Cisco TelePresence Content Server Release 7.0 クイック スタート ガイド

2016 年 8 月

このマニュアルには、Cisco TelePresence Content Server Release 7.0 のインストールと設定についての情報が含まれます。次の項を参照してください。

- 製品の概要（2 ページ）
- 技術仕様（5 ページ）
- ハードウェアおよびソフトウェアの制限（5 ページ）
- Content Server の設置（5 ページ）
- 初期設定の完了（6 ページ）
  - タスク 1：Content Server を接続して電源を入れ、CIMC を設定する（7 ページ）
  - タスク 2：ローカル管理者パスワードを設定する（7 ページ）
  - タスク 3：Windows Server 2012 アクティベーション キーを入力する
  - タスク 4：スタティック IP アドレスを設定する（9 ページ）
  - タスク 5：日時を設定する（9 ページ）
  - タスク 6：リモート デスクトップ接続を有効化する（9 ページ）
  - タスク 7：SQL を設定する
  - タスク 8：セキュリティ証明書をインストールする
  - タスク 9：H.323/SIP 登録設定を行う
  - タスク 10：テスト録画を実行する
- 追加 Content Server 設定（13 ページ）
- トラブルシューティングおよびテクニカル サポート（15 ページ）
- 関連資料（16 ページ）
- マニュアルに関するフィードバックの提出（16 ページ）
- マニュアルの入手方法およびテクニカル サポート（16 ページ）

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

製品の概要

Cisco TelePresence Content Server を使用すると、ビデオ会議を録画して知識を共有し、コミュニケーションを強化することができます。ライブおよびオンデマンドのプレゼンテーションにいつでもどこからでもアクセスできます。さらに、ライブや録画済みのコンテンツを任意のコンピュータに配信したり、自分の好きなポータブル メディア デバイスにダウンロードしたりできます。

このリリースでは、Cisco Content Server Release 7.0 ソフトウェアが稼働する第 4 世代 Content Server のハードウェアを導入します。第 4 世代 Content Server は、Cisco UCS C220 M4 サーバに基づいています（詳細については、Cisco.com で『*Cisco UCS C220 サーバInstallation and Service Guide*』を参照してください）。

図 1 および図 2 に、Content Server の前面パネルおよび背面パネルを示し、表 1 ではサーバの機能について説明します。

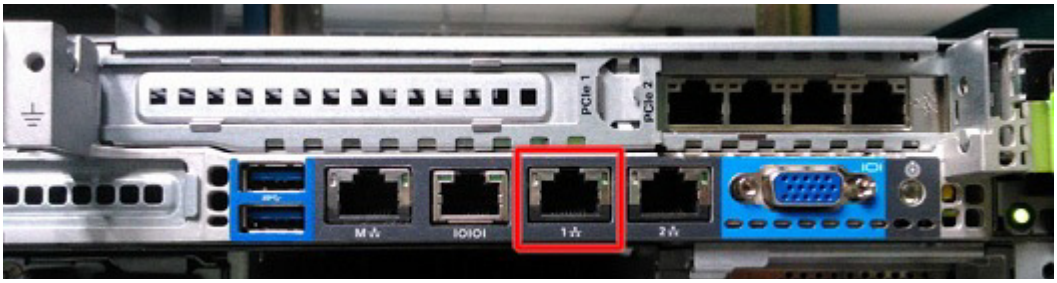
図 1　　Content Server の前面パネル

1	電源ボタン/電源ステータス LED	**6**	電源装置ステータス LED
2	ID ボタン/LED	**7**	ネットワーク リンク アクティビティ LED
3	システム ステータス LED	**8**	資産タグ（シリアル番号）
4	ファン ステータス LED	**9**	KVM[1] コネクタ：**初期設定では、このポートを使用します**
5	温度ステータス LED	**10**	ホットスワップ可能ハード ドライブ（2）（スロット 1 と 2 に 2.5 インチ ドライブを設置、スロット 3 ～ 8 は空）

1. KVM = キーボード、ビデオ、およびマウス

図 2　　Content Server の背面パネル:USB ポート

図 3　　Content Server の背面パネル:LOM ポート



1	電源(2 台)	**6**	1 Gb イーサネット専用管理ポート(図 4 も参照)
2	ライザー上のロープロファイル PCIe スロット 2 (ハーフハイト、ハーフレングス、x8 レーン)	**7**	デュアル 1 Gb イーサネット ポート: LAN1(矢印 7、左のポインタ):**Content Server をネットワークに接続するときは、このポートを使用します**(図 4 を参照) LAN2(矢印 7、右のポインタ):**使用しません**
3	ライザー(フルハイト、ハーフレングス、x16 レーン)標準プロファイル PCIe スロット	**8**	USB ポート(2 個)
4	VGA ビデオ コネクタ	**9**	ID ボタン/LED
5	シリアル ポート(RJ-45 コネクタ):**使用しません**		–

表 1　　Content Server の機能

シャーシ	1 ラック ユニット(1RU)シャーシ 4.32 x 43 x 72.4 cm(1.7 x 16.9 x 28.5 インチ)
プロセッサ	Intel Xeon E5-2665 プロセッサ X 2
メモリ	DDR3[1] による 8 GB の低電圧 DIMM 4 個により、合計 32 GB のメモリを搭載。

表 1　　Content Server の機能 （続き）

ベースボード管理	Cisco Integrated Management Controller（CIMC）ファームウェアを実行する統合 Emulex Pilot-3 ベースボード管理コントローラ（BMC）。 管理および制御に対応した IPMI 2.0。 10/100/1000 イーサネット アウトオブバンド管理インターフェイスを 1 個搭載。 自動化した停電時管理を可能にする CLI および Web GUI による管理ツール。 CIMC 設定に応じて、CIMC には 1 Gb イーサネット専用管理ポートまたは デュアル 1 Gb イーサネット LOM ポートを介してアクセスできます。
ネットワークおよび管理 I/O	このアプライアンスは、背面パネルに次のコネクタを備えています。 1 Gb イーサネット専用管理ポート x 1 1 Gb Base-T イーサネット ポート x 2 RS-232 シリアル ポート（RJ-45 コネクタ）x 1 15 ピン VGA コネクタ x 1 USB 2.0 コネクタ x 2 USB 2 個、VGA 1 個、シリアル コネクタ 1 個を装備した付属 KVM ケーブルを使用する前面パネル KVM コネクタ x 1
前面パネル ロケータ LED	データセンター環境で特定のアプライアンスを直接管理する際に効果的なインジケータ ライトx 1。
電源	最大 2 台の電源装置、各 650 W。 1+1 の冗長構成（冗長構成時にホットプラグ可能）。
冷却装置	ホットプラグ可能なファン モジュール（前面から背面に向かう冷却用）x 5。
PCIe I/O	ライザー上に設けた 2 個の第 3 世代 PCIe[2] 拡張スロットに、RAID[3] カード（SuperCap 電源モジュールによる RAID バックアップ ユニットを備えた LSI MegaRAID SAS9266-8i。RAID-5 を設定）および NIC[4] カード（Broadcom 5709 クアッド ポート 1 Gb イーサネット）を装備しています。 **コメント**　Content Server はデュアル NIC 設定をサポートしません。
ストレージ	ドライブは、ホットプラグ操作可能な、前面パネルのドライブ ベイに取り付けられます。小型フォーム ファクタ：アプライアンスは、2.5 インチ x .55 インチ（63.5 mm x 14mm）の SAS[5] または SATA[6] のハード ドライブまたはソリッド ステート ドライブを 8 台まで収容できます。アプライアンスは、2 つのドライブが取り付けられた状態で出荷されます。 ハード ディスクのオプション：10,000 RPM で動作する 2.5 インチ、600 GB SAS ハード ドライブ。
ディスク管理（RAID）	LSI MegaRAID 9266-8i（RAID 1）
RAID バックアップ	LSI MegaRAID カードには、LSI バッテリ バックアップ ユニットが使用されています。
ビデオ	60 Hz での最大 1600 x 1200、16 bpp の解像度。最大 256 MB のビデオ メモリ。

1. DDR3 = ダブル データ レート、タイプ 3
2. PCIe = Peripheral Component Interconnect Express
3. RAID = Redundant Array of Independent Disks
4. NIC = ネットワーク インターフェイス カード
5. SAS = Serial Attached SCSI（シリアル接続 SCSI）
6. SATA = Serial Advanced Technology Attachment（シリアル ATA）

技術仕様

Content Server の環境仕様と適合規格は、次の URL の製品データ シートに記載されています。
http://www.cisco.com/en/US/products/ps11347/products_data_sheets_list.html

サポートされるハードウェア

第 4 世代（M4 ハードウェア）

- **UCS C220 M4**
- **Intel(R) Xeon(R) E5-2680 v3 CPU @2.50GHz 24 コア**
- **64 GB RAM**

コメント　このハードウェア仕様は M4 ハードウェアの TCS 7.0 アプライアンス用です。TCS 7.0 アプライアンスは、第 3 世代のハードウェアではサポートされません。

TCS 7.0 VM は第 3 世代、第 4 世代、およびサードパーティ製ハードウェアでサポートされます。

ハードウェアおよびソフトウェアの制限

以下に、ソフトウェアとハードウェアの制限を示します。

- TCS 7.0 では、Windows Server 2012 が Windows Media ストリーミング サーバをサポートしないため、オンボックス ストリーミング サーバはありません。ライブ ストリーミングの場合、TCS は外部ストリーミング サーバとともに設定する必要があります。
- TCS 7.0 ソフトウェアは、第 1、第 2、または第 3 世代の Content Server ハードウェアにインストールできません。7.0 のインストーラを実行しようとすると、失敗します。
- TCS 7.0 では、クラスタ内の第 4 世代の Content Server はすべて同じハードウェア バージョンである必要があります。クラスタ内で、古い（第 1、第 2、または第 3 世代）サーバを第 4 世代の Content Server と混在させることはできません。
- USB メディア キットは、第 4 世代 Content Server のソフトウェア再イメージ化にのみ使用されます。第 1、第 2、または第 3 世代サーバ ハードウェア上のソフトウェアのアップグレードには、USB ドライブを使用できません。

Content Server の設置

インストール情報については、次のセクションを参照してください。

- サイト要件および安全性情報（6 ページ）
- 輸送用カートンの内容（6 ページ）
- ラック取り付け（6 ページ）

サイト要件および安全性情報

Cisco.com の『*Cisco UCS C220 Server Installation and Service Guide*』に記載されている要件を満たす設置場所を選択して準備します。

法令準拠と安全性に関する詳しい情報については、Cisco.com の『*Regulatory Compliance and Safety Information for the Cisco UCS C-Series Servers*』を参照してください。

輸送用カートンの内容

サーバを受け取ったら、設置に必要なすべての項目があるかどうか、輸送用カートンの内容を確認してください。サーバを再梱包する場合に備えて、梱包材を保管しておきます。欠品または損傷品が見つかった場合は、製品の購入代理店まで問い合わせてください。

輸送用カートンには、次のものが含まれています。

- Content Server
- USB メディア キット（ソフトウェア再イメージ化のみに使用）
- レール キット
- シリアル ケーブル
- イーサネット ケーブル
- ケーブル キットの電源
- アクセサリ キット
- 製品マニュアルの URL および中国の RoHS 情報を記したカード

ラック取り付け

Content Server のラック取り付け手順については、『*Cisco UCS C220 Server Installation and Service Guide*』の「Installing the Server」の章を参照してください。

初期設定の完了

Content Server の初期設定を完了するには、以下のものが必要です。

- USB キーボード、マウス、および VGA モニタ。
- Windows Server 2012 製品アクティベーション キー：Content Server のシャーシの製品アクティベーション キー ラベルを参照してください。
- 次の IP アドレス、サブネット マスク、およびゲートウェイ：
  - Content Server
  - Cisco Integrated Management Controller（CIMC）設定ユーティリティ

これらは初期設定タスクです。

- タスク 1：Content Server を接続して電源を入れ、CIMC を設定する（7 ページ）
- タスク 2：ローカル管理者パスワードを設定する（7 ページ）
- タスク 3：Windows Server 2012 アクティベーション キーを入力する（8 ページ）

- タスク 4:スタティック IP アドレスを設定する(9 ページ)
- タスク 5:日時を設定する(9 ページ)
- タスク 6:リモート デスクトップ接続を有効化する(9 ページ)
- タスク 7:SQL を設定する(10 ページ)
- タスク 8:セキュリティ証明書をインストールする(10 ページ)
- タスク 9:H.323/SIP 登録設定を行う(11 ページ)
- タスク 10:テスト録画を実行する(12 ページ)

タスク 1:Content Server を接続して電源を入れ、CIMC を設定する

次の手順に従ってください。

ステップ 1 付属の電源コードをサーバの各電源装置に接続し、次に、接地された AC 電源出力に接続します。最初のブート中、サーバがスタンバイ電源モードでブートするまでに約 2 分かかります。電源ステータスは、次のように電源ステータス LED で確認できます(図 1)。

- 消灯:サーバには AC 電力が供給されていません。
- オレンジ:サーバはスタンバイ電源モードです。CIMC と一部のマザーボード機能にだけ電力が供給されています。
- 緑:サーバは主電源モードです。すべてのサーバ コンポーネントに電力が供給されています。

ステップ 2 付属の KVM ケーブルを使用して、USB キーボード、マウス、および VGA モニタを Content Server の前面パネルの KVM コネクタに接続します(図 1)。

または、背面パネルの VGA および USB ポートを使用することもできます。ただし、前面パネルの VGA と背面パネルの VGA は同時に使用できません。同時に使用すると、最初の VGA コネクタが無効になります。

ステップ 3 電源ボタンを押して、サーバをブートします。ブートアップ時に、F8 を押して BIOS CIMC 設定ユーティリティを開きます。

ステップ 4 CIMC Configuration Utility で次の設定を入力します。

a. NIC プロパティ NIC モード:専用(Dedicated)

b. NIC の冗長性:なし(None)

c. IPv4(基本):*CIMP の IP アドレス、サブネット マスク、ゲートウェイ IP アドレス*

コメント Content Server はデュアル NIC 設定をサポートしません。

ステップ 5 **F10** を押して設定を保存し、Content Server を再起動します。

タスク 2:ローカル管理者パスワードを設定する

次の手順に従ってください。

ステップ 1 デフォルト パスワード **Cisco123** を使用して Content Server の Windows Server Manager にログインします。

ステップ 2 [スタート(Start)] > [コントロール パネル(Control Panel)] >[ユーザー アカウント(User Accounts)] > [Windows パスワードの変更(Change your Windows password)] > [パスワードの変更(Change your password)] に移動します。

ステップ 3 [パスワードの変更(Change your password)] ウィンドウでは、現在のパスワード(**Cisco123**)と新しいパスワードを入力し、新しいパスワードを確認します。

ステップ 4 [パスワード変更(Change Password)] をクリックします。

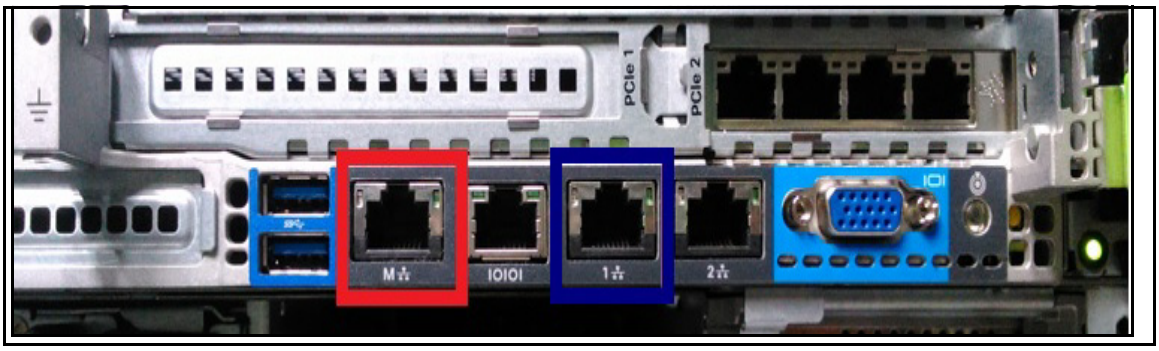
ステップ 5 [OK] をクリックします。

タスク 3:Windows Server 2012 アクティベーション キーを入力する

Windows Server 2012 の物理キーは、Content Server の前面の近くの上部に印刷されたラベル上にあります。Windows Server 2012 オンライン アクティベーション サービスにアクセスするには、インターネット接続が必要です。次の手順に従ってください。

ステップ 1 Content Server をネットワークに接続します。イーサネット ケーブルを使用して、LAN から背面パネルの LAN1 ネットワーク ポート(図 4 で青色のマーク)に接続します。CIMC 管理接続には、赤でマークされたコネクタを使用します。

図 4 ネットワーク接続



ステップ 2 タスク 2:ローカル管理者パスワードを設定するで設定したパスワードを使用して、Content Server の Windows Server Manager にログインします。

ステップ 3 [スタート(Start)] > [管理ツール(Administrative Tools)] > [サーバー マネージャー(Server Manager)] に移動します。[サーバー マネージャー(Server Manager)] ウィンドウで、[Windows のライセンス認証(Activate Windows)] をクリックします。**物理キー**(Content Server のシャーシ ラベルにあります)を入力します。[Next] をクリックします。

Content Server がインターネットに接続されていない場合は、画面の指示に従い、電話を使用して Windows Server 2012 をライセンス認証できます。

ステップ 4 プロダクト キーを確認してライセンス認証したら、[閉じる(Close)] をクリックします。

タスク 4: スタティック IP アドレスを設定する

デフォルトでは、サーバは、ネットワーク内の DHCP サーバによって割り当てられた IP アドレスを自動的に取得します。IP アドレスを、DHCP からスタティックに変更することを推奨します。次の手順に従ってください。

ステップ 1 [スタート(Start)] > [コントロール パネル(Control Panel)] > [ネットワークとインターネット(Network and Internet)] に移動します。

ステップ 2 [ネットワークと共有センター(Network and Sharing Center)] で、[ネットワークの状態とタスクの表示(View network status and tasks)] をクリックします。

ステップ 3 [接続または切断(Connect or disconnect)] セクションで、[ローカル接続(Local Connection)] をクリックします。

ステップ 4 リストから [IPv4] を選択します。[IPv4 プロパティ(IPv4 Properties)] ウィンドウで、[次の IP アドレスを使う(Use the following IP address)] ラジオ ボタンをクリックします。Content Server の *IPv4 アドレス*、*サブネット マスク*、*デフォルト ゲートウェイ*を入力します。[OK] をクリックします。

タスク 5: 日時を設定する

電話会議の開催日時が電話会議リストに正しく表示されるように Content Server の日時を設定する必要があります。次の手順に従ってください。

ステップ 1 タスク 2: ローカル管理者パスワードを設定する で設定した管理者パスワードを使用して Content Server にログインします。

ステップ 2 [サーバー マネージャー(Server Manager)] ウィンドウで、右下隅の日時ボックスをクリックして設定ウィンドウを開きます。または、[スタート(Start)] > [コントロール パネル(Control Panel)] > [時計、言語、および地域(Clock, Language, and Region)] > [日付と時刻の設定(Set the time and date)] に移動します。

ステップ 3 [日付と時刻の設定の変更(Change date and time settings)] をクリックします。

ステップ 4 日付、時刻、タイム ゾーンを更新します。[OK] をクリックします。

タスク 6: リモート デスクトップ接続を有効化する

Cisco Content Server Release 7.0 以降では、Windows Server 2012 の管理と設定はすべて Windows リモート デスクトップ接続を使用してサーバ管理インターフェイスにアクセスすることで行います。Content Server でリモート デスクトップを有効にするには、次の手順に従います。

ステップ 1 タスク 2: ローカル管理者パスワードを設定する で設定した管理者パスワードを使用して Content Server にログインします。

ステップ 2 [スタート(Start)] > [コントロール パネル(Control Panel)] > [システム セキュリティ(System Security)] > [システム(System)] > [リモート設定(Remote Settings)] に移動します。

ステップ 3 [システムのプロパティ(System Properties)] ウィンドウの [リモート(Remote)] タブで、ラジオ ボタンを選択して Content Server でリモート デスクトップを有効にします。[OK] をクリックします。

ステップ 4 Content Server を再起動します。[スタート（Start）] > [ログオフ（Log Off）] > [再起動（Restart）] に移動します。

これで、Content Server から KVM ケーブルを取り外し、Content Server ユーザ インターフェイスにアクセスし、Windows リモート デスクトップ接続を使用して、サーバを引き続き設定できるようになりました。

タスク 7：SQL を設定する

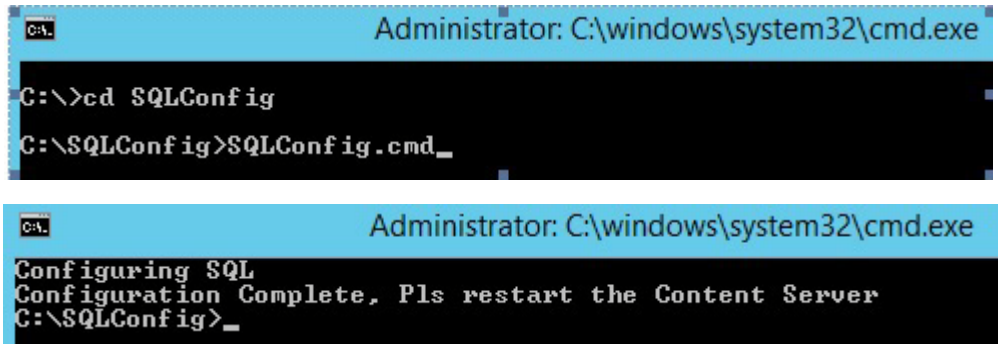
ステップ 1 管理者パスワードを使用して、リモートで Content Server にログインします。

ステップ 2 **コマンド プロンプト**を起動します。

ステップ 3 コマンド プロンプトで、「**cd c:\SQLConfig**」と入力し、現在のディレクトリを c:\SQLConfig に変更します。

ステップ 4 「SQLConfig.cmd」と入力してスクリプトを実行します。次に示す画像を参照してください。

図 5　　SQL の設定



ステップ 5 Content Server を再起動します。[スタート（Start）] > [ログオフ（Log Off）] > [再起動（Restart）] に移動します。

タスク 8：セキュリティ証明書をインストールする

Content Server には、10 年間有効な自己署名証明書が付属しています。自己署名証明書は信頼できる認証局から取得されたものではないため、ユーザがログインするときに、ほとんどのブラウザでサイト ID が確認できないことを示すメッセージが表示されます。

Internet Explorer の信頼済みサイト リストにサーバを追加するか、Firefox で例外を追加することで、ログイン時のエラー メッセージを回避できます。ただし、VeriSign または Comodo などのルート認証局との信頼関係を持つ証明書発行機関からセキュリティ証明書を購入することをお勧めします。これらの認証情報は、ブラウザによって信頼される可能性が高く、信頼済みサイト リストにサーバを追加する必要がなくなります。証明書は、サーバ IP アドレスに関連付けられた Windows マシン名または DNS エントリに対して生成する必要があります。

サーバのデフォルト Web サイトについて購入したセキュリティ証明書をインストールするには、次の手順を実行します。

ステップ 1 コンピュータで、[スタート(Start)] > [すべてのプログラム(All Programs)] > [アクセサリ(Accessories)] > [リモート デスクトップ接続(Remote Desktop)] に移動します

ステップ 2 [リモート デスクトップ接続(Remote Desktop Connection)] ダイアログボックスで、タスク 4:スタティック IP アドレスを設定するで設定した IP アドレスを入力します。

ステップ 3 [接続(Connect)] をクリックします。タスク 2:ローカル管理者パスワードを設定するで設定した管理者パスワードでログインします。[サーバー マネージャー(Server Manager)] ユーザ インターフェイスが表示されます。

ステップ 4 [スタート(Start)] > [インターネット インフォメーション サービス (IIS) マネージャー(Internet Information Services (IIS) Manager)] に移動します。

ステップ 5 [接続(Connections)] の下で、Content Server の Windows 2012 Server の「machine_name(ローカル コンピュータ)」をクリックします。

ステップ 6 machine_name のホーム ウィンドウの [サーバー証明書(Server certificates)] をクリックします。

ステップ 7 [アクション(Actions)] の下の [インポート(Import)] をクリックして、新しい証明書をインポートします。

ステップ 8 Web サーバ証明書ウィザードの指示に従って、現在の証明書を購入した証明書に置き換えます。

詳細については、インターネット インフォメーション サービスのヘルプを参照してください。

管理者が Windows Media Administration Web サイトにログインしたときにセキュリティ警告が表示されるのを回避するために、そのサイトの証明書をインストールすることもできます。Web サイトの証明書をインストールすると、購入した証明書が自己署名証明書の代わりに使用されます。

セキュリティ証明書の有効期限が切れると(サーバが使用するのが購入したセキュリティ証明書か元の自己署名証明書かにかかわらず)、ブラウザに追加の警告が表示されます。IIS Web サーバ証明書ウィザードを使用して、新しい証明書要求を生成できます。この要求後に、サードパーティ ツールを使用して、別の自己署名証明書を作成できます。または、この要求を証明書発行機関に転送できます。新しい証明書をインストールするまで、期限切れの証明書を削除しないでください。証明書を削除すると、あらゆるログイン試行が妨げられます。

タスク 9:H.323/SIP 登録設定を行う

ステップ 1 コンピュータでブラウザを開き、タスク 4:スタティック IP アドレスを設定するで設定した Content Server の IP アドレスを入力します。

ステップ 2 タスク 2:ローカル管理者パスワードを設定するで設定したパスワードを使用して、Content Server の Web インターフェイスにログインします。

ステップ 3 Content Serverの Web インターフェイスで [管理(Management)] > [設定(Configuration)] > [サイト設定(Site settings)] に移動します。

ステップ 4 Cisco TelePresence Management Suite で Content Server を識別するために使用される**システム名**を入力します。

(オプション)Web インターフェイスを使用するときにブラウザのタイトル バーにシステム名を表示するには、[ブラウザのタイトルに表示(Show in browser title)] チェックボックスを選択します。

ステップ 5 H.323 ゲートキーパーを使用する場合、ゲートキーパーの設定セクションで次の操作を行います。

a. [ゲートキーパーを有効化(Gatekeeper enabled)] を選択し、ゲートキーパーの IP アドレスまたは DNS 名を入力します。

b. 必要に応じて **H.323 ID** と **E.164 エイリアス** を入力します。

c. [登録(Registration)] では、[端末(Terminal)] または [ゲートウェイ(Gateway)] を選択します。

d. [ゲートウェイ(Gateway)] モードを選択した場合は、必要に応じて H.323 および E.164 ゲートウェイ プレフィクスを入力します。

ステップ 6 SIP レジストラを使用する場合、SIP の設定セクションで次の操作を行います。

a. [SIP を有効化(SIP enabled)] を選択し、**SIP アドレス(URI)**および **SIP の表示名**を入力します。

b. [サーバ アドレス(Server address)] には、SIP レジストラの IP アドレスまたは DNS 名を入力します。

ステップ 7 [保存(Save)] をクリックします。[登録ステータス(Registration status)] が更新されます(ページの更新が必要になる場合があります)。

ステップ 8 [レコーディングのセットアップ(Recording setup)] > [レコーディング エイリアス(Recording aliases)] に移動します。

ステップ 9 デフォルトのレコーディング エイリアスの [編集(Edit)] をクリックします。各エイリアスでは、次を設定します。

- H.323 ゲートキーパーを使用する場合は、**H.323 ID** と **E.164 エイリアス**を入力します。[保存(Save)] をクリックします。
- SIP レジストラを使用する場合は、**SIP アドレス(URI)**および **SIP の表示名**を入力します。[保存(Save)] をクリックします。

注意 すべての E.164 エイリアスおよび H.323 ID がネットワーク内で一意であり、ゲートキーパーに有効であることを確認します。デフォルトのライブ レコーディング エイリアスの H.323 ID は *Live<serial_number>* であり、デフォルトのオンデマンド レコーディング エイリアスは *OnDemand<serial_number>* です。

レコーディング エイリアスの説明については、オンライン ヘルプを参照してください。SIP URI はネットワーク内で一意であり、SIP レジストラに有効である必要があります。

タスク 10:テスト録画を実行する

ダイヤルしてテスト録画を実行できます。録画が保存されて、変換されます。プロセスが完了すると、録画が [録画の表示(View Recordings)] タブに表示されます。

次の手順に従ってください。

ステップ 1 Content Server の Web インターフェイスで、[管理(Management)] > [録画(Recordings)] > [録画の作成(Create recording)] に移動します

ステップ 2 レコーディング エイリアスを選択します。

ステップ 3 [ダイヤル番号(Dial number)] には、電話をかけるエンドポイント アドレスを入力します。[コールの発信(Place call)] をクリックします。

ステップ 4 [録画の表示(View Recordings)] タブに移動します。進行中の録画については、赤の録画ドット付きサムネイルが表示されます。

ステップ 5 エンドポイントからコールを終了するか、サムネイルをクリックしてから、[録音の編集(Edit recording)] および [コールの終了(End call)] をクリックしてコールを終了します。

ダイヤルしてテスト コールを行うことができます。録画が保存されて、変換されます。プロセスが完了すると、録画が [録画の表示(View Recordings)] タブに表示されます。

次の手順に従ってください。

ステップ 1 Content Server の Web インターフェイスで、[管理(Management)] > [録画設定(Recording setup)] > [レコーディング エイリアス(Recording aliases)] に移動します。

ステップ 2 使用するレコーディング エイリアスの H.323 ID、E.164 エイリアス、または SIP アドレス(URI)を記録します。

ステップ 3 エンドポイントから、記録したアドレスの 1 つをダイヤルします。

ステップ 4 [録画の表示(View Recordings)] タブに移動します。進行中の録画については、赤の録画ドット付きサムネイルが表示されます。

ステップ 5 エンドポイントからコールを終了するか、サムネイルをクリックしてから、[録音の編集(Edit recording)] および [コールの終了(End call)] をクリックしてコールを終了します。

追加 Content Server 設定

以下のタスクのいずれかに関する詳細については、Cisco.com のこのリリースのオンライン ヘルプまたは『*Cisco TelePresence Content Server Administration and User Guide*』を参照してください。

API パスワードの変更

デフォルトの API パスワードを変更することを推奨します。デフォルトの API の設定については、Cisco.com の『*Cisco TelePresence Content Server API Guide*』を参照してください。

1. Content Server の Web インターフェイスで、管理者パスワードでログインします。
2. [管理(Management)] > [設定(Configuration)] > [サイト設定(Site settings)] に移動します。
3. API セクションで、新しいパスワードを [パスワード(Password)] フィールドおよび [パスワードの確認(Password confirm)] フィールドに入力します。
4. [保存(Save)] をクリックします。

認証方式の設定

[管理(Management)] タブの [設定(Configuration)] > [サイト設定(Site settings)] にあるデフォルトの認証オプションは [ローカル(Local)] です。デフォルトの認証方式を LDAP/Active Directory モードまたはドメイン モードに変更することを推奨します。各モードの使い分けに関する詳細については、オンライン ヘルプを参照してください。

グループおよびユーザの追加

グループとユーザを設定し、そのグループやユーザが視聴者、作成者、サイト マネージャのいずれであるかに応じて役割を設定します。[管理(Management)] タブで、[設定(Configuration)] > [グループおよびユーザ(Groups and users)] に移動します。

ゲスト ユーザ アクセスの追加(必要な場合)

録画へのアクセスは、認証されたユーザ(つまり、ログインしているユーザ)のみに制限できます。認証されていないユーザが会議を表示できるようにするには、[サイト設定(Site settings)] の [ユーザ プロパティ(User Properties)] セクションでゲスト アクセスを有効にします。ログインしていないユーザは、会議アクセス許可で [すべてのユーザへのアクセスを許可(Allow access to all users)] が選択されている会議を表示できます。RSS フィードは、ゲスト アクセスが有効化されている場合にのみ使用できます。

メディア サーバの構成

外部ストリーミング サーバを使用するか、マルチキャスト ストリーミングを有効化する場合、メディア サーバでライブ ストリーミング、オンデマンドのストリーミング、または両方を設定する必要があります。[管理(Management)] タブで、[録画のセットアップ(Recording setup)] > [メディア サーバ(Media server)] に移動します。

自動的にメディアを Cisco Media Experience Engine 3500、Cisco Show and Share、Podcast Producer、または iTunes U にアップロードする場合、これらのアプリケーションごとにメディア サーバを作成する必要があります。

デフォルトのメディア サーバ設定の選択

[サイト設定(Site settings)] でシステム デフォルトを作成したメディア サーバ設定を行うことができます。テンプレートを作成する場合、または [出力の管理(Manage outputs)] ページで録画出力を編集する場合に、サーバの設定がデフォルトとして表示されます。

テンプレートの確認および設定

サーバは、編集可能な多数のデフォルト テンプレートによって事前に設定されています。メディア サーバ設定を使用して、新しいテンプレートを作成することもできます。[管理(Management)] タブで、[録画のセットアップ(Recording setup)] > [テンプレート(Templates)] に移動します。

カテゴリの設定

ユーザが検索できるように、録画に表示カテゴリを割り当てることができます。たとえば、マーケティング部門にはすべてのマーケティング録画用のカテゴリがあります。[管理(Management)] タブで、[録画のセットアップ(Recording setup)] > [カテゴリ(Categories)] に移動します。

レコーディング エイリアスの設定

サーバは、多数のデフォルトのレコーディング エイリアスによって事前に設定されています。各レコーディング エイリアスには、コールまたは会議を記録するためにダイヤルできる H.323 ID、E.164 のエイリアス、または SIP URI があります。[管理(Management)] タブで、[録画のセットアップ(Recording setup)] > [レコーディング エイリアス(Recording aliases)] に移動します。

レコーディング エイリアスのシステム デフォルトの選択

システムの H.323 ID、E.164 エイリアス、SIP URI、またはサーバ IP アドレスが呼び出されると、デフォルトのレコーディング エイリアスが使用されます。[サイト設定(Site settings)] の [システム デフォルト(System defaults)] セクションで、デフォルトのレコーディング エイリアスを設定できます。

Content Server を使用するための TMS の設定

Cisco TelePresence Management Suite(TMS)は、スケジュールされた単発の会議または定例会議を記録するのに使用できます。Cisco.com で、このリリースの『*Cisco TelePresence Content Server Administration and User Guide*』およびすべての TMS ドキュメントを参照してください。

バックアップ

サーバのバックアップは、定期的に、またシステム アップグレードの前に行うことを推奨します。バックアップの詳細については、Cisco.com のこのリリースの『*Cisco TelePresence Content Server Administration and User Guide*』を参照してください。

ネットワーク接続ストレージ(NAS)デバイスの使用

メディア ファイルのデフォルトの場所は、ドライブ E: です。ネットワーク接続ストレージ(NAS)デバイスにファイルを保存するように、この場所を変更できます。NAS デバイスを使用することで、録画能力がサーバ上のディスク領域によって制限されないようにできます。NAS に関する詳細については、Cisco.com のこのリリースの『*Cisco TelePresence Content Server Administration and User Guide*』を参照してください。

Content Server のクラスタリング

最大 10 台までのコンテンツ サーバをクラスタして合計コール容量を増加し、冗長性と復元性を改善することができます。Content Server クラスタのシステム要件、設定、および管理の詳細については、Cisco.com のこのリリースの『*Cisco TelePresence Content Server Administration and User Guide*』を参照してください。

トラブルシューティングおよびテクニカル サポート

問題解決のためのサーバ ログの使用

サーバ ログを使用してデバッグ情報を生成し、問題解決において顧客サポートを支援することができます。[管理(Management)] タブから、[診断(Diagnostics)] > [サーバ ログ(Server logs)] に移動して、Content Server のログにアクセスします。

その他のヘルプ

Content Server を設定または使用するときに問題が発生した場合は、オンライン ヘルプで個々の機能と設定がどのように機能するかについての説明を参照してください。また、Cisco.com のこのリリースの『*Cisco TelePresence Content Server Administration and User Guide*』を参照してください。

サポートについてシスコに連絡する際に、次の情報があることを確認してください。

- サーバのシリアル番号と製品モデル番号
- 製品のユーザ インターフェイスに記載されているソフトウェアのビルド番号
- お客様の連絡先となる電子メール アドレスまたは電話番号
- 問題の詳しい説明

関連資料

- Cisco TelePresence Content Server のマニュアル
  http://www.cisco.com/en/US/products/ps11347/tsd_products_support_series_home.html
- Cisco UCS C220 のマニュアル
  http://www.cisco.com/en/US/products/ps10493/tsd_products_support_series_home.html
- シスコのキャプチャ、変換、共有に関するマニュアル
  http://www.cisco.com/en/US/products/ps12130/products_installation_and_configuration_guides_list.html

アクセシビリティとシスコ製品に関する情報

この製品のアクセシビリティについては、シスコのアクセシビリティのチーム（accessibility@cisco.com）にお問い合わせください。

マニュアルに関するフィードバックの提出

本マニュアルに関するフィードバックを送る場合、または誤りや抜けについて報告する場合、画面の左側に表示されているオンラインの組み込みフィードバック フォームを使用できます。また、フィードバックは mxe-doc@cisco.com に送信していただくこともできます。

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*」（ http://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*」に配信登録すると、新しい（または改訂された）シスコ技術情報のリストが RSS フィードとして提供され、リーダー アプリケーションを使ってコンテンツがデスクトップに直接配信されるようにすることができます。RSS フィードは無料のサービスです。