入をインストールする場合は、第 2 章に進んだ後、第 3 章で VM を設定します。 第 2 章 は経験豊富な VMware 管理者を対象にしています。

Cisco Meeting Server を設定し、ライセンスを適用した後は、『導入の計画と準備ガイド』を参照して適切な導入を決定し、その後、対象とする導入に最も関連する導入ガイドと証明書ガイドに従ってください。図 1 を参照してください。 これらのドキュメントは cisco.com で見つけることができます。

図 1：Cisco Meeting Server のインストールと導入のドキュメント



注：Cisco ユーザー用ドキュメントで使用しているアドレス範囲は、RFC 5737 で定義されているものです。これらはドキュメンテーション用に明示的に予約されたものです。 Meeting Server のユーザーマニュアルに記載されている IP アドレスは、特に記載のない限り、お使いのネットワークでルーティング可能な正しい IP アドレスに置き換えてください。

1.3 特定の MMP コマンドの違い

すべての MMP コマンドについては、 MMP コマンドリファレンス を参照してください。 Cisco Meeting Server 2000 を実行すると、仮想化された Cisco Meeting Server と比較して、いくつかの違いがあります。

コマンド	Cisco Meeting Server 2000	Cisco Meeting Server 1000 および仮想 Cisco Meeting Server
shutdown	MMP では利用できません。 電源を切る前に、Cisco UCS マネージャを使用して、ブレードサーバーの電源を 切ってください。	vSphere の電源ボタンは使用しないでください。 **シャットダウン** コマンドを使用してください。
状態	MMP では利用できません。 Cisco UCS Manager	使用不可
シリアル番号:	サーバーのシリアル番号を返します。	使用不可
dns	インターフェイスを指定しないでください。 例 **dns add forwardzone <domain-name> <server ip>**	インターフェイスを指定しないでください。 例 **dns add forwardzone <domain-name> <server ip>**
user evict	バージョン 2.9 から利用可能	応答可能

1.4 異なるプラットフォームで有効になるコンポーネントの違い

下の表は、異なる Cisco Meeting Server プラットフォームで利用できるコンポーネントの一覧です。 プラットフォームでコンポーネントが利用できない場合、そのコンポーネントに特有の MMP および API コマンドは利用できません。 例えば、TURN サーバー用の MMP および API コマンドは、Cisco Meeting Server 2000 では利用できません。

コンポーネント	Cisco Meeting Server 2000	Cisco Meeting Server 1000 および仮想 Cisco Meeting Server
Call Bridge	応答可能	応答可能
Webブリッジ 3	応答可能	応答可能
データベース	応答可能	応答可能
スケジューラ	応答可能	応答可能
TURN サーバ	使用不可	応答可能
レコーダ	使用不可	応答可能
アップローダー	使用不可	応答可能
ストリーマー	使用不可	応答可能
SNMP MIB	機能は現在使用できません	応答可能

2 インストール

この章の内容は、仕様ベースの VM プラットフォームおよび Cisco Meeting Server 1000 への導入に適用されます。セクション 2.2 に従って、VMware ホストを導入してください。
セクション 2.4 に従い、Cisco Meeting Server 1000 を展開してください。

2.1 開始する前に

2.1.1 Cisco Meeting Server ソフトウェアについて

VMware ユーザーの場合、Cisco Meeting Server ソフトウェアは .ova ファイルとして提供されます。 これは、単一のネットワーク インターフェイスを持つ新しい VM と、Cisco Meeting Server アプリケーションを含む仮想ディスクをセットアップするテンプレートです。

インストール後、完全に機能する Cisco Meeting Server が利用できます。これは次のように実行できます。

- 単一のサーバ上で有効になっているすべてのコンポーネントを備えた完全なソリューション (単一結合サーバ展開モデル)、
- 内部ネットワークに導入されたコアサーバーで一部のコンポーネントが有効になっているスプリット導入、および DMZ に導入された Edge サーバーで他のコンポーネントが有効になっているスプリット導入（シングルスプリットサーバー導入モデル）、
- クラスタ化された複数の Call Bridge とデータベースを使用した、スケーラブルでレジリエントな導入により、使用率の増加に対応し、ダウンタイムを最小限に抑えます。

同じ .ova ファイルがすべての展開のインストールに使用されます。

Cisco Meeting Server ソフトウェアをアップグレードするには、ソフトウェアのバージョンに対して公開されているリリースノートの手順に従ってください。

注：

- Meeting Management が必要な 3.0 以降の Smart Licensing の問題を回避するには、Meeting Server を複製するのではなく、毎回新しい Meeting Server をインストールします。 または、完全に工場出荷時の状態にリセットして、すでにクローニングされている VM Meeting Servers に新しい同一の主催者 ID を再割り当てます。
- Meeting Server はセキュアブートをサポートしていません。

2.1.2 VM 導入としての Cisco Meeting Server のホスト要件

Cisco Meeting Server は、VM 導入として、標準的な Cisco サーバーの広い範囲で実行されます。 VM 設定要件と、さまざまな導入に対する UCS のテスト済みリファレンス設定については、このリンク を参照してください。

Cisco Meeting Server は、Intel および AMD プロセッサを搭載した Dell および HP のシステムを含むサードパーティのサーバ上でも動作します。 Klas VoyagerVM や Dtech LABS M3-SE-SVR2 などのスモール フォーム ファクターおよび高耐久システムもサポートされます。このソフトウェアは、VMware ESXi およびクラウドサービスに展開できます。

表 2：サードパーティサーバー上で実行される Cisco Meeting Server のホスト要件

	最小	推奨
サーバーの製造元	任意（Any）	任意（Any）
プロセッサタイプ	Intel Nehalem マイクロアーキテクチャ AMD ブルドーザー・マイクロアーキテクチャ	Intel Xeon 2600 v2 以降
プロセッサ周波数	2.0GHz	2.5Ghz
RAM	論理コアあたり 1GB*	論理コアあたり 1GB*
ストレージ	100GB	100GB

* 追加のメモリは、仮想マシンモニタおよびホスト上の他の VM による使用のために、システムで利用可能である必要があります。

注：Meeting Server は、シングルおよびデュアルソケットサーバーのみをサポートしています。

表 3: 推奨されるコア VM 構成

720p30 コールレッグ	CPU の設定	RAM の設定	システムの例
50	デュアル Intel E5-2680v2	32 GB (8x4 GB)	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
40	デュアル Intel E5-2650v2	32 GB (8x4 GB)	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
25	Single Intel E5-2680v2	16 GB (4x4 GB)	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
15	Single Intel E5-2640v2	8 GB (4x2 GB)	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8

さらに、

- 利用可能なメモリ帯域幅を最大化するために、すべてのメモリチャネルを使用するべきです。NUMA システムに特別な要件はありません。
- 帯域外管理システムは、VM とネットワークポートを共有するように設定すべきではありません。 内部テストでは、パケット損失のバーストおよび音声およびビデオ品質の劣化を引き起こす可能性があることが示されています。 帯域外管理は、専用ネットワークポートを使用するように設定するか、無効にする必要があります。
- 利用可能な場合は、主催者でハイパースレッディングを有効にする必要があります。有効にしないと、容量が最大 30% 減少します。
- AMD と Intel プロセッサを比較する場合、AMD「モジュール」（リソースを共有する「コア」のペア）の数を、Intel の「コア」（「ハイパースレッド」のペアを実行する）の数と比較する必要があります。 内部テストでは、AMD プロセッサは同等の Intel プロセッサの 60-70% の性能を提供することがわかりました。 このため、プロダクション環境には Intel プロセッサの使用が推奨されます。
- Cisco Meeting Server が使用する CPU は、専用である必要があります。 これは次の方法で実現します。
  - 主催者で単一の VM のみを実行している、または
  - 主催者のすべての VM を特定のコアにピニングし、Cisco Meeting Server に指定されたコアの使用のみを許可し、さらに、ハイパーバイザー用に VM がピン留めされていない物理コアを残します。
  - 仮想環境での Unified Communication の共存要件に従う必要があります。 ミーティングの見出しの下にある Cisco Meeting Server をクリックします。
- EVC モードが有効な VMWare ハイパーバイザーが使用されている場合、EVC は以下のいずれかまたはそれ以上のモードに設定されている必要があります。
  "B1"/AMD Opteron™ Generation 4
  “L2”/Intel® Nehalem 世代（以前の Intel® Xeon Core™ i7）
  上記にリストされているものより古い CPU との互換性を強制する EVC モードは、SSE 4.2 が無効になるため、サポートされません。SSE4.2 が必要です。
- メディアコールには Call Bridge のアクティベーションキーが必要です。 アクティベーションキーを取得するには、仮想サーバーの MAC アドレスが必要です。 ライセンスに関する情報は、第 1 章 および付録 B を参照してください。

2.2 仕様ベースのサーバーで VMware 経由でインストールする

注：仮想化導入用の Cisco Meeting Server の各リリースには、新規展開用の .ova ファイルと、最新リリースにアップグレードするためのアップグレードイメージ（.img）があります。

新規インストールについては、このセクションに従ってください。アップグレードについては、リリースノートに従ってください。

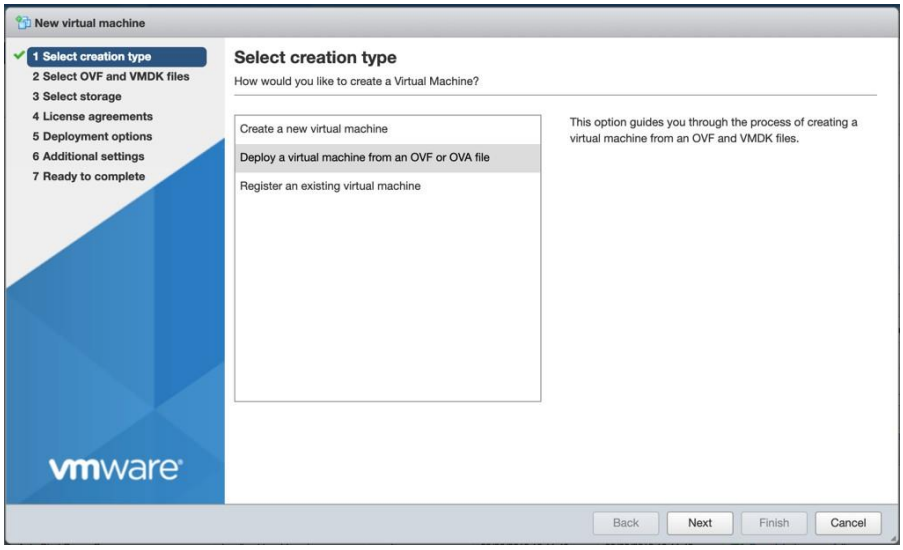
- EVC モードが有効な VMWare ハイパーバイザーが使用されている場合、EVC は以下のいずれかまたはそれ以上のモードに設定されている必要があります。
  "B1"/AMD Opteron™ Generation 4
  “L2”/Intel® Nehalem 世代（以前の Intel® Xeon Core™ i7）
  上記にリストされているものより古い CPU との互換性を強制する EVC モードは、SSE 4.2 が無効になるため、サポートされません。SSE4.2 が必要です。
- メディアコールには Call Bridge のアクティベーションキーが必要です。 アクティベーションキーを取得するには、仮想サーバーの MAC アドレスが必要です。 ライセンスに関する情報は、第 1 章 および付録 B を参照してください。
- OVA を Vcenter にアップロードして展開するとき、発行者フィールドは「(信頼できる証明書)」を表示する必要があります。 OVA のインポート時に、無効な証明書と信頼されていない証明書に関する警告が表示される場合は、次の記事を参照してください: https://kb.vmware.com/s/article/84240 OVA に署名するために使用される証明書に対応する中間およびルート証明書を VECS ストアに追加する必要がある場合があります。 中間証明書またはルート証明書を入手する場合、またはその他の問題については、Cisco テクニカルサポートに連絡してください。

2.3 ESXi ウェブクライアントを使って OVA ファイルから Meeting Server を導入する

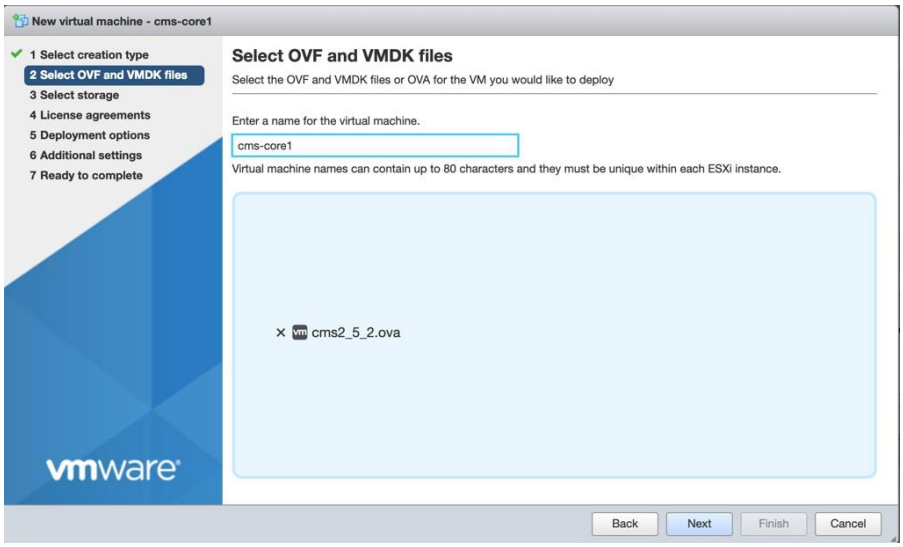
仮想化導入用の Cisco Meeting Server の各リリースには、新規展開用の .ova ファイルと、最新リリースにアップグレードするためのアップグレードイメージ（.img）があります。

新規インストールについては、このセクションに従ってください。アップグレードについては、リリースノートに従ってください。

1. Cisco ウェブサイトから .ova ファイルをダウンロードします。
2. vSphere Client で、左側にある [ナビゲータ（Navigator）] タブにあるホストに移動し、[VM の作成/登録（Create/Register VM）] を選択します。
3. [作成タイプの選択（Select creation type）] で、[OVF または OVA ファイルから仮想マシンを導入する（Deploy a virtual machine from an OVF or OVA file）] を選択し、[次へ（Next）] をクリックします。

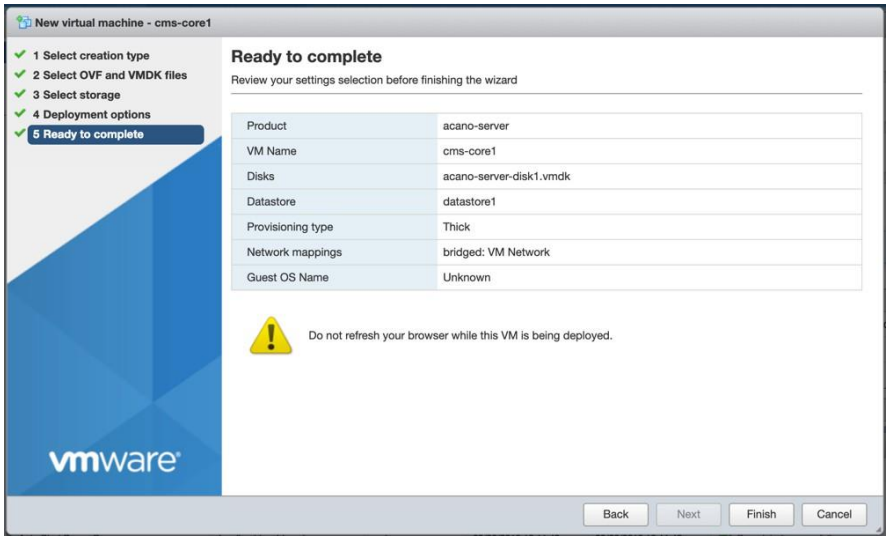


4. 仮想マシンの希望の名前を入力し、.ova ファイル (ステップ 1 でダウンロード) を参照またはドロップして選択します。



5. ウィザードの手順に従います。 選択する必要がある設定は以下の通りです。
   a. VM 構成とディスク ファイルを保存するデータストアを選択します。
   b. VM を接続するネットワーク マッピングを選択します。
   c. ディスクプロビジョニングを [**シック**（Thick）] に設定します。
   d. [**導入後に電源オン**（Power On After Deployment）] が選択されていないことを確認します。
   e. [**完了**] をクリックします。

注：仮想ホストの設定によっては、一部のウィザード設定が表示されなかったり、選択できない場合があります。



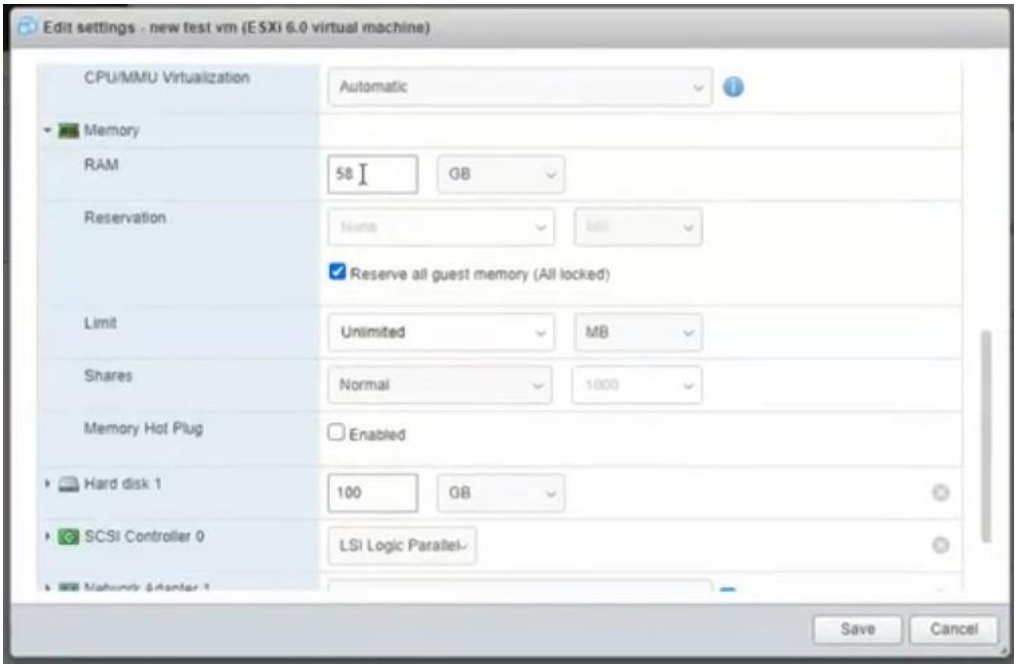
6. 完了すると、新しい Cisco Meeting Server VM が [**仮想マシン**（Virtual Machines）] の一覧に表示されるようになります。
7. VM のリストから Cisco Meeting Server VM を選択します。
8. [**アクション**（Actions）] ボタンから [**設定編集**...（Edit Settings...）] を選択します。
   a. **仮想マシン設定** を編集し、[CPU] をクリックします。 [CPU **数**] を必要な数に設定します (最小値は 4 です)。 スケーリングの詳細については、 導入ガイド を参照してください。 VM 設定要件の詳細については、 https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-meeting-server.html および付録 D を参照してください。
   b. [**ソケットあたりのコア数**（Number of Cores per Socket）] を次のいずれかに設定します。
      - ハイパースレッディング対応のデュアル プロセッサ ホストで、 **ソケットあたりのコア数** を論理コア数から 2 を引いた数に設定します。
      - ハイパースレッディングなしのデュアルプロセッサホストで、[**ソケットあたりのコア数**（Number of Cores per Socket）] を論理コア数から 1 を引いた数に設定します。
      - シングルプロセッサホストで、[**ソケットあたりのコア数**（Number of Cores per Socket）] を論理コアの数に設定します。

   基になるハードウェアをミラーリングするソケットの数を設定することをお勧めします。

注：論理コアの数は、vSphere ウェブクライアントで [**管理**（Manage）] >] [**設定**（Settings）] > [**プロセッサ**（Processors）] をクリックすると確認できます。 詳細については、https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.resmgmt.doc/GUID-E09F36DF-E31F-417D-9865-06E351D8AF15.html を参照してください。

---

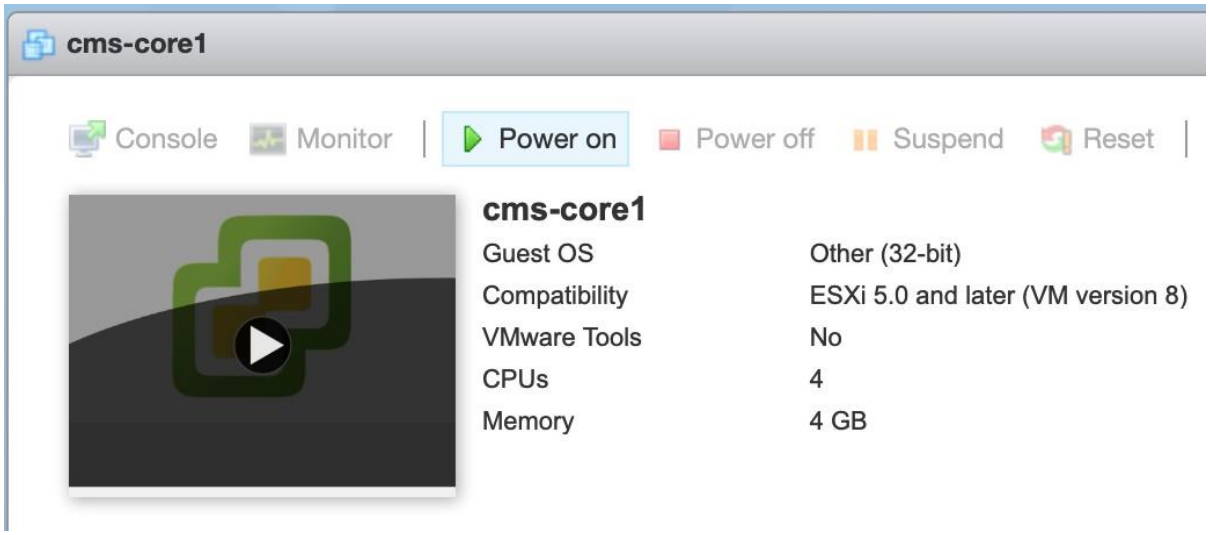
c. [メモリ] をクリックし、RAM が最低 4GB に設定されていることを確認します。



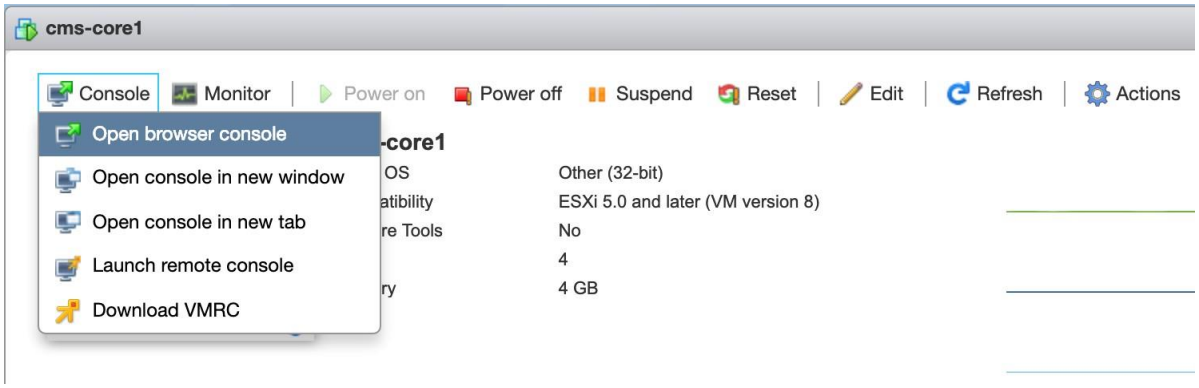
i. M4 および M5v1 バリアントでの ESXi 7.0 ベースのインストールの場合、 **ゲストメモリを予約する** (**すべてロック済み**) チェックボックスを選択します。

d. ディスクスペースを 100GB に設定します。

9. [**電源オン**（Power on）] をクリックします。



10. [**コンソール**] タブをクリックしてブラウザコンソール (VMware Remote Console がインストールされている場合はリモートコンソール) を開きます。



11. ユーザ名「admin」でログインし、「Enter」キーを押してパスワードフィールドをスキップします。 管理者パスワードの変更が求められます。 MMP にログインしています。 第 3 章 に進んでください。

2.4 Cisco Meeting Server 1000 のインストールと初期設定

2.4.1 開始する前に

インストールを完了するには、以下が必要です。

- PAK ライセンス番号
- VMware ライセンスのアクティベーション コードまたは顧客指定の VMware ライセンス キー
- ライセンス取得の手順を完了するためのインターネットおよびメール アクセス
- vSphere Client 6.0 を実行している Windows コンピュータまたはコンピュータに vSphere クライアントをインストールする権限

- 以下のいずれかのコンソール。
  - VGA コネクタおよび USB キーボードを備えたモニタ、
    または
  - シリアルアダプタが接続され、Cisco シリアルケーブル、ターミナルプログラムがあり、Java がインストールされ有効になっている Internet Explorer または Firefox でネットワーク接続された PC

2.4.2 タスク 1：開梱と初回起動

1. Meeting Server、電源コード、コンソールアダプタ、およびラックキットを開梱します。
2. Meeting Server またはオプションでラックマウントの位置を決めます。導入に応じて、『Cisco UCS C220 M5 設置ガイド』または『Cisco UCS C220 M4 設置ガイド』を参照してください。
3. イーサネットケーブルを Meeting Server 背面のイーサネット 1 ポートに接続し、イーサネットネットワークに接続します。
4. 電源コードを各電源に接続し、電源に接続します。
5. Meeting Server 前面の電源ボタンを押します。 最初に電源をオンにした後、自動的に停止と再起動を複数回繰り返します。
6. コンソールを Meeting Server に接続して続行します。 モニタとキーボード、またはネットワーク接続上の仮想コンソールのいずれかを使用することができます。 次のオプションから選択します。

2.4.2.1 コンソールオプション 1 - モニタとキーボード

1. Meeting Server の背面にある VGA ポート、または前面のコンソールポートに VGA 接続のモニタを接続します。
2. キーボードを Meeting Server の背面にある USB ポート、または前面のコンソールポートに接続します。

   起動が完了すると、Meeting Server は自動的に VMware コンソール画面にブートし、モニタに表示されます。

2.4.2.2 コンソールオプション 2 – ネットワーク上の仮想コンソール

Meeting Server に接続するためのモニタとキーボードが利用できない場合は、この方法を使用します。

1. お使いのコンピュータのシリアルポートを、ルーターおよびスイッチに付属の標準的な青い Cisco RJ-45 DB-9 ヌルシリアルケーブルを使って Meeting Server 背面の 10101 とラベル付けされた RJ-45 ポートに接続します。
2. ターミナルプログラムを開き、シリアルポート/アダプタの COM ポートを選択し、ターミナル設定を 115200 ボー、パリティなし、8 データビット、1 ストップビットに設定します。
3. 2 つ目のイーサネット LAN ポートを、Meeting Server 背面の RJ-45 ポート（M1 とラベル付けされています）に接続します。 1 つのネットワーク接続のためのリソースしかない場合、イーサネット 1 に接続されている LAN を取り外し、それを一時的に M1 ポートに使用して仮想コンソールを有効にし、設定後にイーサネット 1 に戻します。 仮想コンソールを使用するには、M1 ポートが接続され、有効な IP アドレスで構成されている必要があります。
4. Meeting Server の電源が接続されていることを確認します。 そうでない場合、CIMC 管理インターフェイスが起動するよう、数分間差し込んでいることを確認します。 CIMC が機能するために Meeting Server の電源がオンになっている必要はありませんが、電源に接続されている必要があります。 （CIMC ステータスの外部インジケータはありません。）
5. ターミナルプログラムで、Escape と 9 のキー**を同時に押して、**ポートを CIMC に切り替えます。 ユーザー名のプロンプトが表示されます。
6. デフォルトのユーザー名とパスワードを入力します（ユーザー名：**admin**、パスワード：**password**）。
7. 初めてログインするとき、パスワードを適切なものに変更するように指示するプロンプトが表示されます。 プロンプトに従って、新しいパスワードを設定します。
8. ログインしたら、コマンドプロンプトで **scope cimc** コマンドを入力します。CIMC メニューを開いたことを反映して、コマンドプロンプトが変わります。
9. **show network detail** コマンドを入力して、管理イーサネットインタフェースの現在の設定を表示します。これには、サーバーが（ネットワーク上で利用可能な場合）DHCP 経由で取得した現在の IP アドレスも表示されます。 表示されている IPv4 アドレスをメモします (DHCP が利用できる場合)。

10. DHCP が利用できず、静的 IP を設定する必要がある場合、次のコマンドを使用し、サンプル値をネットワークに適した値に変更します。 （これらのコマンドは、ユーザーがすでに CIMC 範囲に入っていることを前提としています。）

```
scope network
set dns-use-dhcp no
set dhcp-enabled no
set v4-addr 10.1.2.3
set v4-netmask 255.255.255.0
set v4-gateway 10.1.2.1
commit
```

11. **show network detail** を入力して変更を確定します。 完了したら、コマンド **exit** を 2 回入力して、CIMC からログアウトします。
12. PC のブラウザに切り替え、設定した IP アドレスまたは CIMC シリアルインターフェイスから取得した IP アドレスにアクセスします。 証明書のセキュリティ警告を閉じると、Cisco ランディングページにユーザー名とパスワードのフィールドが表示されます。
13. ユーザー名：**admin** と、初めて CIMC に接続したときに設定したパスワードを使用してログインします。
14. [**サーバーの概要**（Server Summary）] ページが開いたら、[**アクション**（Actions）] の下の [KVM **コンソールの起動**（Launch KVM Console）] リンクをクリックします。 Java 仮想コンソールアプリケーションがロードされます。 お使いのオペレーティングシステムとブラウザによっては、セキュリティ警告やダイアログが表示される場合があります。 アプリケーションがロードされるまで続行します。サーバーに直接接続しているかのように、モニタ画像が表示されます。 サーバーの電源がオフの場合、**「信号がありません」**という大きな緑色のウィンドウが表示されます。
15. サーバーの電源がオフの場合、[**電源**（Power）] メニューから [**電源オン**（Power On）] を選択してサーバーを起動します。 数分後、VMware コンソール画面が表示されます。

ローカルモニタとキーボードを使用して接続しているかのように、仮想コンソールを使用できます。

2.4.3 タスク 2：VMware Network Management を設定する

次の手順を完了するには、モニタまたは仮想コンソール経由でサーバーにアクセスする必要があります。

サーバーの電源がオンになっていることを確認し、VMware コンソール画面が表示されたら、F2 を押して設定するか、F12 を押してシャットダウンします。

1. F2 を押してサーバーの設定を行ってください。 デフォルトのユーザ名は **root** で、デフォルトのパスワードは **c!SCo123** です。

2. デフォルトのパスワードを変更することをお勧めします:
    a. メニューオプションから、矢印キーと Enter キーを使用して、[**パスワードの設定**（Configure Password）] を選択します。
    b. プロンプトに従い、VMware root アカウントに使用するパスワードを設定します。
    メモ: VMware にはパスワードに対する厳しい要件があります。特殊文字、大文字と小文字の混在、アルファベット文字と数字を含む強力なパスワードを使用してください。
3. メニューオプションから、矢印と Enter キーを使用して、[**管理ネットワークの設定**（Configure Management Network）]、[IPv4 **の設定**（IPv4 Configuration）] を選択します。
4. 使用するネットワーク構成 DHCP または静的 IP 割り当てのオプションを選択し、ネットワークに適切な IPv4 アドレス、マスク、およびゲートウェイを構成します。
リマインダ：この IP アドレスは VMware ハイパーバイザー用のものであり、Meeting Server アプリケーション用のものではありません。 使用するアドレスは Meeting Server アプリケーションとは異なる必要があります。
5. （オプション）Meeting Server アプリケーションとは異なる VLAN 経由でハイパーバイザー管理にアクセスする場合、管理インターフェイスが関連付ける VLAN を設定します。
6. Escape を押してメインメニューに戻り、再度 Escape を押してログアウトします。

    画面の左下に VMware 管理 IP アドレスが表示されます。

2.4.3.1 仮想コンソールを使用している場合に役立つ情報

- CIMC は Meeting Server 用の強力な帯域外管理インターフェイスであり、Meeting Server がラックまたはコンピュータ室に設置されている場合に使用することを推奨します。 この管理インターフェイスは VMware または Meeting Server アプリケーションでは使用されないため、接続を維持したい場合は、M1 イーサネットポート用に専用の LAN 接続を確保する必要があります。 (NIC 共有オプションは、Cisco UCS Server のドキュメントにも記載されています。)
- 1 つのネットワーク接続のみで仮想コンソールを使用しており、一時的に M1 インターフェイスにそれを使用していた場合：
    a. インストールを完了するために、仮想コンソールはもう必要ありません。 サーバーの M1 インタフェースからイーサネットケーブルを外し、イーサネット 1 ポートに再接続します。

b. VMware 管理インターフェイスに DHCP を使用している場合、イーサネットケーブルに接続した後、サーバーを再起動して新しい IP アドレスを取得する必要があります。再起動するには、サーバー前面の電源ボタンを短く押します。サーバーが自動シャットダウンを開始します（これには数分かかります）。 電源がオフになったら、電源ボタンを使用してオンにします。 仮想コンソールが使用していたネットワークを切断しているため、サーバーが取得した IP アドレスを確認することはできません。 IP アドレスを確認するには、DHCP 管理者に連絡して、サーバーが割り当てられている IP アドレスを確認します。 Ethernet1 インターフェイスの MAC アドレスは、Cisco Meeting Server 1000 の前面にあるプルアウトタブで見つけることができます。

現在、イーサネットはサーバーの背面にあるイーサネット 1 ポートに接続されているはずです、そして VMware 管理ネットワークが使用している IP アドレスを知る必要があります。

2.4.4 タスク 3：vSphere クライアントを使用して VMware インスタンスを設定する

VMware インスタンスに接続し、Hypervisor の初期構成を完了します。

1. vSphere 6.0 または 6.5 クライアントがインストールされておらず、インストールする必要がある場合、これらの手順に従ってください。
   a. ローカル VMware インスタンスからダウンロードします。
      i. インターネットブラウザを使用して、新しいサーバーの IP を参照します。例：http://IPaddress
      ii. リンクをクリックして、**主催者のインベントリのデータベースを参照します。**
      iii. VMware ネットワーク管理のセットアップで設定したユーザ名 **root** とパスワードを入力してください。
      iv. datastore1\OVA-ISO\VMware\ に移動し、VMware-viclient... リンクをクリックしてクライアントインストーラをダウンロードします。
      v. ダウンロードしたら、ファイルを見つけてプログラムを実行し、vSphere クライアントをインストールします。
2. vSphere クライアントを開き、接続ウィンドウで VMware インスタンスの IP、ユーザー名、**root**、VMware ネットワーク管理の設定で作成したパスワードを入力します。 [**ログイン**] をクリックしてサーバに接続します。
3. サーバに接続するときに SSL 証明書の警告が表示されます。続行するには、[**無視**] をクリックしてください。 接続すると、VMware 評価版の通知が届きます。[OK] をクリックします。

2.4.4.1 VMware NTP の設定

ログが正確になるように、有効な NTP ソースを持つようにハイパーバイザーを構成します。

1. vSphere クライアントで、Meeting Server に接続し、左パネルの Meeting Server をクリックして選択します。
2. 右側パネルで、[**設定**（Configuration）] タブをクリックし、[**ソフトウェア**（Software）] の下で、[**時刻設定**（TIme Configuration）] をクリックします。
3. 表示されたページで、右上隅の **プロパティ** リンクをクリックします。
4. [**プロパティ**（Properties）] ウィンドウで、[NTP **クライアントを有効にする**（NTP Client Enabled）] チェックボックスをオンにして、[**オプション**（Options）] ボタンをクリックします。
5. リストから [NTP **設定**（NTP Settings）] をクリックし、[**追加**（Add）] ボタンをクリックして、使用したい NTP ソースを追加します。
6. リストから **全般** を選択します。
7. サービスを[**主催者と開始および停止**（Start and Stop with the host）] に変更します。
8. [開始] をクリックしてサービスを開始してください。
9. [OK] を 2 回クリックして、時間設定ページを閉じます。

2.4.5 タスク 4：VMware ライセンスを取得、アクティブ化する

VMware ライセンスを Cisco に注文した場合、ライセンスはアクティベーション コードとして別のパッケージで配信されるか、Cisco からメールで届きます。 Cisco Meeting Server1000 ごとに 2 つの 1-CPU ライセンスが必要です。 これらのアクティベーション コードは、VMware の公開ウェブサイトを使用してライセンスキーに変換する必要があります。 このタスクを完了するには、インターネットおよびメールアクセスが必要です。

2.4.5.1 VMware アクティベーションキーをアクティベートする

1. インターネットブラウザを使用して (この作業では Google Chrome 以外のブラウザを使用することを推奨しています)、https://www.vmware.com/OEM/code.do?Name=CISCO-RESELL-AC にアクセスしてください。
2. VMware アカウントでログインします。 お持ちでない場合は、ウェブページに記載されている手順を完了し、新しい VMware プロファイルを作成してください。

3. ログインしたら、ソフトウェア アクティベーション コードの割り当てに関する組織のポリシーに従って、アクティベーション コードを入力します。 これらの手順が完了すると、VMware からライセンスコードがメールで送信されます。
4. ライセンスが VMware アカウントに追加されたら、2 つのシングル CPU ライセンスをシングルのデュアル CPU ライセンスに統合する必要があります。 これは myVMware ポータルで実現します。 これらの手順については、次の VMware KB 記事で詳しく説明しています。https://kb.vmware.com/s/article/2006973
ヒント：ライセンスを VMware プロファイルに追加した直後に、ライセンスを組み合わせる際に問題が発生する場合があります。 この場合、5〜10 分待ってから再度試してください。 引き続き問題が発生する場合は、VMware ライセンスサポートに連絡してライセンスを統合してください。
5. 新しい統合ライセンスキーを入手したら、vSphere クライアントを開き、Meeting Server に接続します（まだ接続していない場合）。そして左パネルのツリーから Meeting Server をクリックします。
6. 右側のパネルで、[**設定**（Configuration）] タブを選択し、[**ソフトウェア**（Software）] で [**ライセンス機能**（Licensed Features）] をクリックします。
7. 現在の評価の詳細が表示されます。ページの右上にある [**編集**] リンクをクリックします。
8. 表示されたウィンドウで、[**このホストに新しいキーを割り当てる**（Assign a new key to this host）] を選択し、Enter ボタンをクリックしてライセンスキーを入力します。
9. [OK] をクリックしてダイアログウィンドウを閉じます。

ハイパーバイザーの基本セットアップが完了しました。

2.4.6 タスク 5：Cisco Meeting Server 1000 コンソールにアクセスする

Meeting Server インスタンス自体は、インスタンス自身の IP アドレスに接続するか、vSphere クライアントコンソール機能を介してアクセスできます。

1. vSphere クライアントを開き、Meeting Server の IP アドレスにユーザー名 **root** と以前に設定したパスワードを使用してログインします。
2. 左側のパネルから Meeting Server を選択し、プラス記号（+）を使用してツリーを展開します。 Cisco Meeting Server という名前の仮想マシンが表示され、電源がオンになっていることを示す緑の矢印が表示されます。

3. ネットワークに DHCP がある場合、現在の Meeting Server の IP アドレスを確認するには、Cisco Meeting Server VM が選択されている間に、[**概要**（Summary）] タブをクリックします。 Meeting Server が取得した IP アドレスが [**全般**（General）] セクションに表示されます。 その IP に ssh で接続することで、Meeting Server ソフトウェアの設定を続行できます。
4. ネットワークに DHCP がない場合は、vSphere クライアントの仮想マシンコンソールおよび Meeting Server の MMP コマンド **ipv4**、または **ipv6** を使用して、VM に IP アドレスを指定する必要があります。第 3 章を参照 （または『MMP コマンドライン リファレンスガイド』を参照してください）。
5. コンソールにアクセスするには、Meeting Server 仮想マシン選択時に、vSphere クライアントの [**コンソール**（Console）] タブをクリックします。 画面が空白の場合、ウィンドウ内をクリックして Enter キーを押します。 ログインプロンプトが表示されます。
   ヒント：コンソールウィンドウの外でマウスを操作できるようにするには、Control キーを押しながら Alt キーを一緒に押します。
6. ユーザ名「admin」でログインし、Enter キーを押してパスワードフィールドをスキップします。
7. パスワードのリセットが求められます。

   注意：パスワードの有効期限は 6 か月です。

残りの設定プロセスは、第 3 章の手順に従います。

3 構成

3.1 独自の Cisco Meeting Server 管理者アカウントを作成する

ユーザー名「admin」は安全性が低いため、セキュリティ上の理由から、独自の管理者アカウントを作成することをお勧めします。 さらに、1 つのアカウントのパスワードをなくした場合に備えて、2 つの管理者アカウントを持っておくことをお勧めします。そうした場合でも、もう一方のアカウントでログインして、なくしたパスワードをリセットできます。

MMP コマンド **`user add <name> admin`** を使用します。詳細については『MMP コマンドリファレンスガイド』を参照してください。 パスワードを 2 回入力するように指示されます。新しいアカウントでログインすると、パスワードの変更が求められます。

注意：パスワードの有効期限は 6 か月です。

新しい管理者アカウントを作成したら、デフォルトの「admin」アカウントを削除します。

メモ：管理者レベルの MMP ユーザーアカウントは、Call Bridge のウェブ管理インターフェイスにログインするためにも使用できます。 ウェブ管理インターフェイスを通じてユーザーを作成することはできません。

3.2 IPv4 用のネットワーク インターフェースをセットアップする

メモ: これらの手順は IPv4 用ですが、IPv6 用の同等のコマンドがあります。 詳細については、 MMP コマンドリファレンス を参照してください。

Cisco Meeting Server の仮想化導入では、最初はインターフェイス「a」という 1 つのネットワーク インターフェイスだけですが、最大で 4 つまでサポートされます（次の項を参照）。MMP は仮想展開のインターフェイス a で実行されます。

1. ネットワークインタフェース速度、二重通信、自動ネゴシエーションのパラメータを設定するには、**`iface`** MMP コマンドを使用します。「a」インタフェースの現在の設定を表示するには、MMP で入力します。

iface a

a. コマンド **iface (a|b|c|d) <speed> (full|on|off)** を使用して、ネットワークインタフェース速度（Mbps）、全二重、および自動ネゴシエーションパラメータを設定します。 たとえば、インターフェイスを 1GE、全二重に設定します。

```
iface a 1000 full
```

b. **iface a autoneg** コマンドを使用して、自動ネゴシエーションのオン/オフを切り替えます。

<on|off>. 次に例を示します。

```
iface a autoneg on
```

メモ: 特別な理由がない限り、ネットワークインタフェースは自動ネゴシエーションを「オン」に設定することを推奨します。

---

2. "a" インターフェイスは、最初は DHCP を使用するように構成されています。 既存の構成を表示するには、次のように入力します。

ipv4 a

a. DHCP IP 割り当てを使用している場合、これ以上の IP 設定は必要ありません。ステップ 3 に進みます。

b. 静的 IP 割り当てを使用している場合:

ipv4 add コマンドを使用して、指定されたサブネットマスクとデフォルトゲートウェイを持つインターフェースに静的 IP アドレスを追加します。

たとえば、ゲートウェイが 10.1.1.1 でプレフィックス長が 16 のアドレス 10.1.2.4 (ネットマスク 255.255.0.0) をインターフェイスに追加するには、次のように入力します。

```
ipv4 a add 10.1.2.4/16 10.1.1.1
```

IPv4 アドレスを削除するには、次のように入力します。

ipv4 a del <address>

3. DNS 構成の設定

Meeting Server は、SRV レコードのルックアップを含むアクティビティの多くで DNS ルックアップを必要とし、簡素化された導入に必要です。 Meeting Server をネットワークのデフォルトの DNS リゾルバに指向することをお勧めします。forwardzone の値にはピリオド「.」を使用します。

a. DNS 設定を出力するには、次のようにタイプします。

dns

b. アプリケーション DNS サーバーを設定するには、次のコマンドを使用します。

dns add forwardzone <domain name> <server IP>

メモ：フォワードゾーンは、ドメイン名とサーバアドレスのペアです。名前が DNS 階層で指定のドメイン名より下にある場合、DNS リゾルバーは指定のサーバーにクエリできます。 任意の特定のドメイン名に対して複数のサーバーを指定して、ロードバランシングとフェイルオーバーを提供できます。 「.」を指定するのが一般的です。これは、すべてのドメイン名に一致する DNS 階層のルート、つまりドメイン名を意味します。

たとえば、

```
dns add forwardzone。 10.1.1.33
```

c. DNS エントリを削除する必要がある場合は、次のコマンドを使用します:

```
dns del forwardzone <domain name> <server IP>
```

たとえば、

```
dns del forwardzone。 10.1.1.33
```

3.3 追加のネットワーク インターフェイスを追加する

Cisco Meeting Server の仮想化展開は、最大 4 つのインターフェイス (a、b、c、d) をサポートします。

必要に応じて、VMWare に 2 番目のネットワーク インターフェイスを追加できます。 しかし、Cisco Meeting Server の 2 つのインターフェースを同じサブネットに配置してはいけません。

1. vSphere Client で、VM を [**ホストとクラスタ（Hosts and Clusters）**] リストで探します。
2. [**仮想マシン設定の編集の選択（Edit Virtual Machine Settings）**] を選択します。
3. VMXNET3 タイプのネットワークアダプタを追加します。

メモ：VMXNET3 以外のイーサネットアダプタを選択すると、ネットワーク接続の問題やライセンスが無効になる可能性があります。

メモ：イーサネットアダプタの追加と変更の詳細は、VMware ウェブページ「仮想ネットワークアダプタを追加、変更する」を参照してください。

4. 新しいアダプタを追加した後、次のコマンドを使用して、MMP で使用するインターフェイスを有効にします。
   例：`ipv4 b enable`
5. VM を再起動して、アドレスとゲートウェイを手動で追加するか、または DHCP によって自動的に取得されます（そのインターフェイスで有効になっている場合）。

3.4 Call Bridge を設定する

Call Bridge には、SIP 通話制御デバイスおよび Lync フロントエンド (FE) サーバとの TLS 接続を確立するために使用されるキーと証明書のペアが必要です。 Lync を使用している場合、この証明書は Lync FE サーバによって信頼される必要があります。

コマンド **callbridge listen** <**インターフェース**>を使用して、リッスンするインターフェースを設定できます（A、B、C または D から選択）。 デフォルトでは、Call Bridge はどのインターフェイスもリッスンしません。

1. 『証明書のガイドライン』の説明に従って、証明書を作成してアップロードします。
2. MMP にログインし、インターフェイス A でリッスンするように Call Bridge を設定します。

   ```
   callbridge listen a
   ```

   メモ: Call Bridge は、別の IP アドレスに NAT されていないネットワーク インターフェイスでリッスンしている必要があります。 これは、リモート サイトと通信するときに、Call Bridge が SIP メッセージのインターフェイスで設定されたものと同じ IP を伝達する必要があるためです。

   ---

3. 次のコマンドを使用して、証明書を使用するように Call Bridge を設定します。これにより、Lync FE サーバーと Call Bridge の間で TLS 接続を確立できます。次に例を示します。

   ```
   callbridge certs callbridge.key callbridge.crt
   ```

   完全なコマンドと CA が提供する証明書バンドルの使用については、『証明書ガイドライン』で説明されています。
4. 変更を適用するために、Call Bridge インターフェイスを再起動します。

   ```
   callbridge restart
   ```

3.5 ウェブ管理インタフェースを設定する

ウェブ管理インターフェイスは、Call Bridge へのインターフェイスとして機能します。Cisco Meeting Server の API はこのウェブインターフェイスを通してルーティングされます。

ウェブ管理インターフェイスの設定には、秘密キー/証明書ペアの作成（セクション 3.5.1 を参照）と、秘密鍵/証明書ペアの MMP へのアップロード（セクション 3.5.2を参照）が含まれます。

ウェブ管理インターフェイスが有効になると、API またはウェブ管理のいずれかを使用して、Call Bridge を設定できます。

3.5.1 ウェブ管理インターフェイス用の証明書を作成する

ウェブ管理インタフェースは HTTPS 経由でのみアクセス可能です。セキュリティ証明書を作成し、それを Cisco Meeting Server にインストールする必要があります。証明書ガイドライン に記載されている手順に従います。本番環境を対象とします。このセクションでは、ラボ環境で自己署名証明書を使ってテストする方法を示します。

メモ：ウェブ管理インターフェイスではなく、API を通じて Call Bridge を設定する場合でも、ウェブ管理インターフェイス用に証明書をアップロードする必要があります。

以下の情報は、Cisco が秘密鍵の生成の要件を満たしていることを信頼していることを前提としています。 必要に応じて、公開 Certificate Authority（CA）を使用して秘密鍵と証明書を外部で生成し、外部で生成されたキー/証明書のペアを SFTP を使用して Cisco Meeting Server の MMP にロードすることもできます。 署名付き証明書を取得したら、セクション 3.5.2 に移動します。

メモ：Cisco Meeting Server をラボ環境でテストする場合、サーバー上でキーと自己署名証明書を生成できます。 自己署名証明書と秘密鍵を作成するには、MMP にログインして次のコマンドを使用します。

pki selfsigned <key/cert basename>

<key/cert basename> で生成される鍵と証明書を指定します。例:

「pki selfsigned webadmin」は、webadmin.key と webadmin.crt（自己署名）を作成します。 自己署名証明書は、プロダクション環境での使用は推奨されていません。

以下の手順では、MMP コマンド **pki csr** を使用して秘密鍵と関連する証明書署名リクエストを生成し、CA 署名用にエクスポートする方法について説明します。

1. MMP にログインし、秘密鍵と証明書の署名リクエストを生成します（CSR）。

   pki csr <key/cert basename> [<attribute>:<value>]

   引数の説明

   <key/cert basename> は新しいキーと CSR を識別する文字列です（例えば、「webadmin」と入力すると「webadmin.key」と「webadmin.csr」ファイルになります）

   許可されているがオプションの属性は次のとおりで、コロンで区切る必要があります。

   - CN：証明書に記載される CommonName です。 DNS A レコードで定義された FQDN を共通名として使用します。これを行わないと、ブラウザの証明書エラーが発生します。
   - OU：部門名

- O：組織
- L：所在地
- ST：都道府県
- C：国
- emailAddress

1 単語以上の長さの値には引用符を使用します。例：

```
pki csr example CN:example.com "OU:Accounts UK" "O:My Company"
```

2. 次のいずれかの場所に CSR を送信します。
   - Verisign などの Certificate Authority（CA）要求者の身元を確認し、署名付き証明書を発行する Verisign。
   - Active Directory 証明書サービスの役割がインストールされた Active Directory サーバーなど、ローカルまたは組織の Certificate Authority への接続については、付録 F を参照してください。

注：署名済み証明書と秘密鍵を Cisco Meeting Server に転送する前に、証明書ファイルを確認してください。 CA が証明書のチェーンを発行している場合、チェーンから証明書を抽出する必要があります。 証明書ファイルを開き、BEGIN CERTIFICATE および END CERTIFICATE の行を含む特定の証明書テキストをコピーして、テキストファイルに貼り付けます。 .crt、.cer または .pem の拡張子を持つ証明書としてファイルを保存します。 残りの証明書チェーンをコピーして別のファイルに貼り付けます。中間証明書チェーンと認識できるように明確な名前を付け、同じ拡張子（.crt、.cer または .pem）を使用します。 中間証明書チェーンは順番通りである必要があります。チェーンを発行した CA の証明書が最初で、ルート CA の証明書がチェーンの最後です。

3.5.2 HTTPS アクセスのためのウェブ管理インタフェースを設定する

注：導入時にウェブ管理者インターフェイスがインターフェイス A のポート 443 を使用するように自動的にセットアップされます。しかし、ウェブブリッジも TCP ポート 443 を使用します。ウェブ管理者インターフェイスとウェブブリッジが同じインターフェイスを使用している場合は、ウェブのポートを変更する必要があります
管理インターフェイスを 445 などの非標準ポートに変更するには、MMP コマンド **`webadmin listen <interface> <port>`** を使用します。

---

1. MMP への SSH 接続を確立してログインします。
2. SFTP を使用して、秘密鍵/証明書のペアと証明書バンドル (オプション) をウェブ管理インターフェイスにアップロードします。
3. 証明書を指定する前にウェブ管理インターフェイスを無効にしてください。

   webadmin disable
4. 次のコマンドを使用して、ステップ 2 でアップロードした秘密鍵/証明書のペアを指定します。

   webadmin certs <keyfile> <certificatefile> [<cert-bundle>]

   keyfile と **certificatefile** は、一致する秘密キーと証明書のファイル名です。 CA が証明書バンドルを提供している場合は、バンドルも証明書とは別のファイルとして含めます。 次に例を示します。

   webadmin certs webadmin.key webadmin.crt webadminBundle.crt
5. ウェブ管理インターフェイスを再起動します。

   webadmin restart
6. ウェブ管理インターフェイスを有効にします。

   webadmin enable

次に例を示します。

```
webadmin certs webadmin.key webadmin.crt
webadmin listen b 443
webadmin restart
webadmin enable
```

ウェブ管理インターフェイスにアクセスできるかどうかをテストします。例えば、https://cms- に相当するものを入力します。server.mycompany.com（または IP アドレス）をブラウザに入力し、以前作成した MMP ユーザーアカウントを使用してログインします。

メモ：バージョン 3.0 からは、ライセンスなしでトライアルモードを 90 日間のフル機能期間として使用できます。 この場合、ウェブ管理インターフェイスには、この期間中、「この CMS は現在ライセンスされていません」と表示されます。 Smart licensing の詳細および 3.0 でのライセンスの仕組みについては付録 B を参照してください。

3.6 スケジューラ用のメールサーバーを設定する

このセクションでは、スケジューラコンポーネント用にメールサーバーを設定する手順について説明します。 ミーティングがスケジュール、キャンセル、または変更されると、メール通知が参加者に送信されます。 スケジューラは、SMTP メールサーバーの設定を介したメール通知の送信をサポートします。

サーバーアドレスとポートの構成、メールプロトコルの有効化、認証のためのユーザー名の設定は、次のスケジューラ MMP コマンドで指定します。

```
scheduler email server <hostname|address> <port>
scheduler email server none
scheduler email username <smtp username>
scheduler email protocol <smtp|smtps>
scheduler email auth <enable|disable>
scheduler email starttls <enable|disable>
```

サーバーアドレスが設定されていない場合、メールはスケジューラで設定されません。 スケジューラがメール招待を送信するには、少なくとも 1 つのメールサーバーを設定する必要があります。 メールは、ミーティングのスケジュールに使用されたスケジューラからではなく、任意のスケジューラから送信できます。 メールサーバーがダウンした場合、別のスケジューラがメールを送信します。

スケジューラは、次のタイプのメール設定をサポートしています。

1. SMTP
2. SMTP と認証済みログイン（Auth Login）
3. SMTP および STARTTLS
4. SMTP（認証ログインと STARTTLS 使用）
5. SMTPS （トランザクション全体でエンドツーエンド TLS 暗号化）
6. SMTPS（認証ログインあり）

メモ：Exchange Server 2016 CU22 - 15.1.2375.7 および Exchange Server 2019 CU11 - 15.2.986.5 の使用をお勧めします。

バージョン 3.4 から、ミーティングの招待状は共通のメールアドレスからすべての参加者に送信できます。 MMP コマンド **`scheduler email common-address address@mail.domain > "<Display name>"`** で Meeting Server 上に共通のメールアドレスと表示名を設定します。 スケジューラが共通のメールアドレスから参加者にミーティング招待状を送信します。

共通メールアドレスが空の場合、スケジューラは開催者のメールアドレスから招待メールを送信します。

メモ：共通メールアドレスが設定されていない場合、SMTP サーバーによる認証では、MMP コマンド **scheduler email username <smtp user-name>** を使用してメールアドレスを設定する必要があります。 MMP で構成されたこのアカウントには、ウェブアプリユーザーの代わりにメールを送信できる適切な権限が必要です。

送信者を識別するために、表示名としてメールアドレスの他に開催者名を含めることもできます。 ウェブアプリを使用してミーティングがスケジュールされると、ウェブアプリはミーティングをスケジュールしているユーザーの名前を開催者の表示名としてスケジューラに送信します。 任意の名前を表示名として設定するには、オプションのパラメータ **organizationDisplayName** をスケジューラ API に含めることができます。

メール招待状が配信されなかった場合、スケジューラは定期的に送信を再試行します。 スケジューラのメールキュークリーンアップは、特定の有効期限後に、キューに入れられた失敗メールをクリーンアップします。

3.6.1 スケジューラメールの設定（SMTP あり）

スケジューラが SMTP 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定ポートでリッスンするように設定します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. スケジューラを有効にします。

   scheduler enable

3.6.2 スケジューラ SMTP（認証ログイン設定あり）

スケジューラが認証ログインを使用して SMTP 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコル用に指定されたポートでリッスンするように設定し、SMTP サーバーが認証ログインをサポートするようにし、認証用のユーザーアカウントを設定します。 MMP で構成されたこのアカウントには、ウェブアプリユーザーの代わりにメールを送信できる適切な権限が必要です。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. [認証ログイン（Auth Login）] オプションを有効にします。

   scheduler email auth enable

4. 認証に使用するユーザー名を設定してください。

   scheduler email username <username>

   パスワードを入力してください。

   ```
   scheduler email username test@test.com
   ```

   パスワードを入力してください：

   パスワードを再度入力してください：

5. スケジューラを有効にします。

   scheduler enable

3.6.3 スケジューラ SMTP と STARTTLS の設定

スケジューラが SMTP および STARTTLS 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定されたポートでリッスンするように設定し、STARTTLS を有効にします。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. メールサーバーとポートを設定します。

scheduler email server <hostname|address> <port>

たとえば、

```
scheduler email server exchange.example.com 25
scheduler email server 10.27.33.55 25
```

3. STARTTLS オプションを有効にします。

   scheduler email starttls enable

4. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

5. スケジューラコンポーネントを有効にします。

   scheduler enable

3.6.4 スケジューラ SMTP（STARTTLS 設定による認証ログインあり）

スケジューラが Auth Login を使用した SMTP および STARTTLS 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定されたポートでリッスンするように設定し、STARTTLS を有効にします。 さらに、SMTP サーバーを有効にしてログイン認証をサポートし、認証に使用されるユーザーアカウントを設定し、STARTTLS を有効にします。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. 指定されたメールサーバーとポートを設定します。

scheduler email server <hostname|address> <port>

たとえば、

```
scheduler email server exchange.example.com 25
scheduler email server 10.27.33.55 25
```

3. [認証ログイン（Auth Login）] オプションを有効にします。

   scheduler email auth enable

4. 認証に使用するユーザー名を設定してください。

   scheduler email username <username>

   パスワードを入力してください。

   ```
   scheduler email username test@test.com
   ```

   パスワードを入力してください：

   もう一度パスワードを入力してください:

5. STARTTLS オプションを有効にします。

   scheduler email starttls enable

6. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

7. スケジューラコンポーネントを有効にします。

   scheduler enable

3.6.5 スケジューラ SMTPS の構成

スケジューラが SMTPS 経由でメール通知を送信できるようにするには、特定のポートでエンドツーエンド SMTP 暗号化をサポートするようにメールサーバーを設定します。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. 指定されたメールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. メールプロトコルを SMTPS 設定します。

   scheduler email protcol smtps

4. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーン内に中間証明書がある場合、ルート CA 証明書を設定するか、代わりにまたはルート証明書、中間証明書 1、中間証明書 2 以降を含む証明書バンドルの順に設定します。

5. スケジューラコンポーネントが SMTPS を使用してメール設定を完了できるようにします。

   scheduler enable

3.6.6 スケジューラ SMTPS（認証ログイン設定あり）

スケジューラが Auth Login を使用した SMTPS 経由でメール通知を送信できるようにするには、特定のポートでエンドツーエンド SMTP 暗号化をサポートするようにメールサーバーを設定します。 さらに、SMTPS サーバーが Auth Login をサポートするようにし、認証に使用するユーザーアカウントを設定します。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. 指定されたメールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. [認証ログイン（Auth Login）] オプションを有効にします。

   scheduler email auth enable

4. 認証に使用されるユーザーのユーザー名を設定します。

   scheduler email username <username>

   パスワードを入力します。

   ```
   scheduler email username test@test.com
   ```

   パスワードを入力してください：

   パスワードを再度入力してください：

5. メールプロトコルを SMTPS 設定します。

   scheduler email protcol smtps

6. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

7. スケジューラコンポーネントが Auth Login で SMTPS を使用してメール設定を完了できるようにします。

   scheduler enable

3.6.7 スケジューラの詳細ログ

スケジューラは、ウェブブリッジ接続、メール通知、およびスケジューラ timedLogging MMP コマンドを使用した API の詳細なログを有効にするオプションをサポートしています。

timedLogging が有効ではない場合、Meeting Server は次の出力を表示します。

```
cms-vm> scheduler timedLogging
{
"webBridge": "0",
"api": "0",
"email": "0"
}
```

timedLogging オプションを有効にするには、次のコマンドを使用します。

scheduler timedLogging (webBridge|api|email) <time>

たとえば、

```
cms-vm> scheduler timedLogging webBridge 600
SUCCESS
```

time 変数は秒単位で表され、設定された継続時間の timedLogging を有効にします。

```
cms-vm> scheduler timedLogging
{
"webBridge": "594",
"api": "0",
"email": "0"
}
```

設定した継続時間が経過するか、特定の調査またはトラブルシューティングの手順が完了したら、SFTP を使用してログファイルをダウンロードします。

付録 A Cisco Meeting Server 1000 の技術仕様

A.1 物理仕様：

シャシー：Cisco UCS C220 M5 ラックサーバー または Cisco UCS C220 M4 ラックサーバー
重さ：18+kg（40 ポンド）
サイズ：高さ 1RU

ラック要件：19 インチ標準ラック

A.2 環境仕様

動作温度：5～35°C（41～95°F）
動作湿度：5～93% 結露しないこと

A.3 電気的仕様

該当する Cisco UCS C220 サーバ設置およびサービスガイドの「電源の仕様」を参照してください。

A.4 ビデオおよび音声仕様：

この表は、Cisco Meeting Server ソフトウェアをホストしているプラットフォーム間でのコールキャパシティの比較を示しています。

表 4：Meeting Server プラットフォーム間のコールキャパシティ

通話のタイプ	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 1000 M6	Cisco Meeting Server 2000 M5v2	Cisco Meeting Server 2000 M6
フル HD の通話 1080p60 ビデオ 720p30 コンテンツ	30	40	218	324
フル HD コール 1080p30 ビデオ 1080p30/4K7 コンテンツ	30	40	218	324

通話のタイプ	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 1000 M6	Cisco Meeting Server 2000 M5v2	Cisco Meeting Server 2000 M6
フル HD 通話 1080p30 ビデオ 720p30 コンテンツ	60	80	437	648
HD 通話 720p30 ビデオ 720p5 コンテンツ	120	160	875	1296
SD 通話 480p30 ビデオ 720p5 コンテンツ	240	320	1250	1875
音声通話（G.711）	2200	3000	3000	3200

メモ：バージョン 3.2 以降の Meeting Server では、Meeting Server 1000 M5v2 および Meeting Server 2000 M5v2 ハードウェアバリアントで増加したコールキャパシティをサポートしています。

A.5 Cisco Meeting Server でサポートされるユーザー数

バージョン 3.3 から、Cisco Meeting Server クラスタは、データベースが置かれているサーバーに応じて、最大 300,000 のユーザーをサポートできます。 クラスタ中のすべてのデータベースは、同じスペックサーバー上になければなりません。

表 5：Cisco Meeting Server でサポートされるユーザー数

Cisco Meeting Server	ユーザーの発信者最大数
Meeting Server 2000 M5v2	300,000
Meeting Server 2000 M5v1	200,000
Meeting Server 2000 M4、Meeting Server 1000 M4、M5v1、M5v2、および仕様ベースのサーバー	75,000

メモ：多数のユーザーを LDAP 同期すると、通話参加時間が長くなる可能性があります。 メンテナンス期間中またはオフピーク時に、Meeting Server に新しいユーザー/スペースを追加することをお勧めします。

付録 B Cisco ライセンス

Cisco Meeting Server のライセンスが必要です。 バージョン 3.4 から、Meeting Server に Smart Licensing が必須になりました。 既存のローカルライセンスは、ライセンスの有効期限が切れるまで引き続きサポートされます。 このセクションでは、Smart Licensing 方式のライセンス情報について説明します。

B.1 スマートライセンシング

Meeting Server のバージョン 3.0 では、Cisco Meeting Management バージョン 3.0（またはそれ以降）を使用する Cisco Meeting Server 上の AC のサポートを導入しました。 このソフトウェア ライセンス モデルへの移行、つまり従来の製品アクティベーション キー（PAK）ライセンスから Smart Licensing への移行により、ライセンスの購入、登録、ソフトウェア管理のユーザー エクスペリエンスが向上します。 また、Meeting Server を他の Cisco 製品のソフトウェアライセンシングに対するアプローチと整合させ、Cisco Smart Account（組織全体のライセンスを表示、保存、管理できる中央リポジトリ）を利用します。

メモ：Cisco Smart Licensing クラウド証明書は 2023 年 2 月に更新されます。更新後、Smart Licensing クラウドで直接、またはオンプレミスの Cisco Smart Software Manager（SSM）を介したすべての通信に影響が及びます。 2023 年 2 月より前に Meeting Management 3.6 にアップグレードすることをお勧めします。一眼レフ/PLR 顧客も、新しいライセンスの取得、手動同期の実行、または新しいコールブリッジの追加を行う場合、ミーティング管理 3.6 にアップグレードする必要があります。

すべての新規ライセンス購入には、引き続き PAK コードが付与されます。参照用に保持しておきます。これは、ミーティング管理が同期するスマートアカウントですべてのライセンスが利用できるためです。

詳細およびスマートアカウントの作成については、https://software.cisco.com に移動して Smart Licensing を選択してください。

Meeting Server のライセンスが 3.0 以前のバージョンからの変更点：

- Cisco Meeting Management バージョン 3.0（またはそれ以降）はバージョン 3.0 で必須です。ミーティング管理は Meeting Server ライセンスファイルを読み取り、製品の登録とスマートアカウント（セットアップされている場合）との対話を処理します。

- スマートアカウントの 1 セットの Meeting Server ライセンスで複数のクラスターのライセンスを取得できるようになり、3.0 以前の場合のように、個々の Meeting Server インスタンスにライセンスファイルをロードする必要がなくなりました。
- Smart Licensing を含むミーティング管理は、クラスターごとに Call Bridge の数を追跡するため、R-CMS-K9 アクティベーション ライセンスの必要性を排除します。
- 既存のライセンスを持たない新規展開の場合：
    - 新しく購入したライセンスは、デフォルトで Smart が有効になっており、スマートアカウントが必要です。ライセンスの詳細をミーティング管理に入力すると、スマートアカウントに保持されているものに対してライセンスの詳細を検証します。
- 各 Call Bridge にローカルライセンスファイルがある既存の展開の場合：
    - Cisco Smart Software Manager（CSSM）ポータル を使用してスマートアカウントに移行し、既存のライセンスをスマートに変換するオプションを選択できます。
- SMP Plus および PMP Plus ライセンスの使用数が組み合わされて、日を超過使用数としてカウントされるかどうかが決定されます（いずれかのライセンスが期限切れの場合、1 日は使用資格の超過使用数とみなされます）。 他の機能ライセンス（例えば、録画またはカスタムレイアウト）については、個別に評価され、Meeting Management 経由で権限付与で有効化されます（ライセンスがスマートアカウントに存在すると想定）。

メモ：「超過」という用語は、ライセンス使用数が利用資格を上回る状況を表すのに使用されています。

メモ：ミーティング管理はすべての 3.0 の展開に必要であるため、顧客が大規模な展開を行う場合、ミーティング管理はアクティブなミーティング管理なしの新しいライセンスのみのモードで導入できます。

B.2 スマートアカウントおよびバーチャルアカウント情報

スマートアカウントにはバーチャルアカウントを含めることができます。バーチャルアカウントを使えば、部門ごとなど、指定の指定ごとにライセンスを整理することができます。Meeting Server および Meeting Management でスマートバーチャルアカウントを使用する際の注意事項は以下の通りです。

- 単一のミーティング管理に対する各 Meeting Server クラスタは、ユーザー定義のスマート バーチャル アカウントにリンクされている必要があります。
- 各バーチャルアカウントは、Smart Licensing を処理するように設定された単一のミーティング管理サーバーのみに接続できます。
- 1 つのミーティング管理のみをスマートに設定します。Smart Licensing の 2 つ目の冗長ミーティング管理を Smart に設定**しないでください。**ライセンス使用数の二重カウントが発生するため、お勧めしません。
- PMP Plus、SMP Plus、および録画/ストリーミングライセンスは、単一のバーチャルアカウント内の単一のミーティング管理インスタンスおよび Smart Licensing を使用して、複数のクラスターにわたって共有できます。
- ACU ライセンスはミーティング管理ライセンスダッシュボードでは利用できません。ACU は 3.0 以降ではサポートされていません。

B.3 Meeting Server でのスマートライセンスの仕組み - 概要

ライセンスが Meeting Server 3.0 以降で動作するためには、Meeting Management が必須です。 Meeting Server と Meeting Management の間の信頼と対話が導入され、Smart を使った新しいライセンスのサポート、または既存の顧客がインストールされたライセンスファイルを使用している場合、この信頼できるリンクにより、ミーティング管理が Meeting Server のライセンスを取得できるようになります。

メモ：Cisco Meeting 管理を使った Smart Licensing の管理の詳細は、『ミーティング管理管理者ガイド』を参照してください。

Smart Licensing を実装するためのワークフローの概要は以下の通りです。

1. ミーティング管理を Smart Licensing バーチャルアカウントに登録します。
2. Meeting Server が最初に起動したとき、ライセンス状況の値は定義されていません。

   メモ：トライアルモードは、90 日間のフル機能の期間、ライセンスなしで使用できます。

   ---

3. Meeting Server は、Smart Licensing を管理するためにセットアップされたミーティング管理インスタンスに最初に接続するときに、Meeting Server にライセンスが以前に適用されているかどうかを確認します。 有効になっていない場合、ライセンスの有効期限が 90 日後に設定されます。

ライセンスの有効期限はミーティング管理に表示され、また付録 B.5 に示すように clusterLicensing API にも返されます。

メモ：機能ライセンスの有効期限は、最大で 90 日後になります。

---

4. Meeting Management は、Meeting Server が準拠していることを確認するために必要なライセンスがあるかどうかを確認するために、クラスターの Meeting Server ライセンスの使用状況を照合し、スマートアカウントに日単位でレポートを行います。 スマートアカウントはミーティング管理に応答し、Meeting Server が準拠しているかどうかを示します。 ミーティング管理では、有効期限を次のように適切に設定します。

   a. ミーティング管理が、ライセンスが存在し、特定の機能の利用権限を下回っていることを確認した場合、有効期限は 90 日後に延長されます。

      メモ：Meeting Server がミーティング管理に接続せず、90 日間の使用状況データを送信しない場合、Meeting Server のライセンスは更新されず、期限切れになります。 ライセンス期限切れ時の強制措置に関する情報は、 セクション B.4 を参照してください。

   ライセンスの使用数が資格を超える場合、またはライセンスが見つからない場合、施行は次のように行われます。

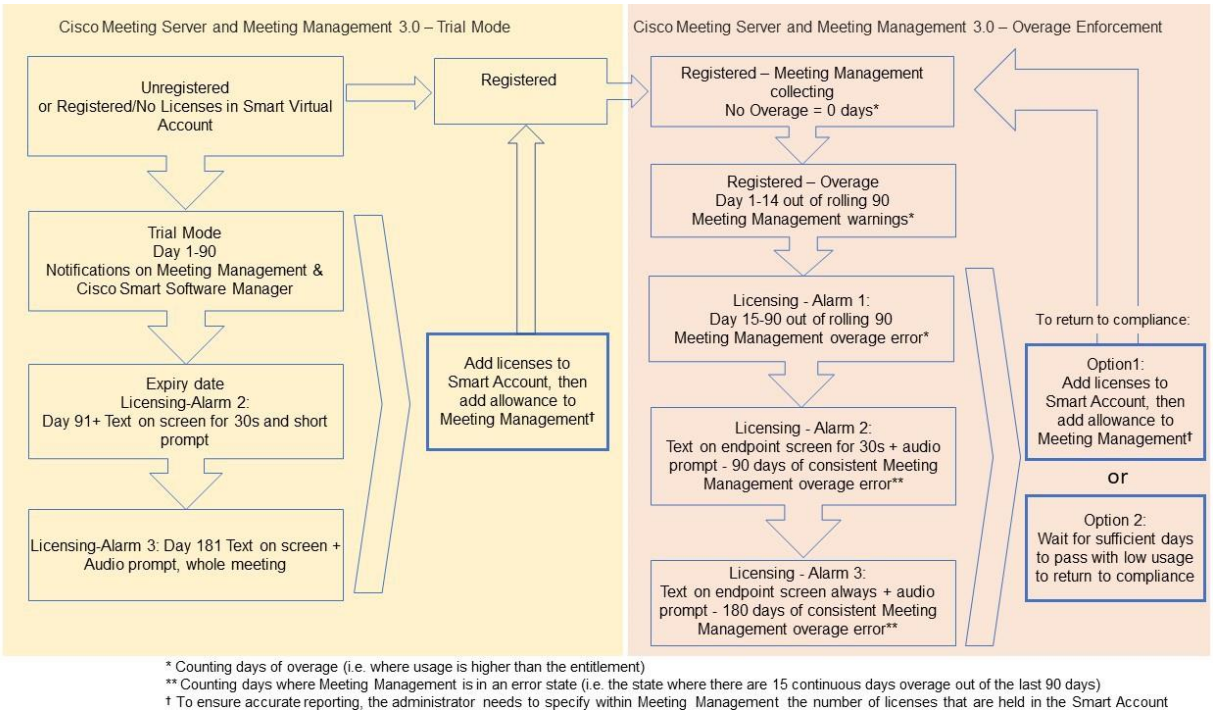
   b. ミーティング管理が過去 90 日間のうち 15 日間未満が非準拠であると特定した場合、これを許可し、Meeting Server の有効期限日をその時点から 90 日後の将来にリセットします。 管理者は「ライセンスが不十分」を通知する視覚的な警告を受け取ります。

   c. ミーティング管理で過去 90 日間のうち 15 日間以上で準拠していないことが確認された場合、第 1 レベルの強制（アラーム 1）が発生します。つまり、ミーティング管理インターフェイスに準拠していないことが通知されます。

   d. 超過が続く場合、ミーティング管理は 90 日のクロックをリセットしません。新しいライセンスを追加するための xx 日間のカウントダウンが表示されます。そうしないと、ミーティングに参加するすべての参加者に対して、アラームレベル 2 と 3 が有効になります 付録 B。

付録 B の左側にトライアルモードで最初に起動してから、右側に超過数の施行に至るまでの強制フローを示します。

図 2：Cisco Meeting Server および Cisco Meeting Management Smart Licensing の強制フロー



B.4 期限切れライセンス機能の強制アクション

以前は、Meeting Server は再起動時にのみライセンスファイルを評価していました。 3.0 から、機能がライセンスされているかどうかの現在のステータスが動的に変更される可能性があります。これは、機能ライセンスの有効期限が切れている場合や（以前は再起動するまで確認できなかった場合）、または API が変更された場合などです。 ミーティング管理で強制措置が Smart Licensing で計算されます。

メモ：Smart Licensing ポータルを使用して、「不十分なライセンス」のメール通知を有効にできます。

ライセンス機能の有効期限が切れると、 表 6 に記載のアクションが行われます。

表 6：期限切れライセンスの強制アクション

機能	アクション
callBridge	有効期限が切れた場合：すべての参加者/すべてのミーティングのミーティングに参加するときに、視覚的なテキストメッセージが画面に 30 秒間表示され、音声プロンプトが再生されます。 （アラームレベル 2） 90 日以上前に期限切れになった場合、またはライセンスが存在しない場合：以前と同じですが、ビジュアルメッセージは永久的なものです。 音声プロンプトにより、「展開はライセンスに準拠していません。管理者に連絡してください」が再生されます。（アラームレベル 3） ただし、暗号化されたコールは、ライセンスなし状態では処理されません。 メモ：上記のアクションを防ぐには、callBridge または callBridgeNoEncryption のみが必要です。
callBridgeNoEncryption	
PMP/SMP	
customizations	有効期限が切れているか、存在しない場合、ミーティング中にカスタマイズ機能はアクティブになりません。
レコーディング	有効期限が切れているか、出席していない場合、新しい録画を開始することはできません（サードパーティのレコーダーかどうかは関係ありません）。 このライセンスは録画とストリーミングを表すため、同じ制限がストリーミングにも適用されます。

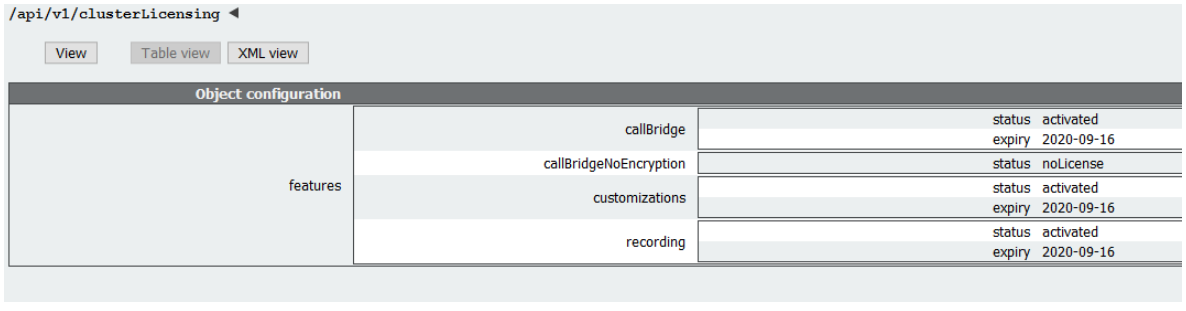
アラーム 2 および 3 をオフにするには、スマートアカウントにライセンスを追加するだけです。

B.5 ライセンス情報を取得する方法（Smart Licensing）

Meeting Server のウェブ管理インターフェイスを使用してクラスタのライセンス情報を取得するには、以下を行います。

1. Meeting Server のウェブ管理インタフェースにログインして [**設定**（Configuration）] > [API] を選択します。
2. API オブジェクトのリストで、/api/v1/clusterLicensing **後にタップします。**
3. クラスターの現在のライセンス状況は、次の例のように表示されます。

図 3：clusterLicensing API - ライセンスステータス



B.6 Cisco Meeting Server ライセンス

次の機能を使用するにはライセンスが必要です。

- Call Bridge
- Call Bridge 暗号化なし
- カスタマイズ（カスタムレイアウト用）
- 録画またはストリーミング

機能ライセンスに加えて、ユーザーライセンスも購入する必要があります。ユーザーライセンスには 2 つの異なるタイプがあります。

- PMP Plus、
- SMP Plus、

メモ：トライアルモードは、90 日間のフル機能の期間、ライセンスなしで使用できます。

ユーザーライセンスの詳細は、セクション B.8 を参照してください。

メモ：Cisco Meeting Server 1000、Cisco Meeting Server、および VM ソフトウェアイメージ用のアクティベーションキーを購入するときは、SIP メディア暗号化を有効にするか無効にするか（暗号化されていない SIP メディア）から選択できます。 暗号化されていない SIP メディアモードとアクティベーションキーの詳細については、 『導入ガイド』を参照してください。

B.6.1 パーソナル Multiparty Plus ライセンス

Personal Multiparty Plus（PMP Plus）は、頻繁にビデオミーティングを主催する特定のユーザーに割り当てられた指名主催者ライセンスを提供します。 これは、Cisco UWL Meetings または Flex Meetings（PMP Plus を含む）を通じて購入できます。 Personal Multiparty Plus は、ビデオ会議のためのオールインワンのライセンス製品です。 これにより、ユーザーはあらゆるサイズの電話会議を開催できます（導入された Cisco Meeting Server ハードウェアの制限内）。 誰でもどのエンドポイントからでもミーティングに参加でき、このライセンスは最大 HD 1080p60 品質のビデオ、音声、コンテンツ共有に対応します。

メモ：Unified Communications Manager を使用すると、アドホック電話会議の開始者を識別することができます。PMP Plus ライセンスが割り当てられている場合は、それが電話会議で使用されます。

メモ：個人の PMP Plus ライセンスを使用するアクティブな通話数を確認するには、パラメータ **callsActive** を API オブジェクトで使用します。**/system/multipartyLicensing/activePersonalLicenses**. 通常、2 つのコールをアクティブにできるため、1 つは開始、もう 1 つは終了とします。 通話が Call Bridge のクラスターで発生する場合、パラメータ **weightedCallsActive** を API オブジェクトで使用します。**/system/multipartyLicensing/activePersonalLicenses** for each Call Bridge in the cluster. クラスター全体の **weightedCallsActive** の合計が、個人のPMP Plusライセンスを使用するクラスタ上の

個別のコール数と一致します。 PMP Plus ライセンスの上限を超えた場合、SMP Plus ライセンスが割り当てられます。セクション B.9 を参照してください。

B.6.2 Shared Multiparty Plus ライセンス

Shared Multiparty Plus（SMP Plus）は、まれにビデオミーティングを主催する複数のユーザーによって共有される同時ライセンスを提供します。 Shared Multiparty Plus は、PMP Plus 主催者ライセンスを持たないすべての従業員がビデオ会議にアクセスできるようにします。 これは、多くの従業員が共有する会議室システムを展開している顧客に最適です。 PMP Plus を持つユーザーまたは SMP Plus ライセンスを使用するユーザーは、同じように優れたエクスペリエンスを得ることができます。スペースでミーティングを主催したり、アドホック ミーティングを開始したり、今後のミーティングをスケジュールしたりできます。 各共有主催者ライセンスは、任意のサイズ (展開されたハードウェアの制限内) の 1 つの同時ビデオ ミーティングをサポートします。

メモ: 必要な SMP Plus ライセンスの数を確認するには、パラメータ **callsWithoutPersonalLicense** を使用します。API **/system /multipartyLicensing**. 通話が Call Bridge のクラスター上にある場合は、パラメータ **weightedCallsWithoutPersonalLicense** を API object **/system/multipartyLicensing** で使用します。> クラスター内の各 Call Bridge に対して。 クラスター全体の **weightedCallsWithoutPersonalLicense** の合計は、SMP Plus ライセンスを必要とするクラスター上の個別の通話の数と一致します。

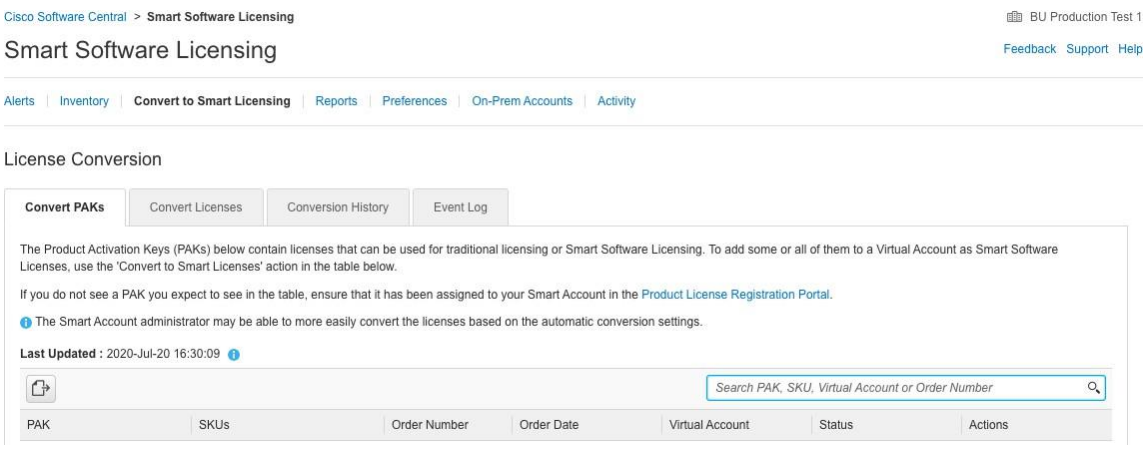
B.7 スマートライセンシング登録プロセス

スマートライセンシングの有効化

1. Cisco Smart Software Manager（CSSM）ポータル にログインし、[Meeting Server ライセンスを持つバーチャルアカウント（Virtual Account with Meeting Server Licenses）] を選択します。
2. 登録トークンを生成します。
3. トークンをクリップボードにコピーします。
4. ライセンスレポートに使用するミーティング管理のインスタンスを開きます。
5. **設定** ページの [**ライセンス**] タブに移動します。
6. [**変更**] をクリックします。
7. [Smart Licensing] を選択し、 [**保存**] を選択します。
8. [**登録**（Register）] をクリックします。
9. 登録トークンを貼り付けます (これにより、ミーティング管理を Smart Licensing ポータルに接続できます)。
10. [**登録**（Register）] をクリックします。
11. 登録が済んだら、バーチャルアカウントにあるライセンス数を確認してください。
12. ミーティング管理で、 **ライセンス** ページに移動します。
13. バーチャルアカウントで所有するライセンスのライセンス情報を入力します。

    バーチャルアカウントに表示されていないライセンスがある場合は、[**ライセンスの変換**] タブを使用し、PAK で検索し、 [**ライセンスの変換**] **を選択します。** 追加 図 4 に従います。 (ライセンスが見つからない場合は、 licensing@cisco.com にメールを送信してケースを開きます。)

図 4: Smart Licensing のライセンス変換



B.8 ユーザーに Personal Multiparty ライセンスを指定する

このプロセスでは、ユーザーが単一の LDAP ソースからインポートされる必要があります。詳細については、『ミーティング管理管理者ガイド』」の「プロビジョニング - ユーザーのインポート」の章を参照してください。

B.8.1 特定のユーザーがライセンスを持っているかどうかを確認するには、以下を行います。

1. API オブジェクトのリストで、[/users **回の後**] **の** [] **をタップします。**
    a. 特定のユーザーの**オブジェクト** ID を選択します
    b. このユーザーに関連付けられた userProfile の**オブジェクト** ID を特定する
2. API オブジェクトのリストで、[/users **回の後**] **の** [] **をタップします。**
    a. 特定のユーザーの**オブジェクト** ID を選択します
    b. パラメータ hasLicenceの設定を確認してください。 true に設定すると、ステップ 1 で特定されたユーザーが Cisco Multiparty ユーザーライセンスに関連付けられます。 false に設定すると、ユーザーに Cisco Multiparty ユーザーライセンスは関連付けられません。

注：userProfile が削除されると、ldapSource およびインポートされたユーザーの userProfile の設定が解除されます。

B.9 Cisco Multiparty ライセンスの割り当て方法

スペースでミーティングが開始されると、Cisco ライセンスがスペースに割り当てられます。Cisco Meeting Server により割り当てられるライセンスは、以下のルールにより決定されます。

- スペース所有者が定義されており、Cisco PMP Plus ライセンスが割り当てられている、Meeting Server からインポートされた LDAP ユーザーに対応する場合、その所有者のライセンスは、その人物が電話会議でアクティブであるかどうかに関係なく割り当てられます。
- ミーティングが Cisco Unified Communications Manager からのアドホックエスカレーションで作成された場合、Cisco Unified Communications Manager はミーティングをエスカレートするユーザーの GUID を提供します。 その GUID が、Meeting Server からインポートされた Cisco PMP Plus ライセンスを持つ LDAP ユーザーに対応する場合、そのユーザーのライセンスが割り当てられます。そうでない場合は、

- ミーティングが Cisco TMS バージョン 15.6 以降からスケジュールされた場合、TMS はミーティングの所有者に情報を提供します。 そのユーザーが、Cisco PMP Plus ライセンスが割り当てられたユーザー ID/メールアドレスで、Meeting Server からインポートされた LDAP ユーザーに対応する場合、そのユーザーのライセンスがミーティングに割り当てられます。そうでない場合は、次に、
- Cisco SMP Plus ライセンスが割り当てられている。

B.10 Cisco Multiparty ライセンスの使用状況を確認する

マルチパーティライセンスの使用状況を表示するには、ミーティング管理を使用することをお勧めします。 ただし、API は使用できます。

表 7 は、Multiparty ライセンスの消費量を決定するために使用できる API オブジェクトとパラメータの一覧です。

表 7: マルチパーティライセンスの使用に関連するオブジェクトとパラメータ

API オブジェクト：	パラメータ	使用目的...
/system/license	個人用、 共有	Cisco Meeting Server のコンポーネントが Multiparty ライセンスを持ち、アクティベートされているかどうかを判別します。 値は次のとおりです: noLicense、アクティブ化、猶予、期限切れ。 有効期限日と上限数も表示されます。
/system/multipartyLicensing	PersonalLicenseLimit、 sharedLicenseLimit、 personalLicenses、 callsWithoutPersonalLicense、 weightedCallsWithoutPersonalLicense	利用可能で使用中のライセンスの数を示します
/system/multipartyLicensing/ activePersonalLicenses	CallsActive、 weightedCallsActive	Personal Multiparty Plus ユーザライセンスを使用しているアクティブなコール数を示します。
/userProfiles	hasLicense	ユーザーが Cisco Multiparty ユーザーライセンスに関連付けられているかどうかを示します。

Cisco Multiparty ライセンスをサポートするための、これらの追加のオブジェクトとフィールドの詳細については、『Cisco Meeting Server API リファレンスガイド』を参照してください。

B.11 SMP Plus ライセンスの使用数を計算する

次の特定のシナリオにおいて、ミーティングで使用される SMP Plus ライセンスは、フルライセンスの 1/6 に減らされます。

- 出席者がビデオを使用していない音声のみの電話会議
- Lync ゲートウェイ通話（Meeting Server が記録またはストリーミングを行っている場合を除く）
- ウェブアプリと 1 つの SIP エンドポイント、または 2 つのウェブアプリが関係する Meeting Server が録画またはストリーミング中の場合を除き、録画中またはストリーミング中は完全な電話会議と見なされ、SMP Plus ライセンスが消費されます。

フル SMP Plus ライセンスは、所有者のプロパティが未定義のスペースからインスタンス化された音声/ビデオ会議、PMP Plus ライセンスを持たないインポートされた LDAP ユーザーが所有、または PMP Plus ライセンスがすでに使用されているインポートされた LDAP ユーザーが所有する音声ビデオ会議です。これは参加者数に関係ありません。

メモ: ポイントツーポイント通話は次のように定義されます:

- Meeting Server 上に永久スペースがない
- レコーダーまたはストリーマを含めて 2 人未満の参加者
- Lync AVMCU で主催されている参加者がいない、

これには、Lync ゲートウェイ通話だけでなく、他のタイプの通話 (ポイントツーポイント ウェブ アプリからウェブ アプリ、ウェブ アプリから SIP、および SIP から SIP) が含まれます。

B.12 Meeting Server からライセンス使用状況のスナップショットを取得する

管理者は Meeting Server からライセンスの使用状況を取得できます。 これらにはウェブ管理インターフェイスからはアクセスできません。代わりに、POSTMAN:

導入内の Meeting Server の主催者 ID を取得するには、**`/system/MPLicenseUsage/knownHosts`** で GET を使用します。 リストの最初のページ以外の主催者 ID を取得するために必要な場合は、オフセットと制限を指定します。

`/system/MPLicenseUsage` で GET を使用して、指定された主催者 ID を持つ Meeting Server の Call Bridge からライセンスの使用状況を取得します。 スナップショットの開始時刻と終了時刻を指定します。
使用中のパーソナルライセンス数、使用中の音声のみ、ポイントツーポイント、または音声でもポイントツーポイントでもないライセンスの数、記録されている通話の数、ストリーミングされた通話の数に関する情報を提供します。

メモ: メモ:個人ライセンスと共有ライセンスは、通話がスパンする Call Bridge の数で正規化されます。

B.13 ライセンスレポート

ミーティング管理には、過去 90 日間のライセンスレポート/使用情報があります。Cisco Smart Software Manager にはライセンスレポート情報も含まれます。 録画ライセンスの使用は同時に録画する会議の数を示し、同様にストリーミング ライセンスの使用は同時にストリーミングする会議の数を示します。

B.14 レガシーライセンスファイルによる方法

このセクションは、従来のライセンス方法を使用している場合にのみ適用されます。 バージョン 3.4 から、従来のライセンスのサポートは廃止されました。 既存のローカルライセンスは、ライセンスの有効期限が切れるまで引き続きサポートされます。

B.14.1 ライセンスファイルを入手、入力する

Cisco Meeting Server のすべての仮想化導入にはライセンスファイルが必要です。ライセンスファイルは仮想サーバーの MAC アドレス用です。

注：既存の導入に Cisco Meeting Server 2.0 をアップロードする場合、Acano サーバー用に発行された「acano.lic」ライセンスを引き続き使用することができます。 しかし、展開を拡張したい場合は、Cisco ライセンスを購入する必要があります。

ライセンスを購入した後、従来のライセンス方法を使用している場合にのみ、この章に従って Cisco Meeting Server にライセンスを適用してください。

B.14.1.1 ライセンスファイルを Cisco Meeting Server に転送する

このセクションは、すでに Meeting Server に必要なライセンスを Cisco パートナーから購入しており、PAK コードを受け取っていることを前提としています。

これらの手順に従い、次のアドレスを使用して、Cisco ライセンス登録ポータルサイトを使用して Meeting Server の MAC アドレスに PAK コードを登録します。

1. サーバーの MMP にログインして Meeting Server の MAC アドレスを取得し、MMP コマンド **`iface a`** を入力します。

   メモ: これは VM の MAC アドレスであり、VM がインストールされているサーバプラットフォームの MAC アドレスではありません。

   ---

2. Cisco ライセンス登録ポータルサイト を開いて、Meeting Server の PAK コードと MAC アドレスを登録します。
3. PAK に R-CMS-K9 アクティベーション ライセンスがない場合、機能ライセンスに加えてこの PAK が必要になります。
4. ライセンスポータルからライセンスファイルの zip 圧縮されたコピーがメールで送信されます。Zip ファイルを解凍し、結果として得られた xxxxx.lic ファイルの名前を **`cms.lic`**。

5. SFTP クライアントを使用して Meeting Server にログインし、 **cms.lic** ファイルを Meeting Server ファイルシステムにコピーします。
6. MMP コマンドを使用して Call Bridge を再起動する **callbridge restart**
7. Call Bridge を再起動したら、MMP コマンドを入力してライセンスのステータスを確認します。 **license**
   アクティブ化された機能と有効期限が表示されます。

B.14.1.2 ライセンスファイルの転送後

ライセンスを適用するには、Call Bridge を再起動する必要があります。 ただし、これを行う前に、Call Bridge 証明書と、Call Bridge がリッスンするポートを設定しておく必要があります。

ライセンスファイルが適用されると、ウェブ管理インターフェイスにログインしたときに、「Call Bridge はアクティベーションが必要です」というバナーは表示されなくなります。

メモ：バージョン 3.0 からは、ライセンスなしでトライアルモードを 90 日間のフル機能期間として使用できます。 この場合、ウェブ管理インターフェイスには、この期間中、「この CMS は現在ライセンスされていません」と表示されます。 Smart licensing の詳細および 3.0 でのライセンスの仕組みについては付録 B を参照してください。

注：単一の結合された、または Core または Edge サーバーの分割として複数のサーバーをクラスタ化して導入する場合は、『スケーラビリティとレジリエンス導入ガイド』の付録*「クラスタ内で Call Bridge ライセンスを共有する」*を参照してください。これは、従来のライセンス方法を使用している場合の詳細情報です。 それ以外の場合は、「スマートライセンス」の項を参照してください。スマートアカウントの 1 セットの Meeting Server ライセンスで複数のクラスターにライセンスを付与できるようになりました。3.0 以前の場合のように、個々の Meeting Server インスタンスにライセンスファイルをロードする必要はありません。

Cisco Meeting Server を設定する準備ができました。 ここから展開に適したガイドを参照してください:

- 単一統合サーバー導入ガイド（単一のホストサーバーに導入する場合）
- シングル分割サーバー導入ガイド（分割 Core/Edge 導入に導入する場合）
- スケーラビリティ & レジリエンスガイド（複数のサーバー（単一統合、または分割された Core または Edge サーバー）をクラスタ化して展開する場合）。

Cisco Meeting Server をシャットダウンするときは、vSphere 電源ボタンではなく、**shutdown** コマンドを必ず使用してください。

B.14.2 従来のライセンス方法を使用して Cisco ユーザーライセンスを取得する

このセクションは、すでに Meeting Server に必要なライセンスを Cisco パートナーから購入しており、PAK コードを受け取っていることを前提としています。

これらの手順に従い、Cisco ライセンス登録ポータルサイトを使用して、Meeting Server の MAC アドレスに PAK コードを登録します。

1. サーバーの MMP にログインして Meeting Server の MAC アドレスを取得し、MMP コマンド **`iface a`** を入力します。

   メモ: これは VM の MAC アドレスであり、VM がインストールされているサーバプラットフォームの MAC アドレスではありません。

   ---

2. Cisco ライセンス登録ポータルサイト を開き、Meeting Server の PAK コードと MAC アドレスを登録します。
3. PAK に R-CMS-K9 アクティベーション ライセンスがない場合、機能ライセンスに加えてこの PAK が必要になります。
4. ライセンスポータルからライセンスファイルの zip 圧縮されたコピーがメールで送信されます。Zip ファイルを解凍し、結果として得られた xxxxx.lic ファイルの名前を **`cms.lic`**。
5. SFTP クライアントを使用して Meeting Server にログインし、 **`cms.lic`** ファイルを Meeting Server ファイルシステムにコピーします。
6. MMP コマンドを使用して Call Bridge を再起動する **`callbridge restart`**
7. Call Bridge を再起動したら、MMP コマンドを入力してライセンスのステータスを確認します。
   `license`
   アクティブ化された機能と有効期限が表示されます。

付録 C ブランディング

Meeting Server で主催される参加者のミーティング体験の一部は、ブランド化することができます。これには次のような要素が含まれます。

- [セルフビュー] ペイン内のウェブアプリのサインイン背景画像、サインイン ロゴ、サインイン ロゴの下のテキスト、アイコン、カスタム仮想背景画像、およびブラウザー タブ上のテキスト
- IVR メッセージ
- SIP および Lync 参加者のスプラッシュ画面の画像、およびすべての音声プロンプト/メッセージ、
- ミーティング招待状のテキスト。

単一のリソース セットのみが指定された単一のブランドを適用する場合 (ウェブ アプリのサインイン ページ 1 つ、音声プロンプト 1 つ、招待テキスト 1 つ)、これらのリソースは展開内のすべてのスペース、IVR、およびウェブ ブリッジに使用されます。。 複数のブランディングにより、異なるスペース、IVR、ウェブ ブリッジに異なるリソースを使用できます。 リソースは、システム、テナント、スペース、または IVR レベルで、API を使用して割り当てることができます。

詳細については、 カスタマイズのガイドライン ブランディングの詳細については、を参照してください。

付録 D VM をサイジングする

Cisco Meeting Server は、柔軟性を最大限に高めるように設計されており、スケーラビリティに優れ、Cisco Meeting Server 2000、Cisco Meeting Server 1000、および VM の導入を「組み合わせる」ことができます。 例えば、VM をエッジサーバとして使用し、Cisco Meeting Server 2000 および Cisco Meeting Server 1000 をコアで拡張性の高い分散アーキテクチャに使用したり、標準化された単一サーバ上の VM 展開内のすべてのコンポーネントを配置したりします。

Cisco Meeting Server ソフトウェアが動作するさまざまな標準的なサーバーや仕様にも、最大限の柔軟性が引き継がれています。 付録 E では、最も一般的な仮想化技術の 1 つである VMware について詳細に説明します。 Cisco Meeting Server ソフトウェアは、例えば、ポータブルで堅牢なフォームファクターを必要とするアプリケーションなど、より特殊なサーバー上でも効果的に稼働します。

仮想マシン（VM）導入では、Cisco Meeting Server 全体または Cisco Meeting Server の個々のコンポーネントを実行できます。 例：

- 展開をテストする目的で、すべてのコンポーネントを単一の VM で実行できます。 図 5 を参照。

  注：運用中のネットワークでは、レコーダーとストリーマコンポーネントは、電話会議を主催するサーバーとは別の Meeting Server 上で有効にする必要があります。

- 単一の VM は、Cisco Meeting Server 2000 または Cisco Meeting Server 1000 に接続され、コアネットワークで Call Bridge を実行する TURN サーバーのエッジコンポーネントとして Web Bridge を実行できます。また、他のコアコンポーネントを実行する別の VM もあります。

  注：Cisco Expressway がネットワークのエッジで使用されている場合、VM 上の TURN サーバーコンポーネントを有効にする必要はありません。ウェブブリッジは、Call Bridge が電話会議をホストしている Meeting Server 上に存在する必要があります。

- 1 台の VM はエッジコンポーネントを実行し、2 台目の VM は Call Bridge とデータベースを実行し、3 台目の VM は他のコアコンポーネントを実行します。

図 5 は、1 台のサーバーで有効になっている Cisco Meeting Server のソフトウェアコンポーネントを示しています。 図 6 は、エッジサーバーとコアサーバに展開された Cisco Meeting Server のソフトウェアコンポーネントを示しています。

図 5：1 台のサーバーで有効にした Cisco Meeting Server ソフトウェアコンポーネント

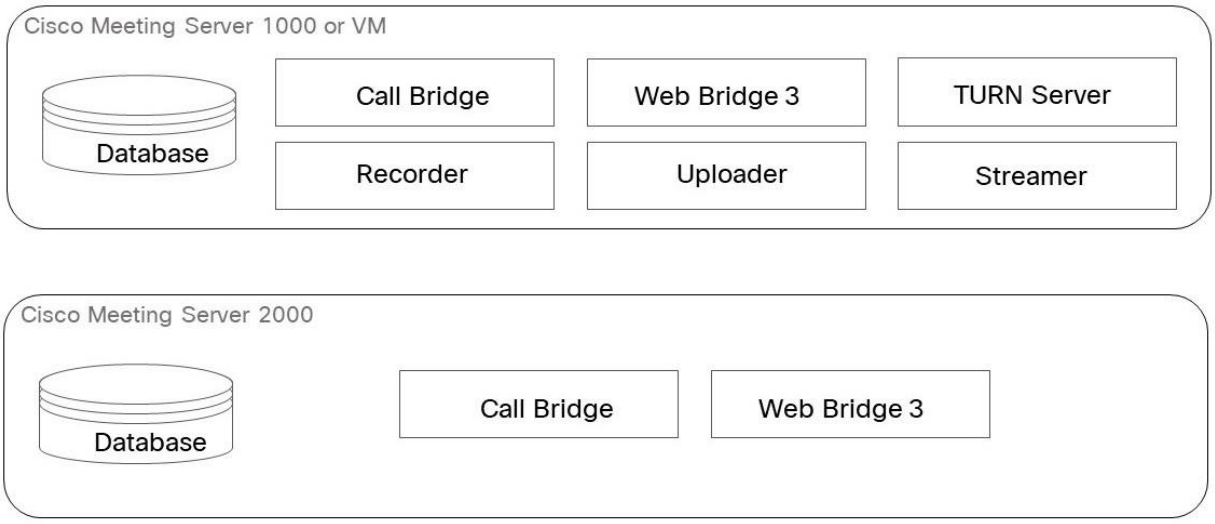
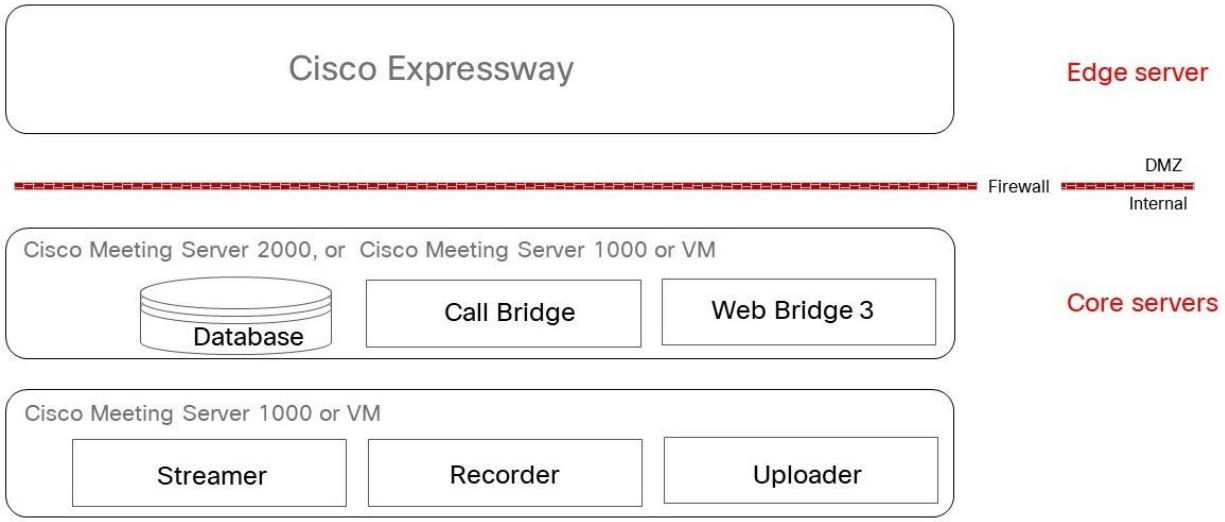


図 6：Cisco Meeting Server のソフトウェアコンポーネントとエッジにある TURN サーバーおよびウェブブリッジ 3



VM が 1 つまたは複数の Cisco Meeting Server コンポーネントを実行するように設定されている場合、Cisco はホスト全体を VM 専用として使用することを推奨しています。 これにより、リアルタイム メディア アプリケーションに最高のパフォーマンスが提供され、高品質のエンド ユーザー エクスペリエンスが保証されます。 VM のサイズは、使用されているコンポーネントによって異なります。

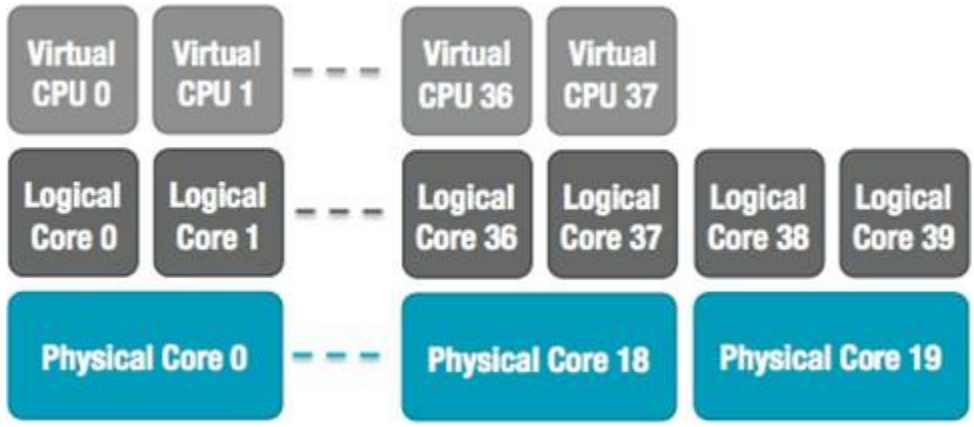
D.1 Call Bridge VM

Call Bridge は、Cisco Meeting Server のメディア トランスコーディングを実行します。このコンポーネントは、コンポーネントの中で最も高い要件があります。

2.5GHz で動作する Intel Xeon 2600 シリーズ（またはそれ以降）CPU の各物理コアは、ハイパースレッディングが有効な場合、約 2.5 720p30 H.264 コールレッグを処理できます。 容量は CPU コアの数と周波数に直線的にスケールするため、20 物理コアを持つ 2 ソケット E5-2680v2 システムは、50 の同時 720p30 H.264 コールレッグを処理できます。

ホスト物理コアのうち 1 つを除いて、VM はすべてを使用するように設定する必要があります。 ハイパースレッディングが有効な場合、利用可能な論理コアの数は物理コアの数の 2 倍であるため、上記のデュアル E5-2680v2 システムでは 40 個の仮想 CPU があり、そのうち 38 個を VM に割り当てる必要があります。 基になるハードウェアをミラーリングするソケットの数を設定することをお勧めします。

図 7: デュアル E5-2680v2 ホストへの仮想 CPU コア割り当て



ホストのオーバーサブスクリプションは、Cisco Meeting Server VM の仮想 CPU の数を誤って設定するか、VM 間で CPU リソースを競合することにより、スケジューリングの遅延を引き起こし、メディア品質が低下します。 物理コアの数を超える vCPU の数を割り当てることは、CPU リソースのオーバーコミットメントとなります。 この CPU のオーバーコミットは、VM CPU 使用率の統計に歪みをもたらし、CPU 準備完了時間が長くなります。 CPU の割り当てはワークロード固有の考慮事項であるため、より一般的なアドバイスと競合する場合があります。 この vCPU の割り当ては、Cisco Meeting Server に対して意図的なものであり、主催者から最高のパフォーマンスを抽出するための経験的テストの結果です。 上記の推奨に従って正しく設定された Cisco Meeting Server VM は、キャパシティを超えた場合にフレームレートおよび/または解像度をドロップすることにより、スムーズに性能を下げます。

基礎となる各物理 CPU コアの 1 GB RAM は、RAM の最小割り当ては 4GB で VM に割り当てる必要があります。 上記のシステムでは、VM は使用中の 19 個の物理 CPU コアに対応する 19GB で構成する必要があります。

Call Bridge 仮想マシンの RAM 要件は、vCPU あたり 1GB で、最低 4GB の RAM が必要ですが、推奨される最小値は 8GB です。 75,000 cospace を超える導入で cospace のスケールを増やすには、すべての Call Bridge とデータベース仮想マシンで、100,000 cospaceあたり 1GB の追加の RAM が必要です。 上記の Call Bridge 仮想マシンの例では、50 HD ポートと 275,000 ポートをサポートするために、cospace に 50 HD ポート数をサポートするには 38GB の RAM が必要で、さらに 75,000 を超える cospace には 200,000 ポート数をサポートするために 2GB が必要です。

D.2 ウェブエッジ仮想マシン

Expressway (Large OVA または CE1200) は、中規模のウェブ アプリのスケール要件を持つ展開 (つまり、800 コール以下) に推奨されるソリューションです。 Expressway (Medium OVA) は、小規模なウェブ アプリ スケール要件を持つ展開 (つまり、200 コール以下) に推奨されるソリューションです。 しかし、より大きなウェブ アプリ スケールを必要とする展開では、バージョン 3.1 から、必須のソリューションとして Cisco Meeting Server ウェブ エッジを推奨します。

D.2.1 エッジサーバーの設定

エッジ サーバ ロールでは、2 つの仮想マシン ハードウェア構成がサポートされます。 これらの設定は、サポートされる最小ハードウェア要件と能力を定義します。

「小規模」エッジサーバ

1 x Cisco Meeting Server VM、サポート対象 Cisco ハードウェアのための次の仕様

- 4 GB RAM
- 4 vCPU
- 1Gbps ネットワークインタフェース

「大型の」エッジサーバー

1 x Cisco Meeting Server VM、サポート対象 Cisco ハードウェアのための次の仕様

- 8 GB RAM
- 16 vCPU
- 10Gbps ネットワークインタフェース

推奨プロセッサ仕様:

2.5GHz 以上で動作する Intel Xeon E5 2600 などのプロセッサ仕様を推奨します。 1 vCPU 対 1 物理 CPU を推奨します。

NIC 要件:

Cisco は、TURN Server に単一の NIC 構成を使用する分割サーバ展開をテストおよび検証しました。 そのため、バージョン 3.0 から、1 つのインターフェイスでのみ TURN Server のリスニングポートを設定することをお勧めします。

共存サポート:

Edge サーバーは他の VM と共存できます。 ただし、各 4 vCPU VM には 1 Gbps NIC 要件があり、16 vCPU には 10Gbps NIC 要件があります。 VM ホストは、すべてのアプリケーションに対して十分な NIC 容量を必要とします。

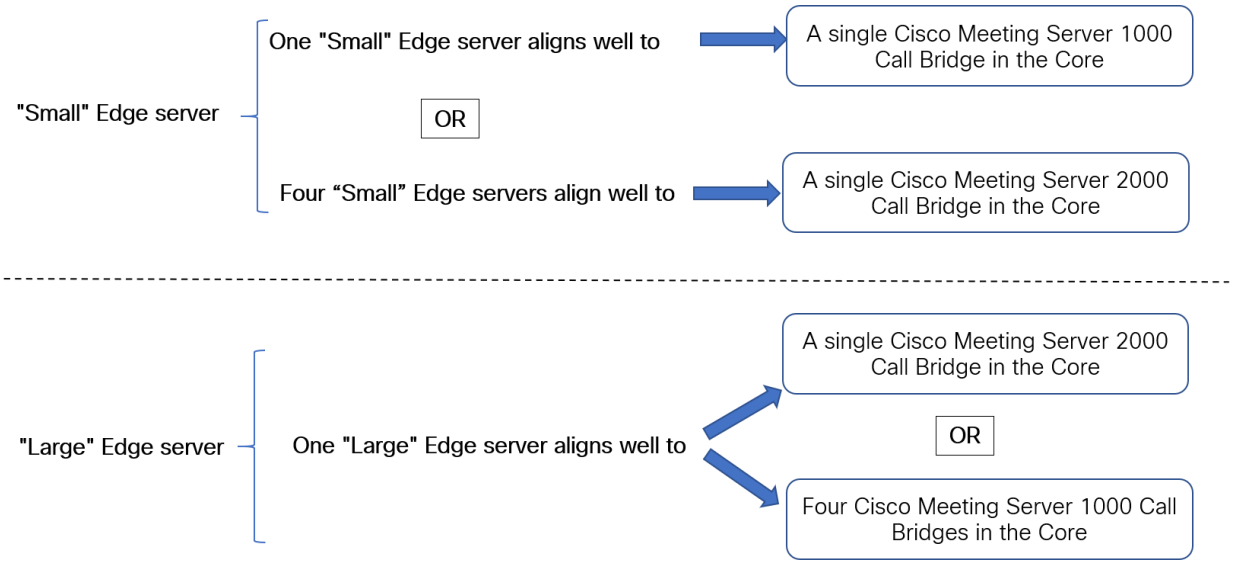
注：

- Meeting Server 1000 M4 ハードウェアは 1Gbps NIC をサポートします。 Meeting Server M5 以降のハードウェアは 10Gbps NIC をサポートします。

表 8：Edge Server ウェブアプリのコールキャパシティ

通話のタイプ	**小規模** Edge VM **コールキャパシティ**	**大規模** Edge VM **コールキャパシティ**
フル HD コール 1080p30 ビデオ	100	350
HD 通話 720p30 ビデオ	175	700
SD 通話 448p30 ビデオ	250	1000
音声通話（G.711）	850	3000

2 台の Edge サーバ設定は、Call Bridge に Cisco Meeting Server アプライアンスを使用する場合に、Edge の容量とコア Call Bridge の容量を簡単に一致させる容量を提供します。



コア Call Bridge がサポートする Call Bridge コールキャパシティ、および使用されている Edge サーバーハードウェア設定を確認して、必要な Edge サーバーの数を決定します。

D.2.2 展開の考慮事項

- 同じ Call Bridge または Call Bridge グループにサービスを提供するすべてのエッジサーバーは、同じ性能、つまり、4 つの vCPU すべてまたは 16 個の vCPU であり、両方の混在ではないものにすることを推奨します。
- スケーラブルまたは復元力のある展開の場合、Call Bridge グループを設定することを推奨します。 これにより、TURN サーバーの一意のグループを各 Call Bridge グループに割り当てることができます。これは、ロードバランシングを支援し、TURN サーバーと Call Bridge の地理的位置を適切に維持するのに役立ちます。
- ウェブアプリが SIP スケール（クラスターごとに最大 24 Call Bridges）に一致するように、複数のエッジサーバーをサポートします。 ただし、Call Bridge グループは、グループごとに最大 10 台のエッジサーバーのみをサポートします。 10 を超えるエッジサーバーを必要とするスケーラブルまたはレジリエントな導入の場合、複数の Call Bridge グループが必要になります。
- Meeting Server のエッジソリューションをサポートするために、TURN スケーラビリティモードを有効にする新しい MMP コマンド **`turn highcapacity-mode (enable|disable)`** が導入されました。 この設定はデフォルトでは有効になっています。

Cisco Meeting Server ウェブエッジソリューションの展開の詳細については、『導入ガイド（バージョン 3.1 以降）』を参照してください。

D.3 データベース仮想マシン

メモ: このセクションは、1 つまたは複数の外部データベースの使用を選択した場合にのみ適用されます。

データベースのホストサーバーの CPU 要件は中程度ですが、大きなストレージとメモリを必要とします。 適格な VM ホストを必須にするものではありませんが、以下を推奨します。

- 8 vCPU、8GB[1] RAM、100GB データストア

  (OVF はこれらのパラメータに設定されるため、これらは展開後のデフォルトになります)
- Sandy Bridge (またはそれ以降) クラスの Intel プロセッサ (例: E5-2670 または E5-2680 v2)
- データストアは、高 IO/秒 SAN またはローカル SSD ストレージのいずれかに存在する必要があります
- データは、OS と同じ仮想ディスク上にある必要があります。

Cisco Meeting Server 1000 のホストとして現在使用されている Cisco UCS C220 を使用できますが、VM データベースはサーバーリソースのわずかな割合しか使用しません。 必要に応じて、このサーバーを使用して、他の VM を VM データベースと同じサーバーでホストすることもできます。

1データベース VM の RAM の要件は、8GB に加えて、75,000 cospaces を超える部分については、100,000 cospaces ごとに 1GB の RAM が必要です。 たとえば、375k cospaces をサポートする導入のデータベース VM では、75,000 cospaces を超える部分の 300,000 cospaces をサポートするために、8GB の最小 RAM 要件に加えて 3GB の RAM が必要になります。

D.4 レコーダーとストリーマ VM

注：新しい内部 SIP レコーダーおよびストリーマサービスは、外部の録画またはストリーミングサービスとして使用できません。これらのサービスは、Meeting Server Call Bridge から渡される特定の SIP ヘッダーパラメータに依存しています。 Meeting Server コールブリッジ以外の任意のソースからの通話が接続すると、レコーダー/ストリーマは特定の SIP ヘッダーを見つけられないため、通話を拒否します。

D.4.1 新しい内部 SIP レコーダーコンポーネントの VM のサイジング

レコーダーの本番環境での使用で推奨される展開は、最小で 4 つの vCPU コアと 4GB の RAM を備えた専用 VM で実行することです。 各録画タイプのパフォーマンスとリソース使用率を次の表に示します。

表 9: 内部 SIP レコーダーのパフォーマンスとリソース使用率

録画設定	vCPU あたりの録画数	1 回の録画で必要な RAM	時間あたりのディスクバジェット	最大同時録画
720p	2	0.5GB	1GB	40
1080p	1	1GB	2GB	20
音声	16	100MB	150MB	100

注意すべき重要なポイント (新しい内部レコーダーコンポーネントにのみ適用されます):

- パフォーマンスは、vCPU を追加すると、最大でホストの物理コアの数まで直線的に増加します。

D.4.2 新しい内部 SIP ストリーマ コンポーネントの仮想マシンのサイジング

ストリーマを本番環境で使用する場合に推奨される展開は、最低 4 つの vCPU コアと 4 GB の RAM を備えた専用 VM で実行することです。 次の表は、推奨される 3 つの最小仕様とそれらが処理できるストリーム数を示しています。

表 10: 内部 SIP ストリーマの推奨仕様

vCPU の数	RAM	720p ストリーム数	1080p ストリーム数	音声のみのストリーム数
4	4GB	50	37	100
4	8GB	100	75	200
8	8GB	200	150	200

注意すべき重要なポイント (新しい内部ストリーマコンポーネントにのみ適用されます):

- vCPU の数は、物理コアの数を超過してはならない。
- サポートされている 720p ストリームの最大数は、vCPU の追加に関係なく、200 です。
- サポートされる 1080p ストリームの最大数は、vCPU の追加に関係なく、150 です。
- サポートされる音声のみのストリームの最大数は、vCPU の追加に関係なく、200 です。

D.5 ウェブスケジューラ

スケジューラは、エンドユーザーがウェブアプリ経由でミーティングをスケジュールできるようにする Meeting Server コンポーネントです。 Meeting Server 1000、Meeting Server 2000、および VM 導入上の Meeting Server でサポートされています。 スペックベースの VM プラットフォーム上の Meeting Server では、スケジューラコンポーネントを実行するために、追加で 4 GB の RAM が必要です。 Meeting Server 1000 および Meeting Server 2000 には、追加 RAM 要件はありません。スケジューラは、SMTP メールサーバーの設定により、メール通知の送信をサポートします。 メールサーバー設定の詳細については、Cisco Meeting Server 設置ガイドを参照してください。

1 つのスケジューラが 150,000 件のミーティングをサポートします。2 つまたは 3 つのスケジューラを追加してレジリエンスを提供できますが、定員は 150,000 件のスケジュールされたミーティングのままです。 スケジュール済みミーティングのデータは Meeting Server のデータベースに保存され、クラスター化およびシングルボックスデータベース導入の両方がサポートされています。

スケジューラは、Meeting Server MMP を使用して、新しいコンポーネントとして導入されます。 スケジューラが有効になると、スケジューラはループバック インターフェイスを介して Call Bridge に API 要求を行います。 そのため、スケジューラは、Call Bridge もホストしている Meeting Server に導入する必要があります。 スケジューラがリモート Call Bridge を使用するように設定することはできません。 スケジューラの導入方法の詳細については、『Cisco Meeting Server 導入ガイド』を参照してください。

D.6 ミーティングアプリ

ファイル共有やアンケートなどのウェブアプリ機能は、MeetingApps サービスで導入されます。MeetingApps は、他のサービスなしでスタンドアロンの Meeting Server ノードで設定する必要があります。 参加者が外部または内部ネットワークのどちらから参加しているかに応じて、MeetingApps を DMZ ネットワークまたは内部ネットワークで設定できます。

MeetingApps サービスは、Meeting Server 2000 では設定できません。MeetingApps は、Meeting Server の仕様ベースの仮想化導入でのみ設定することをお勧めします。 ただし、以下の仕様の VM 導入では、ミーティングアプリと共に Meeting Server 2000 または Meeting Server 1000 を Call Bridge またはウェブブリッジとして使用できます。

vCPU の数	RAM	ディスク容量
8	16 GB	100 GB

MMP コマンド **meetingapps** を使用して、Meeting Server の VM 導入で MeetingApps を設定できます。

付録 E VMware に関する追加情報

E.1 VMware

コア VM はホスト全体を使用するように設定する必要があります。 これにより、ESXi カーネルが管理およびネットワーク操作を実行するために CPU コアが利用できるようになります。

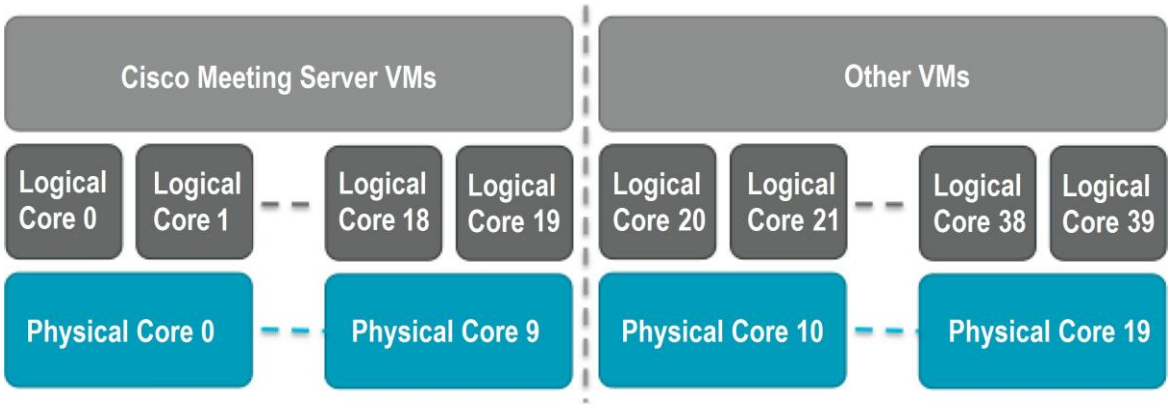
内部テストの一環として、さまざまな CPU とサーバ構成のベンチマークを定期的に実施しています。 これらのテスト中、時間の経過とともに合成呼び出しが追加され、VM への要求が徐々に増加し、キャパシティを超えるように押し上げます。 ユーザエクスペリエンスの質を保証するために、いくつかの内部統計が監視されます。 さらに、ESXi 統計が監視され、診断ログが収集されます。

推奨はしませんが、競合を防ぐために CPU アイソレーションドメインが作成されている限り、Cisco Meeting Server VM と一緒に他の VM を実行することは可能です。 この技術は「アンチピニング」と呼ばれ、すべての VM をコアのサブセットに明示的にピニングします。 Cisco Meeting Server VM は、そのコアにピン留めされた唯一の VM である必要があり、他のすべての VM は、他のコアに明示的にピン留めされる必要があります。

たとえば、20 コア デュアル E5-2680v2 ホストが利用できるが、25 個の同時 720p30 コール レッグしか必要ない場合、アンチピニングを使用できます。 2.5 コール/コアの比率を使用すると、この容量を提供するには 10 個の物理コアが必要です。 10 コアは他のタスクに使用できます。

ハイパースレッディングを有効にすると、40 の論理コアが利用可能になり、ESXi はこれらの論理コアにインデックス 0-39 のラベルを付けます。 Cisco Meeting Server VM には 20 個の仮想 CPU が割り当てられ、アフィニティ 0-19 のスケジュールで設定されている必要があります。 ホストで実行されている他のすべての VM は、隔離ドメインのペアを作成するために、アフィニティ 20-39 で明示的に構成する必要があります。 ESXi ハイパーバイザー用に、VM が無い物理コアを固定しておくことが必要な場合もあります。

図 8: ピン留めによって作成された VM 分離ドメイン



VMXNet3 仮想ネットワークアダプタは、他のアダプタタイプよりも必要なオーバーヘッドが小さいため、好まれます。 すべての仮想ネットワークアダプタは同じタイプである必要があります。

VMware Fault Tolerance (FT) は、シングル仮想コア VM に制限されているため、サポートされていません。 VMware vCenter Operations Manager などの高レベルのツールは完全にサポートされています。

注：VMWare ハイパーバイザーを使用して EVC モードを有効にする場合、EVC を次のいずれかまたはそれ以上のモードに設定する必要があります。

“B1”/AMD Opteron™ Generation 4
“L2”/Intel® Nehalem 世代（以前の Intel® Xeon Core™ i7）

上記にリストされているものより古い CPU との互換性を強制する EVC モードは、SSE 4.2 が無効になるため、サポートされません。SSE4.2 が必要です。

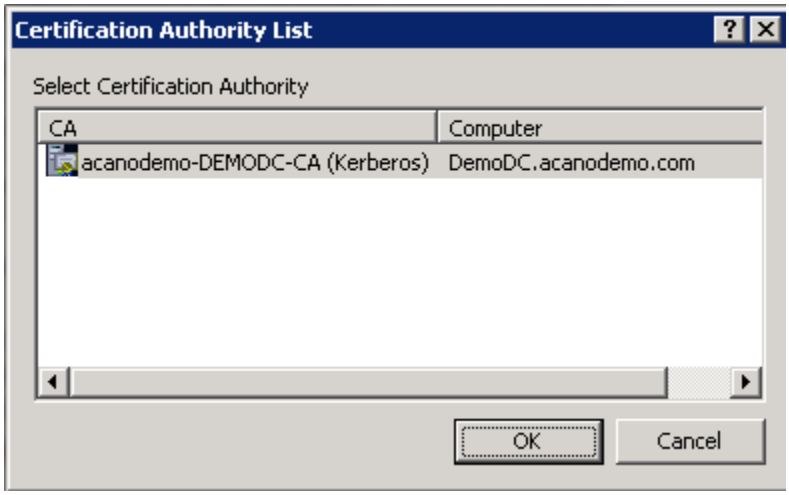
付録 F ローカルの Certificate Authority によって署名された証明書を作成する

この付録では、Active Directory 証明書サービスの役割がインストールされた Microsoft Active Directory サーバなどのローカル CA を使用して、CSR に署名する手順について説明します。

1. ファイルを CA に転送します。
2. CA サーバーのコマンドライン管理シェルで以下のコマンドを発行し、パスと CSR 名をお客様の情報に置き換えます。

   ```
   certreq -submit -attrib "CertificateTemplate:WebServer"
   C:\Users\Administrator\Desktop\webadmin.csr
   ```

3. コマンドを入力すると、次のような CA 選択リストが表示されます。 正しい CA を選択し、[OK] をクリックします。

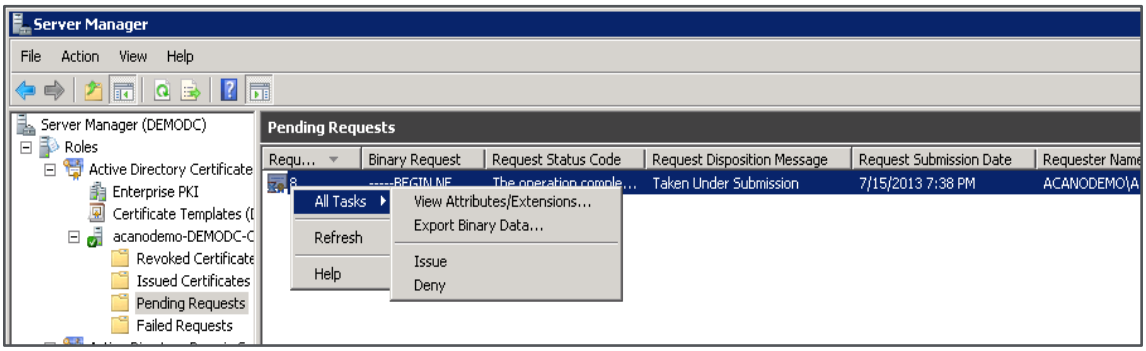


4. 次のいずれかを実行します。
   - Windows アカウントに証明書を発行する権限がある場合、生成された証明書を webadmin.crt などとして保存するように指示されます。 下記の手順 c に進みます。
   - 生成された証明書を発行するプロンプトが表示されず、代わりにコマンドプロンプトウィンドウに、「証明書の要求が保留中: 取得済み、送信中」というメッセージが表示され、次のように要求 ID がリストされている場合は、 RequestID をメモし、次の手順を実行してから手順 c に進みます。

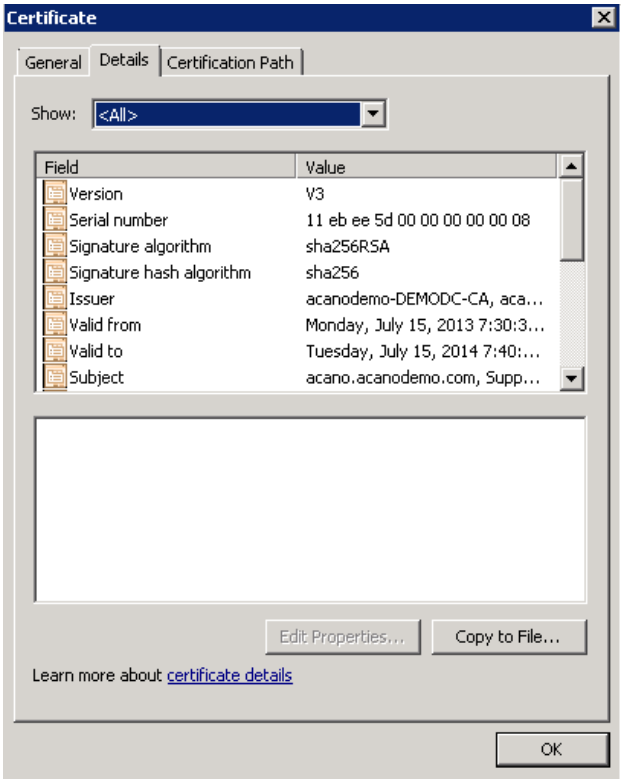
```
C:\Users\Administrator>certreq -submit -attrib "CertificateTemplate:WebServer" C
:\Users\Administrator\Desktop\demokitcsr.pem
Active Directory Enrollment Policy
  {0BD5D0B7-591F-4C77-AFEC-3C0E470F77D5}
  ldap:
RequestId: 8
RequestId: "8"
Certificate request is pending: Taken Under Submission (0)

C:\Users\Administrator>_
```

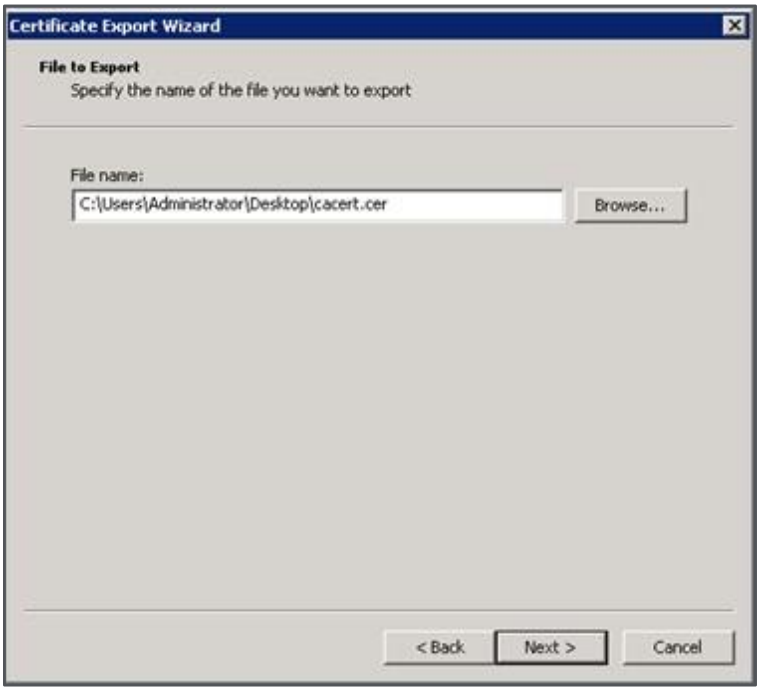
5. CA の [サーバ マネージャ] ページを使用して、[CA ロール] の下の [保留中のリクエスト] フォルダを見つけます。
6. [CMD] ウィンドウに表示されたリクエスト ID に一致する保留中のリクエストを右クリックし、[ ] > [**すべてのタスク**] **を選択します。** の問題。



7. 結果として署名された証明書は、[発行された証明書] フォルダーにあります。 証明書をダブルクリックして開き、[**詳細**] タブを開きます (右を参照)。



8. [**ファイルにコピー**] をクリックして、証明書のエクスポートウィザードを開始します。
9. [Base-64 エンコード X.509 (.CER)] を選択して [**次へ**] をクリックします。
10. 証明書を保存する場所を参照し、 **webadmin** などの名前を入力して、[**次へ**] をクリックします。



11. 作成された証明書の名前を **`webadmin.crt`** に変更します。

SFTP を使用して、証明書（例：webadmin.crt）と秘密キーを Cisco Meeting Server の MMP に転送します。 セクション 3.5.2 を参照してください。

注意: ウェブ登録機能がインストールされた CA を使用している場合は、BEGIN CERTIFICATE REQUEST および END CERTIFICATE REQUEST の行を含む CSR テキストをコピーして送信することができます。 証明書が発行されたら、証明書のみをコピーし、証明書チェーンはコピーしません。 BEGIN CERTIFICATE および END CERTIFICATE の行を含むすべてのテキストを含めて、テキストファイルに貼り付けてください。 .crt、.cer または .pem の拡張子を持つ証明書としてファイルを保存します。

Cisco 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。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。 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、シスコシステムズ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システムズ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。

★定型★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。 ★定型★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。

この文書の印刷されたハード コピーおよび複製されたソフト コピーは、すべて管理対象外と見なされます。 最新版については、現在のオンライン バージョン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。 各オフィスの住所と電話番号は、当社の Web サイト www.cisco.com/go/offices. をご覧ください。

Cisco の商標または登録商標