



IM and Presence Service リリース 14 コンフィギュレーション およびアドミニストレーション

初版：2021年3月31日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



目次

第 I 部 :	システムを計画します 23
第 1 章	システムを計画します 1
	IM and Presence サービスの概要 1
	IM and Presence Service のコンポーネント 2
	計画の概要 5
	導入の計画 5
	IM and Presence サービスの展開の規模 6
	機能展開オプション 7
	標準導入 vs 中央クラスタ 10
	マルチノードの拡張性機能 10
	マルチノードの拡張性の要件 10
	OVA の要件 11
	展開の拡張性オプション 11
	WAN の導入 14
	WAN 経由のクラスタ内展開 14
	WAN 経由の展開のマルチノード設定 14
	WAN 経由のクラスタ間展開 15
	SAML シングルサインオン展開 16
	サードパーティ統合 16
	サードパーティクライアント統合 17

第 II 部 :	システムの設定 19
----------	------------

第 2 章

ドメインの設定 21

ドメイン設定の概要 21

ドメイン設定例 22

ドメイン前提条件の設定 24

ドメインタスクフローの設定 25

ハイアベイラビリティの無効化 26

IM and Presence サービスの無効化 26

IM and Presence サービスのデフォルトドメインを設定します 28

IM アドレス ドメインの追加または更新 29

IM アドレス ドメインの削除 30

XMPP クライアントおよび TLS 証明書を再生成します 31

IM and Presence サービスの開始 31

プレゼンス冗長グループでハイアベイラビリティを有効化する 32

第 3 章

IPv6 の設定 35

IPv6 設定の概要 35

IPv6 タスクフローの設定 36

IM and Presence サービスの Eth0 での IPv6 の有効化 36

IPv6 エンタープライズパラメータの有効化 37

サービスの再起動 37

IM and Presence ノードに IPv6 アドレスを割り当てます 38

IM and Presence サービスの Eth0 での IPv6 の無効化 39

第 4 章

IM アドレッシングスキームの設定 41

IM アドレッシングスキームの概要 41

User@Default_Domain を使用している IM アドレス 41

ディレクトリ URI を使用した IM アドレス 42

複数の IM ドメイン 43

IM アドレッシング方式の前提条件 43

IM アドレッシングスキームタスクフローの設定 43

ユーザプロビジョニングの検証	44
ハイ アベイラビリティの無効化	45
サービスの停止 (Stop Services)	46
IM アドレス スキームの割り当て	46
IM アドレスの例	48
サービスの再起動	48
高可用性を有効にする	49
ディレクトリ URI への LDAP ソースの割り当て	50
Directory URI を手動で割当ます	51

第 5 章

冗長性およびハイ アベイラビリティの設定	53
プレゼンス冗長グループの概要	53
高可用性	54
プレゼンス冗長グループの前提条件	54
プレゼンス冗長グループのタスク フロー	55
データベース レプリケーションの確認	55
確認サービス	56
プレゼンス冗長グループの設定	57
フェールオーバー用のハートビート間隔の設定	58
高可用性を有効にする	60
ユーザー割り当てモードの設定	60
手動によるフェールオーバー、フォールバック、リカバリの開始	61
ノード状態定義	62
ノード状態、原因、および推奨処置	63
ダウンタイムをほぼゼロに抑える IM and Presence フェールオーバーの機能拡張	71
冗長性の連携動作と制約事項	74

第 6 章

ユーザ設定値の設定	77
エンド ユーザ設定の概要	77
サービスプロファイル	77
機能グループ テンプレートの概要	78

ユーザ設定の前提条件	78
ユーザ設定タスクフローの設定	79
ユーザー割り当てモードの設定	80
IM and Presence UC サービスの追加	80
サービス プロファイルの設定	81
機能グループ テンプレートの設定	82

第 7 章

LDAP ディレクトリの設定 83

LDAP 同期の概要	83
[エンドユーザ用LDAP認証 (LDAP Authentication for End Users)]	84
Cisco モバイルおよびリモートアクセス クライアントとエンドポイントに対するディレ トリ サーバユーザの検索	84
LDAP 同期の前提条件	85
LDAP 同期設定のタスク フロー	85
Cisco DirSync サービスの有効化	86
LDAP ディレクトリ同期の有効化	87
LDAP フィルタの作成	88
LDAP ディレクトリの同期の設定	88
エンタープライズ ディレクトリ ユーザー検索の設定	91
ディレクトリ サーバの UDS 検索用の LDAP 属性	92
LDAP 認証の設定	93
LDAP アグリーメント サービス パラメータのカスタマイズ	94
LDAP ディレクトリ サービス パラメータ	95
LDAP同期済みユーザのローカル ユーザへの変換	95
アクセス コントロール グループへの LDAP 同期済みユーザの割り当て	96
XMPP クライアントにおける連絡先検索のための LDAP ディレクトリ統合	96
LDAP アカウント ロックの問題	98
XMPP クライアントの LDAP サーバの名前とアドレスの設定	98
XMPP クライアントの LDAP 検索設定	100
Cisco XCP ディレクトリ サービスのオン	103

第 8 章

IM and Presence サービス用に Cisco Unified Communications Manager を設定します 105

統合の概要 105

Cisco Unified Communications Manager 統合の前提条件 105

Cisco Unified Communications Manager の SIP トランク設定 107

SIP トランク セキュリティ プロファイルの設定 108

IM and Presence サービスの SIP トランクの設定 109

SRV クラスタ名の設定 110

SIP パブリッシュ トランクの設定 111

プレゼンス ゲートウェイの設定 111

Cisco Unified Communications Manager でサービスを確認する 112

クラスタ外の Cisco Unified Communications Manager の電話でのプレゼンス表示の設定 112

Cisco Unified Communications Manager を TLS ピアとして追加 113

Unified Communications Manager の TLS Context を設定します 113

第 9 章

集中展開の設定 115

集中展開の概要 115

集中型クラスタの展開アーキテクチャ 118

集中型クラスタの使用例 119

集中展開の前提条件 119

集中展開設定のタスク フロー 121

IM and Presence を Feature Group Template から有効化 123

IM and Presence 中央クラスタでの LDAP 同期の完了 124

一括管理経由で IM and Presence を有効にする 125

リモート テレフォニー クラスタの追加 126

IM and Presence UC サービスの設定 127

IM and Presence のサービス プロファイルの作成 128

テレフォニー クラスタでの Presence ユーザーの無効化 128

OAuth 更新ログインを設定する 130

ILS ネットワークの設定 130

ILS へのクラスタ ID の設定 131

テレフォニー クラスタでの ILS の有効化	132
ILS ネットワークが動作していることを確認する	133
モバイルおよびリモートアクセスの設定	134
サブドメインの SSO 対応リモートテレフォニー クラスタを使用した IM and Presence の中央 集中クラスタのセットアップ	135
電話機のプレゼンスを中央集中型導入に統合する	136
集中展開の相互作用と制限事項	138

第 10 章

高度なルーティングを設定する	139
高度なルーティングの概要	139
高度なルーティングの前提条件	140
高度なルーティング設定のタスク フロー	140
ルーティング通信方法の設定	141
Cisco XCP ルータの再起動	142
セキュアなルータツールータ通信の設定	143
クラスタ ID の設定	144
プレゼンス更新のスロットルレートを設定する	144
スタティック ルートの設定	145
SIP プロキシ サーバを設定します。	146
IM and Presence Service のルート組み込みテンプレートの設定	146
IM and Presence Service のスタティック ルートの設定	148

第 11 章

証明書の設定	153
証明書の概要	153
証明書の前提条件	155
Cisco Unified Communications Manager との証明書の交換	156
IM and Presence サービスへの Cisco Unified Communications Manager 証明書のインポート	156
IM and Presence サービスからの証明書のダウンロード	157
IM and Presence 証明書を Cisco Unified Communications Manager にインポート	158
IM and Presence サービスに認証局 (CA) をインストールする	159

CA ルート証明書チェーンをアップロードする	159
Cisco Intercluster Sync Agent サービスの再起動	160
他のクラスタとの CA 証明書の同期の検証	161
IM and Presence Service に証明書をアップロードします。	162
証明書のアップロード (Upload Certificates)	163
Cisco Tomcat サービスの再起動	164
クラスタ間同期の検証	164
すべてのノードで Cisco XCP ルータ サービスを再起動します。	165
Cisco XCP XMPP Federation Connection Manager サービスの再起動	166
XMPP フェデレーションのセキュリティ証明書でのワイルドカードの有効化	166
CSR の生成	167
証明書署名要求のキー用途拡張	168
自己署名証明書の生成	169
IM and Presence Service からの自己署名信頼証明書の削除	169
Cisco Unified Communications Manager からの自己署名 Tomcat 信頼証明書の削除	170
証明書モニタリング タスク フロー	171
証明書モニタ通知の設定	172
OCSP による証明書失効の設定	173

第 12 章

セキュリティ設定の構成	175
セキュリティの概要	175
セキュリティ設定構成のタスク フロー	175
ログイン バナーの作成	176
安全な XMPP 接続の設定	177
IM and Presence Service での SIP セキュリティの設定	178
TLS ピア サブジェクトの設定	178
TLS コンテキストの設定	178
FIPSモード	179

第 13 章

クラスタ間ピアの設定	183
クラスタ間ピアの概要	183

クラスタ間ピアの前提条件	183
クラスタ間ピアの設定のタスクフロー	184
ユーザプロビジョニングを確認する	185
Cisco AXL Web サービスの有効化	185
同期エージェントを有効にする	186
クラスタ間ピアの設定	187
XCP ルータ サービスを再起動します。	189
Intercluster Sync Agent がオンであることを確認します。	189
クラスタ間ピア ステータスの確認	190
Intercluster Sync Agent の Tomcat 信頼証明書の更新	191
クラスタ間ピアの定期同期エラーからの自動リカバリを有効化	191
クラスタ間ピアの同期間隔の設定	192
クライアント間ピア定期同期の証明書同期の無効化	193
クラスタ間ピア接続の削除	193
クラスタ間ピアリングの連携動作と制限事項	194

 第 14 章

プッシュ通知の設定 195

プッシュ通知の概要	195
プッシュ通知設定	199

 第 III 部 :

機能の設定 201

 第 15 章

アベイラビリティとインスタントメッセージの設定 203

アベイラビリティとインスタントメッセージの概要	203
アベイラビリティとインスタントメッセージの前提条件	204
アベイラビリティとインスタントメッセージのタスクフロー	205
プレゼンス共有の設定	205
インスタントメッセージを有効にする	206
可用性およびインスタントメッセージングの相互作用および制限	207

 第 16 章

アドホック チャットおよび常設チャットの設定 209

グループチャットルームの概要	209
グループチャットの前提条件	210
グループチャットと常設チャットのタスクフロー	211
グループチャットシステム管理者の設定	211
チャットルーム設定を設定します	212
Cisco XCP Text Conference Manager を再起動します	213
常設チャット用の外部データベースの設定	214
外部データベースの接続の追加	215
グループチャットと持続チャットのインタラクションと制限	216
常設チャットの例 (HA なし)	219
Cisco IM and Presence の常設チャットの境界	220

第 17 章

常設チャットの高可用性の設定	225
持続チャットにおける高可用性の概要	225
常設チャットの高可用性 - クラスタ間の例	226
常設チャット (非 HA) と常設チャット HA の要件の比較	226
常設チャット前提条件の高可用性	228
常設チャットにおける高可用性のタスクフロー	228
外部データベースのセットアップ	229
外部データベースの接続の追加	229
常設チャットにおける高可用性の確認	230
Cisco XCP Text Conference Manager サービスの起動	231
外部データベースのマージ	232
常設チャットにおける高可用性の使用例	234
常設チャットにおける高可用性のフェールオーバー使用例	235
高可用性常設チャットのフォールバック使用例	236

第 18 章

マネージド ファイル転送の設定	239
マネージド ファイル転送の概要	239
マネージド ファイル転送の通話フロー	240
マネージド ファイル転送の前提条件	241

外部データベースの前提条件	241
外部ファイル サーバの要件	241
マネージドファイル転送のタスク フロー	244
外部データベースの接続の追加	245
外部ファイル サーバのセットアップ	246
外部ファイルサーバーのユーザの作成	247
外部ファイル サーバのディレクトリを設定	248
外部ファイルサーバーの公開鍵を取得する	249
IM and Presence Service での外部ファイル サーバのプロビジョニング	250
外部ファイル サーバ フィールド	251
Cisco XCP ファイル転送マネージャのアクティベーションの確認	253
マネージド ファイル転送の有効化	253
ファイル転送オプション	255
外部サーバステータスの確認	256
外部ファイルサーバと公開キーのトラブルシューティング	256
マネージドファイル転送の管理	257
<hr/>	
第 19 章	複数のデバイスのメッセージングの設定 259
	マルチデバイスメッセージング の概要 259
	複数デバイスのメッセージングの前提条件 260
	複数のデバイスのメッセージングの設定 260
	マルチ デバイス メッセージングのフローの使用例 261
	マルチデバイスメッセージングにおける静音モードの使用例 261
	マルチデバイスメッセージング のインタラクションと制限 262
	複数のデバイスのメッセージングのカウンタ 263
	デバイス容量のモニタリング 264
	デバイス キャパシティ モニタリングのユーザセッション レポート 266
<hr/>	
第 20 章	エンタープライズ グループの設定 269
	エンタープライズグループの概要 269
	エンタープライズ グループの前提条件 270

エンタープライズ グループの設定タスク フロー	271
LDAP ディレクトリからのグループ同期の確認	271
エンタープライズ グループの有効化	272
セキュリティグループを有効にする	273
セキュリティグループフィルタの作成	273
LDAP ディレクトリからセキュリティグループを同期する	274
セキュリティグループのための Cisco Jabber の設定	275
ユーザ グループの表示	275
エンタープライズ グループの導入モデル (Active Directory)	276
エンタープライズ グループの制限事項	279

第 21 章

ブランディングのカスタマイズ	283
ブランディングの概要	283
ブランディングの前提条件	283
ブランディングの有効化	284
ブランディングの無効化	284
ブランディング ファイルの要件	285

第 22 章

高度な機能の設定	291
ストリーム管理	291
ストリーム管理の設定	292
Microsoft Outlook とのカレンダー統合	293
フェデレーション	293
メッセージアーカイバ	294
Remote Call Control; リモート呼制御	295

第 IV 部 :

システムの管理	297
----------------	------------

第 23 章

チャットの管理	299
チャット管理の概要	299
チャットノードエイリアスの概要	300

チャットの前提条件の管理	300
チャットのタスクフローの管理	301
チャットルーム所有者がチャットルーム設定を編集できるようにする	302
クライアントでのインスタントメッセージ履歴のログ記録の許可	303
外部データベーステキスト会議レポートの表示	303
チャットルーム設定を設定します	304
チャットルーム数の設定	304
チャットルームメンバー設定を設定します	304
可用性の設定	306
利用者数の設定	307
チャットメッセージの設定	308
モデレータ管理されたルームの設定	309
履歴の設定	310
チャットルームをシステムのデフォルトにリセットします	310
チャットノードエイリアスの管理	311
チャットノードのエイリアスの管理	311
チャットエイリアスの管理にモードを割り当てます	311
チャットノードエイリアスを手動で追加	312
常設チャット用の外部データベースの消去	314
チャット相互作用の管理	315
<hr/>	
第 24 章	マネージドファイル転送管理 317
マネージドファイル転送管理の概要	317
マネージドファイル転送管理の前提条件	318
マネージドファイル転送管理のタスクフロー	318
AFT_LOG テーブル例クエリおよび出力	319
外部データベースのディスク使用量	320
サービスパラメータのしきい値の設定	321
XCP File Transfer Manager のアラームの設定	322
マネージドファイル転送のアラームとカウンタ	322
マネージドファイル転送の外部データベースを消去する	324

第 25 章

エンドユーザの管理 327

- エンドユーザの管理の概要 327
 - プレゼンス認証の概要 327
 - ユーザー ID とディレクトリ URI の検証 328
- エンドユーザーのタスクフローを管理する 329
 - プレゼンス認証ポリシーを割り当てる 330
 - ユーザデータに対するデータモニタチェックの設定 331
 - ユーザー ID とディレクトリ URI 検証チェックのスケジュール設定 331
 - 電子メールアラート用の電子メールサーバをセットアップします。 332
 - 電子メールアラートの有効化 333
 - システムトラブルシューターを介してユーザデータを検証する 333
 - CLI を介してユーザー ID とディレクトリ URI を検証する 334
 - ユーザー ID とディレクトリ URI CLI 検証の例 335
 - ユーザー ID とディレクトリ URI のエラー 336
 - ユーザのプレゼンス設定を表示 338
- プレゼンスの連携動作と制限事項 341

第 26 章

ユーザを集中展開に移行する 343

- 集中展開のユーザ移行概要 343
- 中央クラスタ移行のための前提作業 343
- 中央クラスタタスクフローへの移行 345
 - 移行元クラスタから連絡先リストをエクスポートする 347
 - 移行元クラスタで高可用性を無効にする 348
 - IM and Presence UC サービスの設定 349
 - IM and Presence のサービス プロファイルの作成 350
 - テレフォニー クラスタでの Presence ユーザーの無効化 350
 - 中央クラスタの OAuth 認証を有効にする 352
 - 中央クラスタで高可用性を無効にする 352
 - 中央および移行クラスタのピア関係の削除 353
 - Cisco クラスタ間同期エージェントの停止 354

IM and Presence を Feature Group Template から有効化	354
中央クラスタでの LDAP 同期の完了	355
一括管理経由で IM and Presence を有効にする	356
連絡先を中央クラスタにインポート	357
Cisco Intercluster Sync Agent	358
中央クラスタで高可用性を有効にする	359
クラスタを移行する残りのピアの削除	359

第 27 章

ユーザの移行 361

ユーザ移行の概要	361
ユーザ移行の前提条件	361
ユーザの移行タスクフロー	361
古いエントリの削除	363
移行の標準プレゼンスの設定	364
Intercluster Sync Errors を確認	364
移行のための必須サービスの起動	365
ユーザ連絡先リストのエクスポート	365
LDAP を介してユーザを移行する	367
外部 LDAP ディレクトリの更新	367
新しいクラスタでの LDAP の設定	368
新しいクラスタへのユーザの手動での移動	369
ユーザの IM and Presence の手動での無効化	369
ユーザの手動インポート	370
新しいクラスタの IM and Presence Service のユーザの有効化	370
一括管理からのユーザの移行	371
ユーザーをCSVファイルにエクスポート	372
CSV エクスポートファイルをダウンロードします	373
CSV エクスポートファイルを新しいクラスタにアップロードします	374
ユーザ テンプレートの設定	374
ユーザを新しいクラスタにインポート	375
一括管理によるユーザー移行の確認	375

ホーム クラスタでの連絡先リストのインポート 376

古いクラスタのユーザの更新 377

第 28 章

ロケールの管理 379

ロケールの管理の概要 379

ユーザ ロケール 380

ネットワーク ロケール 380

ロケールの管理の前提条件 380

IM and Presence Service へのロケールインストーラのインストール 381

エラーメッセージロケールリファレンス 382

ローカライズされたアプリケーション 385

第 29 章

サーバの管理 387

サーバの管理の概要 387

サーバアドレスの変更 387

クラスタからの IM and Presence ノードの削除 388

削除したサーバをクラスタに戻す 389

インストール前のクラスタへのノードの追加 389

プレゼンス サーバのステータスの表示 390

ハイ アベイラビリティでのサービスの再起動 391

ホスト名の設定 392

第 30 章

システムのバックアップ 395

バックアップの概要 395

バックアップの前提条件 396

バックアップ タスク フロー 396

バックアップ デバイスの設定 397

バックアップ ファイルのサイズの予測 398

スケジュール バックアップの設定 399

手動バックアップの開始 401

現在のバックアップ ステータスの表示 402

バックアップ履歴の表示	402
バックアップの連携動作と制限事項	403
バックアップの制約事項	403
リモートバックアップ用 SFTP サーバ	404

第 31 章

システムの復元	407
復元の概要	407
マスター エージェント	407
ローカル エージェント	407
復元の前条件	408
復元タスク フロー	408
最初のノードのみの復元	409
後続クラスタ ノードの復元	411
パブリッシュの再構築後の 1 回のステップでのクラスタの復元	413
クラスタ全体の復元	415
前回正常起動時の設定へのノードまたはクラスタの復元	416
ノードの再起動	417
復元ジョブ ステータスのチェック	418
復元履歴の表示	418
データ認証	419
トレース ファイル	419
コマンドライン インターフェイス	419
アラームおよびメッセージ	421
アラームおよびメッセージ	421
復元の連携動作と制約事項	425
復元の制約事項	425
トラブルシューティング	426
より小さい仮想マシンへの DRS 復元の失敗	426

第 32 章

連絡先リストの一括管理	427
一括管理の概要	427

一括管理の前提条件	427
一括管理のタスクフロー	428
ユーザ連絡先 ID の一括名前変更	429
ユーザ連絡先 ID の一括名前変更	430
非プレゼンス連絡先リストの一括エクスポート	430
ユーザの場所の詳細の一括エクスポート	431
エクスポート連絡先リストのファイルの詳細	432
非プレゼンス連絡先リストの一ファイルの詳細	433
ユーザの場所の詳細をエクスポートするファイルの詳細	434
ユーザ連絡先リストの一括インポート	435
連絡先リストの最大サイズの確認	435
入力ファイルのアップロード	435
新しい一括管理ジョブの作成	440
一括管理ジョブの結果の確認	441

第 33 章

システムのトラブルシューティング	443
トラブルシューティングの概要	443
システムトラブルシューターを実行する	443
診断の実行	444
診断ツールの概要	445
トラブルシューティングのためのトレースログの使用	446
トレースによる一般的な IM and Presence の問題	447
CLI 経由の共通トレース	449
CLI 経由でトレースを実行する	453
RTMT 経由の共通トレース	454
ユーザー ID エラーおよびディレクトリ URI エラーのトラブルシューティング	455
重複したユーザー ID エラーの受信	455
重複または無効なディレクトリ URI エラーの受信	456

第 V 部 :

参考情報	459
-------------	------------

第 34 章	Cisco Unified Communications Manager での TCP および UDP ポートの使用	461
	Cisco Unified Communications Manager の TCP と UDP ポートの使用に関する概要	461
	ポート説明	463
	Cisco Unified Communications Manager サーバ間のクラスタ間ポート	463
	共通サービス ポート	467
	Cisco Unified Communications Manager と LDAP ディレクトリとの間のポート	471
	CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求	471
	Cisco Unified Communications Manager から電話機への Web 要求	472
	電話機と Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信	473
	ゲートウェイと Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信	475
	アプリケーションと Cisco Unified Communications Manager との間の通信	479
	CTL クライアントとファイアウォールとの通信	481
	HP サーバ上の特殊なポート	481
	ポート参照	482
	ファイアウォールアプリケーションインスペクションガイド	482
	IETF TCP/UDP ポート割り当てリスト	482
	IP テレフォニー設定とポート使用に関するマニュアル	482
	VMware ポート割り当てリスト	483
第 35 章	IM and Presence サービスのポートの使用情報	485
	IM and Presence サービス ポートの使用方法の概要	485
	テーブルで照合する情報	486
	IM and Presence サービス ポート リスト	486
第 36 章	追加の要件	505
	ハイアベイラビリティログインプロファイル	505
	ハイアベイラビリティ ログインプロファイルに関する重要事項	505
	ハイアベイラビリティ ログインプロファイルテーブルの使用	506

高可用性 ログイン設定の例	507
単一クラスタ コンフィギュレーション	508
500 ユーザフル UC (1vCPU 700MHz 2GB) のアクティブ/アクティブ プロファイル	508
500 ユーザフル UC (1vCPU 700MHz 2GB) のアクティブ/スタンバイ プロファイル	508
1000 ユーザフル UC (1vCPU 1500MHz 2GB) のアクティブ/アクティブ プロファイル	508
1000 ユーザフル UC (1vCPU 1500MHz 2GB) のアクティブ/スタンバイ プロファイル	509
2000 ユーザフル UC (1vCPU 1500Mhz 4GB) のアクティブ/アクティブ プロファイル	509
2000 ユーザフル UC (1vCPU 1500Mhz 4GB) のアクティブ/スタンバイ プロファイル	509
5000 ユーザフル UC (4 GB 2vCPU) のアクティブ/アクティブ プロファイル	510
5000 ユーザフル UC (4 GB 2vCPU) のアクティブ/スタンバイ プロファイル	510
15000 ユーザフル UC (4 vCPU 8GB) のアクティブ/アクティブ プロファイル	511
15000 ユーザフル UC (4 vCPU 8GB) のアクティブ/スタンバイ プロファイル	512
25000 ユーザフル UC (6 vCPU 16GB) のアクティブ/アクティブ プロファイル	513
25000 ユーザフル UC (6 vCPU 16GB) のアクティブ/スタンバイ プロファイル	514
XMPP 標準への準拠	515
設定変更通知およびサービス再起動通知	516



第 1 部

システムを計画します

- [システムを計画します \(1 ページ\)](#)



第 1 章

システムを計画します

- [IM and Presence サービスの概要 \(1 ページ\)](#)
- [計画の概要 \(5 ページ\)](#)
- [導入の計画 \(5 ページ\)](#)
- [機能展開オプション \(7 ページ\)](#)
- [標準導入 vs 中央クラスタ \(10 ページ\)](#)
- [マルチノードの拡張性機能 \(10 ページ\)](#)
- [WAN の導入 \(14 ページ\)](#)
- [SAML シングル サインオン展開 \(16 ページ\)](#)
- [サードパーティ統合 \(16 ページ\)](#)
- [サードパーティクライアント統合 \(17 ページ\)](#)

IM and Presence サービスの概要

IM and Presence サービスの管理は、IM and Presence サービスノードに対して個別に手動で設定を変更できる Web ベースのアプリケーションです。このガイドの手順では、このアプリケーションを使用して機能を設定する方法について説明します。

IM and Presence サービスでは多彩な機能を持つ Cisco Jabber Unified Communications クライアント、または XMPP 準拠のサードパーティ製 IM and presence クライアントのいずれかを選択できます。IM and Presence サービスは、インスタントメッセージング、ファイル転送も提供し、永続的なグループチャットルームをホストおよび構成する機能を備えています。

IM and Presence サービスおよび Cisco Unified Communications Manager によるオンプレミス展開では、以下のサービスが使用可能です。

- プレゼンス
- インスタントメッセージング
- ファイル転送
- 音声接続 (Audio Calls)
- ビデオ

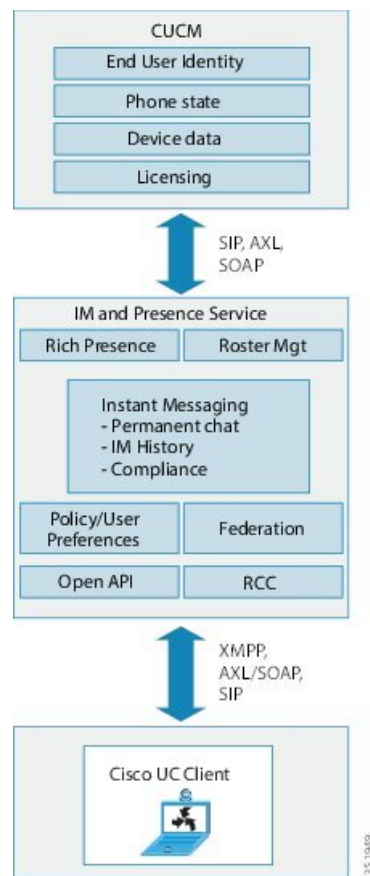
- ボイスメール (Voicemail)
- 会議

詳細については、[Cisco Unified Communications Manager のマニュアル](#)を参照してください。

IM and Presence Service のコンポーネント

次の図は、主なコンポーネントや Cisco Unified Communications Manager と IM and Presence Service 間のインターフェイスなど、IM and Presence Service 展開の概要を示します。

図 1: IM and Presence Service の基本的な展開



SIP インターフェイス

SIP インターフェイスを有効にするには、次の設定を行う必要があります。

- Cisco Unified Communications Manager のプレゼンス情報交換のためにはIM and Presence サーバを指すように SIP トランクを設定する必要があります。
- IM and Presence で、Cisco Unified Communications Manager をプレゼンス ゲートウェイとして設定すると、IM and Presence サービスはSIP トランクを介して SIP SUBSCRIBE メッセージを Cisco Unified Communications Manager に送信できます。

AXL/SOAP インターフェイス

AXL/SOAP インターフェイスは、Cisco Unified Communications Manager からのデータベースの同期を処理し、IM and Presence Service データベースにデータを入力します。データベース同期をアクティブにするには、Cisco Sync Agent ネットワーク サービスが実行されている必要があります。

Sync Agent は、デフォルトでは IM and Presence サービス クラスタ内のすべてのノードにわたるすべてのユーザを等しくロードバランシングします。しかし、クラスタ内の特定のノードにユーザを手動で割り当てることもできます。

シングルおよびデュアルノードの IM and Presence Service で Cisco Unified Communications Manager とのデータベース同期を実行する場合の推奨される同期化間隔については、IM and Presence Service の SRND マニュアルを参照してください。



(注) AXL インターフェイスは、アプリケーション開発者の連携動作がサポートされていません。

LDAP インターフェイス

Cisco Unified Communications Manager は、すべてのユーザ情報を手動設定または LDAP を介した直接同期によって取得します。IM and Presence Service は、Cisco Unified Communications Manager からこのユーザ情報をすべて同期します (AXL/SOAP インターフェイスを使用)。

IM and Presence Service は、Cisco Jabber クライアントのユーザの LDAP 認証および IM and Presence Service ユーザ インターフェイスを提供します。Cisco Jabber ユーザが IM and Presence Service にログインし、LDAP 認証が Cisco Unified Communications Manager で有効になっている場合、IM and Presence Service はユーザー認証用の LDAP ディレクトリに直接移動します。ユーザが認証されると、IM and Presence Service は Cisco Jabber にこの情報を転送し、ユーザログインを続行します。

XMPP インターフェイス

XMPP 接続は、XMPP ベースのクライアントのプレゼンス情報交換やインスタントメッセージ動作を処理します。IM and Presence サービスは、XMPP ベースのクライアントの一時的 (アドホック) および永続的 (常設) チャットルームをサポートします。IM ゲートウェイは、IM and Presence サービス展開における SIP ベースのクライアントと XMPP ベースのクライアント間の IM 相互運用性をサポートします。

CTI インターフェイス

CTI (コンピュータテレフォニーインテグレーション) インターフェイスは、IM and Presence ノードにおけるユーザのすべての CTI 通信を処理して、Cisco Unified Communications Manager 上の電話機を制御します。CTI 機能を使用すると、Cisco Jabber クライアントのユーザはデスクフォン制御モードでアプリケーションを実行できます。

CTI 機能は、Microsoft Lync for Remote Call Control(RCC) の IM and Presence サービス統合にも使用されます。詳細は、*Microsoft Lync Server* を使用した、*IM and Presence* サービスのリモート通話コントロールをご覧ください。

Cisco Unified Communications Manager の IM and Presence Service ユーザの CTI 機能を設定するには、ユーザが CTI 対応グループに関連付けられ、そのユーザに割り当てられているプライマリ内線が CTI に対応している必要があります。

Cisco Jabber デスクフォン制御を設定するには、CTI サーバおよびプロファイルを設定し、そのプロファイルにデスクフォンモードでアプリケーションを使用するユーザを割り当てる必要があります。ただし、すべての CTI 通信は Cisco Unified Communications Manager と Cisco Jabber の間で直接実行され、IM and Presence Service サーバを介しません。

Cisco IM and Presence Data Monitor サービス

Cisco IM and Presence Data Monitor は IM and Presence サービスの IDS 複製状態をモニタします。他の IM and Presence サービスは Cisco IM and Presence データモニタに依存しているため、IDS 複製が安定した状態になるまで起動を遅らせることができます。

Cisco IM and Presence Data Monitor は、Cisco Unified Communications Manager から Cisco Sync Agent の同期のステータスをチェックします。依存サービスは、IDS の複製が設定され、IM and Presence データベースパブリッシャノードの Sync Agent が Cisco Unified Communications Manager からの同期を完了させた後にのみ、起動できます。タイムアウトになると、IDS の複製と Sync Agent が完了していなくても、パブリッシャノードの Cisco IM and Presence Data Monitor は依存サービスの起動を許可します。

サブスクライバノードで、IDS の複製が正常に確立されるまで、Cisco IM and Presence Data Monitor は機能サービスの起動を遅らせます。Cisco IM and Presence Data Monitor は、クラスタ内の問題のあるサブスクライバノードのみで機能サービスの開始を遅らせます。問題があるノードが 1 台あるからといって、すべてのサブスクライバノードで機能サービスの開始を遅らせることはありません。たとえば、IDS の複製が node1 および node2 で正常に確立されたが、node3 では確立されない場合、Cisco IM and Presence Data Monitor により、機能サービスは node1 および node2 で開始できますが、node3 では機能サービスの開始が遅れます。

Cisco IM and Presence Data Monitor は、IM and Presence データベースパブリッシャノードで異なる動作をします。Cisco UP Replication Watcher サービスは、タイムアウトが発生するまで機能サービスの開始を遅らせます。タイムアウトが発生すると、IDS の複製が正常に確立されていなくても、パブリッシャノード上ですべての機能サービスの開始を許可します。

ノードの機能サービスの起動を遅らせる場合は、Cisco IM and Presence Data Monitor がアラームを生成します。次に、IDS の複製がそのノードで正常に確立されたときに通知を生成します。

Cisco IM and Presence Data Monitor は、新しいマルチノードインストールと、ソフトウェアアップグレード手順の両方に影響します。パブリッシャノードおよびサブスクライバノードが同じ IM and Presence リリースを実行し、IDS の複製がサブスクライバノードで正常に確立された場合にのみ両方が完了します。

ノードの IDS 複製のステータスを確認するには、次の手順を実行します。

- CLI コマンド `utils dbreplication runtimestate` を実行する

- Cisco Unified IM and Presence Reporting Tool を使用します。「IM and Presence Database Status」レポートに、クラスタの詳細なステータスが表示されます。

Cisco Sync Agent のステータスを確認するには、Cisco Unified CM IM and Presence の管理インターフェイスに移動し、[診断 (Diagnostics)] > [システム ダッシュボード (System Dashboard)] を選択します。Cisco Unified Communications Manager パブリッシャ ノードの IP アドレスと同期ステータスを検索します。

計画の概要

システムを設定する前に、システムの配置方法を計画していることを確認してください。IM and Presence サービスには、さまざまな企業のニーズを満たすように設計されたさまざまな展開オプションがあります。

ニーズを満たす IM and Presence サービスの展開を含む Cisco Collaboration システムを設計する方法の詳細については、次の URL を参照してください。*Cisco Collaboration System Solution Reference Network Design*<http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html>。

導入の計画

システムを設定する前に、必ずクラスタトポロジとシステムの配置方法を計画してください。

手順

	コマンドまたはアクション	目的
ステップ 1	コラボレーションの導入規模を決定する	詳細については、 http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html にて『Cisco Collaboration System Solution Reference Network Design Guide』の「Collaboration Solution Sizing Guidance」の章を参照してください。
ステップ 2	どの機能をデプロイするかを決めます。	詳細については、 機能展開オプション (7 ページ) を参照してください。
ステップ 3	標準展開と IM and Presence 中央クラスタ展開のどちらをインストールするかを決定します	IM and Presence サービスをテレフォニーと同じクラスタに展開するのか、それとも IM and Presence 向けの集中型クラスタを展開するのかを決定します。詳細については、「標準展開 vs 中央クラスタ」

	コマンドまたはアクション	目的
		標準導入 vs 中央クラスタ (10 ページ) を参照してください。
ステップ 4	展開するクラスターノード数を計画します。	IM and Presence マルチノードスケラビリティ機能を使用すると、ニーズに合わせて展開の規模を調整できます。詳細については、マルチノードの拡張性の要件 (10 ページ) を参照してください。
ステップ 5	冗長性を追加する方法を計画します。	展開の拡張性オプション (11 ページ)
ステップ 6	地理的なサイトを計画する	ハードウェアを1か所から保守するために、1か所に設置できます。ただし、WAN を介してクラスタを展開して、複数のサイトを展開することで地理的な冗長性を追加することもできます。詳細については、次の項を参照してください。 <ul style="list-style-type: none"> • WAN 経由のクラスタ内展開 (14 ページ) • WAN 経由のクラスタ間展開 (15 ページ)
ステップ 7	SAML シングルサインオンを設定するかどうかを決定します。	詳細については、SAML シングルサインオン展開 (16 ページ) を参照してください。
ステップ 8	サードパーティ製のアプリケーションと統合するかどうかを決めます。	これには、Microsoft Outlook の予定表の統合、およびサードパーティシステムとの連携が含まれます。詳細については、サードパーティ統合 (16 ページ) を参照してください。

IM and Presence サービスの展開の規模

コラボレーション展開の規模を決める方法については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html>で『Cisco Collaboration System Solution Reference Network Design』の「Collaboration Solution Sizing Guidance」を参照してください。

機能展開オプション

IM and Presence Service をインストールし、基本的な展開でユーザを設定した後に使用できる主な機能には、基本 IM、可用性、アドホック グループ チャットの機能があります。

オプション機能を追加することで、基本的な展開を拡張できます。次の図に、IM and Presence Service の機能展開オプションを示します。

次の表に、IM and Presence Service の機能展開オプションのリストを示します。

表 1: IM and Presence サービスの機能展開オプション

コア IM とアベイラビリティ機能	高度な IM 機能 (オプション)	豊富な Unified Communications アベイラビリティ機能 (オプション)	リモート デスク フォン制御 (オプション)
ユーザ アベイラビリティの表示 リッチテキスト IM のセキュアな送受信 ファイル転送 アドホック グループ チャット 連絡先の管理 ユーザの履歴 Cisco Jabber のサポート 複数のクライアント デバイスのサポート : Microsoft windows、MAC、Mobile、タブレット、IOS、Android、BB Microsoft Office の統合 LDAP ディレクトリの統合 個人用ディレクトリおよび友人リスト オープン API システム トラブルシューティング		Cisco テレフォニーのアベイラビリティ Microsoft Outlook の予定表の統合 (オンプレミスの Exchange またはホスティングされた Office 365 の展開)	リモート Cisco IP 電話制御 リモート ソフトフォン コントロール Microsoft Remote Call Control の統合

コア IM とアベイラビリティ機能	高度な IM 機能 (オプション)	豊富な Unified Communications アベイラビリティ機能 (オプション)	リモートデスクフォン制御 (オプション)
	<p>常設チャット</p> <p>マネージドファイル転送</p> <p>メッセージアーカイバ</p> <p>サードパーティ製 XMPP クライアントのサポートのカレンダー</p> <p>高可用性</p> <p>拡張性：WAN 経由のマルチノードサポートおよびクラスタリング</p> <p>クラスタ間ピアリング</p> <p>企業連携：</p> <ul style="list-style-type: none"> • IM and Presence サービスの統合 • Cisco Webex Messenger の統合 • Business/Office365 サーバー統合向け Microsoft Lync/Skype • IBM SameTime の統合 • Cisco Jabber XCP <p>パブリック連携：</p> <ul style="list-style-type: none"> • Google Talk、AOL の統合 • XMPP サービスまたは BOT • サードパーティの Exchange サービスの統合 <p>IM コンプライアンス</p> <p>SAML シングルサインオン</p> <p>カスタム ログインバナー</p>		

標準導入 vs 中央クラスタ

システムをインストールする前に、IM and Presence サービスの標準配置を導入するか、IM and Presence サービスの中央クラスタを使用するかを決定する必要があります。

- Cisco Unified Communications Manager 上の IM and Presence サービス（標準配置）：標準配置では、IM and Presence サービスクラスタは Cisco Unified Communications Manager テレフォニーノードと同じサーバにインストールされます。IM and Presence クラスタは、テレフォニークラスタと同じプラットフォームおよび多くの同じサービスを共有します。このオプションでは、テレフォニークラスタと IM and Presence クラスタとの 1×1 マッピングが必要です。
- 集中型 IM and Presence クラスタ：この配置では、IM and Presence サービスクラスタはテレフォニークラスタとは別にインストールされます。トポロジの計画方法によっては、IM and Presence 中央クラスタをテレフォニークラスタとは全く別のハードウェアサーバーにインストールすることができます。この導入オプションでは、テレフォニークラスタと IM and Presence クラスタの 1 対 1 のマッピング要件が削除され、それぞれの展開の種類をニーズに応じて適切に拡張できます。



(注) IM and Presence 中央クラスタには、Cisco Unified Communications Manager のインスタンスがいまだに含まれています。ただし、このインスタンスは、データベースやプロビジョニング向けのもので、テレフォニーを処理するものではありません。テレフォニー統合では、IM and Presence 中央クラスタは別の Cisco Unified Communications Manager テレフォニークラスタに接続する必要があります。

このドキュメントに記載の手順は、標準的な展開と中央クラスタ展開の両方に使用できます。ただし、中央クラスタを展開する場合は、[集中展開の設定 \(115ページ\)](#) のタスクも完了して、テレフォニークラスタと IM and Presence クラスタを適切に配置する必要があります。

マルチノードの拡張性機能

マルチノードの拡張性の要件

IM and Presence サービスはマルチノードの拡張性をサポートします。

- クラスタあたり 6 個のノード
- 完全な Unified Communication (UC) モード展開でノードあたり最大 25,000 ユーザを持つクラスタあたり 75,000 ユーザ
- プレゼンス冗長グループでクラスタあたり 25,000 ユーザ、およびハイアベイラビリティの展開でクラスタあたり 75,000 ユーザ。

- ユーザあたりの最大連絡先の管理可能なカスタマー定義制限（デフォルトは無制限）
- IM and Presence サービスはマルチノード機能をもつクラスタ間展開をサポートしています。

OVA の要件

以下の OVA 要件が適用されます。

- クラスタ間環境では、最小限の OVA を 15,000 ユーザに導入することを推奨します。すべてのクラスタが少なくとも 15,000 ユーザが OVA を実行している限り、複数のクラスタを異なる OVA のサイズで実行することが可能です。
- 常設チャットの展開には、少なくとも 15,000 ユーザ OVA を導入することを推奨します。
- 中央集中型の導入の場合は、最小 OVA 15,000 ユーザと、25,000 ユーザ IM and Presence OVA を推奨します。15,000 ユーザ OVA は、25000 ユーザにまで拡張できます。25K OVA テンプレートと高可用性を有効にした 6 ノードクラスタでは、IM and Presence サービスの中央展開で最大 75,000 のクライアントをサポートしています。25K OVA で 75K ユーザをサポートするには、XCP ルータのデフォルト トレース レベルを [情報 (Info)] から [エラー (Error)] に変更する必要があります。中央クラスタのユニファイドコミュニケーション マネージャー パブリッシュ ノードでは、次の要件が適用されます。
 - 25000 IM およびプレゼンス OVA (最大75000ユーザ) は、中央クラスタのユニファイドコミュニケーション マネージャー パブリッシュ ノードにインストールされた1万 ユーザ OVA を使用して展開できます。
 - 15000 IM およびプレゼンス OVA (最大45,000ユーザ) は、中央クラスタのユニファイドコミュニケーション マネージャー パブリッシュ ノードにインストールされた 7500 ユーザ OVA を使用して展開できます。



- (注) Multiple Device Messaging を有効にする場合は、各ユーザが複数の Jabber クライアントを持つ可能性があるため、ユーザ数ではなくクライアント数に応じた展開にします。たとえば、ユーザ数が 25,000 人で、各ユーザが 2 台の Jabber クライアントを保持している場合、導入環境には 5 万ユーザのキャパシティが必要となります。

拡張性は、展開内のクラスタの数によって異なります。VM の設定要件および OVA テンプレートの詳細については、次の URL で、「*Virtualization for Unified CM IM and Presence*」を参照してください。https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html

展開の拡張性オプション

IM and Presence Service クラスタは、最大 6 台のノードをサポートできます。最初に 6 台未満のノードをインストールした場合は、追加ノードをいつでもインストールできます。より多くの

ユーザをサポートするためにIM and Presence展開を拡張する場合、設定したマルチノード展開モデルを考慮する必要があります。次の表で、各マルチノード展開モデルの拡張性オプションについて説明します。

表 2:

構成モード	拡張性オプション	
	既存のプレゼンス冗長グループへの新しいノードの追加	新しいプレゼンスへの新しいノードの追加 冗長グループ
平衡型非冗長ハイ アベイラビリティ展開	既存のプレゼンス冗長グループに新しいノードを追加すると、新しいノードが既存のノードと同じ数のユーザをサポートできます。プレゼンス冗長グループは、ユーザの数の2倍をサポートできます。また、そのプレゼンス冗長グループ内の既存のノードと新しいノードのユーザに平衡型ハイ アベイラビリティを提供します。	新しいプレゼンス冗長グループに新しいノードを追加すると、展開でより多くのユーザをサポートできます。 これはプレゼンス冗長グループ内のユーザに平衡型ハイ アベイラビリティを提供しません。平衡型ハイ アベイラビリティを実現するには、プレゼンス冗長グループに2番目のノードを追加する必要があります。

構成モード	拡張性オプション	
	既存のプレゼンス冗長グループへの新しいノードの追加	新しいプレゼンスへの新しいノードの追加 冗長グループ
平衡型冗長ハイ アベイラビリティ展開	<p>既存のプレゼンス冗長グループに新しいノードを追加すると、新しいノードが既存のノードと同じユーザをサポートできます。たとえば、既存のノードが5,000人のユーザをサポートする場合、新しいノードは同じ5,000人のユーザをサポートします。また、そのプレゼンス冗長グループ内の既存のノードと新しいノードのユーザに平衡型冗長ハイアベイラビリティを提供します。</p> <p>(注) 既存のノード上のユーザ数に応じて、プレゼンス冗長グループ内でのユーザの再割り当てが必要になることがあります。</p>	<p>新しいプレゼンス冗長グループに新しいノードを追加すると、展開でより多くのユーザをサポートできます。</p> <p>これはプレゼンス冗長グループ内のユーザに平衡型ハイアベイラビリティを提供しません。平衡型ハイアベイラビリティを実現するには、プレゼンス冗長グループに2番目のノードを追加する必要があります。</p>
アクティブ/スタンバイ冗長ハイアベイラビリティ展開	<p>既存のプレゼンス冗長グループに新しいノードを追加すると、プレゼンス冗長グループの既存のノードのユーザにハイアベイラビリティが提供されます。これは、ハイアベイラビリティ拡張機能だけを提供します。展開でサポートできるユーザ数は増えません。</p>	<p>新しいプレゼンス冗長グループに新しいノードを追加すると、展開でより多くのユーザをサポートできます。</p> <p>これはプレゼンス冗長グループ内のユーザにハイアベイラビリティを提供しません。ハイアベイラビリティを実現するには、プレゼンス冗長グループに2番目のノードを追加する必要があります。</p>

WAN の導入

IM and Presence サービスは、クラスタ内およびクラスタ間展開両方における WAN 経由のクラスタリング展開をサポートします。このオプションを使用すると、配置に地理的な冗長性を追加できます。

WAN 経由のクラスタ内展開

IM and Presence Service では、このモジュールに記載された推奨帯域幅を使用した WAN 経由のクラスタ内展開をサポートしています。IM and Presence Service では、プレゼンス冗長グループ内の 1 つのノードが 1 つの地理的なサイトに存在し、プレゼンス冗長グループ内の 2 番目のノードが別の地理的な場所にあるような、WAN 上で地理的に分割された単一のプレゼンス冗長グループをサポートします。

このモデルは、地理的な冗長性およびリモート フェールオーバー（たとえば、リモートサイトのバックアップ IM and Presence Service ノードへのフェールオーバー）を提供できます。このモデルでは、IM and Presence Service ノードを Cisco Unified Communications Manager データベースパブリッシュ ノードと共存させる必要はありません。Cisco Jabber クライアントは、IM and Presence Service ノードに対してローカルまたはリモートからアクセスできます。

このモデルは、クライアントのハイ アベイラビリティをサポートし、サービスまたはハードウェアがホームの IM and Presence Service ノードで失敗した場合、クライアントはリモートピアの IM and Presence Service ノードにフェールオーバーします。障害が発生したノードが再度オンラインになると、クライアントはホームの IM and Presence Service ノードに自動的に再接続します。

WAN 経由でリモート フェールオーバーを備えた IM and Presence Service を展開する場合は、次の制約事項に注意してください。

- このモデルは、システム レベルのハイ アベイラビリティのみをサポートします。特定の IM and Presence Service コンポーネントに、シングルポイント障害が存在する場合があります。これらのコンポーネントは、Cisco Sync Agent、Cisco Intercluster Sync Agent、および Cisco Unified CM IM and Presence の管理インターフェイスです。

IM and Presence Service は、WAN 経由のクラスタリング展開において複数のプレゼンス冗長グループをサポートします。WAN 経由のクラスタリング展開の規模については、IM and Presence Service SRND を参照してください。

詳細については、*IM and Presence Service Solution Reference Network Design* (SRND) を参照してください。

WAN 経由の展開のマルチノード設定

WAN 経由のクラスタ内展開用に IM and Presence Service のマルチノード機能を設定する場合は、マルチノードの項で説明するように IM and Presence Service プレゼンス冗長グループ、ノード、およびユーザー割り当てを設定します。ただし、次の推奨事項に注意してください。

- 最適なパフォーマンスを得るため、ホームの IM and Presence Service ノードにユーザの大部分を割り当てることを推奨します。この展開モデルでは、WAN 経由でリモート IM and Presence Service ノードに送信されるメッセージの量が少なくなりますが、セカンダリ ノードへのフェールオーバー時間は、フェールオーバーするユーザの数によって異なります。
- WAN 経由のハイ アベイラビリティ展開モデルを設定する場合は、プレゼンス冗長グループ全体の DNS SRV アドレスを設定できます。この場合、IM and Presence Service は、DNS SRV で指定されたノードへの最初の PUBLISH 要求メッセージを送信し、応答メッセージは、ユーザのホストノードを示します。IM and Presence Service はホストノードにそのユーザに対する後続の PUBLISH メッセージをすべて送信します。このハイ アベイラビリティの展開モデルを設定する前に、WAN 経由で送信される可能性があるメッセージの量に十分な帯域幅があるかどうかを検討する必要があります。

WAN 経由のクラスタ間展開

IM and Presence Service では、このモジュールに記載された推奨帯域幅を使用した WAN 経由のクラスタ間展開をサポートしています。クラスタ間配置を配置するときに考慮事項が適用されます。

- クラスタ間ピア - クラスタ間ピアと呼ばれる、スタンドアロンの IM and Presence サービス クラスタを相互接続するピア関係を設定できます。このクラスタ間ピアの機能を使用すると、ある IM and Presence Service クラスタ内のユーザは、同じドメイン内のリモート IM and Presence Service クラスタのユーザのアベイラビリティ情報を通信およびサブスクライブできます。クラスタ間ピアの設定方法については、[クラスタ間ピアの設定 \(187ページ\)](#)を参照してください。
- ノード名 - 任意の IM and Presence サービス ノードに定義したノード名は、すべてのクラスタ内の他のすべての IM and Presence サービス ノードで解決可能でなければなりません。したがって、各 IM and Presence Service ノード名はノードの FQDN である必要があります。ネットワークに DNS が展開されていない場合は、各ノード名が IP アドレスである必要があります。
- IM アドレス スキーム - クラスタ間展開の場合、各クラスタ内のすべてのノードは同じ IM アドレス スキームを使用する必要があります。あるクラスタ内のいずれかのノードが、リリース 10 以前のあるバージョンの IM and Presence Service を実行している場合、下位互換性のために、すべてのノードが UserID@Default_Domain の IM アドレス スキームを使用するように設定する必要があります。
- ルーターツルーター通信 - デフォルトでは、IM and Presence サービスは、クラスタ間ルーターツルーター コネクタとしてクラスタ内のすべてのノードを割り当てます。IM and Presence Service は、AXL インターフェイスを介してクラスタ間にクラスタ間ピア接続を確立すると、ホームおよびリモートクラスタのすべてのクラスタ間ルーターツルーター コネクタ ノードからの情報を同期化します。

ローカルクラスタ内の各ルーター間コネクタノードとリモートクラスタ内の各ルーターコネクタノード間の接続を保護するために TLS を使用する安全なルーター間通信を設定することもできます。

SAML シングル サインオン展開

セキュリティアサーションマークアップ言語 (SAML) シングルサインオン機能を使用すると、管理ユーザは、IM and Presence サービスを含む複数の Cisco Collaboration アプリケーションのいずれか1つのみにサインインした後、それらのアプリケーションにアクセスできます。この機能は、次のようにして管理者の仕事を簡素化します。

- シングルサインイン後に多数の Cisco Collaboration アプリケーションにアクセスするには、シングルログインが必要です。
- 必要なパスワードは1つだけです - アプリケーションごとに異なるパスワードを覚えておく必要はもうありません。
- 管理者は、すべてのパスワードと認証を単一の ID プロバイダー (IdP) から管理できます。

SAML シングルサインオンを設定および構成する方法の詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>でCisco Unified Communications ソリューション用 SAML SSO 導入ガイドをご覧ください。

サードパーティ統合

IM and Presence サービスは、さまざまなサードパーティシステムと統合されています。次の表は、統合の概要を記載し、その構成方法を説明しているドキュメントへのリンクを示しています。

マニュアルのタイトル	このマニュアルの構成
IM and Presence サービス用 Microsoft Outlook の予定表統合	IM and Presence ユーザのプレゼンスステータスで Microsoft Outlook からの予定表情報を使用するために、オンプレミスの Microsoft Exchange サーバまたはホスティングされた Office 365 サーバと接続するように IM and Presence サービスを設定します。

マニュアルのタイトル	このマニュアルの構成
IM and Presence サービスのドメイン間フェデレーション	<p>次のシステムとのドメイン間フェデレーション用に IM and Presence サービスを設定します。これにより、IM and Presence ユーザは他のシステム上のユーザと IM and Presence を交換できます。</p> <ul style="list-style-type: none"> • Microsoft Lync • Microsoft Skype for Business • Microsoft Office 365 • GoogleTalk • AOL • IBM SameTime • Cisco Webex Messenger • 他の IM and Presence サービス企業
IM and Presence サービスのパーティションイントラドメインフェデレーション	<p>パーティション化されたドメイン間フェデレーションの Microsoft Lync または Skype for Business との IM and Presence サービスの設定。この統合を使用して、ユーザを IM and Presence サービスに移行している間も、ネットワーク内の通信を維持できます。</p>
Microsoft Lync Server を使用した、IM and Presence サービスのリモート通話コントロール	<p>Microsoft Lync for Microsoft Remote Call Control(RCC) と統合するための Cisco Unified Communications Manager および IM and Presence サービスの設定。この統合を使用すると、企業ユーザが Microsoft Lync (サードパーティ製デスクトップインスタントメッセージング (IM) アプリケーション) 経由で Cisco Unified IP Phone または Cisco IP Communicator Phone を制御できるようになります。</p>

サードパーティクライアント統合

このセクションでは、サードパーティクライアント統合のためのいくつかの要件について概説します。

サポートされているサードパーティ製 XMPP クライアント

IM and Presence Service は、アベイラビリティおよびインスタントメッセージ (IM) サービスのためにサードパーティ製 XMPP クライアントアプリケーションを IM and Presence Service と統合できるように、標準ベースの XMPP をサポートしています。サードパーティ製 XMPP クライアントが、Cisco ソフトウェア開発キット (SDK) にある標準ベースの XMPP に準拠している必要があります。

このモジュールでは、XMPP クライアントを IM and Presence Service と統合するための設定要件について説明します。XMPP ベースの API (Web) クライアントアプリケーションを IM and Presence Service と統合する場合は、Cisco Developer ポータルにある IM and Presence Service の開発者マニュアルを参照してください。

<http://developer.cisco.com/>

ライセンス要件

XMPP クライアントアプリケーションのユーザごとに IM and Presence Service 機能を割り当てる必要があります。IM and Presence 機能は、User Connect Licensing (UCL) と Cisco Unified Workspace Licensing (CUWL) の両方に含まれています。

ライセンスについての詳細は、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html> で『*System Configuration Guide for Cisco Unified Communications Manager*』の「Smart Software Licensing」の章を参照してください。

Cisco Unified Communications Manager での XMPP クライアント統合

XMPP クライアントを統合する前に、Cisco Unified Communications Manager で次のタスクを実行します。

- ライセンス要件を設定します。
- ユーザとデバイスを設定します。デバイスを各ユーザに関連付け、ユーザをラインアピアランスに関連付けます。

XMPP 連絡先検索のための LDAP 統合

XMPP クライアントアプリケーションのユーザが LDAP ディレクトリから連絡先を検索および追加できるようにするには、IM and Presence サービスで XMPP クライアントのサードパーティー LDAP 設定を実行します。

XMPP クライアントの DNS 設定

XMPP クライアントを IM and Presence Service と統合する場合は、展開内の DNS SRV を有効にする必要があります。XMPP クライアントは、DNS SRV クエリを実行して、通信する XMPP ノード (IM and Presence Service) を検索し、XMPP ノードのレコードルックアップを実行して IP アドレスを取得します。



(注) IM and Presence Service の展開で複数の IM ドメインを設定した場合は、各ドメインに DNS SRV レコードが必要です。すべての SRV レコードは、同じ結果セットに解決できます。



第 II 部

システムの設定

- [ドメインの設定 \(21 ページ\)](#)
- [IPv6 の設定 \(35 ページ\)](#)
- [IM アドレッシングスキームの設定 \(41 ページ\)](#)
- [冗長性およびハイアベイラビリティの設定 \(53 ページ\)](#)
- [ユーザ設定値の設定 \(77 ページ\)](#)
- [LDAP ディレクトリの設定 \(83 ページ\)](#)
- [IM and Presence サービス用に Cisco Unified Communications Manager を設定します \(105 ページ\)](#)
- [集中展開の設定 \(115 ページ\)](#)
- [高度なルーティングを設定する \(139 ページ\)](#)
- [証明書の設定 \(153 ページ\)](#)
- [セキュリティ設定の構成 \(175 ページ\)](#)
- [クラスタ間ピアの設定 \(183 ページ\)](#)
- [プッシュ通知の設定 \(195 ページ\)](#)



第 2 章

ドメインの設定

- [ドメイン設定の概要 \(21 ページ\)](#)
- [ドメイン前提条件の設定 \(24 ページ\)](#)
- [ドメインタスクフローの設定 \(25 ページ\)](#)

ドメイン設定の概要

[IM and Presence ドメイン (IM and Presence Domain)] ウィンドウに次のタイプのドメインが表示されます。

- 管理者が管理する IM アドレス ドメイン。これらは、手動で追加済であるが、どのユーザにも割り当てられていない内部ドメインか、Sync Agent によって自動的に追加されたが、その後でユーザのドメインが変更されたために使用されていない内部ドメインです。
- システムが管理する IM アドレス ドメイン。これらは、ユーザが展開で使用し、手動または自動のいずれでも追加できる内部ドメインです。

ドメインが [IM and Presence ドメイン (IM and Presence Domain)] ウィンドウに表示されている場合は、ドメインは有効になっています。ドメインを有効にする必要はありません。ローカルの IM アドレスドメインを手動で追加、更新、削除できます。

2 個のクラスタでドメインを設定することはできますが、ピアクラスタのみで使用されている場合に限りです。これは、ローカルクラスタのシステムが管理するドメインとして表示されますが、ピアクラスタで使用中等であると識別されます。

Cisco Sync Agent サービスが夜間監査を実行し、ローカルクラスタ、およびクラスタ間が設定されている場合はピアクラスタの各ユーザのディレクトリ URI を確認して、一意のドメインのリストを自動的に構築します。クラスタ内のユーザにドメインが割り当てられると、そのドメインは管理者管理からシステム管理に変わります。クラスタ内のユーザがドメインを使用しなくなった場合は、ドメインは管理者が管理するドメインに戻ります。

ドメイン設定例

Cisco Unified Communications Manager IM and Presence Service は、任意の数の DNS ドメインへの柔軟なノード展開をサポートします。この柔軟性をサポートするには、展開内のすべての IM and Presence サービス ノードにそのノードの完全修飾ドメイン名 (FQDN) に設定されたノード名が必要です。IM and Presence サービス用の次のサンプルノード展開オプションについて、以下に説明します。

- 異なる DNS ドメインとサブドメインを持つ複数のクラスタ
- 異なる DNS ドメインまたはサブドメインを持つ単一のクラスタ
- DNS ドメインが Unified Communications Manager ドメインと異なる単一クラスタ

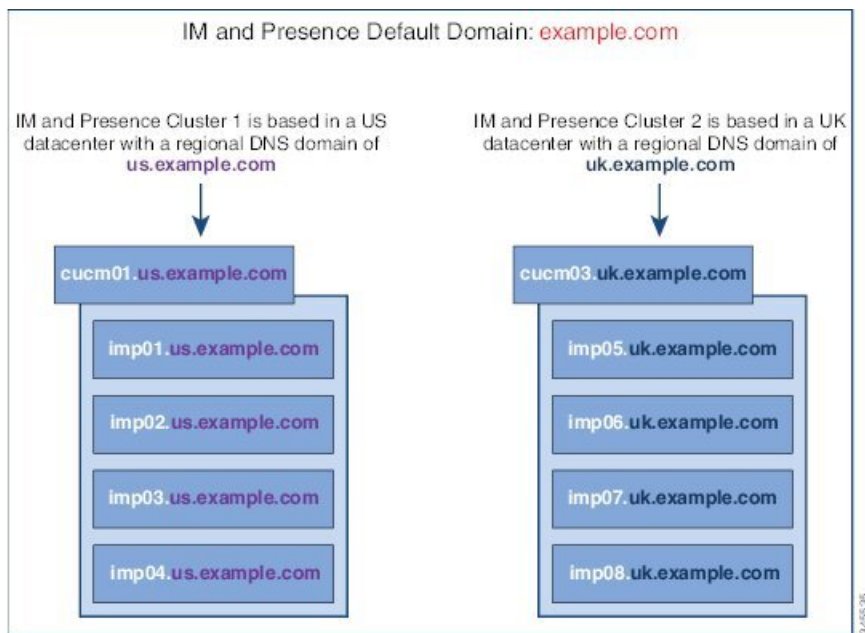


(注) ある IM and Presence サービス ノード名がホスト名だけに基いている場合、すべての IM and Presence サービス ノードが同じ DNS ドメインを共有する必要があります。

システムによって、IM and Presence サービスのデフォルト ドメインまたは DNS ドメインと一致するように設定される他の IM ドメインは必要はありません。IM and Presence サービス展開に共通のプレゼンスドメインを配置し、ノードを複数の DNS ドメインに展開できます

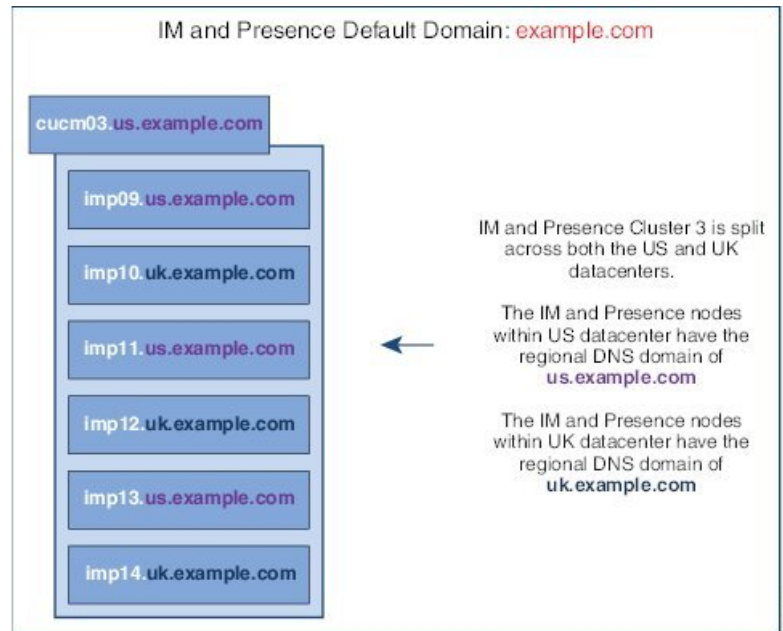
異なる DNS ドメインとサブドメインを持つ複数のクラスタ

IM and Presence Service は、ピアの IM and Presence Service クラスタを構成するノードとは異なる DNS ドメインまたはサブドメイン内の 1 つの IM and Presence Service クラスタに関連付けられたノードをサポートします。次の図に、サポートされている展開シナリオの例を示します。



異なる DNS ドメインまたはサブドメインを持つ単一のクラスター

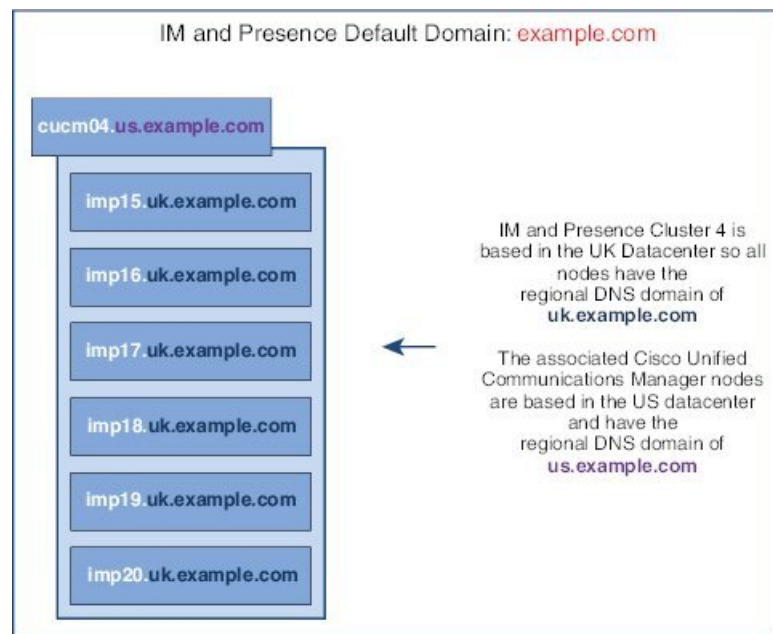
IM and Presence Service は、複数の DNS ドメインまたはサブドメインに展開された IM and Presence Service クラスター内へのノードの配置をサポートします。次の図に、サポートされている展開シナリオの例を示します。



(注) ハイ アベイラビリティは、プレゼンス冗長グループ内の 2 台のノードが別々の DNS ドメインまたはサブドメインにあるシナリオでも完全にサポートされます。

DNS ドメインが Unified Communications Manager ドメインと異なる単一クラスター

IM and Presence Service は、関連する Cisco Unified Communications Manager クラスとは異なる DNS ドメインへの IM and Presence Service ノードの配置をサポートします。次の図に、サポートされている展開シナリオの例を示します。



- (注) Cisco Unified Communications Manager とのアベイラビリティ統合をサポートするには、**CUCM Domain** の SIP Proxy サービス パラメータが Cisco Unified Communications Manager クラスタの DNS ドメインと一致する必要があります。

デフォルトで、このサービスパラメータは IM and Presence データベース パブリッシャ ノードの DNS ドメインに設定されます。IM and Presence データベース パブリッシャ ノードの DNS ドメインが Cisco Unified Communications Manager クラスタの DNS ドメインと異なる場合、Cisco Unified Communications Manager クラスタのドメインを使用してこのサービスパラメータを編集する必要があります。

ドメイン前提条件の設定

- この機能を使用するには、IM and Presence Service および Cisco Unified Communications Manager のすべてのノードおよびクラスタが複数のドメインをサポートする必要があります。IM and Presence サービス クラスタ内のすべてのノードがリリース 10.0 以降で実行されていることを確認します。
- アドレス指定用にディレクトリ URI を必ず設定してください。詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html> で、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure URI Dialing」を参照してください。

ドメインタスクフローの設定

IM and Presence サービスのドメインを設定するには、次の作業を完了してください。

手順

	コマンドまたはアクション	目的
ステップ 1	ハイ アベイラビリティの無効化 (26 ページ)	高可用性が有効になっている場合は、一時的に無効にする必要があります。デフォルトドメインを変更すると、サービスを一時的に停止する必要があります。高可用性が有効になっている間にサービスを停止すると、システムのフェイルオーバーが発生します。
ステップ 2	IM and Presence サービスの無効化 (26 ページ)	ドメインを変更する前に、重要なサービスを停止してください。
ステップ 3	IM and Presence サービスのデフォルトドメインを設定します (28 ページ)	IM and Presence サービス クラスタのデフォルト ドメイン値を設定します。この手順は DNS または非 DNS 展開両方に適用できます。
ステップ 4	これらのタスクのいずれかを実行してください。 <ul style="list-style-type: none"> IM アドレス ドメインの追加または更新 (29 ページ) IM アドレス ドメインの削除 (30 ページ) 	これはオプションです。これらの作業は、ローカルクラスタの管理者管理ドメインを追加、編集、または削除する場合にのみ実行してください。
ステップ 5	XMPP クライアントおよび TLS 証明書を再生成します (31 ページ)	TLS XMPP フェデレーションを使用している場合、新しい XMPP クライアントおよび TLS 証明書の生成に進みます。
ステップ 6	IM and Presence サービスの開始 (31 ページ)	ドメイン設定が完了したら、サービスを再起動します。
ステップ 7	プレゼンス冗長グループでハイ アベイラビリティを有効化する (32 ページ)	高可用性を設定している場合は、もう一度有効にします。 (注) 高可用性を有効にする前に、開始したサービスがすべてのクラスタノードで実行されていることを確認してください。

ハイアベイラビリティの無効化

高可用性を設定している場合は、デフォルトドメインを設定する前に、各プレゼンス冗長グループでそれを無効にする必要があります。デフォルトのドメイン変更のためにサービスを停止したときに高可用性が有効になっていると、フェイルオーバーが発生します。



(注) [プレゼンス冗長グループの詳細] ページには、クラスタで高可用性が無効になっている場合でも、すべてのアクティブな JSM セッションが表示されます。

始める前に

各プレゼンス冗長グループの各クラスタノードに割り当てられたアクティブユーザ数を記録します。この情報は、[Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] の [システム (System)] > [プレゼンス トポロジ (Presence Topology)] ウィンドウで見つけることができます。後で高可用性を再度有効にするときにこれらの番号が必要になります。

手順

- ステップ 1 Cisco Unified CM Administration のユーザ インターフェイスから、[システム (System)] > [プレゼンス冗長グループ (Presence Redundancy Groups)] を選択します。
- ステップ 2 検索をクリックしてグループを選択します。
- ステップ 3 [プレゼンス冗長グループの設定 (Presence Redundancy Group Configuration)] ウィンドウで、[ハイアベイラビリティを有効にする (Enable High Availability)] チェックボックスをオフにします。
- ステップ 4 [保存 (Save)] をクリックします。
- ステップ 5 各プレゼンス冗長グループに対してこの手順を繰り返します。
- ステップ 6 完了したら、さらに変更を加える前に、新しい HA 設定がクラスタ全体にわたって同期されるまで、少なくとも 2 分待機します。

次のタスク

[IM and Presence サービスの無効化 \(26 ページ\)](#)

IM and Presence サービスの無効化

この手順を使用して、デフォルトドメインに変更を加える前に IM and Presence サービスを停止します。クラスタ内のすべてのノードでこの手順を実行します。

始める前に

高可用性が無効になっていることを確認してください。詳細については、[ハイアベイラビリティの無効化 \(26 ページ\)](#) を参照してください。

手順

-
- ステップ 1** [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
- ステップ 2** [サーバ (Server)] リストから、サービスを非アクティブ化するノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3** **IM and Presence サービス (IM and Presence Services)** で、次のサービスを選択解除します。
- **Cisco Client Profile Agent**
 - **Cisco Sync Agent**
 - **Cisco XCP Router**
- ステップ 4** [Stop] をクリックします。
- ステップ 5** [関連リンク (Related Links)] ドロップダウン リストから [サービスのアクティベーション (Service Activation)] を選択し、[移動 (Go)] をクリックします。
- ステップ 6** **IM and Presence サービス (IM and Presence Services)** で、次のサービスを選択解除します。
- **Cisco SIP Proxy**
 - **Cisco Presence Engine**
- ステップ 7** [保存 (Save)] をクリックします。
- ステップ 8** これらのサービスを無効にしたすべてのノードのリストを作成します。デフォルトドメインへの変更が完了したら、サービスを再起動する必要があります。
-

次のタスク

IM and Presence サービスのデフォルトメインを設定します。

- [IM and Presence サービスのデフォルトメインを設定します \(28 ページ\)](#)

また、デフォルトドメインがすでに設定されている場合は、ドメインを追加、編集、または削除するためにこれらのタスクのいずれかを実行します。

- [IM アドレス ドメインの追加または更新 \(29 ページ\)](#)
- [IM アドレス ドメインの削除 \(30 ページ\)](#)

IM and Presence サービスのデフォルトメインを設定します

このサービスを使用して IM and Presence サービスクラスタのデフォルト ドメイン値を設定します。DNS または非 DNS 展開が存在する場合、この手順を適用できます。

この手順では、IM and Presence Service のクラスタのデフォルト ドメインだけを変更します。そのクラスタ内のすべての IM and Presence Service ノードに関連付けられている DNS ドメインは変更されません。IM and Presence サービス ノードの DNS ドメインを変更する方法の手順については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>で『*Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service*』を参照してください。



- (注) Cisco Unified Communications Manager に IM and Presence Service パブリッシャのノードを追加すると、デフォルト ドメインが設定されます。ノードのインストール中、Cisco Unified Communications Manager からデフォルト ドメイン 値が取得できない場合、デフォルト ドメイン値は「DOMAIN.NOT.SET」にリセットされます。IM and Presence Service のデフォルト ドメイン値を有効なドメイン値に変更するには、この手順を使用します。

始める前に

高可用性が無効になっていること、および不可欠な IM and Presence サービスが停止していることを確認してください。詳細は、[IM and Presence サービスの無効化 \(26 ページ\)](#) を参照してください。

手順

- ステップ 1 IM and Presence サービスのデータベース パブリッシャ ノードにログインします。
- ステップ 2 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[プレゼンス (Presence)] > [設定 (Settings)] > [詳細設定 (Advanced Configuration)] を選択します。
- ステップ 3 [デフォルト ドメイン (Default Domain)] を選択します。
- ステップ 4 [ドメイン名 (Domain Name)] フィールドに、新しいプレゼンス ドメインを入力し、[保存 (Save)] を選択します。

システムアップデートは完了まで最長で1時間かかる場合があります。アップデートに失敗すると、[再試行 (Re-try)] ボタンが表示されます。変更を再適用するには、[再試行 (Re-try)] をクリックします。または [取消 (Cancel)] をクリックします。

次のタスク

TLS XMPP フェデレーションを使用した場合、[XMPP クライアントおよび TLS 証明書を再生成します \(31 ページ\)](#) に進みます。

IM アドレス ドメインの追加または更新

ローカルクラスタで管理者管理ドメインを追加または編集できます。他のクラスタに関連付けられている、システムが管理するかまたは管理者が管理するドメインは編集できません。

システム管理ドメインが使用中であるため、編集できません。その IM アドレス ドメインのシステムにユーザが存在しない場合（たとえば、ユーザが削除された場合）、システム管理ドメインは自動的に管理者の管理ドメインになります。管理者の管理ドメインは編集または削除できます。

始める前に

高可用性が無効になっていること、および不可欠な IM and Presence サービスが停止していることを確認してください。詳細は、[IM and Presence サービスの無効化 \(26 ページ\)](#)

手順

-
- ステップ 1** Cisco Unified CM IM and Presence Administration で、**Presence > > ドメイン**を選択します。
すべての管理者の管理 IM アドレス ドメインとシステム管理 IM アドレス ドメインを表示する [ドメインの検索と一覧 (Find and List Domains)] ウィンドウが表示されます。
 - ステップ 2** 次のいずれかの操作を実行します。
 - [新規追加 (Add New)] をクリックすることで、新しいドメインを追加します。[ドメイン (Domains)] ウィンドウが表示されます。
 - ドメインのリストから編集するドメインを選択します。[ドメイン (Domains)] ウィンドウが表示されます。
 - ステップ 3** 最大 255 文字の一意的なドメイン名を [ドメイン名 (Domain Name)] フィールドに入力し、[保存 (Save)] をクリックします。
各ドメイン名はクラスタ全体で一意的である必要があります。指定できる値は、すべての大文字または小文字 (a-zA-Z)、すべての番号 (0-9)、ハイフン (-)、またはドット (.) です。ドメイン ラベルの区切り文字はドットです。ドメイン ラベルの先頭文字をハイフンにすることはできません。最後のラベル（たとえば、.com）の先頭文字を数字にすることはできません。たとえば、Abc.1om は無効なドメインです。
-

次のタスク

TLS XMPP フェデレーションを使用した場合、[XMPP クライアントおよび TLS 証明書を再生成します \(31 ページ\)](#)に進みます。

IM アドレス ドメインの削除

Cisco Unified CM IM and Presence の管理 GUI を使用して、ローカル クラスタにある管理者の管理 IM アドレス ドメインを削除できます。

システム管理ドメインは使用中のため削除できません。その IM アドレス ドメインのシステムにユーザが存在しない場合（たとえば、ユーザが削除された場合）、システム管理ドメインは自動的に管理者の管理ドメインになります。管理者の管理ドメインは編集または削除できません。



- (注) ローカル クラスタとピア クラスタの両方に設定された管理者の管理ドメインを削除すると、ドメインは管理者の管理ドメインのリストに保持されます。ただし、そのドメインはピアクラスタでのみ設定済みとマークされます。完全にエントリを削除するには、設定されたすべてのクラスタからドメインを削除する必要があります。

始める前に

高可用性が無効になっていること、および不可欠な IM and Presence サービスが停止していることを確認してください。詳細は、[IM and Presence サービスの無効化 \(26 ページ\)](#)を参照してください。

手順

- ステップ 1** Cisco Unified CM IM and Presence Administration で、**Presence > ドメイン**を選択します。
- すべての管理者の管理 IM アドレス ドメインとシステム管理 IM アドレス ドメインを表示する **ドメインの検索と一覧 (Find and List Domains)** ウィンドウが表示されます。
- ステップ 2** 次の方法の 1 つを使用して削除する管理者の管理ドメインを選択し、次に [選択項目の削除 (Delete Selected)] をクリックします。
- 削除するドメインの横のチェックボックスをオンにします。
 - 管理者の管理ドメインのリストのドメインをすべて選択するには、[すべてを選択 (Select All)] をクリックします。
- ヒント** すべての選択をクリアするには、[すべてをクリア (Clear All)] をクリックします。
- ステップ 3** [OK] をクリックして削除を確定するか、[取消 (Cancel)] をクリックします。

次のタスク

TLS XMPP フェデレーションを使用した場合、[XMPP クライアントおよび TLS 証明書を再生成します \(31 ページ\)](#)に進みます。

XMPP クライアントおよび TLS 証明書を再生成します

IM ドメインを変更したら、XMPP クライアント証明書または TLS 証明書を再生成する必要があります。

手順

- ステップ 1 [Cisco Unified IM and Presence OS の管理 (Cisco Unified IM and Presence OS Administration)] で、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- ステップ 2 [検索 (Find)] をクリックして、証明書の一覧を生成します。
- ステップ 3 **cup-xmpp-s2s** 証明書をクリックしてください。
- ステップ 4 証明書の詳細ウィンドウで、**再生成** をクリックします。

IM and Presence サービスの開始

デフォルトドメインに変更を加えたら、この手順を使用してすべてのクラスタノードで IM and Presence サービスを再起動します。

始める前に

[XMPP クライアントおよび TLS 証明書を再生成します \(31 ページ\)](#)

手順

- ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンタ-ネットワークサービス (Control Center - Network Services)] を選択します。
- ステップ 2 [サーバ (Server)] リストから、サービスを再アクティブ化するノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3 **IM and Presence** サービス領域で、次のサービスを選択します。
 - Cisco Client Profile Agent
 - Cisco Sync Agent
 - Cisco XCP Router
- ステップ 4 [再起動 (Restart)] をクリックします。

ステップ 5 [関連リンク (Related Links)] ドロップダウンリストから [サービスのアクティベーション (Service Activation)] を選択し、[移動 (Go)] をクリックします。

ステップ 6 **IM and Presence** サービス領域で、次のサービスを選択します。

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

ステップ 7 [保存 (Save)] をクリックします。

次のタスク

[プレゼンス冗長グループでハイアベイラビリティを有効化する \(32 ページ\)](#)

プレゼンス冗長グループでハイアベイラビリティを有効化する

デフォルトドメインを変更して **IM and Presence** サービスを再起動した後、プレゼンス冗長グループの高可用性を有効にできます。

始める前に

すべてのサービスが実行されている必要があります **IM** と **プレゼンス** 高可用性を有効にする前に、データベースパブリッシャノードとサブスクライバノードを追加してください。サービスを再起動してから 30 分以内である場合は、ハイアベイラビリティを再度有効にする前に **Cisco Jabber** セッションが再作成されたことを確認します。十分な時間を確保しない場合、セッションが作成されていない **Jabber** クライアントで **プレゼンス** は機能しません。

Cisco Jabber セッションの数を取得するには、すべてのクラスタ ノードで `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI コマンドを実行します。アクティブセッションの数は、ハイアベイラビリティを無効にした際に記録したユーザ数と一致するはずです。

次の段階で、シスコのリアルタイム監視ツール (RTMT) を使用して、パブリッシャとサブスクライバの両方でパフォーマンスカウンタ "CiscoPresenceEngine" ActiveJsmSessions を監視する必要があります。

- パブリッシャまたはサブスクライバを再起動した後
- **Cisco XCP Router** の再起動後
- **Cisco Presence Engine** の再起動後

高可用性を有効にする前に、"CiscoPresenceEngine" ActiveJsmSessions の数がノードに割り当てられたユーザの数と同じである必要があることを確認してください。



(注) 必ずユーザの `ActiveJsmSessions` の作成が完了した後でのみ、高可用性を有効にします。

手順

- ステップ 1 Cisco Unified CM Administration のユーザ インターフェイスから、[システム (System)] > [プレゼンス冗長グループ (Presence Redundancy Groups)] を選択します。
 - ステップ 2 検索をクリックしてグループを選択します。
[プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウが表示されます。
 - ステップ 3 [ハイ アベイラビリティを有効にする (Enable High Availability)] チェックボックスをチェックします。
 - ステップ 4 [保存 (Save)] をクリックします。
 - ステップ 5 各プレゼンス冗長グループでこの手順を繰り返します。
-

■ プレゼンス冗長グループでハイアベイラビリティを有効化する



第 3 章

IPv6 の設定

- IPv6 設定の概要 (35 ページ)
- IPv6 タスク フローの設定 (36 ページ)

IPv6 設定の概要

IM and Presence Service と Cisco Unified Communications Manager 間の接続に IPv4 を使用していても、IM and Presence Service では外部とのやりとりに IPv6 を使用できます。

IM and Presence Service ノードで次のいずれかの項目に IPv6 を設定する場合、ノードは着信する IPv4 パケットを受け入れず、自動的に IPv4 の使用に復帰することはありません。

- 外部データベースへの接続
- LDAP サーバへの接続
- Exchange サーバへの接続。
- フェデレーション展開

フェデレーションでは、IPv6 が有効な外国企業へのフェデレーション リンクをサポートする必要がある場合は、IM and Presence Service で IPv6 を有効にする必要があります。これは、IM and Presence Service ノードとフェデレーション企業間に ASA がインストールされている場合にも当てはまります。ASA は、IM and Presence Service ノードに対して透過的です。

コマンドライン インターフェイスを使用して IPv6 パラメータを設定する場合の詳細については <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html> で『*Administration Guide for Cisco Unified Communications Manager*』および『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

IPv6 タスク フローの設定

手順

	コマンドまたはアクション	目的
ステップ 1	IM and Presence サービスの Eth0 での IPv6 の有効化 (36 ページ)	クラスタ内の各 IM and Presence サービスノードの Eth0 ポートで IPv6 を有効にします。変更を適用するには、各ノードを再起動する必要があります。
ステップ 2	IPv6 エンタープライズ パラメータの有効化 (37 ページ)	Egh0 ポートで IPv6 を有効にしたら、IM and Presence Service クラスタの IPv6 エンタープライズ パラメータを有効にする必要があります。
ステップ 3	サービスの再起動 (37 ページ)	変更を適用するには、IM and Presence サービスを再起動する必要があります。
ステップ 4	IM and Presence ノードに IPv6 アドレスを割り当てます (38 ページ)	IM and Presence サービスノードに IPv6 アドレスを割り当てます。

IM and Presence サービスの Eth0 での IPv6 の有効化

クラスタの各 IM and Presence サービス ノードの Eth0 ポートで IPv6 を有効にするには、Cisco Unified IM and Presence Operating System 管理 GUI を使用します。

手順

ステップ 1 Cisco Unified IM and Presence OS Administration で、**Settings > IP > Ethernet IPv6** を選択します。

ステップ 2 Ethernet IPv6 Configuration ウィンドウで、**IPv6 を有効にする** をチェックします。

ステップ 3 [アドレス ソース (Address Source)] を選択します。

- ルーター アドバタイズメント
- DHCP
- 手動入力

[手動入力 (Manual Entry)] を選択した場合は、**IPv6 アドレス**、**サブネットマスク**、および **デフォルト ゲートウェイ** の値を入力します。

ステップ 4 [リブートを使用した更新 (Update with Reboot)] チェックボックスをオンにします。

ヒント 予定されていたメンテナンス時間中などに、後で手動でノードを再起動する場合は、[リブートを使用した更新 (Update with Reboot)] チェックボックスはオンにしないでください。ただし、変更した内容はノードがリブートされるまで有効になりません。

ステップ 5 [保存 (Save)] をクリックします。

[リブートを使用した更新 (Update with Reboot)] チェックボックスをオンにした場合は、ノードがリブートされ、変更が適用されます。

次のタスク

[IPv6 エンタープライズパラメータの有効化 \(37 ページ\)](#)

IPv6 エンタープライズパラメータの有効化

IM and Presence Service クラスターの IPv6 エンタープライズパラメータを有効にするには [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] を使用します。

始める前に

[IM and Presence サービスの Eth0 での IPv6 の有効化 \(36 ページ\)](#)

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] を選択します。

ステップ 2 [エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウで、IPv6 パネルに対して [True] を選択します。

ステップ 3 [保存 (Save)] をクリックします。

次のタスク

[サービスの再起動 \(37 ページ\)](#) 変更を適用するには。

サービスの再起動

IPv6 エンタープライズパラメータを有効にしてから、この手順を使用して IM and Presence サービスを再起動します。



ヒント [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] を使用してシステム再起動通知をモニタするには、[システム (System)]>[通知 (Notifications)] を選択します。

始める前に

[IPv6 エンタープライズ パラメータの有効化 \(37 ページ\)](#)

手順

- ステップ 1** [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)]>[コントロールセンタ-ネットワークサービス (Control Center - Network Services)] を選択します。
- ステップ 2** [サーバ (Server)] リストから、サービスを再アクティブ化するノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3** **IM and Presence サービス (IM and Presence Services)** 領域で、[Cisco XCP Router] を選択します。
- ステップ 4** [再起動 (Restart)] をクリックします。
- ステップ 5** [関連リンク (Related Links)] ドロップダウンリストから [サービスのアクティベーション (Service Activation)] を選択し、[移動 (Go)] をクリックします。
- ステップ 6** **IM and Presence サービス** 領域で、次のサービスを選択します。
 - Cisco SIP Proxy
 - Cisco Presence Engine
- ステップ 7** [保存 (Save)] をクリックします。

IM and Presence ノードに IPv6 アドレスを割り当てます

IM and Presence ノードに IPv6 アドレスを割り当てるには、Cisco Unified Communications Manager でこの手順を使用します。

始める前に

また、Cisco Unified OS の管理で IPv6 Eth0 ポートを有効にし、IPv6 エンタープライズパラメータを有効にする必要もあります。

手順

- ステップ 1 Cisco Unified Communications Manager のパブリッシャ ノードにログインします
- ステップ 2 Cisco Unified CM の管理から、[システム (System)] > [サーバ (Server)] を選択します。
- ステップ 3 次の作業のいずれかを実行します。
 - 新しいサーバを追加するには、[新規追加 (Add New)] をクリックします。
 - 既存のサーバを更新するには、編集したいサーバをクリックします。
- ステップ 4 新しいサーバを追加する場合は、**サーバの種類** ドロップダウンメニューから、**CUCMIM と プレゼンス** を選択して次をクリックします。
- ステップ 5 サーバーの **IPv6 アドレス** を入力します。
- ステップ 6 [保存 (Save)] をクリックします。
- ステップ 7 各 IM and Presence Service ノードで繰り返します。

IM and Presence サービスの Eth0 での IPv6 の無効化

IPv6 を無効にしたい場合、IPv6 を使用しないクラスタの IM and Presence サービス ノードの Eth0 ポートの IPv6 を無効にするために、**Cisco Unified IM and Presence Operating System** の管理 GUI を使用します。変更を適用するには、ノードを再起動する必要があります。



- (注) IPv6 を使用するクラスタのいずれのノードも使用しない場合は、IPv6 エンタープライズ パラメータがクラスタで無効になっていることを確認します。

手順

- ステップ 1 Cisco Unified CM IM and Presence OS Administration で、設定 > IP > Ethernet IPv6 を選択します。
- ステップ 2 Ethernet IPv6 Configuration ウィンドウで、**IPv6 を有効にする** のチェックを外します。
- ステップ 3 [リポートを使用した更新 (Update with Reboot)] チェックボックスをオンにします。

ヒント 予定されていたメンテナンス時間中などに、後で手動でノードを再起動する場合は、[リポートを使用した更新 (Update with Reboot)] チェックボックスはオンにしないでください。ただし、変更した内容はノードがリポートされるまで有効になりません。
- ステップ 4 [保存 (Save)] をクリックします。

[リブートを使用した更新 (**Update with Reboot**)] チェックボックスをオンにした場合は、ノードがリブートされ、変更が適用されます。



第 4 章

IM アドレッシングスキームの設定

- [IM アドレッシングスキームの概要 \(41 ページ\)](#)
- [IM アドレッシング方式の前提条件 \(43 ページ\)](#)
- [IM アドレッシングスキームタスクフローの設定 \(43 ページ\)](#)

IM アドレッシングスキームの概要

IM and Presence Service は、次の 2 種類の IM アドレス指定スキームをサポートしています。

- *UserID@Default_Domain* は、IM and Presence Service をインストールする場合の、デフォルトの IM アドレススキームです。
- Directory URI IM アドレススキームは、複数のドメイン、ユーザのメールアドレスの調整、および Microsoft SIP URI の調整をサポートしています。

同じ IM アドレススキームをすべての IM and Presence Service クラスタで使用する必要があります。

User@Default_Domain を使用している IM アドレス

IM and Presence Service のデフォルトのアドレッシングスキームは *UserID@Default_Domain* です。

UserID @ Default_Domain IM アドレススキームを使用する場合、すべての IM アドレスは単一のデフォルトの IM ドメインの一部です。デフォルトドメイン値は、すべてのクラスタ全体で一貫している必要があります。なぜなら、IM アドレスは IM and Presence のデフォルトドメインの一部であるため、複数ドメインはサポートされません。

UserID は、フリーフォームまたは LDAP から同期することができます。次のフィールドがサポートされます。

- sAMAccountName
- ユーザプリンシパル名 (UPN)
- 電子メールアドレス

- 従業員番号
- 電話番号

UserID を Cisco Unified Communications Manager の LDAP フィールドにマップする場合、その LDAP マッピングはすべてのクラスタ全体で一貫している必要があります。

ユーザー ID は電子メールアドレスにマッピングできますが、IM URI が電子メールアドレスに等しいという意味ではありません。代わりに、`<email-address>@Default_Domain` となります。たとえば、`amckenzie@example.com @sales-example.com` です。選択した設定をマッピングする Active Directory (AD) は、IM and Presence サービス クラスタ内のすべてのユーザに対してグローバルに適用されます。個々のユーザに対して異なるマッピングを設定することはできません。

ディレクトリ URI を使用した IM アドレス

ディレクトリ URI のアドレス スキームを使用して、ユーザの IM アドレスを Cisco Unified Communications Manager のディレクトリ URI に合わせます。

ディレクトリ URI の IM アドレス スキームには、次の IM アドレス指定機能があります。

- 複数ドメインのサポート。IM アドレスは、1 つの IM and Presence Service ドメインだけを使用する必要はありません。
- ユーザのメールアドレスの調整。ユーザのメールアドレスと合わせるように Cisco Unified Communications Manager のディレクトリ URI を設定することが可能で、メール、IM、音声、および動画の通信にユーザの ID を一貫して指定できるようになります。
- Microsoft SIP URI の調整。Microsoft SIP URI と合わせるように Cisco Unified Communications Manager のディレクトリ URI を設定することで、Microsoft OCS/Lync から IM and Presence Service への移行時に、ユーザの ID を確実に維持できるようになります。

IM アドレス スキームとしてディレクトリ URI を使用するようノードを設定する場合は、ディレクトリ URI をサポートするクライアントのみを展開することを推奨します。ディレクトリ URI をサポートしないクライアントは、ディレクトリ URI IM アドレス スキームが有効になっている場合は動作しません。ディレクトリ URI をサポートしないクライアントが展開されている場合は、`UserID@Default_Domain` IM アドレス スキームを使用し、ディレクトリ URI IM アドレス スキームは使用しないでください。

ディレクトリ URI IM アドレス設定はグローバルであり、クラスタ内のすべてのユーザに適用されます。クラスタ内の個々のユーザに対して異なるディレクトリ URI IM アドレスを設定できません。

外部 LDAP ディレクトリからディレクトリ URI をプロビジョニングする方法についての詳細は、[LDAP ディレクトリの設定 \(83 ページ\)](#) を参照してください。

複数の IM ドメイン

IM and Presence Service は、複数の IM アドレス ドメイン全体で IM アドレッシングをサポートし、システム内のすべてのドメインを自動的にリストします。ドメインを追加、編集、または削除できます。IM ドメインの設定については、[ドメイン設定の概要 \(21 ページ\)](#) を参照してください。

Cisco Expressway と相互運用する場合は、<http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html> の『Cisco Expressway Administrator Guide』を参照してください。

IM アドレッシング方式の前提条件

IM and Presence Service のデフォルト ドメインと、使用する IM アドレス スキームは、IM and Presence Service クラスタ全体で一貫している必要があります。事前準備、[IM and Presence サービスのデフォルトメインを設定します \(28 ページ\)](#)。

設定する IM アドレス スキームはすべてのユーザ JID に影響を与え、別の設定を持つ可能性があるクラスタ間での通信を中断せずに段階的に実行することはできません。

展開したクライアントが IM アドレスとしてディレクトリ URI をサポートしない場合は、管理者がディレクトリ URI IM アドレス スキームを無効にする必要があります。

IM アドレッシングスキーム タスク フローの設定

IM アドレッシングスキームを設定するには、次のタスクを以下の順番で完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザプロビジョニングの検証 (44 ページ)	エンドユーザが正しくプロビジョニングされていること、および重複または無効なユーザがないことを確認します。
ステップ 2	ハイ アベイラビリティの無効化 (45 ページ)	プレゼンス冗長性グループのハイ アベイラビリティは、一時的に無効にする必要があります。IM アドレッシングスキームを設定するには、サービスを一時的に停止する必要があります。高可用性が有効になっている間にサービスを停止すると、システムのフェイルオーバーが発生します。
ステップ 3	サービスの停止 (Stop Services) (46 ページ)	IM アドレス スキームの設定を更新する前に、基本の IM and Presence Service を

	コマンドまたはアクション	目的
		停止します。必ず所定の順序でサービスを停止してください。
ステップ 4	IM アドレススキームの割り当て (46 ページ)	新しいドメインおよび IM アドレススキームを設定したり、既存のドメインおよびアドレススキームを更新したりするには、次の手順を使用します。
ステップ 5	サービスの再起動 (48 ページ)	IM アドレススキームを設定したら、サービスを再起動します。これは、ユーザアドレス情報を更新したり新規ユーザをプロビジョニングしたりする前に実行する必要があります。必ず所定の順序でサービスを起動してください。
ステップ 6	高可用性を有効にする (49 ページ)	IM アドレッシングスキームを設定し、IM and Presence サービスを再起動した後で、プレゼンス冗長グループの高可用性を有効にできます。すべてのサービスが実行されている必要があります IM とプレゼンス高可用性を有効にする前に、データベースパブリッシュノードとサブスクライバノードを追加してください。
ステップ 7	ディレクトリ URI を IM アドレッシングスキームとして選択すると： <ul style="list-style-type: none"> ディレクトリ URI への LDAP ソースの割り当て (50 ページ) Directory URI を手動で割当ます (51 ページ) 	これはオプションです。外部の LDAP ディレクトリからユーザを同期している場合は、ディレクトリの URI 値に LDAP ソースフィールドを設定します。 LDAP 以外のユーザの場合は、ディレクトリ URI を手動でプロビジョニングする必要があります。これは、ユーザ単位または一括管理ツールを使用して実行できます。

ユーザプロビジョニングの検証

アドレス指定方式を設定する前に、この手順を使用してエンドユーザが正しくプロビジョニングされていることを確認します。

手順

- ステップ 1 Cisco Unified CM IM and Presence Administration から、[診断 (Diagnostics)] > [システムトラブルシュータ (System Troubleshooter)] を選択します。

システムトラブルシューターが実行されます。

- ステップ 2 ユーザトラブルシューターセクション**で、エンドユーザが正しくプロビジョニングされていること、および重複または無効なユーザがないことを確認します。

次のタスク

[ハイアベイラビリティの無効化 \(45 ページ\)](#)

ハイアベイラビリティの無効化

クラスタの各プレゼンス冗長グループのハイアベイラビリティの無効化。アドレッシングスキームを編集するには、サービスを一時的に停止する必要があります。ハイアベイラビリティが有効な間にサービスを停止すると、システムのフェールオーバーが行われます。



- (注) [プレゼンス冗長グループの詳細] ページには、クラスタで高可用性が無効になっている場合でも、すべてのアクティブな JSM セッションが表示されます。

始める前に

各プレゼンス冗長グループの各クラスタノードに割り当てられたアクティブユーザ数を記録します。この情報は、[Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] の [システム (System)] > [プレゼンス トポロジ (Presence Topology)] ウィンドウで見つけることができます。後で高可用性を再度有効にするときにこれらの番号が必要になります。

手順

- ステップ 1** Cisco Unified CM Administration のユーザ インターフェイスから、[システム (System)] > [プレゼンス冗長グループ (Presence Redundancy Groups)] を選択します。
- ステップ 2** 検索をクリックしてグループを選択します。
- ステップ 3** [プレゼンス冗長グループの設定 (Presence Redundancy Group Configuration)] ウィンドウで、[ハイアベイラビリティを有効にする (Enable High Availability)] チェックボックスをオフにします。
- ステップ 4** [保存 (Save)] をクリックします。
- ステップ 5** 各プレゼンス冗長グループに対してこの手順を繰り返します。
- ステップ 6** 完了したら、さらに変更を加える前に、新しい HA 設定がクラスタ全体にわたって同期されるまで、少なくとも 2 分待機します

次のタスク

[サービスの停止 \(Stop Services\) \(46 ページ\)](#)

サービスの停止 (Stop Services)

IM アドレススキームの設定を更新する前に、基本の IM and Presence Service を停止します。必ず所定の順序でサービスを停止してください。

始める前に

[ハイアベイラビリティの無効化 \(45 ページ\)](#)

手順

-
- ステップ 1** [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター - ネットワーク サービス (Control Center - Network Services)] を選択します。
- ステップ 2** 次の IM and Presence Service を停止します。この順序で、サービスを選択し、[停止 (Stop)] ボタンをクリックしてください。
- a) Cisco Sync Agent
 - b) Cisco Client Profile Agent
- ステップ 3** 両方のサービスが停止したら、[ツール (Tools)] > [コントロールセンター - 機能サービス (Control Center - Feature Services)] を選択し、次のサービスをこの順序で停止します。
- a) Cisco Presence Engine
 - b) Cisco SIP Proxy
- ステップ 4** 両方のサービスが停止したら、[ツール (Tools)] > [コントロールセンター - 機能サービス (Control Center - Feature Services)] を選択し、次のサービスを停止します。
- Cisco XCP Router
- (注) XCP Router サービスを停止すると、すべての関連 XCP 機能サービスが自動的に停止します。
-

次のタスク

[IM アドレススキームの割り当て \(46 ページ\)](#)

IM アドレススキームの割り当て

新しいドメインおよびIMアドレススキームを設定したり、既存のドメインおよびアドレススキームを更新したりするには、次の手順を使用します。



(注) 設定する IM アドレススキームは、必ずすべてのクラスタ間で一致するようにしてください。

始める前に

[サービスの停止 \(Stop Services\)](#) (46 ページ)

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[プレゼンス (Presence)] > [設定 (Settings)] > [詳細設定 (Advanced Configuration)] を選択します。

ステップ 2 新しいデフォルトドメインを割り当てるには、[デフォルトドメイン (Default Domain)] チェックボックスにマークを付け、テキストボックスに新しいドメインを入力します。

ステップ 3 アドレススキームを変更するには、[IM Address Scheme (IM アドレススキーム)] チェックボックスにマークを入れ、ドロップダウンリストボックスから次のいずれかのオプションを選択します。

- [UserID@[Default_Domain]] - 各 IM ユーザアドレスは、UserID からデフォルトドメインとともに取得されます。これがデフォルト設定です。
- [ディレクトリ URI (Directory URI)] - 各 IM ユーザアドレスは、Cisco Unified Communications Manager でそのユーザに関して設定されているディレクトリ URI と一致します。

(注) このオプションを選択すると、展開されたすべてのクライアントが、IM アドレスとしてディレクトリ URI をサポートし、EDI ベースまたは UDS ベースのディレクトリ統合を使用する必要があります。Jabber との UDS ベースの統合については、Jabber のリリース 10.6 以降を実行している必要があります。

ステップ 4 [保存 (Save)] をクリックします。

ステータス領域の更新進行状況を監視できます。

IM アドレススキームとしてディレクトリ URI を選択する場合、展開クライアントが複数ドメインをサポートできることを確認するプロンプトが表示される場合があります。続行するには [OK (OK)] をクリックします。または [取消 (Cancel)] をクリックします。

ユーザが [ディレクトリ URI (Directory URI)] 設定を無効にしている場合は、ダイアログボックスが表示されます。続行するには、[OK (OK)] をクリックし、または [取消 (Cancel)] をクリックします。次に、IM アドレススキームを再設定する前にユーザ設定をします。

システムアップデートは完了まで最長で 1 時間かかる場合があります。変更を再適用するには、[再試行 (Re-try)] をクリックします。または [取消 (Cancel)] をクリックします。

次のタスク

アドレッシングスキームとして `user@default_domain` を設定していて、ディレクトリ URI を使用していない場合は、[サービスの再起動 \(48 ページ\)](#) に進みます。

アドレス指定方式としてディレクトリ URI を設定した場合は、次のいずれかのオプションを選択します。

- [ディレクトリ URI への LDAP ソースの割り当て \(50 ページ\)](#)
- [Directory URI を手動で割当ます \(51 ページ\)](#)

IM アドレスの例

IM and Presence サービスで使用可能な IM アドレス オプションの例。

IM and Presence Service デフォルト ドメイン : cisco.com		
ユーザ: John Smith		
ユーザー ID : js12345		
Mail ID: jsmith@cisco-sales.com		
SIPURI: john.smith@webex.com		

IM アドレス形式	ディレクトリ URI マッピング	IM アドレス (IM Address)
<userid>@<domain>	適用対象外	js12345@cisco.com
Directory URI	mailid	jsmith@cisco-sales.com
Directory URI	msRTCSIP-PrimaryUserAddress	john.smith@webex.com

サービスの再起動

IM アドレス スキームを設定したら、サービスを再起動します。これは、ユーザアドレス情報を更新したり新規ユーザーをプロビジョニングしたりする前に実行する必要があります。必ず所定の順序でサービスを起動してください。

始める前に

- [IM アドレス スキームの割り当て \(46 ページ\)](#)
- ディレクトリ URI をアドレッシングスキームとして設定した場合は、サービスを再起動する前に次のいずれかのオプションを実行します。
 - [ディレクトリ URI への LDAP ソースの割り当て \(50 ページ\)](#)
 - [Directory URI を手動で割当ます \(51 ページ\)](#)

手順

-
- ステップ 1** [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター - ネットワーク サービス (Control Center - Network Services)] を選択します。
- ステップ 2** サービスを選択し、[起動 (Start)] ボタンをクリックして、次のサービスを起動します。
- Cisco XCP Router
- ステップ 3** サービスが起動したら、[ツール (Tools)] > [コントロールセンター - 機能サービス (Control Center - Feature Services)] を選択し、次のサービスをこの順序で起動します。
- a) Cisco SIP Proxy
 - b) Cisco Presence Engine
- ステップ 4** 次の手順に進む前に、Cisco Presence Engine サービスがすべてのノードで実行中であることを確認します。
- ステップ 5** [ツール (Tools)] > [コントロールセンター - ネットワークサービス (Control Center - Network Services)] を選択し、次のサービスをこの順序で起動します。
- a) Cisco Client Profile Agent
 - b) Cisco Sync Agent
-

次のタスク

[高可用性を有効にする \(49 ページ\)](#)

高可用性を有効にする

IM アドレス指定方式を設定してサービスを再起動したら、この手順を使用して、クラスタ内の各プレゼンス冗長グループに対して高可用性を再度有効にします

始める前に

すべてのサービスが実行されている必要があります IM とプレゼンス高可用性を有効にする前に、データベースパブリッシャノードとサブスクライバノードを追加してください。サービスを再起動してから 30 分以内である場合は、ハイアベイラビリティを再度有効にする前に Cisco Jabber セッションが再作成されたことを確認します。十分な時間を確保しない場合、セッションが作成されていない Jabber クライアントでプレゼンスは機能しません。

Cisco Jabber セッションの数を取得するには、すべてのクラスタ ノードで `show perf query counter Cisco Presence Engine ActiveJsmSessions` CLI コマンドを実行します。アクティブセッションの数は、ハイアベイラビリティを無効にした際に記録したユーザ数と一致するはずですが。

手順

-
- ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
- ステップ 2 [サーバ (Server)] リストから、サービスを再アクティブ化するノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3 **IM and Presence** サービス領域で、次のサービスを選択します。
- Cisco Client Profile Agent
 - Cisco Sync Agent
 - Cisco XCP Router
- ステップ 4 [再起動 (Restart)] をクリックします。
- ステップ 5 [関連リンク (Related Links)] ドロップダウン リストから [サービスのアクティベーション (Service Activation)] を選択し、[移動 (Go)] をクリックします。
- ステップ 6 **IM and Presence** サービス領域で、次のサービスを選択します。
- Cisco SIP Proxy
 - Cisco Presence Engine
- ステップ 7 [保存 (Save)] をクリックします。
-

ディレクトリ URI への LDAP ソースの割り当て

外部 LDAP ディレクトリからユーザを同期している場合は、この手順を使用してディレクトリ URI の割り当てに使用される外部 LDAP ディレクトリ ソースフィールドを割り当てることができます。LDAP ディレクトリの同期が行われると、設定したフィールドの値からディレクトリ URI が割り当てられます。



- (注) 最初の LDAP 同期がすでに発生している場合、Cisco Unified Communications Manager では、LDAP ディレクトリの既存の構成に編集を追加できません。外部 LDAP ディレクトリに追加された新しい項目を同期することはできませんが、Cisco Unified Communications Manager で LDAP 設定を編集することはできません。LDAP ディレクトリを既に同期している場合
- 一括管理ツールを使用して、ディレクトリ URI をユーザに割り当てます。詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。
 - ディレクトリ URI を手動でユーザに割り当てます
-

始める前に

[IM アドレス スキームの割り当て \(46 ページ\)](#)

手順

ステップ 1 Cisco Unified CM の管理から、[システム (System)] > [LDAP] > [LDAP ディレクトリ (LDAP Directory)] を選択します。

ステップ 2 ディレクトリ URI ドロップダウン リストから、次のいずれかのオプションを選択します。

- **メール** : ユーザのメールアドレスと合わせるように Directory URI をマップして、メール、IM、音声、および動画の通信にユーザの ID を一貫して指定できるようになります。
- **msRTCSIP-PrimaryUserAddress**: Directory URI を Microsoft OCS/Lync SIP URI にマップします。

(注) LDAP URI が同期されるまで、ディレクトリ URI はプロビジョニングされません。LDAP ディレクトリ同期の設定の詳細については、[LDAP ディレクトリの設定 \(83 ページ\)](#) を参照してください。

次のタスク

[サービスの再起動 \(48 ページ\)](#)

Directory URI を手動で割当ます

LDAP を使用していない場合は、この手順を使用してユーザごとにディレクトリ URI を手動で入力できます。



- (注) Bulk Administration Tool を使用して、csv ファイルを介して多数のエンドユーザにディレクトリ URI をプロビジョニングすることもできます。一括管理の使用の詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html> で『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

LDAP ディレクトリをまだ同期していない場合は、LDAP ディレクトリ同期を介してユーザのディレクトリ URI をプロビジョニングできます。

始める前に

[IM アドレス スキームの割り当て \(46 ページ\)](#)

手順

- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] で、[ユーザの管理 (User Management)] > [エンド ユーザ (End User)] を選択します。
 - ステップ 2 適切な検索条件を入力し、[検索 (Find)] をクリックします。
 - ステップ 3 設定したいエンドユーザを選択します。
 - ステップ 4 ユーザ情報エリアで、ディレクトリ URI を **ディレクトリ URI** フィールドに入力します。
 - ステップ 5 [保存 (Save)] をクリックします。
-

次のタスク

[サービスの再起動 \(48 ページ\)](#)



第 5 章

冗長性およびハイ アベイラビリティの設定

- [プレゼンス冗長グループの概要 \(53 ページ\)](#)
- [プレゼンス冗長グループの前提条件 \(54 ページ\)](#)
- [プレゼンス冗長グループのタスク フロー \(55 ページ\)](#)
- [手動によるフェールオーバー、フォールバック、リカバリの開始 \(61 ページ\)](#)
- [ダウンタイムをほぼゼロに抑える IM and Presence フェールオーバーの機能拡張 \(71 ページ\)](#)
- [冗長性の連携動作と制約事項 \(74 ページ\)](#)

プレゼンス冗長グループの概要

プレゼンス冗長グループは、同じクラスタからの 2 つの IM and Presence Service ノードで設定されています。プレゼンス冗長グループ内の各ノードは、ピア ノードのステータスまたはハートビートをモニタします。IM and Presence Service クライアントおよびアプリケーションで冗長性と回復性の両方を実現するようにプレゼンス冗長グループを設定できます。

- **フェールオーバー**：プレゼンス冗長グループ内の IM and Presence サービス ノード上で 1 つ以上の重要なサービスが失敗した場合、またはグループ内のノードが失敗した場合に、そのプレゼンス冗長グループ内で行われます。クライアントは、そのグループ内のもう 1 つの IM and Presence サービス ノードに自動で接続します。
- **フォールバック**：以下のいずれかの状況で、フォールバック コマンドが CLI または Cisco Unified Communications Manager から発行されると行われます。
 - 失敗した IM and Presence サービス ノードがサービスを再開し、すべての重要なサービスが動作している場合。そのグループのフェールオーバーが発生したクライアントは、使用可能になると回復したノードと再接続します。
 - 重要なサービスの不具合のために、アクティブ化されていたバックアップ IM and Presence サービス ノードが失敗し、ピア ノードがフェールオーバー状態であり、自動回復フォールバックをサポートしている場合。

たとえば、プレゼンス冗長グループを使用していると、ローカルの IM and Presence サービス ノードのサービスまたはハードウェアで障害が発生した場合、Cisco Jabber クライアントはバックアップ用 IM and Presence サービス ノードにフェールオーバーします。障害の発生したノードがオンラインに戻ると、自動フォールバックを設定している場合、クライアントはローカルの IM and Presence サービス ノードに自動的に再接続します。自動フォールバックを設定していない場合、障害の発生したノードがオンラインに戻ったらフォールバックを手動で開始できます。

冗長性と回復性に加え、プレゼンス冗長グループでは、クラスタのハイアベイラビリティを設定することもできます。

高可用性

IM and Presence Service は複数ノードのハイアベイラビリティ展開をサポートします。

プレゼンス冗長グループを構成した後、グループのハイアベイラビリティを有効にできます。高可用性には、ペアのノードが必要です。各ノードには、独立型のデータベースと一連のユーザが存在し、これらは、共通のユーザをサポートできる共有アベイラビリティデータベースとともに運用されます。

すべての IM and Presence Service ノードが、プレゼンス冗長グループに属している必要があります。このグループは、単一の IM and Presence Service ノード、またはペアの IM and Presence Service ノードで構成されている場合があります。

2つの異なるモードを使用してハイアベイラビリティを構成できます。

- バランスモード：このモードでは、コンポーネントの障害や停電が原因で1つのノードが停止するイベント時に自動ユーザロードバランシングとユーザフェールオーバーを含む冗長ハイアベイラビリティを提供します。
- アクティブ/スタンバイモード：アクティブノードが停止すると、スタンバイノードはアクティブノードを自動的に引き継ぎます。自動ロードバランシングは行いません。

IM and Presence Service の展開をハイアベイラビリティ展開として設定することを推奨します。シングル展開では、ハイアベイラビリティと非ハイアベイラビリティの両方を、プレゼンス冗長グループに設定しておくことが許可されますが、この設定は推奨されません。

プレゼンス冗長グループの前提条件

WAN 経由での導入では、IM およびプレゼンス クラスタごとに少なくとも 10 Mbps の専用の帯域幅が必要であり、往復遅延は 80 ミリ秒を超えないことが必要です。帯域幅がこの推奨事項未満の場合、パフォーマンスに悪影響を及ぼす場合があります。

プレゼンス冗長グループのタスク フロー

1つのIM and Presence Service ノードは、1つのプレゼンス冗長グループのみに割り当てることができます。高可用性を実現するには、同じクラスタから2つのノードをプレゼンス冗長グループに割り当て、グループの高可用性を確保する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	データベース レプリケーションの確認 (55 ページ)	データベース レプリケーションが IM and Presence サービス クラスタで設定されていることを確認します。
ステップ 2	確認サービス (56 ページ)	重要なサービスがプレゼンス冗長グループに追加予定のノード上で実行されていることを確認します。
ステップ 3	プレゼンス冗長グループの設定 (57 ページ)	IM and Presence Service クライアントとアプリケーションの冗長性とリカバリを提供します。
ステップ 4	フェールオーバー用のハートビート間隔の設定 (58 ページ)	これはオプションです。プレゼンス冗長グループ内の各ノードは、ピア ノードのステータスまたはハートビートをモニタします。ノードが自身のピアを監視する間隔を設定できます。
ステップ 5	高可用性を有効にする (60 ページ)	これはオプションです。プレゼンス冗長グループを設定した際にハイ アベイラビリティを有効にしなかった場合、この手順を実行します。
ステップ 6	ユーザー割り当てモードの設定 (60 ページ)	Sync Agent が IM and Presence サービス クラスタのさまざまなノード全体にユーザを分散する方法を設定します。この設定は、システムがフェールオーバーとロード バランシングを処理する方法に影響します。

データベース レプリケーションの確認

プレゼンス冗長グループのハイアベイラビリティを有効にする前に、データベースレプリケーションが IM and Presence サービス クラスタでセットアップされるようにします。

手順

ステップ 1 次のいずれかの方法を使用して、CLI セッションを開始します。

- リモート システムの場合は、SSH を使用して Cisco Unified オペレーティング システムにセキュアに接続します。SSH クライアントで、**ssh adminname@hostname** およびパスワードを入力します。
- シリアルポートへの直接接続を介して、自動的に表示されるプロンプトでクレデンシャルを入力します。

ステップ 2 **utils dbreplication status** コマンドを実行して、データベーステーブルのエラーまたはミスマッチを確認します。

ステップ 3 **utils dbreplication runtimestate** コマンドを実行して、データベースレプリケーションがノードでアクティブであることを確認します。

出力にはすべてのノードが一覧表示されます。データベースレプリケーションがセットアップされて正常であれば、各ノードの **replication setup** の値は **2** になります。

2 以外の値が返される場合は、続行する前にエラーを解決する必要があります。

次のタスク

[確認サービス \(56 ページ\)](#)

確認サービス

重要なサービスがプレゼンス冗長グループに追加予定のノード上で実行されていることを確認します。ハイ アベイラビリティをオンにする前に、重要なサービスを実行する必要があります。重要なサービスがいずれのノードでも動作していない場合、障害状態に高可用性をオンにするとプレゼンス冗長グループは **Failed** 状態になります。重要なサービスが1つのノードで実行されていない場合、高可用性をオンにすると、そのノードが他のノードにフェールオーバーします。

始める前に

[データベース レプリケーションの確認 \(55 ページ\)](#)

手順

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。

ステップ 2 [サーバ (Server)] リストから、適切なノードを選択し、[移動 (Go)] をクリックします。

ステップ 3 [IM and Presence サービス (IM and Presence Services)] で、次のサービスが開始されていることを確認します。

- **Cisco Client Profile Agent**
- **Cisco Sync Agent**
- **Cisco XCP Router**

ステップ 4 [関連リンク (Related Links)] ドロップダウン リストから [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択し、[移動 (Go)] をクリックします。

ステップ 5 [IM and Presence サービス (IM and Presence Services)] で、次のサービスが開始されていることを確認します。

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

次のタスク

[プレゼンス冗長グループの設定 \(57 ページ\)](#)

プレゼンス冗長グループの設定

Cisco Unified Communications Manager を使用して、IM and Presence サービス ノードの冗長性を設定します。

各プレゼンス冗長グループには、IM and Presence サービスの2つのノードを含めることができます。各ノードを割り当てることができるプレゼンス冗長グループは1つだけです。プレゼンス冗長グループのノードはどちらも同じクラスタ上にあり、同じIM and Presence サービスデータベース パブリッシャ ノードを持つ必要があります。

始める前に

- [確認サービス \(56 ページ\)](#)
- プレゼンス 冗長グループに追加する IM and Presence サービス ノードが同じソフトウェアバージョンを実行していることを確認します。

手順

ステップ 1 Cisco Unified CM の管理から、[システム (System)] > [プレゼンス冗長グループ (Presence Redundancy Groups)] を選択します。

ステップ 2 [新規追加 (Add New)] をクリックします。

ステップ 3 プレゼンス冗長グループの一意的名前を入力します。

アンダースコア (_) およびダッシュ (-) を含む最大 128 文字の英数字を入力できます。

ステップ 4 グループの説明を入力します。

最大 128 文字の英数字と記号を入力できますが、二重引用符 (") 、パーセント記号 (%) 、アンパサンド (&) 、バックスラッシュ (\) 、山カッコ (< >) は使用できません。

ステップ 5 IM and Presence Service の 2 つの異なるノードを [プレゼンス サーバ (Presence Server)] フィールドで選択し、グループに割り当てます。

ステップ 6 (任意) [高可用性を有効にする (Enable High Availability)] チェックボックスをオンにして、プレゼンス冗長グループの高可用性を有効にします。

ステップ 7 [保存 (Save)] をクリックします。

次のタスク

[フェールオーバー用のハートビート間隔の設定 \(58 ページ \)](#)

フェールオーバー用のハートビート間隔の設定

ピアがアクティブであることを確認するために、プレゼンス冗長グループ内の各ピアがピアノードのハートビート (つまりステータス) を監視するためのキープアライブ設定を決定するオプションのサービスパラメータを設定します。設定されたタイマーが期限切れになった後にピアノードが応答しなくなった場合、フェールオーバーを開始できます。



(注) シスコは、これらのサービスパラメータにデフォルト値を設定することを推奨します。ただし、ニーズに合わせて値を再設定することもできます。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。

ステップ 2 [サーバ (Server)] ドロップダウンメニューから、IM and Presence ノードを選択します

ステップ 3 [サービス (Service)] ドロップダウンメニューから、[Cisco Server Recovery Manager (Active)] を選択します。

ステップ 4 **General Server Recovery Manager** のパラメータ (クラスタ全体) で、クラスタ全体のキープアライブ設定を構成し、プレゼンス冗長グループ内の各ノードがそのピアノードのハートビートの監視に使用するようにします。ピアノードが応答しない場合、フェールオーバーを開始できます。

- **サービスポート** - このパラメータは、Cisco Server Recovery Manager がピアとの通信に使用するポートを指定します。デフォルトは 22001 です。

- **管理 PRC ポート** - このパラメータは、Cisco Server Recovery Manager が管理 RPC 要求を行うために使用するポートを指定します。デフォルトは 20075 です。
- **重要なサービスの遅延** - このパラメータは、フェールオーバーが開始されるまでに重要なサービスを停止できる期間を秒単位で指定します。デフォルトは 90 です。
- **自動フォールバックを有効にする** - このパラメータは、自動フォールバックを実行するかどうかを指定します。フェールオーバーが発生した場合、IM and Presence サービスは、プライマリノードが正常な状態に戻ってから 30 分後に、ユーザをバックアップノードからプライマリノードに自動的に移動します。デフォルト値は [False] です。
- **初期化キープアライブ（ハートビート）タイムアウト** - このパラメータは、フェールオーバーが開始される前の初期化中にハートビートがピアで失われる可能性がある期間を秒単位で指定します。デフォルトは 120 です。
- **初期化キープアライブ（ハートビート）タイムアウト** - このパラメータは、フェールオーバーが開始される前の初期化中にハートビートがピアで失われる可能性がある期間を秒単位で指定します。デフォルトは 60 です。
- **キープアライブ（ハートビート）間隔** - このパラメータは、ピアに送信されるキープアライブ（ハートビート）メッセージの間隔を秒単位で指定します。デフォルトは 15 です。
- **[XCP Authentication Serviceのモニタリングの有効化（Enable monitoring of XCP Authentication Service）]** : このパラメータを使用して、Cisco XCP Authentication Service をモニタするようにシステムを設定し、ノードでサービスの障害が発生したときにピアノードへの自動フェールオーバーを開始することができます。[XCP Authentication Serviceのモニタリングの有効化（Enable monitoring of XCP Authentication Service）] フィールドで、サービスパラメータの値を [TRUE] に設定します。

ステップ 5 次の追加パラメータを設定します。これは、CUPC 8.5 以降のクライアントが、再ログインを試行するまでの待機時間を現します。上記のパラメータとは異なり、これらのパラメータはクラスターノードごとに個別に設定する必要があります。

- **クライアントの再ログインの下限** - このパラメータは、このサーバへの再ログインを試みる前に CUPC 8.5（以上）が待機する必要がある最小秒数を指定します。デフォルトは 120 です。
- **クライアントの再ログインの上限** - このパラメータは、このサーバへの再ログインを試行するまでに CUPC 8.5（以上）が待機する最大秒数を指定します。デフォルトは 537 です。

ステップ 6 [保存 (Save)] をクリックします。

次のタスク

プレゼンス冗長グループを設定した際にハイアベイラビリティを有効にしていない場合は、[高可用性を有効にする \(60 ページ\)](#)

高可用性を有効にする



注意 IM and Presence Service クラスタのレプリケーションのセットアップに失敗したが、すべての重要なサービスが実行されている場合、現在の冗長グループで有効な場合は、すぐにフェールオーバーする場合があります。

始める前に

- [プレゼンス冗長グループの設定 \(57 ページ\)](#)
- IM and Presence Service クラスタでレプリケーションがセットアップされていることを確認します。
- すべての重要なサービスが動作していることを確認します。

手順

- ステップ 1** Cisco Unified CM の管理から、[システム (System)] > [プレゼンス冗長グループ (Presence Redundancy Groups)] を選択します。
- ステップ 2** 検索情報を指定し、[検索 (Find)] をクリックします。
- ステップ 3** 設定したプレゼンス冗長グループを選択します。
- ステップ 4** 高可用性を有効にするには、[高可用性を有効にする (Enable High Availability)] チェックボックスをオンにします。
- ステップ 5** [保存 (Save)] をクリックします。

ユーザー割り当てモードの設定

この手順を使用すると、Sync Agent がクラスタ内のノードにユーザを分散させる方法を設定できます。この設定により、フェールオーバーおよびロード バランシングを管理できます。

手順

- ステップ 1** Cisco Unified CM の管理から、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] を選択します。
- ステップ 2** [ユーザ管理パラメータ (User Management Parameters)] 領域で、[プレゼンスサーバのユーザー割り当てモード (User Assignment Mode for Presence Server)] パラメータに次のいずれかのオプションを選択します。

- [バランス (Balanced)]: このモード (デフォルト) では、ユーザを各サブクラスタのそれぞれのノードに均等に割り当て、各ノードにユーザの合計数が均等に分散するようにします。これがデフォルトのオプションです。
- [アクティブスタンバイ (Active-Standby)]: このモードでは、サブクラスタの最初のノードにすべてのユーザを割り当て、セカンダリ サーバをバックアップのままにします。
- [なし (None)]: このモードでは、Sync Agent でクラスタのノードにユーザが割り当てられません。

ステップ3 [保存 (Save)]をクリックします。

手動によるフェールオーバー、フォールバック、リカバリの開始

プレゼンス冗長グループの IM and Presence サービス ノードの手動フェールオーバー、フォールバック、またはリカバリを開始するにはこの手順を使用します。

- 手動フェールオーバー - 手動フェールオーバーを開始すると、**Cisco Server Recovery Manager** は失敗したノードの重要なサービスを停止します。失敗したノードのすべてのユーザが切断されるので、バックアップ ノードに再ログインする必要があります。手動でフォールバックしない限り、重要なサービスは再開されません。
- 手動フォールバック - 手動フォールバックを開始すると、**Cisco Server Recovery Manager** はプライマリ ノード上の重要なサービスを再起動し、フェールオーバーされていたすべてのユーザを切断します。切断されたユーザは、割り当てられたノードに再ログインする必要があります。
- 手動リカバリ - 手動リカバリは、プレゼンス冗長グループ内の両方のノードが失敗状態にある場合に必要となります。この場合、IM and Presence Service はプレゼンス冗長グループの両方のノード上で、**Cisco Server Recovery Manager** サービスを再起動します。

手順

ステップ1 Cisco Unified CM の管理から、[システム (System)] > [プレゼンス冗長グループ (Presence Redundancy Groups)]を選択します。

ステップ2 検索をクリックし、該当するノードを含むプレゼンス冗長グループを選択します。

ステップ3 次のいずれかを実行します。使用可能なボタンは、ノードの現在の状態によって異なることに留意してください。

- フェイルオーバーをクリックしてアクティブノードのフェイルオーバーを開始します。
- フェイルオーバーをクリックして、フェイルオーバーしたノードのフォールバックを開始します。

- 両方のノードがフェイルオーバーしていてそれらを回復したい場合、**回復**をクリックします。



(注) CLI を使用して Cisco Unified Communications Manager または IM and Presence サービスからこれらのアクションを開始することもできます。詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。



(注) ノードの1つがフェールオーバー状態の間は、IM and Presence サービスクラスタにエンドユーザを追加できません。

ノード状態定義

表 3: プレゼンス冗長グループのノード状態の定義

状態	説明
初期化中 (Initializing)	これは、Cisco Server Recovery Manager サービスが開始されたときの初期 (遷移) 状態であり、一時的な状態です。
アイドル (Idle)	フェールオーバーが発生してサービスが停止されると、IM and Presence サービスはアイドル状態になります。アイドル状態では、IM and Presence サービス ノードがアベイラビリティ サービスやインスタントメッセージサービスを提供しません。[Cisco Unified CMの管理(Cisco Unified CM Administration)] ユーザインターフェイスを使用して、このノードへのフォールバックを手動で開始できます。
標準	これは安定した状態です。IM and Presence サービスが正常に稼働しています。この状態では、[Cisco Unified CMの管理(Cisco Unified CM Administration)] ユーザインターフェイスを使用して、このノードへのフェールオーバーを手動で開始できます。
バックアップモードで 実行中 (Running in Backup Mode)	これは安定した状態です。IM and Presence サービス ノードが、そのピアノードのバックアップとして機能中です。ユーザは、この (バックアップ) ノードに移動しました。
テイク オーバー中 (Taking Over)	これは遷移状態です。IM and Presence サービス ノードが、そのピアノードへのテイクオーバー中です。
フェールオーバー中 (Failing Over)	これは遷移状態です。IM and Presence サービス ノードが、そのピアノードによってテイクオーバーされているところです。

状態	説明
フェールオーバー済み (Failed Over)	これは安定した状態です。IM and Presence サービス ノードがフェールオーバーしましたが、重要なサービスはダウンしていません。この状態では、[Cisco Unified CMの管理(Cisco Unified CM Administration)] ユーザ インターフェイスを使用して、このノードへのフォールバックを手動で開始できます。
フェールオーバー済み/ 重要なサービスが実行 されていません(Failed Over with Critical Services Not Running)	これは安定した状態です。IM and Presence サービス ノード上の重要なサービスの一部が、停止したか失敗しました。
フォールバック中 (Falling Back)	これは遷移状態です。システムが、バックアップ モードで実行中のノードからこの IM and Presence サービス ノードへのフォールバック中です。
テイク バック中 (Taking Back)	これは遷移状態です。失敗した IM and Presence サービス ノードが、そのピアからテイクバックされているところです。
障害モードで実行中 (Running in Failed Mode)	遷移状態または[バックアップモードで実行中(Running in Backup Mode)]状態のときにエラーが発生しました。
不明	ノード状態は不明です。 原因として、IM and Presence サービス ノード上でハイ アベイラビリティが正しく有効にされなかったことが考えられます。プレゼンス冗長グループの両方のノード上で、Server Recovery Manager サービスを再起動してください。

ノード状態、原因、および推奨処置

[Cisco Unified CMの管理(Cisco Unified CM Administration)] ユーザ インターフェイスを使用してグループを選択する場合、[プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウのプレゼンス冗長グループでノードのステータスを表示できます。

表 4: プレゼンス冗長グループノードのハイ アベイラビリティ状態、原因、および推奨されるアクション

ノード 1		ノード 2		原因/推奨処置
状態	理由 (Reason)	状態	理由 (Reason)	
標準	標準	標準	標準	標準

ノード 1		ノード 2		原因/推奨処置
状態	理由 (Reason)	状態	理由 (Reason)	
フェールオーバー中 (Failing Over)	管理者からの要求 (On Admin Request)	テイクオーバー中 (Taking Over)	管理者からの要求 (On Admin Request)	管理者がノード1からノード2への手動フェールオーバーを開始しました。手動フェールオーバーの処理中です。
アイドル (Idle)	管理者からの要求 (On Admin Request)	バックアップモードで実行中 (Running in Backup Mode)	管理者からの要求 (On Admin Request)	管理者が開始したノード1からノード2への手動フェールオーバーが完了しました。
テイクバック中 (Taking Back)	管理者からの要求 (On Admin Request)	フォールバック中 (Falling Back)	管理者からの要求 (On Admin Request)	管理者がノード2からノード1への手動フォールバックを開始しました。手動フォールバックの処理中です。
アイドル (Idle)	初期化	バックアップモードで実行中 (Running in Backup Mode)	管理者からの要求 (On Admin Request)	管理者はノード1が「アイドル」状態の間にノード1でSRMサービスを再起動します。
アイドル (Idle)	初期化	バックアップモードで実行中 (Running in Backup Mode)	初期化	プレゼンス冗長グループが手動フェールオーバーモードであるとき、管理者がプレゼンス冗長グループの両方のノードを再起動したか、両方のノード上のSRMサービスを再起動しました。
アイドル (Idle)	管理者からの要求 (On Admin Request)	バックアップモードで実行中 (Running in Backup Mode)	初期化	管理者は、ノード2がバックアップモードで動作中、ノード1のハートビートがタイムアウトする前にノード2でSRMサービスを再起動します。

ノード 1		ノード 2		原因/推奨処置
状態	理由 (Reason)	状態	理由 (Reason)	
フェールオーバー中 (Failing Over)	管理者からの要求 (On Admin Request)	テイクオーバー中 (Taking Over)	初期化	管理者は、ノード2がテイクオーバー中、ノード1のハートビートがタイムアウトする前にノード2でSRMサービスを再起動します。
テイクバック中 (Taking Back)	初期化	フォールバック中 (Falling Back)	管理者からの要求 (On Admin Request)	管理者は、テイクバック中、ノード2のハートビートがタイムアウトする前にノード1でSRMサービスを再起動します。テイクバックプロセスが完了すると、両方のノードが正常状態になります。
テイクバック中 (Taking Back)	自動フォールバック (Automatic Fallback)	フォールバック中 (Falling Back)	自動フォールバック (Automatic Fallback)	ノード2からノード1への自動フォールバックが開始され、進行中です。
フェールオーバー済み (Failed Over)	初期化 (Initialization) または重要なサービス停止 (Critical Services Down)	バックアップモードで実行中 (Running in Backup Mode)	重要なサービスのダウン	次のいずれかの条件が発生すると、ノード1は[フェールオーバー済み(Failed Over)]状態に遷移します。 <ul style="list-style-type: none"> ノード1のリポートにより、重要なサービスが稼働状態に戻る。 ノード1が[フェールオーバー済み/重要なサービスが実行されていません(Failed Over with Critical Services Not Running)]状態であるとき、管理者がノード1上で重要なサービスを開始する。 <p>ノード1が[フェールオーバー済み(Failed Over)]状態に遷移するとき、プレゼンス冗長グループのノードを[正常(Normal)]状態に復元するために、管理者がノード1を手動フォールバックできる状態にある。</p>

ノード1		ノード2		
状態	理由 (Reason)	状態	理由 (Reason)	原因/推奨処置
フェールオーバー済み/重要なサービスが実行されていません (Failed Over with Critical Services not Running)	重要なサービスのダウン	バックアップモードで実行中 (Running in Backup Mode)	重要なサービスのダウン	ノード1上で重要なサービスがダウンしています。IM and Presence サービスは、ノード2への自動フェールオーバーを実行します。 推奨処置： <ol style="list-style-type: none"> 1. ノード1にダウンしている重要なサービスがないかどうかを確認し、手動でのそのサービスの開始を試みます。 2. ノード1上の重要なサービスが開始されない場合は、ノード1をリブートします。 3. リブート後にすべての重要なサービスが起動して実行中になったら、手動フォールバックを実行してプレゼンス冗長グループのノードを[正常(Normal)]状態に復元します。
フェールオーバー済み/重要なサービスが実行されていません (Failed Over with Critical Services not Running)	データベース障害 (Database Failure)	バックアップモードで実行中 (Running in Backup Mode)	データベース障害 (Database Failure)	ノード1上のデータベース サービスがダウンしています。IM and Presence サービスは、ノード2への自動フェールオーバーを実行します。 推奨処置： <ol style="list-style-type: none"> 1. ノード1をリブートします。 2. リブート後にすべての重要なサービスが起動して実行中になったら、手動フォールバックを実行してプレゼンス冗長グループのノードを[正常(Normal)]状態に復元します。

ノード 1		ノード 2		原因/推奨処置
状態	理由 (Reason)	状態	理由 (Reason)	
障害モードで実行中 (Running in Failed Mode)	重要なサービスの開始が失敗	障害モードで実行中 (Running in Failed Mode)	重要なサービスの開始が失敗	<p>他のノードからプレゼンス冗長グループのノードへのテイクバック中は、重要なサービスを開始できません。</p> <p>推奨処置。テイクバック中のノード上で、次の操作を実行します。</p> <ol style="list-style-type: none"> 1. ノードにダウンしている重要なサービスがないかどうかを確認します。これらのサービスを手動で開始するには、[プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウで[リカバリ(Recovery)]をクリックします。 2. 重要なサービスが開始されない場合は、ノードをリポートします。 3. リポート後にすべての重要なサービスが起動して実行中になったら、手動フォールバックを実行してプレゼンス冗長グループのノードを[正常(Normal)]状態に復元します。
障害モードで実行中 (Running in Failed Mode)	重要なサービスのダウン	障害モードで実行中 (Running in Failed Mode)	重要なサービスのダウン	<p>バックアップノード上で重要なサービスがダウンしました。両方のノードが失敗状態に入ります。</p> <p>推奨処置：</p> <ol style="list-style-type: none"> 1. バックアップノードにダウンしている重要なサービスがないかどうかを確認します。これらのサービスを手動で開始するには、[プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウで[リカバリ(Recovery)]をクリックします。 2. 重要なサービスが開始されない場合は、ノードをリポートします。

ノード1		ノード2		原因/推奨処置
状態	理由 (Reason)	状態	理由 (Reason)	
ネットワーク接続が失われているためにノード1がダウンしているか、SRM サービスが実行されていません。		バックアップモードで実行中 (Running in Backup Mode)	ピアダウン	<p>ノード2がノード1からのハートビートを見失いました。IM and Presence サービスは、ノード2への自動フェールオーバーを実行します。</p> <p>推奨処置。ノード1が起動したら、次の操作を実行します。</p> <ol style="list-style-type: none"> 1. プレゼンス冗長グループのノード間のネットワーク接続を確認し、修復します。ノード間のネットワーク接続を再確立すると、ノードが失敗状態になる場合があります。 [プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウで[リカバリ(Recovery)]をクリックして、ノードを「通常」状態に復元します。 2. SRMサービスを開始し、手動フォールバックを実行して、プレゼンス冗長グループのノードを[正常(Normal)]状態に復元します。 3. (ノードがダウンしている場合) ノード1を修復し、電源を入れます。 4. ノードが起動し、すべての重要なサービスが実行中になったら、手動フォールバックを実行してプレゼンス冗長グループのノードを[正常(Normal)]状態に復元します。

ノード 1		ノード 2		原因/推奨処置
状態	理由 (Reason)	状態	理由 (Reason)	
	(電源切断、ハードウェア障害、シャットダウン、リブートなどにより) ノード1がダウンしています。	バックアップモードで実行中 (Running in Backup Mode)	ピアリブート	<p>ノード1上で次のような条件が発生したため、IM and Presence サービスはノード2への自動フェールオーバーを実行しました。</p> <ul style="list-style-type: none"> • ハードウェア障害 • 電源切断 • 再起動 • shutdown <p>推奨処置 :</p> <ol style="list-style-type: none"> 1. ノード1を修復し、電源を入れます。 2. ノードが起動し、すべての重要なサービスが実行中になったら、手動フォールバックを実行してプレゼンス冗長グループのノードを [正常(Normal)] 状態に復元します。
[フェールオーバー/重要なサービスが実行されていません (Failed Over with Critical Services not Running)] または [フェールオーバー完了 (Failed Over)]	初期化	バックアップモード (Backup Mode)	初期化中のピアダウン	<p>起動中、ノード2はノード1を参照しません。</p> <p>推奨処置 :</p> <p>ノード1が起動し、すべての重要なサービスが実行中になったら、手動フォールバックを実行してプレゼンス冗長グループのノードを [正常(Normal)] 状態に復元します。</p>

ノード 1		ノード 2		原因/推奨処置
状態	理由 (Reason)	状態	理由 (Reason)	
障害モードで実行中 (Running in Failed Mode)	[Cisco Server Recovery Manager によるユーザのテイクオーバーが失敗(Cisco Server Recovery Manager Take Over Users Failed)]	障害モードで実行中 (Running in Failed Mode)	[Cisco Server Recovery Manager によるユーザのテイクオーバーが失敗(Cisco Server Recovery Manager Take Over Users Failed)]	テイクオーバー プロセス中のユーザ移動は失敗します。 推奨処置 : データベースエラーの可能性がります。[プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウで、[リカバリ(Recovery)] をクリックしてください。問題が解決しない場合は、ノードをリブートします。
障害モードで実行中 (Running in Failed Mode)	Cisco Server Recovery Manager によるユーザのテイクバックが失敗 (Cisco Server Recovery Manager Take Back Users Failed)	障害モードで実行中 (Running in Failed Mode)	Cisco Server Recovery Manager によるユーザのテイクバックが失敗 (Cisco Server Recovery Manager Take Back Users Failed)	フォールバック プロセス中にユーザの移動に失敗しました。 推奨処置 : データベースエラーの可能性がります。[プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウで、[リカバリ(Recovery)] をクリックしてください。問題が解決しない場合は、ノードをリブートします。
障害モードで実行中 (Running in Failed Mode)	不明	障害モードで実行中 (Running in Failed Mode)	不明	他のノードの SRM が障害状態である、または内部システム エラーが発生すると、ノードの SRM が再起動します。 推奨処置 : [プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウで、[リカバリ(Recovery)] をクリックしてください。問題が解決しない場合は、ノードをリブートします。

ノード 1		ノード 2		原因/推奨処置
状態	理由 (Reason)	状態	理由 (Reason)	
バックアップがアクティブ (Backup Activated)	データベース障害からの自動回復 (Auto Recover Database Failure)	フェールオーバーがサービスに影響 (Failover Affected Services)	データベースの自動リカバリに失敗	バックアップ ノード上でデータベースがダウンしました。ピア ノードがフェールオーバーモードであり、プレゼンス冗長グループのすべてのユーザをテイクオーバーできます。自動リカバリ操作が自動的に行われ、すべてのユーザはプライマリ ノードに移動されます。
バックアップがアクティブ (Backup Activated)	データベース障害からの自動回復 (Auto Recover Database Failure)	フェールオーバーがサービスに影響 (Failover Affected Services)	重要なサービス停止からの自動回復 (Auto Recover Critical Service Down)	バックアップ ノード上で重要なサービスがダウンしました。ピア ノードがフェールオーバーモードであり、プレゼンス冗長グループのすべてのユーザをテイクオーバーできます。自動リカバリ操作が自動的に行われ、すべてのユーザはピア ノードに移動されます。
不明		不明		ノード状態は不明です。 原因として、IM and Presence サービス ノード上でハイ アベイラビリティが正しく有効にされなかったことが考えられます。 推奨処置： プレゼンス冗長グループの両方のノード上で、Server Recovery Manager サービスを再起動してください。

ダウンタイムをほぼゼロに抑える IM and Presence フェールオーバーの機能拡張

IM and Presence Service が拡張され、ノードおよびクラスタのアップグレードおよびフェールオーバー時の影響を減らして、Jabber サービスの停止を最小限に抑えます。

リリース 14 では、IM and Presence サービスは Jabber クライアントとのデュアル接続をサポートしています。クライアント側で有効にすると、この種の接続により、高可用性フェールオーバーイベント中のサービスダウンタイムがはるかに短くなります（ほぼゼロ）。

これにより、次が役立ちます。

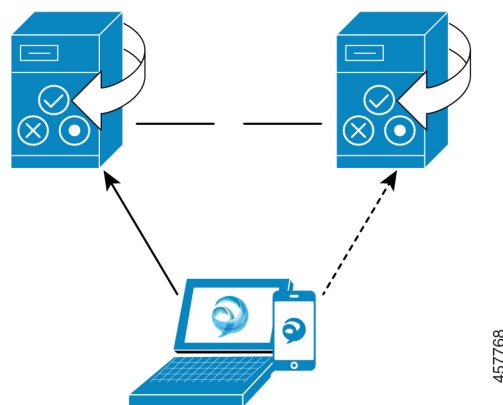
- IM and Presence Service の直接標準アップグレード中に Jabber クライアントへのサービスの中断を最小限に抑える
- プライマリノードとセカンダリノード間のユーザセッションのシームレスな移行を実現

Jabber クライアントでいくつかの追加設定でこの機能を有効にできます。Jabber でのデュアル接続を有効にする方法の詳細については、[Cisco Jabber 14 のパラメータリファレンスガイド](#)の「*EnableDualConnections* と *Inactive_Connection_Activation_Timer* パラメータ」を参照してください。

可能な限り短いダウンタイムを維持するために、次の前提条件を満たしていることを確認して、この機能拡張を有効にします。

- アップグレード中は高可用性（HA）を有効にしてください。
- リリースの互換性: モバイルおよびリモートアクセスユーザの場合は、Cisco Unified CM および IM and Presence リリース 14、Jabber リリース 14、Expressway 14。

図 2: IM Presence フェールオーバーの機能拡張



フェールオーバーの場合、この機能拡張により、ダウンタイムがゼロに近くなります。これは、Cisco Jabber クライアントが IM and Presence ノードとのデュアル接続を維持することで実現されます。アクティブな接続は、クライアントのログインプロセス中に作成されるプライマリノードで維持されます。バックアップノードとの非アクティブな接続は、クライアントの再ログイン下限とクライアントの再ログイン上限の値の間のランダムな間隔の後に作成されます。これらの制限は、Cisco Server Recovery Manager サービスのサービスパラメータとして設定されます。

フェールオーバーが発生すると、Jabber クライアントは「非アクティブ」接続をアクティブ化してサーバと通信します。非アクティブな接続がすでにバックアップノードに作成されている場合、Jabber のダウンタイムは最小限に抑えられます。



(注) Jabber のこのフェールオーバー拡張機能は、無制限 (XU) バージョンの IM and Presence サービスでは機能しません。これは、Jabber などの XMPP クライアントと IM and Presence サービス間の安全な TLS 接続が無制限バージョンで無効になっているためです。

制限付きバージョンでは、[セキュリティ設定] ページ ([システム]>[セキュリティ]>[設定]) で [XMPP クライアントから IM/P サービスのセキュアモードを有効にする] オプションがデフォルトで有効になっており、フェールオーバー拡張機能を Jabber と連携させることができます。フェールオーバー拡張を使用する場合は、このモードをオフにしないことをお勧めします。この制限事項の詳細については、CSCvx94284 を参照してください。

デュアル登録が確立した場合の確認方法

デュアル登録の確立を確認するために、プライマリノードに X ユーザを、セカンダリノードに Y を割り当てたシナリオを検討してください。プライマリノードの *JsmSessionsClient* カウンタと *JsmSessionsClientInactive* カウンタを確認すると、*JsmSessionsClient* に接続されているユーザの総数が X で、*JsmSessionsClientInactive* が Y であることがわかります。同時に、セカンダリノードでは、*JsmSessionsClient* は Y で、*JsmSessionsClientInactive* は X です。

デュアル登録を無効にする方法

サーバで HA を無効にすることなく、クライアント側で HA を無効にすることで、デュアル登録を無効にできます。また、HA を無効にすると、デュアル登録がサーバからクライアントに提供され、クライアントが非アクティブな接続を確立しようとすることはできません。Jabber でのデュアル接続を有効にする方法の詳細については、Cisco Jabber 14 のパラメータリファレンスガイドの「*EnableDualConnections* と *Inactive_Connection_Activation_Timer* パラメータ」を参照してください。

アップグレード中のダウンタイムゼロを監視するカウンタ

ダウンタイムをゼロにするためのアップグレードプロセスを追跡するには、リアルタイム監視ツールを使用して次のカウンタを監視できます。

表 5: アップグレード中のダウンタイムゼロを監視するカウンタ

カウンタ	説明
ActiveJsmSessions	このカウンタは、発行元ノードに割り当てられたアクティブなユーザの数を示します。フェールオーバー中は、プライマリ (アップグレード) ノードに対して 0 が表示され、アクティブなユーザがプライマリノードからバックアップノードに加算されます。
InactiveJsmSessions	このカウンタは、サブスクリバノードに割り当てられたアクティブなユーザの数を示します。

カウンタ	説明
JsmSessionsComposed	このカウンタは、JSM でアクティブな構成済みセッションの数を表します。
JsmSessionsClientInactive	このカウンタは、IDM に対して非アクティブなクライアントセッションの数を表します。
JsmSessionsClient	このカウンタは、IDM に対して非アクティブなクライアントセッションの数を表します。
JsmSessionsClientInactive	このカウンタは、IDM に対して非アクティブなクライアントセッションの数を表します。

冗長性の連携動作と制約事項

機能	データのやり取り
ユーザーの追加	いずれかのクラスタノードがフェールオーバー状態の間は、IM and Presence サービスクラスタに新規ユーザーを追加できません。
マルチデバイスメッセージング	フェールオーバーが発生した場合、マルチデバイスメッセージング機能により、IM and Presence サービスでサーバ回復に遅延が発生します。マルチデバイスメッセージングが設定されているシステムでサーバのフェールオーバーが発生すると、通常、[Cisco Server Recovery Manager] サービスパラメータで指定された時間の2倍かかります。

機能	データのやり取り
<p>プッシュ通知の高可用性</p>	<p>高可用性は、11.5 (1) SU3 時点のプッシュ通知配置でサポートされています。プッシュ通知が有効になっていて、ノードがフェールオーバーすると、iPhone および iPad クライアント上の Cisco Jabber に対して次のことが起こります。</p> <ul style="list-style-type: none"> • フォアグラウンドモードの Cisco Jabber クライアントの場合、Jabber クライアントはバックアップノードに自動的にログインし、メインノードが回復するまで引き継ぎます。バックアップノードが引き継ぐときも、メインノードが回復するときも、サービスに中断はありません。 • バックグラウンドモードの Cisco Jabber クライアントの場合、バックアップノードが引き継ぎますが、プッシュ通知が送信されるまでに遅延があります。Jabber クライアントはバックグラウンドモードであるため、ネットワークへのアクティブな接続がないため、バックアップノードに自動的にログインしません。バックアップノードは、プッシュ通知を送信する前に、バックグラウンドモードにあるすべてのフェイルオーバーユーザに対して JSM セッションを再作成する必要があります。 <p>遅延の長さはシステム負荷によって異なります。テストによると、HA ペアでユーザが均等に分散された 15,000 ユーザの OVA の場合、フェイルオーバー後にプッシュ通知が送信されるまでに 10〜20 分かかります。この遅延は、バックアップノードが引き継ぐとき、およびメインノードが回復した後にも発生します。</p> <p>(注) ノード障害または予期しない Cisco XCP Router のクラッシュの場合、IM 履歴を含むユーザの IM セッションは、ユーザアクションを必要とすることなく維持されます。ただし、Cisco Jabber on iPhone または iPad のクライアントが保留モードであった場合、クラッシュしたときにサーバ上にキューされていた未開封メッセージを取得することはできません。</p>

機能	データのやり取り
<p>ユーザの一時的なプレゼンスステータス</p>	<p>ユーザの一時的なプレゼンスステータスで、フェールオーバー、フォールバック、およびユーザの移動の後に、古いプレゼンスステータスが表示されます。これは、一時的なプレゼンスに対するサブスクリプションが削除されたためであり、ユーザの有効な一時的プレゼンスステータスを表示するためには、ユーザが一時的なプレゼンスに登録し直す必要があります。</p> <p>たとえば、ユーザ A がユーザ B の一時的なプレゼンスに登録されており、ユーザ B が割り当てられている IM and Presence ノードでフェールオーバーが発生した場合、ユーザ B がバックアップノードに再ログインした後も、ユーザ B はユーザ A に対してオフラインと表示されます。これは、ユーザ B の一時的なプレゼンスに対するサブスクリプションが削除され、ユーザ A が削除を認識していないためです。ユーザ A は、ユーザ B の一時的な存在を再度サブスクライブする必要があります。</p> <p>ユーザ A が Jabber クライアントから User B の検索を削除すると、ユーザ B の一時的なプレゼンスの検索を試みるまでに、ユーザ A は少なくとも 30 秒待つ必要があります。一致しない場合、ユーザ A にはユーザ B の古いプレゼンスが表示されます。Jabber クライアントは、有効な一時プレゼンスステータスを取得するために、同じユーザに対する 2 回の検索の間で少なくとも 30 秒待つ必要があります。</p>



第 6 章

ユーザ設定値の設定

- [エンドユーザ設定の概要 \(77 ページ\)](#)
- [ユーザ設定の前提条件 \(78 ページ\)](#)
- [ユーザ設定タスクフローの設定 \(79 ページ\)](#)

エンドユーザ設定の概要

サービスプロファイルや機能グループテンプレートなどのユーザ設定を使用して、LDAP ディレクトリ同期を介してエンドユーザに共通の設定を適用できます。LDAP ディレクトリの同期が行われると、設定された設定が同期されたすべてのユーザに適用されます。



(注) この章では、特に IM and Presence サービスに適用されるユーザ設定について説明します。ボイスメールや会議などの UC サービスを含む、一般的な UC ユーザ設定については、の「エンドユーザの設定」を参照してください。Cisco Unified Communications Manager システムコンフィギュレーションガイド。LDAP 同期の一部としてこれらの設定を適用できます。

サービスプロファイル

サービスプロファイルには共通ユニファイド コミュニケーション (UC) サービスの設定が含まれています。異なるユーザグループごとに異なるサービスプロファイルを設定でき、その結果、各グループのユーザが、仕事に合わせて設定された適切なサービスを利用できます。エンドユーザが IM and Presence サービスにアクセスできるようにするには、IM and Presence サービスが含まれるようにサービスプロファイルを設定します。

エンドユーザにサービスプロファイルを適用するには、次の方法を使用します。

- LDAP 同期されたユーザ向け：LDAP ディレクトリからエンドユーザをインポートした場合、サービスプロファイルを機能グループテンプレートに割り当てることができ、その機能グループテンプレートをエンドユーザに適用できます。テンプレートの設定は、同期されているすべてのユーザに適用されます。

- アクティブなローカルユーザ（つまり、LDAP ユーザ以外） - 一括管理ツールを使用して CSV ファイルまたはスプレッドシートを介してサービスプロファイル設定を適用します。一括管理ツールの使用方法の詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html> を参照してください。

それ以外の場合は、ユーザごとに手動でユーザ設定を構成できます。

機能グループテンプレートの概要

機能グループテンプレートを使用すると、LDAP ディレクトリの同期を通じて、共通設定をエンドユーザのグループにすばやく適用できます。たとえば、機能グループテンプレートを使用して、エンドユーザに対して **IM and Presence** サービスを有効にすることができます。これは、**IM and Presence** 対応のサービスプロファイルをテンプレートに適用することによって実現されます。機能グループテンプレートを LDAP ディレクトリ同期に適用すると、同期が行われると、設定されたサービスプロファイルとユーザプロファイルの設定を含むテンプレートからの設定が、同期されたすべてのユーザに適用されます。

機能グループテンプレート設定には、機能グループテンプレートに割り当てられる次のプロファイルが含まれます。

- ユーザプロファイル：一連の共通の電話および電話回線の設定が含まれます。ユーザプロファイルには、共通の電話回線設定を割り当てるユニバーサル回線テンプレートと、共通の電話設定を割り当てるユニバーサルデバイステンプレートを設定する必要があります。これらのテンプレートは、セルフプロビジョニングするように設定されているユーザが自身の電話を設定する際に役立ちます。
- サービスプロファイル：IM and Presence サービス、ディレクトリ、ボイスメールなどの一般的な UC サービスのグループが含まれています。

ユーザ設定の前提条件

ユーザを移動したい場合 IM and Presence サービスクラスタの場合は、エンドユーザを設定する前に設定する必要があります。Cisco Unified CM IM and Presence の管理を使用して、ユーザを移行し、連絡先リストをエクスポートおよびインポートする方法についての詳細。



- (注) クラスタ間でのユーザの移行を、パーティション化ドメイン内フェデレーションに使用されるユーザ移行ツールと混同しないでください。



- (注) Cisco Jabber を VPN 経由で接続している場合は、IM and Presence Service と Cisco Jabber クライアント間の TLS ハンドシェイク中に、IM and Presence サーバでクライアントの IP サブネットに対する逆引き参照が実行されます。逆引き参照に失敗すると、クライアントマシンで TLS ハンドシェイクがタイムアウトします。

ユーザ設定タスクフローの設定

IM and Presence サービスに対してエンドユーザを有効にするなど、共通のサービスおよび機能設定を使用してユーザテンプレートを設定するには、次の作業を実行します。LDAP 同期が完了すると、テンプレート設定がエンドユーザに適用されます。



- (注) この章のタスクフローは、IM and Presence サービスに特に適用されるユーザ設定です。ボイスメールや会議などの UC サービスを含む、一般的な UC ユーザ設定については、の「エンドユーザの設定」を参照してください。Cisco Unified Communications Manager システムコンフィギュレーションガイド。LDAP 同期の一部としてこれらの設定を適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザー割り当てモードの設定 (80 ページ)	ユーザー割り当てモードを平衡、アクティブ-スタンバイ、またはなしに設定します。
ステップ 2	IM and Presence UC サービスの追加 (80 ページ)	IM and Presence UC サービスを Cisco Unified Communications Manager に設定する。
ステップ 3	サービスプロファイルの設定 (81 ページ)	追加した IM and Presence UC サービスが含まれるサービス プロファイルを設定します。
ステップ 4	機能グループ テンプレートの設定 (82 ページ)	他の共通の機能設定に加えて設定したサービスプロファイルを含む機能グループ テンプレートを設定します。

次のタスク

LDAP 同期を完了して、LDAP 同期ユーザに設定を適用します。

ユーザー割り当てモードの設定

この手順を使用すると、Sync Agent がクラスタ内のノードにユーザを分散させる方法を設定できます。

手順

ステップ 1 Cisco Unified CM の管理から、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] を選択します。

ステップ 2 [ユーザ管理パラメータ (User Management Parameters)] 領域で、[プレゼンスサーバのユーザー割り当てモード (User Assignment Mode for Presence Server)] パラメータに次のいずれかのオプションを選択します。

- [バランス (Balanced)] : このモード (デフォルト) では、ユーザを各サブクラスタのそれぞれのノードに均等に割り当て、各ノードにユーザの合計数が均等に分散するようにします。これがデフォルトのオプションです。
- [アクティブスタンバイ (Active-Standby)] : このモードでは、サブクラスタの最初のノードにすべてのユーザを割り当て、セカンダリサーバをバックアップのままにします。
- [なし (None)] : このモードでは、Sync Agent でクラスタのノードにユーザが割り当てられません。

ステップ 3 [保存 (Save)] をクリックします。

次のタスク

[IM and Presence UC サービスの追加 \(80 ページ\)](#)

IM and Presence UC サービスの追加

Cisco Unified Communications Manager でこの手順を使用して、IM and Presence サービス用の UC サービスを追加します。

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [UC サービス (UC Service)] を選択します。

ステップ 2 [新規追加 (Add New)] をクリックします。

ステップ 3 [UC サービスタイプ (UC Service Type)] ドロップダウンリストボックスから、[IM and Presence] を選択します。

ステップ 4 [製品タイプ (Product Type)] ドロップダウンリストボックスから、[Unified CM (IM and Presence)] を選択します。

ステップ 5 IM and Presence サービスの [名前 (Name)] と [説明 (Description)] を入力します。

ステップ 6 [ホスト名/IPアドレス (Hostname/IP Address)] フィールドに、IM and Presence サービスをホストするサーバのホスト名、IP アドレス、または DNS SRV を入力します。

ステップ 7 [保存 (Save)] をクリックします。

次のタスク

IM and Presence サービスのユーザを有効にするには、UC サービスをサービス プロファイルに割り当て、そのプロファイルをユーザに割り当てます。

[サービス プロファイルの設定 \(81 ページ\)](#)。

サービス プロファイルの設定

この手順を使用すると、IM and Presence サービスが含まれるサービス プロファイルを設定できます。

始める前に

[IM and Presence UC サービスの追加 \(80 ページ\)](#)

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [サービスプロファイル (Service Profile)] を選択します。

ステップ 2 次のいずれかを実行します。

- [検索 (Find)] をクリックし、既存のプロファイルを選択します。
- [新規追加 (Add New)] をクリックして新しいプロファイルを作成します。

ステップ 3 [IM and Presenceプロファイル (IM and Presence Profile)] セクションで、**プライマリ IM and Presence** サーバを選択します。

ステップ 4 [サービスプロファイルの設定 (Service Profile Configuration)] ウィンドウで、残りのフィールドを入力します。フィールドとその設定を含むヘルプは、オンラインヘルプを参照してください。

ステップ 5 [保存 (Save)] をクリックします。

次のタスク

[機能グループ テンプレートの設定 \(82 ページ\)](#)

機能グループテンプレートの設定

共通の機能設定と、設定した IM and Presence 対応サービス プロファイルを含む機能グループテンプレートを設定します。

始める前に

[サービスプロファイルの設定 \(81 ページ\)](#)

手順

-
- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] で、[ユーザ管理 (User Management)] > [ユーザ/電話の追加 (User/Phone Add)] > [機能グループテンプレート (Feature Group Template)] を選択します。
 - ステップ 2 [新規追加] をクリックします。
 - ステップ 3 機能グループテンプレートの [名前 (Name)] と [説明 (Description)] を入力します。
 - ステップ 4 このテンプレートを使用するすべてのユーザのホーム クラスタとしてローカルクラスタを使用する場合は、[ホームクラスタ (Home Cluster)] チェック ボックスをオンにします。
 - ステップ 5 このテンプレートを使用するユーザがインスタントメッセージおよびプレゼンス情報を交換できるようにするには、[Unified CM IM and Presenceのユーザを有効化 (Enable User for Unified CM IM and Presence)] チェックボックスをオンにします。
 - ステップ 6 ドロップダウンリストから、[サービスプロファイル (Services Profile)] および [ユーザプロファイル (User Profile)] を選択します。
 - ステップ 7 [機能グループテンプレートの設定 (Feature Group Template Configuration)] ウィンドウの残りのフィールドに入力します。フィールドの説明については、オンラインヘルプを参照してください。
 - ステップ 8 [保存] をクリックします。
-

次のタスク

この機能グループテンプレートを含むLDAPディレクトリ同期を設定します。LDAP同期を完了すると、テンプレート内の IM and Presence の設定が同期済みユーザに適用されます。[LDAP同期設定のタスクフロー \(85 ページ\)](#) を参照してください。



第 7 章

LDAP ディレクトリの設定

- [LDAP 同期の概要 \(83 ページ\)](#)
- [LDAP 同期の前提条件 \(85 ページ\)](#)
- [LDAP 同期設定のタスク フロー \(85 ページ\)](#)

LDAP 同期の概要

Lightweight Directory Access Protocol (LDAP) の同期は、システムのエンドユーザのプロビジョニングと設定を支援します。LDAP の同期中、システムは外部 LDAP ディレクトリから Cisco Unified Communications Manager データベースにユーザのリストと関連するユーザデータをインポートします。インポートしている間に、エンドユーザを設定することもできます。



- (注) Unified Communication Manager は、LDAPS (SSL を使用した LDAP) をサポートしますが、StartTLS を使用した LDAP はサポートしていません。LDAP サーバ証明書を Unified Communication Manager に Tomcat-Trust 証明書としてアップロードします。

サポートされている LDAP ディレクトリの詳細については、*Cisco Unified Communications Manager* と *IM and Presence Service* の互換性マトリクスを参照してください。

LDAP 同期では、以下の機能がアドバタイズされます。

- **エンドユーザのインポート** : LDAP 同期を使用して、システムの初期設定時にユーザー一覧を会社の LDAP ディレクトリから Unified Communication Manager のデータベースにインポートできます。機能グループテンプレート、ユーザプロファイル、サービスプロファイル、ユニバーサルデバイス、回線テンプレートなどの設定項目が設定されている場合は、設定をユーザに適用することができ、また、同期プロセス中に設定したディレクトリ番号とディレクトリ Uri を割り当てることができます。LDAP 同期プロセスは、ユーザーリストとユーザー固有のデータをインポートし、設定した構成テンプレートを適用します。



- (注) 初期同期が実行された以降は、LDAP 同期を編集することはできません。

- **スケジュールされた更新**：Unified Communication Manager をスケジュールされた間隔で複数のLDAPディレクトリと同期するように設定できます。これによって確実にデータベースが定期的に更新され、すべてのユーザデータを最新に保ちます。
- **エンドユーザの認証**：LDAP同期を使用して、システムがCisco Unified Communications Manager データベースではなく、LDAPディレクトリに対してエンドユーザーパスワードを認証するように設定できます。LDAP認証によって、企業は、すべての企業内アプリケーションに対応する単一のパスワードをエンドユーザに割り当てることができます。この機能は、PIN またはアプリケーションユーザーパスワードには適用されません。
- **シスコ モバイルおよびリモートアクセスのクライアントおよびエンドポイントのディレクトリ サーバ ユーザ検索**：社内ディレクトリサーバが企業ファイアウォール外で運用されている場合でも検索できます。この機能を有効にすると、ユーザデータ サービス (UDS) がプロキシとして機能し、Unified Communications Manager データベースにユーザ検索要求を送信する代わりに、それを社内ディレクトリに送信します。

[エンドユーザ用LDAP認証 (LDAP Authentication for End Users)]

LDAP同期を使用して、システムがCisco Unified Communications Manager データベースではなく、LDAPディレクトリに対してエンドユーザパスワードを認証するように設定できます。LDAP認証によって、企業は、すべての企業内アプリケーションに対応する単一のパスワードをエンドユーザに割り当てることができます。この機能は、PIN またはアプリケーションユーザーパスワードには適用されません。

Cisco モバイルおよびリモートアクセス クライアントとエンドポイントに対するディレクトリ サーバ ユーザの検索

以前のリリースでは、Cisco Mobile とリモートアクセスクライアント（たとえば、Cisco Jabber）またはエンドポイント（たとえば、Cisco DX 80 電話）を使用しているユーザが企業ファイアウォールの外部でユーザ検索を実行した場合、結果はCisco Unified Communications Manager に保存されたユーザアカウントに基づいていました。データベースには、ローカルで設定されたか、または社内ディレクトリから同期されたユーザアカウントも含まれています。

このリリースでは、Cisco Mobile およびリモートアクセスクライアントとエンドポイントは、企業ファイアウォールの外部で動作している場合でも、社内ディレクトリサーバを検索できます。この機能を有効にすると、ユーザデータサービス (UDS) がプロキシとして機能し、Cisco Unified Communications Manager データベースにユーザ検索要求を送信する代わりに、それを社内ディレクトリに送信します。

この機能を使用して、次の結果を実現できます。

- **地理的な場所に関係なく、同じユーザ検索結果を提供する**：モバイルおよびリモートアクセスクライアントとエンドポイントは、社内ディレクトリを使用してユーザ検索を実行できます。企業ファイアウォールの外部で接続されている場合でも実行可能です。

- Cisco Unified Communications Manager データベースに設定されるユーザアカウントの数を削減する：モバイルクライアントは、社内ディレクトリ内のユーザー検索できます。以前のリリースでは、ユーザー検索結果はデータベースに設定されているユーザに基づいていました。今回のリリースでは、ユーザー検索のためだけにユーザアカウントをデータベースに設定または同期する必要がなくなりました。管理者は、クラスタによって管理されているユーザアカウントを設定すれば作業が完了します。データベース内のユーザアカウントの合計数が削減すると、データベース全体のパフォーマンスが改善される一方、ソフトウェアアップグレードの時間枠が短縮されます。

この機能を設定するには、[LDAP 検索の設定 (LDAP Search Configuration)] ウィンドウで [企業ディレクトリ サーバでのユーザー検索を有効にする (Enable user search to Enterprise Directory Server)] オプションを有効にし、LDAP ディレクトリ サーバの詳細を設定する必要があります。詳細については、[エンタープライズディレクトリ ユーザー検索の設定 \(91 ページ\)](#) の手順を参照してください。

LDAP 同期の前提条件

前提条件のタスク

LDAP ディレクトリからエンドユーザをインポートする前に、次のタスクを実行します。

- ユーザアクセスの設定
- クレデンシャルポリシーの設定
- 機能グループテンプレートの設定

自分のシステムにデータを同期するユーザについて、アクティブディレクトリサーバ上の電子メール ID フィールドが確実に単一エントリまたは空白になっているようにします。

LDAP 同期設定のタスクフロー

外部LDAPディレクトリからユーザリストをプルし、Unified Communication Manager のデータベースにインポートするには、以下のタスクを使用します。



- (注) LDAP ディレクトリをすでに一度同期している場合、外部LDAPディレクトリから新しい項目を同期することはできますが、Unified Communication Manager 内の新しい設定をLDAPディレクトリ同期に追加することはできません。この場合、一括管理ツールと、[ユーザの更新 (Update Users)] や [ユーザの挿入 (Insert Users)] などのメニューを使用できます。『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco DirSync サービスの有効化 (86 ページ)	Cisco Unified Serviceability にログインし、Cisco DirSync サービスを有効にします。
ステップ 2	LDAP ディレクトリ同期の有効化 (87 ページ)	Unified Communication Manager の LDAP ディレクトリ同期を有効化します。
ステップ 3	LDAP フィルタの作成 (88 ページ)	オプション Unified Communication Manager に社内 LDAP ディレクトリからユーザのサブセットだけを同期するには、LDAP フィルタを作成します。
ステップ 4	LDAP ディレクトリの同期の設定 (88 ページ)	アクセス制御グループ、機能グループのテンプレートとプライマリ エクステンションのフィールド設定、LDAP サーバのロケーション、同期スケジュール、および割り当てなどの LDAP ディレクトリ同期を設定します。
ステップ 5	エンタープライズ ディレクトリ ユーザー検索の設定 (91 ページ)	オプション エンタープライズ ディレクトリ サーバ ユーザを検索するシステムを設定します。システムの電話機とクライアントをデータベースの代わりにエンタープライズ ディレクトリ サーバに対してユーザの検索を実行するように設定するには、次の手順に従います。
ステップ 6	LDAP 認証の設定 (93 ページ)	オプション エンドユーザーパスワード認証に LDAP ディレクトリを使用するには、LDAP 認証を設定します。
ステップ 7	LDAP アグリーメント サービス パラメータのカスタマイズ (94 ページ)	オプション 任意指定の [LDAP 同期 (LDAP Synchronization)] サービス パラメータを設定します。ほとんどの導入の場合、デフォルト値のままです。

Cisco DirSync サービスの有効化

Cisco DirSync サービスをアクティブにするには、Cisco Unified Serviceability で次の手順を実行します。社内 LDAP ディレクトリでエンドユーザの設定を同期するには、このサービスをアクティブにする必要があります。

手順

- ステップ 1 Cisco Unified Serviceability から、[ツール (Tools)] > [サービスのアクティベーション (Service Activation)] を選択します。
- ステップ 2 [サーバ (Server)] ドロップダウン リストからパブリッシャ ノードを選択します。
- ステップ 3 [ディレクトリ サービス (Directory Services)] の下の [Cisco DirSync] オプション ボタンをクリックします。
- ステップ 4 [保存] をクリックします。

LDAP ディレクトリ同期の有効化

エンド ユーザの設定を社内 LDAP ディレクトリから同期させるには、以下の手順で Unified Communication Manager を設定します。



- (注) LDAP ディレクトリをすでに一度同期している場合、外部 LDAP ディレクトリから新しい項目を同期することはできませんが、Unified Communications Manager 内の新しい設定を LDAP ディレクトリ同期に追加することはできません。また、機能グループテンプレートやユーザプロフィールなどの基になる構成アイテムの編集を追加することもできません。すでに1回のLDAP同期を完了しており、別の設定でユーザを追加する場合は、ユーザの更新やユーザの挿入などの一括管理メニューを使用できます。

手順

- ステップ 1 Cisco Unified CM Administration から、[システム (System)] > [LDAP] > [LDAPシステム (LDAP System)] を選択します。
- ステップ 2 Unified Communications Manager で、LDAP ディレクトリからユーザをインポートするには、**LDAP サーバからの同期を有効にする** チェックボックスをオンにします。
- ステップ 3 **LDAP サーバタイプ** ドロップダウン リストから、使用する LDAP ディレクトリ サーバの種類を選択します。
- ステップ 4 [ユーザ IDのLDAP属性 (LDAP Attribute for User ID)] ドロップダウン リストで、[エンドユーザの設定 (End User Configuration)] ウィンドウの [ユーザー ID (User ID)] フィールドに関して、Unified Communications Manager で同期する社内 LDAP ディレクトリから属性を選択します。
- ステップ 5 [保存] をクリックします。

LDAP フィルタの作成

LDAP フィルタを作成することで、LDAP 同期を LDAP ディレクトリからのユーザのサブセットのみに制限することができます。LDAP フィルタを LDAP ディレクトリに適用する場合、Unified Communications Manager は、フィルタに一致するユーザのみを LDAP ディレクトリからインポートします。



(注) LDAP フィルタを設定する場合は、RFC4515 に指定されている LDAP 検索フィルタ標準に準拠する必要があります。

手順

- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] で、[システム (System)] > [LDAP(LDAP)] > [LDAP フィルタ (LDAP Filter)] を選択します。
- ステップ 2 [新規追加 (Add New)] をクリックして、新しい LDAP フィルタを作成します。
- ステップ 3 [フィルタ名 (Filter Name)] テキストボックスに、LDAP フィルタの名前を入力します。
- ステップ 4 [フィルタ (Filter)] テキストボックスに、フィルタを入力します。フィルタは、UTF-8 で最大 1024 文字まで入力できます。また、丸カッコ (()) で囲みます。
- ステップ 5 [保存] をクリックします。

LDAP ディレクトリの同期の設定

LDAP ディレクトリと同期するように Unified Communications Manager を設定するには、この手順を使用します。LDAP ディレクトリ同期により、エンドユーザのデータを外部の LDAP ディレクトリから Unified Communication Manager データベースにインポートして、エンドユーザの設定ウィンドウに表示することができます。ユニバーサル回線とデバイステンプレートを使用する機能グループテンプレートがセットアップされている場合は、新しくプロビジョニングされるユーザとその内線番号に自動的に設定を割り当てることができます。



ヒント アクセス制御グループまたは機能グループテンプレートを割り当てる場合は、LDAP フィルタを使用して、インポートを同じ設定要件のユーザグループに限定できます。

手順

- ステップ 1 Cisco Unified CM Administration で、[System (システム)] > [LDAP (LDAP)] > [LDAP Directory (LDAP ディレクトリ)] を選択します。
- ステップ 2 次のいずれかの手順を実行します。

- [検索 (Find)] をクリックし、既存の LDAP ディレクトリを選択します。
- [新規追加 (Add New)] をクリックして、新しい LDAP ディレクトリを作成します。

ステップ 3 [LDAPディレクトリの設定 (LDAP Directory Configuration)] ウィンドウで、次のように入力します。

- [LDAP設定名 (LDAP Configuration Name)] フィールドで、LDAP ディレクトリに一意の名前を割り当てます。
- [LDAP マネージャ識別名 (LDAP Manager Distinguished Name)] フィールドに、LDAP ディレクトリ サーバにアクセスできるユーザー ID を入力します。
- パスワードの詳細を入力し、確認します。
- [LDAPユーザー検索スペース (LDAP User Search Space)] フィールドに、検索スペースの詳細を入力します。
- [ユーザ同期用のLDAPカスタムフィルタ (LDAP Custom Filter for Users Synchronize)] フィールドで、[ユーザのみ (Users Only)] または [ユーザとグループ (Users and Groups)] を選択します。
- (オプション) 特定のプロファイルに適合するユーザのサブセットのみにインポートを限定する場合は、[グループ用LDAPカスタムフィルタ (LDAP Custom Filter for Groups)] ドロップダウンリストから LDAP フィルタを選択します。

ステップ 4 **LDAP ディレクトリ同期スケジュール** フィールドに、外部 LDAP ディレクトリとデータ同期を行うために Unified Communication Manager が使用するスケジュールを作成します。

ステップ 5 [同期対象の標準ユーザ フィールド (Standard User Fields To Be Synchronized)] セクションを記入します。各エンドユーザのフィールドで、それぞれ LDAP 属性を選択します。同期プロセスが LDAP 属性の値を Unified Communication Manager のエンドユーザ フィールドに割り当てます。

ステップ 6 URIダイヤリングを展開する場合は、ユーザのプライマリディレクトリURIアドレスに使用されるLDAP属性が割り当てられていることを確認してください。

ステップ 7 **同期するカスタムユーザフィールド** のセクションで、必要な LDAP 属性を持つカスタムユーザフィールド名を入力します。

ステップ 8 インポートしたエンドユーザを、インポートしたすべてのエンドユーザに共通するアクセスコントロールグループに割り当てるには、次の手順を実行します。

- [アクセス コントロール グループに追加 (Add to Access Control Group)] をクリックします。
- ポップアップ ウィンドウで、インポートされたエンドユーザに割り当てる各アクセス制御グループごとに、対応するチェックボックスをオンにします。
- [選択項目の追加 (Add Selected)] をクリックします。

ステップ 9 機能グループ テンプレート を割り当てる場合は、[機能グループテンプレート (Feature Group Template)] ドロップダウンリストからテンプレートを選択します。

(注) エンドユーザは、そのユーザが存在しない初回のみ、割り当てられた機能グループテンプレートと同期されます。既存の [機能グループテンプレート (Feature Group Template)] が変更され、関連付けられた LDAP の完全同期が実行される場合、変更点は更新されません。

- ステップ 10** インポートされた電話番号にマスクを適用して、プライマリ内線番号を割り当てるには、次の手順を実行します。
- [挿入されたユーザの新規回線を作成するために、同期された電話番号にマスクを適用する (Apply mask to synced telephone numbers to create a new line for inserted users)] チェックボックスをオンにします。
 - [マスク (Mask)] を入力します。たとえば、インポートされた電話番号が 8889945 である場合、11XX のマスクによって 1145 のプライマリ内線番号が作成されます。
- ステップ 11** ディレクトリ番号のプールからプライマリ内線番号を割り当てる場合は、次の手順を実行します。
- [同期された LDAP 電話番号に基づいて作成されなかった場合、プールリストから新しい回線を割り当て (Assign new line from the pool list if one was not created based on a synced LDAP telephone number)] チェックボックスをオンにします。
 - [DN プールの開始 (DN Pool Start)] テキストボックスと [DN プールの終了 (DN Pool End)] テキストボックスに、プライマリ内線番号を選択するディレクトリ番号の範囲を入力します。
- ステップ 12** [LDAPサーバ情報 (LDAP Server Information)] セクションで、LDAP サーバのホスト名または IP アドレスを入力します。
- ステップ 13** TLS を使用して LDAP サーバに対するセキュアな接続を作成する場合は、[TLSを使用 (Use TLS)] チェックボックスをオンにします。
- ステップ 14** [保存] をクリックします。
- ステップ 15** LDAP同期を完了するには、**完全同期の実行**をクリックします。それ以外の場合は、スケジュールされた同期を待つことができます。
-



- (注) LDAP で削除されたユーザは、24 時間後に Unified Communications Manager から自動的に削除されます。また、削除されたユーザが次のデバイスのモビリティユーザとして設定されている場合、これらの非アクティブなデバイスも自動的に削除されます。
- [リモート接続先プロファイル (Remote Destination Profile)]
 - リモート接続先プロファイル テンプレート
 - モバイルスマート クライアントプロファイル
 - CTI リモート デバイス
 - Spark リモート デバイス
 - Nokia S60
 - Cisco Dual Mode for iPhone
 - IMS-integrated Mobile (基本)
 - キャリア統合モバイル
 - [Cisco Dual Mode for Android]

エンタープライズ ディレクトリ ユーザー検索の設定

データベースではなくエンタープライズ ディレクトリ サーバに対してユーザー検索を実行するように、システムの電話機とクライアントを設定するには、次の手順を使用します。

始める前に

- LDAP ユーザー検索に選択するプライマリ、セカンダリ、および第 3 サーバが Unified Communication Manager のサブスクライバ ノードに到達可能なネットワークにあることを確認します。
- [システム (System)] > [LDAP] > [LDAPシステム (LDAP System)] を選択し、[LDAPシステムの設定 (LDAP System Configuration)] ウィンドウの [LDAPサーバタイプ (LDAP Server Type)] ドロップダウン リストから LDAP サーバのタイプを設定します。

手順

- ステップ 1** Cisco Unified CM の管理で、[システム (System)] > [LDAP] > [LDAP 検索 (LDAP Search)] を選択します。
- ステップ 2** エンタープライズ LDAP ディレクトリ サーバを使用してユーザー検索を実行するには、[エンタープライズ ディレクトリ サーバのユーザ検索を有効にする (Enable user search to Enterprise Directory Server)] チェックボックスをオンにします。

ステップ 3 [LDAP 検索の設定 (LDAP Search Configuration)] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 4 [保存] をクリックします。

(注) OpenLDAP サーバでルーム オブジェクトとして表される会議室を検索するには、カスタム フィルタを (`(objectClass=intOrgPerson)(objectClass=rooms)`) に設定します。これにより、Cisco Jabber のクライアントがルーム名で電話会議室を検索し、ルームに関連付けられている番号をダイヤルできるようになります。

会議室は、ルーム オブジェクトの OpenLDAP サーバに、**givenName**、**sn**、**mail**、**displayName**、または **telephonenumber** の属性が設定されていると検索可能です。

ディレクトリ サーバの UDS 検索用の LDAP 属性

次の表に、[エンタープライズディレクトリ サーバに対するユーザ検索を有効化 (Enable user search to Enterprise Directory Server)] オプションが有効になっている場合に、UDS ユーザ検索要求で使用される LDAP 属性の一覧を示します。このようなタイプのディレクトリ要求の場合、UDS はプロキシとして機能して、社内ディレクトリ サーバに検索要求をリレーします。



(注) UDS ユーザの応答タグは、いずれかの LDAP 属性にマッピングされることがあります。属性のマッピングは、[LDAP サーバタイプ (LDAP Server Type)] ドロップダウンリストから選択するオプションによって決まります。このドロップダウンリストには、[システム (System)] > [LDAP] > [LDAP システムの設定 (LDAP System Configuration)] ウィンドウからアクセスします。

UDS ユーザの応答タグ	LDAP 属性
userName	<ul style="list-style-type: none"> • samAccountName • uid
firstName	givenName
lastName	sn
[middleName]	<ul style="list-style-type: none"> • [initials] • middleName
nickName	nickName
displayName	displayName
phoneNumber	<ul style="list-style-type: none"> • telephonenumber • ipPhone

UDS ユーザの応答タグ	LDAP 属性
homeNumber	homephone
mobileNumber	mobile
email	メールアドレス
directoryUri	<ul style="list-style-type: none"> • [msRTCSIP-primaryuseraddress] • [mail]
部署	<ul style="list-style-type: none"> • 部署 • departmentNumber
manager	manager
タイトル	タイトル
ポケットベル	ポケットベル

LDAP 認証の設定

LDAP 認証を有効にして、会社の LDAP ディレクトリに割り当てられているパスワードに対してエンドユーザーパスワードが認証されるようにするには、この手順を実行します。この設定は、エンドユーザのパスワードにのみ適用され、エンドユーザの PIN またはアプリケーションユーザーパスワードには適用されません。

手順

- ステップ 1** Cisco Unified CM の管理で、[システム (System)] > [LDAP] > [LDAP 認証 (LDAP Authentication)] を選択します。
- ステップ 2** [エンドユーザ用 LDAP 認証の使用 (Use LDAP Authentication for End Users)] チェックボックスをオンにして、ユーザー認証に LDAP ディレクトリを使用します。
- ステップ 3** [LDAP マネージャ識別名 (LDAP Manager Distinguished Name)] フィールドに、LDAP ディレクトリにアクセス権がある LDAP マネージャのユーザー ID を入力します。
- ステップ 4** [パスワードの確認 (Confirm Password)] フィールドに、LDAP マネージャのパスワードを入力します。
- ステップ 5** [LDAP ユーザー検索ベース (LDAP User Search Base)] フィールドに、検索条件を入力します。
- ステップ 6** [LDAP サーバ情報 (LDAP Server Information)] セクションで、LDAP サーバのホスト名または IP アドレスを入力します。
- ステップ 7** TLS を使用して LDAP サーバに対するセキュアな接続を作成する場合は、[TLS を使用 (Use TLS)] チェックボックスをオンにします。

ステップ 8 [保存] をクリックします。

次のタスク

[LDAP アグリーメント サービス パラメータのカスタマイズ \(94 ページ\)](#)

LDAP アグリーメント サービス パラメータのカスタマイズ

LDAP アグリーメントのシステムレベルでの設定をカスタマイズする、任意指定のサービスパラメータを設定するには、この手順を実行します。これらのサービスパラメータを設定しない場合、Unified Communications Manager により、LDAP ディレクトリ統合のデフォルト設定が適用されます。パラメータの説明については、ユーザインターフェイスでパラメータ名をクリックしてください。

サービス パラメータを使用して次の設定をカスタマイズできます。

- [最大アグリーメント数 (Maximum Number of Agreements)] : デフォルト値は 20 です。
- [最大ホスト数 (Maximum Number of Hosts)] : デフォルト値は 3 です。
- [ホスト障害時の再試行の遅延 (秒) (Retry Delay On Host Failure (secs))] : ホスト障害のデフォルト値は 5 です。
- [ホストリスト障害時の再試行の遅延 (分) (Retry Delay On HotList failure (mins))] : ホストリスト障害のデフォルト値は 10 です。
- [LDAP接続のタイムアウト (秒) (LDAP Connection Timeouts (secs))] : デフォルト値は 5 です。
- [遅延同期の開始時間 (分) (Delayed Sync Start time (mins))] : デフォルト値は 5 です。
- [ユーザカスタマーマップの監査時間 (User Customer Map Audit Time)]

手順

ステップ 1 Cisco Unified CM Administration から、[システム (System)] > [サービスパラメータ (Service Parameters)] を選択します。

ステップ 2 [サーバ (Server)] ドロップダウン リスト ボックスからパブリッシャ ノードを選択します。

ステップ 3 [サービス (Service)] ドロップダウン リスト ボックスから、[Cisco DirSync] を選択します。

ステップ 4 Cisco DirSync サービス パラメータの値を設定します。

ステップ 5 [保存] をクリックします。

LDAP ディレクトリ サービス パラメータ

サービス パラメータ	説明
Maximum Number of Agreements	自分で設定できる LDAP ディレクトリの最大数。デフォルト設定は 20 です。
Maximum Number of Hosts	フェールオーバー用に設定できる LDAP ホスト名の最大数。デフォルト値は 3 です。
Retry Delay on Host Failure (secs)	ホストで障害が発生した後、Cisco Unified Communications Manager が最初の LDAP サーバ (ホスト名) への接続を再試行する前の遅延秒数です。デフォルト値は 5 です。
Retry Delay on HostList Failure (mins)	ホストリストで障害が発生した後、Cisco Unified Communications Manager が設定された各 LDAP サーバ (ホスト名) への接続を再試行する前の遅延分数です。デフォルトは 10 です。
LDAP Connection Timeout (secs)	Cisco Unified Communications Manager が LDAP 接続を確立できる秒数です。指定した時間内に接続を確立できない場合、LDAP サービスプロバイダーは接続試行を中止します。デフォルトは 5 です。
Delayed Sync Start Time (mins)	Cisco DirSync サービスの起動後に、Cisco Unified Communications Manager がディレクトリ同期プロセスを開始するまでの遅延分数です。デフォルトは 5 です。

LDAP同期済みユーザのローカル ユーザへの変換

LDAP ディレクトリと Cisco Unified Communications Manager を同期すると、LDAP に同期されたエンドユーザについては、ローカルユーザに変換しないかぎり、[エンドユーザの設定 (End User Configuration)] ウィンドウ内のフィールドは編集できません。

[エンドユーザの設定 (End User Configuration)] ウィンドウで LDAP 同期ユーザのフィールドを編集するには、そのユーザをローカルユーザに変換します。ただし、この変換を行うと、Cisco Unified Communications Manager を LDAP ディレクトリと同期したときにエンドユーザが更新されなくなります。

手順

- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] で、[エンドユーザ (End Users)] > [エンドユーザ管理 (End User Management)] を選択します。
- ステップ 2 [検索 (Find)] をクリックして、エンドユーザを選択します。
- ステップ 3 [ローカルユーザへの変換 (Convert to Local User)] ボタンをクリックします。
- ステップ 4 [エンドユーザ設定 (End User Configuration)] ウィンドウでフィールドを更新します。

ステップ5 [保存 (Save)] をクリックします。

アクセスコントロールグループへのLDAP同期済みユーザの割り当て

LDAP と同期するユーザをアクセスコントロールグループに割り当てるには、次の手順を実行します。

始める前に

エンドユーザと外部LDAPディレクトリが同期されるように Cisco Unified Communications Manager を設定する必要があります。

手順

- ステップ1 Cisco Unified CM の管理で、[システム (System)] > [LDAP (LADP)] > [LDAP ディレクトリ (LDAP Directory)] を選択します。
- ステップ2 [検索 (Find)] をクリックし、設定したLDAPディレクトリを選択します。
- ステップ3 [アクセスコントロールグループに追加 (Add to Access Control Group)] ボタンをクリックします。
- ステップ4 このLDAPディレクトリのエンドユーザに適用するアクセスコントロールグループを選択します。
- ステップ5 [選択項目の追加 (Add Selected)] をクリックします。
- ステップ6 [保存 (Save)] をクリックします。
- ステップ7 [完全同期を実施 (Perform Full Sync)] をクリックします。
Cisco Unified Communications Manager が外部LDAPディレクトリと同期し、同期したユーザが正しいアクセスコントロールグループに挿入されます。

(注) 同期したユーザは、アクセスコントロールグループを初めて追加した時のみ、選択したアクセスグループに挿入されます。完全同期の実行後にLDAPに追加するグループは、同期したユーザに適用されません。

XMPPクライアントにおける連絡先検索のためのLDAPディレクトリ統合

次のトピックでは、サードパーティ製XMPPクライアントのユーザがLDAPディレクトリから連絡先を検索および追加できるように IM and Presence Service でLDAP設定を行う方法について説明します。

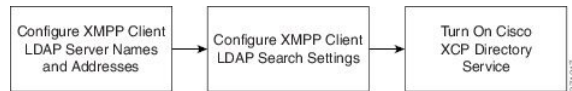
IM and Presence Service の JDS コンポーネントは、LDAPディレクトリとのサードパーティ製XMPPクライアント通信を処理します。サードパーティ製XMPPクライアントは、IM and

Presence Service の JDS コンポーネントにクエリを送信します。JDS コンポーネントは、プロビジョニングされた LDAP サーバに LDAP クエリを送信し、XMPP クライアントに結果を返します。

ここで説明する設定を実行する前に、XMPP クライアントを Cisco Unified Communications Manager および IM and Presence Service に統合するための設定を実行します。サードパーティ製 XMPP クライアントアプリケーションの統合に関するトピックを参照してください。

図 3: XMPP クライアントにおける連絡先検索のための LDAP ディレクトリ統合のワークフロー

次のワークフローの図は、XMPP クライアントで連絡先を検索するために LDAP ディレクトリを統合する手順の概要です。



次の表に、XMPP クライアントで連絡先を検索するために LDAP ディレクトリを統合するタスクのリストを示します。詳細な手順については、関連するタスクを参照してください。

表 6: XMPP クライアントにおける連絡先検索のための LDAP ディレクトリ統合のタスク リスト

タスク	説明
XMPP クライアントの LDAP サーバの名前とアドレスの設定	LDAP サーバと IM and Presence Service の間で SSL を有効にし、セキュア接続を設定していた場合は、ルート CA 証明書を <code>xmpp-trust-certificate</code> として IM and Presence Service にアップロードします。 ヒント 証明書のサブジェクト CN は LDAP サーバの FQDN と一致する必要があります。
XMPP クライアントの LDAP 検索の設定	IM and Presence Service でサードパーティ製 XMPP クライアントの連絡先を検索できるように LDAP 検索設定を指定する必要があります。プライマリ LDAP サーバ 1 台とバックアップ LDAP サーバを最大 2 台指定できます。 ヒント オプションとして、LDAP サーバから vCard の取得をオンにすることや、vCard を IM and Presence Service のローカルデータベースに保存することができます。
Cisco XCP ディレクトリサービスのオン	サードパーティ製 XMPP クライアントのユーザが LDAP ディレクトリから連絡先を検索および追加できるようにするには、XCP ディレクトリ サービスをオンにする必要があります。 ヒント LDAP サーバの設定およびサードパーティ製 XMPP クライアントの LDAP 検索設定を行うまでは、Cisco XCP ディレクトリ サービスをオンにしないでください。そのようにしないと、サービスは実行を停止します。

LDAP アカウント ロックの問題

サードパーティ製 XMPP クライアントに対して設定する LDAP サーバのパスワードを間違えて入力し、IM and Presence Service で XCP サービスを再起動すると、JDS コンポーネントは、不正なパスワードで LDAP サーバに複数回サインインしようとします。数回失敗した後でアカウントをロックアウトするように LDAP サーバが設定されている場合、LDAP サーバはある時点で JDS コンポーネントをロックアウトする可能性があります。JDS コンポーネントが LDAP に接続する他のアプリケーション（IM and Presence Service で必要とは限らないアプリケーション）と同じ資格情報を使用している場合、これらのアプリケーションも LDAP からロックアウトされます。

この問題を解決するには、既存の LDAP ユーザと同じロールと特権を持つ別のユーザを設定し、JDS だけがこの 2 番目のユーザとしてサインインできるようにします。LDAP サーバに間違ったパスワードを入力した場合は、JDS コンポーネントだけが LDAP サーバからロックアウトされます。

XMPP クライアントの LDAP サーバの名前とアドレスの設定

Secure Socket Layer (SSL) を有効にする場合は、LDAP サーバと IM and Presence Service の間にセキュア接続を設定し、cup-xmpp-trust 証明書としてルート認証局 (CA) 証明書を IM and Presence Service にアップロードします。証明書のサブジェクト共通名 (CN) は、LDAP サーバの完全修飾ドメイン名 (FQDN) に一致させる必要があります。

証明書チェーン (ルートノードから信頼できるノードへの複数の証明書) をインポートする場合は、リーフ ノードを除くチェーン内のすべての証明書をインポートします。たとえば、CA が LDAP サーバの証明書に署名した場合は、CA 証明書のみをインポートし、LDAP サーバの証明書はインポートしません。

IM and Presence Service と Cisco Unified Communications Manager 間の接続が IPv4 であっても、IPv6 を使用して LDAP サーバに接続できます。IPv6 がエンタープライズパラメータまたは IM and Presence Service ノードの ETH0 のいずれかで無効になった場合でも、そのノードで内部 DNS クエリを実行し、サードパーティ製 XMPP クライアントの外部 LDAP サーバのホスト名が解決可能な IPv6 アドレスであれば、外部 LDAP サーバに接続できます。



ヒント サードパーティ製クライアントの外部 LDAP サーバのホスト名は [LDAP サーバ - サードパーティ製 XMPP クライアント (LDAP Server - Third-Party XMPP Client)] ウィンドウで設定します。

始める前に

LDAP ディレクトリのホスト名または IP アドレスを取得します。

IPv6 を使用して LDAP サーバに接続する場合は、LDAP サーバを設定する前に、エンタープライズパラメータと展開内の各 IM and Presence Service ノードの Eth0 で IPv6 を有効にします。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] > [アプリケーション (Application)] > [サードパーティ製クライアント (Third-Party Clients)] > [サードパーティ製 LDAP サーバ (Third-Party LDAP Servers)] を選択します。

ステップ 2 [新規追加 (Add New)] をクリックします。

ステップ 3 LDAP サーバの ID を入力します。

ステップ 4 LDAPサーバのホスト名を入力します。

IPv6 接続の場合は、LDAP サーバの IPv6 アドレスを入力できます。

ステップ 5 TCP または SSL 接続をリッスンする LDAP サーバのポート番号を指定します。

デフォルトポートは 389 です。SSL を有効にする場合は、ポート 636 を指定します。

ステップ 6 LDAP サーバのユーザ名とパスワードを指定します。これらの値は、LDAP サーバで設定したクレデンシャルと一致する必要があります。

この情報については、LDAP ディレクトリのマニュアルまたは LDAP ディレクトリの設定を確認してください。

ステップ 7 SSL を使用して LDAP サーバと通信するには、[SSL の有効化 (Enable SSL)] をオンにします。

(注) SSL が有効になっている場合、入力できるホスト名の値は、LDAP サーバのホスト名または FQDN です。使用する値は、セキュリティ証明書の CN または SAN フィールドの値と一致している必要があります。

IP アドレスを使用する必要がある場合は、この値が証明書の CN または SAN フィールドにも使用されている必要があります。

ステップ 8 [保存 (Save)] をクリックします。

ステップ 9 クラスタ内のすべてのノードで Cisco XCP Router サービスを起動します (このサービスがまだ動作していない場合)。



ヒント

- SSL を有効にすると、IM and Presence Service が SSL 接続を確立した後で、SSL 接続の設定およびデータの暗号化と復号化のときにネゴシエーション手順が実行されるため、XMPP の連絡先検索が遅くなる可能性があります。その結果、ユーザが展開内で XMPP の連絡先検索を広範囲に実行する場合、これがシステム全体のパフォーマンスに影響を与えることがあります。
- LDAP サーバの証明書のアップロード後、LDAP サーバのホスト名とポート値で通信を確認するには、証明書インポート ツールを使用できます。[Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] > [システム (System)] > [セキュリティ (Security)] > [証明書インポート ツール (Certificate Import Tool)] を選択します。
- サードパーティ製 XMPP クライアント用の LDAP サーバの設定を更新した場合は、Cisco XCP ディレクトリ サービスを再起動します。[Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] > [ツール (Tools)] > [コントロール センターの機能サービス (Control Center - Feature Services)] を選択して、このサービスを再起動します。

次のタスク

XMPP クライアントの LDAP 検索の設定に進みます。

XMPP クライアントの LDAP 検索設定

IM and Presence サービスでサードパーティ製 XMPP クライアントの連絡先を検索できるようにする LDAP 検索設定を指定する必要があります。

サードパーティ製 XMPP クライアントは、検索のたびに LDAP サーバに接続します。プライマリ サーバへの接続に失敗すると、XMPP クライアントは最初のバックアップ LDAP サーバを試し、それが使用不可能な場合は、2 番目のバックアップサーバを試します（以下同様）。システムのフェールオーバー中に処理中の LDAP クエリがあると、その LDAP クエリは次に使用可能なサーバで完了します。

オプションで LDAP サーバからの vCard の取得をオンにできます。vCard の取得をオンにした場合：

- 社内 LDAP ディレクトリは vCards を保存します。
- XMPP クライアントが自身の vCard、または連絡先の vCard を検索すると、vCard は JDS サービスによって LDAP から取得されます。
- クライアントは、社内 LDAP ディレクトリを編集することを許可されていないため、自身の vCard を設定または変更できません。

LDAP サーバからの vCard の取得をオフにした場合

- IM and Presence サービスはローカル データベースに vCard を保存します。
- XMPP クライアントが自身の vCard、または連絡先の vCard を検索すると、vCard はローカルの IM and Presence サービス データベースから取得されます。

- クライアントは、自身の vCard を設定または変更できます。

次の表はXMPP クライアントの LDAP 検索の設定の一覧です。

表 7: XMPP クライアントの LDAP 検索設定

フィールド	設定
LDAPサーバタイプ (LDAP Server Type)	LDAP サーバタイプをこのリストから選択します。 <ul style="list-style-type: none"> • Microsoft Active Directory • [汎用ディレクトリ サーバ (Generic Directory Server)] : 他のサポートされている LDAP サーバタイプ (iPlanet、Sun ONE、または OpenLDAP) を使用する場合は、このメニュー項目を選択します。
User Object Class (ユーザ オブジェクト クラス)	LDAP サーバタイプに適切なユーザ オブジェクト クラスの値を入力します。この値は、LDAP サーバで設定されたユーザ オブジェクト クラスの値と一致する必要があります。 Microsoft Active Directory を使用する場合、デフォルト値は [ユーザ (user)] です。
Base Context (ベース コンテキスト)	LDAP サーバに適切なベース コンテキストを入力します。この値は、LDAP サーバの設定済みドメインおよび/または組織構造と一致している必要があります。
User Attribute (ユーザー属性)	LDAP サーバタイプに適切なユーザー属性値を入力します。この値は、LDAP サーバで設定されたユーザー属性値と一致する必要があります。 Microsoft Active Directory を使用する場合、デフォルト値は [sAMAccountName] です。 ディレクトリ URI IM アドレス スキームが使用され、ディレクトリ URI がメールまたは msRTCSIPPrimaryUserAddress にマッピングされた場合、メールまたは msRTCSIPPrimaryUserAddress はユーザー属性として指定する必要があります。
LDAP Server 1 (LDAP サーバ 1)	プライマリ LDAP サーバを選択します。
LDAP Server 2 (LDAP サーバ 2)	(任意) バックアップ LDAP サーバを選択します。

フィールド	設定
LDAP Server 3 (LDAP サーバ 3)	(任意) バックアップ LDAP サーバを選択します。

始める前に

XMPP クライアントの LDAP サーバの名前とアドレスを指定します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] > [アプリケーション (Application)] > [サードパーティ クライアント (Third-Party Clients)] > [サードパーティ LDAP 設定 (Third-Party LDAP Settings)] を選択します。

ステップ 2 次の各フィールドに情報を入力します。

ステップ 3 ユーザが連絡先の vCard を要求し、LDAP サーバから vCard 情報を取得できるようにする場合は、[LDAP から vCard を作成 (Build vCards from LDAP)] をオンにします。ユーザが連絡先リストに参加するときにクライアントが自動的に vCard を要求できるようにする場合は、チェックボックスをオフのままにします。この場合、クライアントはローカル IM and Presence サービス データベースから vCard 情報を取得します。

ステップ 4 vCard FN フィールドを作成するために必要な LDAP フィールドを入力します。ユーザが連絡先の vCard を要求すると、クライアントは、vCard FN フィールドの値を使用して連絡先リストに連絡先の名前を表示します。

ステップ 5 検索可能な LDAP 属性テーブルで、適切な LDAP ユーザ フィールドにクライアント ユーザ フィールドをマッピングします。

Microsoft Active Directory を使用すると、IM and Presence サービスはテーブルにデフォルト属性値を読み込みます。

ステップ 6 [保存 (Save)] をクリックします。

ステップ 7 Cisco XCP Router サービスを起動します (このサービスがまだ動作していない場合)。

ヒント サードパーティ製 XMPP クライアント用の LDAP 検索の設定を更新した場合は、Cisco XCP ディレクトリ サービスを再起動します。[Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] > [ツール (Tools)] > [コントロール センターの機能サービス (Control Center - Feature Services)] を選択して、このサービスを再起動します。

次のタスク

Cisco XCP ディレクトリ サービスをオンに設定します。

Cisco XCP ディレクトリ サービスのオン

サードパーティ製 XMPP クライアントのユーザが LDAP ディレクトリから連絡先を検索および追加できるようにするには、Cisco XCP ディレクトリ サービスをオンにする必要があります。クラスタ内のすべてのノードで Cisco XCP ディレクトリ サービスをオンにします。



- (注) LDAP サーバおよびサードパーティ製 XMPP クライアントの LDAP 検索設定を設定するまでは、Cisco XCP ディレクトリ サービスをオンにしないでください。Cisco XCP ディレクトリ サービスをオンにするが、LDAP サーバおよびサードパーティ製 XMPP クライアントの LDAP 検索を設定しない場合、サービスは開始してから再度停止します。

始める前に

LDAP サーバおよびサードパーティ製 XMPP クライアントの LDAP 検索を設定します。

手順

- ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] > [ツール (Tools)] > [サービスの開始 (Service Activation)] を選択します。
- ステップ 2 [サーバ (Server)] メニューから [IM and Presence サービス (IM and Presence Service)] ノードを選択します。
- ステップ 3 [Cisco XCP ディレクトリ サービス (Cisco XCP Directory Service)] を選択します。
- ステップ 4 [保存 (Save)] をクリックします。



第 8 章

IM and Presence サービス用に Cisco Unified Communications Manager を設定します

- 統合の概要 (105 ページ)
- Cisco Unified Communications Manager 統合の前提条件 (105 ページ)
- Cisco Unified Communications Manager の SIP トランク設定 (107 ページ)

統合の概要

このセクションでは、IM and Presence サービスの設定を完了するために、Cisco Unified Communications Manager で完了すべきタスクを詳細に説明します。

Cisco Unified Communications Manager 統合の前提条件

IM and Presence Service を設定して Cisco Unified Communications Manager に統合する前に、以下の一般的な設定タスクを Cisco Unified Communications Manager で完了するようにしてください。Cisco Unified Communications Manager の設定手順の詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html> の *System Configuration Guide for Cisco Unified Communications Manager* を参照してください。

次の表に、IM and Presence Service の統合に不可欠な設定作業を示します。フィールドおよびそのオプションの説明については、オンライン ヘルプを参照してください。

表 8: Cisco Unified Communications Manager で必要な設定

タスク	説明
ユーザ クレデンシヤル ポリシーを修正する	<p>ユーザのクレデンシヤル ポリシーの有効期限を設定することを推奨します。クレデンシヤル ポリシーの有効期限を必要としない唯一のユーザ タイプは、アプリケーション ユーザです。</p> <p>Cisco Unified Communications Manager は、Cisco Unified Communications Manager のユーザを認証するために LDAP サーバを使用している場合はクレデンシヤル ポリシーを使用しません。</p> <p>Cisco Unified CM Administration > の [ユーザ管理] > [ユーザ設定] > [クレデンシヤル ポリシーのデフォルト]</p>
電話機を設定し、各電話機にディレクトリ番号 (DN) を関連付ける	<p>[CTI からデバイスを制御可能 (Allow Control of Device from CTI)] を有効にして、電話がクライアントと相互運用できるようにします。</p> <p>[Cisco Unified CM の管理 (Cisco Unified CM Administration)] > [デバイス (Device)] > [電話 (Phone)]</p>
ユーザを設定し、各ユーザにデバイスを関連付ける	<p>ユーザー ID 値が各ユーザで一意になっていることを確認します。</p> <p>[Cisco Unified CM の管理 (Cisco Unified CM Administration)] > [ユーザ管理 (User Management)] > [エンド ユーザ (End User)]</p>
ユーザをライン アピアランスに関連付ける	<p>詳細については、次の項を参照してください。</p> <p>[Cisco Unified CM の管理 (Cisco Unified CM Administration)] > [デバイス (Device)] > [電話 (Phone)]</p>
CTI 対応ユーザ グループにユーザを追加する	<p>デスクフォン制御を有効にするには、CTI 対応ユーザ グループにユーザを追加する必要があります。</p> <p>[Cisco Unified CM の管理 (Cisco Unified CM Administration)] > [ユーザ管理 (User Management)] > [ユーザ グループ (User Group)]</p>
証明書交換	<p>Cisco Unified Communications Manager と IM and Presence サービスの間の証明書交換は、インストールプロセス中に自動的に処理されます。ただし、問題があり、証明書交換を手動で完了する必要がある場合は、Cisco Unified Communications Manager との証明書の交換 (156 ページ) を参照してください。</p>



- (注) IM and Presence サービスにアップロードする Cisco Unified Communications Manager Tomcat 証明書の SAN フィールドにホスト名が含まれている場合、それらのすべてが IM and Presence サービスから解決可能である必要があります。IM and Presence サービスは、DNS 経由でホスト名を解決できる必要があります。そうでないと、Cisco Sync Agent サービスが開始されません。これは、Cisco Unified Communications Manager サーバのノード名にホスト名、IP アドレス、または FQDN を使用するかどうかにかかわらず当てはまります。

Cisco Unified Communications Manager の SIP トランク設定

Cisco Unified Communications Manager への SIP トランク接続を設定するには、これらのタスクを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	SIP トランク セキュリティ プロファイルの設定 (108 ページ)	Cisco Unified Communications Manager と IM and Presence サービスの間のトランク接続用の SIP トランクセキュリティプロファイルを設定します。
ステップ 2	IM and Presence サービスの SIP トランクの設定 (109 ページ)	SIP トランクセキュリティプロファイルを SIP トランクに割り当て、Cisco Unified Communications Manager と IM and Presence サービスの間のトランク接続を設定します。
ステップ 3	SRV クラスタ名の設定 (110 ページ)	これはオプションです。この手順は、Cisco Unified Communications Manager と IM and Presence サービスの間の SIP トランクで DNS SRV を使用していて、IM and Presence のデフォルトドメイン以外の SRV アドレスを使用している場合にのみ実行してください。この場合は、 SRV クラスタ名 サービスパラメータを設定します。それ以外の場合は、この作業をスキップできます。
ステップ 4	プレゼンス ゲートウェイの設定 (111 ページ)	IM and Presence サービスで、Cisco Unified Communications Manager をプレゼンスゲートウェイとして割り当てます。これにより、システムはプレゼンス情報を交換できます。

	コマンドまたはアクション	目的
ステップ 5	SIP パブリッシュ トランクの設定 (111 ページ)	これはオプションです。IM and Presence 用に SIP PUBLISH トランクを設定するには、この手順を使用します。この設定をオンにすると、Cisco Unified Communications Manager は、Cisco Unified Communications Manager で IM and Presence Service のライセンスが供与されたユーザに関連付けられたすべてのライン アピアランスの電話の利用状況をパブリッシュします。
ステップ 6	Cisco Unified Communications Manager で サービスを確認する (112 ページ)	必要なサービスが Cisco Unified Communications Manager で実行されていることを確認します。
ステップ 7	クラスタ外の Cisco Unified Communications Manager の電話でのプレゼンス表示の設定 (112 ページ)	Cisco Unified Communications Manager を IM and Presence Service の TLS ピアサブジェクトとして設定します。IM and Presence Service クラスタ外にある Cisco Unified Communications Manager からの電話利用状況を許可する場合、TLS が必要です。

SIP トランク セキュリティ プロファイルの設定

Cisco Unified Communications Manager で、IM and Presence サービスとのトランク接続用に SIP トランクセキュリティプロファイルを設定します。

手順

ステップ 1 Cisco Unified CM Administration > システム > セキュリティ > SIP トランク セキュリティ プロファイルで、検索をクリックします。

ステップ 2 [Non Secure SIP Trunk Profile] をクリックします。

ステップ 3 [コピー (Copy)] をクリックします。

ステップ 4 プロファイル名を入力します。例えば、IMP-SIP-Trunk-Profile。

ステップ 5 次の手順を完了します。

- デバイス セキュリティ モードは **非セキュア** に設定されています。
- **Incoming Transport Type** は **TCP+UDP** に設定されています。
- **Outgoing Transport Type** は **TCP** に設定されています。

ステップ 6 次のチェックボックスをオンにします。

- [プレゼンスのSUBSCRIBEの許可 (Accept Presence Subscription)]
- [Out-of-Dialog REFERの許可 (Accept Out-of-Dialog REFER)]
- [Unsolicited NOTIFYの許可 (Accept unsolicited notification)]
- [Replacesヘッダーの許可 (Accept replaces header)]

ステップ7 [保存 (Save)]をクリックします。

次のタスク

[IM and Presence サービスの SIP トランクの設定 \(109 ページ\)](#)

IM and Presence サービスの SIP トランクの設定

Cisco Unified Communications Manager と IM and Presence サービス クラスタの間の SIP トランク接続を設定します。

始める前に

[SIP トランク セキュリティ プロファイルの設定 \(108 ページ\)](#)

手順

-
- ステップ1 [Cisco Unified CM の管理 (Cisco Unified CM Administration) から、[デバイス (Device)] > [トランク (Trunk)] を選択します。
 - ステップ2 [新規追加 (Add New)] をクリックします。
 - ステップ3 [トランク タイプ (Trunk Type)] ドロップダウン リスト ボックスから、[SIP トランク (SIP Trunk)] を選択します。
 - ステップ4 [Device Protocol] ドロップダウン リストから [SIP] を選択します。
 - ステップ5 [トランク サービス タイプ (Trunk Service Type)] ドロップダウン リスト ボックスから、[なし (None)] を選択します。
 - ステップ6 [次へ (Next)] をクリックします。
 - ステップ7 [デバイス名 (Device Name)] フィールドに、トランクの名前を入力します。例えば、IMP-SIP トランク。
 - ステップ8 ドロップダウン リスト ボックスから [デバイス プール (Device Pool)] を選択します。
 - ステップ9 の中に SIP 情報 セクションで、IM and Presence クラスタのアドレス情報を入力して、IM and Presence サービスにトランクを割り当てます。
 - IM and Presence サービスに DNS SRV レコードを使用している場合は、宛先アドレスは **SRV** ですチェックボックスにチェックして、SRV を宛先アドレスフィールドに入力します。

- あるいは、宛先アドレスフィールドに、IM and Presence ノードの IP アドレスまたは FQDN を入力します。(+) ボタンをクリックして追加ノードを追加します。16 ノードまで入力できます。

- ステップ 10 [宛先ポート (Destination Port)] に、[5060] を入力します。
- ステップ 11 [SIP トランク セキュリティ プロファイル (SIP Trunk Security Profile)] ドロップダウン リスト ボックスから、前のタスクで作成した SIP トランク セキュリティ プロファイルを選択します。
- ステップ 12 [SIP プロファイル (SIP Profile)] ドロップダウン リストから、たとえば[標準 SIP プロファイル (Standard SIP Profile)] などのプロファイルを選択します。
- ステップ 13 [保存 (Save)] をクリックします。

次のタスク

Cisco Unified Communications Manager と IM and Presence サービスの間の SIP トランクで DNS SRV を使用していて、IM and Presence のデフォルトドメイン以外のアドレスを使用している場合、[SRV クラスタ名の設定 \(110 ページ\)](#)。

それ以外の場合は、[SIP パブリッシュ トランクの設定 \(111 ページ\)](#) に進みます。

SRV クラスタ名の設定

Cisco Unified Communications Manager と IM and Presence サービスの間の SIP トランクで DNS SRV を使用していて、IM and Presence のデフォルトドメイン以外のアドレスを使用している場合、[SRV クラスタ名サービスパラメータを設定します](#)。それ以外の場合は、この作業をスキップできます。

手順

- ステップ 1 Cisco Unified CM IM and Presence Serviceability から、[システム (System)] > [サービスパラメータ (Service Parameters)] を選択します。
- ステップ 2 [サーバ (Server)] ドロップダウンメニューから、IM and Presence パブリッシャー ノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3 [サービス (Service)] ドロップダウンから、[Cisco SIP プロキシ (Cisco SIP Proxy)] サービスを選択します。
- ステップ 4 SRV クラスタ名フィールドに、SRV アドレスを入力します。
- ステップ 5 [保存 (Save)] をクリックします。

SIP パブリッシュ トランクの設定

IM and Presence 用に SIP PUBLISH トランクを設定するには、このオプションの手順を使用します。この設定をオンにすると、Cisco Unified Communications Manager は、Cisco Unified Communications Manager で IM and Presence Service のライセンスが供与されたユーザーに関連付けられたすべてのライン アピアランスの電話の利用状況をパブリッシュします。

手順

- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で [プレゼンス (Presence)] > [設定 (Settings)] > [標準設定 (Standard Configuration)] を選択します。
- ステップ 2 **CUCM IM および Presence Publish Trunk** ドロップダウンから、その IM and Presence サービス用に Cisco Unified Communications Manager に設定した SIP トランクを選択します。
- ステップ 3 [保存 (Save)] をクリックします。

(注) この新しい設定を保存すると、Cisco Unified Communications Manager の **IM and Presence** パブリッシュ トランク サービス パラメータもこの新しい設定で更新されます。

次のタスク

[Cisco Unified Communications Manager でサービスを確認する \(112 ページ\)](#)

プレゼンス ゲートウェイの設定

この手順を IM and Presence Service で使用して Cisco Unified Communications Manager をプレゼンス ゲートウェイとして割り当てます。この設定は、Cisco Unified Communications Manager と IM and Presence サービスのプレゼンス情報交換を可能にします。

手順

- ステップ 1 **Cisco Unified CM IM and Presence Administration** > [プレゼンス (Presence)] > [ゲートウェイ (Gateways)] から。
- ステップ 2 [新規追加 (Add New)] をクリックします。
- ステップ 3 [(プレゼンス ゲートウェイ) **Presence Gateway**] ドロップダウンリストボックスから、**CUCM** を選択します。
- ステップ 4 [説明 (Description)] を入力します。
- ステップ 5 [プレゼンス ゲートウェイ (Presence Gateway)] フィールドから、次のオプションのいずれかを選択します。

- Cisco Unified Communications Manager パブリッシャー ノードの IP アドレスまたは FQDN

- Cisco Unified Communications Manager サブスクリバノードに解決される DNS SRV

ステップ 6 [保存 (Save)] をクリックします。

次のタスク

[SIP パブリッシュ トランクの設定 \(111 ページ\)](#)

Cisco Unified Communications Manager でサービスを確認する

この手順を使用して必要なサービスが Cisco Unified Communications Manager ノードで実行されていることを確認します。

手順

-
- ステップ 1 Cisco Unified Serviceability から、[ツール (Tools)] > [コントロール センター - 機能サービス (Control Center - Feature Services)] の順に選択します。
- ステップ 2 [サーバ (Server)] メニューから、[Cisco Unified Communications Manager] クラスタ ノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3 次のサービスが実行されていることを確認します。実行されていない場合、開始します。
- Cisco CallManager
 - Cisco TFTP
 - Cisco CTIManager
 - Cisco AXL Web Service (IM and Presence と Cisco Unified Communications Manager 間のデータ同期用)
- ステップ 4 上記のサービスのいずれかが実行されていない場合は、サービスを選択して[開始 (Start)] をクリックします。
-

クラスタ外の Cisco Unified Communications Manager の電話でのプレゼンス表示の設定

IM and Presence Service クラスタ外にある Cisco Unified Communications Manager から電話利用状況を許可できます。しかし、IM and Presence Service がクラスタ外の Cisco Unified Communications Manager から SIP PUBLISH を受け入れるようにするには、Cisco Unified Communications Manager が、IM and Presence の TLS 信頼ピアとしてリストされる必要があります

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified Communications Manager を TLS ピアとして追加 (113 ページ)	Cisco Unified Communications Manager を IM and Presence Service の TLS ピアとして追加します。
ステップ 2	Unified Communications Manager の TLS Context を設定します (113 ページ)	Cisco Unified Communications Manager TLS ピアの追加

Cisco Unified Communications Manager を TLS ピアとして追加

IM and Presence Service がクラスタ外の Cisco Unified Communications Manager から SIP PUBLISH を受け入れるようにするには、Cisco Unified Communications Manager が、IM and Presence Service の TLS 信頼ピアとしてリストされる必要があります。

手順

-
- ステップ 1 [\[Cisco Unified CM IM and Presence Administration\]](#) > [\[システム \(System\)\]](#) > [\[セキュリティ \(Security\)\]](#) > [\[TLS ピア サブジェクト \(TLS Peer Subjects\)\]](#) で、[\[Add New \(新規追加\)\]](#) を選択します。
- ステップ 2 [\[ピア サブジェクト名 \(Peer Subject Name\)\]](#) フィールドに外部 Cisco Unified Communications Manager の IP アドレスを入力します。
- ステップ 3 [\[説明 \(Description\)\]](#) フィールドにノードの名前を入力します。
- ステップ 4 [\[保存 \(Save\)\]](#) をクリックします。
-

次のタスク

[TLS コンテキストの設定 \(178 ページ\)](#)

Unified Communications Manager の TLS Context を設定します

次の手順を使用して、前のタスクで設定した Cisco Unified Communications Manager の TLS ピアを、選択した TLS ピアに追加します。

始める前に

[Cisco Unified Communications Manager を TLS ピアとして追加 \(113 ページ\)](#)

手順

- ステップ 1** Cisco Unified CM IM and Presence Administration > [システム (System)] > [セキュリティ (Security)] > [TLS コンテキスト設定 (TLS Context Configuration)] で、[検索 (Find)] をクリックします。
- ステップ 2** [Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context] をクリックします。
- ステップ 3** 使用可能な TLS ピア サブジェクトのリストから、Cisco Unified Communications Manager に設定した TLS ピア サブジェクトを選択します。
- ステップ 4** この TLS ピア サブジェクトを [選択された TLS ピア サブジェクト (Selected TLS Peer Subjects)] に移動します。
- ステップ 5** [保存 (Save)] をクリックします。
- ステップ 6** すべてのクラスタノードで Cisco OAMAgent を再起動します。
- [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
 - [サーバ (Server)] ドロップリストボックスから、IM and Presence サーバを選択して、[移動 (Go)] をクリックします
 - [IM and Presence サービス (IM and Presence Services)] の下で、[Cisco OAMAgent] を選択し、[リスタート(Restart)] をクリックします
 - すべてのクラスタノードでサービスを再起動します。
- ステップ 7** OAM エージェントが再起動したら、Cisco Presence Engine を再起動します。
- [ツール (Tools)] > [コントロール センター - 機能サービス (Control Center - Feature Services)] の順に選択します。
 - [サーバ (Server)] ドロップリストメニューから、IM and Presence ノードを選択して、[移動 (Go)] をクリックします。
 - [IM and Presence サービス (IM and Presence Services)] で、[Cisco Presence Engine] を選択して、[再起動 (Restart)] をクリックします。
 - すべてのクラスタノードでサービスを再起動します。
-

次のタスク

[Cisco Unified Communications Manager でサービスを確認する \(112 ページ\)](#)



第 9 章

集中展開の設定

- [集中展開の概要 \(115 ページ\)](#)
- [集中展開の前提条件 \(119 ページ\)](#)
- [集中展開設定のタスクフロー \(121 ページ\)](#)
- [サブドメインの SSO 対応リモートテレフォニークラスタを使用した IM and Presence の中央集中クラスタのセットアップ \(135 ページ\)](#)
- [電話機のプレゼンスを中央集中型導入に統合する \(136 ページ\)](#)
- [集中展開の相互作用と制限事項 \(138 ページ\)](#)

集中展開の概要

IM and Presence の集中展開では、IM and Presence 展開とテレフォニー展開を別々のクラスタに展開できます。中央の IM and Presence クラスタは、企業の IM and Presence を処理し、リモートの Cisco Unified Communications Manager のテレフォニークラスタは、企業の音声コールおよびビデオ コールを処理します。

集中展開オプションでは、標準展開と比較して次の利点がもたらされます。

- 集中展開オプションでは、IM and Presence サービス クラスタに対して 1x1 の比率のテレフォニークラスタは必要ありません。IM and Presence 展開とテレフォニー展開をそれぞれ個別のニーズに合わせて拡張できます。
- IM and Presence サービスにフルメッシュ トポロジは必要ありません。
- テレフォニーから独立したバージョン：IM and Presence 集中クラスタは、Cisco Unified Communications Manager のテレフォニークラスタとは異なるバージョンを実行している可能性があります。
- 中央クラスタから IM and Presence のアップグレードと設定を管理できます。
- コストの低いオプション、特に多数の Cisco Unified Communications Manager クラスタを使用する大規模な展開の場合
- サードパーティとの簡単な XMPP フェデレーション

- Microsoft Outlook との予定表統合をサポート。統合を設定する方法の詳細は、**IM** およびプレゼンスサービス との *Microsoft Outlook* 予定表の統合ガイドを参照してください。

OVA の要件

中央集中型の導入の場合は、最小 OVA 15,000 ユーザと、25,000 ユーザ IM and Presence OVA を推奨します。15,000 ユーザ OVA は、25000 ユーザにまで拡張できます。25K OVA テンプレートと高可用性を有効にした 6 ノードクラスタでは、IM and Presence サービスの中央展開で最大 75,000 のクライアントをサポートしています。25K OVA で 75K ユーザをサポートするには、XCP ルータのデフォルト トレース レベルを [情報 (Info)] から [エラー (Error)] に変更する必要があります。中央クラスタのユニファイド コミュニケーション マネージャー パブリッシュ ノードでは、次の要件が適用されます。

- 25000 IM およびプレゼンス OVA (最大75000ユーザ) は、中央クラスタのユニファイド コミュニケーション マネージャー パブリッシュ ノードにインストールされた1万ユーザ OVA を使用して展開できます。
- 15000 IM およびプレゼンス OVA (最大45,000ユーザ) は、中央クラスタのユニファイド コミュニケーション マネージャー パブリッシュ ノードにインストールされた 7500 ユーザ OVA を使用して展開できます。



- (注) Multiple Device Messaging を有効にする場合は、各ユーザが複数の Jabber クライアントを持つ可能性があるため、ユーザ数ではなくクライアント数に応じた展開にします。たとえば、ユーザ数が 25,000 人で、各ユーザが 2 台の Jabber クライアントを保持している場合、導入環境には 5 万ユーザのキャパシティが必要となります。

集中展開のためのクラスタ間設定

2 つの中央集中型クラスタ間でクラスタ間設定がサポートされています。クラスタ間ピアリング設定は、25K (25K OVA) デバイスを持つ 1 つのクラスタと、15K (15K OVA) デバイスを持つもう 1 つのクラスタでテストされ、パフォーマンス上の問題は見られませんでした。

集中展開のセットアップと標準 (分散) 展開

次の表では、IM and Presence サービスの標準的な展開と比較した、IM and Presence の集中型クラスタ展開の設定の違いについて説明します。

設定段階	標準展開との違い
インストールフェーズ	<p>IM and Presence 中央展開のインストールプロセスは、標準展開と同じです。ただし、中央展開では、IM and Presence 中央クラスタはテレフォニークラスタとは別にインストールされ、別のハードウェアサーバ上に配置される場合があります。トポロジの計画方法によっては、IM and Presence の中央クラスタをテレフォニークラスタとは別の物理ハードウェアにインストールすることができます。</p> <p>IM and Presence の中央クラスタの場合は、引き続き Cisco Unified Communications Manager をインストールしてから、IM and Presence サービスを同じサーバにインストールする必要があります。ただし、IM and Presence の中央クラスタの Cisco Unified Communications Manager インスタンスは、主にデータベースおよびユーザプロビジョニング用であり、音声コールまたはビデオ通話を処理しません。</p>
設定フェーズ	<p>標準（分散）展開と比較して、IM and Presence サービスの集中展開を設定するには、次の追加設定が必要です。</p> <ul style="list-style-type: none"> • テレフォニー クラスタと IM and Presence サービスの中央クラスタの両方にユーザを同期させ、両方のデータベースに存在させる必要があります。 • テレフォニー クラスタでは、エンドユーザを IM and Presence で有効にするべきではありません。 • テレフォニー クラスタでは、サービス プロファイルに IM and Presence サービスが含まれていて、IM and Presence 中央クラスタを指している必要があります。 • IM and Presence 中央クラスタでは、IM and Presence サービスに対してユーザを有効にする必要があります。 • IM and Presence 中央クラスタのデータベース パブリッシャ ノードで、リモート Cisco Unified Communications Manager のテレフォニー クラスタ ピアを追加します。 <p>IM and Presence サービスの標準展開で使用される以下の設定は、集中展開では必要ありません。</p> <ul style="list-style-type: none"> • プレゼンス ゲートウェイは不要です。 • SIP パブリッシュ トランクは不要です。 • IM and Presence の中央クラスタではサービスプロファイルは必要ありません。サービスプロファイルは、中央クラスタが接続するテレフォニー クラスタで設定されます。

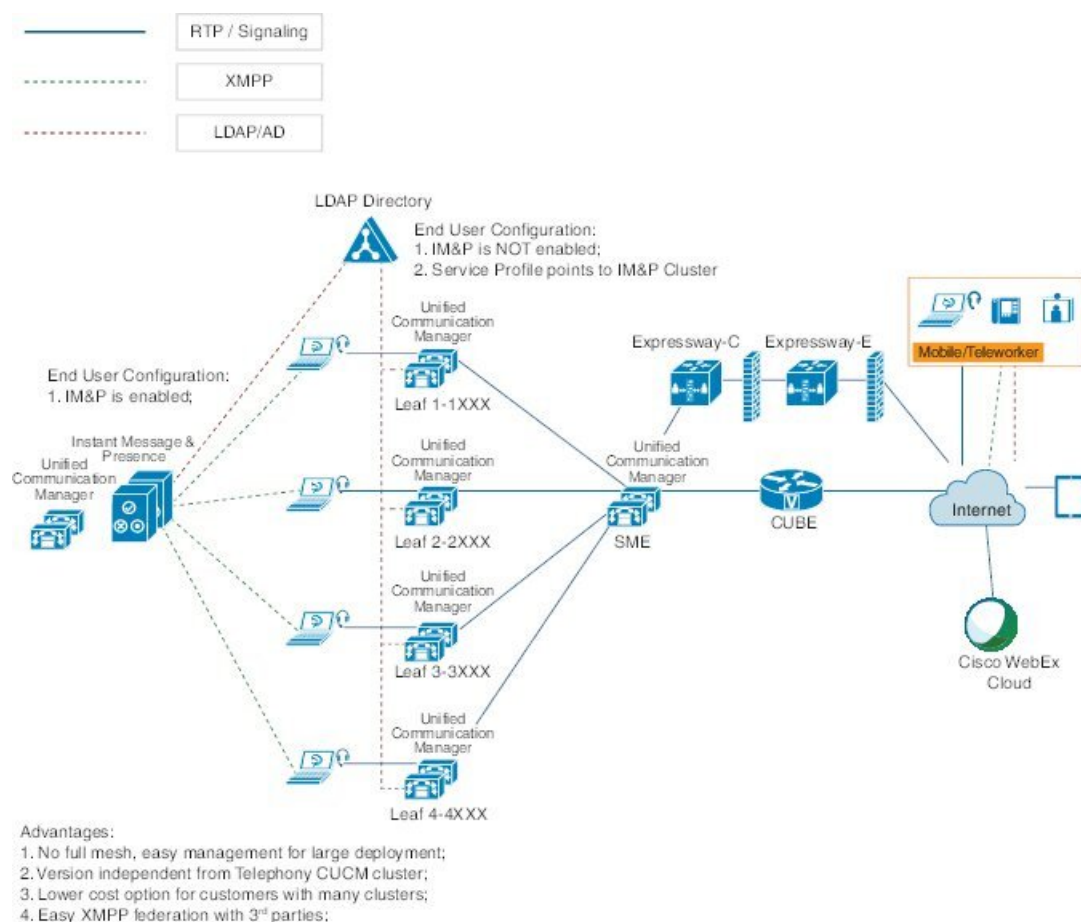
集中型クラスタの展開アーキテクチャ

次の図は、この展開オプションのクラスタ アーキテクチャを示しています。Cisco Jabber クライアントは、音声およびビデオ通話のために複数の Cisco Unified Communications Manager クラスタに接続します。この例では、Cisco Unified Communications Manager のテレフォニークラスタは、Session Management Edition 展開ではリーフクラスタです。高度なプレゼンスの場合、Cisco Jabber クライアントは IM and Presence サービスの中央クラスタに接続します。IM and Presence 中央クラスタは、Jabber クライアントのインスタントメッセージおよびプレゼンスを管理します。



(注) IM and Presence クラスタには、Cisco Unified Communications Manager のインスタンスが 이미だに含まれています。ただし、このインスタンスは、データベースやユーザプロビジョニングなどの共有機能を処理するためのもので、テレフォニーを処理するものではありません。

図 4: IM and Presence サービスの集中型クラスタ アーキテクチャ



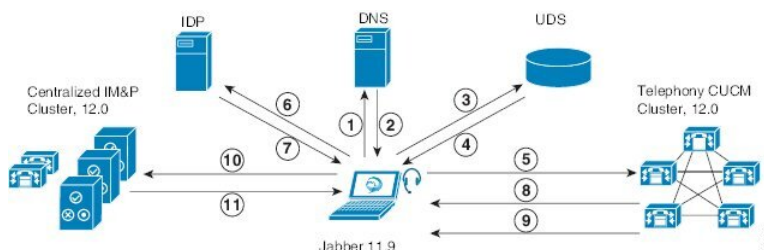
30135336

集中型クラスタの使用例

テレフォニーと IM and Presence クラスタを接続するために、アクセス キーを交換するための新しいシステムが導入されています。次の図は、SSO ログインのフローを示しています。

- [1]-[2] : DNS に問い合わせ、SRV レコードを取得します。
- [3]-[4] : UDS に問い合わせ、ホームの Cisco Unified Communications Manager クラスタを取得します。
- [5]-[8] : SAML SSO を通じて Cisco Unified Communications Manager クラスタからアクセス トークンと更新トークンを取得します。
- [9] : UC サービス プロファイルを読み取ります。サービス プロファイルは、IM and Presence プロファイルを含み、IM and Presence 中央クラスタを指します。
- [10] : クライアントは、SOAP および XMPP インターフェイスを介して同じアクセス トークンを使用して、IM and Presence クラスタに登録します。
- [11] : トークンが検証され、応答が Jabber クライアントに返されます。

図 5: IM and Presence サービスの集中型クラスタの使用例



集中展開の前提条件

IM and Presence サービスの集中展開には、次の要件が必要です。

- IM and Presence サービスの中央クラスタは、リリース 11.5 (1) SU4 以降を実行している必要があります。
- IM and Presence 中央クラスタと共に動作するローカル Cisco Unified Communications Manager インスタンスは、IM and Presence 中央クラスタと同じリリースを実行している必要があります。
- リモート Cisco Unified Communications Manager テレフォニークラスタは、リリース 10.5 (2)以降を実行している必要があります。
- Cisco Jabber はリリース 11.9 以降を実行している必要があります。
- プッシュ通知のインスタントメッセージングをサポートするには、IM and Presence サービスが少なくとも 11.5 (1) SU4 を実行している必要があります。

- iOS デバイス用のすべてのインスタントメッセージが Apple Push Notification Service (ANS) ソリューションを使用できるように、中央集中型 IM and Presence クラスタの CUCM サイトファリングノードで Cisco Cloud Onboarding を有効にする必要があります。

さらに、リーフ CUCM クラスタで Cisco Cloud Onboarding オプションを有効にする必要もあります。通常、これらのクラスタに登録されている TCT デバイスでは、iOS 用 Jabber が iOS によって一時停止または無効にされている場合に、APN を介してコールをルーティングすることができます。

IM and Presence Service クラスタで Cisco Cloud Onboarding を有効にする方法の詳細については、『[プッシュ通知導入ガイド](#)』の「*Cisco Cloud Onboarding* の有効化」の章を参照してください。

- Cisco Unified Communications Manager の機能は、IM and Presence 中央クラスタで実行されるローカルインスタンスではなく、リモートテレフォニークラスタで実行されている Cisco Unified Communications Manager のバージョンに基づいています。次に例を示します。
 - プッシュ通知コールをサポートするには、リモートテレフォニークラスタが少なくとも 11.5 (1) SU4 を実行している必要があります。
 - OAuth Refresh Logins サポートでは、リモート Cisco Unified Communications Manager テレフォニークラスタが少なくとも 11.5 (1) SU4 を実行している必要があります。
 - SAML SSO をサポートするには、リモートテレフォニークラスタが少なくとも 11.5 (1) SU4 を実行している必要があります。
- **Cisco AXL Web Service** 機能サービスが、すべてのクラスタで実行されている必要があります。このサービスはデフォルトで有効になっていますが、Cisco Unified Serviceability の [サービスのアクティベーション (Service Activation)] ウィンドウからアクティブになっていることを確認できます。
- 集中展開では、豊富なプレゼンスが Cisco Jabber によって処理されます。ユーザの電話のプレゼンスは、ユーザが Cisco Jabber にログインしている場合にのみ表示されます。

DNS の要件

IM and Presence 中央クラスタには、Cisco Unified Communications Manager テレフォニー クラスタのパブリッシャ ノードを指す DNS SRV レコードが必要です。テレフォニー展開に ILS ネットワークが含まれている場合、DNS SRV はハブ クラスタを指している必要があります。この DNS SRV レコードは「_cisco-uds」を参照しているはずですが。

SRV レコードは、特定のサービスをホストするコンピューターを識別するために使用されるドメインネームシステム (DNS) リソースレコードです。SRV リソースレコードは、Active Directory のドメインコントローラを検索するために使用されます。ドメインコントローラの SRV ロケータリソースレコードを確認するには、次の方法を使用します。

Active Directory は、次のフォルダに SRV レコードを作成します。ここで、Domain Name はインストールされたドメインの名前を示します。

- 前方参照ゾーン/ドメイン名/_msdcs / dc / _sites /デフォルトの最初のサイト名/_tcp

- 前方参照ゾーン/ドメイン名/_msdcs/dc/_tcp

これらの場所では、次のサービスの SRV レコードが表示されます。

- _kerberos
- _ldap
- _cisco_uds : SRV レコードを示します

下記のパラメータは、SRV レコードの作成中に設定する必要があります。

- サービス : _cisco_uds
- プロトコル : _tcp
- ウェイト : 0 から始まります (0 が最高の優先順位です)
- ポート番号 : 8443
- ホスト : サーバの fqdn 名

Jabber クライアントを実行しているコンピュータからの DNS SRV レコードの例は次のとおりです。

```
nslookup -type=all _cisco-uds._tcp.dcloud.example.com
Server: ad1.dcloud.example.com
Address: x.x.x.x
_cisco-uds._tcp.dcloud.example.com SRV service location:
priority = 10
weight = 10
port = 8443
svr hostname = cucm2.dcloud.example.com
cucm2.dcloud.example.com internet address = x.x.x.y
```

集中展開設定のタスクフロー

集中展開オプションを使用するために新規 IM and Presence サービス展開を構成する場合は、これらのタスクを完了します。



(注) このタスクフローは、新しい IM and Presence サービスの展開にのみ使用してください。

表 9: 集中型クラスタ設定のタスクフロー

	IM and Presence 中央クラス タ	リモートテレフォニー ク ラス タ	目的
ステッ プ 1	IM and Presence を Feature Group Template から有効化 (123 ページ)		IM and Presence 中央クラス タで、IM and Presence サー ビスを有効にするテンプ レートを構成します。
ステッ プ 2	IM and Presence 中央クラス タでの LDAP 同期の完了 (124 ページ)		LDAP 同期を完了して、IM and Presence 中央クラス タの LDAP 同期ユーザに設定 を伝播します。
ステッ プ 3	一括管理経由で IM and Presence を有効にする (125 ページ)		これはオプションです。 LDAP 同期がすでに完了し ている場合は、一括管理を 使用して、ユーザに対して IM and Presence を有効にし ます。
ステッ プ 4	リモートテレフォニー ク ラス タの追加 (126 ペ ージ)		リモートテレフォニー ク ラス タを IM and Presence 中 央クラスタに追加します。
ステッ プ 5		IM and Presence UC サービ スの設定 (127 ページ)	テレフォニークラスタで、 IM and Presence 中央クラス タを指す UC サービスを追加 します。
ステッ プ 6:		IM and Presence のサービス プロファイルの作成 (128 ページ)	サービス プロファイルに IM and Presence UC サービ スを追加します。Cisco Jabber クライアントはこの プロファイルを使用して、 IM and Presence 中央クラス タを検索します。
ステッ プ 7		テレフォニークラスタでの Presence ユーザーの無効化 (128 ページ)	テレフォニークラスタで、 IM and Presence 中央クラス タを指すようにプレゼン スユーザ設定を編集します。
ステッ プ 8:		OAuth 更新ログインを設定 する (130 ページ)	テレフォニークラスタで OAuth を設定すると、中央 クラスタの機能が有効にな ります。

	IM and Presence 中央クラスタ	リモート テレフォニー クラスタ	目的
ステップ 9		ILS ネットワークの設定 (130 ページ)	複数のテレフォニークラスタが存在する場合は、ILS を設定する必要があります。
ステップ 10		モバイルおよびリモートアクセスの設定	集中展開の場合のモバイルおよびリモートアクセスの設定。

次の作業

- クラスタ間ネットワークの一部として中央クラスタを他の IM and Presence クラスタに接続する場合は、クラスタ間ピアリングを設定します。
- IM and Presence 管理者コンソールで中央集中型導入に新しくエントリを作成する場合、Cisco XCP 認証サービスを再起動する必要があります。

IM and Presence を Feature Group Template から有効化

この手順を使用して、中央クラスタの IM and Presence 設定を使用して機能グループテンプレートを設定します。機能グループテンプレートを LDAP ディレクトリ設定に追加して、同期されたユーザに IM and Presence を設定できます。



- (注) 機能グループテンプレートは、初期同期がまだ行われていない LDAP ディレクトリ設定にのみ適用できます。中央クラスタから LDAP 設定を同期した後は、Cisco Unified Communications Manager で LDAP 設定を編集することはできません。ディレクトリをすでに同期している場合は、一括管理を使用して IM and Presence をユーザに設定する必要があります。詳細については、[一括管理経由で IM and Presence を有効にする \(125 ページ\)](#) を参照してください。

手順

- ステップ 1** IM and Presence 集中型クラスタの Cisco Unified CM の管理インターフェイスにログインします。このサーバにはテレフォニーが設定されてはいけません。
- ステップ 2** [ユーザ管理 (User Management)] > [ユーザ電話/追加 (User Phone/Add)] > [機能グループテンプレート (Feature Group Template)] を選択します。
- ステップ 3** 次のいずれかを実行します。
- [検索 (Find)] をクリックし、既存のテンプレートを選択します。
 - [新規追加 (Add New)] をクリックして新しいテンプレートを作成します。

ステップ 4 次の両方のチェックボックスをオンにします。

- [ホームクラスタ (Home Cluster)]
- [Unified CM IM and Presence のユーザを有効にする (Enable User for Unified CM IM and Presence)]

ステップ 5 [機能グループ テンプレートの設定 (Feature Group Template Configuration)] ウィンドウの残りのフィールドに入力します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 6 [保存 (Save)] をクリックします。

次のタスク

設定をユーザに伝達するには、最初の同期がまだ行われていない LDAP ディレクトリ構成に機能グループテンプレートを追加してから、最初の同期を完了する必要があります。

[IM and Presence 中央クラスタでの LDAP 同期の完了 \(124 ページ\)](#)

IM and Presence 中央クラスタでの LDAP 同期の完了

IM and Presence サービスの中央クラスタで LDAP 同期を完了し、機能グループ テンプレートを使用して IM and Presence サービスを持つユーザを設定します。



- (注) 初期同期が行われた後で LDAP 同期設定に編集を適用することはできません。初期同期がすでに行われている場合は、代わりに一括管理を使用してください。LDAP ディレクトリ同期を設定する方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure End Users」を参照してください。

始める前に

[IM and Presence を Feature Group Template から有効化 \(123 ページ\)](#)

手順

ステップ 1 IM and Presence 集中型クラスタの Cisco Unified CM の管理インターフェイスにログインします。このサーバにはテレフォニーが設定されてはいけません。

ステップ 2 [システム (System)] > [LDAP] > [LDAP ディレクトリ (LDAP Directory)] の順に選択します。

ステップ 3 次のいずれかを実行します。

- a) [検索 (Find)] をクリックし、既存の LDAP ディレクトリ同期を選択します。
- b) [新規追加 (Add New)] をクリックして、新しい LDAP ディレクトリを作成します。

- ステップ 4** [機能グループテンプレート (Feature Group Template)] ドロップダウンリストボックスから、前のタスクで作成した IM and Presence 対応の機能グループテンプレートを選択します。
- ステップ 5** [LDAPディレクトリ (LDAP Directory)] ウィンドウで残りのフィールドを設定します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。
- ステップ 6** [保存 (Save)] をクリックします。
- ステップ 7** [完全同期を実施 (Perform Full Sync)] をクリックします。

Cisco Unified Communications Manager が、データベースを外部の LDAP ディレクトリと同期します。エンドユーザが、IM and Presence サービスで構成されます。

次のタスク

[リモートテレフォニー クラスタの追加 \(126 ページ\)](#)

一括管理経由で IM and Presence を有効にする

ユーザをすでに中央クラスタに同期させていて、それらのユーザが IM and Presence サービスに対して有効になっていない場合は、一括管理の [ユーザの更新 (Update Users)] 機能を使用して IM and Presence サービスを有効にします。



- (注) 一括管理の [ユーザのインポート] または [ユーザの挿入] 機能を使用して、csv ファイルを介して新規ユーザーをインポートすることもできます。手順については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。インポートしたユーザで、下記のオプションが選択されていることを確認します。

- [ホームクラスタ (Home Cluster)]
- [Unified CM IM and Presence のユーザを有効にする (Enable User for Unified CM IM and Presence)]

手順

- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] から、[一括管理 (Bulk Administration)] > [ユーザ (Users)] > [ユーザの更新 (Update Users)] > [クエリ (Query)] の順に選択します。
- ステップ 2** フィルタから、ホームクラスタが有効になっているを選択し、検索をクリックします。ウィンドウに、これが自分のホームクラスタであるすべてのエンドユーザが表示されます。
- ステップ 3** [次へ (Next)] をクリックします。
の中に **ユーザ設定の更新** ウィンドウの左端のチェックボックスは、このクエリでこの設定を編集するかどうかを示します。左のチェックボックスをオンにしないと、クエリはそのフィールドを更新しません。右側のフィールドは、このフィールドの新しい設定を示しています。2つ

のチェックボックスが表示される場合は、左側のチェックボックスをオンにしてフィールドを更新し、右側のチェックボックスに新しい設定を入力する必要があります。

ステップ 4 サービス設定で、次の各フィールドの左側のチェックボックスをオンにしてこれらのフィールドを更新することを示し、次に隣接するフィールド設定を次のように編集します。

- **ホームクラスタ** - このクラスタをホームクラスタとして有効にするには、右側のチェックボックスをオンにします。
- **[Unified CM IM and Presence でのユーザの有効化 (Enable User for Unified CM IM and Presence)]** - 右チェックボックスをオンにします。この設定により、中央クラスタがこれらのユーザの IM and Presence サービスのプロバイダーとして有効になります。

ステップ 5 更新したい残りのフィールドをすべて入力します。フィールドとその設定を含むヘルプは、オンラインヘルプを参照してください。

ステップ 6 [ジョブ情報 (Job Information)] で、[今すぐ実行 (Run Immediately)] を選択します。

ステップ 7 [送信 (Submit)] をクリックします。

リモート テレフォニー クラスタの追加

この手順を使用して、リモート テレフォニー クラスタを集中型 IM and Presence サービス クラスタに追加します。



(注) 複数のテレフォニークラスターがある場合は、ILSを展開する必要があります。この場合、IM and Presence 中央クラスタが接続するテレフォニークラスタは、ハブクラスタでなければなりません。

手順

- ステップ 1** IM and Presence サービスの集中型クラスタでデータベース パブリッシャ ノードにログインします。
- ステップ 2** Cisco Unified CM IM and Presence Administration から、[システム (System)] > [集中展開 (Centralized Deployment)] を選択します。
- ステップ 3** [検索 (Find)] をクリックして、現在のリモート Cisco Unified Communications Manager クラスタのリストを表示します。クラスタの詳細を編集する場合は、クラスタを選択し、[Edit Selected] をクリックします。
- ステップ 4** [新規追加 (Add New)] をクリックして、新しいリモート Cisco Unified Communications Manager のテレフォニー クラスタを追加します。
- ステップ 5** 追加するテレフォニー クラスタごとに、次のフィールドに入力します。

- [ピアアドレス (Peer Address)] : リモート Cisco Unified Communications Manager のテレフォニー クラスタ上のパブリッシャ ノードの FQDN、ホスト名、IPv4 アドレス、または IPv6 アドレス。
- [AXL ユーザ名 (AXL Username)] : リモート クラスタ上の AXL アカウントのログイン ユーザ名。
- [AXL パスワード (AXL Password)] : リモート クラスタ上の AXL アカウントのパスワード。

ステップ 6 [保存して同期 (Save and Synchronize)] ボタンをクリックします。
IM and Presence サービスが、キーをリモート クラスタと同期させます。

次のタスク

[IM and Presence UC サービスの設定 \(127 ページ\)](#)

IM and Presence UC サービスの設定

リモート テレフォニー クラスタでこの手順を使用して、IM and Presence サービスの中央 クラスタを指す UC サービスを設定します。テレフォニー クラスタ内のユーザは、IM and Presence セントラルクラスタから IM and Presence サービスを受けます。

手順

- ステップ 1** テレフォニー クラスタで Cisco Unified CM の管理インターフェイスにログインします。
- ステップ 2** [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [UC サービス (UC Service)] を選択します。
- ステップ 3** 次のいずれかを実行します。
- a) [検索 (Find)] をクリックし、編集する既存のサービスを選択します。
 - b) [新規追加 (Add New)] をクリックして、新しい UC サービスを作成します。
- ステップ 4** [UC サービスタイプ (UC Service Type)] ドロップダウンリスト ボックスから、[IM and Presence] を選択し、[次へ (Next)] をクリックします。
- ステップ 5** [製品タイプ (Product type)] ドロップダウン リスト ボックスから、[IM and Presence サービス (IM and Presence Service)] を選択します。
- ステップ 6** クラスタの一意の [名前 (Name)] を入力します。これはホスト名である必要はありません。
- ステップ 7** [ホスト名/IP アドレス (HostName/IP Address)] に、IM and Presence 集中型クラスタ データベースのパブリッシャ ノードのホスト名、IPv4 アドレス、または IPv6 アドレスを入力します。
- ステップ 8** [保存 (Save)] をクリックします。
- ステップ 9** 推奨。この手順を繰り返して、2 番目の IM and Presence サービスを作成します。ホスト名/IP アドレス field は、中央クラスタ内の加入者ノードを指します。

次のタスク

[IM and Presence のサービス プロファイルの作成 \(128 ページ\)](#)。

IM and Presence のサービス プロファイルの作成

リモート テレフォニー クラスタでこの手順を使用して、IM and Presence 中央クラスタを指すサービスプロファイルを作成します。テレフォニークラスタ内のユーザは、このサービスプロファイルを使用して、中央クラスタから IM and Presence サービスを取得します。

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [サービスプロファイル (Service Profile)] を選択します。

ステップ 2 次のいずれかを実行します。

- a) [検索 (Find)] をクリックし、編集する既存のサービス プロファイルを選択します。
- b) [新規追加 (Add New)] をクリックして、新しいサービス プロファイルを作成します。

ステップ 3 の中に **IM とプレゼンスプロファイル** セクションで、前のタスクで設定した IM and Presence サービスを設定します。

- a) [プライマリ (Primary)] ドロップダウンリストからデータベースパブリッシャ ノードを選択します。
- b) **セカンダリ (Secondary)** ドロップダウンリストから、サブスクリバノードサービスを選択して下さい。

ステップ 4 [保存 (Save)] をクリックします。

次のタスク

[テレフォニー クラスタでの Presence ユーザーの無効化 \(128 ページ\)](#)

テレフォニー クラスタでの Presence ユーザーの無効化

テレフォニー展開でLDAP同期が既に完了している場合は、一括管理ツールを使用してIM and Presence ユーザ用のテレフォニークラスタのユーザ設定を編集します。この設定では、プレゼンスユーザが IM and Presence サービスの中央クラスタを参照するようになります。



(注) この手順は、テレフォニークラスターでLDAP同期が既に完了していることを前提としています。ただし、最初のLDAP同期がまだ完了していない場合は、Presence ユーザの Central Deployment 設定を最初の同期に追加できます。この場合は、テレフォニークラスターで次の手順を実行します。

- 設定したサービス プロファイルを含む機能グループ テンプレートを設定します。それが あることを確認してくださいホームクラスターオプションを選択して **Unified CM の IM and Presence** に対してユーザーを有効にするオプションが選択されていません。
- に LDAP ディレクトリ設定追加する機能グループテンプレート LDAP ディレクトリに同期します。
- 初期同期を完了してください。

機能グループテンプレートおよびLDAPディレクトリを設定する方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure End Users」を参照してください。

手順

- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] から、[クエリ (Query)] > [一括管理 (Bulk Administration)] > [ユーザ (Users)] > [ユーザの更新 (Update Users)] > [クエリ (Query)] の順に選択します。
- ステップ 2** フィルタから、**ホームクラスターが有効になっている**を選択し検索をクリックします。ウィンドウに、これが自分のホームクラスターであるすべてのエンドユーザが表示されます。
- ステップ 3** [次へ (Next)] をクリックします。
の中に**ユーザ設定の更新**ウィンドウの左端のチェックボックスは、このクエリでこの設定を編集するかどうかを示します。左のチェックボックスをオンにしないと、クエリはそのフィールドを更新しません。右側のフィールドは、このフィールドの新しい設定を示しています。2つのチェックボックスが表示される場合は、左側のチェックボックスをオンにしてフィールドを更新し、右側のチェックボックスに新しい設定を入力する必要があります。
- ステップ 4** サービス設定で、次の各フィールドの左端のチェックボックスをオンにしてこれらのフィールドを更新するように指定してから、隣接する設定を次のように編集します。
 - **ホームクラスター** - テレフォニークラスターをホームクラスターとして有効にするには、右側のチェックボックスをオンにします。
 - **[Unified IM and Presenceでのユーザの有効化 (Enable User for Unified IM and Presence)]** - 右チェックボックスをオフにします。この設定は、テレフォニークラスターを IM and Presence のプロバイダーとして無効にします。
 - **UC サービス概要** - ドロップダウンから、前のタスクで設定したサービスプロファイルを選択します。この設定では、IM and Presence セントラルクラスターが IM and Presence サービスのプロバイダーになります。

(注) Expressway モバイルおよびリモートアクセスの構成の詳細については、<https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>で『*Mobile and Remote Access via Cisco Expressway Deployment Guide*』を参照してください。

ステップ5 必要な残りのフィールドをすべて入力してください。フィールドとその設定を含むヘルプは、オンラインヘルプを参照してください。

ステップ6 [ジョブ情報 (Job Information)] で、[今すぐ実行 (Run Immediately)] を選択します。

ステップ7 [送信 (Submit)] をクリックします。

次のタスク

[OAuth 更新ログインを設定する \(130 ページ\)](#)

OAuth 更新ログインを設定する

テレフォニークラスターでOAuth 更新ログインを有効にします。これにより、中央クラスタの機能も有効になります。

手順

ステップ1 テレフォニー クラスタで Cisco Unified CM の管理にログインします。

ステップ2 [システム (System)] > [エンタープライズ パラメータ (Enterprise Parameters)] と選択します。

ステップ3 [SSO設定 (SSO Configuration)] で、[更新ログインフローによるOAuth (OAuth with Refresh Login Flow)] エンタープライズ パラメータを [有効 (Enabled)] に設定します。

ステップ4 パラメータ設定を編集した場合は、**保存する** をクリックします。

ILS ネットワークの設定

リモートテレフォニー クラスタが複数存在する IM and Presence 集中型クラスタでは、クラスタ間検索サービス (ILS) を使用して、IM and Presence 中央クラスタのリモートテレフォニー クラスタをプロビジョニングできます。ILS はネットワークを監視し、新しいクラスタやアドレス変更などのネットワーク変更をネットワーク全体に伝播します。



(注) このタスクの流れは、IM and Presence 集中型クラスタの展開に関する ILS 要件に重点を置いています。グローバルダイヤルプランレプリケーションやURIダイヤルの設定など、テレフォニーに関する ILS の追加設定については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure the Dial Plan」を参照してください。

始める前に

ILS を導入する場合は、次のことを確認してください。

- ILS ネットワーク トポロジを計画します。どのテレフォニー クラスタがハブとスポークになるのかを把握する必要があります。
- IM and Presence 中央クラスタが接続するテレフォニー クラスタは、ハブ クラスタでなければなりません。
- ハブ クラスタのパブリッシャ ノードを指す DNS SRV レコードを設定する必要があります。

ILS ネットワークの設計については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html> で『Cisco Collaboration System Solution Reference Network Design』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	ILS へのクラスタ ID の設定 (131 ページ)	テレフォニー クラスタごとに固有のクラスタ ID を設定します。クラスタ ID が StandAloneCluster (デフォルト設定) に設定されている間、ILS は機能しません。
ステップ 2	テレフォニー クラスタでの ILS の有効化 (132 ページ)	ILS ネットワーク内の各テレフォニー クラスタのパブリッシャ ノードで ILS を設定およびアクティブ化します。
ステップ 3	ILS ネットワークが動作していることを確認する (133 ページ)	ILS が動作しているときは、すべてのリモートクラスタを「最新」の同期ステータスを持つテレフォニー クラスタの ILS 設定 ウィンドウから確認できます。

ILS へのクラスタ ID の設定

ILS ネットワーク内の各クラスタには、一意のクラスタ ID が必要です。この手順を使用して、テレフォニー クラスタに一意のクラスタ ID を割り当てます。

手順

ステップ 1 パブリッシャ ノードで Cisco Unified CM 管理にログインします。

ステップ 2 [システム (System)] > [エンタープライズ パラメータ (Enterprise Parameters)] と選択します。

ステップ 3 [クラスタID (Cluster ID)] パラメータの値を StandAloneCluster から設定した一意の値に変更します。クラスタ ID が StandAloneCluster の間は、ILS は機能しません。

ステップ 4 [保存 (Save)] をクリックします。

ステップ 5 ILS ネットワークに参加させる各テレフォニー クラスタのパブリッシャ ノードでこの手順を繰り返します。各クラスタには一意の ID が必要です。

次のタスク

[テレフォニー クラスタでの ILS の有効化 \(132 ページ\)](#)

テレフォニー クラスタでの ILS の有効化

この手順を使用して、Cisco Unified Communications Manager のテレフォニー クラスタで ILS を設定およびアクティブ化します。



- (注)
- スポーク クラスタを設定する前に、ハブ クラスタを設定します。
 - フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

始める前に

[ILS へのクラスタ ID の設定 \(131 ページ\)](#)

手順

ステップ 1 テレフォニー クラスタのパブリッシャ ノードで Cisco Unified CM の管理にログインします。

ステップ 2 [拡張機能 (Advanced Features)] > [ILS設定 (ILS Configuration)] を選択します。

ステップ 3 [役割 (Role)] ドロップダウン リスト ボックスから、設定するクラスタのタイプに応じて、[ハブクラスタ (Hub Cluster)] または [スポーククラスタ (Spoke Cluster)] を選択します。

ステップ 4 [リモートクラスタとのグローバルダイヤルプランのレプリケーションデータの交換 (Exchange Global Dial Plan Replication Data with Remote Clusters)] チェックボックスをオンにします。

ステップ 5 [ILS認証の詳細 (ILS Authentication Details)] を設定します。

- a) さまざまなクラスタ間で TLS 認証を使用する場合は、[TLS証明書の使用 (Use TLS Certificates)] チェックボックスをオンにします。

(注) TLS を使用する場合は、クラスタ内のノード間で CA 署名付き証明書を交換する必要があります。

- b) パスワード認証を使用する場合 (TLS を使用するかどうかに関係なく) は、[パスワードの使用 (Use Password)] チェックボックスをオンにして、パスワードの詳細を入力します。

ステップ 6 [保存 (Save)] をクリックします。

ステップ7 [ILSクラスタ登録 (ILS Cluster Registration)] ポップアップで、登録の詳細を設定します。

- [登録サーバ (Registration Server)] テキストボックスに、このクラスタに接続するハブクラスタのパブリッシャ ノードの IP アドレスまたは FQDN を入力します。これがネットワーク内の最初のハブクラスタである場合は、このフィールドを空白のままにしておくことができます。
- [このクラスタにあるパブリッシャでクラスタ間検索サービスをアクティブ化 (Activate the Intercluster Lookup Service on the publisher in this cluster)] チェックボックスがオンになっていることを確認します。

ステップ8 [OK] をクリックします。

ステップ9 ILS ネットワークに追加する各テレフォニー クラスタのパブリッシャ ノードでこの手順を繰り返します。
設定した同期値によっては、クラスタ情報がネットワーク全体に伝播する間に遅延が生じることがあります。

クラスタ間で Transport Layer Security (TLS) 認証を使用するには、ILS ネットワークの各クラスタのパブリッシャ ノード間で、Tomcat 証明書を交換する必要があります。Cisco Unified オペレーティング システムの管理から、証明書の一括管理機能を使用して、以下を行います。

- 証明書を各クラスタのパブリッシャ ノードから中央の場所にエクスポートします
- エクスポートされた証明書を ILS ネットワークに統合します
- ネットワークの各クラスタのパブリッシャ ノードに証明書をインポートします

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』の「Manage Certificates」の章を参照してください。

次のタスク

ILS が稼働し、証明書を交換した後 (必要に応じて)、[ILS ネットワークが動作していることを確認する \(133 ページ\)](#)

ILS ネットワークが動作していることを確認する

この手順を使用して、ILS ネットワークが稼働していることを確認します。

手順

ステップ1 任意のテレフォニー クラスタでパブリッシャ ノードにログインします。

ステップ2 Cisco Unified CM の管理から、[詳細機能 (Advanced Features)] > [ILS設定 (ILS Configuration)] を選択します。

ステップ 3 [ILS クラスタとグローバルダイヤルプランインポート済みカタログ (ILS Clusters and Global Dial Plan Imported Catalogs)] セクションをオンにします。ILS ネットワーク トポロジが表示されます。

モバイルおよびリモートアクセスの設定

Cisco Unified Communications の Mobile & Remote Access は Cisco Collaboration Edge アーキテクチャの中核を成します。Cisco Jabber などのエンドポイントがエンタープライズ ネットワーク外にある場合、それらのエンドポイントで、Cisco Unified Communications Manager によって提供される登録、呼制御、プロビジョニング、メッセージング、およびプレゼンスサービスを使用できます。Expressway は、Unified CM 登録にセキュアなファイアウォール トラバーサルと回線側サポートを提供します。

全体的なソリューションは以下を提供します。

1. **オフプレミスアクセス**：企業ネットワーク外においても、Jabber および EX/MX/SX シリーズクライアントで一貫したエクスペリエンスを提供。
2. **セキュリティ**：セキュアな Business-to-Business (B2B) コミュニケーション。
3. **クラウド サービス**：エンタープライズクラスの柔軟性と拡張性に優れたソリューションにより、Webex の統合とさまざまなサービス プロバイダーに対応。
4. **ゲートウェイと相互運用性サービス**：メディアおよびシグナリングの正規化、非標準エンドポイントのサポート。

設定

すべてのテレフォニー リーフ クラスタ上のモバイルおよびリモートアクセスを Expressway-C で設定するには、**設定** → **ユニファイドコミュニケーション** → **Unified CM サービス** を選択します。

Expressway-C で集中 IM&P クラスタのモバイルおよびリモートアクセスを設定するには、**[設定 (Configuration)]** → **[ユニファイド コミュニケーション (Unified Communications)]** → **[IM and Presence サービス ノード (IM and Presence Service nodes)]** を選択します。

Expressway-C で「モバイルとリモートアクセス」を有効にするには、**設定** → 「**モバイルとリモートアクセス**」を有効にするを選択し、下の表に従って、制御オプションを選択します。

表 10: OAuth 有効化設定

認証パス (Authentication path)	UCM / LADP 基本認証
OAuth トークンによる承認 (更新あり) (Authorize by OAuth token with refresh)	オン
OAuth トークンによる承認 (Authorize by OAuth token)	オン
ユーザ資格情報で承認	不可

Jabber iOS クライアントによる組み込みの Safari ブラウザの使用の許可	不可
内部認証の可用性の確認 (Check for internal authentication availability)	はい

表 11: OAuth 無効化設定

認証パス (Authentication path)	UCM / LADP 基本認証
OAuth トークンによる承認 (更新あり) (Authorize by OAuth token with refresh)	オフ
ユーザ資格情報で承認	オン
Jabber iOS クライアントによる組み込みの Safari ブラウザの使用の許可	オフ
内部認証の可用性の確認 (Check for internal authentication availability)	はい



(注) モバイルおよびリモートアクセスの基本設定については、次の章を参照してください。
<https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>

サブドメインの SSO 対応リモートテレフォニークラスタを使用した IM and Presence の中央集中クラスタのセットアップ

IM and Presence の中央集中型導入では、リモートテレフォニークラスタに複数のサブドメインがある場合、SSO が有効なリモートアクセスクライアント (Jabber など) に対して、小さい差し込みリソースのログインを有効にできます。

このセクションでは、SSO 対応のリモートテレフォニークラスタ内で、サブドメインユーザが Jabber にログインする手順について説明します。中央集中型クラスタと、その中央集中型クラスタに関連付けられた SSO 対応リモートテレフォニークラスタで構成される、中央集中型導入のシナリオを検討してください。

サブドメインの SSO 対応ログインを設定するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理にログインして、次の手順を実行します。

- a) LDAP からリーフノードにユーザを同期し、[ディレクトリ URI] フィールドを [メール ID] に設定して SSO を有効にします。LDAP ユーザを同期する方法については、[LDAP 同期の概要 \(83 ページ\)](#) を参照してください。
- b) 同じユーザをリモートテレフォニーノードに同期し、[ディレクトリ URI] フィールドを [メール ID] に設定します。
- c) [エンドユーザー設定] ページ ([エンドユーザー] > [エンドユーザー管理]) で、[Cisco Unified IM and Presence サービスのユーザを有効にする (関連する UC サービスプロファイルで IM and Presence を設定する)] オプションをオンにして、集中型クラスタと同じユーザを使用します。このオプションは、IM and Presence ノードの [サービス設定] にあります。
- d) [エンドユーザーの設定] ページ ([エンドユーザー] > [エンドユーザー管理]) で、[権限情報 (Permission Information)] セクションから Cisco CallManager (CCM) のエンドユーザーグループにユーザを追加します。
- e) リモートテレフォニークラスタ上の IM and Presence のユーザを無効にします。これを行うには、ServiceSettings の下の [Cisco Unified IM and Presence サービスのユーザを有効にする (関連する UC サービスプロファイルで IM and Presence を設定する)] オプションのチェックを外します。
- f) リモートテレフォニークラスタ用の中央クラスタに UC サービスを作成します ([ユーザー管理] > [ユーザ設定] > [UC Service の設定])。
- g) 中央クラスタ上にサービスプロファイルを作成し、これをシステムのデフォルトのサービスプロファイルとして設定し、IM and Presence ノードを IM and Presence プロファイル ([ユーザー管理] > [ユーザ設定] > [サービスプロファイル]) に追加します。
- h) 中央クラスタ上で更新ログインフローによる OAuth を有効にします。[エンタープライズパラメーターの構成] ページで、[更新ログインフローによる OAuth] パラメータを [有効] に設定します。

ステップ 2 Cisco Unified IM and Presence 管理コンソールにログインし、リーフノードを IM and Presence Service ノード ([システム] > [中央集中型導入]) に追加します。

電話機のプレゼンスを中央集中型導入に統合する

中央集中型の導入では、中央集中型 IM and Presence ノードに複数の SIP トランクを設定することで、リモート CUCM クラスタから電話機のプレゼンス情報を取得できます。

プレゼンスゲートウェイとして 1 つの CUCM クラスタのみを設定できる標準導入とは異なり、システムは中央集中型導入でこの制限を回避します。これにより、管理者は IM and Presence ノードにプレゼンスゲートウェイとして複数の CUCM クラスタを追加できます。これは、リモート CUCM クラスタから電話機のプレゼンス情報を取得するのに役立ちます。

次の手順では、リモートの Cisco Unified CM クラスタおよび対応する IM and Presence ノードで SIP トランクなどの追加設定を構成する手順を示します。

手順

ステップ 1 Cisco Unified CM の管理のユーザインターフェイスから、次の手順を実行します。

- a) [デバイス]>[トランク]を選択します。新しい SIP トランクを追加し、リーフクラスタとして IM and Presence ノードにポイントします。
- b) [システム]>[サービスパラメータの設定]を選択し、**CallManager** を選択します。[**IM and Presence の公開トランク**] フィールドに、前の手順で追加したリーフクラスタトランクの IP アドレスを入力します。
- c) クラスタ内で利用可能なすべてのユーザのプレゼンスを有効にします。バックエンドでの 1 回の試みで、**Unified CM IM and Presence のユーザの有効化**（関連付けられた UC サービスプロファイルの**IM and Presence の設定**）チェックボックスを、[**エンドユーザ設定**] ページのすべてのユーザに対して、1 回の試行で設定できます。

ステップ 2 Cisco Unified CM の IM and Presence の管理から、次の手順を実行します。

- a) **Cisco Unified CM IM and Presence の管理**のユーザインターフェイスで、[**プレゼンス**]>[**プレゼンスゲートウェイ**]を選択し、リモート CUCM クラスタの IP アドレスを入力します。
- b) リモートの Cisco Unified CM の IP アドレスを追加して、[**システム**]>[**セキュリティ**]>[**着信 ACL**]を選択し、新しい ACL を作成します。
- c) [**システム**]>[**セキュリティ**]>[**TLS ピアサブジェクト**]を選択し、リモートの Cisco Unified CM の IP アドレスを追加します。
- d) [**システム (System)**]>[**セキュリティ (Security)**]>[**TLS コンテキスト設定 (TLS Context Configuration)**]を選択します。[**TLS ピアサブジェクトのマッピング**]セクションで、前の手順のリモート Cisco Unified CM 用に作成された TLS ピアサブジェクトを [**利用可能な TLS ピアサブジェクト**]ボックスから選択し、[**選択した TLS ピアサブジェクト**]ボックスに移動します。

ステップ 3 すべてのクラスタノードで **Cisco OAMAgent** を再起動します。

ステップ 4 Cisco Presence Engine を再起動します。

- (注) IM and Presence サービスの中央集中型導入では、Cisco Jabber のステータスを [**応答不可 (DND)**]に変更できます。制御下の Cisco IP 電話および Jabber デバイスにも同じステータスが反映されます。ただし、中央集中型導入では、複数のデバイスが同じディレクトリ番号 (DN) で設定されている共有回線では、DND ステータスの変更は反映されません。

集中展開の相互作用と制限事項

機能	データのやり取り
ILS ハブクラスタ	ILS ハブクラスタが停止していて、複数のテレフォニークラスタが存在する場合、中央クラスタ機能は機能しません。
ILS の展開	IM and Presence 中央クラスタを展開していて、ILS も展開している場合は、テレフォニークラスタにだけ ILS を展開できます。ILS を IM and Presence 中央クラスタの Cisco Unified Communications Manager インスタンスには展開できません。このインスタンスはプロビジョニング専用であり、テレフォニーを処理しません。
高度なプレゼンス	集中展開では、豊富なプレゼンスが Cisco Jabber によって計算されます。ユーザのテレフォニープレゼンスは、ユーザが Jabber にログインしている場合にのみ表示されます。
Unified Communications Manager のクラスタ ID。	<p>集中型展開では、統合コミュニケーションマネージャークラスタステータスがOAuth 更新ログインの同期として表示されます。この機能は、11.5 (1) の SU3 以降で利用可能です。</p> <p>Unified Communications Manager を 11.5 (1) SU3 またはそれ以前のリリースに追加すると、OAuth 更新ログインがサポートされないため、Cisco Unified CM IM and Presence のシステム > 集中展開では、クラスタステータスが「未同期」として表示されます。これらのクラスタは、SSO または LDAP ディレクトリ クレデンシャルを使用した IM およびプレゼンスサービスの集中型展開に対応しています。</p> <p>(注) Cisco Jabber のユーザログインには機能上の影響はありません。</p>



第 10 章

高度なルーティングを設定する

- [高度なルーティングの概要 \(139 ページ\)](#)
- [高度なルーティングの前提条件 \(140 ページ\)](#)
- [高度なルーティング設定のタスク フロー \(140 ページ\)](#)

高度なルーティングの概要

高度なルーティングを設定して、システムが次の種類の接続を確立する方法を決定します。

- クラスタ内の IM and Presence サービスノード間のクラスタ間接続。
- 同じプレゼンスドメインを共有する IM and Presence サービスクラスタ間のクラスタ間接続。
- 異なるプレゼンスドメイン間のフェデレーション接続用の SIP スタティックルート。スタティックルートは固定パスであり、ダイナミックルートよりも優先されます。

クラスタ間およびクラスタ内接続

クラスタ間接続とクラスタ内接続を確立するには、2つのモードがあります。

- Multicast DNS (MDNS) - MDNS ルーティングは DNS レコードを使用してノード間の接続を設定します。クラスタ内のすべてのノードが同じマルチキャストドメインにある場合は、MDNS ルーティングを使用できます。
- ルータ間 (デフォルトオプション) - ルータ間は、IP アドレスとユーザ情報を使用して、ノード間の接続を動的に設定します。クラスタ内のノードが同じマルチキャストドメインにない場合、またはそれらが異なるサブネットにある場合は、ルーター間接続を使用します。



(注) XCP ルート ファブリックに参加する新しい XCP ルータをシームレスにサポートできるため、MDNS ルーティングを推奨します。

高度なルーティングの前提条件

ルーティングを設定する前に、システムがこれらの要件を満たしていることを確認してください。要件は、使用するルーティング方法の種類（MDNS ルーティングまたはルータ間）によって異なります。

MDNS ルーティングの前提条件

以下の前提条件があります。

- IOS ネットワークでマルチキャスト DNS を設定しておく必要があります。ネットワークでマルチキャスト DNS を無効にすると、MDNS パケットはクラスタ内の他のノードに到達できません。一部のネットワークでは、マルチキャストはデフォルトで有効であるか、特定のネットワーク領域で有効です。たとえば、クラスタからのノードを含む領域で有効にできます。このようなネットワークでは、MDNS ルーティングを使用するために、ネットワークで追加設定を行う必要はありません。ネットワークでマルチキャスト DNS が無効になっている場合、MDNS ルーティングを使用するには、ネットワーク機器の設定変更を実行する必要があります。
- すべてのノードが同じマルチキャストドメイン内にあることを確認してください。

ルーター間の前提条件

ネットワークで DNS が利用できる場合は、クラスタノード名として IP アドレス、ホスト名、または FQDN を使用できます。ただし、ネットワークで DNS が使用できない場合は、ノード名に IP アドレスを使用する必要があります。

IP アドレスを使用するためにノード名を再設定する必要がある場合は、<http://www.cisco.com/c/en/us/support/%20unified-communications/unified-communications-manager-callmanager/%20products-maintenance-guides-list.html>にある「Cisco Unified Communications Manager および IM and Presence サービスの IP アドレスとホスト名の変更の『ノード名変更』」を参照します。

高度なルーティング設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ルーティング通信方法の設定 (141 ページ)	ルーティング通信の種類によって、IM and Presence サービスがクラスタノード間のルータ接続を確立するために使用するルーティング方式が決まります。単一ノードの IM and Presence Service 展開の場合は、ルーティング通信タイプをデ

	コマンドまたはアクション	目的
		フォルト設定のままにすることを推奨します。
ステップ 2	Cisco XCP ルータの再起動 (142 ページ)	ルーティング通信タイプを編集した場合は、Cisco XCP Router を再起動する必要があります。
ステップ 3	セキュアなルータツールータ通信の設定 (143 ページ)。	これはオプションです。ルーター間通信を構成している場合は、同じクラスター内または異なるクラスター内の XMPP ルーター間に安全な TLS 接続を構成できます。 (注) このオプションはパフォーマンスが低下する可能性があるため、IM and Presence サービスが安全でないネットワーク上で実行されている場合にのみ有効にしてください。
ステップ 4	クラスター ID の設定 (144 ページ)	MDNS ルーティングを使用している場合は、クラスター ID はクラスター内のすべてのノードで共有され、値はクラスターごとに一意です。必要に応じて、この手順を使ってクラスター ID を更新できます。
ステップ 5	プレゼンス更新のスロットレートを設定する (144 ページ)	これはオプションです。メッセージで Cisco XCP Router に送信されるアベイラビリティ (プレゼンス) 変更のレート (秒当たり) を設定できます。この値を設定すると、IM and Presence サービスはアベイラビリティ (プレゼンス) 変更のレートを設定値に合わせて小さくします。
ステップ 6	スタティック ルートの設定 (145 ページ)	スタティックルートを設定したいと思う場合これらのタスクを完了して下さい。

ルーティング通信方法の設定

ルーティング通信の種類によって、IM and Presence サービスがクラスターノード間のルータ接続を確立するために使用するルーティング方式が決まります。単一ノードの IM and Presence Service 展開の場合は、ルーティング通信タイプをデフォルト設定のままにすることを推奨します。



注意 クラスタ設定を完了し、IM and Presence Service 展開へのユーザ トラフィックの受け入れを開始する前に、ルーティング通信タイプを設定する必要があります。

始める前に

MDNS ルーティングを使用する場合は、IOS ネットワーク全体で MDNS を有効にする必要があります。

手順

- ステップ 1 IM and Presence データベース パブリッシャ ノードで、[Cisco Unified CM IM and Presence Administration] にログインします。
- ステップ 2 [System (システム)] > [Service Parameters (サービス パラメータ)] を選択します。
- ステップ 3 [サーバ (Server)] ドロップダウン リスト ボックスから、[IM and Presence サービス (IM and Presence Service)] ノードを選択します。
- ステップ 4 [サービス (Service)] ドロップダウン リスト ボックスから、[Cisco XCP ルータ (Cisco XCP Router)] を選択します。
- ステップ 5 XCP ルータのグローバル設定 (クラスタ全体) で、ルーティング通信タイプサービスパラメータのルーティングタイプを選択します：
 - [マルチキャスト DNS (MDNS) (Multicast DNS (MDNS))] - クラスタのノードが同じマルチキャスト ドメインにある場合は、この方法を選択します。
 - [ルータツールータ (Router-to-Router)] - クラスタのノードが同じマルチキャスト ドメイン内にはない場合、この方法を選択します。これがデフォルト設定です。

(注) ルータツールータ接続を使用する場合、展開では、IM and Presence Service が XCP ルートファブリックを確立している間、追加のパフォーマンスのオーバーヘッドが発生します。
- ステップ 6 [保存 (Save)] をクリックします。

次のタスク

この設定を編集した場合は、[Cisco XCP ルータの再起動 \(142 ページ\)](#)

Cisco XCP ルータの再起動

ルーティング通信タイプを編集した場合は、Cisco XCP Router サービスを再起動する必要があります。

始める前に

[ルーティング通信方法の設定 \(141 ページ\)](#)

手順

-
- ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)]>[コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
 - ステップ 2 [サーバ (Server)] リストから、サービスを再アクティブ化するノードを選択し、[移動 (Go)] をクリックします。
 - ステップ 3 [IM and Presence サービス (IM and Presence Services)] 領域で、[Cisco XCP Router] を選択します。
 - ステップ 4 [再起動 (Restart)] をクリックします。
-

次のタスク

ルータツールータルーティングが設定されている場合は、[セキュアなルータツールータ通信の設定 \(143 ページ\)](#)

MDNS ルーティングが設定されている場合は、[クラスタ ID の設定 \(144 ページ\)](#)。

セキュアなルータツールータ通信の設定

あなたが持っている場合ルーター間通信が設定されている場合は、この任意の手順を使用して、同じクラスタ内または異なるクラスタ内の XMPP ルータ間で安全な TLS 接続を使用できます。IM and Presence サービスは XMPP 証明書を XMPP 信頼証明書として自動的にクラスタ内またはクラスタ間で複製します。



-
- (注) このオプションはパフォーマンスが低下する可能性があるため、IM and Presence サービスが安全でないネットワーク上で実行されている場合にのみ有効にしてください。
-

手順

-
- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] から、[システム (System)]>[セキュリティ (Security)]>[設定 (Settings)] を選択します。
 - ステップ 2 [XMPP ルータツールータ セキュア モードの有効化 (Enable XMPP Router-to-Router Secure Mode)] チェックボックスをチェックします。
 - ステップ 3 [保存 (Save)] をクリックします。
-

次のタスク

[プレゼンス更新のスロットルレートを設定する \(144 ページ\)](#)

クラスタ ID の設定

MDNS ルーティングを使用している場合は、**クラスタ ID** はクラスタ内のすべてのノードで共有され、値はクラスタごとに一意です。必要に応じて、この手順を使って**クラスタ ID** を更新できます。



(注) インストール時に、システムはデフォルトの固有の**クラスタ ID** を各 IM and Presence サービス クラスタに割り当てます。変更が必要な場合以外は、デフォルト設定値のままにすることを推奨します。

手順

ステップ 1 IM and Presence サービス データベース パブリッシャ ノードで、[Cisco Unified CM IM and Presence Administration] にログインします。

ステップ 2 [プレゼンス (Presence)] > [設定 (Settings)] > [標準設定 (Standard Configuration)] を選択します。

ステップ 3 **クラスタ ID** フィールドの値を確認します。ID を編集する必要がある場合は、新しい値を入力してください。

IM and Presence サービスは、クラスタ ID 値でのアンダースコア文字 (_) を許可しません。クラスタ ID 値にこの文字が含まれていないことを確認します。

ステップ 4 [保存 (Save)] をクリックします。

クラスタ ID を編集した場合、新しい設定はすべてのクラスタノードに複製されます。

次のタスク

[プレゼンス更新のスロットルレートを設定する \(144 ページ\)](#)

プレゼンス更新のスロットルレートを設定する

このオプションの手順を使用して、メッセージで Cisco XCP Router に送信されるアベイラビリティ (プレゼンス) 変更のレート (秒あたり) を設定できます。この設定は、IM and Presence サービスがアベイラビリティ (プレゼンス) 変更のレートを設定値に合わせて小さくする際の負荷を防ぐのに役立ちます。

手順

- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。
- ステップ 2 [サーバ (Server)] ドロップダウンリスト ボックスから、[IM and Presence サービス (IM and Presence Service)] ノードを選択します。
- ステップ 3 [サービス (Service)] ドロップダウンリストボックスから、[Cisco Presence Engine] を選択します。
- ステップ 4 [クラスタ全体のパラメータ (Parameters that apply to all servers)] セクションで、[プレゼンス変更スロットル レート (Presence Change Throttle Rate)] サービスパラメータを編集します。有効範囲は 10 から 100 で、デフォルト設定は 50 です。
- ステップ 5 [保存 (Save)] をクリックします。

次のタスク

フェデレーション接続に SIP スタティックルートを設定したい場合は、[スタティックルートの設定 \(145 ページ\)](#)。

スタティック ルートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	SIP プロキシサーバを設定します。 (146 ページ)	SIP プロキシサーバを設定します。WAN 配置の場合は、IM and Presence サービスで TCP 方式イベントルーティングを有効にすることを推奨します。
ステップ 2	IM and Presence Service のルート組み込みテンプレートの設定 (146 ページ)	スタティックルートに埋め込みワイルドカードが含まれている場合は、ルート埋め込みテンプレートを設定する必要があります。
ステップ 3	IM and Presence Service のスタティックルートの設定 (148 ページ)	スタティック ルートを設定します。

SIP プロキシ サーバを設定します。

SIP プロキシ サーバを設定します。

手順

- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[プレゼンス (Presence)] > [ルーティング (Routing)] > [設定 (Settings)] を選択します。
- ステップ 2 [メソッド/イベントルーティングのステータス (Method/Event Routing Status)] で [オン (On)] を選択します。WAN 配置の場合は、IM and Presence サービスで TCP 方式イベントルーティングを有効にすることを推奨します。
- ステップ 3 [優先プロキシサーバ (Preferred Proxy Server)] で [デフォルト SIP プロキシ TCP リスナー (Default SIP Proxy TCP Listener)] を選択します。
- ステップ 4 [保存 (Save)] をクリックします。

IM and Presence Service のルート組み込みテンプレートの設定

スタティックルートに埋め込みワイルドカードが含まれている場合は、ルート埋め込みテンプレートを設定する必要があります。

手順

- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [サービスパラメータ (Service Parameters)] を選択します。
- ステップ 2 [サーバ (Server)] ドロップダウンから、IM and Presence サービスノードを選択します。
- ステップ 3 [サービス (Service)] ドロップダウンリストから、[Cisco SIP Proxy] を選択します。
- ステップ 4 ルーティングパラメータ (クラスタ全体) で、RouteEmbedTemplate フィールドにテンプレートを入力します。最大5つのテンプレートを定義できます。単一ルート組み込みテンプレートに定義できるスタティックルートの数に制限はありません。
- ステップ 5 [保存 (Save)] をクリックします。

次のタスク

[IM and Presence Service のスタティックルートの設定 \(148 ページ\)](#)

ルート組み込みテンプレート

組み込みのワイルドカードを含む任意のスタティックルートパターンにルート組み込みテンプレートを定義する必要があります。ルート組み込みテンプレートには、組み込みのワイルドカードの先頭の数字、数字の長さ、および場所に関する情報が含まれます。ルート組み込みテンプレートを定義する前に、次のサンプルテンプレートを考慮してください。

ルート組み込みテンプレートを定義するときは、「.」に続く文字がスタティック ルートの実際のテレフォニーの数字と一致する必要があります。次のルート組み込みテンプレートのサンプルでは、これらの文字を「x」で表しています。

サンプル ルート組み込みテンプレート A

ルート組み込みテンプレート : 74..78xxxxx*

このテンプレートでは、IM and Presence Service は、組み込みのワイルドカードでスタティック ルートの次のセットを有効にします。

表 12: 組み込みワイルドカードで設定したスタティック ルート - テンプレート A

宛先パターン (Destination Pattern)	ネクスト ホップ宛先
74..7812345*	1.2.3.4:5060
74..7867890*	5.6.7.8.9:5060
74..7811993*	10.10.11.37:5060

このテンプレートでは、IM and Presence Service は次のスタティック ルート エントリを有効にしません。

- 73..7812345* (最初の文字列がテンプレートで定義されている「74」ではない)
- 74..781* (宛先パターンの数字の長さがテンプレートと一致しない)
- 74...7812345* (ワイルドカードの数がテンプレートと一致しない)

サンプル ルート組み込みテンプレート B

ルート組み込みテンプレート : 471...xx*

このテンプレートでは、IM and Presence Service は、組み込みのワイルドカードでスタティック ルートの次のセットを有効にします。

表 13: 組み込みワイルドカードで設定したスタティック ルート - テンプレート B

宛先パターン (Destination Pattern)	ネクスト ホップ宛先
471...34*	20.20.21.22
471...55*	21.21.55.79

このテンプレートでは、IM and Presence Service は次のスタティック ルート エントリを有効にしません。

- 47...344* (最初の文字列がテンプレートで定義されている「471」ではない)
- 471...4* (文字列の長さがテンプレートと一致しない)
- 471.450* (ワイルドカードの数がテンプレートと一致しない)

IM and Presence Service のスタティック ルートの設定

この手順を使用して、スタティックルートを設定します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

手順

- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[ルーティング (Routing)] > [スタティック ルート (Static Routes)] を選択します。
- ステップ 2 [新規追加 (Add New)] をクリックします。
- ステップ 3 宛先パターンに、ルートパターンを入力します。
- ステップ 4 [ネクスト ホップ (Next Hop)] フィールドに、次のホップサーバーの IP アドレス、FQDN またはホスト名を入力します。
- ステップ 5 ネクストホップポートに、次のホップサーバの宛先ポートを入力します。デフォルトポートは 5060 です。
- ステップ 6 ルートタイプドロップダウンから、ルートの種類を選択します。ユーザまたはドメイン。
- ステップ 7 プロトコルの種類ドロップダウンリストボックスから、スタティックルートのプロトコルを選択します。TCP、UDP または TLS。
- ステップ 8 [スタティック ルートの設定 (Static Route Configuration)] ウィンドウの残りのフィールドに入力します。
- ステップ 9 [保存 (Save)] をクリックします。

スタティック ルートのパラメータ設定

次の表は、IM and Presence Service で設定できるスタティック ルート パラメータ設定の一覧です。

表 14: IM and Presence Service のスタティック ルートパラメータ設定

フィールド	説明
宛先パターン (Destination Pattern)	<p>着信番号のパターンを 255 文字以内で指定します。</p> <p>SIP プロキシでは、100 本のスタティック ルートにだけ同じルートパターンを割り当てることができます。この制限を超えた場合、IM and Presence Service はエラーをログに記録します。</p> <p>ワイルドカードの使用方法</p> <p>単一文字のワイルドカードとして「.」を、複数文字のワイルドカードとして「*」を使用できます。</p> <p>IM and Presence Service は、スタティック ルートにおける組み込みのワイルドカード文字である「.」をサポートします。ただし、組み込みのワイルドカードを含むスタティック ルートのルート組み込みテンプレートを定義する必要があります。組み込みのワイルドカードを含むスタティック ルートは、ルート組み込みテンプレートの少なくとも 1 つと一致する必要があります。ルート組み込みテンプレートの定義については、ルート組み込みテンプレートのトピック（次の「関連トピック」内）を参照してください。</p> <p>電話機の場合：</p> <ul style="list-style-type: none"> • ドットはパターンの末尾に置くことも、パターンに組み込むこともできます。パターンにドットを組み込む場合は、パターンに一致するルート組み込みテンプレートを作成する必要があります。 • アスタリスクは、パターン最後のみに使用できます。 <p>IP アドレスおよびホスト名の場合：</p> <ul style="list-style-type: none"> • アスタリスクはホスト名の一部として使用できます。 • ドットはホスト名のリテラル値の役割を果たします。 <p>エスケープ文字とアスタリスクの連続 (*) はリテラル * と一致し、任意の場所で使用できます。</p>
説明	<p>特定のスタティック ルートの説明を 255 文字以内で指定します。</p>
ネクスト ホップ (Next Hop)	<p>着信先（ネクスト ホップ）のドメイン名または IP アドレスを指定し、完全修飾ドメイン名（FQDN）またはドット付き IP アドレスのいずれかにすることができます。</p> <p>IM and Presence Service では、DNS SRV ベースのコールルーティングをサポートしています。DNS SRV をスタティック ルート用のネクストホップとして指定する場合は、このパラメータを該当する DNS SRV の名前に設定します。</p>

フィールド	説明
ネクスト ホップ ポート (Next Hop Port)	<p>着信先 (ネクストホップ) のポート番号を指定します。デフォルトポートは 5060 です。</p> <p>IM and Presence Service では、DNS SRV ベースのコール ルーティングをサポートしています。DNS SRV をスタティックルート用のネクストホップとして指定する場合は、このパラメータを 0 に設定します。</p>
ルート タイプ (Route Type)	<p>ルートタイプを指定します ([ユーザ (User)] または [ドメイン (Domain)])。デフォルト値は [ユーザ (User)] です。</p> <p>たとえば、SIP URI sip:19194762030@myhost.com 要求で、ユーザ部分は 19194762030 で、ホスト部分は myhost.com です。ルートタイプとして [ユーザ (User)] を選択すると、IM and Presence Service は SIP トラフィックをルーティングするためにユーザ部分の値 19194762030 を使用します。ルートタイプとして [ドメイン (Domain)] を選択すると、IM and Presence Service は SIP トラフィックをルーティングするために myhost.com を使用します。</p>
プロトコル タイプ (Protocol Type)	<p>このルートのプロトコルタイプ (TCP、UDP、または TLS) を指定します。デフォルト値は TCP です。</p>
プライオリティ (Priority)	<p>このルートのプライオリティレベルを指定します。値が小さいほど、プライオリティが高くなります。デフォルト値は 1 です。</p> <p>値の範囲 : 1 ~ 65535</p>

フィールド	説明
重み (Weight)	<p>ルートの重み付けを指定します。このパラメータは、複数のルートのプライオリティが同じ場合に限り使用します。値が大きいほど、ルートのプライオリティが高くなります。</p> <p>値の範囲：1 ～ 65535</p> <p>例：次のプライオリティと重み付けが関連付けられた 3 本のルートがあるとします。</p> <ul style="list-style-type: none"> • 1、20 • 1、10 • 2、50 <p>この例では、スタティックルートが適切な順序で表示されています。プライオリティルートは、最低値のプライオリティ (値 1) が基準となります。2 つのルートが同じプライオリティを共有している場合、値の高いほうの重量パラメータによってプライオリティルートが決定します。この例では、IM and Presence Service はプライオリティ値として 1 が設定されている両方のルートに SIP トラフィックを送信し、重み付けに従ってトラフィックを分散させます。重み付けが 20 のルートは、重み付けが 10 のルートの 2 倍のトラフィックを受信します。この例では、IM and Presence Service はプライオリティ 1 の両方のルートを試み、両方が失敗した場合だけプライオリティ 2 のルートを使用しようとします。</p>
固有性の低いルートを許可 (Allow Less-Specific Route)	固有性の低いルートを許可することを示します。デフォルト設定はオンです。
サービス中 (In Service)	ルートをアウト オブ サービスにするかどうかを指定します。ルートをアウト オブ サービスにするかどうかを指定します。
[ルートのブロック (Block Route)] チェックボックス	オンにすると、スタティックルートがブロックされます。デフォルト設定は、ブロック解除です。



第 11 章

証明書の設定

- [証明書の概要](#) (153 ページ)
- [証明書の前提条件](#) (155 ページ)
- [Cisco Unified Communications Manager との証明書の交換](#) (156 ページ)
- [IM and Presence サービスに認証局 \(CA\) をインストールする](#) (159 ページ)
- [IM and Presence Service に証明書をアップロードします。](#) (162 ページ)
- [CSR の生成](#) (167 ページ)
- [自己署名証明書の生成](#) (169 ページ)
- [証明書モニタリング タスク フロー](#) (171 ページ)

証明書の概要

証明書は ID を保護し、IM and Presence サービスと他のシステムとの間に信頼関係を構築するために使用されます。証明書を使用して、IM and Presence サービスを Cisco Unified Communications Manager、Cisco Jabber クライアント、または任意の外部サーバに接続できます。証明書がないと、不正な DNS サーバが使用されていたのか、それとも他のサーバにルーティングされていたのかを知ることは不可能です。

IM and Presence サービスが使用できる証明書には、主に 2 つのクラスがあります。

- **自己署名証明書** - 自己署名証明書は、証明書を発行したのと同じサーバによって署名されます。企業内では、自己署名証明書を使用して他の内部システムに接続することができます。ただし、それらの接続が安全でないネットワークを経由していない場合に限りです。たとえば、IM and Presence サービスは、Cisco Unified Communications Manager への内部接続用の自己署名証明書を生成します。
- **CA 署名付き証明書** - サードパーティの認証局 (CA) によって署名された証明書です。これらは、公的な CA (Verisign、Entrust、Digicert など) またはサーバ (Windows 2003、Linux、Unix、IOS など) によって署名され、サーバ/サービス証明書の有効性を管理できます。CA 署名付き証明書は自己署名証明書よりも安全であり、通常はあらゆる WAN 接続に使用されます。たとえば、他の企業とのフェデレーション接続または WAN 接続を使用するクラスタ間ピア設定では、外部システムとの信頼関係を構築するために CA 署名付き証明書が必要になります。

CA 署名付き証明書は自己署名証明書よりも安全です。一般に、自己署名証明書は内部接続に適していますが、WAN 接続または公衆インターネットを経由する接続には CA 署名証明書を使用する必要があります。

マルチサーバ証明書

IM and Presence サービスは、一部のシステムサービスに対してマルチサーバ SAN 証明書もサポートしています。マルチサーバ証明書の証明書署名要求 (CSR) を生成すると、証明書がいずれかのクラスターノードにアップロードされると、結果として得られるマルチサーバ証明書とそれに関連付けられた署名証明書のチェーンが自動的にすべてのクラスターノードに配布されます。

IM and Presence Services の証明書タイプ

IM and Presence サービス内では、さまざまなシステムコンポーネントにさまざまな種類の証明書が必要です。ここでは、IM and Presence Service のクライアントとサービスに必要なさまざまな証明書について説明します。



(注) 証明書名が -ECDSA で終わる場合、その証明書/キータイプは楕円曲線 (EC) です。それ以外の場合は、RSA です。

表 15: 証明書タイプおよびサービス

証明書タイプ	サービス	証明書信頼ストア	マルチサーバサポート	注記
tomcat、 tomcat-ECDSA	Cisco Client Profile Agent、 Cisco AXL Web Service、 Cisco Tomcat	tomcat- trust	あり	IM and Presence Service のクライアント認証の一部として Cisco Jabber クライアントに提示されます。 Cisco Unified CM IM およびプレゼンス管理ユーザインターフェイスを移動するときに、Web ブラウザに表示されます。 関連する信頼ストアを使用し、ユーザのクレデンシャルを認証するために、IM and Presence Service が確立した設定済みの LDAP サーバとの接続を確認します。
ipsec		ipsec-trust	なし	IPSec ポリシーが有効になっている場合に使用します。

証明書タイプ	サービス	証明書信頼ストア	マルチサーバサポート	注記
cup, cup-ECDSA	Cisco SIP Proxy、 Cisco Presence Engine	cup-trust	なし	Expressway-Cに証明書を提示して、SIP フェデレーションユーザ用の IM and Presence を取得します。IM and Presence プロキシは、クライアントとサーバの両方として動作します。 プレゼンスエンジンは、これらの証明書を Exchange/Office 365 との通信に使用してカレンダープレゼンスを取得します。プレゼンスエンジンは、クライアントとしてのみ動作します。
cup-xmpp、 cup-xmpp-ECDSA	Cisco XCP Connection Manager、 Cisco XCP Web Connection Manager、 Cisco XCP Directory service、 Cisco XCP Router サービス	cup-xmpp-trust	あり	XMPP セッションの作成中に、Cisco Jabber クライアント、サードパーティ製 XMPP クライアント、または CAXL ベースのアプリケーションに提示されます。 関連する信頼ストアを使用して、サードパーティ製 XMPP クライアントの LDAP 検索操作を実行中に Cisco XCP Directory サービスが確立した接続を確認します。 ルーティング通信タイプがルータ間に設定されている場合に、IM and Presence Service サーバ間にセキュアな接続を確立するときに Cisco XCP Router によって関連する信頼ストアが使用されます。
cup-xmpp-s2s、 cup-xmpp-s2s-ECDSA	Cisco XCP XMPP Federation Connection Manager	cup-xmpp-trust	あり	外部フェデレーション XMPP への接続時に XMPP ドメイン間フェデレーションを行うために提示されます。

証明書的前提条件

Cisco Unified Communications Manager で次の項目を設定します。

- IM and Presence サービスの SIP トランク セキュリティ プロファイルの設定
- IM and Presence Service の SIP トランクを設定します。
 - SIP トランクにセキュリティ プロファイルを関連付けます。

- IM and Presence Service 証明書のサブジェクト共通名 (CN) を SIP トランクに設定します。

Cisco Unified Communications Manager との証明書の交換

Cisco Unified Communications Manager との証明書の交換には以下のタスクを完了します。



- (注) Cisco Unified Communications Manager と IM and Presence サービス間の証明書交換は、インストールプロセス中に自動的に処理されます。ただし、証明書交換を手動で完了する必要がある場合は、これらの作業を完了してください。

手順

	コマンドまたはアクション	目的
ステップ 1	IM and Presence サービスへの Cisco Unified Communications Manager 証明書のインポート (156 ページ)	IM and Presence サービスに Cisco Unified Communications Manager からの証明書をインポートします。
ステップ 2	IM and Presence サービスからの証明書のダウンロード (157 ページ)	IM and Presence Service から証明書をダウンロードします。次の各証明書を Cisco Unified Communications Manager にインポートする必要があります。
ステップ 3	IM and Presence 証明書を Cisco Unified Communications Manager にインポート (158 ページ)	証明書の交換を完了するには、IM and Presence サービス証明書を Cisco Unified Communications Manager の Callmanager-trust ストアにアップロードします。

IM and Presence サービスへの Cisco Unified Communications Manager 証明書のインポート

この手順を使用して IM and Presence サービスに Cisco Unified Communications Manager からの証明書をインポートします。

手順

- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [セキュリティ (Security)] > [証明書インポートツール (Certificate Import Tool)] を選択します。
- ステップ 2 [証明書信頼ストア (Certificate Trust Store)] メニューから [IM and Presence (IM/P) サービス信頼 (IM and Presence (IM/P) Service Trust)] を選択します。
- ステップ 3 Cisco Unified Communications Manager ノードの IP アドレス、ホスト名、または FQDN を入力します。
- ステップ 4 Cisco Unified Communications Manager ノードと通信するポート番号を入力します。
- ステップ 5 [送信 (Submit)] をクリックします。

(注) 証明書インポートツールのインポート操作が完了すると、Cisco Unified Communications Manager に正常に接続したかどうか、また、Cisco Unified Communications Manager から証明書が正常にダウンロードされたかどうか報告されます。証明書インポートツールで障害が報告された場合、推奨処置についてはオンラインヘルプを参照してください。[Cisco Unified IM and Presence OS の管理 (Cisco Unified IM and Presence OS Administration)] > [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択して、手動で証明書をインポートすることもできます。

(注) ネゴシエートされる TLS 暗号方式に応じて、証明書インポートツールにより、RSA ベースの証明書または ECDSA ベースの証明書のいずれかがダウンロードされます。

- ステップ 6 Cisco SIP プロキシ サービスを再起動します。
 - a) IM and Presence サービスで [Cisco Unified IM and Presence サービスサビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター - 機能サービス (Control Center - Feature Services)] を選択します。
 - b) [サーバ (Server)] ドロップダウンリストから [IM and Presence Service] ノードを選択し、[移動 (Go)] をクリックします。
 - c) Cisco SIP Proxy を選択し、再起動をクリックします。

次のタスク

[IM and Presence サービスからの証明書のダウンロード \(157 ページ\)](#)

IM and Presence サービスからの証明書のダウンロード

この手順を使用して IM and Presence Service から証明書をダウンロードします。次の各証明書を Cisco Unified Communications Manager にインポートする必要があります。

手順

ステップ 1 IM and Presence サービスで、[**Cisco Unified IM and Presence OS の管理 (Cisco Unified IM and Presence OS Administration)**] から、[**セキュリティ (Security)**] > [**証明書の管理 (Certificate Management)**] を選択します。

ステップ 2 [検索 (Find)] をクリックします。

ステップ 3 cup.pem ファイルを選択します。

(注) cup-ECDSA.pem を選択することもできます。

ステップ 4 [ダウンロード] をクリックして、ローカル コンピュータにファイルを保存します。

ヒント IM and Presence サービスが表示する cup.csr ファイルへのアクセスに関するすべてのエラーを無視してください。Cisco Unified Communications Manager と交換する証明書に CA (認証局) が署名する必要はありません。

次のタスク

[IM and Presence 証明書を Cisco Unified Communications Manager にインポート \(158 ページ\)](#)

IM and Presence 証明書を Cisco Unified Communications Manager にインポート

証明書の交換を完了するには、IM and Presence サービス証明書を Cisco Unified Communications Manager の Callmanager-trust ストアにアップロードします。

始める前に

[IM and Presence サービスからの証明書のダウンロード \(157 ページ\)](#)

手順

ステップ 1 Cisco Unified OS の管理にログインします。

ステップ 2 [セキュリティ (Security)] > [証明書管理 (Certificate Management)] を選択します。

ステップ 3 [証明書のアップロード] をクリックします。

ステップ 4 [証明書名 (Certificate Name)] メニューから [**Callmanager-trust**] を選択します。

ステップ 5 IM and Presence サービスから以前にダウンロードした証明書を閲覧し、選択します。

ステップ 6 [ファイルのアップロード (Upload File)] をクリックします。

ステップ 7 Cisco CallManager サービスを再起動します。

- a) Cisco Unified Serviceability から、[ツール (Tools)] > [コントロール センター - 機能サービス (Control Center - Feature Services)] の順に選択します。
- b) [サーバ (Server)] ドロップダウンリスト ボックスから、Cisco Unified Communications Manager ノードを選択し、[Go (移動)] をクリックします。
- c) **Cisco CallManager** サービスを選択して[再起動 (Restart)] をクリックします。

IM and Presence サービスに認証局 (CA) をインストールする

IM and Presence サービスでサードパーティの認証局 (CA) によって署名された証明書を使用するには、まずその CA のルート証明書信頼チェーンを IM and Presence サービスにインストールする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	CA ルート証明書チェーンをアップロードする (159 ページ)	この手順を使用して、CA のルート証明書チェーンをサードパーティの認証局から IM and Presence サービスにアップロードします。
ステップ 2	Cisco Intercluster Sync Agent サービスの再起動 (160 ページ)	証明書をアップロードしたら、Cisco Intercluster Sync Agent サービスを再起動します。
ステップ 3	他のクラスタとの CA 証明書の同期の検証 (161 ページ)	CA 証明書チェーンがすべてのピアクラスタに複製されたことを確認します。

CA ルート証明書チェーンをアップロードする

この手順を使用して、署名している認証局 (CA) から IM and Presence データベースパブリッシュャノードに証明書チェーンをアップロードします。チェーンはチェーン内の複数の証明書で構成され、各証明書は後続の証明書に署名します。

- ルート証明書 > 中間 1 証明書 > 中間 2 証明書

手順

- ステップ 1 IM and Presence データベース パブリッシュャ ノードで、[Cisco Unified CM IM and Presence OS Administration] にログインします。

- ステップ2 [セキュリティ (Security)] > [証明書管理 (Certificate Management)] を選択します。
- ステップ3 [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate chain)] をクリックします。
- ステップ4 [証明書名 (Certificate Name)] ドロップダウンリストから、以下のいずれか1つを選択します。
- CA 署名付きの tomact 証明書をアップロードする場合は、**トムキャット信頼**を選択します。
 - CA 署名の cup-xmpp 証明書または CA 署名の cup-xmpp-s2s をアップロードする場合は、**cup-xmpp-trust**を選択します。
- ステップ5 署名付き証明書の説明を入力します。
- ステップ6 [参照 (Browse)] をクリックしてルート証明書のファイルを見つけます。
- ステップ7 [ファイルのアップロード (Upload File)] をクリックします。
- ステップ8 [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate chain)] ウィンドウを使用して、各中間証明書を同じ方法でアップロードします。中間証明書ごとに、チェーン内の前の証明書の名前を入力する必要があります。

次のタスク

[Cisco Intercluster Sync Agent サービスの再起動 \(160 ページ\)](#)

Cisco Intercluster Sync Agent サービスの再起動

IM and Presence データベース パブリッシュャ ノードにルートおよび中間証明書をアップロードしたら、そのノードで Cisco Intercluster Sync Agent サービスを再起動する必要があります。このサービスの再起動することにより、ただちに CA 証明書が他のすべてのクラスタに同期されます。

手順

- ステップ1 [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
- ステップ2 [サーバ (Server)] ドロップダウンリスト ボックスから、証明書をインポートする先の [IM and Presence Service] ノードを選択し、[移動 (Go)] をクリックします。
- (注) Command Line Interface から、`utils service restart Cisco Intercluster Sync Agent` コマンドで Cisco Intercluster Sync Agent サービスを再起動することも可能です。
- ステップ3 **Cisco Intercluster Sync Agent** サービスを選択して、**再起動**をクリックします。

次のタスク

[クラスタ間同期の検証 \(164 ページ\)](#)

他のクラスタとの CA 証明書の同期の検証

Cisco Intercluster Sync Agent サービスが再起動した後、CA 証明書が他のクラスタに正しく同期されたことを確認する必要があります。他の IM and Presence データベース パブリッシャの各ノードで、次の手順を実行します。



(注) この手順の情報は、-ECDSA で終わる証明書にも適用されます。

手順

- ステップ 1 Cisco Unified CM IM and Presence Administration で、[診断 (Diagnostics)] > [システムトラブルシュータ (System Troubleshooter)] を選択します。
- ステップ 2 [クラスタ間トラブルシュータ (Inter-clustering Troubleshooter)] で、[各 TLS 対応クラスタ間ピアが正常にセキュリティ証明書を交換しました (Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates)] テストを検索し、テストに合格していることを確認します。
- ステップ 3 テストでエラーが表示される場合は、クラスタ間ピアの IP アドレスを記録します。この IP アドレスは、CA 証明書をアップロードしたクラスタを参照している必要があります。次のステップを続行し、問題を解決します。
- ステップ 4 [プレゼンス (Presence)] > [クラスタ間 (Inter-Clustering)] を選択し、[システムトラブルシュータ (System Troubleshooter)] ページで識別したクラスタ間ピアに関連付けられているリンクをクリックします。
- ステップ 5 [強制手動同期 (Force Manual Sync)] をクリックします。
- ステップ 6 クラスタ間ピア ステータス パネルの自動リフレッシュには、60 秒かかります。
- ステップ 7 [証明書のステータス (Certificate Status)] フィールドに「セキュアな接続です (Connection is secure)」が表示されていることを確認します。
- ステップ 8 [証明書のステータス (Certificate Status)] フィールドに「セキュアな接続です (Connection is secure)」が表示されていない場合は、IM and Presence データベース パブリッシャ ノードで Cisco Intercluster Sync Agent サービスを再起動してから、ステップ 5 ~ 7 を繰り返します。
 - 管理者 CLI からサービスを再起動するには、utils service restart Cisco Intercluster Sync Agent コマンドを実行します。
 - また、Cisco Unified IM and Presence Serviceability の GUI からこのサービスを再起動できます。
- ステップ 9 この時点で [証明書のステータス (Certificate Status)] フィールドに「セキュアな接続です (Connection is secure)」が表示されていることを確認します。これは、クラスタ間同期がク

IM and Presence Service に証明書をアップロードします。

ラスタ間で正常に確立され、アップロードした CA 証明書がほかのクラスタに同期していることを意味します。

次のタスク

各 IM and Presence Service ノードへ署名付き証明書をアップロードします。

IM and Presence Service に証明書をアップロードします。

次のタスクを実行して、IM and Presence サービスに証明書をアップロードします。CA 署名付き証明書または自己署名証明書をアップロードできます。

始める前に

サードパーティの認証局 (CA) によって署名された CA 署名付き証明書を使用するには、その CA のルート証明書チェーンを IM and Presence サービスにインストールしておく必要があります。詳細は、[IM and Presence サービスに認証局 \(CA\) をインストールする \(159 ページ\)](#) を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書のアップロード (Upload Certificates) (163 ページ)	IM and Presence Service に署名付き証明書をアップロードします。
ステップ 2	Cisco Tomcat サービスの再起動 (164 ページ)	(Tomcat 証明書のみ)。Cisco Tomcat サービスを再起動します。
ステップ 3	クラスタ間同期の検証 (164 ページ)	(Tomcat 証明書のみ)。Cisco Tomcat サービスがクラスタ内の影響を受けるすべてのノードに対して再起動した後、クラスタ間同期が正常に動作していることを確認する必要があります。
ステップ 4	すべてのノードで Cisco XCP ルータ サービスを再起動します。 (165 ページ)	証明書を cup-xmpp ストアにアップロードした場合は、すべてのクラスタノードで Cisco XMP Router を再起動してください。
ステップ 5	Cisco XCP XMPP Federation Connection Manager サービスの再起動 (166 ページ)	(XMPP フェデレーションのみ)。XMPP フェデレーション用に cup-xmpp ストアに証明書をアップロードした場合は、Cisco XCPXMPP フェデレーション接続

	コマンドまたはアクション	目的
		マネージャサービスを再起動してください。
ステップ 6	XMPP フェデレーションのセキュリティ証明書でのワイルドカードの有効化 (166 ページ)	(XMPP フェデレーションのみ)。TLS を介して XMPP フェデレーション用の証明書を cup-xmpp ストアにアップロードした場合は、XMPP セキュリティ証明書のワイルドカードを有効にする必要があります。これはグループチャットに必要です。

証明書のアップロード (Upload Certificates)

この手順を使用して、各 IM and Presence Service ノードに証明書をアップロードします。



(注) クラスタに必要なすべての tomcat 証明書に署名し、それらを同時にアップロードすることを推奨します。この方法を使用すると、クラスタ間通信のリカバリに要する時間が短縮されます。



(注) この手順の情報は、-ECDSA で終わる証明書にも適用されます。

始める前に

証明書が CA によって署名されている場合は、その CA のルート証明書チェーンもインストールする必要があります。そうしないと、CA 署名付き証明書は信頼できません。CA 証明書がすべてのクラスタに正しく同期されている場合は、各 IM and Presence Service ノードに適切な署名付き証明書をアップロードできます。

手順

- ステップ 1 [Cisco Unified IM and Presence OS の管理 (Cisco Unified IM and Presence OS Administration)] で、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- ステップ 2 [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate chain)] をクリックします。
- ステップ 3 証明書の目的を選択します。例えば、tomcat。
- ステップ 4 署名付き証明書の説明を入力します。
- ステップ 5 アップロードするファイルを検索するには、[参照 (Browse)] をクリックします。
- ステップ 6 [ファイルのアップロード (Upload File)] をクリックします。

ステップ7 各 IM and Presence Service ノードで繰り返します。

次のタスク

Cisco Tomcat サービスを再起動します。

Cisco Tomcat サービスの再起動

各 IM and Presence サービス ノードに tomcat 証明書をアップロードしたら、各ノードで Cisco Tomcat サービスを再起動する必要があります。

手順

ステップ1 管理 CLI にログインします。

ステップ2 次のコマンドを実行します。 `utils service restart Cisco Tomcat`

ステップ3 各ノードで繰り返します。

次のタスク

クラスタ間同期が正常に動作していることを確認します。

クラスタ間同期の検証

Cisco Tomcat サービスがクラスタ内の影響を受けるすべてのノードに対して再起動した後、クラスタ間同期が正常に動作していることを確認する必要があります。他のクラスタの各 IM and Presence データベース パブリッシャ ノードで次の手順を実行します。

手順

ステップ1 **Cisco Unified CM IM and Presence Administration** で、**[診断 (Diagnostics)] > [システムトラブルシュータ (System Troubleshooter)]** を選択します。

ステップ2 **[クラスタ間トラブルシュータ (Inter-clustering Troubleshooter)]** で、**[各 TLS 対応クラスタ間ピアがセキュリティ証明書を正常に交換していることを確認する (Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates)]** テストを検索し、テストに合格していることを確認します。

ステップ3 テストでエラーが表示される場合は、クラスタ間ピアの IP アドレスを記録します。この IP アドレスは、CA 証明書をアップロードしたクラスタを参照している必要があります。次のステップを続行し、問題を解決します。

- ステップ 4** [プレゼンス (Presence)] > [クラスタ間 (Inter-Clustering)] を選択し、システム トラブルシューター (System Troubleshooter) ページで識別したクラスタ間ピアに関連付けられているリンクをクリックします。
- ステップ 5** [強制手動同期 (Force Manual Sync)] をクリックします。
- ステップ 6** [ピアの Tomcat 証明書も再同期します (Also resync peer's Tomcat certificates)] チェックボックスをオンにし、[OK] をクリックします。
- ステップ 7** クラスタ間ピア ステータス パネルの自動リフレッシュには、60 秒かかります。
- ステップ 8** [証明書のステータス (Certificate Status)] フィールドに「セキュアな接続です (Connection is secure) 」が表示されていることを確認します。
- ステップ 9** [証明書のステータス (Certificate Status)] フィールドに「セキュアな接続です (Connection is secure) 」が表示されていない場合は、IM and Presence データベース パブリッシャ ノードで Cisco Intercluster Sync Agent サービスを再起動してから、ステップ 5 ~ 8 を繰り返します。
- 管理者 CLI からサービスを再起動するには、`utils service restart Cisco Intercluster Sync Agent` コマンドを実行します。
 - また、Cisco Unified IM and Presence Serviceability の GUI からこのサービスを再起動できません。
- ステップ 10** この時点で [証明書のステータス (Certificate Status)] フィールドに「セキュアな接続です (Connection is secure) 」が表示されていることを確認します。これは、クラスタ間同期が、このクラスタと、証明書をアップロードしたクラスタの間で再確立されていることを意味します。

すべてのノードで Cisco XCP ルータ サービスを再起動します。

各 IM and Presence Service ノードに `cup-xmpp` の証明書や `cup-xmpp-ECDSA` の証明書をアップロードしたら、各ノードで Cisco XCP Router サービスを再起動する必要があります。



- (注) また、Cisco Unified IM and Presence Serviceability GUI から Cisco XCP Router サービス を再起動できません。

手順

- ステップ 1** 管理 CLI にログインします。
- ステップ 2** 次のコマンドを実行します。 `utils service restart Cisco XCP Router`
- ステップ 3** 各ノードで繰り返します。

Cisco XCP XMPP Federation Connection Manager サービスの再起動

各 IM and Presence サービス のフェデレーション ノードに cup-xmpp-s2s の証明書や cup-xmpp-s2s-ECDSA の証明書をアップロードしたら、各フェデレーションノードの Cisco XCP XMPP Federation Connection Manager サービスを再起動する必要があります。

手順

-
- ステップ 1 管理 CLI にログインします。
 - ステップ 2 次のコマンドを実行します。 `utils service restart Cisco XCP XMPP Federation Connection Manager`
 - ステップ 3 各フェデレーション ノードで繰り返します。
-

XMPP フェデレーションのセキュリティ証明書でのワイルドカードの有効化

XMPP フェデレーションのパートナー間での TLS を介してのグループ チャットをサポートするには、XMPP セキュリティ証明書に対するワイルドカードを有効にする必要があります。

デフォルトでは、XMPP フェデレーションセキュリティ証明書の cup-xmpp-s2s および cup-xmpp-s2s-ECDSA には IM and Presence サービス展開によってホストされるすべてのドメインが含まれます。これらは、証明書内のサブジェクト代替名 (SAN) エントリとして追加されます。同じ証明書内のホストされているすべてのドメインにワイルドカードを指定する必要があります。そのため、`example.com` の SAN エントリの代わりに、XMPP セキュリティ証明書には `*.example.com` の SAN エントリが含まれている必要があります。グループチャットのサーバエイリアスは、IM and Presence サービス システムでホストされているいずれかのドメインのサブドメインであるため、ワイルドカードが必要です。例：「`conference.example.com`」



-
- (注) 任意のノード上の cup-xmpp-s2s または cup-xmpp-s2s-ECDSA 証明書を表示するには、**Cisco Unified IM and Presence OS Administration** > [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択し、**cup-xmpp-s2s** または **cup-xmpp-s2s-ECDSA** リンクをクリックします。
-

手順

-
- ステップ 1 [システム (System)] > [セキュリティの設定 (Security Settings)] を選択します。
 - ステップ 2 [XMPP フェデレーションセキュリティ証明書でのワイルドカードの有効化 (Enable Wildcards in XMPP Federation Security Certificates)] をオンにします。

ステップ3 [保存 (Save)] をクリックします。

次のタスク

Cisco XMPP Federation Connection Manager サービスが実行しており、XMPP フェデレーションが有効になっているクラスタ内のすべてのノードで XMPP フェデレーションセキュリティ証明書を作成する必要があります。このセキュリティ設定は、すべての IM and Presence サービスクラスタで有効にし、TLS を介しての XMPP フェデレーションをサポートする必要があります。

CSR の生成

この手順を使用して証明書署名要求 (CSR) を生成します。CSR をサードパーティーの認証局に送信して、CA が署名した証明書を提供できるようにします。

手順

-
- ステップ1 Cisco Unified OS の管理から、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
 - ステップ2 [CSRの生成 (Generate CSR)] ボタンをクリックします。[証明書署名要求の作成 (Generate Certificate Signing Request)] ポップアップが表示されます。
 - ステップ3 証明書の目的ドロップダウンリストから、生成している証明書の種類を選択します。
 - ステップ4 [配信 (Distribution)] ドロップダウンから、IM and Presence サーバーを選択します。マルチサーバ証明書の場合は、マルチサーバ (SAN) を選択します。
 - ステップ5 キー長およびハッシュアルゴリズムを入力します。
 - ステップ6 残りのフィールドをすべて入力して生成をクリックします。
 - ステップ7 CSR をローカルコンピュータにダウンロードします。
 - a) [CSR のダウンロード (Download CSR)] をクリックします。
 - b) [証明書の用途 (Certificate Purpose)] ドロップダウン リストで、証明書名を選択します。
 - c) CSR のダウンロード

次のタスク

CSR をサードパーティーの認証局に送信して、CA が署名した証明書を発行できるようにします。

証明書署名要求のキー用途拡張

次の表には、Unified Communications Manager と IM and Presence Service の CA 証明書の証明書署名要求 (CSR) のキーの用途拡張が表示されています。

Table 16: Cisco Unified Communications Manager CSR キーの用途拡張

	マルチサーバ	キーの拡張用途			キーの用途				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント 認証 (1.3.6.1.5.5.7.3.2)	IP セキュリ ティ末端シ テム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号 化	キー証明書署 名	鍵共有
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		
CAPF (パブリッシャ のみ)	N	Y			Y	Y		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
信頼検証サービス (TVS)	Y	Y	Y		Y	Y	Y		

Table 17: IM and Presence Service CSR キーの用途拡張

	マルチサーバ	キーの拡張用途			キーの用途				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント 認証 (1.3.6.1.5.5.7.3.2)	IP セキュリ ティ末端シ テム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号 化	キー証明書署 名	鍵共有
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		Y
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

自己署名証明書の生成

自己署名証明書を生成するには、次の手順を使用します。

手順

- ステップ 1 Cisco Unified OS の管理から、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- ステップ 2 [自己署名証明書の作成 (Generate Self-signed)] をクリックします。新しい自己署名証明書を生成するポップアップが表示されます。
- ステップ 3 証明書の目的ドロップダウンリストから、生成している証明書の種類を選択します。
- ステップ 4 分布ドロップダウンから、サーバの名前を入力します。
- ステップ 5 適切なキーの長さを選択します。
- ステップ 6 ハッシュアルゴリズムから、暗号化アルゴリズムを選択します。例えば、SHA256 です。
- ステップ 7 [Generate] をクリックします。

IM and Presence Service からの自己署名信頼証明書の削除

同じクラスタ内のノード間でサービスアビリティ用のクロスナビゲーションをサポートするために、IM and Presence サービスと Cisco Unified Communications Manager の間の Cisco Tomcat サービス信頼ストアが自動的に同期されます。

元の自己署名信頼証明書を CA 署名証明書に置き換えた場合、元の自己署名信頼証明書はサービス信頼ストアに残ります。この手順を使用して、Cisco Unified Communications Manager と IM and Presence サービスの両方にある自己署名証明書を削除することもできます。

始める前に



- 重要** CA 署名付き証明書を追加したら、指定された IM and Presence Service ノード上で Cisco Intercluster Sync Agent サービスが定期的なクリーンアップタスクを実行するのを 30 分待機するようにします。

手順

- ステップ 1 [Cisco Unified Operating System Administration] から、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- ステップ 2 [検索 (Find)] をクリックします。

[証明書の一覧 (Certificate List)] が表示されます。

(注) 証明書の名前は、サービス名と証明書タイプの2つの部分で構成されています。たとえば tomcat-trust では、tomcat がサービスで trust が証明書タイプです。

削除できる自己署名付き信頼証明書は、次のとおりです。

- Tomcat および Tomcat-ECDSA : tomcat-trust
- Cup-xmpp および Cup-xmpp-ECDSA : cup-xmpp-trust
- Cup-xmpp-s2s および Cup-xmpp-s2s-ECDSA : cup-xmpp-trust
- Cup および Cup-ECDSA : cup-trust
- Ipsec : ipsec-trust

ステップ 3 削除する自己署名付き信頼証明書のリンクをクリックします。

重要 サービス信頼ストアに関連付けられているサービスに対して、CA 署名付き証明書がすでに設定されていることを確認します。

新しいウィンドウが表示され、証明書の詳細が示されます。

ステップ 4 [削除 (Delete)] をクリックします。

(注) [削除 (Delete)] ボタンは、その証明書を削除する権限がある場合にのみ表示されません。

ステップ 5 クラスタ内、およびでクラスタ間ピアの各 IM and Presence Service ノードに対してこの手順を繰り返し、不要な自己署名信頼証明書が展開全体で完全に削除されるようにします。

次のタスク

サービスが Tomcat である場合は、Cisco Unified Communications Manager ノード上の IM and Presence Service ノードの自己署名付き tomcat-trust 証明書を確認する必要があります。[Cisco Unified Communications Manager からの自己署名 Tomcat 信頼証明書の削除 \(170 ページ\)](#) を参照してください。

Cisco Unified Communications Manager からの自己署名 Tomcat 信頼証明書の削除

クラスタ内の各ノードについて、Cisco Unified Communications Manager サービス信頼ストアには1つの自己署名 tomcat 信頼証明書があります。Cisco Unified Communications Manager ノードから削除する対象となるのは、これらの証明書だけです。



(注) 次の手順の情報は、-EC 証明書にも適用されます。

始める前に

CA 署名付き証明書でクラスタの IM and Presence Service ノードをすでに設定し、証明書が Cisco Unified Communications Manager ノードに伝達されるよう 30 分間待機したことを確認します。

手順

- ステップ 1** Cisco Unified Operating System の管理ページで、[セキュリティ(Security)] > [証明書の管理(Certificate Management)] を選択します。
[証明書の一覧 (Certificate List)] ウィンドウが表示されます。
- ステップ 2** 検索結果をフィルタリングするには、ドロップダウンリストから [証明書 (Certificate)] および [で始まる (begins with)] を選択し、空のフィールドに tomcat-trust と入力します。[検索 (Find)] をクリックします。
[証明書の一覧 (Certificate List)] ウィンドウが拡張され、tomcat-trust の証明書が示されます。
- ステップ 3** IM and Presence Service ノードのホスト名、または名前の FQDN が含まれているリンクを特定します。これらは、このサービスおよび IM and Presence Service ノードに関連付けられている自己署名証明書です。
- ステップ 4** IM and Presence Service ノードの自己署名 tomcat-trust 証明書のリンクをクリックします。
新しいウィンドウが表示され、tomcat-trust 証明書の詳細が示されます。
- ステップ 5** 証明書の詳細で、Issuer Name CN= と Subject Name CN= の値が一致している、つまり自己署名の証明書であることを確認します。
- ステップ 6** 自己署名の証明書であることが確認され、CA 署名付き証明書が Cisco Unified Communications Manager ノードに確実に伝達されたと判断できる場合には、[削除 (Delete)] をクリックします。
(注) [削除 (Delete)] ボタンは、削除する権限が与えられている証明書に関してのみ表示されます。
- ステップ 7** クラスタ内の各 IM and Presence Service ノードに対して、手順 4、5、および 6 を繰り返します。

証明書モニタリングタスクフロー

次のタスクを行い、証明書ステータスと有効期限を自動的にモニタするようシステムを設定します。

- 証明書の有効期限が近づいているときは、電子メールで通知する
- 有効期限が切れた証明書を失効させる

手順

	コマンドまたはアクション	目的
ステップ 1	証明書モニタ通知の設定 (172 ページ)	証明書の自動モニタリングを構成します。システムは定期的に証明書ステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。
ステップ 2	OCSP による証明書失効の設定 (173 ページ)	期限切れの証明書が自動的に失効するように OCSP を設定します。

証明書モニタ通知の設定

Unified Communications Manager または IM and Presence サービスの自動証明書モニタリングを設定します。システムは定期的に証明書のステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。



- (注) [Cisco Certificate Expiry Monitor] ネットワーク サービスを実行している必要があります。デフォルトでこのサービスは有効化されていますが、[ツール (Tools)] > [コントロールセンター - ネットワーク サービス (Control Center - Network Services)] を選択し、[Cisco Certificate Expiry Monitor サービス (Cisco Certificate Expiry Monitor Service)] の状態が [実行中 (Running)] であることを検証して Cisco Unified Serviceability でサービスが実行中であることを確認できます。

手順

- ステップ 1 (Unified Communications Manager の証明書モニタリングのために) Cisco Unified OS の管理にログインするか、(IM and Presence サービスの証明書モニタリングのために) Cisco Unified IM and Presence の管理にログインします。
- ステップ 2 [セキュリティ (Security)] > [証明書モニタ (Certificate Management)] を選択します。
- ステップ 3 [通知開始時期 (Notification Start Time)] フィールドに、数値を入力します。この値は、近づきつつある有効期限の通知を、有効期限の何日前にシステムが開始するかを表します。
- ステップ 4 [通知頻度 (Notification Frequency)] フィールドには、通知を行う頻度を入力します。
- ステップ 5 これはオプションです。[電子メール通知を有効にする (Enable E-mail notification)] チェックボックスをオンにして、近づきつつある証明書有効期限に関する電子メールアラートをシステムに送信させます。

- ステップ 6** [LSC モニタリングを有効にする (Enable LSC Monitoring)] チェック ボックスをオンにして、LSC 証明書を証明書ステータス チェックに含めます。
- ステップ 7** [電子メール ID (E-mail IDs)] フィールドに、システムが通知を送信する電子メールアドレスを入力します。複数の電子メールアドレスは、セミコロンで区切って入力できます。
- ステップ 8** [保存 (Save)] をクリックします。

(注) 証明書モニタ サービスは、デフォルトで 24 時間ごとに 1 回だけ実行します。証明書モニタ サービスを再起動すると、サービスが開始され、24 時間後に実行する次のスケジュールが計算されます。証明書の有効期限が 7 日以内に近づいても、この周期は変化しません。このサービスは、証明書の有効期限が切れる 1 日前から、有効期限が切れた後も 1 時間おきに実行します。

次のタスク

Online Certificate Status Protocol (OCSP) を設定し、期限切れの証明書をシステムが自動的に失効させるようにします。詳細については、次を参照してください。[OCSP による証明書失効の設定 \(173 ページ\)](#)

OCSP による証明書失効の設定

オンライン証明書ステータスプロトコル (OCSP) を有効にして、証明書の状態を定期的にチェックし、期限切れの証明書を自動的に失効させます。

始める前に

システムに OCSP チェックに必要な証明書があることを確認します。OCSP 応答属性を設定されているルート CA 証明書または中間 CA 証明書を使用することができます。または、tomcat-trust へアップロードされている指定された OCSP 署名証明書を使用することができます。

手順

-
- ステップ 1** (Unified Communications Manager の証明書失効のために) Cisco Unified OS の管理にログインするか、(IM and Presence サービスの証明書失効のために) Cisco Unified IM and Presence の管理にログインします。
- ステップ 2** [セキュリティ (Security)] > [証明書失効 (Certificate Revocation)] を選択します。
- ステップ 3** [OCSP の有効化 (Enable OCSP)] チェック ボックスをオンにして、次のタスクのいずれかを実行します。
- OCSP チェックの OCSP レスポンダを指定する場合は、[設定済み OCSP URI を使用する (Use configured OCSP URI)] ボタンを選択し、[OCSP 設定済み URI (OCSP Configured URI)] フィールドにレスポンスの URI を入力します。
 - OCSP レスポンス URI で証明書を設定する場合は、[証明書からの OCSP URI を使用する (Use OCSP URI from Certificate)] ボタンを選択します。

ステップ4 [失効チェックを有効にする (Enable Revocation Check)] チェック ボックスをオンにします。

ステップ5 [チェック間隔 (Check Every)] フィールドに失効チェックの間隔を入力します。

ステップ6 [保存 (Save)] をクリックします。

ステップ7 これはオプションです。CTI、IPsecまたはLDAPリンクがある場合は、これらの長期性接続のOCSP失効サポートを有効にするために、上記の手順に加えて次の手順も行う必要があります。

- a) Cisco Unified CM の管理から、[システム (System)] > [エンタープライズ パラメータ (Enterprise Parameters)] を選択します。
 - b) [証明書の失効や有効期限 (Certificate Revocation and Expiry)] で、[証明書有効性チェック (Certificate Validity Check)] パラメーターを [True] に設定します。
 - c) [有効性チェック頻度 (Validity Check Frequency)] パラメーターの値を設定します。
(注) 証明書失効ウィンドウの [失効チェックを有効にする (Enable Revocation Check)] パラメーターの間隔値は、[有効性チェック頻度 (Validity Check Frequency)] エンタープライズ パラメーターの値よりも優先されます。
 - d) [保存 (Save)] をクリックします。
-



第 12 章

セキュリティ設定の構成

- [セキュリティの概要 \(175 ページ\)](#)
- [セキュリティ設定構成のタスク フロー \(175 ページ\)](#)

セキュリティの概要

この章では、IM and Presence サービスでセキュリティ設定を行う手順について説明します。IM and Presence サービスでは、安全な TLS 接続を設定し、FIPS モードなどの拡張セキュリティ設定を有効にできます。

IM and Presence サービスは Cisco Unified Communications Manager とプラットフォームを共有します。Cisco Unified Communications Manager でのセキュリティの設定手順については、*Security Guide for Cisco Unified Communications Manager*を参照してください。

セキュリティ設定構成のタスク フロー

これらのオプションのタスクを完了して、IM and Presence サービスのセキュリティを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	ログイン バナーの作成 (176 ページ)	ユーザが IM and Presence サービス インターフェイスへのログイン時に確認する必要があるログインバナーを作成します。
ステップ 2	安全な XMPP 接続の設定 (177 ページ)	XMPP セキュリティを設定するためにこれらのタスクを完了して下さい。
ステップ 3	TLS ピア サブジェクトの設定 (178 ページ)	TLS ピアを設定したい場合は、これらのタスクを設定してください。

	コマンドまたはアクション	目的
ステップ 4	TLS コンテキストの設定 (178 ページ)	TLS ピアに TLS コンテキストと TLS 暗号を設定します。
ステップ 5	FIPS モード (179 ページ)	展開を FIPS 準拠にしたい場合は、FIPS モードを有効にできます。セキュリティを強化するために、拡張セキュリティモードと共通コンプライアンスモードを有効にすることもできます。

ログインバナーの作成

ユーザが IM and Presence サービス インターフェイスへのログインの一部として確認するバナーを作成できます。任意のテキストエディタを使用して .txt ファイルを作成し、ユーザに対する重要な通知を含め、そのファイルを Cisco Unified IM and Presence OS の管理ページにアップロードします。

このバナーはすべての IM and Presence サービス インターフェイスに表示され、法的な警告や義務などの重要な情報をログインする前にユーザに通知します。Cisco Unified CM IM and Presence の管理、Cisco Unified IM and Presence オペレーティング システムの管理、Cisco Unified IM and Presence のサービスアビリティ、Cisco Unified IM and Presence のレポート、および IM and Presence のディザスタリカバリ システムのインターフェースでは、このバナーがユーザがログインする前後に表示されます。

手順

-
- ステップ 1 バナーに表示する内容を含む .txt ファイルを作成します。
 - ステップ 2 Cisco Unified IM and Presence オペレーティング システムの管理にサインインします。
 - ステップ 3 [ソフトウェア アップグレード (Software Upgrades)] > [ログイン メッセージのカスタマイズ (Customized Logon Message)] を選択します。
 - ステップ 4 [参照 (Browse)] を選択し .txt ファイルを検索します。
 - ステップ 5 [ファイルのアップロード (Upload File)] をクリックします。

バナーは、ほとんどの IM and Presence サービス インターフェイスでログインの前後に表示されます。

(注) .txt ファイルは、各 IM and Presence サービス ノードに個別にアップロードする必要があります。

安全な XMPP 接続の設定

TLS を使用して安全な XMPP 接続を有効にするには、この手順を使用してください。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] から、[システム (System)] > [セキュリティ (Security)] > [設定 (Settings)] を選択します。

ステップ 2 適切なチェックボックスをオンにして、次の XMPP セキュリティ設定を有効にします。

表 18: IM and Presence Service での XMPP セキュリティの設定

設定	説明
Enable XMPP Client To IM/P Service Secure Mode (XMPP クライアントと IM/P サービス間のセキュアモードの有効化)	有効な場合は、IM and Presence サービスはクラスタ内の XMPP クライアントアプリケーションにセキュアな TLS 接続を確立します。 この設定はデフォルトでは有効になっています。このセキュアモードをオフにしないことを推奨します。ただし、XMPP クライアントアプリケーションが非セキュアモードでクライアントログインクレデンシャルを保護できる場合を除きます。セキュアモードをオフにする場合は、他の方法で XMPP のクライアントツーノード通信を保護できることを確認してください。
Enable XMPP Router-to-Router Secure Mode (XMPP ルータ ツールータセキュアモードの有効化)	この設定をオンにすると、IM and Presence サービスは同じクラスタ内または別のクラスタ内の XMPP ルータ間にセキュアな TLS 接続を確立します。IM and Presence サービスは XMPP 証明書を XMPP 信頼証明書として自動的にクラスタ内またはクラスタ間で複製します。XMPP ルータは、同じクラスタ内または別のクラスタ内にある他の XMPP ルータとの TLS 接続を確立しようとし、TLS 接続の確立に使用できます。
Enable Web Client to IM/P Service Secure Mode (Web クライアントと IM/P サービス間のセキュアモードの有効化)	この設定をオンにすると、IM and Presence サービスは、IM and Presence サービスノードと XMPP ベースの API クライアントアプリケーション間のセキュアな TLS 接続を確立します。この設定をオンにした場合は、IM and Presence サービスの <code>cup-xmpp-trust</code> リポジトリに Web クライアントの証明書または署名付き証明書をアップロードします。

ステップ 3 [保存 (Save)] をクリックします。

次のタスク

[XMPP クライアント ツー IM/P サービスのセキュアモードを有効にする (Enable XMPP Client To IM/P Service Secure Mode)] 設定を更新した場合は、Cisco XCP Connection Manager を再起動します。

IM and Presence Service での SIP セキュリティの設定

TLS ピア サブジェクトの設定

IM and Presence サービス証明書をインポートすると、IM and Presence サービスは自動的に TLS ピア サブジェクトを TLS ピア サブジェクト リストおよび TLS コンテキスト リストに追加しようとします。要件に合わせて TLS ピア サブジェクトおよび TLS コンテキストが設定されていることを確認します。

手順

- ステップ 1 Cisco Unified CM IM and Presence Administration で、[システム (System)] > [セキュリティ (Security)] > [TLS ピア サブジェクト (TLS Peer Subjects)] を選択します。
- ステップ 2 [新規追加 (Add New)] をクリックします。
- ステップ 3 ピア サブジェクト名に対して次の手順のいずれかを実行します。
 - a) ノードが提示する証明書のサブジェクト CN を入力します。
 - b) 証明書を開き、CN を探してここに貼り付けます。
- ステップ 4 [説明 (Description)] フィールドにノードの名前を入力します。
- ステップ 5 [保存 (Save)] をクリックします。

次のタスク

TLS コンテキストを設定します。

TLS コンテキストの設定

この手順を使用して、TLS コンテキストと TLS 暗号を TLS ピア サブジェクトに割り当てます。



- (注) IM and Presence サービス証明書をインポートすると、IM and Presence サービスは自動的に TLS ピア サブジェクトを TLS ピア サブジェクト リストおよび TLS コンテキスト リストに追加しようとします。

始める前に

[TLS ピア サブジェクトの設定 \(178 ページ\)](#)

手順

-
- ステップ 1** Cisco Unified CM IM and Presence Administrationで、[システム (System)] > [セキュリティ (Security)] > [TLS コンテキスト設定 (TLS Context Configuration)] に移動します。
- ステップ 2** [検索 (Find)] をクリックします。
- ステップ 3** [Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context] を選択します。
- ステップ 4** 使用可能な TLS ピア サブジェクトのリストから、設定した TLS ピア サブジェクトを選択します。
- ステップ 5** > をクリックして、この TLS ピア サブジェクトを [選択された TLS ピア サブジェクト (Selected TLS Peer Subjects)] に移動します。
- ステップ 6** TLS 暗号のマッピングオプションの設定：
- 利用可能な TLS 暗号そして選択された TLS 暗号ボックスで利用可能な TLS 暗号のリストを確認します。
 - 現在選択されていない TLS 暗号を有効にしたい場合は、> 矢印を使用して暗号を選択された TLS 暗号に移動します。
- ステップ 7** [保存 (Save)] をクリックします。
- ステップ 8** Cisco SIP プロキシ サービスを再起動します。
- [Cisco Unified IM and Presenceのサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-機能サービス (Control Center - Feature Services)] を選択します。
 - [サーバ (Server)] ドロップダウンリストから [IM and Presence Service] ノードを選択し、[移動 (Go)] をクリックします。
 - Cisco SIP Proxy サービスを選択して[再起動 (Restart)] をクリックします。
-

FIPSモード

IM and Presence Serviceには、一連の拡張システムセキュリティモードが含まれています。この機能を使用すると、暗号化、データとシグナリング、および監査ログなどのアイテムを対象とした、より厳格なセキュリティガイドラインおよびリスク管理制御下でシステムが動作します。

- FIPS モード：IM and Presence サービスは FIPS モードで動作するように設定できます。これにより、システムは FIPS または米国およびカナダの政府標準の暗号化モジュール規格に準拠できます。
- 拡張セキュリティモード-拡張セキュリティモードは FIPS 対応システム上で動作し、データ暗号化要件、厳格な認証情報ポリシー、連絡先検索のためのユーザー認証、厳格な監査ログ要件などの追加のリスク管理制御を提供します。

- 共通基準モード：共通基準モードは、FIPS 対応システム上でも、システムを TLS や x.509 v3 証明書の使用などの一般的な基準ガイドラインに準拠するための追加制御機能を提供します。



(注) 外部データベースが MSSQL の場合、メッセージアーカイバ、テキスト会議マネージャ、ファイル転送マネージャなどのサービスをコモンクライトリア モードで動作させるには、次の手順を実行する必要があります。

1. MSSQL データベースをホストしているサーバで、TLS 1.1 以降をサポートするように設定します。
2. IM and Presence Service にデータベース証明書を再アップロードします。
3. [外部データベースの設定 (Enable SSL)] ページの [SSLの有効化 (Enable SSL)] チェックボックスをオンにします。[Cisco Unified CM IM and Presenceの管理 (Cisco Unified CM IM and Presence Administration)] > [メッセージ (Messaging)] > [外部サーバの設定 (External Server Setup)] > [外部データベース (External Databases)] を選択して、外部データベースを設定します。

FIPS モード、拡張セキュリティモード、共通基準モードを Cisco Unified Communications Manager および IM and Presence Service で有効にする方法は、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html> の *Cisco Unified Communications Manager セキュリティ ガイド* の、「FIPS モードの設定」の章を参照してください。

FIPS の Microsoft Outlook カレンダー統合

IM and Cisco Presence Service サーバで FIPS モードを有効にすると、Exchange Web サービス情報を取得するためにサポートされるのは NTLMv2 だけになります。FIPS モードが無効の場合は、既存の動作と同様に NTLMv1 と NTLMv2 の両方がサポートされます。基本認証は、FIPS モードが有効か無効かにかかわらず、どちらの場合にもサポートされます。

Presence Engine サービスには、[FIPSモードのExchange Server認証 (FIPS Mode Exchange Server Authentication)] という新しいサービスパラメータが導入されています。これにより、Microsoft Outlook カレンダー統合機能を通じて Exchange Server との接続を確立するときに Presence Engine で使用される認証の種類を確認できます。

[FIPSモードのExchange Server認証 (FIPS Mode Exchange Server Authentication)] サービスパラメータは、[自動 (Auto)] または [基本のみ (Basic Only)] に設定できます。

サービスパラメータを [自動 (Auto)] に設定した場合：Presence Engine は最初に NTLMv2 をネゴシエートし、NTLMv2 ネゴシエーションが失敗した場合にのみ「基本認証」にフォールバックします。FIPS モードでは NTLMv1 はネゴシエートされません。

サービス パラメータを [基本のみ (Basic Only)] に設定した場合 : Exchange Server が NTLM と基本認証の両方を許可するように設定されている場合でも、Presence Engine は「基本認証」を使用するように強制されます。



(注) サービス パラメータ設定を変更した場合は、Cisco Presence Engine を再起動する必要があります。



第 13 章

クラスタ間ピアの設定

- クラスタ間ピアの概要 (183 ページ)
- クラスタ間ピアの前提条件 (183 ページ)
- クラスタ間ピアの設定のタスクフロー (184 ページ)
- クラスタ間ピアリングの連携動作と制限事項 (194 ページ)

クラスタ間ピアの概要

クラスタ間ピアにより、1つのクラスタ内のユーザが、同じドメイン内の異なるクラスタにいるユーザと通信したり、プレゼンスをサブスクライブしたりできます。大規模展開では、クラスタ間ピアリングを使用してリモート IM and Presence クラスタに接続できます。

クラスタ間ピアリングは、ローカルクラスタとリモートクラスタの両方のデータベースパブリッシュャノードで設定されます。

クラスタ間配置のサイズ設定とパフォーマンスの推奨事項については、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html#48016でCisco コラボレーションシステムソリューションリファレンスネットワークデザイン (SRND) の「コラボレーションインスタントメッセージおよびプレゼンス」を参照してください。

クラスタ間ピアの前提条件

ネットワークで IM and Presence Service クラスタ間ピアを設定する前に、次の点に注意してください。

- 必要に応じて全クラスタのシステム トポロジを設定し、ユーザを割り当てます。
- クラスタ間ピア接続が正常に機能するには、2つのクラスタ間にファイアウォールがある場合、次のポートが開いたままになっている必要があります。
 - 8443 (AXL)
 - 7400 (XMPP)
 - 5060 (SIP) (SIP フェデレーション使用時のみ)

- クラスタ間環境では、最小限の OVA を 15,000 ユーザに導入することを推奨します。すべてのクラスタが少なくとも 15,000 ユーザが OVA を実行している限り、複数のクラスタを異なる OVA のサイズで実行することが可能です。



(注) クラスタ間ピアリングは、Cisco Business Edition 6000 サーバに IM and Presence サービスが導入されている場合はサポートされません。

クラスタ間ピアの設定のタスクフロー

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザプロビジョニングを確認する (185 ページ)	クラスタ間ピアを設定する前に、エンドユーザが正しくプロビジョニングされていることを確認してください。
ステップ 2	Cisco AXL Web サービスの有効化 (185 ページ)	Cisco AXL Web サービスは、すべてのローカルおよびリモートの IM and Presence ノードでアクティブになっている必要があります。この手順を使用して、サービスが実行されていることを確認してください。
ステップ 3	同期エージェントを有効にする (186 ページ)	各クラスタ間ピアのデータベースパブリッシャノードで同期エージェントを有効にします。
ステップ 4	クラスタ間ピアの設定 (187 ページ)	クラスタ間ピアを設定するには、各クラスタのデータベースパブリッシャノードでこの作業を実行します。
ステップ 5	Intercluster Sync Agent がオンであることを確認します。 (189 ページ)	Intercluster Sync Agent は、IM and Presence Service クラスタ内のすべてのノードで実行されている必要があります。Intercluster Sync Agent パラメータが実行されていることを確認するには、この手順を使用します。
ステップ 6	クラスタ間ピア ステータスの確認 (190 ページ)	クラスタ間ピア設定が機能することを確認します。

	コマンドまたはアクション	目的
ステップ 7	Intercluster Sync Agent の Tomcat 信頼証明書の更新 (191 ページ)	クラスタ間ピアの tomcat 証明書のステータスが同期されない場合は、Tomcat 信頼証明書を更新する必要があります。
ステップ 8	クラスタ間ピアの定期同期エラーからの自動リカバリを有効化 (191 ページ)	クラスタ間ピアの定期同期エラーからの自動リカバリを有効にするには、次の手順を使用します。
ステップ 9	クラスタ間ピアの同期間隔の設定 (192 ページ)	クラスタ間ピアの同期の時間間隔を設定するには、次の手順を使用します。
ステップ 10	クライアント間ピア定期同期の証明書同期の無効化 (193 ページ)	証明書同期の無効化/有効化を、ホスト間定期同期の一部として設定するには、次の手順を使用します。

ユーザプロビジョニングを確認する

この手順を使用して、クラスタ間ピアを設定する前にエンドユーザが正しくプロビジョニングされていることを確認します。

手順

-
- ステップ 1** Cisco Unified CM IM and Presence Administration から、**[診断 (Diagnostics)] > [システムトラブルシューター (System Troubleshooter)]** を選択します。
システムトラブルシューターが実行されます。
- ステップ 2** ユーザトラブルシューターセクションで、エンドユーザが正しくプロビジョニングされていること、および重複または無効なユーザがないことを確認します。
-

次のタスク

[Cisco AXL Web サービスの有効化 \(185 ページ\)](#)

Cisco AXL Web サービスの有効化

Cisco AXL Web サービスは、すべてのローカルとリモートの IM and Presence クラスタノードで実行されている必要があります。デフォルトにより、このサービスは実行されます。ただし、この手順を使用してサービスが実行されていることを確認できます。



- (注) Cisco AXL Web サービスを有効にすると、システムは AXL 権限を持つクラスタ間アプリケーションユーザを作成します。リモートの IM and Presence Service ノードでクラスタ間ピアを設定するには、クラスタ間アプリケーションユーザのユーザ名とパスワードが必要です。

手順

- ステップ 1** [Cisco Unified IM and Presenceのサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-機能サービス (Control Center - Feature Services)] を選択します。
- ステップ 2** [サーバ (Server)] リストから、サービスを再アクティブ化するノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3** [データベースおよび管理サービス (Database and Admin Services)] エリアで、[Cisco AXL Web サービス (Cisco AXL Web Service)] の[状態]を選択します。
- サービスが起動したら、アクションは不要です。
 - サービスが実行されていない場合は、サービスを選択して[再起動 (Restart)] をクリックします。
- ステップ 4** ローカルクラスタとリモートクラスタのすべてのクラスタノードでこの手順を繰り返します。

次のタスク

[同期エージェントを有効にする \(186 ページ\)](#)

同期エージェントを有効にする

Cisco Sync Agent は、ローカルおよびリモートの各クラスタ間ピアのデータベースパブリッシャノードで実行している必要があります IM and Presence データベースパブリッシャノード。

手順

- ステップ 1** [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
- ステップ 2** [サーバ (Server)] ドロップダウンリスト ボックスから、IM and Presence データベースパブリッシャノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3** IM and Presence サービスで、Cisco Sync Agent ステータスが実行中であることを確認します。
- ステップ 4** サービスが実行されていない場合は、サービスを選択して[再起動 (Restart)] をクリックします。

ステップ5 クラスタ内ごとに、この手順を繰り返します。

次のタスク

Cisco Sync Agent が Cisco Unified Communications Manager からのユーザ同期を完了した後、[クラスタ間ピアの設定 \(187 ページ\)](#)

クラスタ間ピアの設定

ローカルクラスタとリモートクラスタの両方のデータベースパブリッシャノードでこの手順を使用して、クラスタ間ピア関係を設定します。

始める前に

- Sync Agent がローカルクラスタとリモートクラスタのCisco Unified Communications Manager からのユーザ同期化を完了したことを確認します。Sync Agent がユーザの同期化を完了する前にクラスタ間ピア接続を設定した場合は、クラスタ間ピア接続のステータスは**失敗**として表示されます。
- リモートの IM and Presence サービス ノードのクラスタ間アプリケーションユーザの AXL ユーザ名とパスワードを取得していることを確認します。

手順

- ステップ1** [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[**プレゼンス (Presence)**] > [**クラスタ間 (Inter-Clustering)**] を選択します。
- ステップ2** [新規追加 (Add New)] をクリックします。
- ステップ3** [**ピアアドレス (Peer address)**] フィールドに、リモートクラスタのデータベースパブリッシャノードのノード名を入力します。このフィールドは IP アドレス、ホスト名、または FQDN ですが、サーバを定義する実際のノード名と一致している必要があります。

(注) ・ノード名が使用するアドレスのタイプを確認するには、リモートクラスタ上の Cisco Unified CM IM and Presence 管理にログインして、**システム > プレゼンス トポロジ**を選択します。このウィンドウには、各クラスタノードのノード名およびサーバの詳細が表示されます。

・マルチクラスタ環境の一部のクラスタでは、スプリットブレイン現象が発生する場合があります。たとえば、クラスタ A があった場合、マルチクラスタのピアはクラスタ B、C、D、および E があるとします。クラスタ A 内のノードは、スプリットブレイン現象の際に、マルチクラスタ環境の他のクラスタ B、C、D、E と通信する必要があるため、スプリットブレイン現象の発生中に DNS にアクセス可能である必要があります。

スプリットブレイン現象が発生して、クラスタ A のノードが DNS にアクセスできない場合、A、B、C、D、および E クラスタノードの IP アドレスは、ホスト名と FQDN ではなく、ノード名として設定する必要があります。

クラスタ A、B、C、および E のノードが FQDN またはホスト名を使用して定義されていると、スプリットブレイン現象が発生して DNS にアクセスできない場合、IM Presence 情報が失われたり、クラスタ A と B、C、D、E 間での IM 履歴が失われたりするなど、サービス障害が発生します。

ステップ 4 AXL クレデンシャルの入力

ステップ 5 SIP 通信の優先プロトコルを入力します。

(注) すべての IM and Presence サービスクラスタのクラスタ間トランク転送として **TCP** (デフォルト設定) を使用することを推奨します。この設定がネットワーク構成とセキュリティのニーズに合っている場合は、この設定を変更できます。

ステップ 6 [保存 (Save)] をクリックします。

ステップ 7 GUI ヘッダーの右上にある通知を確認します。Cisco XCP ルータを再起動するように通知された場合、次の操作を行います。それ以外の場合は、このステップを省略できます。

- a) [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
- b) [サーバ (Server)] ドロップリストボックスから、IM and Presence ノードを選択して、[移動 (Go)] をクリックします。
- c) [Cisco XCP Router] を選択し、[リスタート (Restart)] をクリックします。
- d) 全クラスタ ノードで上記の手順を繰り返します。

ステップ 8 各リモートピアクラスタのデータベースパブリッシャノードでこの手順を繰り返します。

ヒント クラスタ間転送プロトコルとして **TLS** を選択する場合は、**IM and Presence** サービスは、クラスタ間ピアの間で証明書を自動的に交換して、セキュアな TLS 接続を確立しようとしています。**IM and Presence** サービスは、証明書交換がクラスタ間ピアのステータスのセクションで正常に行われるかどうかを示します。

次のタスク

[Intercluster Sync Agent がオンであることを確認します。](#) (189 ページ)

XCP ルータ サービスを再起動します。

ローカルクラスタ内のすべてのノードで Cisco XCP Router サービスを再起動します。リモートクラスタの全ノードでも同様にします。

始める前に

[クラスタ間ピアの設定](#) (187 ページ)

手順

-
- ステップ 1** [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
 - ステップ 2** [サーバ (Server)] リストから、サービスを再アクティブ化するノードを選択し、[移動 (Go)] をクリックします。
 - ステップ 3** [IM and Presence サービス (IM and Presence Services)] 領域で、[Cisco XCP Router] を選択します。
 - ステップ 4** [再起動 (Restart)] をクリックします。

次のタスク

[Intercluster Sync Agent がオンであることを確認します。](#) (189 ページ)

Intercluster Sync Agent がオンであることを確認します。

クラスタ間同期エージェントネットワークサービスは、クラスタ間ピア間でユーザ情報を同期します。この手順を使用して、各クラスタ間ピアのすべてのクラスタノードでサービスが実行されていることを確認します。

手順

-
- ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)]>[コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
 - ステップ 2 [サーバ (Server)] メニューから、IM and Presence サービス ノードを選択し、[移動 (Go)] をクリックします。
 - ステップ 3 Cisco クラスタ間同期エージェントが実行ステータスを表示していることを確認します。
 - ステップ 4 サービスが実行されていない場合は、サービスを選択して[起動 (Start)] をクリックします。
 - ステップ 5 各クラスタ間ピアの全クラスタ ノードに対してこの手順を繰り返します。
-

次のタスク

[クラスタ間ピアステータスの確認 \(190 ページ\)](#)

クラスタ間ピアステータスの確認

この手順を使用して、クラスタ間ピア設定が正しく機能していることを確認します。

手順

-
- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[プレゼンス (Presence)]>[クラスタ間 (Inter-Clustering)] を選択します。
 - ステップ 2 検索条件メニューからピアアドレスを選択します。
 - ステップ 3 [検索 (Find)] をクリックします。
 - ステップ 4 [クラスタ間ピアステータス (Inter-cluster Peer Status)] ウィンドウで次の操作を実行します。
 - a) クラスタ間ピアの各結果エントリの横にチェック マークがあることを確認します。
 - b) [関連ユーザ (Associated Users)] の値がリモートクラスタのユーザ数と等しいことを確認します。
 - c) クラスタ間転送プロトコルとして TLS を選択した場合は、[証明書のステータス (Certificate Status)] 項目に TLS 接続のステータスが表示され、IM and Presence Service が正常にクラスタ間でセキュリティ証明書を交換したかが示されます。証明書が同期されない場合は、(このモジュールで説明されているように) 手動で Tomcat 信頼証明書を更新する必要があります。その他の証明書交換エラーについては、オンラインヘルプで推奨処置を確認してください。
 - ステップ 5 システムトラブルシューターを実行します。
 - a) Cisco Unified CM IM and Presence Administration から、[診断 (Diagnostics)]>[システムトラブルシューター (System Troubleshooter)] を選択します。

- b) [クラスタ間トラブルシュータ (Inter-Clustering Troubleshooter)] セクションで、各クラスタ間ピア接続エントリのステータスの横にチェック マークがあることを確認します。

次のタスク

[Intercluster Sync Agent の Tomcat 信頼証明書の更新 \(191 ページ\)](#)

Intercluster Sync Agent の Tomcat 信頼証明書の更新

接続エラーがローカル クラスタで発生した場合、および「破損した」Tomcat 信頼証明書がリモート クラスタに関連付けられている場合、この手順を使用して Tomcat 信頼証明書を更新します。

クラスタ間ピアの tomcat 証明書のステータスが同期されない場合は、Tomcat 信頼証明書を更新する必要があります。クラスタ間展開では、新しいリモート クラスタを指すように既存のクラスタ間ピア設定を再利用する場合にこのエラーが発生します。このエラーは、初めて IM and Presence をインストールしたとき、または IM and Presence Service のホスト名またはドメイン名を変更した場合、あるいは Tomcat 証明書を再生成した場合にも発生することがあります。

手順

-
- ステップ 1** [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[プレゼンス (Presence)] > [クラスタ間 (Inter-Clustering)] を選択します。
- ステップ 2** リモート クラスタと証明書を同期するには、[強制同期 (Force Sync)] を選択します。
- ステップ 3** 表示される確認ウィンドウで、[ピアの Tomcat 証明書も再同期 (Also resync peer's Tomcat certificates)] を選択します。
- ステップ 4** [OK] をクリックします。

(注) 自動的に同期していない証明書がある場合は、[Intercluster Peer Configuration] ウィンドウに進みます。X でマークされた証明書はすべて、不足している証明書であり、手動でコピーする必要があります。

クラスタ間ピアの定期同期エラーからの自動リカバリを有効化

Cisco Intercluster Sync Agent が「InterClusterSyncAgentPeerPeriodicSyncingFailure」アラームを発生させ、Intercluster ピアの定期的な同期が 2 時間を超えた場合に自動的に再起動するようにするには、この手順を使用してこのサービスパラメータを有効にします。

手順

-
- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。
- ステップ 2 [サーバ (Server)] リストから、「Intercluster Sync Agent の一般的なパラメータ」を設定する IM and Presence ノードを選択します。
- ステップ 3 サービスリストから、**Cisco Intercluster Sync Agent(Active)**を選択します。
- ステップ 4 をセットするクラスタ間ピアの定期同期エラーに対する自動回復を有効にするサービスパラメータ有効にします。
- ステップ 5 [保存 (Save)] をクリックします。

(注) あれば「クラスタ間ピア定期同期エラーに対する自動回復を有効にする」 service パラメータが Enabled に設定されており、定期的な同期が 2 時間を超えて停止した場合

- **InterClusterSyncAgentPeerPeriodicSyncingFailure** アラームが発生します。
- **Cisco** クラスタ間同期エージェントサービスは自動的に再開されます。

「クラスタ間ピア定期同期エラーの自動回復を有効にする」が無効になっている場合は、

- **InterClusterSyncAgentPeerPeriodicSyncingFailure** アラームが発生します。
 - **Cisco** クラスタ間同期エージェント サービスは自動的に再開されません。
-

クラスタ間ピアの同期間隔の設定

クラスタ間ピアの同期の時間間隔を設定するには、次の手順を使用します。サービスパラメータ [クラスタ間ピアの定期同期間隔 (分) (Inter Cluster Peer Periodic Sync Interval (mins))] を使用すると、ダイナミック ICSA の定期同期の時間間隔を設定できます。クラスタ間ピアの同期間隔のデフォルト設定は 30 分です。

手順

-
- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。
- ステップ 2 [サーバ (Server)] リストから、「Intercluster Sync Agent の一般的なパラメータ」を設定する IM and Presence ノードを選択します。
- ステップ 3 サービスリストから、**Cisco Intercluster Sync Agent(Active)**を選択します。
- ステップ 4 [クラスタ間ピアの定期同期間隔 (分) (Inter Cluster Peer Periodic Sync Interval (mins))] サービスパラメータを適切な間隔に設定します。指定範囲は 30 ~ 1444 分で、デフォルトは 30 分です。

ステップ5 [保存 (Save)] をクリックします。

(注) 新しい設定は、次のクラスタ間同期の実行時から有効になります。

クラスタ間ピアの同期に失敗すると、Cisco Intercluster Sync Agent サービスは同期間隔を4回完了した後に再起動します。たとえば、このパラメータが40分に設定されている場合、サービスは160分(4*40)後に再起動します。

クライアント間ピア定期同期の証明書同期の無効化

証明書同期を、証明書間同期プロセスの一部として無効にするには、次の手順を使用します。クラスタ間定期同期中のサービスパラメータ証明書同期では、管理者がクラスタ間定期同期の一部として証明書同期を無効または有効にできます。このサービスパラメータのデフォルト値は、証明書同期の実行 (Perform certificate sync) です。

手順

ステップ1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。

ステップ2 [サーバ (Server)] リストから、Intercluster Sync Agent の一般的なパラメータを設定する IM and Presence ノードを選択します。

ステップ3 サービスリストから、Cisco Intercluster Sync Agent(Active)を選択します。

ステップ4 クラスタ間定期同期中にサービスパラメータの証明書同期を [証明書同期を実行しない (Do not perform certificate sync)] に設定します。

ステップ5 [保存 (Save)] をクリックします。

(注) 展開環境で、証明書の同期に関連する、証明書の定期同期中にパフォーマンスの低下またはCPU使用率の増加が発生した場合は、次の手順を使用してサービスパラメータを設定できます。

クラスタ間ピア接続の削除

クラスタ間ピア関係を削除する場合は、この手順を使用します。

手順

ステップ1 IM and Presence サービスのデータベース パブリッシャ ノードにログインします。

ステップ2 Cisco Unified CM IM and Presence 管理で、プレゼンス(Presence) > クラスタ間(Inter-Clustering) を選択します。

ステップ 3 [検索(Find)]をクリックし、削除するクラスタ間ピアを選択します。

ステップ 4 [削除 (Delete)]をクリックします。

ステップ 5 ピア クラスタでこれらの手順を繰り返します。

(注) IM and Presence サービスが拡張され、クラスタ間ピアを削除した後、IM and Presence クラスタ内の各ノードで XCP ルータが再起動されるのを防ぐためです。この機能拡張により、管理者はノードのシーケンシャル再起動によるオーバーヘッドを大幅に軽減し、Jabber サービスを停止することで、大規模クラスタを効果的に管理できます。

クラスタ間ピアリングの連携動作と制限事項

機能	連携動作と制限事項
Cisco Business Edition 6000	クラスタ間ピアリングは、Cisco Business Edition 6000 サーバに IM and Presence サービスが導入されている場合はサポートされません。
クラスタ制限 (Cluster Limit)	クラスタ間ピアリングを使用すると、クラスタ間メッシュに最大 30 個の IM and Presence サービス クラスタをデプロイできます。
マルチクラスタ展開でのクラスタ間同期エージェントのリソース不足	<p>ICSA では、多数のクラスタを持つマルチクラスタ展開では、より多くのリソースが必要になります。リソース不足のため、ICSA または SRM に関する問題に直面した場合に備えて次に示す Cisco SIP プロキシ サービス パラメータをデフォルト値の 20 から 10 の新しい値に変更することをお勧めします。</p> <ul style="list-style-type: none"> • 最大プロセス数 • 最大スベアプロセス数 • 最大プロセス数 <p>変更を有効にするには、SIP プロキシ サービスを再起動します。</p> <p>SRM および ICSA サービスを再起動します。</p>



第 14 章

プッシュ通知の設定

- [プッシュ通知の概要 \(195 ページ\)](#)
- [プッシュ通知設定 \(199 ページ\)](#)

プッシュ通知の概要

クラスタでプッシュ通知が有効になっている場合、および IM and Presence Service は、サスペンドモード（バックグラウンドモードとも呼ばれます）で動作している Android および iOS 用 Cisco Jabber または Cisco Webex クライアントに音声通話、ビデオ通話、インスタントメッセージの通知をプッシュするために、Google と Apple のクラウドベースのプッシュ通知サービスを使用します。プッシュ通知によって、システムは Cisco Jabber または Cisco Webex と永続的な通信を維持できます。プッシュ通知は、エンタープライズネットワーク内から接続する Android および iOS 用 Cisco Jabber および Cisco Webex クライアントと、Expressway のモバイルおよびリモートアクセス機能を通じてオンプレミス展開に登録するクライアントの両方で必要となります。

プッシュ通知の動作

Android および iOS プラットフォームデバイスにインストールされているクライアントは、起動時に、IM and Presence Service、および Google と Apple のクラウドに登録します。モバイルおよびリモートアクセスの展開では、クライアントは Expressway 経由でオンプレミスサーバに登録します。Cisco Jabber および Cisco Webex クライアントがフォアグラウンドモードになっている限り、および IM and Presence Service は、コールとインスタントメッセージをクライアントに直接送信することができます。

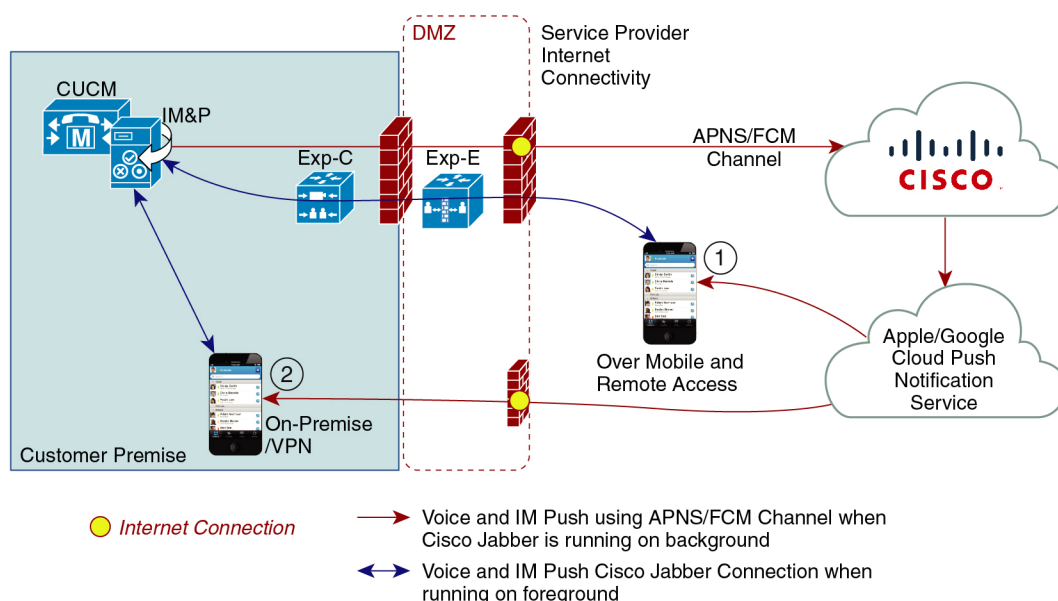
ただし、Cisco Jabber または Cisco Webex クライアントが（たとえばバッテリー寿命を長持ちさせるために）サスペンドモードに移行すると、標準の通信チャンネルは使用不可となり、および IM and Presence Service がクライアントと直接通信することはできなくなります。プッシュ通知は、パートナークラウドを介してクライアントに到達するための別のチャンネルを提供します。



(注) 次のいずれかの条件が当てはまる場合、Cisco Jabber および Cisco Webex は保留モードで動作しているとみなされます。

- Cisco Jabber または Cisco Webex アプリケーションがオフスクリーンで（つまりバックグラウンドで）実行されている
- Android または iOS デバイスがロックされている
- Android または iOS デバイスの画面がオフになっている

図 6: プッシュ通知のアーキテクチャ



449023

上の図は、Android および iOS 用 Cisco Jabber または Cisco Webex クライアントが、バックグラウンドで動作している場合と停止している場合の動作を示したものです。この図では、(1) クライアントが Expressway 経由でオンプレミスの Cisco Unified Communications Manager および IM and Presence Service 展開に接続するも展開と、(2) エンタープライズネットワーク内からオンプレミス展開に直接接続する Android および iOS 用 Cisco Jabber または Cisco Webex Teams クライアントを示しています。



(注) iOS13 の Apple クライアントおよびサポートされている Android クライアントでは、音声通話とメッセージは別々のプッシュ通知チャネル（「VoIP」と「Message」）を使用して、バックグラウンドモードで動作しているクライアントに到達します。ただし、全般的なフローはどちらのチャネルでも同じです。iOS 12では、音声通話とメッセージは同じチャネルを使用して配信されます。

Cisco Jabber および Cisco Webex のプッシュ通知の動作

次の表は、 および IM and Presence Service に登録された Cisco Jabber または Cisco Webex iOS クライアントの、iOS 12 および iOS 13 での動作を説明したものです。

Cisco Jabber または Cisco Webex クライアントの動作モード	Cisco Jabber が iOS12 デバイスで実行されている場合	Cisco Jabber が iOS13 デバイスまたは Android デバイスで実行されている場合
フォアグラウンドモード	<p>音声/ビデオ通話</p> <p>標準の SIP 通信チャネルを使用して、音声通話とビデオ通話を Cisco Jabber または Cisco Webex Teams クライアントに直接送信します。</p> <p>通話の場合、はプッシュ通知もフォアグラウンドモードの Cisco Jabber または Cisco Webex クライアントに送信します。ただし、通話の確立には、プッシュ通知チャネルではなく標準の SIP チャネルが使用されます。</p> <p>メッセージ</p> <p>IM and Presence Service は、標準の SIP 通信チャネルを使用してメッセージをクライアントに直接送信します。メッセージの場合、フォアグラウンドモードのクライアントにプッシュ通知は送信されません。</p>	動作は iOS12 の場合と同じです。

Cisco Jabber または Cisco Webex クライアントの動作モード	Cisco Jabber が iOS12 デバイスで実行されている場合	Cisco Jabber が iOS13 デバイスまたは Android デバイスで実行されている場合
<p>サスペンドモード (バックグラウンドモード)</p>	<p>音声コールまたはビデオ通話</p> <p>標準の通信チャンネルは使用できません。Unified CM はプッシュ通知チャンネルを使用します。</p> <p>通知を受信すると、Cisco Jabber または Cisco Webex クライアントは自動的にフォアグラウンドモードに戻り、クライアントが呼出音を鳴らします。</p> <p>メッセージング</p> <p>標準の通信チャンネルは使用できません。IM and Presence サービスはプッシュ通知チャンネルを使用して、次のように IM 通知を送信します。</p> <ol style="list-style-type: none"> 1. IM and Presence サービスは、シスコクラウドのプッシュ REST サービスに IM 通知を送信し、その後通知は Apple クラウドに転送されます。 2. Apple クラウドは Cisco Jabber または Cisco Webex クライアントに IM 通知をプッシュし、Cisco Jabber または Cisco Webex クライアントに通知が表示されます。 3. ユーザが通知をクリックすると、Cisco Jabber または Cisco Webex クライアントは再びフォアグラウンドに移行します。Cisco Jabber または Cisco Webex クライアントは、IM and Presence Service とのセッションを再開し、インスタントメッセージをダウンロードします。 <p>(注) Cisco Jabber または Cisco Webex クライアントがサスペンドモードの間、ユーザのプレゼンスステータスは「退席中」と表示されます。</p>	<p>iOS13 では、コールトラフィックとメッセージトラフィックは別々のプッシュ通知チャンネルに分けられます。コールには「VoIP」チャンネル、メッセージングには「Message」チャンネルが使用されます。</p> <p>音声コールまたはビデオ通話</p> <p>標準の通信チャンネルは使用できません。Unified CM は「VoIP」プッシュ通知チャンネルを使用します。</p> <p>VoIP 通知を受け取ると、Jabber は発信者 ID を使用して CallKit を起動します。</p> <p>この動作は、Cisco Jabber または Cisco Webex iOS クライアントに適用されません。</p> <p>メッセージング</p> <p>標準の通信チャンネルは使用できません。IM and Presence Service は、「Message」プッシュ通知チャンネルを使用します。</p> <ol style="list-style-type: none"> 1. IM and Presence サービスは、シスコクラウドのプッシュ REST サービスに IM 通知を送信し、その後通知は Apple クラウドに転送されます。 2. Apple クラウドは、Cisco Jabber または Cisco Webex クライアントに IM 通知をプッシュします。 3. ユーザが通知をクリックすると、Cisco Jabber または Cisco Webex クライアントはフォアグラウンドモードに移行します。Cisco Jabber または Cisco Webex クライアントは、IM and Presence Service とのセッションを再開し、メッセージをダウンロードします。 <p>(注) Cisco Jabber または Cisco Webex クライアントがサスペンドモードの間、ユーザのプレゼンスは「退席中」と表示されます。</p>

プッシュ通知がサポートされるクライアント

クライアント	OS	プラットフォームクラウド	クラウドサービス
iPhone および iPad の Cisco Jabber	iOS	Apple 社	Apple プッシュ通知サービス (APNS)
Android の Cisco Jabber	Android	Google	Android PNS サービス
iOS の Webex	iOS	Apple 社	Apple プッシュ通知サービス (APNS)
Android の Webex	Android	Google	Android PNS サービス

プッシュ通知設定

プッシュ通知を設定および展開する方法の詳細については、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>で*iPhone* および *iPad* での *Cisco Jabber* へのプッシュ通知の配置を参照してください。



第 III 部

機能の設定

- [アベイラビリティとインスタントメッセージの設定 \(203 ページ\)](#)
- [アドホック チャットおよび常設チャットの設定 \(209 ページ\)](#)
- [常設チャットの高可用性の設定 \(225 ページ\)](#)
- [マネージドファイル転送の設定 \(239 ページ\)](#)
- [複数のデバイスのメッセージングの設定 \(259 ページ\)](#)
- [エンタープライズグループの設定 \(269 ページ\)](#)
- [ブランディングのカスタマイズ \(283 ページ\)](#)
- [高度な機能の設定 \(291 ページ\)](#)



第 15 章

アベイラビリティとインスタントメッセージの設定

- [アベイラビリティとインスタントメッセージの概要 \(203 ページ\)](#)
- [アベイラビリティとインスタントメッセージの前提条件 \(204 ページ\)](#)
- [アベイラビリティとインスタントメッセージのタスクフロー \(205 ページ\)](#)
- [可用性およびインスタントメッセージングの相互作用および制限 \(207 ページ\)](#)

アベイラビリティとインスタントメッセージの概要

IM and Presence Service を使用すると、ユーザは自分の在席ステータスを連絡先と共有できます。

ポイントツーポイント インスタント メッセージは、一度に 2 人のユーザ間のリアルタイム会話をサポートします。IM and Presence Service は、送信者から受信者へのユーザ間のメッセージを直接交換します。ポイントツーポイントのインスタントメッセージを交換するには、ユーザはインスタントメッセージクライアントでオンラインになっている必要があります。

インスタントメッセージング機能は次のとおりです。

インスタントメッセージの分岐

複数のインスタントメッセージクライアントにログインしている連絡先にユーザがインスタントメッセージを送信すると、IM and Presence サービスは各クライアントにインスタントメッセージを配信します。IM and Presence Service は、連絡先が応答するまでインスタントメッセージを各クライアントに分岐し続けます。連絡先が応答すると、IM and Presence Service は連絡先が応答したクライアントのみにインスタントメッセージを配信します。

オフライン インスタントメッセージ

ログインしていない連絡先（オフライン）にユーザがインスタントメッセージを送信すると、IM and Presence サービスはそのインスタントメッセージを保存し、オフライン連絡先が自分のインスタントメッセージクライアントにサインインした後にそれを配信します。

インスタントメッセージのブロードキャスト

ユーザが同時に複数の連絡先にインスタントメッセージを送信することを可能にする機能です。たとえば、ユーザは大規模な連絡先グループに通知を送信できます。

すべてのインスタントメッセージクライアントがブロードキャストをサポートしているわけではないことに留意してください。

連絡先リストの最大サイズ

ユーザの連絡先リストの最大サイズを設定します。これはユーザが連絡先リストに追加できる連絡先の数です。この設定は、Cisco Jabber クライアント アプリケーションとサードパーティ クライアント アプリケーションの連絡先リストに適用されます。

連絡先の最大数に到達したユーザは、連絡先リストに新しい連絡先を追加できず、他のユーザもそのユーザを連絡先として追加できません。ユーザが連絡先リストの最大サイズに近く、最大数を超える連絡先を連絡先リストに追加すると、IM and Presence Service は超過した連絡先を追加しません。たとえば、IM and Presence Service の連絡先リストの最大サイズが 200 であるとします。ユーザに 195 件の連絡先があり、ユーザが 6 件の新しい連絡先をリストに追加しようとする、IM and Presence Service は 5 件の連絡先を追加し、6 件目の連絡先を追加しません。



ヒント 連絡先リストのサイズが上限に到達しているユーザがいると、**Cisco Unified CM IM and Presence の管理**の [システム トラブルシュータ (System Troubleshooter)] に表示されます。

アベイラビリティとインスタントメッセージの前提条件

SIP 間のインスタントメッセージでは、次のサービスが IM and Presence Service で実行されている必要があります。

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router

SIP と XMPP 間のインスタントメッセージでは、次のサービスが IM and Presence Service で実行されている必要があります。

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router
- Cisco XCP Text Conference Manager

アベイラビリティとインスタントメッセージのタスクフロー

IM and Presence Service のアベイラビリティとインスタントメッセージを設定するために次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	プレゼンス共有の設定 (205 ページ)	この手順を使用して、プレゼンスと IM のアベイラビリティ共有のクラスタ全体の設定を構成します。プレゼンス共有を使用すると、ユーザは互いの IM の可用性ステータスを表示できます。
ステップ 2	インスタントメッセージを有効にする (206 ページ)	ユーザがインスタントメッセージを交換できるようにシステムを設定します。

プレゼンス共有の設定

この手順を使用して、プレゼンスと IM のアベイラビリティ共有のクラスタ全体の設定を構成します。プレゼンス共有を使用すると、ユーザは互いの IM の可用性ステータスを表示できます。



(注) 可用性の共有が無効になっている場合

- ユーザはクライアントアプリケーションで自分の可用性ステータスを表示できますが、他のユーザのステータスはグレー表示されます。
- ユーザがチャットルームに入ると、自身の可用性ステータスは**未知**として表示されます。

手順

- ステップ 1** [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[プレゼンス (Presence)] > [設定 (Settings)] > [標準設定 (Standard Configuration)] を選択します。
- ステップ 2** クラスタ全体のプレゼンス共有を有効にするには、**可用性共有を有効にする**チェックボックスをチェックします。

(注) 個々の Cisco Jabber ユーザは、Cisco Jabber クライアント内でポリシー設定を再設定することによって、自分の Jabber クライアントに対してこの設定を有効または無効にすることができます。

ステップ 3 他のユーザの承認を必要とせずユーザが他のユーザのプレゼンスを表示できるようにする場合は、承認を求められることなく、ユーザが他のユーザの在席状況を表示できるようにするチェックボックスをチェックします。それ以外の場合、すべてのプレゼンス要求は他のユーザによって承認されなければなりません。

(注) 個々のエンドユーザは、Cisco Jabber クライアント内でポリシー設定を再設定することによってこの設定を上書きできます。

ステップ 4 最大連絡先リストサイズそして最大ウォッチャー（ユーザあたり）設定の最大値を設定します。最大値を使いたくない場合は、それぞれの制限なしチェックボックスをチェックします。

ステップ 5 これはオプションです。連絡先リストに登録されていない他のユーザのプレゼンスステータスを Cisco Jabber ユーザが一時的に登録できるようにする場合は、アドホックプレゼンス購読を有効にするチェックボックスをオンにして、アドホックプレゼンスの追加設定を行います。

ステップ 6 プレゼンス設定ウィンドウの追加の設定を完了します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 7 [保存 (Save)] をクリックします。

ステップ 8 Cisco XCP Router および Cisco Presence Engine サービスを再起動します：

- a) Cisco Unified IM and Presence Serviceability にログインして、[ツール (Tools)] > [コントロールセンター - 機能サービス (Control Center - Feature Services)] を選択します。
- b) Cisco Presence Engine サービスを選択して[再起動 (Restart)] をクリックします。
- c) [ツール (Tools)] > [コントロールセンター - ネットワーク サービス (Control Center - Network Services)] を選択します。
- d) [Cisco XCP Router] サービスを選択し、[リスタート (Restart)] をクリックします。

(注) 編集したフィールドによっては、サービスを再起動する必要はありません。編集したフィールドについては、オンラインヘルプを参照してください。

次のタスク

[インスタントメッセージを有効にする \(206 ページ\)](#)

インスタントメッセージを有効にする

ユーザがインスタントメッセージを交換できるようにシステムを設定します。

始める前に

[プレゼンス共有の設定 \(205 ページ\)](#)

手順

ステップ 1 Cisco Unified CM IM and Presence Administration で、[メッセージング (Messaging)] > [設定 (Settings)] を選択します。

ステップ 2 [Enable instant messaging] チェックボックスをオンにします。

ステップ 3 展開のニーズに合ったチェックボックスオプションをオンにします。フィールドの説明については、オンライン ヘルプを参照してください。

- オフライン中の相手へのインスタントメッセージの送信を無効にする
- クライアントでのインスタントメッセージ履歴のログ記録を可能にする (サポートされているクライアントのみ) (Allow clients to log instant message history (on supported clients only))
- インスタントメッセージでの切り取り/貼り付けを可能にする (Allow cut & paste in instant messages)

ステップ 4 [保存 (Save)] をクリックします。

可用性およびインスタントメッセージングの相互作用および制限

機能	制約事項
可用性の共有	この設定をオフにすると、ユーザは自分の可用性ステータスだけを表示できます。可用性情報は、クラスター内の他のユーザとは共有されません。さらに、クラスターの外部から受け取った可用性情報も共有されません。



第 16 章

アドホック チャットおよび常設チャットの の設定

- [グループチャットルームの概要 \(209 ページ\)](#)
- [グループチャットの前提条件 \(210 ページ\)](#)
- [グループチャットと常設チャットのタスクフロー \(211 ページ\)](#)
- [グループチャットと持続チャットのインタラクションと制限 \(216 ページ\)](#)
- [常設チャットの例 \(HA なし\) \(219 ページ\)](#)
- [Cisco IM and Presence の常設チャットの境界 \(220 ページ\)](#)

グループチャットルームの概要

グループチャットは、2人以上のユーザ間のインスタントメッセージングセッションです。IM and Presence Service は、アドホック チャット ルームまたは常設チャット ルームいずれかのグループチャットをサポートします。インスタントメッセージングを有効にすると、アドホックチャットルームのサポートはデフォルトで有効になりますが、常設チャットルームをサポートするようにシステムを設定する必要があります。

アドホック チャットルーム

アドホック チャットルームは、1人のユーザがチャットルームに接続されている限り存続するグループチャットセッションです。最後のユーザが会議室を離れると、アドホックチャットルームはシステムから削除されます。インスタントメッセージ会話のレコードは永続的に維持されません。インスタントメッセージングが有効になると、アドホックチャットルームはデフォルトで有効になります。

アドホック チャットルームは、既定ではパブリック ルームですが、プライベートに再構成できます。ただし、ユーザーがパブリックまたはプライベートのアドホックルームに参加する方法は、使用している XMPP クライアントの種類によって異なります。

- Cisco Jabber ユーザは、アドホック チャットルーム(パブリックまたはプライベート)に参加するために招待される必要があります。

- サードパーティの XMPP クライアントのユーザーは、任意のアドホック チャット ルーム (パブリックまたはプライベート) に参加するように招待したり、ルーム検出サービスを利用して参加するパブリック専用のアドホック ルームを検索したりできます。

常設チャット ルーム

永続的なチャット ルームは、すべてのユーザがルームを離れても存続するグループ チャット セッションです。ユーザは議論を続けるために時間をかけて同じ部屋に戻ることが期待されません。

常設チャットルームは、ユーザが協力し特定のトピックに関する知識を共有したり、そのトピックに関する発言のアーカイブを検索したり (この機能が **IM and Presence Service** で有効になっている場合)、そのトピックのディスカッションにリアルタイムで参加したりできるように作成されました。

常設チャットルーム用にシステムを設定する必要があります。さらに、常設チャットでは、外部データベースを配置する必要があります。

常設チャットルームは、デスクトップクライアントとモバイル Jabber クライアントの両方 (iOS クライアントと Android クライアントの両方を含む) でサポートされています。モバイルクライアントの場合は、最低限 Jabber リリースの 12.1 (0) を実行している必要があります。

グループチャットの前提条件

アドホックチャットの前提条件

アドホックチャットルームを展開している場合は、インスタントメッセージングが有効になっていることを確認してください。詳細については、[インスタントメッセージを有効にする \(206 ページ\)](#) を参照してください。

常設チャットの前提条件

常設チャットルームを展開している場合：

- インスタントメッセージングが有効になっていることを確認してください。詳細については、[インスタントメッセージを有効にする \(206 ページ\)](#) を参照してください。
- 外部データベースを配置する必要があります。データベースの設定とサポート情報については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html> で *IM and Presence* サービスデータベースセットアップガイドを参照してください。
- 常設チャットに高可用性を導入するかどうかを決定します。この展開タイプは、常設チャットルームに冗長性とフェイルオーバーを追加します。ただし、外部データベースの要件は、高可用性なしで機能を導入する場合は多少異なります。
- 常設チャットの展開には、少なくとも 15,000 ユーザ OVA を導入することを推奨します。

グループチャットと常設チャットのタスクフロー

手順

	コマンドまたはアクション	目的
ステップ 1	グループチャットシステム管理者の設定 (211 ページ)	常設チャットシステムを管理するためのシステム管理者を追加します。
ステップ 2	チャットルーム設定を設定します (212 ページ)	基本チャットルーム設定を設定します。オプションで、常設チャットの有効化。
ステップ 3	Cisco XCP Text Conference Manager を再起動します (213 ページ)	常設チャットを展開している場合、Cisco XCP Text Conference Manager サービスが実行していることを確認します。
ステップ 4	常設チャット用の外部データベースの設定 (214 ページ)	常設チャットでは、各ノードに一意の外部データベース インスタンスを設定する必要があります。 (注) 常設チャット用の高可用性を導入する場合は、HA の導入時にデータベースの要件がわずかに異なるため、この章の残りの作業をスキップできません。
ステップ 5	外部データベースの接続の追加 (215 ページ)	IM and Presence サービスで、外部データベースへの接続を設定します。
ステップ 6	ある外部データベースから別のデータベースに常設チャット ルームを移行する	IM and Presence サービスで、既存の外部データベースから、すべての常設チャットルームとグループを、同じデータベースの種類または異なる種類の別のデータベースに移行します。外部データベースの移行を実行する方法の詳細については、Cisco IM and Presence データベースセットアップガイド 12.5(1)SU2 リリースの「常設チャット ルームを外部データベース間で移行する」セクションを参照してください。

グループチャット システム管理者の設定

常設チャットシステムを管理するためのシステム管理者を追加します。

手順

ステップ 1 [メッセージング (Messaging)] > [グループチャットシステムの管理者 (Group Chat System Administrators)] を選択します。

ステップ 2 [グループチャットシステムの管理者を有効にする (Enable Group Chat System Administrators)] のチェックボックスをオンにします。

設定が有効または無効の場合、Cisco XCP ルータを再起動します。システム管理者の設定を有効に設定すると、システム管理者を動的に追加できます。

ステップ 3 [新規追加 (Add New)] をクリックします。

ステップ 4 IM アドレスを入力します。

例

IM アドレスは name@domain の形式である必要があります。

ステップ 5 ニックネームおよび説明を入力します。

ステップ 6 [保存 (Save)] をクリックします。

次のタスク

[チャットルーム設定を設定します \(212 ページ\)](#)

チャットルーム設定を設定します

Room Member や Occupancy などの基本的なチャットルーム設定、および 1 部屋あたりの最大ユーザ数を構成します。

オプションで、常設チャットを有効にするチェックボックスをチェックすることで、常設チャットを有効にできます。

手順

ステップ 1 [Cisco Unified CM IM and Presenceの管理 (Cisco Unified CM IM and Presence Administration)] から、[メッセージング (Messaging)] > [グループチャットおよび常設チャット (Group Chat and Persistent Chat)] を選択します。

ステップ 2 システムが自動的にプライマリグループチャットサーバのエイリアスを管理するチェックボックスをチェックする、またはチェックしないことにより、システムでチャットノードエイリアスを管理するかどうかを設定します。

- チェックあり - システムはチャットノードエイリアスを自動的に割り当てます。これはデフォルト値です。
- チェックなし - 管理者は自分のチャットノードエイリアスを割り当てることができます。

ステップ3 参加者全員が退室した後もチャットルームをそのままにしておきたい場合は、**常設チャットを有効にする**チェックボックスにチェックします。

(注) これはクラスタ全体の設定です。クラスタ内の任意のノードで永続的なチャットが有効になっている場合は、任意のクラスタのクライアントで、そのノード上の **Text Conference** インスタンスおよびそのノードでホストされているチャットルームを検出できます。

リモートクラスタからのユーザは、そのリモートクラスタで常設チャットが有効になっていなくても、ローカルクラスタ上の **Text Conference** インスタンスおよびチャットルームを検出できます。

ステップ4 常設チャットを有効にすることを選択した場合は、以下のフィールドのそれぞれの値を設定します。

- 許可されるパーシステントチャットルームの最大数 (Maximum number of persistent chat rooms allowed)
- データベース接続数
- データベース接続のハートビート間隔 (秒) (Database connection heartbeat interval (seconds))
- パーシステントチャットルームのタイムアウト値 (分) (Timeout value for persistent chat rooms (minutes))

(注) シスコのサポート担当者に連絡せずに、**データベース接続のハートビート間隔値**をゼロに設定しないでください。ハートビート間隔は、通常、ファイアウォールを介して接続を開いたままにするのに使用されます。

ステップ5 **部屋の設定**で、最大部屋数を割り当てます。

ステップ6 **グループチャットと常設チャットの設定**ウィンドウの残りの設定を完了します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ7 [保存 (Save)] をクリックします。

次のタスク

[Cisco XCP Text Conference Manager を再起動します \(213 ページ\)](#)

Cisco XCP Text Conference Manager を再起動します

チャット設定を編集したか、チャットノードに1つ以上のエイリアスを追加した場合は、**Cisco XCP テキスト会議マネージャ**サービスを再起動します。

手順

-
- ステップ 1** [Cisco Unified IM and Presenceのサービスアビリティ (Cisco Unified IM and Presence Serviceability)] で、[ツール (Tools)] > [コントロールセンター-機能サービス (Control Center - Feature Services)] を選択します。
- ステップ 2** [サーバ (Server)] ドロップダウンリストから、IM and Presence ノードを選択して、[移動 (Go)] をクリックします。
- ステップ 3** [IM and Presence サービス (IM and Presence Services)] セクションで、[Cisco XCP Text Conference Manager] ラジオボタンをクリックし、[起動 (Start)] または [再起動 (Restart)] ボタンをクリックします。
- ステップ 4** リスタートに時間がかかることを示すメッセージが表示されたら、[OK] をクリックします。
- ステップ 5** (任意) サービスが完全に再起動されたことを確認するには、[更新 (Refresh)] をクリックします。
-

次のタスク

常設チャットの高可用性を展開する場合は、[常設チャットにおける高可用性のタスクフロー \(228 ページ\)](#) を進みます。

それ以外の場合は、[常設チャット用の外部データベースの設定 \(214 ページ\)](#) に進みます。

常設チャット用の外部データベースの設定



- (注) このトピックでは、高可用性なしの常設チャットについて説明します。常設チャットに高可用性を展開する場合は、外部データベースの設定情報ではなく、該当する章を参照してください。
-

常設チャットルームを設定する場合は、常設チャットルームをホストするノードごとに、個別の外部データベースインスタンスを設定する必要があります。また、次の点に注意してください。

- 永続的なチャットが有効な場合は、外部データベースを Text Conference Manager サービスに関連付ける必要があります。また、データベースがアクティブで到達可能である必要があります。そうでない場合は、Text Conference Manager は起動しません。
- 常設チャットのログ記録に外部データベースを使用する場合は、データベースが大量の情報を処理するのに十分な大きさであることを確認してください。チャットルームのすべてのメッセージをアーカイブすることはオプションですが、ノードのトラフィックが増え、外部データベースのディスク領域が消費されます。
- データベースサイズを監視し、期限切れのレコードを自動的に削除するジョブを設定するには、外部データベースクリーンアップユーティリティを使用します。

- 外部データベースへの接続数を設定する前に、書き込む IM の数およびそのトラフィック総量を考慮します。設定する接続数によって、システムを拡張できます。システムのデフォルト設定はほとんどのインストールに適していますが、特定の展開にパラメータを適応させることもできます。

外部データベースを設定する方法については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html>で *IM and Presence* サービスの外部データベース設定ガイドを参照してください。

次のタスク

[外部データベースの接続の追加 \(215 ページ\)](#)

外部データベースの接続の追加

IM and Presence サービスから常設チャット外部データベースへの接続を設定します。IM and Presence サービスのクラスタ間全体には、少なくとも1つの一意の論理外部データベースインスタンス（テーブルスペース）が必要です。

手順

- ステップ 1** [Cisco Unified CM IM and Presence 管理 (Cisco Unified CM IM and Presence Administration)] から、[メッセージ (Messaging)] > [外部サーバ設定 (External Server Setup)] > [外部データベース (External Databases)] を選択します。
- ステップ 2** [新規追加 (Add New)] をクリックします。
- ステップ 3** [データベース名 (Database Name)] フィールドに、外部データベースインスタンスの名前を入力します。
- ステップ 4** データベースの種類 ドロップダウンリストから、展開する外部データベースの種類を選択します。
- ステップ 5** データベースのユーザ名とパスワード情報を入力します。
- ステップ 6** [Hostname] フィールドにホストのデータベースのホスト名または IP アドレスを入力します。
- ステップ 7** 外部データベース設定ウィンドウの残りの設定を完了します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。
- ステップ 8** [保存 (Save)] をクリックします。
- ステップ 9** この手順を繰り返して、各外部データベースインスタンスへの接続を作成します。

グループチャットと持続チャットのインタラクションと制限

表 19: グループチャットと持続チャットのインタラクションと制限

機能の相互作用	制約事項
ルームへの参加のアーカイブ	ルームの入退室をアーカイブすると、トラフィックが増加し、外部データベースサーバの領域が消費されるため、これを行うかどうかは任意です。
匿名ルームでのチャット	Cisco Jabber 経由でチャットを展開する場合（グループチャットまたは持続チャットのいずれか）は、[グループチャットとパーシステントチャットの設定（Group Chat and Persistent Chat Settings）] ウィンドウで [デフォルトで、ルームは匿名です（Rooms are anonymous by default）] および [ルームのオーナーは、ルームを匿名にするかどうかを変更できます（Room owners can change whether or not rooms are anonymous）] オプションが選択されていないことを確認してください。いずれかのチェックボックスをオンにすると、チャットは失敗します。
データベース接続の問題	Text Conference Manager サービスが起動した後で外部データベースとの接続が失敗した場合、Text Conference Manager サービスはアクティブなままで動作を継続します。ただし、メッセージはデータベースに書き込まれなくなり、接続が回復するまで新しい永続的なルームを作成できません。
OVA の要件	<p>常設チャットまたはクラスタ間ピアリングを展開している場合、これらの機能に展開できる最小 OVA サイズは 5000 ユーザ OVA です。少なくとも 15,000 ユーザの OVA を展開することをお勧めします。ユーザベースの規模によっては、集中型展開では 25,000 ユーザの OVA が必要になる場合があります。OVA オプションとユーザ容量の詳細については、次のサイトを参照してください。</p> <p>(注) すべての IMP ノードに少なくとも 15000 ユーザ OVA を展開することを強く推奨します。</p> <p>https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html</p>

機能の相互作用	制約事項
Microsoft SQL Server での常設チャット文字数の制限	<p>メッセージの本文（HTML タグとテキストメッセージを含む）が 4000 文字を超えるチャットメッセージは配信されません。これらのメッセージは拒否され、アーカイブされません。この問題は、Microsoft SQL Server がリリース 11.5 (1) SU3 以降の外部データベースとして使用されている場合に発生します。詳細については、CSCvd89705 を参照してください。</p>
ピアクラスタがサポートされていないリリースを実行している Jabber Mobile 用の常設チャット	<p>Jabber モバイル用の常設チャットは 11.5 (1) SU5 で導入され、11.5 (1) SU の以前のリリースではサポートされません。この機能は 12.0 (1) または 12.0 (1) SU1 でもサポートされていません。</p> <p>このリリースで Jabber モバイル用の常設チャットを展開し、Jabber Mobile 用の常設チャットルームをサポートしないピアクラスタでクラスタ間ピアリングを設定している場合、Jabber モバイルクライアントには次の条件が適用されます。</p> <p>常設チャットルームが 11.5 (1) などのサポートされていないリリースでホストされている場合：</p> <ul style="list-style-type: none"> • サポートされているクラスタに所属する Jabber モバイルクライアントは、サポートされていないクラスタでホストされている常設チャットルームに参加できますが、ルームをミュートすることはできません。彼らはグローバルミュートオプションを見られるでしょう、しかしそれはうまくいきません。 • サポートされていないピアクラスタに所属している Jabber モバイルクライアントは、常設チャットルームに参加できません。 <p>常設チャットルームが、11.5 (1) SU5 などのサポートされているリリースでホストされている場合：</p> <ul style="list-style-type: none"> • サポートされているクラスタに所属している Jabber モバイルクライアントの参加者は、モバイル機能に関する常設チャットをすべて使用できます。 • サポートされていないピアクラスタの Jabber モバイルクライアントは、常設チャットルームに参加できません。 <p>(注) 常設チャットの検索機能は、Jabber 設定ファイル (<i>jabber-config.xml</i>) が IM 履歴を無効にするように設定されている場合は動作しません。</p>

機能の相互作用	制約事項
外部データベース接続および Cisco XCP Text Conferencing サービス	<p>スプリットブレイン現象が発生すると、サブスクライバまたはパブリッシャがピア Text Conferencing サービスを検出するか、いずれかのノードがダウンした場合、サブスクライバまたはパブリッシャは、通常の状態からバックアップへの移行を試みます。</p> <p>この操作中に、ピアチャットルームの読み込みで外部データベースへの接続に失敗した場合、Cisco XCP Text Conferencing サービスはシャットダウンします。</p>
高可用性が設定されている場合にサポートされるパーシステントチャットルームの数	<p>IM & P の導入でサポートされるパーシステントチャットルームの最大数は、サブクラスターあたり 5000 です。</p> <p>高可用性を有効にしている場合は、ノードあたり最大 2500 ルームを作成することを推奨します。（ただし、システムは最大で 1 ノードあたり最大 5000 ルームを作成できます）。高可用性導入環境では、ノードあたり 2500 ルームが設定されている場合、フェールオーバー時には、バックアップノード上にホストされている 5000 ルームより多くのルームが存在することになります。このため、トラフィックの負荷によっては、予期しないパフォーマンスの問題が発生する可能性があります。</p> <p>システム上の 5000 ルームの負荷は、ルーム内の参加者の数、ルーム内のメッセージ交換の割合、メッセージのサイズにも依存します。Cisco コラボレーションサイジングツールを使用して、パーシステントチャット導入のための適切な OVA セットアップを確認します。コラボレーションサイジングツールの詳細については、次を参照してください。 https://cucst.cloudapps.cisco.com/landing</p> <p>サブクラスター内の両方のノード間で均等にルームのバランスをとることを推奨します。また、IM&P クラスターに複数のサブクラスターがある場合は、すべてのサブクラスターにわたってルームのロードバランシングを行うことを推奨します。現在の IM & P には、ルームを自動的にロードバランシングするメカニズムがありません。ルームのロードバランシングは、ルームを作成するユーザの責任で行います。ルームの作成時に、ユーザは Jabber 機能を使用して、自動的にランダムノードをルーム作成用を選択していることを確認する必要があります。</p>

機能の相互作用	制約事項
アドホック チャット ルームをプライベートに する	<p>アドホック チャット ルームは既定でパブリックですが、次の構成のメンバーのみに設定できます。</p> <ol style="list-style-type: none"> 1. [Cisco Unified CM IM and Presenceの管理 (Cisco Unified CM IM and Presence Administration)] から、[メッセージング (Messaging)]>[グループチャットおよび常設チャット (Group Chat and Persistent Chat)] を選択します。 2. [ルームは既定でメンバー専用にする] チェック ボックスをオンにします。 3. [ルームのオーナーは、ルームをメンバー専用にするかどうかを変更できます (Room owners can change whether or not rooms are for members only)] チェックボックスをオフにします。 4. [他のユーザをメンバー専用ルームに招待できるのはモデレータのみです (Only moderators can invite people to members-only rooms)] チェックボックスをオフにします。 5. [保存 (Save)] をクリックします。 6. Cisco XCP Text Conference サービスを再起動します。

常設チャットの例 (HA なし)

次の2つの例は、常設チャットの高可用性が導入されていない場合のクラスタ間ピアリングとともに常設チャット機能を示しています。

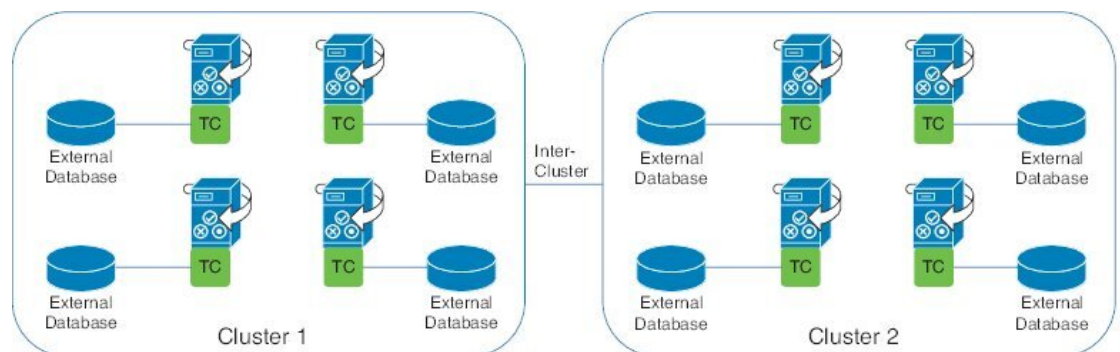


(注) 常設チャットを展開している場合は、常設チャットルームに冗長性を追加するために、常設チャットの高可用性を表示することをお勧めします。

常設チャット (HA なし) すべてのクラスタ間ノードで有効

常設チャット (HA なし) クラスタ間ネットワーク内のすべてのノードで有効。すべてのノードに常設チャット用の外部データベースが関連付けられているため、すべてのノードで常設チャットルームをホストできます。

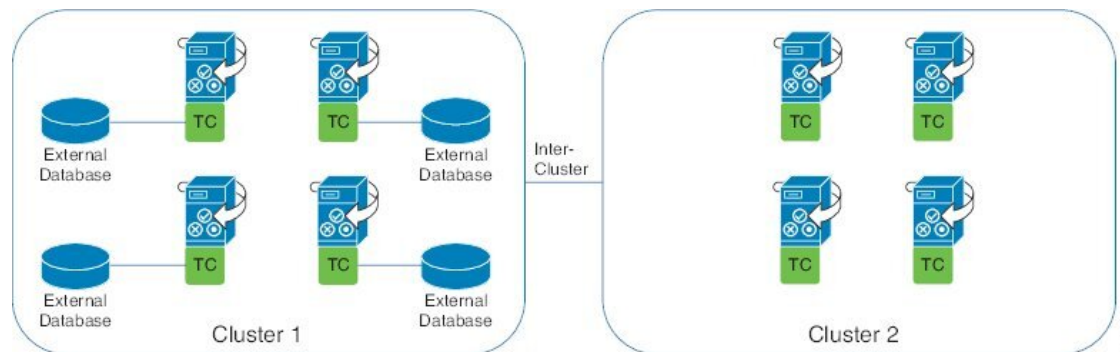
Cisco Text Conferencing サービスは、いずれのクラスタのすべてのノードで実行されているため、いずれかのクラスタのすべてのユーザも、いずれかのクラスタの任意のノードでホストされている常設チャットルームに参加できます。



常設チャット（HAなし）クラスタ間ネットワークの1つのクラスタで有効

常設チャット用に設定されているのは、クラスタ1内のノードのみです。（HAなし）外部データベースがあります。ノードは常設チャットルームをホストするように構成されていないため、クラスタ2では外部データベースは必要ありません。

ただし、Cisco Text Conference Manager サービスはいずれかのクラスタ内のすべてのノードで実行されているため、どちらかのクラスタ内のすべてのユーザーがクラスタ1でホストされている常設チャットルームに参加できます。



Cisco IM and Presence の常設チャットの境界

このセクションでは、IMおよびプレゼンスの永続的なチャット (PChat)境界を表すマトリックスについて説明し、さまざまな依存関係を明確にする例を示します。

永続的なチャット境界を導き出す場合は、次の前提事項が存在します。

1. エイリアス/サーバ/サブクラスタ/クラスタごとのルーム数に関しては、次の点に従います。
 1. サーバーには、複数のテキスト会議のエイリアスが含まれている場合があります。
 2. サブクラスタには2つのサーバー（ノード）が含まれます。
 3. 1つのクラスタには、最大3つのサブクラスタを含めてもよい。

2. 高い利用可能性(HA)が有効になっている場合、サポートされているすべての部屋番号が半減します。[常設チャット ルームの最大数]の最大許容値は 2500 です。
3. 例: 1 部屋あたり平均 100 人のユーザを想定すると、IM and Presence サービスは次の機能をサポートできます。
 1. HA を使用しないサーバーあたり 3500 の常設チャット ルーム
 2. HA を備えたサーバーごとに 1750 の常設チャット ルーム。
 3. 1 分間に 1 つのメッセージを 1 回使用すると、サーバーごとに最大 273 の常設チャット ルームをアクティブにできます。

これらの依存関係を明確にする例を次に示します。

タイムスライスごとにサポートされる部屋は、次の式を使用して、サポートされる部屋の合計数を犠牲にして増加できます。

サポートされる新しいルーム数=現在サポートされているルーム数*タイム スライスあたりサポートされている現在のルーム数 (%) / タイム スライスごとにサポートされる新しいルーム数 (%)

表 20: 25K OVA 常設チャット容量テーブル (サーバー単位)

ルームあたりの平均ユーザ数	サポートされている PChat ルームの数	タイムスライスごとにサポートされるルーム メッセージの頻度 = 1/分	タイムスライスごとにサポートされるルーム メッセージの頻度 = 3分
2	5000	100 %	100 %
5	5000	100 %	58%
10	5000	99%	33%
15	5000	69%	23 %
20	5000	53 %	18%
30	5000	36%	12%
50	5000	22%	7%
100	3497	16 %	5%
200	2064	14%	5%
500	926	12%	4 %
1,000	482	12%	4 %



(注) これは、ユーザの30%が2つのデバイス/クライアントを持っていることを前提としています。

25K OVA の例:

ルームあたりの平均ユーザー数 = 10

メッセージ頻度 = 3/分

現在サポートされているルーム数 = 5000

現在のルームはタイム スライスごとにサポート = 33%

新しいルームはタイム スライスごとにサポートされます = 50%

結果 :

新しい部屋サポート = $5000 * 33/50 = 3300$

表 21: 15K OVA 常設チャット容量テーブル (サーバー単位)

ルームあたりの平均 ユーザ数	サポートされている PChat ルームの数	タイムスライスごとに サポートされるルーム メッセージの頻度 = 1/ 分	タイムスライスごとに サポートされるルーム メッセージの頻度 = 3 分
2	5000	100 %	80%
5	5000	100 %	41%
10	5000	67%	22%
15	5000	46 %	15%
20	5000	35%	12%
30	5000	24 %	8 %
50	5000	14%	5%
100	3497	10%	3 %
200	2064	9%	3 %
500	926	8 %	3 %
1,000	482	7 %	2 %



(注) これは、ユーザの30%が2つのデバイス/クライアントを持っていることを前提としています。

15K OVA の例:

ルームあたりの平均ユーザ数 = 5

メッセージ頻度 = 3/分

現在サポートされているルーム数 = 5000

現在のルームはタイム スライスごとにサポート = 41%

新しいルームはタイム スライスごとにサポートされます = 50%

結果 :

新しい部屋サポート = $5000 * 41/50 = 4100$

表 22: 5K OVA 常設チャット容量テーブル (サーバー単位)

ルームあたりの平均ユーザ数	サポートされている PChat ルームの数	タイムスライスごとにサポートされるルーム メッセージの頻度 = 1/分	タイムスライスごとにサポートされるルーム メッセージの頻度 = 3分
2	5000	94%	31%
5	5000	53 %	18%
10	4654	33%	11%
15	4261	26 %	9%
20	3929	21 %	7%
30	3399	17%	6 %
50	2677	13 %	4 %
100	1748	10%	3 %
200	1032	9%	3 %
500	463	8 %	3 %
1,000	241	7 %	2 %



(注) これは、ユーザの 30% が 2 つのデバイス/クライアントを持っていることを前提としています。

5K OVA の例:

ルームあたりの平均ユーザ数 = 2

メッセージ頻度 = 3/分

現在サポートされているルーム数 = 5000

現在のルームはタイム スライスごとにサポート = 31%

新しいルームはタイム スライスごとにサポートされます = 50%

結果 :

新しい部屋サポート = $5000 * 31/50 = 3100$



第 17 章

常設チャットの高可用性の設定

- [持続チャットにおける高可用性の概要 \(225 ページ\)](#)
- [常設チャット前提条件の高可用性 \(228 ページ\)](#)
- [常設チャットにおける高可用性のタスクフロー \(228 ページ\)](#)
- [常設チャットにおける高可用性の使用例 \(234 ページ\)](#)

持続チャットにおける高可用性の概要

常設チャットの高可用性 (HA) は常設チャットルームを使用していて、システムの冗長性がプレゼンス冗長グループで構成されている場合に展開できるオプションの機能です。

常設チャットの高可用性により、常設チャットルームに冗長性とフェイルオーバー機能が追加されます。IM and Presence Service ノードの障害またはテキスト会議 (TC) サービスの障害時は、サービスによりホストされているすべての常設チャットルームが自動的にバックアップノードまたは TC サービスによってホストされます。フェールオーバー後、Cisco Jabber クライアントはシームレスに常設チャットルームを使用し続けることができます。

外部データベース

常設チャット (非 HA) と常設チャット HA のセットアップの主な違いは、外部データベースの要件に関するものです。

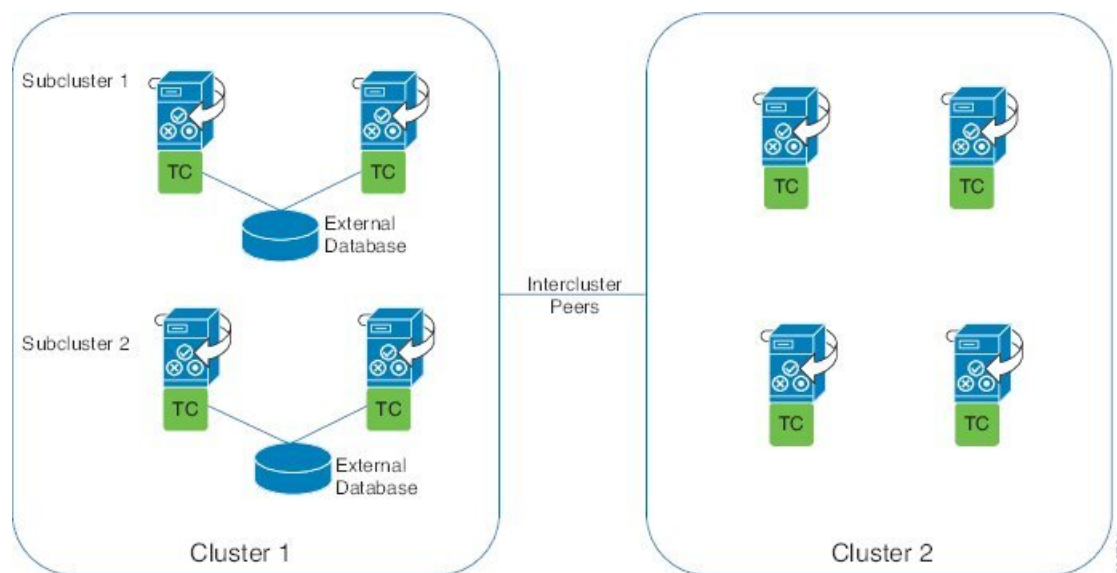
- 常設チャットが HA なしで展開されている場合、外部データベースは個々のチャットノードにのみ接続します。常設チャットルームをホストする各ノードには、個別の外部データベースインスタンスが必要です。チャットノードに障害が発生した場合、そのノードでホストされていた常設チャットルームは、チャットノードが復旧するまで使用できなくなります。
- 常設チャットの高可用性がデプロイされている場合、外部データベースインスタンスはサブクラスタ (プレゼンス冗長グループ) 内の両方のノードに接続します。常設チャットノードに障害が発生した場合、サブクラスタ内のバックアップノードが引き継ぎ、チャットを中断することなく続行できます。

常設チャットの高可用性 - クラスタ間の例

次の図は、常設チャットの高可用性がクラスタ1にのみデプロイされているクラスタ間ネットワークを示しています。常設チャットの高可用性により、各サブクラスターは外部データベースをホストします。クラスタ2では、常設チャットの高可用性が有効になっていないため、外部データベースは必要ありません。ただし、Cisco Text Conference Manager サービスはすべてのノードで実行されているため、クラスタ2のユーザは、クラスタ1でホストされている常設チャットルームに参加できます。



- (注) この例では、クラスタ1のチャットルームだけが常設チャットルームをホストするように構成されています。外部データベースインスタンスとともに、クラスタ2ノードに常設チャットサポートを追加することもできます。この場合、どちらのクラスタのすべてのユーザも、どちらのクラスタの任意のノードでホストされている常設チャットルームに参加できます。



常設チャット（非 HA）と常設チャット HA の要件の比較

常設チャットルームを展開している場合、常設チャットルームにフェールオーバー機能を追加するだけでなく、常設チャットの高可用性を展開することをお勧めします。これは必須ではありません。

次の表に、高可用性の有無にかかわらずデプロイされた常設チャットの違いを示します。

表 23: 高可用性ありとなしの常設チャットの比較

	常設チャット（HA なし）	常設チャット HA
データベース要件	<p>永続チャットルームをホストするクラスタノードごとに、個別の外部データベースインスタンスが必要です。これらの外部データベースインスタンスは、同じ外部データベースサーバ上に作成できます。</p> <p>おすすめ：最適なパフォーマンスとスケーラビリティを得るには、IM and Presence クラスタの各ノードまたは冗長グループに固有の論理外部データベースインスタンスを導入してください。これは必須ではありません。</p> <p>最低必要条件 IM and Presence クラスタ間ネットワークでの常設チャットには、少なくとも1つの外部データベースインスタンスが必要です。ただし、この配置は使用率の高いネットワークには不十分な場合があります。</p> <p>サポートされているデータベースの種類</p> <ul style="list-style-type: none"> • PostgreSQL（バージョン 9.1 以降） • Oracle • Microsoft SQL Server 	<p>常設チャットルームをホストする各サブクラスタ（プレゼンス冗長グループ）ごとに、個別の外部データベースインスタンスが必要です。これらの外部データベースインスタンスは、同じ外部データベースサーバ上に作成できます。</p> <p>おすすめ：最適なパフォーマンスとスケーラビリティを得るには、IM and Presence クラスタの各ノードに個別の外部データベースインスタンスを導入してください。これは必須ではありません。</p> <p>最低必要条件 IM and Presence クラスタ間ネットワーク上の常設チャット HA には、少なくとも1つの外部データベースインスタンスが必要です。ただし、この配置は使用率の高いネットワークには不十分な場合があります。</p> <p>サポートされているデータベースの種類</p> <ul style="list-style-type: none"> • PostgreSQL（バージョン 9.1 以降） • Oracle • Microsoft SQL Server（11.5（1）SU2 以降）

	常設チャット (HA なし)	常設チャット HA
常設チャットノードが失敗したときの動作	<ul style="list-style-type: none"> 障害が発生したノードでホストされている常設チャットルームは、ノードが復旧するまでアクセスできません。 クラスタの冗長性が設定されている場合、障害が発生したノードに所属するユーザは、サブクラスタ内のバックアップノードにフェイルオーバーします。ただし、障害が発生したノードから常設チャットルームにアクセスすることはできません。 	<ul style="list-style-type: none"> 常設チャットルームは、サブクラスタ内のバックアップノードにフェイルオーバーします。ユーザはサービスを中断することなくメッセージングを継続できます。 障害が発生したノードをホームとするユーザもフェイルオーバーします。

常設チャット前提条件の高可用性

常設チャットの高可用性を設定する前に、次のことを確認してください。

- 常設チャット ルームが有効である。詳細については、[チャット ルーム設定を設定します \(212 ページ\)](#) を参照してください。
- 高可用性は各プレゼンス冗長グループで有効です。詳細については、[プレゼンス冗長グループのタスク フロー \(55 ページ\)](#) を参照してください。
- 外部データベースを設定済です。データベースの設定とサポート情報については、*IM and Presence* サービスのデータベースセットアップガイドを参照してください。

常設チャットにおける高可用性のタスクフロー

手順

	コマンドまたはアクション	目的
ステップ 1	外部データベースのセットアップ (229 ページ)	常設チャットルームがホストされているサブクラスタごとに、個別の外部データベースインスタンスが必要です。これらの別々の外部データベースインスタンスは、同じデータベースサーバでホストできます。
ステップ 2	外部データベースの接続の追加 (229 ページ)	IM and Presence サービスからの外部データベースへの接続を設定します。

	コマンドまたはアクション	目的
ステップ 3	常設チャットにおける高可用性の確認 (230 ページ)	常設チャットの高可用性のシステム設定を確認してください。
ステップ 4	Cisco XCP Text Conference Manager サービスの起動 (231 ページ)	Cisco XCP Text Conference Manager サービスがいずれかのノードで停止した場合は、この前提条件を使用して開始します。
ステップ 5	外部データベースのマージ (232 ページ)	これはオプションです。常設チャットが複数の外部データベースで構成されていた以前のリリースからアップグレードする場合は、この手順を使用して外部データベースを単一のデータベースにマージします。

外部データベースのセットアップ

常設チャットの高可用性を展開するには、常設チャットルームがホストされている各サブクラスターごとに個別の外部データベースインスタンスが必要です。これらの別々の外部データベースインスタンスは、同じデータベースサーバでホストできます。

サブクラスターは、IM and Presence ノード（プレゼンス冗長グループ）の冗長ペアです。6 ノードの IM and Presence クラスターに最大 3 つのサブクラスターを含めることができます。6 ノードの IM and Presence クラスターで常設チャットの HA が有効になっている場合、3 つの外部データベースインスタンスと 3 つのサブクラスターペアが必要です。

外部データベース接続には、PostgreSQL、Oracle、または Microsoft SQL Server を使用できます。設定の詳細については、*IM and Presence* サービスのデータベース設定ガイドを参照してください。

次のタスク

[外部データベースの接続の追加 \(229 ページ\)](#)

外部データベースの接続の追加

IM and Presence サービスから常設チャットの高可用性外部データベースインスタンスへの接続を設定します。両方のプレゼンス冗長グループ ノードが同じ一意の論理外部データベースインスタンスに割り当てられていることを確認します。

手順

-
- ステップ 1** [Cisco Unified CM IM and Presence 管理 (Cisco Unified CM IM and Presence Administration)] から、[メッセージ (Messaging)] > [外部サーバ設定 (External Server Setup)] > [外部データベース (External Databases)] を選択します。
- ステップ 2** [新規追加 (Add New)] をクリックします。
- ステップ 3** [データベース名 (Database Name)] フィールドに、外部データベースインスタンスの名前を入力します。
- ステップ 4** データベースの種類ドロップダウンリストから、展開する外部データベースの種類を選択します。
- ステップ 5** データベースのユーザ名とパスワード情報を入力します。
- ステップ 6** [Hostname] フィールドにホストのデータベースのホスト名または IP アドレスを入力します。
- ステップ 7** 外部データベース設定ウィンドウの残りの設定を完了します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。
- ステップ 8** [保存 (Save)] をクリックします。
- ステップ 9** この手順を繰り返して、各外部データベースインスタンスへの接続を作成します。
-

次のタスク

[常設チャットにおける高可用性の確認 \(230 ページ\)](#)

常設チャットにおける高可用性の確認

この手順を使用して、システムが常設チャットの高可用性に設定されていることを確認します。



-
- (注) プレゼンス冗長グループ (サブクラスタ) の高可用性を既に有効にしている、チャットルーム設定に常設チャットが含まれている場合は、常設チャットの高可用性が完了している可能性があります。
-

手順

-
- ステップ 1** 各サブクラスタで高可用性が有効になっていることを確認します。
- Cisco Unified CM の管理から、[システム (System)] > [プレゼンス冗長グループ (Presence Redundancy Groups)] を選択します。
 - 検索をクリックして、確認したいプレゼンス冗長グループを選択します。
 - [高可用性を有効にする (Enable High Availability)] チェックボックスがチェックされていることを確認します。チェックボックスがオフの場合は、チェックを付けます。

- d) [保存 (Save)] をクリックします。
- e) クラスタ内の各プレゼンス冗長グループに対してこれらの手順を繰り返します。

ステップ 2 常設チャットが有効になっていることを確認します。

- a) [Cisco Unified CM の管理 (Cisco Unified CM Administration)] から、[メッセージング (Messaging)] > [グループチャットと常設チャット (Group Chat and Persistent Chat)] を選択します。
- b) [常設チャットの有効化 (Enable Persistent Chat)] チェック ボックスがチェックされていることを確認します。チェックボックスがオフの場合は、チェックを付けます。
- c) [保存 (Save)] をクリックします。

ステップ 3 Cisco Unified CM の管理ページから、Cisco XCP テキスト会議マネージャサービスがすべてのクラスタノードで実行されていることを確認します。

- a) [システム (System)] > [プレゼンス トポロジ (Presence Topology)] を選択します。
- b) 各クラスタノードで、表示をクリックして、ノードの詳細を表示する
- c) ノードステータスで、Cisco XCP テキスト会議マネージャサービスが開始済であることを確認します。
- d) 左側のナビゲーションバーで、プレゼンス トポロジをクリックして、クラスタトポロジに戻り、すべてのクラスタノードのステータスを確認するまで上記の手順を繰り返します。

次のタスク

Cisco XCP テキスト会議マネージャサービスを有効にする必要がある場合、[Cisco XCP Text Conference Manager サービスの起動 \(231 ページ\)](#)。

Cisco XCP Text Conference Manager サービスの起動

この手順を使用して Cisco XCP Text Conference Manager サービスを起動します。これらのノードのユーザが常設チャットルームに参加できるようにするには、このサービスがすべてのクラスタノードで実行されている必要があります。

手順

- ステップ 1** [Cisco Unified IM and Presenceのサービスアビリティ (Cisco Unified IM and Presence Serviceability)] で、[ツール (Tools)] > [コントロールセンター-機能サービス (Control Center - Feature Services)] を選択します。
- ステップ 2** [サーバ (Server)] ドロップダウンリストから、IM and Presence クラスタ ノードを選択して、[移動 (Go)] をクリックします。
- ステップ 3** [IM and Presenceサービス (IM and Presence Services)] で、[Cisco XCPテキスト会議マネージャ (Cisco XCP Text Conference Manager)] を選択し、[開始(Restart)] をクリックします。
- ステップ 4** [OK] をクリックします。

ステップ5 (任意) サービスが完全に再起動されたことを確認するには、[更新 (Refresh)] をクリックします。

外部データベースのマージ

外部データベースをマージするには、以下の手順を使用します。



(注) Microsoft SQL データベースに関しては、外部データベースのマージはサポートされていません。

これはオプションです。11.5(1)より前のリリースからアップグレードし、冗長性を管理するために複数の外部データベースが使用されていた場合は、外部データベースマージツールを使用して外部データベースを単一のデータベースにマージします。

例

11.5(1)より前のリリースからアップグレードした場合で、各常設チャットノードを別々の外部データベースインスタンスに接続するように常設チャットを設定した場合は、この手順を使用してサブクラスタ内の2つのデータベースを両方のノードに接続する単一データベースにマージします。

始める前に

- 2つのソースおよび対象データベースが、プレゼンス冗長グループの各 IM and Presence Service ノードに正しく割り当てられていることを確認します。これにより両方のスキーマが有効であることが確認されます。
- 対象データベースのテーブルスペースをバックアップします。
- 対象データベース上に、新しくマージされたデータベースが十分に収まる領域があることを確認します。
- ソースデータベースと対象データベース用に作成されたデータベース ユーザに、次のコマンドを実行する権限があることを確認します。

- CREATE TABLE

- CREATE PUBLIC DATABASE LINK

- データベースユーザにこれらの権限がない場合は、次のコマンドを使用して付与することができます。

- PostgreSQL :

```
CREATE EXTENSION : dblink を作成し、スーパーユーザ権限または dbowner 権限を要求します。その後、次のコマンドを実行して dblink の EXECUTE 権限を付与します。
```

```
GRANT EXECUTE ON FUNCTION DBLINK_CONNECT(text) to &lt;user&gt;;
```



```
GRANT EXECUTE ON FUNCTION DBLINK_CONNECT(text,text) to &lt;user&gt;;
```

• Oracle :

```
GRANT CREATE TABLE TO <user_name>;
```

```
GRANT CREATE PUBLIC DATABASE LINK TO <user_name>;
```

- PostgreSQL 外部データベースを使用している場合は、`pg_hba.conf` ファイルに次のアクセスが設定されていることを確認してください。
 - IM and Presence パブリッシャノードには、各外部データベースへのフルアクセス権が必要です。
 - 外部 PostgreSQL データベースは、各データベースインスタンスへのフルアクセス権を持っている必要があります。たとえば、外部データベースが 192.168.10.1 で設定されている場合、各データベースインスタンスは `pg_hba.conf` ファイルで次のように設定する必要があります。host dbName ユーザ名□192.168.10.0 / 24 パスワード。

手順

-
- ステップ 1** IM and Presence Service パブリッシャノード上の [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] にサインインします。
- ステップ 2** プレゼンス冗長グループの各 IM and Presence Service ノードの [システム (System)] > [サービス (Services)] ウィンドウで Cisco XCP Text Conference Service を停止します。
- ステップ 3** [メッセージング (Messaging)] > [外部データベースの設定 (External Server Setup)] > [外部データベース ジョブ (External Database Jobs)] をクリックします。
- ステップ 4** マージジョブのリストを表示するには、[検索 (Search)] をクリックします。新しいジョブを追加するには、[マージジョブの追加 (Add Merge Job)] を選択します。
- ステップ 5** [外部データベースのマージ (Merging External Databases)] ウィンドウで、次の情報を入力します。
- [データベース タイプ (Database Type)] ドロップダウン リストから [Oracle] または [Postgres] を選択します。
 - マージされたデータを含む 2 つのソース データベースと対象データベースの IP アドレスとホスト名を選択します。
- [データベース タイプ (Database Type)] に [Oracle] を選択した場合、テーブルスペース名とデータベース名を入力します。[データベース タイプ (Database Type)] に [Postgres] を選択した場合、データベース名を指定します。
- ステップ 6** [Feature テーブル (Feature Tables)] ペインで、[Text Conference (TC)] チェックボックスがデフォルトでオンになっています。現在のリリースでは、その他の選択肢はありません。
- ステップ 7** [選択したテーブルの検証 (Validate Selected Tables)] をクリックします。
- (注) Cisco XCP Text Conference サービスが停止していなければ、エラー メッセージが表示されます。サービスが停止していれば、検証は完了します。

- ステップ 8** [検証の詳細 (Validation Details)] ペインにエラーがなければ、[選択したテーブルをマージ (Merge Selected Tables)] をクリックします。
- ステップ 9** マージが正常に完了したら、[外部データベースの検索と一覧表示 (Find And List External Database Jobs)] ウィンドウがロードされます。ウィンドウを更新し、新しいジョブを表示するには、[検索 (Find)] をクリックします。
- ウィンドウを更新し、新しいジョブを表示するには、[検索 (Find)] をクリックします。
- 詳細を表示するには、ジョブの [ID] をクリックします。
- ステップ 10** Cisco XCP Router サービスを再起動します。
- ステップ 11** 両方の IM and Presence Service ノードで Cisco XCP Text Conference Service を開始します。
- ステップ 12** 新しくマージされた外部データベース (対象データベース) をプレゼンス冗長グループに再割り当てする必要があります

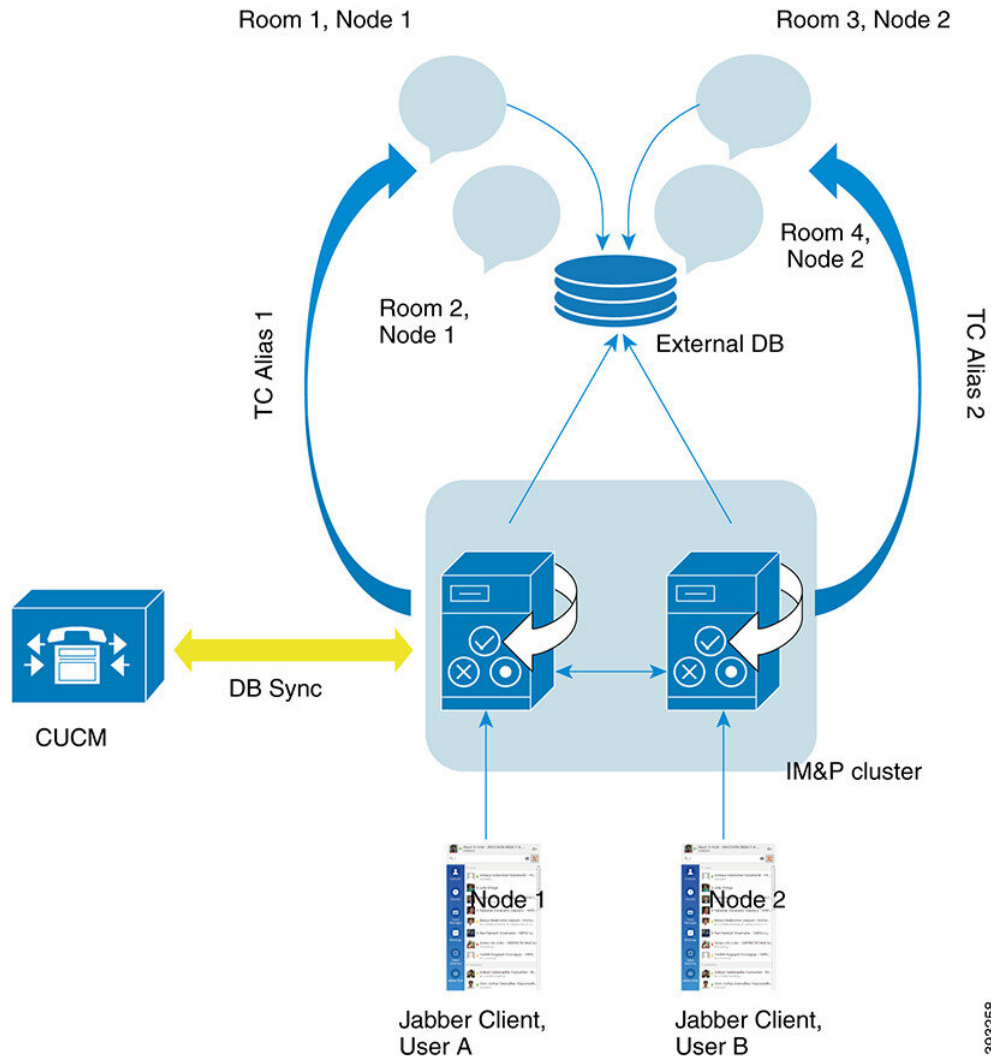
常設チャットにおける高可用性の使用例

次に、フェールオーバーとフェールバックにおける持続チャットの高可用性フローを示します。この例では、2つのノードを持つ IM and Presence クラスタを扱います。IM and Presence クラスタは最大6つのノードを持つことができ、これにより3つのサブクラスタを使用できます。常設チャットルームがすべてのノードでホストされている場合は、3つの独立した外部データベースインスタンスが必要です。



- (注) この機能強化のために、テキスト会議 (TC) サービスは不可欠なサービスとして位置付けられています。その結果、TC の高可用性のフェールオーバーのフローは、ノードの別の重要なサービス (Cisco XCP ルータ サービスなど) の障害によりフェールオーバーが引き起こされたとしても同様になります。

図 7: 持続チャットにおける高可用性の構造



393268

常設チャットにおける高可用性のフェールオーバー使用例

この例では、2つの高可用性（HA）ペアまたはサブクラスタを持つ4つのIM and Presence サービスノードに4人のユーザがいます。ユーザは次のように割り当てられています。

サブクラスタ 1	サブクラスタ 2
<ul style="list-style-type: none"> Andy はノード 1A にいます - ノード 1A はチャットルームをホストしています ボブはノード 1B にいます 	<ul style="list-style-type: none"> キャサリンはノード 2A にいます デボラはノード 2B にいます

- 4人のユーザ全員が、ノード 1A でホストされている同じチャットルームでチャットしています。

2. テキスト会議 (TC) サービスがノード 1A で失敗します。
3. 90 秒後に、Server Recovery Manager (SRM) は TC の重要なサービスの障害を特定し、自動フェールオーバーを開始します。
4. ノード 1B はユーザを 1A から引き継いで、HA の状態 [バックアップモードで実行中 (Running in Backup Mode)] に遷移する前に、[フェールオーバー済み(重要なサービスは非実行) (Failed Over with Critical Services not Running)] 状態に遷移します。
5. HA フェールオーバー モデルに沿って Andy はノード 1A から自動的にサインアウトし、バックアップ ノード 1B にサインインします。
6. 他のユーザは影響を受けませんが、ノード 1B でホストされているチャットルームに引き続きメッセージを投稿します。
7. アンディは持続チャットルームに入り、引き続きメッセージを読んだりルームに送信したりできます。

高可用性常設チャットのフォールバック使用例

この例では、2つの高可用性 (HA) ペアまたはサブクラスタを持つ4つの IM and Presence サービスノードに4人のユーザがいます。ユーザは次のように割り当てられています。

サブクラスタ 1	サブクラスタ 2
<ul style="list-style-type: none"> • Andy はノード 1A にいます-ノード 1A はチャットルームをホストしています • ボブはノード 1B にいます 	<ul style="list-style-type: none"> • キャサリンはノード 2A にいます • デボラはノード 2B にいます

1. 4人のユーザ全員が、ノード 1A でホストされている同じチャットルームでチャットしています。
2. テキスト会議 (TC) サービスがノード 1A で失敗します。
3. ノード 1B はユーザを 1A から引き継いで、HA の状態 [バックアップモードで実行中 (Running in Backup Mode)] に遷移する前に、[フェールオーバー済み(重要なサービスは非実行) (Failed Over with Critical Services not Running)] に遷移します。
4. HA フェールオーバー モデルに沿って Andy が自動的にサインアウトし、バックアップ ノード 1B にサインインします。
5. Bob、Catherine、Deborah は影響を受けませんが、ノード 1B でホストされているチャットルームに引き続きメッセージを投稿します。
6. IM and Presence Service 管理者は、手動フォールバックを開始します。
7. ノード 1A は [テイクバック中 (Taking Back)] に遷移し、ノード 1B は [フォールバック中 (Falling Back)] に遷移します。

8. Andy はノード 1B からサインアウトしました。Bob、Catherine、Deborah は常設チャットルームを使用し、**フォールバック**が発生したらルームはノード 1A に戻ります。
9. ノード 1B は、HA の状態 [**フォールバック中 (Falling Back)**] から [**正常 (Normal)**] に遷移し、そのピア ノード ルームをアンロードします。
10. ノード 1A は、HA の状態 [**テイクバック中 (Taking Back)**] から [**正常 (Normal)**] に遷移し、そのチャットルームをアンロードします。
11. アンディは持続チャットルームに入り、引き続きメッセージを読んだりルームに送信したりできます。



第 18 章

マネージド ファイル転送の設定

- [マネージド ファイル転送の概要 \(239 ページ\)](#)
- [マネージド ファイル転送の前提条件 \(241 ページ\)](#)
- [マネージド ファイル転送のタスク フロー \(244 ページ\)](#)
- [外部ファイルサーバと公開キーのトラブルシューティング \(256 ページ\)](#)
- [マネージド ファイル転送の管理 \(257 ページ\)](#)

マネージド ファイル転送の概要

マネージド ファイル転送 (MFT) を使用すると、Cisco Jabber などの IM and Presence サービス クライアントは他のユーザ、アドホック グループ チャット ルーム、および永続的なチャット ルームにファイルを転送できます。ファイルは外部ファイルサーバのリポジトリに保存され、トランザクションが外部データベースのログに記録されます。

マネージド ファイル転送機能を展開するには、次のサーバも展開する必要があります。

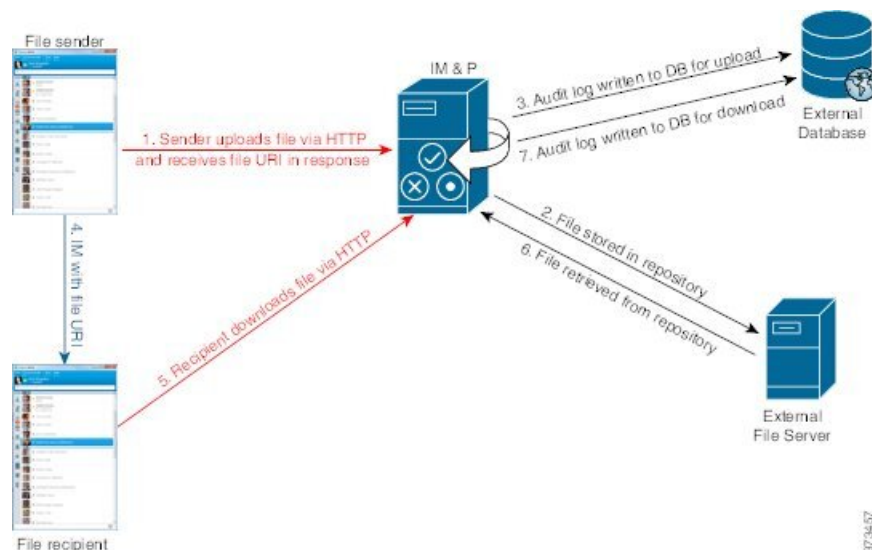
- **外部データベース** - すべてのファイル転送は外部データベースに記録されます。
- **外部ファイルサーバ** - 転送された各ファイルのコピーは、外部ファイルサーバのリポジトリに保存されます。



(注) この設定はファイル転送に固有な設定であり、法規制コンプライアンスのためのメッセージアーカイバ機能には影響しません。

使用例については、[マネージド ファイル転送の通話フロー \(240 ページ\)](#)

マネージドファイル転送の通話フロー



1. 送信者はHTTP経由でファイルをIM and Presence サービス サーバにアップロードし、サーバはファイルのURIを応答として返します。
2. IM and Presence サービスサーバは、ファイルをファイルサーバリポジトリに送信して保存します。
3. IM and Presence サービスは外部データベース ログテーブルに、アップロードを記録する項目を書き込みます。
4. 送信者が受信者にIMを送信します。IMにはファイルのURIが含まれています。
5. 受信者は、IM and Presence Service にファイルのHTTP要求を送信します。IM and Presence サービスはリポジトリからファイルを読み取り (6)、ログテーブルにダウンロードを記録 (7) した後で、ファイルを受信者に送信します。

グループチャットや常設チャットルームにファイルを転送するためのフローもこれと類似していますが、異なる点として送信者はチャットルームにIMを送信し、チャットルームの各参加者は個別にファイルダウンロード要求を送信します。



- (注) ファイルのアップロードが発生すると、そのドメインで使用可能な企業内のすべてのマネージドファイル転送サービスの中からマネージドファイル転送サービスが選択されます。ファイルアップロードは、このマネージドファイル転送サービスを実行しているノードに関連付けられた外部データベースと外部ファイルサーバのログに記録されます。あるユーザがこのファイルをダウンロードすると、この2番目のユーザのホームがどこかにあるかには関係なく、同じマネージドファイル転送サービスがその要求を処理して、同じ外部データベースおよび同じ外部ファイルサーバのログに記録します。

マネージドファイル転送の前提条件

- 外部データベースと外部ファイルサーバも配置する必要があります。
- すべてのクライアントが、割り当てられている IM and Presence Service ノードの完全な FQDN を解決できることを確認してください。これはマネージドファイル転送が機能するために必要です。

外部データベースの前提条件



ヒント

常設チャットやメッセージアーカイブを展開している場合は、すべての機能に同じ外部データベースとファイルサーバを割り当てることができます。サーバの容量を判断する際には、見込まれる IM トラフィック、ファイル転送数、およびファイルサイズを考慮するようにします。

外部データベースをインストールし、設定します。サポートされているデータベースを含む詳細については、*IM and Presence* サービスのデータベース設定ガイドをご覧ください。

さらに、次の注意事項に従ってください。

- IM and Presence サービス クラスタ内の各 IM and Presence サービス ノードに対して 1 つの固有の論理外部データベース インスタンスが必要です。
- 外部データベースは、仮想化プラットフォームと非仮想化プラットフォームの両方でサポートされています。
- ログに記録されるメタデータの完全なリストについては、『*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*』の『外部データベースツール』にある AFT_LOG テーブルを参照してください。
- IPv6 を使用して外部データベースに接続している場合は、[IPv6 の設定 \(35 ページ\)](#) を確認してください。

外部ファイルサーバの要件

外部ファイルサーバをセットアップするときには、次のガイドラインに従ってください。

- ファイルサーバの容量に応じて、各 IM and Presence Service ノードは自身の Cisco XCP ファイル転送ディレクトリを必要としますが、複数のノードで同じ物理ファイルサーバインスタンスを共有できます。
- ファイルサーバは ext4 ファイルシステム、SSHv2、および SSH ツールをサポートする必要があります。
- ファイルサーバは、4.9 ~ 6.x 間の OpenSSH バージョンをサポートする必要があります。

- IM and Presence Service と外部ファイルサーバの間のネットワークスループットは、1秒間に60MBを超えている必要があります。

ファイルサーバの転送速度を判別するために、マネージドファイル転送を有効化した後で、`show fileserver transferspeed` CLI コマンドを使用できます。なお、システムの稼働率が高いときにこのコマンドを実行すると、コマンドから返される値に影響を与えることがあります。このコマンドの詳細については、「*Command Line Interface Guide for Cisco Unified Communications Solutions*」をこのリンクで参照してください。

外部ファイルサーバに対するパーティションの推奨事項

サーバ上で稼働している他のアプリケーションが書き込まないように、ファイル転送ストレージ専用の別のパーティションを1つ以上作成することをシスコでは推奨しています。すべてのファイルストレージディレクトリを、これらのパーティションに作成してください。

次の点に注意してください。

- パーティションを作成する場合、IM and Presence Service のデフォルトファイルサイズ(0)を設定すると、最大4GBまでファイルを転送できることに注意してください。マネージドファイル転送をセットアップするときには、この設定を低い値にすることができます。
- 1日あたりのアップロード数と平均ファイルサイズを考慮してください。
- 予想されるファイル容量を保持するのに十分なディスク領域がパーティションにあることを確認します。
- たとえば12000人のユーザが1時間あたり平均100KBのファイルを2つ転送すると、1日8時間では19.2GBになります。

外部ファイルサーバのディレクトリ構造

次の例に示すように、最初のファイル転送が発生すると、タイムスタンプ付きのサブディレクトリが自動生成されます。

- IM and Presence Service ノード上にパス `/opt/mftFileStore/node_1/` を作成します。
- ディレクトリ `/files/` が自動生成されます。
- 3つの `/chat_type/` ディレクトリ (`im`、`persistent`、`groupchat`) が自動的に生成されます。
- 日付のディレクトリ `/YYYYMMDD/` が自動生成されます。
- 時間のディレクトリ `/HH/` が自動生成されます。1時間以内に1,000個を超えるファイルが転送されると、追加のロールオーバーディレクトリ `/HH.n/` が作成されます。
- ファイルは、自動生成されたエンコードリソース名付きで保存されます（これ以降、`file_name` と表します）。

この例では、ファイルの完全パスは
/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name となります。

この例のパスを使用すると：

- 2014年8月11日 15.00～15.59 UTC に1対1 IM で転送されたファイルは、次のディレクトリに配置されます。
/opt/mftFileStore/node_1/files/im/20140811/15/file_name
- 2014年8月11日 16.00～16.59 UTC に常設グループチャットで転送されたファイルは、次のディレクトリに配置されます。
/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name
- 2014年8月11日 16.00～16.59 UTC にアドホックチャットで転送された1001番目のファイルは、次のディレクトリに配置されます。
/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name
- 1時間単位の中でファイル転送が発生しない場合、その期間にはディレクトリが作成されません。



(注) IM and Presence Service とファイルサーバの間のトラフィックは SSHFS を使用して暗号化されますが、ファイルの内容は、暗号化されていない形式でファイルサーバに書き込まれます。

外部ファイルサーバのユーザー認証

IM and Presence Service は、次のように SSH キーを使用して自身とファイルサーバを認証します。

- IM and Presence Service のパブリック キーはファイルサーバに保存されます。
- SSHFS は、接続中に IM and Presence Service のプライベート キーを検証します。これにより、すべてのファイルの内容が確実に暗号化されます。
- ファイルサーバのパブリック キーは、IM and Presence Service に格納されます。これにより IM and Presence Service は設定済みのファイルサーバに確実に接続し、中間者攻撃を最小限に抑えることができます。



(注) ノードの公開キーはノードの割り当てが解除されると無効になります。ノードが再び割り当てられると、新しいノード公開キーが自動的に生成されます。このキーを外部ファイルサーバで再設定する必要があります。

マネージドファイル転送のタスクフロー

IM and Presence サービスでマネージドファイル転送機能を設定し、外部ファイルサーバを設定するには、次の作業を完了してください。

始める前に

マネージドファイル転送用に外部データベースと外部ファイルサーバの両方を設定します。要件については、

- [外部データベースの前提条件](#) (241 ページ)
- [外部ファイルサーバの要件](#) (241 ページ)

外部データベースの設定方法については、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>でIM and Presence サービスの外部データベース設定ガイドを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	外部データベースの接続の追加 (245 ページ)	IM and Presence サービスからの外部データベースへの接続を設定します。
ステップ 2	外部ファイルサーバのセットアップ (246 ページ)	ファイルサーバ上でユーザ、ディレクトリ、所有、権限、および他のタスクを設定する前に、外部サーバーをセットアップします。
ステップ 3	外部ファイルサーバーのユーザの作成 (247 ページ)	外部ファイルサーバーのユーザのセットアップ
ステップ 4	外部ファイルサーバのディレクトリを設定 (248 ページ)	外部ファイルサーバの最上位ディレクトリ構造を設定します。
ステップ 5	外部ファイルサーバの公開鍵を取得する (249 ページ)	外部ファイルサーバーの公開鍵を取得します。
ステップ 6	IM and Presence Service での外部ファイルサーバのプロビジョニング (250 ページ)	外部ファイルサーバの次の情報を取得します。
ステップ 7	Cisco XCP ファイル転送マネージャのアクティベーションの確認 (253 ページ)	マネージドファイル転送が有効になっている各ノードで、Cisco XCP File Transfer Manager サービスがアクティブである必要があります。

	コマンドまたはアクション	目的
ステップ 8	マネージドファイル転送の有効化 (253 ページ)	IM and Presence サービスでのマネージドファイル転送の有効化
ステップ 9	外部サーバステータスの確認 (256 ページ)	外部データベースの設定と外部ファイルサーバの設定に問題がないことを確認します。

外部データベースの接続の追加

IM and Presence サービスからの外部データベースへの接続を設定します。マネージドファイル転送では、各 IM and Presence Service ノードに対して 1 つの固有の論理外部データベース インスタンスが必要です。

始める前に

各外部データベースをセットアップします。詳細は、*IM and Presence* サービスの外部データベース設定ガイドを参照してください。

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>

手順

- ステップ 1 [Cisco Unified CM IM and Presence 管理 (Cisco Unified CM IM and Presence Administration)] から、[メッセージ (Messaging)] > [外部サーバ設定 (External Server Setup)] > [外部データベース (External Databases)] を選択します。
- ステップ 2 [新規追加 (Add New)] をクリックします。
- ステップ 3 [データベース名 (Database Name)] フィールドに、外部データベースインスタンスの名前を入力します。
- ステップ 4 データベースの種類 ドロップダウンリストから、展開する外部データベースの種類を選択します。
- ステップ 5 データベースのユーザ名とパスワード情報を入力します。
- ステップ 6 [Hostname] フィールドにホストのデータベースのホスト名または IP アドレスを入力します。
- ステップ 7 外部データベース設定ウィンドウの残りの設定を完了します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。
- ステップ 8 [保存 (Save)] をクリックします。
- ステップ 9 この手順を繰り返して、各外部データベースインスタンスへの接続を作成します。

外部ファイルサーバのセットアップ

ファイルサーバ上でユーザ、ディレクトリ、所有、権限、および他のタスクを設定する前に、外部サーバをセットアップします。

始める前に

外部ファイルサーバの設計上の推奨事項を確認してください。詳細については、[外部ファイルサーバの要件 \(241 ページ\)](#) を参照してください。

手順

ステップ 1 サポート対象のバージョンの Linux をインストールします。

ステップ 2 次のいずれかのコマンドを root として入力し、ファイルサーバが SSHv2 および OpenSSH 4.9 以降をサポートしていることを確認します。

```
# telnet localhost 22

Trying ::1...

Connected to localhost.

Escape character is '^]'.

SSH-2.0-OpenSSH_5.3

または

# ssh -v localhost

OpenSSH_5.3p1, OpenSSL 1.0.0-fips 29 Mar 2010

debug1: Reading configuration data /root/.ssh/config ...

...debug1: Local version string SSH-2.0-OpenSSH_5.3

...
```

ステップ 3 プライベート/パブリック キーの認証を許可するには、`/etc/ssh/sshd_config` ファイルで以下のフィールドがはいに設定されていることを確認します。

- `RSAAuthentication` はい
- `PubkeyAuthentication` はい

ファイル内でこれらの行をコメントアウトした場合、設定をそのまま保持することが可能です。

ヒント また、セキュリティを強化するために、ファイル転送ユーザ（この例では `mftuser`）に対してパスワードログインを無効にすることもできます。これにより、必ず SSH のパブリック/プライベート キー認証によってログインされるようになります。

ステップ 4 サーバ上で稼動している他のアプリケーションが書き込まないように、ファイル転送ストレージ専用の別のパーティションを1つ以上作成することをシスコでは推奨しています。すべてのファイルストレージディレクトリを、これらのパーティションに作成してください。

次のタスク

[外部ファイルサーバーのユーザの作成 \(247 ページ\)](#)

外部ファイルサーバーのユーザの作成

外部ファイルサーバーのユーザのセットアップ

始める前に

[外部ファイルサーバのセットアップ \(246 ページ\)](#)

手順

ステップ 1 root としてファイルサーバ上で、マネージドファイル転送機能のユーザを作成します。このユーザは、ファイルストレージのディレクトリ構造（この例では `mftuser` を使用）を所有し、ホームディレクトリを強制的に作成します（`-m`）。

```
# useradd -m mftuser
```

```
# passwd mftuser
```

ステップ 2 マネージドファイル転送ユーザに切り替えます。

```
# su mftuser
```

ステップ 3 `~mftuser` ホームディレクトリの下に、キーストアとして使用する `.ssh` ディレクトリを作成します。

```
$ mkdir ~mftuser/.ssh/
```

ステップ 4 `.ssh` ディレクトリの下に `authorized_keys` ファイルを作成します。このファイルは、マネージドファイル転送が有効になっている各ノードについて、パブリックキーを保持するのに使われます。

```
$ touch ~mftuser/.ssh/authorized_keys
```

ステップ 5 パスワードを使用しない SSH が機能するように、正しい権限を設定します。

```
$ chmod 700 ~mftuser (directory)
```

```
$ chmod 700 ~/.ssh (directory)
```

```
$ chmod 700 ~/.ssh/authorized_keys (file)
```

(注) いくつかのLinuxシステムでは、SSHの設定によってこれらの権限が異なることがあります。

次のタスク

[外部ファイルサーバのディレクトリを設定 \(248 ページ\)](#)

外部ファイルサーバのディレクトリを設定

外部ファイルサーバの最上位ディレクトリ構造を設定します。

任意のディレクトリ名を付けて、任意のディレクトリ構造を作成することができます。マネージドファイル転送が有効になっている各ノード用にディレクトリを必ず作成してください。後で、IM and Presence Service でマネージドファイル転送を有効にするときに、各ディレクトリをノードに割り当てる必要があります。



重要 マネージドファイル転送が有効になっている各ノード用に1つのディレクトリを作成する必要があります。



(注) ファイルサーバのパーティション/ディレクトリは、ファイルの格納に使用される IM and Presence Service ディレクトリにマウントされます。

始める前に

[外部ファイルサーバーのユーザの作成 \(247 ページ\)](#)

手順

ステップ 1 root ユーザーに切り替えます。

```
$ exit
```

ステップ 2 マネージドファイル転送が有効になっている IM and Presence Service のすべてのノードのディレクトリを格納するために、最上位のディレクトリ構造（この例では /opt/mftFileStore/）を作成します。

```
# mkdir -p /opt/mftFileStore/
```

ステップ 3 /opt/mftFileStore/ の占有者として *mftuser* を指定します。

```
# chown mftuser:mftuser /opt/mftFileStore/
```


ステップ 4 `mftuser` に、`mftFileStore` ディレクトリに対する占有権を付与します。

```
# chmod 700 /opt/mftFileStore/
```

ステップ 5 `mftuser` に切り替えます。

```
# su mftuser
```

ステップ 6 マネージドファイル転送が有効になっている各ノードに関して、`/opt/mftFileStore/` の下にサブディレクトリを作成します（後で、マネージドファイル転送を有効にするときに各ディレクトリを1つのノードに割り当てます）。

```
$ mkdir /opt/mftFileStore/{node_1,node_2,node_3}
```

- (注)
- これらのディレクトリとパスは、**外部ファイルサーバディレクトリ**フィールドで使用され、**Cisco Unified CM IM and Presence Administration** でファイルサーバをプロビジョニングするときに設定します。
 - 複数の **IM and Presence Service** ノードがこのファイルサーバに書き込む場合は、前述の例で3つのノード `{node_1,node_2,node_3}` に設定したように、各ノードのターゲットディレクトリを定義する必要があります。
 - 各ノードのディレクトリ内では、転送タイプのサブディレクトリ (`im`、`groupchat`、および `persistent`) が **IM and Presence Service** によって自動的に作成されます。その後のすべてのディレクトリも同様です。

次のタスク

[外部ファイルサーバの公開鍵を取得する \(249 ページ\)](#)

外部ファイルサーバの公開鍵を取得する

外部ファイルサーバーの公開鍵を取得します。

始める前に

[外部ファイルサーバのディレクトリを設定 \(248 ページ\)](#)

手順

ステップ 1 ファイルサーバのパブリック キーを取得するには、次のように入力します。

```
$ ssh-keyscan -t rsa host
```

`host` はファイルサーバのホスト名、FQDN、または IP アドレスです。

- 警告**
- ファイル サーバのパブリック キーをスプーフィングする「中間者攻撃」を防ぐには、`ssh-keyscan -t rsa host` コマンドで返されるパブリック キーの値が、ファイル サーバの実際のパブリック キーであることを確認する必要があります。
 - ファイル サーバで、（このシステムでは `/etc/ssh/` の下にある）`ssh_host_rsa_key.pub` ファイルの場所へ移動し、パブリック キー ファイルの内容と、`ssh-keyscan -t rsa host` コマンドで返されたパブリック キー値を比べて、ホスト以外の部分が一致することを確認してください（ファイル サーバの `ssh_host_rsa_key.pub` ファイルにはホストが存在しません）。

ステップ 2 `ssh_host_rsa_key.pub` ファイルの内容ではなく、`ssh-keyscan -t rsa host` コマンドの結果をコピーします。サーバのホスト名、FQDN、または IP アドレスから最後まで、キー値全体を必ずコピーしてください。

(注) ほとんどの場合、サーバのキーはホスト名または FQDN で始まりますが、IP アドレスで始まることもあります。

たとえば、次の内容をコピーします。

```
hostname ssh-rsa AAAQEAzRevlQCH1KFAhXwhd5UvEFzJs...
...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ==
```

(... を追加)。

ステップ 3 `ssh-keyscan -t rsa host` コマンドの結果をテキストファイルに保存します。これは、「*IM and Presence Service* での外部ファイル サーバの展開」の手順でファイル サーバを設定するときに必要になります。

ステップ 4 作成した `authorized_keys` ファイルを開き、開いたままにしておきます。後で、IM and Presence サービスでファイルサーバをプロビジョニングするときに、必要になります。

(注) 公開鍵を取得できない場合は、[外部ファイルサーバと公開キーのトラブルシューティング \(256 ページ\)](#) で詳細なヘルプを参照してください。

次のタスク

[IM and Presence Service での外部ファイル サーバのプロビジョニング \(250 ページ\)](#)

IM and Presence Service での外部ファイル サーバのプロビジョニング

マネージド ファイル転送を有効にするクラスタ内の各ノードについて、1 つの外部ファイル サーバインスタンスを設定する必要があります。

外部ファイル サーバインスタンスは、外部ファイル サーバの物理インスタンスである必要はありません。ただし、ある 1 つのホスト名に関して、それぞれの外部ファイル サーバインスタンス用に一意の外部ファイルサーバディレクトリパスを指定する必要があります。同じノードから、すべての外部ファイル サーバインスタンスを設定できます。

始める前に

[外部ファイルサーバの公開鍵を取得する \(249 ページ\)](#)

外部ファイルサーバの次の情報を取得します。

- ホスト名、FQDN、または IP アドレス
- パブリック キー
- ファイルストレージディレクトリへのパス
- ユーザ名 (User name)

手順

-
- ステップ 1** [Cisco Unified CM IM and Presence 管理 (Cisco Unified CM IM and Presence Administration)] で、[メッセージ (Messaging)] > [外部サーバ設定 (External Server Setup)] > [外部ファイルサーバ (External File Servers)] を選択します。
- ステップ 2** [新規追加 (Add New)] をクリックします。
[外部ファイルサーバ (External File Servers)] ウィンドウが表示されます。
- ステップ 3** サーバの詳細を入力します。フィールドとその設定オプションの詳細については、[外部ファイルサーバフィールド \(251 ページ\)](#) を参照してください。
- ステップ 4** [保存 (Save)] をクリックします。
- ステップ 5** マネージドファイル転送が有効になっているクラスターノードごとに別々の外部ファイルサーバインスタンスを作成するまで、この手順を繰り返します。
-

次のタスク

[Cisco XCP ファイル転送マネージャのアクティベーションの確認 \(253 ページ\)](#)

外部ファイルサーバフィールド

フィールド	説明
名前	ファイルサーバの名前を入力します。すぐに識別できるよう、サーバ名はできるだけ説明的な名前にしてください。 最大文字数は 128 文字です。使用できる文字は英数字、ダッシュ、および下線文字です。

フィールド	説明
ホスト/IP アドレス (Host/IP Address)	<p>ファイルサーバのホスト名または IP アドレスを入力します。</p> <p>(注)</p> <ul style="list-style-type: none"> • [ホスト/IPアドレス (Host/IP Address)]フィールドに入力する値は、下記の [外部ファイルサーバパブリックキー (External File Server Public Key)]フィールドで指定するキーの先頭部分と一致する必要があります。 • この設定を変更した場合は、Cisco XCP Router サービスを再起動する必要があります。
外部ファイルサーバパブリックキー (External File Server Public Key)	<p>ファイルサーバのパブリックキー (テキストファイルに保存するよう指示されたキー) を、このフィールドに貼り付けます。</p> <p>キーを保存しなかった場合は、次のコマンドを実行してファイルサーバからそれを取得できます。</p> <pre>\$ ssh-keyscan -t rsa host</pre> <p>(ファイルサーバ上で) <i>host</i> は、ファイルサーバの IP アドレス、ホスト名、または FQDN です。</p> <p>ホスト名、FQDN、または IP アドレスから始まって末尾まで、キーのテキスト全体をコピー/ペーストする必要があります。たとえば、次の内容をコピーします。</p> <pre>extFileServer.cisco.com ssh-rsa AAAQEAzRevlQCH1KFAAnXwhd5UvEFzJs... ...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ==</pre> <p>(... を追加)。</p> <p>重要 この値は必ず、[ホスト/IPアドレス (Host/IP Address)]フィールドに入力したホスト名、FQDN、または IP アドレスで始まる必要があります。たとえば [ホスト/IPアドレス (Host/IP Address)]フィールドで <code>extFileServer</code> が使用されている場合は、このフィールドの先頭部分は <code>extFileServer</code> となり、その後に <code>rsa</code> キー全体が続きます。</p>
外部ファイルサーバディレクトリ (External File Server Directory)	<p>ファイルサーバディレクトリ階層の最上位のパス (例: <code>/opt/mftFileStore/node_1/</code>)。</p>
ユーザ名 (User Name)	<p>外部ファイルサーバ管理者のユーザ名。</p>

Cisco XCP ファイル転送マネージャのアクティベーションの確認

マネージドファイル転送が有効になっている各ノードで、Cisco XCP File Transfer Manager サービスがアクティブである必要があります。

このサービスが開始可能なのは、外部データベースと外部ファイルサーバがすでに割り当てられており、しかもサービスがデータベースに接続してファイルサーバをマウントできる場合だけです。

始める前に

[IM and Presence Service](#) での外部ファイルサーバのプロビジョニング (250 ページ)

手順

- ステップ 1** クラスタ内のいずれかのノードで [Cisco Unified IM and Presenceのサービスアビリティ (Cisco Unified IM and Presence Serviceability)] ユーザ インターフェイスにログインします。
- ステップ 2** [ツール (Tools)] > [サービス アクティベーション (Service Activation)] を選択します。
- ステップ 3** サーバド롭ダウンから、マネージドファイル転送が有効になっているノードを選択し、[移動 (Go)] をクリックします。
- ステップ 4** Cisco XCP ファイル転送マネージャサービスのアクティベーションステータスが起動済であることを確認します。
- ステップ 5** サービスが無効になっている場合は、Cisco XCP ファイル転送マネージャチェックボックスをチェックして、保存するをクリックします。
- ステップ 6** マネージドファイル転送が有効になっているすべてのノードで、この手順を繰り返します。

次のタスク

[マネージドファイル転送の有効化](#) (253 ページ)

マネージドファイル転送の有効化

IM and Presence サービスでのマネージドファイル転送の有効化

手順

- ステップ 1** Cisco Unified CM IM and Presence Administration にサインインし、[メッセージング (Messaging)] > [ファイル転送 (File Transfer)] を選択します。[ファイル転送 (File Transfer)] ウィンドウが開きます。
- ステップ 2** [ファイル転送設定 (File Transfer Configuration)] エリアで、展開に応じて [マネージドファイル転送 (Managed File Transfer)] または [マネージドおよびピアツーピアファイル転送

(**Managed and Peer-to-Peer File Transfer**)] のいずれかを選択します。 [ファイル転送オプション \(255 ページ\)](#) を参照してください

ステップ 3 [最大ファイルサイズ (Maximum File Size)] を入力します。 0 を入力すると、最大サイズ (4 GB) が適用されます。

(注) この変更を有効にするには、Cisco XCP Router サービスを再起動する必要があります。

ステップ 4 [マネージドファイル転送の割り当て (Managed File Transfer Assignment)] エリアで、クラスタの各ノードに対して外部データベースと外部ファイル サーバを割り当てます。

- a) 外部データベース : ドロップダウンリストから、外部データベースの名前を選択します。
- b) 外部ファイル サーバ : ドロップダウン リストから、外部ファイル サーバの名前を選択します。

ステップ 5 [保存 (Save)] をクリックします。

[保存 (Save)] をクリックすると、それぞれの割り当てに対して [ノードパブリックキー (Node Public Key)] リンクが表示されます。

ステップ 6 マネージド ファイル転送が有効になるクラスタ内の各ノードについて、ノードのパブリックキー全体を外部ファイル サーバの `authorized_keys` ファイルにコピーする必要があります。

- a) ノードのパブリックキーを表示するには、[マネージドファイル転送の割り当て (Managed File Transfer Assignment)] エリアをスクロールダウンして [ノードパブリックキー (Node Public Key)] リンクをクリックします。ノードの IP アドレス、ホスト名、FQDN を含めて、ダイアログボックスの内容全体をコピーします。

例 :

```
ssh-rsa
yc2EAAAABIwAAAQEA...
...5s+tusrtBBuciCkH5gfXwrsFS000AlfFvwnfq1xmKmIS9W2rf0Qp+A+G4MVpTxHgaonw== imp@imp_node
```

(... を追加) 。

- 警告**
- マネージドファイル転送機能が設定されている場合、[ファイル転送タイプ (File Transfer Type)] が [無効 (Disabled)] または [ピアツーピア (Peer-to-Peer)] に変更されると、マネージドファイル転送のすべての設定が削除されます。
 - 外部データベースおよびファイル サーバからノードが割り当て解除されると、ノードのキーは無効になります。

- b) 外部ファイル サーバ上で、`mftuser` のホームディレクトリの下に作成した `~mftuser/.ssh/authorized_keys` ファイルがまだ開いていない場合は、これを開いて、(新しい行で) 各ノードのパブリックキーを付加します。

(注) `authorized_keys` ファイルには、ファイルサーバに割り当てられている、マネージドファイル転送が有効な各 IM and Presence Service ノードのパブリックキーが含まれる必要があります。

- c) `authorized_keys` ファイルを保存して閉じます。

- ステップ7** (オプション) マネージドファイル転送サービスパラメータを設定して、外部ファイルサーバのディスク領域に関する RTMT アラートが生成されるしきい値を定義します。
- ステップ8** マネージドファイル転送が有効になっているすべてのノード上で、Cisco XCP Router を再起動します。『Cisco XCP Router サービスの再起動』を参照してください。

次のタスク

[外部サーバステータスの確認 \(256 ページ\)](#)

ファイル転送オプション

次のいずれかのファイル転送オプションを[ファイル転送 (File Transfer)]ウィンドウで設定できます。

ファイル転送オプション	説明
Disabled	クラスタのファイル転送が無効です。
ピアツーピア	[ピアツーピア (Peer-to-Peer)]のファイル転送は許可されますが、サーバではファイルのアーカイブや保存が行われません。グループチャットのファイル転送はサポートされません。
マネージドファイル転送	1対1およびグループのファイル転送が許可されます。ファイル転送がデータベースのログに記録され、転送されたファイルはサーバに保存されます。クライアントがマネージドファイル転送をサポートしている必要もあります。そうでない場合、ファイル転送は許可されません。
マネージドファイル転送およびピアツーピアファイル転送	1対1およびグループのファイル転送が許可されます。ファイル転送がデータベースのログに記録され、転送されたファイルはサーバに保存されます (ただしクライアントがマネージドファイル転送をサポートする場合のみ)。クライアントがマネージドファイル転送をサポートしていない場合、このオプションはピアツーピアオプションと同等になります。



- (注) マネージドファイル転送がノードで設定されていて、ファイル転送タイプを無効またはピアツーピアに変更した場合は、そのノードの外部データベースと外部ファイルサーバにマップされた設定が削除されることに注意してください。データベースとファイルサーバの設定は残りますが、そのノードでマネージドファイル転送を再び有効にする場合は、データベースとファイルサーバの再割り当てが必要になります。

IM and Presence Service リリース 10.5(2) 以降にアップグレードすると、アップグレード前の設定に応じて、無効またはピアツーピアが選択されます。

外部サーバステータスの確認

外部データベースの設定と外部ファイルサーバの設定に問題がないことを確認します。

始める前に

[マネージドファイル転送の有効化 \(253 ページ\)](#)

手順

-
- ステップ 1** 外部データベースのステータスを確認するには
- [Cisco Unified CM IM and Presence 管理 (Cisco Unified CM IM and Presence Administration)] で、[メッセージ (Messaging)] > [外部サーバ設定 (External Server Setup)] > [外部データベース (External Databases)] を選択します。
 - [外部データベースのステータス (External Database Status)] エリアに示される情報を確認します。
- ステップ 2** 外部ファイルサーバが割り当てられたことを確認する必要がある IM and Presence Service ノードで、次のようにします。
- [Cisco Unified CM IM and Presence 管理 (Cisco Unified CM IM and Presence Administration)] で、[メッセージ (Messaging)] > [外部サーバ設定 (External Server Setup)] > [外部ファイルサーバー (External File Servers)] を選択します。
 - [外部ファイルサーバのステータス (External File Server Status)] エリアに示される情報を確認して、接続に問題がないことを確認します。
-

外部ファイルサーバと公開キーのトラブルシューティング

サーバのプライベート/パブリック キー ペアが生成される時、プライベート キーは通常、`/etc/ssh/ssh_host_rsa_key` に書き込まれます。

パブリック キーは `/etc/ssh/ssh_host_rsa_key.pub` に書き込まれます。

これらのファイルがない場合は、以下の手順に従ってください。

手順

ステップ 1 次のコマンドを入力します。

```
$ ssh-keygen -t rsa -b 2048
```

ステップ 2 ファイル サーバのパブリック キーをコピーします。

ホスト名、FQDN、またはIPアドレスから、パブリック キーのテキストの文字列全体をコピーする必要があります（例：`hostname ssh-rsa AAAAB3NzaC1yc...`）。ほとんどのLinux環境では、サーバのホスト名またはFQDNがキーに含まれています。

ヒント `$ ssh-keygen -t rsa -b 2048` コマンドの出力にホスト名が含まれていない場合は、代わりに `$ ssh-keyscan hostname` コマンドの出力を使用します。

ステップ 3 このファイルサーバを使用するように設定されているIM and Presence Serviceの各ノードについて、[外部ファイルサーバ設定 (External File Server Configuration)] ウィンドウの[外部ファイルサーバパブリックキー (External File Server Public Key)] フィールドにパブリック キーを貼り付けてください。

重要 マネージドファイル転送機能には、パスワードを使用しないSSHを設定する必要があります。パスワードを使用しないSSHを設定する手順の詳細については、SSHDマニュアル ページを参照してください。

(注) パブリッシャ ノードからサブスクリバ ノードにステータスを確認するとき、および逆方向に確認するとき、「この外部ファイルサーバ用の診断テストは次から実行される場合があります (The diagnostics tests for this External File Server may be run from here.)」という情報メッセージが表示されます。

ログに「pingable」:「-7」と表示されます。これは、外部ファイルサーバが構成されていない他のノードのステータスを表示していることを意味します。

パブリッシャノードに外部ファイルサーバを設定し、パブリッシャノードの公開鍵は外部ファイルサーバの「Authorized_key」で共有されます。ファイル。

マネージド ファイル転送の管理

マネージドファイル転送を設定した後は、機能を継続的に管理する必要があります。たとえば、ファイルサーバとデータベースの増加を管理するためのシステムを整備する必要があります。



第 19 章

複数のデバイスのメッセージングの設定

- [マルチデバイスメッセージングの概要 \(259 ページ\)](#)
- [複数デバイスのメッセージングの前提条件 \(260 ページ\)](#)
- [複数のデバイスのメッセージングの設定 \(260 ページ\)](#)
- [マルチデバイスメッセージングのフローの使用例 \(261 ページ\)](#)
- [マルチデバイスメッセージングにおける静音モードの使用例 \(261 ページ\)](#)
- [マルチデバイスメッセージングのインタラクションと制限 \(262 ページ\)](#)
- [複数のデバイスのメッセージングのカウンタ \(263 ページ\)](#)
- [デバイス容量のモニタリング \(264 ページ\)](#)
- [デバイス キャパシティ モニタリングのユーザセッションレポート \(266 ページ\)](#)

マルチデバイスメッセージングの概要

マルチデバイスメッセージング (MDM) により、現在サインインしているすべてのデバイス間で追跡される、1対1のインスタントメッセージ (IM) 交換が実現します。デスクトップクライアントとモバイルデバイスを使用し、どちらも MDM が有効な場合、メッセージは両方のデバイスに送信されるか、または CC で送信されます。既読通知は、会話の参加中に両方のデバイスで継続的に同期されます。

MDM を使用すると、デバイス間を移動しながら IM 会話を維持できます。たとえばデスクトップコンピュータから IM 会話を開始し、会議のためにデスクから離れる必要があるばあい、モバイルデバイスでその会話を続けることができます。MDM 対応にするには、クライアントはサインインする必要があります。サインアウトしたクライアントには、送受信された IM および通知は表示されません。

MDM は、モバイルデバイスのバッテリーを節約できる静音モードをサポートします。Jabber クライアントは、モバイルクライアントが使用されていないときは自動的に静音モードに切り替わります。静音モードはクライアントが再びアクティブになるとオフになります。

複数デバイスのメッセージングの前提条件

インスタントメッセージングを有効にする必要があります。詳細については、次を参照してください。



- (注) Multiple Device Messaging を有効にする場合は、各ユーザが複数の Jabber クライアントを持つ可能性があるため、ユーザ数ではなくクライアント数に応じた展開にします。たとえば、ユーザ数が 25,000 人で、各ユーザが 2 台の Jabber クライアントを保持している場合、導入環境には 5 万ユーザのキャパシティが必要となります。

複数のデバイスのメッセージングの設定

マルチデバイスメッセージングはデフォルトで有効になっています。この手順を使用して、機能を無効にしたり、無効にした後に再び有効にしたりできます。

手順

- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。
- ステップ 2 [サーバ (Server)] ドロップダウンリストから、[IM and Presence サービス パブリッシャ (IM and Presence Service Publisher)] ノードを選択します。
- ステップ 3 [サービス (Service)] ドロップダウンリストから、[Cisco XCP ルータ (アクティブ) (Cisco XCP Router (Active))] を選択します。
- ステップ 4 マルチデバイスメッセージングを有効にするドロップダウンリストから有効 (デフォルト値) または無効を選択します。
- ステップ 5 [保存 (Save)] をクリックします。
- ステップ 6 Cisco XCP Router サービスを再起動します。
 - a) Cisco Unified IM and Presence Serviceability にログインして、[ツール (Tools)] > [コントロールセンタ - ネットワーク サービス (Control Center - Network Services)] を選択します。
 - b) [サーバ (Server)] ドロップダウンリストボックスから IM and Presence パブリッシャ ノードを選択します。
 - c) [IM and Presence サービス (IM and Presence Services)] の下で、[Cisco XCP ルータ (Cisco XCP Router)] を選択し、[リスタート(Restart)] をクリックします

マルチ デバイス メッセージングのフローの使用例

このフローでは、ユーザ (Alice) がラップトップとモバイルデバイスで MDM を有効化した際にメッセージと通知がどのように処理されるかについて説明しています。

1. Alice はラップトップ上で Jabber クライアントを開いており、モバイルデバイスでも Jabber を使用しています。

2. Alice は Bob からインスタントメッセージ (IM) を受け取ります。

Alice のラップトップが通知を受信すると、新しいメッセージインジケータが表示されます。モバイルデバイスには通知ではなく、新しいメッセージとして表示されます。



(注) IM は必ずすべての MDM 対応クライアントに一齐送信されます。通知はアクティブな Jabber クライアントにのみ表示されます。アクティブな Jabber クライアントがない場合は、すべての Jabber クライアントに通知が送信されます。

3. Alice は 20 分間 Bob とチャットしました。

ラップトップでチャットする一方、モバイルデバイスでは新しいメッセージを受信し、既読として処理されます。モバイルデバイスには通知が送信されません。

4. Alice は 3 人目のユーザ (Colin) から 3 通のチャットメッセージを受信します。この際も Alice のデバイスはステップ 2 と同じように動作します。

5. Colin からのメッセージには応答せず、ラップトップを閉じます。帰路で Alice は Bob から別のメッセージを受信します。

この状況では、ラップトップとモバイルデバイスの両方で新しいメッセージを受信し、通知を表示します。

6. Alice はモバイルデバイスを開き、Bob と Colin から送信された新しいメッセージを見つけます。これらのメッセージはラップトップにも送済みです。

7. Alice がモバイルデバイスでメッセージを読むと、メッセージはラップトップとモバイルデバイスの両方で既読になります。

マルチデバイスメッセージングにおける静音モードの使用例

このフローでは、モバイルデバイス上でマルチデバイスメッセージングが静音モードを有効にする手順について説明します。

1. Alice は、ラップトップとモバイルデバイスで Jabber を使用しています。Bob からのメッセージを読み、ラップトップ上の Jabber から返信します。

2. モバイルデバイスで別のアプリケーションを使い始めます。ここで Jabber はバックグラウンドで動作し続けます。
3. Jabber がバックグラウンドで実行している間、静音モードは自動的に有効になります。
4. Bob が Alice に別のメッセージを送信します。Alice のモバイルデバイスでは Jabber が静音モードにあるため、メッセージは配信されません。Alice から Bob への応答メッセージはバッファとして保存されます。
5. メッセージのバッファリングは、次のトリガーイベントのいずれかが発生するまで続きます。
 - <iq> スタンザが受信される。
 - 他の Alice のデバイスでアクティブなクライアントがない場合に、<message> スタンザが受信される。



(注) アクティブなクライアントとは、過去 5 分間に、使用可能なプレゼンス ステータスまたはインスタント メッセージのいずれかを送信した最後のクライアントのことです。

- バッファの制限に達した。

6. Alice がモバイルデバイスの Jabber に戻ると、再びアクティブになります。バッファとして保存された Bob のメッセージが配信され、Alice から閲覧可能になります。

マルチデバイスメッセージングのインタラクションと制限

次の表は、マルチデバイスメッセージング (MDM) 機能との機能の相互作用および制限事項をまとめたものです。

表 24: マルチデバイスメッセージングのインタラクションと制限

機能	連携動作または制限事項
Cisco Jabber Clients	MDM はバージョン 11.7 以降のすべての Jabber クライアントによりサポートされます。
グループ チャット	グループチャットはチャットルームに参加したデバイスでのみ使用できます。
メッセージアーカイバ	MDM は Message Archiver 機能と互換性があります。
マネージドファイル転送	ファイル転送は、アクティブデバイスでのみ使用できます。

機能	連携動作または制限事項
Expressway を介したモバイルおよびリモートアクセス	Cisco Expressway 経由で IM and Presence サービスに接続するモバイルおよびリモートアクセスクライアントの場合、MDM を使用するには少なくとも Expressway X8.8 を実行している必要があります。
Server Recovery Manager	フェールオーバーが発生した場合、マルチデバイスメッセージング機能により、IM and Presence サービスでサーバ回復に遅延が発生します。マルチデバイスメッセージングが設定されているシステムでサーバのフェールオーバーが発生すると、通常、 [Cisco Server Recovery Manager] サービスパラメータで指定された時間の 2 倍かかります。
サードパーティ製クライアント	MDM は、この機能をサポートしていないサードパーティ製クライアントと互換性があります。

複数のデバイスのメッセージングのカウンタ

マルチデバイスメッセージング (MDM) は、Cisco XCP MDM カウンタグループから次のカウンタを使用します。

カウンタ名	説明
MDMSessions	MDM が有効な現在のセッション数。
MDMSilentModeSessions	サイレントモードにおける現在のセッション数。
MDMQuietModeSessions	静音モードにおける現在のセッション数。
MDMBufferFlushes	MDM バッファフラッシュの合計数。
MDMBufferFlushesLimitReached	バッファサイズ全体の上限に到達したことで発生した MDM バッファフラッシュの合計数。
MDMBufferFlushPacketCount	最後のタイムスライスでフラッシュされたパケットの数。
MDMBufferAvgQueuedTime	MDM バッファがフラッシュされるまでの平均時間 (秒)。

デバイス容量のモニタリング

Multiple Device Messaging (MDM) を有効にすると、複数のデバイスからログインする各ユーザにより、IM and Presence サーバのトラフィック負荷が増加します。アクティブなログインユーザ数が一定の上限に達すると、リソース不足（メモリ消費や CPU 使用率の上昇）のために予期しないパフォーマンスの問題やエラーが発生することになります。

これらの問題に対処するには、デバイス キャパシティ モニタリング機能が役立ちます。この機能は、ノードで作成されたセッション数のモニタリングを支援する追加のカウンタを実装します。

IM & P ノードでは、次の Jabber Session Manager (JSM) セッションが作成されます。

- 構築された JSM セッション：ユーザがノードに割り当てられたときに作成されます。
- アクティブ JSM セッション
 - オンプレミスのユーザ ログイン。
 - オフプレミスのユーザ ログイン。
- ファントム JSM セッション：プッシュが有効なユーザに対して作成され、HA フェールオーバーのユースケースを処理します。
- Spark 相互運用 JSM セッション：ハイブリッドユーザに対して作成されます。

JSM セッションを監視するために、次のカウンタが導入されます。

- **JsmClientSessionsActive**
- **JsmPhantomSessionsActive**
- **JsmHybridSessionsActive**

さらに、JSM のしきい値を監視する新しいカウンタ **JSMSessionsExceedsThreshold** が導入されます。これは、JSM セッションカウンタと OVA サイズに基づいて計算されます。

このカウンタのしきい値制限がデフォルト値の 80% を超過して 10 分間が経過すると、システムはリアルタイム監視ツール (RTMT) で「**JSMSessionsExceedsThreshold**」アラートを発生させます。

RTMT を使用したアラート値の設定

RTMT を使用して **JSMSessionsExceedsThreshold** アラート値を設定するには、次の手順を使用します。

手順

- ステップ 1** リアルタイム監視ツール (RTMT) にログインし、[システム (System)] > [ツール (Tools)] > [Alert Central] を選択します。
- ステップ 2** [IM and Presence] をクリックし、**JSMSessionsExceedsThreshold** というアラート名を選択します。
- ステップ 3** [**JSMSessionsExceedsThreshold**] を右クリックし、[アラート/プロパティの設定 (Set Alert/Properties)] を選択します。

- ステップ 4** アラートを有効にするには、[アラートの有効化 (Enable Alert)] チェックボックスをオンにします。
- ステップ 5** JSM セッション数のしきい値超過のパーセンテージ制限を設定します。デフォルト値は 80% です。
- ステップ 6** [保存 (Save)] をクリックします。
- ステップ 7** アラートの頻度とスケジュールを設定します。デフォルトでは、アラートは 10 分ごとにトリガーされます。
- ステップ 8** [次へ (Next)] をクリックします。
- ステップ 9** [保存 (Save)] をクリックします。

ノードあたりの JSM セッションのサポート

次の表は、ノードあたりにサポート可能な JSM セッションの総数をテストに基づいて示しています。

OVA サイズ	JSM セッションカウントは OVA キャパシティの 1.5 倍
5K OVA	7.5K
15,000 OVA	22.5 k
25K OVA	37.5 k



- (注) 高可用性が有効になっていて、両方のノードがアクティブ-アクティブ構成にある場合は、次のようになります。
1. カスタムアラームはノードごとにしか設定できないという制限があるため、ノードあたりのサポート可能な JSM セッションの総数は、上記の容量の 50% になります。
 2. HA 設定に基づいて JSM Sessions Exceeds Threshold カウンタ値を変更する必要があります。

推奨措置：

カスタムアラートが生成された場合は、その特定のノードについて、RTMT ツールのメモリおよび CPU 使用率のカウンタを確認します。メモリと CPU 使用率のカウンタの値がしきい値制限を超える場合は、IM & P ノード間でユーザのロードバランスを行うことをお勧めします。現在、IM & P には、ノード間でユーザを自動的にロードバランシングするメカニズムがありません。

デバイス キャパシティ モニタリングのユーザ セッション レポート

ユーザ セッション レポートを表示するには、この手順を使用します。このレポートでは、クラスタ、サブクラスタ、およびノードレベルの複数のデバイスからログインしているアクティブユーザの詳細を確認できます。

手順

- ステップ 1 Cisco Unified IM and Presence Reporting にログインします。
- ステップ 2 [システムレポート (System Reports)] > [IM and Presence ユーザセッションレポート (IM and Presence User Sessions Report)] を選択します。
- ステップ 3 レポート ウィンドウで [レポートの生成 (Generate Report)] (棒グラフ) アイコンを選択して、現在の時刻のユーザセッション レポートを生成します。
- ステップ 4 [OK] をクリックします。
- ステップ 5 [レポート名 (Report Name)] 列で、[IM and Presence ユーザセッションレポート (IM and Presence User Sessions Report)] をクリックします。
 - (注)
 - このレポートの生成には、およそ 2 分以上かかることがあります。
 - このレポートには、プレゼンス冗長グループ、ノード名、1 つ以上のデバイスからログインしているユーザの数、クラスタ、サブクラスタ、およびノードレベルのセッションの合計数が、レポートの生成日時と共に表示されます。
- ステップ 6 [レポート (Reports)] ウィンドウの右側にある [ダウンロード (download)] (緑の矢印) アイコンをクリックして、クラスタ、サブクラスタ、およびノード レベルのユーザセッション レポートを CSV 形式でダウンロードします。
- ステップ 7 [1 つ以上のデバイスからログインしているユーザの数 (Count of users logged in from one or more devices)] 列に表示されている値をクリックして、特定のノードに関するユーザ ベースの詳細レポートを生成します。
- ステップ 8 [レポート (Reports)] ウィンドウの右側にある [ダウンロード (download)] (緑の矢印) アイコンをクリックして、ノードごとのユーザ レベルの詳細情報を CSV 形式でダウンロードします。
 - (注) [セッション数 (Number of sessions)] 列の上にマウスマウスカーソルを合わせると、[デバイスタイプ (device type)] ツールチップに、ログインに使用したデバイスのタイプが表示されます。

たとえば、デバイスタイプはデスクトップ、iPad、iPhone になる可能性があります。

(注) Android タブレットを使用してログインした場合、デバイスタイプはデスクトップとして表示されます。



第 20 章

エンタープライズグループの設定

- [エンタープライズグループの概要 \(269 ページ\)](#)
- [エンタープライズグループの前提条件 \(270 ページ\)](#)
- [エンタープライズグループの設定タスクフロー \(271 ページ\)](#)
- [エンタープライズグループの導入モデル \(Active Directory\) \(276 ページ\)](#)
- [エンタープライズグループの制限事項 \(279 ページ\)](#)

エンタープライズグループの概要

エンタープライズグループを設定すると、Cisco Unified Communications Manager は、データベースを外部 LDAP ディレクトリと同期するときにユーザグループを含めます。Cisco Unified CM の管理では、[ユーザグループ (User Groups)] ウィンドウで同期されたグループを表示できます。

この機能は、管理者が以下を行う場合にも役立ちます。

- 機能のコメントセット (たとえば、セールスチームやアカウンティングチーム) と同様の特性を持つユーザのプロビジョニング。
- 特定のグループのすべてのユーザを対象にしたメッセージの送信。
- 特定のグループのすべてのメンバーへの統一されたアクセスの設定

この機能は、Cisco Jabber ユーザが共通特性を共有するユーザの連絡先リストをすばやく作成するのにも役立ちます。Cisco Jabber ユーザは、外部 LDAP ディレクトリでユーザグループを検索し、それらを連絡先リストに追加できます。たとえば、Jabber ユーザは外部 LDAP ディレクトリを検索してセールスグループを連絡先リストに追加することで、すべてのセールスチームメンバーを連絡先リストに追加することができます。グループが外部ディレクトリで更新されると、ユーザの連絡先リストは自動的に更新されます。

エンタープライズグループは、Windows 上の Microsoft Active Directory で外部 LDAP ディレクトリとしてサポートされています。



- (注) エンタープライズグループ機能を無効にすると、Cisco Jabber ユーザは、エンタープライズグループを検索したり、自分の連絡先リストに追加済みのグループを表示したりできません。ユーザがログイン中にその機能を無効にすると、そのユーザがログアウトするまでグループは表示されます。ユーザが再度ログインすると、グループは表示されません。

セキュリティグループ

セキュリティグループは、エンタープライズグループのサブ機能です。Cisco Jabber ユーザは、セキュリティグループを検索して、自分の連絡先リストに追加できます。この機能を設定するには、管理者がカスタマイズしたLDAPフィルタを設定し、設定されたLDAPディレクトリの同期に適用する必要があります。セキュリティグループは、Microsoft Active Directory のみサポートされています。

許可されるエントリの最大数

エンタープライズグループを設定するときは、グループを処理する連絡先リストの最大値を設定してください。

- 連絡先リストで許可されるエントリの最大数は、連絡先リスト内のエントリ数と、すでに連絡先リストに追加されているグループ内のエントリ数の合計です。
- 連絡先リストの最大エントリ数 = (連絡先リストのエントリ数) + (グループのエントリ数)
- エンタープライズグループ機能が有効になっている場合、連絡先リストのエントリ数が許可されている最大エントリ数より少ない場合、Cisco Jabber ユーザはグループをコンタクトリストに追加できます。機能が無効になっているときに許容される最大エントリ数を超えると、その機能が有効になるまでユーザは制限されません。機能が有効になってからユーザが引き続きログインすると、エラーメッセージは表示されません。ユーザがログアウトして再度ログインすると、余分な項目をクリアするように求めるエラーメッセージが表示されます。

エンタープライズグループの前提条件

この機能は、以下の条件でLDAPディレクトリの同期スケジュールを設定していることを前提としています。LDAPディレクトリ同期を設定方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Import Users from LDAP Directory」の章を参照してください。

- Cisco DirSync サービスが有効になっている必要があります。
- LDAPディレクトリ同期には、ユーザとグループの両方が含まれている必要があります。

- 通常のLDAPディレクトリ同期は、[LDAPディレクトリ同期スケジュール(LDAP Directory Synchronization Schedule)] で設定されているとおりにスケジュールされている必要があります。

サポートされる LDAP ディレクトリ

エンタープライズグループでは、Microsoft Active Directory のみがサポートされています。

エンタープライズグループの設定タスクフロー

エンタープライズグループ機能を設定するためにこれらのタスクを完了して下さい。

手順

	コマンドまたはアクション	目的
ステップ 1	LDAPディレクトリからのグループ同期の確認 (271 ページ)	LDAPディレクトリの同期にユーザとグループの両方が含まれていることを確認します。
ステップ 2	エンタープライズグループの有効化 (272 ページ)	Cisco Jabber ユーザが Microsoft Active Directory のエンタープライズグループを検索して自分の連絡先リストに追加できるようにするには、次のタスクを実行します。
ステップ 3	セキュリティグループを有効にする (273 ページ)	(任意) Cisco Jabber ユーザがセキュリティグループを検索して自分の連絡先リストに追加できるようにするには、次のタスクフローを完了します。
ステップ 4	ユーザグループの表示 (275 ページ)	(オプション) Cisco Unified Communications Manager データベースと同期するエンタープライズグループおよびセキュリティグループを表示します。

LDAP ディレクトリからのグループ同期の確認

この手順を使用して、LDAPディレクトリの同期にユーザとグループの両方が含まれていることを確認します。

手順

-
- ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。 **サーバ > LDAP > LDAPディレクトリ**
 - ステップ 2 [検索 (Find)] をクリックし、エンタープライズグループを同期する LDAP ディレクトリを選択します。
 - ステップ 3 [同期 (Synchronize)] フィールドで [ユーザとグループ (Users and Groups)] が選択されていることを確認します。
 - ステップ 4 [LDAPディレクトリの設定 (LDAP Directory configuration)] ウィンドウの残りのフィールドに入力します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。
 - ステップ 5 [保存 (Save)] をクリックします。
-

エンタープライズグループの有効化

LDAPディレクトリ同期にエンタープライズグループを含めるようにシステムを設定します。

手順

-
- ステップ 1 Cisco Unified CM の管理から、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] を選択します。
 - ステップ 2 [ユーザ管理パラメータ (User Management Parameters)] で、[Cisco IM and Presenceでのディレクトリグループの操作 (Directory Group Operations on Cisco IM and Presence)] パラメータを [有効 (Enabled)] に設定します。
 - ステップ 3 [プレゼンス情報を許可するためにサイズ設定された最大エンタープライズグループ (Maximum Enterprise Group Sized to allow Presence Information)] パラメータの値を入力します。許可される範囲は 1 ~ 200 ユーザで、デフォルト値は 100 ユーザです。
 - ステップ 4 [エンタープライズグループの同期モード (Syncing Mode for Enterprise Groups)] ドロップダウンリストから、定期的に行う LDAP 同期を [なし (None)]、[差分同期 (Differential Sync)]、[完全同期 (Full Sync)] から選択して設定します。

(注) これらのフィールドの構成の詳細については、エンタープライズパラメータのヘルプを参照してください。
 - ステップ 5 [保存 (Save)] をクリックします。
-

セキュリティグループを有効にする

Cisco Jabber ユーザがセキュリティグループを自分の連絡先リストに追加できるようにする場合は、以下のオプションのタスクを実行して、セキュリティグループを LDAP ディレクトリ同期に追加します。



(注) セキュリティグループの同期は、Microsoft Active Directory からのみ実行できます。



(注) 最初の同期がすでに発生した Cisco Unified Communications Manager では、LDAP ディレクトリの既存の構成に新しい設定を追加できません。

手順

	コマンドまたはアクション	目的
ステップ 1	セキュリティグループフィルタの作成 (273 ページ)	ディレクトリグループとセキュリティグループの両方をフィルタ処理する LDAP フィルタを作成します。
ステップ 2	LDAPディレクトリからセキュリティグループを同期する (274 ページ)	新しい LDAP フィルタを LDAP ディレクトリ同期に追加します。
ステップ 3	セキュリティグループのための Cisco Jabber の設定 (275 ページ)	既存のサービスプロファイルを更新して、そのサービスプロファイルに関連付けられた Cisco Jabber ユーザに、セキュリティグループを検索および追加するためのアクセス権が付与されるようにします。

セキュリティグループフィルタの作成

セキュリティグループをフィルタリングする LDAP フィルタを作成します。

手順

ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。 **システム > LDAP > ldap フィルタ**。

ステップ 2 [新規追加 (Add New)] をクリックします。

ステップ 3 [フィルタ名] ボックスに一意の名前を入力します。例えば、syncSecurityGroups。

ステップ 4 [フィルタ (Filter)] ボックスに (&(objectClass=group)(CN=*)) と入力します。

ステップ 5 [保存 (Save)] をクリックします。

LDAP ディレクトリからセキュリティグループを同期する

LDAP ディレクトリ同期にセキュリティグループフィルタを追加し、同期を完了します。



(注) 最初の LDAP 同期がすでに発生している場合、Cisco Unified Communications Manager では、LDAP ディレクトリの既存の構成に新しい設定を追加できません。



(注) LDAP ディレクトリ同期を新しく設定する方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure End Users」の項目を参照してください。

始める前に

[セキュリティグループフィルタの作成 \(273 ページ\)](#)

手順

ステップ 1 Cisco Unified CM の管理で、[システム (System)] > [LDAP (LADP)] > [LDAP ディレクトリ (LDAP Directory)] を選択します。

ステップ 2 次のいずれかを実行します。

- [新規追加 (Add New)] をクリックして、新しい LDAP ディレクトリを作成します。
- [検索 (Find)] をクリックして、同期されるセキュリティグループから LDAP ディレクトリを選択します。

ステップ 3 [グループの LDAP カスタム フィルタ (LDAP Custom Filter for Groups)] ドロップダウン リストから、作成したセキュリティグループフィルタを選択します。

ステップ 4 [保存 (Save)] をクリックします。

ステップ 5 [LDAP ディレクトリの構成 (LDAP Directory Configuration)] ウィンドウの残りのフィールドを設定します。フィールドおよびその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 6 [完全同期を今すぐ実施 (Perform Full Sync Now)] をクリックして、すぐに同期します。これを行わない場合には、セキュリティグループはスケジュールされた LDAP 同期が次に発生した際に同期されます。

セキュリティグループのための Cisco Jabber の設定

既存のサービスプロファイルを更新して、そのサービスプロファイルに関連付けられている Cisco Jabber ユーザが LDAP ディレクトリから自分の連絡先リストにセキュリティグループを追加できるようにします。



- (注) 新しいサービス プロファイルを設定し、Cisco Jabber ユーザに割り当てる方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の章「Configure Service Profiles」を参照してください。

始める前に

[LDAP ディレクトリからセキュリティグループを同期する \(274 ページ\)](#)

手順

- ステップ 1** [サービス プロファイルの設定 (Service Profile Configuration)] ウィンドウの残りのフィールドに入力します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。
- ステップ 2** [検索 (Find)] をクリックし、Jabber ユーザが使用するサービスプロファイルを選択します。
- ステップ 3** [ディレクトリ プロファイル (Directory Profile)] で、[Jabber にセキュリティグループの検索と追加を許可 (Allow Jabber to Search and Add Security Groups)] チェックボックスをオンにします。
- ステップ 4** [保存 (Save)] をクリックします。
このサービスプロファイルに関連付けられた Cisco Jabber ユーザは、セキュリティグループを検索して追加できるようになります。
- ステップ 5** Cisco Jabber ユーザが使用するすべてのサービスプロファイルに対して、この手順を繰り返します。

ユーザ グループの表示

次の手順を使用して、Cisco Unified Communications Manager データベースと同期されているエンタープライズグループおよびセキュリティグループを表示できます。

手順

- ステップ 1** Cisco Unified CM Administration で、次のいずれかを選択します。ユーザ管理 > ユーザ設定 > ユーザ・グループ。
[ユーザ グループの検索/一覧表示 (Find and List User Group)] ウィンドウが表示されます。

- ステップ 2** 検索条件を入力して [検索 (Find)] をクリックします。
検索条件に一致するユーザ グループのリストが表示されます。
- ステップ 3** ユーザグループに属するユーザの一覧を表示するには、必要なユーザグループをクリックします。
[ユーザ グループの設定 (User Group Configuration)] ウィンドウが表示されます。
- ステップ 4** 検索条件を入力して [検索 (Find)] をクリックします。
検索条件に一致するユーザのリストが表示されます。
- リスト内のユーザをクリックすると、[エンド ユーザの設定 (End User Configuration)] ウィンドウが表示されます。

エンタープライズ グループの導入モデル (Active Directory)

エンタープライズ グループ機能は、Active Directory 用に次の 2 つの導入オプションを提供します。

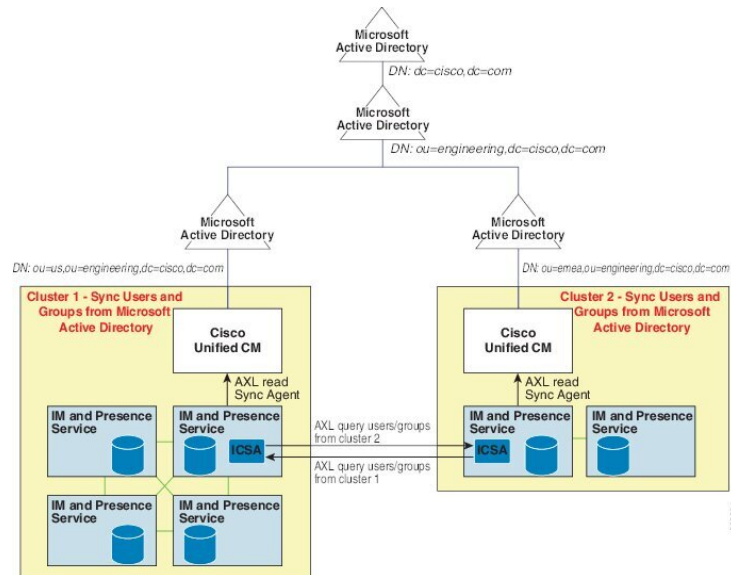


- 重要** Cisco Intercluster Sync Agent サービス経由でデータを同期する前に、クラスタ 1 とクラスタ 2 に、UserGroup レコード、UserGroupMember レコード、UserGroupWatcherList レコードの一意のセットが含まれていることを確認します。両方のクラスタにレコードの一意のセットが含まれている場合、同期後には両方のクラスタにすべてのレコードのスーパーセットが含まれています。

エンタープライズ グループ導入モデル 1

この導入モデルでは、クラスタ 1 とクラスタ 2 が Microsoft Active Directory からの異なるユーザとグループのサブセットを同期します。Cisco Intercluster Sync Agent サービスは、データをクラスタ 2 からクラスタ 1 に複製して、ユーザとグループの完全なデータベースを作成します。

図 8: エンタープライズ グループ導入モデル 1



エンタープライズ グループ導入モデル 2

この導入モデルでは、クラスタ 1 が Microsoft Active Directory からのすべてのユーザとグループを同期します。クラスタ 2 は、Microsoft Active Directory からのユーザのみを同期します。Cisco Intercluster Sync Agent サービスは、グループ情報をクラスタ 1 からクラスタ 2 に複製します。



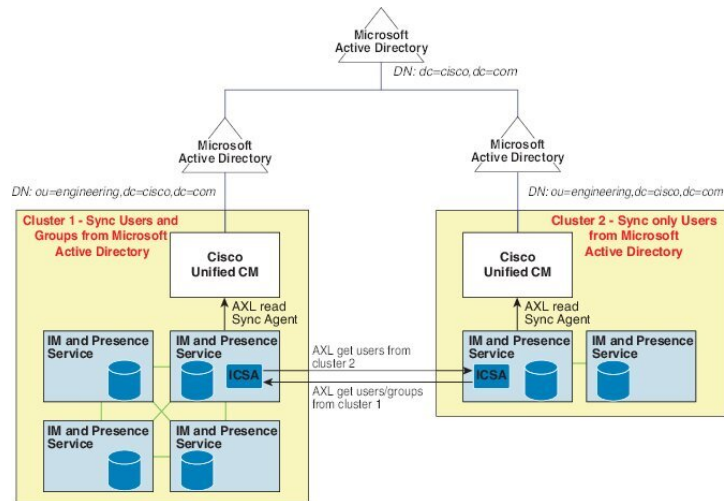
注意

この導入モデルを使用する場合は、1つのクラスタ内のグループデータだけが同期されていることを確認します。そうでない場合は、エンタープライズグループ機能が想定どおりに機能しません。

[Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] > [プレゼンス (Presence)] > [クラスタ間設定 (Inter-Clustering)] ウィンドウで設定を確認できます。

クラスタ間ピア テーブルで [エンタープライズ グループ LDAP 設定 (Enterprise Groups LDAP Configuration)] パラメータのステータスを確認します。[矛盾は見つかりませんでした (No conflict found)] は、ピア間に設定ミスがないことを意味します。矛盾が見つかった場合は、[エンタープライズ グループの矛盾 (Enterprise GroupConflicts)] リンクをクリックして、表示された [詳細 (details)] ボタンをクリックします。これにより、レポート ウィンドウが開いて、詳細なレポートが表示されます。

図 9: エンタープライズ グループ導入モデル 2



エンタープライズグループの制限事項

表 25: エンタープライズグループの制限事項

制限事項	説明
全員をブロック (Block everyone)	<p>Cisco Jabber ユーザが [全員をブロック] を有効にした場合このブロックは、Cisco Jabber ポリシー設定内の機能であるため、ブロックしているユーザの連絡先リストに連絡先としてリストされていない限り、他の Jabber ユーザがブロックしているユーザとの IM and Presence の表示または交換を禁止します。</p> <p>たとえば、Cisco Jabber ユーザ (Andy) は、自分の個人的な Jabber 設定内の [全員をブロック] を有効にしています。次のリストは、Andy の個人用連絡先リストに含まれているかどうかにかかわらず、Andy のブロックが他の Jabber ユーザにどのように影響するかを示しています。ブロックに加えて、Andy には以下のような個人用連絡先リストがあります。</p> <ul style="list-style-type: none"> • Bob を含む - Bob は Andy の個人用連絡先リストに登録されているため、ブロックしていても IM を送信したり、Andy のプレゼンスを表示したりできます。 • キャロルを省略 - ブロックされているので、キャロルはアンディのプレゼンスを表示したり、IM を送信したりできません。 • 個人的な連絡先として Deborah を省略します。ただし、Deborah は、Andy が連絡先としてリストしている企業グループのメンバーです - Deborah は、Andy のプレゼンスを表示したり、Andy に IM を送信したりすることはできません。 <p>Andy の連絡先リストの企業グループのメンバーであるにもかかわらず、Deborah は Andy のプレゼンスを閲覧したり、IM を Andy に送信したりすることはできないことに留意してください。エンタープライズグループ連絡先の動作の詳細については、CSCvg48001 を参照してください。</p>

制限事項	説明
10.x クラスタとのクラスタ間ピアリング	<p>エンタープライズグループは、リリース 11.0(1)以降でサポートされます。</p> <p>同期されたグループに 10.x クラスタ間ピアからのグループメンバーが含まれている場合、より高いクラスタ上のユーザは 10.x クラスタからの同期されたメンバーのプレゼンスを確認できません。これは、エンタープライズグループの同期用に 11.0(1) で導入されたデータベース更新が原因です。この更新は 10.x リリースの一部ではありません。</p> <p>より高いクラスタをホームにしているユーザが 10.x クラスタをホームにしているグループメンバーのプレゼンスを確認できることを保証するには、より高いクラスタ上のユーザが自分の連絡先リストに 10.x ユーザを手動で追加する必要があります。手動で追加されたユーザに関するプレゼンスの問題は存在しません。</p>
複数レベルのグループ分け	複数レベルのグループ分けは、グループ同期に対して許可されません。
グループ専用同期	ユーザグループとユーザが同じ検索ベース内に存在する場合、グループ専用同期は許容されません。代わりに、ユーザグループとユーザが同期されます。
ユーザグループの最大数	<p>Microsoft Active Directory サーバから Unified Communications Manager データベースに最大 15000 のユーザグループを同期できます。各ユーザグループには 1 ~ 200 人のユーザを含めることができます。[Cisco Unified CM IM and Presence Administration] > [システム (System)] > [サービスパラメータ (Service Parameters)] ウィンドウで、正確な数量を設定できます。</p> <p>データベース内のユーザアカウントの最大数は 160,000 を超えることはできません。</p>
ユーザグループの移行	ユーザグループを組織単位間で移動する場合は、元の単位に対して完全同期を実行してから、新しい単位に対して完全同期を実行する必要があります。
ローカルグループ	ローカルグループはサポートされません。Microsoft Active Directory から同期されたグループのみがサポートされます。
IM and Presence Service ノードに割り当てられていないグループメンバー	IM and Presence Service ノードに割り当てられていないグループメンバーは、プレゼンスバブルが灰色表示されて連絡先リストに表示されます。ただし、これらのメンバーは、連絡先リストで許可されるユーザの最大数を計算する際に考慮されます。

制限事項	説明
Microsoft Office Communications Server からの移行	Microsoft Office Communications Server からの移行中は、ユーザが IM and Presence Service ノードに完全に移行されるまで、グループ エンタープライズ機能がサポートされません。
LDAP 同期	同期の進行中に、[LDAPディレクトリの設定 (LDAP Directory Configuration)] ウィンドウで同期オプションを変更しても、既存の同期は影響を受けません。たとえば、同期の進行中に同期オプションを [ユーザとグループ (Users and Groups)] から [ユーザのみ (Users Only)] に変更しても、ユーザとグループの同期はそのまま継続されます。
エッジ経由のグループ検索機能	エッジ経由のグループ検索機能は、このリリースで提供されますが、完全にテストされているわけではありません。そのため、エッジ経由のグループ検索のフルサポートは保証できません。フルサポートは今後のリリースで提供される予定です。
Cisco Intercluster Sync Agent サービスの定期同期	外部 LDAP ディレクトリでグループ名またはグループメンバー名を更新すると、定期 Cisco Intercluster Sync Agent サービス同期の後でしか Cisco Jabber 連絡先リストが更新されません。通常、Cisco Intercluster Sync Agent サービスの同期は 30 分ごとに実行されます。
LDAP 設定内の別々の同期アグリーメント経由のユーザとユーザグループの同期	ユーザとユーザグループが同じ同期アグリーメントの一部として Cisco Unified Communications Manager データベースに同期されている場合は、同期後に、Cisco Unified Communications Manager データベースで、想定されているようにユーザとグループの関連付けが更新されます。ただし、ユーザとユーザグループが別々の同期アグリーメントの一部として同期されている場合は、最初の同期後、ユーザとグループはデータベースで関連付けされないことがあります。データベース内のユーザとグループの関連付けは、同期アグリーメントが処理される順序によって異なります。ユーザがグループより前に同期された場合は、データベース内でグループを関連付けに使用できない可能性があります。その場合は、グループとの同期アグリーメントがユーザとの同期アグリーメントより前にスケジュールされるようにします。そうでない場合は、グループをデータベースに同期した後、ユーザは次の手動同期または定期的に同期タイプを設定してユーザとグループとして同期した後にグループに関連付けられます。契約の同期タイプがユーザとグループとして設定されている場合にのみ、ユーザおよび対応するグループ情報がマップされます。 。

制限事項	説明
エンタープライズグループの 検証済 OVA 情報	<p>検証 シナリオ</p> <p>2つのクラスタを持つクラスタ間の導入では、クラスタ A とクラスタ B が使用されています。</p> <p>クラスタ A は、Active Directory から同期される 160 k ユーザの IM and Presence Service で 15K OVA および 15K ユーザが有効になっています。15K OVA クラスタでは、ユーザあたりのエンタープライズグループの検証され、サポートされる平均数は 13 のエンタープライズグループです。</p> <p>クラスタ B では、Active Directory から同期される 160 k ユーザの IM and Presence Service で 25K OVA および 25K ユーザが有効になっています。25K OVA クラスタでは、ユーザあたりのエンタープライズグループの検証され、サポートされる平均数は 8 のエンタープライズグループです。</p> <p>名簿に記載されているユーザの個人連絡先と、ユーザの名簿に含まれるエンタープライズグループからの連絡先の、検証済およびサポートされる合計は、200 以下です。</p> <p>(注) 2つ以上のクラスタがある環境では、これらの数量はサポートされていません。</p>



第 21 章

ブランディングのカスタマイズ

- [ブランディングの概要](#) (283 ページ)
- [ブランディングの前提条件](#) (283 ページ)
- [ブランディングの有効化](#) (284 ページ)
- [ブランディングの無効化](#) (284 ページ)
- [ブランディング ファイルの要件](#) (285 ページ)

ブランディングの概要

ブランディング機能を使用すると、IM and Presence サービスにカスタマイズされたブランディングを適用できます。ブランディングのカスタマイズは、Cisco Unified CM IM and Presence Administration のログインおよび設定ウィンドウに表示されます。追加または変更できる項目には次のものがあります。

- 企業ロゴ
- 背景色
- 枠線色
- フォントの色

ブランディングの前提条件

指定されたフォルダ構造とファイルを使用してブランディング zip ファイルを作成する必要があります。詳細については、[ブランディングファイルの要件](#) (285 ページ) を参照してください。

ブランディングの有効化

この手順を使用して、IM and Presence サービス クラスタのブランディングのカスタマイズを有効にします。SAML SSO が有効になっていても、ブランディングの更新が表示されます。

始める前に

IM and Presence サービスがアクセスできる場所に、IM and Presence のカスタマイズを含む branding.zip ファイルを保存します。

手順

-
- ステップ 1** Cisco Unified IM and Presence OS の管理にログインします。
 - ステップ 2** [ソフトウェアアップグレード (Software Upgrades)] > [ブランディング (Branding)] を選択します。
 - ステップ 3** リモート サーバを参照し、branding.zip ファイルを選択します。
 - ステップ 4** [ファイルのアップロード (Upload File)] をクリックします。
 - ステップ 5** [ブランディングの有効化 (Enable Branding)] をクリックします。
(注) **utils Branding enable CLI** コマンドを実行して、ブランディングを有効にすることもできます。
 - ステップ 6** ブラウザを更新して、変更を確認します。
 - ステップ 7** すべての IM and Presence サービスのクラスタ ノードでこの手順を繰り返します。
-

ブランディングの無効化

この手順を使用して、IM and Presence サービス クラスタのブランディングを無効にします。



-
- (注) ブランディングを無効にするには、特権レベル4のアクセス権を持つマスター管理者アカウントを使用する必要があります。これは、インストール時に作成されるメインの管理者アカウントです。
-

手順

-
- ステップ 1** Cisco Unified IM and Presence OS の管理にログインします。

ステップ 2 [ソフトウェアアップグレード (Software Upgrades)] > [ブランディング (Branding)] を選択します。

ステップ 3 [ブランディングの無効化 (Disable Branding)] をクリックします。

(注) **utils Branding disable** CLI コマンドを実行して、ブランディングを無効にすることもできます。

ステップ 4 ブラウザを更新して、変更を確認します。

ステップ 5 すべての IM and Presence サービスのクラスタ ノードでこの手順を繰り返します。

ブランディング ファイルの要件

カスタマイズされたブランディングをシステムに適用する前に、仕様に従って branding.zip ファイルを作成します。リモート サーバ上で、ブランディング フォルダを作成し、指定されたコンテンツをフォルダに入れます。すべてのイメージファイルとサブフォルダを追加したら、フォルダ全体を圧縮し、ファイルを branding.zip として保存します。

ヘッダーに勾配効果を作成するために、ヘッダーに単一のイメージを使用するか、または6つのイメージの組み合わせを使用するかに応じて、フォルダ構造に2つのオプションがあります。

表 26: フォルダ構造オプション

ブランディング オプション	フォルダ構造
単一ヘッダー オプション	<p>ヘッダーの背景 (吹き出し項目3) に1つのイメージが必要な場合は、ブランディング フォルダに次のサブフォルダとイメージファイルが含まれている必要があります。</p> <pre> Branding (folder) cup (folder) BrandingProperties.properties (properties file) brandingHeader.gif (652*1 pixel) ciscoLogo12pxMargin.gif (44*44 pixel) </pre>

ブランディングオプション	フォルダ構造
勾配ヘッダーオプション	<p>ヘッダーの背景（吹き出し項目 3、4、5）に勾配イメージを作成する場合は、勾配効果を作成するために6つの個別のイメージファイルが必要です。ブランディングフォルダには、これらのサブフォルダとファイルが含まれている必要があります。</p> <pre> Branding (folder) cup (folder) BrandingProperties.properties (file) brandingHeaderBegLTR.gif (652*1 pixel image) brandingHeaderBegRTR.gif (652*1 pixel image) brandingHeaderEndLTR.gif (652*1 pixel image) brandingHeaderEndRTR.gif (652*1 pixel image) brandingHeaderMidLTR.gif (652*1 pixel image) brandingHeaderMidRTR.gif (652*1 pixel image) ciscoLogo12pxMargin.gif (44*44 pixel image) </pre>

ユーザインターフェイスのブランディングオプション

次の画像に、[Cisco Unified CM IM and Presence Administration] ユーザインターフェイスのブランディングオプションを示します。

図 10: 管理ログイン画面のブランディングオプション

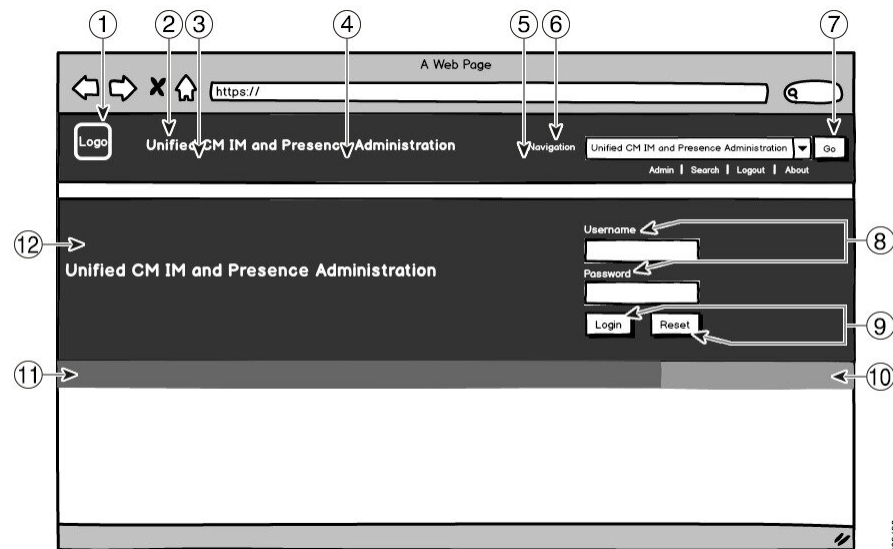
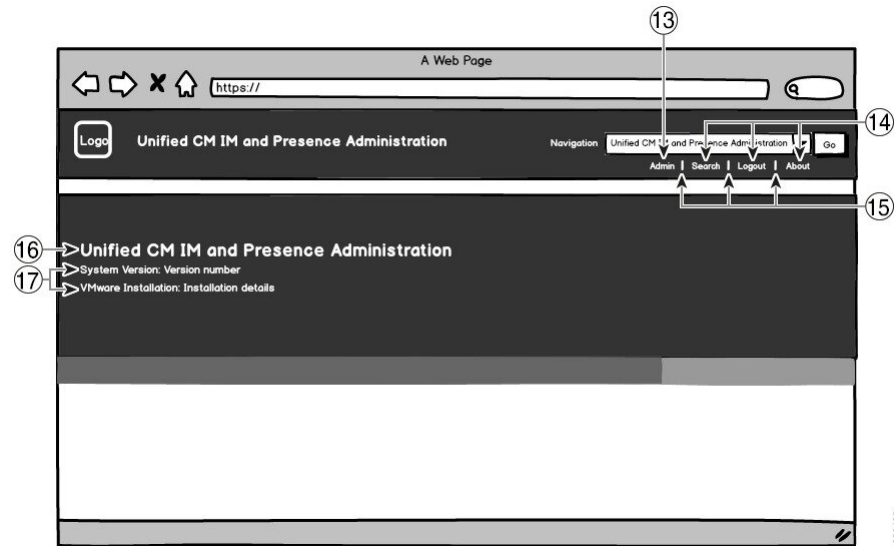


図 11: 管理ログイン中の画面のブランディング オプション



次の表に、上記の画面キャプチャの吹き出し項目のカスタマイズ方法を示します。

表 27: ユーザーインターフェイスのブランディング オプション

項目	説明	ブランディングの編集
ログイン画面イメージ		
1	企業ロゴ	IM and Presence サービス インターフェイスにロゴを追加するには、会社のロゴを次のファイル名で44x44 ピクセルイメージとして保存します。 ciscoLogo12pxMargin.gif (44*44 ピクセル)
2	ヘッダーの Unified CM IM and Presence Administration のテキスト	header.heading.color
3	ヘッダーの背景 (勾配オプション: 左側)	ヘッダーイメージに勾配効果を適用する場合は、左側に次のイメージを使用します。 <ul style="list-style-type: none"> • brandingHeaderBegLTR.gif (652 x 1 ピクセル) • brandingHeaderBegLTR.gif (652 x 1 ピクセル)

項目	説明	ブランディングの編集
4	ヘッダーの背景	<p>ヘッダーの1つのイメージを使用する場合：</p> <ul style="list-style-type: none"> • brandingHeader.gif (652 x 1 ピクセル) <p>それ以外の場合、勾配効果を持つヘッダーを作成する場合は、次の画像を使用します。</p> <ul style="list-style-type: none"> • brandingHeaderMidLTR.gif (652 x 1 ピクセル) • brandingHeaderMidRTR.gif (652 x 1 ピクセル)
5	ヘッダーの背景 (勾配オプション：右側)	<p>ヘッダーに勾配効果を使用する場合は、右側のヘッダーに次のイメージを使用します。</p> <ul style="list-style-type: none"> • brandingHeaderEndLTR (652 x 1 ピクセル) • brandingHeaderEndRTR (652 x 1 ピクセル)
6	ナビゲーション テキスト	header.navigation.color
7	[移動 (Go)] ボタン	header.go.font.color header.go.background.color
8	ユーザ名およびパスワードのテキスト	splash.loginfield.color
9	[ログイン (Login)] および [リセット (Reset)] ボタン	splash.button.text.color splash.button.color
10	背景下の色：右側	splash.hex.code.3
11	背景下の色：左側	splash.hex.code.2
12	Banner	splash.hex.code.1
ログイン後イメージ		
13	ログインしたユーザのテキスト (たとえば、「管理者」ユーザ)	header.text.bold.color

項目	説明	ブランディングの編集
14	[検索 (Search)]、[バージョン情報 (About)]、[ログアウト (Logout)] リンク	header.link.color
15	リンク デイバイダ	header.divider.color
16	バナーの Unified CM IM and Presence Administration のテキスト (ログイン後)	splash.login.text.color
17	システムのバージョンおよび VMware インストールのテキスト	splash.version.color

ブランディング プロパティの編集例

ブランディングプロパティは、プロパティファイル (BrandingProperties.properties) に 16 進コードを追加することで編集できます。プロパティ ファイルは HTML ベースの 16 進コードを使用します。たとえば、ナビゲーションテキスト項目 (吹き出し項目 #6) の色を赤に変更する場合は、プロパティ ファイルに次のコードを追加します。

```
header.navigation.color="#FF0000"
```

このコードで、header.navigation.color は編集するブランディング プロパティで、"#FF0000" は新しい設定 (赤) です。



第 22 章

高度な機能の設定

- ストリーム管理 (291 ページ)
- Microsoft Outlook とのカレンダー統合 (293 ページ)
- フェデレーション (293 ページ)
- メッセージアーカイブ (294 ページ)
- Remote Call Control; リモート呼制御 (295 ページ)

ストリーム管理

IM and Presence Service では、インスタントメッセージングのストリーム管理がサポートされています。ストリーム管理は、XEP-0198 仕様を使用して実装されています。これは、2 つの XMPP エンティティ間(スタンザ受信確認とストリームの再開の機能を含む)をアクティブに管理するための Extensible Messaging and Presence Protocol (XMPP) を定義します。XEP-0198 の詳細については、次の仕様を参照してください。 <http://xmpp.org/extensions/xep-0198.html>

IM and Presence Service と Cisco Jabber 間の通信が一時的に失われた場合、ストリーム管理によって、通信の停止中に送信されるすべてのインスタントメッセージが失われることはありません。設定可能なタイムアウト期間によって、メッセージの処理方法が決まります。

- Cisco Jabber がタイムアウト期間内に IM and Presence Service との通信を再確立した場合、メッセージは再送信されます。
- Cisco Jabber が IM and Presence Service との通信をタイムアウト期間内に再確立しない場合、メッセージは送信者に返されます。
- タイムアウト期間の経過後に送信されたメッセージはオフラインで保存され、Cisco Jabber が IM and Presence Service との通信を再開するときに配信されます。

ストリームの管理は、クラスタ全体でデフォルトで有効になっています。ストリーム管理サービスパラメータを使用すると、この機能を設定できます。

ストリーム管理の設定

IM and Presence Service のストリーム管理 (XEP-0198) を設定するには、次の手順を使用します。

手順

- ステップ 1 Cisco Unified CM IM and Presence Administration から、[システム (System)] > [サービスパラメータ (Service Parameters)] を選択します。
- ステップ 2 サーバ ドロップダウンから、IM とプレゼンスノードを選択します。
- ステップ 3 サービス ドロップダウンから、Cisco XCP ルータを選択します。
- ステップ 4 [ストリーム管理の有効化 (Enable Stream Management)] サービスパラメータを [有効 (Enabled)] に設定します。
- ステップ 5 [ストリーム管理パラメータ (クラスタ全体) (Stream Management Parameters (Clusterwide))] で、ストリーム管理パラメータを設定します。

表 28: ストリーム管理サービスパラメータ

サービスパラメータ	説明
ストリーム管理の有効化	ストリーム管理のクラスタ全体を有効または無効にします。デフォルトの設定はイネーブルです。
ストリーム管理のタイムアウト	切断されたセッションを再開できる期間の長さ (秒数) は、タイムアウトによって制御されます。クライアントがより長いタイムアウトをネゴシエートしようとした場合 (または希望するタイムアウトを指定しなかった場合)、この最大値が適用されます。 このタイムアウト後に送信されたメッセージはすべて、Cisco Jabber が IM and Presence Service を使用して再度ログインする前に、オフラインで保存され、再度ログインした後に再送信されます。 指定範囲は 30 秒 ~ 90 秒です。デフォルト値は 60 秒です。
ストリーム管理バッファ (Stream Management Buffer)	ストリーム管理が有効なセッションのバッファに保持される、パケット (パケット履歴) の最大数を定義します。バッファで利用できる履歴よりも多くの履歴をクライアントが必要としている場合、ストリームの再開は失敗します。 指定範囲は 5 ~ 150 パケットで、デフォルト値は 100 パケットです。

サービスパラメータ	説明
確認応答リクエスト率	<p>クライアントに対して最後に受信したスタンザのカウンタを提供するように要求する前に、サーバが送信するスタンザの数を定義します。値を小さくするとネットワークトラフィックが増加しますが、サーバでのスタンザ履歴バッファの削減に役立ち、メモリの使用量が減少します。</p> <p>この範囲は 1 ~ 64 スタンザで、デフォルト値は 5 です。</p> <p>(注) 確認応答リクエスト率が小さいと、ネットワークトラフィックが増加しますが、メモリ使用量は減少します。</p>

ステップ 6 [保存 (Save)] をクリックします。

Microsoft Outlook とのカレンダー統合

この機能を使用して、ユーザは Microsoft Outlook の予定表/会議のステータスを IM and Presence サービスサーバの可用性ステータスに組み込むことができます。ユーザが会議に参加している場合、そのステータスはユーザのプレゼンスステータスの一部として表示されます。この機能は、IM and Presence サービスをオンプレミス Microsoft Exchange Server またはホスト型 Office 365 サーバに接続することによって実現できます。

Microsoft Outlook とのカレンダー統合の設定方法については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html> で IM and Presence サービスのための Microsoft Outlook とのカレンダー統合文書を参照してください。

フェデレーション

IM and Presence サービスでは、IM and Presence サービスが管理する任意のドメイン内からフェデレーションネットワークを作成できます。フェデレーションの展開には、主に 2 つの種類があります。

- ドメイン間フェデレーション - この統合により、IM and Presence サービスが外部ドメインユーザとアベイラビリティ情報やインスタントメッセージング (IM) を交換したどのドメイン内からの IM and Presence サービスユーザもイネーブルにします。外部ドメインは、Microsoft、Google、IBM、または AOL のサーバによって管理されている場合があります。IM and Presence サービスは、さまざまなプロトコルを使用して外部ドメインのサーバと通信できます。
- パーティション化されたドメイン内フェデレーション：この統合により、IM and Presence サービスと Microsoft サーバ（たとえば、Microsoft Lync）が共通のドメインまたは一連のドメインをホストします。この統合により、単一の企業内の IM and Presence サービスクラ

イアントユーザと Microsoft Lync ユーザがインスタントメッセージングと可用性を交換できるようになります。

- SIP オープンフェデレーション：Cisco IM and Presence サービスは、Cisco Jabber クライアントで SIP オープンフェデレーションをサポートします。管理者は SIP オープンフェデレーションを設定して、Cisco Jabber ユーザが、利用可能なすべてのドメインのユーザとのシームレスなフェデレーションを行えるようにすることができます。オープンフェデレーションは、単一のスタティックルートを使用するすべてのドメインに対して設定できます。スタティックルートにより、Cisco Jabber は任意の外部ドメインとフェデレーションを行うことができます。さらに重要な点として、個々のドメインに対して SIP フェデレーションを設定および管理する場合にかかる時間が大幅に削減されます。

フェデレーションの詳細な設定手順については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html>にある『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』または『*Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

メッセージアーカイバ

多くの業界では、インスタントメッセージが、他のビジネス レコードと同じ適合認定のガイドラインに従うことが求められています。これらの規制を順守するには、ご使用のシステムがすべてのビジネスレコードを記録してアーカイブする必要があり、アーカイブされたレコードが取得可能になっている必要があります。

IM and Presence Service は単一クラスター ネットワーク構成、クラスター間ネットワーク構成、または連動ネットワーク構成における次の IM アクティビティ用のデータを収集して、インスタントメッセージング (IM) コンプライアンスをサポートをしています。

- ポイントツーポイント メッセージ
- グループチャット：これには、Ad-hoc または一時チャットメッセージと、常設チャットメッセージがあります。
- IM Compliance のコンポーネント
- IM Compliance 用サンプル トポロジおよびメッセージフロー

IM コンプライアンスの設定の詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html>で『*Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

Remote Call Control; リモート呼制御

リモート通話コントロール (RCC) を使用すると、企業ユーザが Microsoft Lync (サードパーティ製デスクトップインスタントメッセージング (IM) アプリケーション) 経由で Cisco Unified IP Phone または Cisco IP Communicator を制御できるようになります。ユーザが Microsoft Lync クライアントにサインインすると、Lync サーバは IM and Presence サービス ノードを通じて Cisco Unified Communications Manager へ、Lync クライアントでのユーザのアクションに応じた通話機能のセットアップ、終了、保持を指示します。

Remote Call Control の設定についての詳細は、<http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html>で『*Remote Call Control with Microsoft Lync Server for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。



第 **IV** 部

システムの管理

- [チャットの管理 \(299 ページ\)](#)
- [マネージドファイル転送管理 \(317 ページ\)](#)
- [エンドユーザの管理 \(327 ページ\)](#)
- [ユーザを集中展開に移行する \(343 ページ\)](#)
- [ユーザの移行 \(361 ページ\)](#)
- [ロケールの管理 \(379 ページ\)](#)
- [サーバの管理 \(387 ページ\)](#)
- [システムのバックアップ \(395 ページ\)](#)
- [システムの復元 \(407 ページ\)](#)
- [連絡先リストの一括管理 \(427 ページ\)](#)
- [システムのトラブルシューティング \(443 ページ\)](#)



第 23 章

チャットの管理

- [チャット管理の概要 \(299 ページ\)](#)
- [チャットの前提条件の管理 \(300 ページ\)](#)
- [チャットのタスクフローの管理 \(301 ページ\)](#)
- [チャット相互作用の管理 \(315 ページ\)](#)

チャット管理の概要

IM and Presence サービスでは、チャットルームを管理したり、チャットルームにアクセスできる人を制御したりするために使用できる設定が提供されます。これには次の機能が含まれます。

- 新しいルームを作成したり、作成したルームのメンバーおよび設定を管理します。
- そのルームのメンバーだけがアクセスできるように永続的なチャットルームへのアクセスを制限する。
- チャットルームに管理者を割り当てます。
- ルームに他のユーザを招待します。
- ルームに表示されるメンバーのプレゼンスステータスを確認します。ルームに表示されるプレゼンスステータスは、ルームへのメンバーの参加を示しますが、全体のプレゼンスステータスが反映されないことがあります。

IM and Presence Service では、チャットノードのエイリアスも管理できます。チャットノードエイリアスを使用すると、ユーザが特定のノード上の特定のチャットルームを検索し、それらのチャットルームに参加できます。

さらに、IM and Presence サービスはトランスクリプトを保存し、このチャットルームの履歴を、チャットルームに参加したばかりのメンバーを含むルームメンバーにも利用できるようにします。新旧のメンバーが利用できるようにする既存のアーカイブの量を設定できます。

チャットノードエイリアスの概要

システムの各チャットノードに一意のエイリアスが必要です。チャットノードエイリアスは、(任意のドメイン内の) ユーザが特定のノード上の特定のチャットルームを検索し、これらのルームのチャットに入室できるように各チャットノードに一意のアドレスを作成します。チャットノードエイリアスは、そのノード上に作成された各チャットルームの一意の ID の一部を形成します。たとえば、エイリアス `conference-3-mycup.cisco.com` は、そのノードに作成されたチャットルーム `roomjid@conference-3-mycup.cisco.com` の名前付けに使用されます。

チャットノードエイリアスを割り当てるには、2つのモードがあります。

- システム生成 - システムは各チャットノードに一意のエイリアスを自動的に割り当てます。システムは、命名規則 `conference-x-clusterid.domain` を使用して、デフォルトではチャットノードごとに1個のエイリアスを自動生成します。
 - `conference` はハードコードされたキーワードです
 - `x` はノード ID を示す一意の整数値です
 - `clusterid` は構成されたエンタープライズパラメータです
 - ドメイン構成済みドメインです

たとえば、システムは次のように割り当てます。 `conference-3-mycup.cisco.com`

- 手動 - チャットノードエイリアスを手動で割り当てるには、システム生成エイリアスを無効にする必要があります。手動管理されたエイリアスにより、特定の要件に合うエイリアスを使用してチャットノードに名前を付けられる完全な柔軟性が得られます。たとえば、`congerence-x-clusterid.domain` 命名規則がデプロイメントのニーズに合わない場合に、次のようにします。

ノードごとに複数のエイリアスを割り当てる

ノード単位で各チャットノードに複数のエイリアスを関連付けることができます。ノードごとに複数のエイリアスを関連付けると、ユーザはこれらのエイリアスを使用して追加のチャットルームを作成できます。この機能は、システム生成のエイリアスと手動で作成されたエイリアスの両方に適用されます。

チャットの前提条件の管理

常設チャットが有効になっていることを確認してください。

チャットのタスクフローの管理

手順

	コマンドまたはアクション	目的
ステップ 1	チャットルーム所有者がチャットルーム設定を編集できるようにする (302 ページ)	チャットルームの所有者がチャットルームの設定を編集できるようにするかどうかを設定します。それ以外の場合は、管理者だけがチャットルーム設定を編集できます。
ステップ 2	クライアントでのインスタントメッセージ履歴のログ記録の許可 (303 ページ)	ユーザがインスタントメッセージ履歴をローカルでコンピューターに記録することを防止または許可できます。
ステップ 3	外部データベーステキスト会議レポートの表示 (303 ページ)	この手順を使用して、常設チャットルームの詳細を表示できる外部データベーステキスト会議レポートを表示します。
ステップ 4	<p>チャットルーム設定を編集します。チャットルームの設定を更新するには、以下のタスクを任意の順序で実行します。</p> <ul style="list-style-type: none"> • チャットルーム数の設定 (304 ページ) • チャットルームメンバー設定を設定します (304 ページ) • 可用性の設定 (306 ページ) • 利用者数の設定 (307 ページ) • チャットメッセージの設定 (308 ページ) • モデレータ管理されたルームの設定 (309 ページ) • 履歴の設定 (310 ページ) 	(注) 常設チャット設定を更新する場合、Cisco XCP Text Conference Manager サービスを再起動するために [Cisco Unified IM and Presence サービスアビリティ (Cisco Unified IM and Presence Serviceability)] で、[ツール (Tools)] > [コントロールセンター - 機能サービス (Control Center - Feature Services)] を選択します。
ステップ 5	チャットルームをシステムのデフォルトにリセットします (310 ページ)	チャット設定をシステムデフォルトにリセットする場合は、このオプションの作業を完了してください。アドホックチャットはデフォルトで有効になっていますが、常設チャットはデフォルトで無効になっています。このタスクを完了すると、常設チャットが無効になります。

	コマンドまたはアクション	目的
ステップ 6	チャット ノードのエイリアスの管理 (311 ページ)	エイリアスは、(任意のドメイン内の) ユーザが特定のノード上の特定のチャットルームを検索し、これらのルームのチャットに入室できるように各チャットノードに一意のアドレスを作成します。システムの各チャット ノードに一意のエイリアスが必要です。
ステップ 7	常設チャット用の外部データベースの消去 (314 ページ)	これはオプションです。外部データベースを監視し、期限切れのレコードを削除するジョブを設定するには、外部データベースクリーンアップユーティリティを使用します。これにより、新しいレコード用に常に十分なディスク容量が確保されます。

チャットルーム所有者がチャットルーム設定を編集できるようにする

チャットルームの所有者がチャットルームの設定を編集できるようにする場合は、この手順を使用します。



(注) クライアントからこれらの設定をどの程度行えるかは、クライアントの実装や、クライアントがこれらの設定を行うインターフェイスを提供しているかどうかで決まります。

手順

ステップ 1 [Cisco Unified CM IM and Presenceの管理 (Cisco Unified CM IM and Presence Administration)] で、[メッセージング (Messaging)] > [グループチャットとパーシステントチャット (Group Chat and Persistent Chat)] を選択します。

ステップ 2 ルームのオーナーは、ルームをメンバー専用にするかどうかを変更できます (**Room owners can change whether or not rooms are for members only**) チェックボックスの値を設定します。

- チェック済み - チャットルームの所有者は、チャットルームの設定を編集する管理権限を持っています。
- チェックなし - 管理者だけがチャットルーム設定を編集できます。

ステップ 3 [保存 (Save)] をクリックします。

ステップ 4 [Cisco Unified IM and Presenceのサービスアビリティ (Cisco Unified IM and Presence Serviceability)] で、[ツール (Tools)] > [コントロールセンター-機能サービス (Control Center - Feature Services)] を選択します。

ステップ5 Cisco XCP Text Conference Manager サービスの再起動

クライアントでのインスタントメッセージ履歴のログ記録の許可

ユーザがコンピュータでインスタントメッセージ履歴をローカルにログ記録することを防止または許可できます。クライアント側では、アプリケーションがこの機能をサポートしている必要があります。これは、インスタントメッセージのログ記録の防止を実行する必要があります。

手順

ステップ1 Cisco Unified CM IM and Presence Administration で、[メッセージング (Messaging)] > [設定 (Settings)] を選択します。

ステップ2 次のようにインスタントメッセージ履歴のログ記録の設定を行います。

- クライアントアプリケーションのユーザに IM and Presence サービスでインスタントメッセージ履歴のログ記録を許可する場合は、[クライアントでインスタントメッセージ履歴のログ記録を許可 (サポートされるクライアントでのみ) (Allow clients to log instant message history (on supported clients only))] をオンにしてください。
- クライアントアプリケーションのユーザに IM and Presence サービスでインスタントメッセージ履歴のログ記録を許可しない場合は、[クライアントでインスタントメッセージ履歴のログ記録を許可 (サポートされるクライアントでのみ) (Allow clients to log instant message history (on supported clients only))] をオフにしてください。

ステップ3 [保存 (Save)] をクリックします。

外部データベーステキスト会議レポートの表示

この手順を使用して、外部データベースのテキスト会議レポートを表示します。このレポートを使用すると、展開内の常設チャットルームの詳細を表示できます。

手順

ステップ1 [Cisco Unified CM IM and Presence Administration] にサイン インします

ステップ2 [メッセージング (Messaging)] > [グループチャットと常設チャット (Group Chat and Persistent Chat)] を選択します。

ステップ3 常設チャットデータベースの割り当てで、[報告書 (Report)] ボタンをクリックします。

ステップ4 選択範囲を特定の基準を満たす会議室に限定する場合は、フィルタツールを使用します。

ステップ5 [検索(Find)] をクリックします。

ステップ6 特定のチャットルームを選択してそのルームの詳細を表示します。

チャットルーム設定を設定します

チャットルーム数の設定

ユーザが作成できるルーム数を制限するには、ルーム設定を使用します。チャットルームの数を制限すると、システムのパフォーマンスをサポートし、拡張できます。ルーム数の制限は、起こり得るサービスレベル攻撃の軽減にも役立ちます。

手順

- ステップ1 [Cisco Unified CM IM and Presenceの管理 (Cisco Unified CM IM and Presence Administration)] で、[メッセージング (Messaging)] > [グループチャットとパーシステントチャット (Group Chat and Persistent Chat)] を選択します。
 - ステップ2 許可したチャットルームの最大数を変更するには、[許可されるルームの最大数 (Maximum number of rooms allowed)] のフィールドに値を入力します。デフォルトでは 5500 に設定されています。
 - ステップ3 [保存 (Save)] をクリックします。
-

チャットルームメンバー設定を設定します

メンバー設定では、チャットルームのメンバーシップを制御できます。このような制御は、メンバーシップの制御によって防止できるサービスレベル攻撃を軽減する上でユーザの役に立ちます。必要に応じてメンバーを設定します。

手順

- ステップ1 [Cisco Unified CM IM and Presenceの管理 (Cisco Unified CM IM and Presence Administration)] で、[メッセージング (Messaging)] > [グループチャットとパーシステントチャット (Group Chat and Persistent Chat)] を選択します。
 - ステップ2 ルームメンバーの設定の説明に従って、ルームメンバーの設定を構成します。
 - ステップ3 [保存 (Save)] をクリックします。
 - ステップ4 [Cisco Unified IM and Presenceのサービスアビリティ (Cisco Unified IM and Presence Serviceability)] で、[ツール (Tools)] > [コントロールセンター-機能サービス (Control Center - Feature Services)] を選択します。
 - ステップ5 Cisco XCP Text Conference Manager サービスを再起動します。
-

ルームメンバーの設定



- (注) 常設チャットルームは、作成時のセットアップを継承します。後で行った変更は、既存のルームには適用されません。これらの変更は、変更を有効にした後で、作成されたルームにのみ適用されます。

表 29:

フィールド	説明
デフォルトではルームはメンバー専用です (Rooms are for members only by default)	デフォルトでメンバー専用ルームとしてルームを作成する場合は、このチェックボックスをオンにします。メンバー専用ルームには、そのルームの所有者または管理者が設定した許可リストのユーザのみがアクセスできます。このチェックボックスは、デフォルトでオフになっています。 (注) 許可リストにはそのルームに許可されているメンバーのリストが含まれています。このリストは、メンバー専用ルームの所有者または管理者によって作成されます。
他のユーザをメンバー専用ルームに招待できるのはモデレーターのみです (Only moderators can invite people to members-only rooms)	モデレーターのみがルームへのユーザの招待を行えるようにルームを設定する場合は、このチェックボックスをオンにします。このチェックボックスをオフにしている場合は、メンバーが他のユーザをルームに参加するよう招待できます。デフォルトでは、このチェックボックスはオフになっています。
ルームのオーナーは、ルームをメンバー専用にするかどうかを変更できます (Room owners can change whether or not rooms are for members only)	メンバー専用のルームかどうかをルーム所有者が変更できるように設定する場合は、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。 (注) ルーム所有者は、そのルームを作成したユーザか、(許可されている場合は) ルーム作成者または所有者によって所有者ステータスを持つ者として指定されたユーザです。ルーム所有者は、ルーム設定の変更やルーム破棄のほか、その他のすべての管理機能を実行できます。

フィールド	説明
ルームのオーナーは、他のユーザをメンバー専用ルームに招待できるのはモデレーターに限定するかどうかを変更できます (Room owners can change whether or not only moderators can invite people to members-only rooms)	部屋の所有者がメンバーに他のユーザを部屋に招待できるように部屋を設定する場合は、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。
ユーザは自分自身をメンバーとしてルームに追加できます (Users can add themselves to rooms as members)	すべてのユーザがルームへの入室をいつでも要求できるようにルームを設定する場合は、このチェックボックスをオンにします。このチェックボックスがオンになっている場合、ルームはオープンメンバーシップになります。このチェックボックスは、デフォルトでオフになっています。
ルームのオーナーは、ユーザが自分自身をメンバーとしてルームに追加できるようにするかどうかを変更できます (Room owners can change whether users can add themselves to rooms as members)	ステップ 5 に記載されている設定をルーム所有者がいつでも変更できるようにルームを設定する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。

可用性の設定

アベイラビリティの設定は、ルーム内のユーザの可視性を決定します。

手順

-
- ステップ 1 [Cisco Unified CM IM and Presenceの管理 (Cisco Unified CM IM and Presence Administration)] で、[メッセージング (Messaging)] > [グループチャットとパーシステントチャット (Group Chat and Persistent Chat)] を選択します。
 - ステップ 2 可用性の設定の説明に従って、可用性メンバーの設定を構成します。
 - ステップ 3 [保存 (Save)] をクリックします。
 - ステップ 4 [Cisco Unified IM and Presenceのサービスアベイラビリティ (Cisco Unified IM and Presence Serviceability)] で、[ツール (Tools)] > [コントロールセンター-機能サービス (Control Center - Feature Services)] を選択します。
 - ステップ 5 Cisco XCP Text Conference Manager サービスの再起動
-

可用性の設定

フィールド	説明
ルーム内にいないメンバーや管理者がルームに表示されたままです (Members and administrators who are not in a room are still visible in the room)	ユーザが現在オフラインの場合でも、ユーザをルームリストに登録したい場合は、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。
ルームのオーナーは、ルーム内にいないメンバーや管理者がルームに表示されたままにするかどうかを変更できます (Room owners can change whether members and administrators who are not in a room are still visible in the room)	部屋の所有者がメンバーまたは管理者の表示を変更できるようにする場合は、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。
ルームは古いクライアントと下位互換性があります (Rooms are backwards-compatible with older clients)	このサービスを古いグループチャット1.0クライアントで正常に機能させる場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。
ルームのオーナーは、ルームが古いクライアントと下位互換性があるかようにするかどうかを変更できます (Room owners can change whether rooms are backwards-compatible with older clients)	部屋の所有者がチャットルームの下位互換性を制御できるようにする場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。
デフォルトで、ルームは匿名です (Rooms are anonymous by default)	ルームにユーザのニックネームは表示しても、Jabber ID は公開しない場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。
ルームのオーナーは、ルームを匿名にするかどうかを変更できます (Room owners can change whether or not rooms are anonymous)	ユーザの Jabber ID の匿名レベルをルーム所有者が管理できるようにする場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。

利用者数の設定

占有設定は、特定の時間にチャットルームに参加できるユーザ数を決定します。

手順

- ステップ 1** ルーム内で許可されるユーザのシステム最大数を変更するには、[同時にルームに入室できるユーザ数 (How many users can be in a room at one time)] のフィールドに値を入力します。デフォルト値は 1000 に設定されています。

(注) ルーム内のユーザの総数は、設定する値を超えることはできません。ルーム内のユーザの総数には、通常のユーザと非表示のユーザの両方が含まれます。

- ステップ 2** ルーム内で許可される非表示ユーザの数を変更するには、[同時に入室できる非表示ユーザ数 (How many hidden users can be in a room at one time)] のフィールドに値を入力します。非表示のユーザは他のユーザには表示されません。また、ルームにメッセージを送信できません。さらに、プレゼンス更新を送信しません。非表示のユーザは、ルーム内のすべてのメッセージを表示したり、他のユーザのプレゼンス更新を受信したりできます。デフォルト値は 1000 です。
- ステップ 3** ルーム内に許可されるユーザのデフォルトの最大数を変更するには、[デフォルトのルーム最大利用者数 (Default maximum occupancy for a room)] のフィールドに値を入力します。デフォルト値は 50 に設定され、ステップ 1 で設定された値よりも大きくできません。
- ステップ 4** デフォルトのルーム利用者数をルーム所有者が変更できるようにする場合は、[ルーム所有者がデフォルトのルーム最大利用者数を変更できます (Room owners can change default maximum occupancy for a room)] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。
- ステップ 5** [保存 (Save)] をクリックします。

チャットメッセージの設定

チャットメッセージ設定を使用して、役割に基づいた特権をユーザに付与します。ほとんどの場合、役割は、ビジターからモデレーターへの階層に存在します。たとえば、参加者はビジターができることはすべて実行できます。また、モデレーターは参加者ができることはすべて実行できます。

デフォルトでは、このチェックボックスはオフになっています。

手順

- ステップ 1** [ルーム内からプライベートメッセージを送信するためにユーザに必要な最小参加レベル (Lowest participation level a user can have to send a private message from within the room)] のドロップダウンリストから次のいずれかを選択します。
- [ビジター (Visitor)] を選択すると、ビジター、参加者、およびモデレータがルーム内の他のユーザにプライベートメッセージを送信できます。これはデフォルト設定です。
 - [参加者 (Participant)] を選択すると、参加者およびモデレーターがルーム内の他のユーザにプライベートメッセージを送信できます。
 - [モデレータ (Moderator)] を選択すると、モデレーターのみがルーム内の他のユーザにプライベートメッセージを送信できます。
- ステップ 2** プライベートメッセージの最小参加レベルをルーム所有者が変更できるようにする場合は、[ルーム内からプライベートメッセージを送信するためにユーザに必要な最小参加レベルをルーム所有者が変更できます (Room owners can change the lowest participation level a user can have

to send a private message from within the room)] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

ステップ 3 [ルームの件名を変更するためにユーザに必要な最小参加レベル (Lowest participation level a user can have to change a room's subject)] のドロップダウンリストから次のいずれかを選択します。

- a) **[参加者 (Participant)]** を選択すると、参加者およびモデレータがルームの件名を変更できます。これがデフォルト設定です。
- b) **[モデレータ (Moderator)]** を選択すると、モデレータのみがルームの件名を変更できます。

ビジターは、ルームの件名を変更できません。

ステップ 4 ルームの件名を更新するための最小参加者レベルをルーム所有者が変更できるようにする場合は、**[ルームの件名を変更するためにユーザに必要な最小参加レベルをルーム所有者が変更できます (Room owners can change the lowest participation level a user can have to change a room's subject)]** チェックボックスをオンにします。

ステップ 5 メッセージからすべての拡張可能ハイパーテキストマークアップ言語 (XHTML) を削除する場合は、**[すべての XHTML フォーマットをメッセージから削除します (Remove all XHTML formatting from messages)]** チェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。

ステップ 6 XHTML フォーマット設定をルーム所有者が変更できるようにする場合は、**[ルーム所有者が XHTML フォーマット設定を変更できます (Room owners can change XHTML formatting setting)]** チェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。

ステップ 7 **[保存 (Save)]** をクリックします。

モデレータ管理されたルームの設定

モデレータが管理するルームは、ルーム内のボイス特権を付与または取り消す機能をモデレータに提供します (グループチャットの場合、ボイスはチャットメッセージをルームに送信する機能のことです)。ビジターはモデレータが管理するルームでインスタントメッセージを送信できません。

手順

ステップ 1 モデレータの役割をルームで適用する場合は、**[デフォルトでモデレータがルームを管理します (Rooms are moderated by default)]** チェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。

ステップ 2 ルームをモデレータが管理するかどうかをルーム所有者が変更できるようにするには、**[デフォルトでモデレータがルームを管理するかどうかをルーム所有者が変更できます (Room owners can change whether rooms are moderated by default)]** チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

ステップ3 [保存 (Save)]をクリックします。

履歴の設定

履歴設定を使用して、ルームで取得し、表示するメッセージのデフォルト値および最大値を設定し、履歴クエリを使用して取得できるメッセージ数を管理します。ユーザがルームに入室すると、そのユーザはルームのメッセージ履歴に送信されます。履歴設定は、ユーザが受信する過去のメッセージ数を決定します。

手順

- ステップ1 ユーザがアーカイブから取得できるメッセージの最大数を変更するには、[アーカイブから取得できるメッセージの最大数 (Maximum number of messages that can be retrieved from the archive)]のフィールドに値を入力します。デフォルト値は100に設定されています。これは、次の設定の上限としての役割を果たします。
- ステップ2 ユーザがチャットルームに入室するときに表示される以前のメッセージの数を変更するには、[デフォルトで表示されるチャット履歴内のメッセージ数 (Number of messages in chat history displayed by default)]のフィールドに値を入力します。デフォルト値は15に設定され、ステップ1で設定された値よりも大きくできません。
- ステップ3 ユーザがチャットルームに入室したときに表示される以前のメッセージの数をルーム所有者が変更できるようにする場合は、[ルーム所有者がチャット履歴に表示されるメッセージ数を変更できます (Room owners can change the number of messages displayed in chat history)]チェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。
- ステップ4 [保存 (Save)]をクリックします。

チャットルームをシステムのデフォルトにリセットします

アドホックチャットルームと常設チャットルームの両方のグループチャット設定をシステムのデフォルトにリセットする場合は、この手順を使用します。



- (注) アドホックチャットはデフォルトで有効になっていますが、常設チャットはデフォルトで無効になっています。このタスクを完了すると、常設チャットが無効になります

手順

- ステップ1 Cisco Unified CM IM and Presence Administration で、[メッセージング (Messaging)]> [設定 (Settings)]を選択します。
- ステップ2 [デフォルトに設定 (Set to Default)]をクリックします。

ステップ3 [保存 (Save)] をクリックします。

チャットノードエイリアスの管理

チャットノードのエイリアスの管理

これらのタスクを実行して、クラスターのチャットノードエイリアスを管理します。システムにエイリアスを自動的に管理させることも、自分でエイリアスを更新することもできます。

手順

	コマンドまたはアクション	目的
ステップ1	チャットエイリアスの管理にモードを割り当てます (311 ページ)	システムにチャットノードエイリアスを管理させるのか、手動で管理させるのかを割り当てます。
ステップ2	チャットノードエイリアスを手動で追加 (312 ページ)	クラスターのチャットノードエイリアスを追加、編集、または削除します。

チャットエイリアスの管理にモードを割り当てます

システムを使用してチャットノードエイリアスを `conference-x-clusterid.domain` 命名規則を使って自動的に割り当てるかどうか、またはそれらを手動で割り当てるかどうかを設定します。

始める前に

チャットノードのエイリアスについては、[チャットノードエイリアスの概要 \(300 ページ\)](#) を参照してください。

手順

ステップ1 [Cisco Unified CM IM and Presenceの管理 (Cisco Unified CM IM and Presence Administration)] で、[メッセージング (Messaging)] > [グループチャットとパーシステントチャット (Group Chat and Persistent Chat)] を選択します。

ステップ2 システムで生成されたエイリアスを有効または無効にします。

- システムがチャットノードのエイリアスを自動的に割り当てるようにしたい場合は、システムがプライマリグループチャットサーバのエイリアスを自動的に管理しますをチェックします。

ヒント [メッセージング (Messaging)] > [グループチャットサーバのエイリアスマッピング (Group Chat Server Alias Mapping)] を選択して、システムで生成されたエイリアスが [プライマリグループサーバのエイリアス (Primary Group Chat Server Aliases)] の下にリストされていることを確認します。

- チャットノードエイリアスを手動で割り当てたい場合は、[System Automatically Manages Primary Group チャットサーバエイリアス (System Automatically Manages Primary Group Chat Server Aliases)] をオフにします。

次のタスク

- チャットノードにシステムで生成されたエイリアスを設定する場合でも、ノードと複数のエイリアスを必要に応じて関連付けることができます。
- 外部ドメインとフェデレーションすると、エイリアスが変更され、新しいエイリアスが使用可能であることをフェデレーション相手に通知する場合があります。すべてのエイリアスを外部にアダプタイズするには、DNS を設定し、DNS レコードとしてエイリアスをパブリッシュします。
- システム生成エイリアス設定を更新したら、これらの操作のいずれかを実行します：Cisco XCP Text Conference Manager の再起動。
- チャットノードエイリアスを追加、編集、または削除するには、[チャットノードエイリアスを手動で追加 \(312 ページ\)](#)。

チャットノードエイリアスを手動で追加

この手順を使用して、手動でチャットノードのエイリアスを追加、編集、または削除します。手動でチャットノードのエイリアスを管理するには、システムで生成されたエイリアスを使用するデフォルト設定をオフにする必要があります。システムで生成されたエイリアスをオフにすると、既存のエイリアス (conference-x-clusterid.domain) は、[会議サーバのエイリアス (Conference Server Aliases)] の下にリストされる標準の編集可能なエイリアスに戻ります。これにより、古いエイリアスとそのエイリアスに関連付けられているチャットルームのアドレスが維持されます。

チャットノードに手動で複数のエイリアスを割り当てることができます。システムで生成されたエイリアスがチャットノードにすでに存在する場合でも、ノードに追加エイリアスを手動で関連付けることができます。

手動管理されるエイリアスでは、クラスター ID またはドメインが変更された場合、手動でエイリアスリストを更新するのは管理者の責任です。システムで生成されたエイリアスが変更された値を自動的に組み込みます。



- (注) これは必須ではありませんが、ノードに新しいチャットノードのエイリアスを割り当てる場合はドメインを常を含めることを推奨します。追加エイリアスには、`newalias.domain` の表記を使用します。ドメインを確認するには、**[Cisco Unified CM IM and Presenceの管理 (Cisco Unified CM IM and Presence Administration)] > [プレゼンスの設定 (Presence Settings)] > [詳細設定 (Advanced Settings)]** を選択します。

始める前に

[チャットエイリアスの管理にモードを割り当てます \(311 ページ\)](#)

手順

- ステップ 1** **[Cisco Unified CM IM and Presenceの管理 (Cisco Unified CM IM and Presence Administration)]** で、**[メッセージング (Messaging)] > [グループチャットサーバエイリアスマッピング (Group Chat Server Alias Mapping)]** を選択します。
- ステップ 2** **[検索(Find)]** をクリックします。
- [グループチャットサーバエイリアス] ウィンドウに既存のノードエイリアスが表示されます。
- ステップ 3** 新しいエイリアスを追加するには
- [新規追加 (Add New)]** をクリックします。
 - グループチャットサーバのエイリアスフィールド**に、新しいエイリアスを入力します。
 - サーバの名前** ドロップダウンリストボックスから、エイリアスを割り当てるサーバを選択します。
 - [保存 (Save)]** をクリックします。
- ステップ 4** 既存のエイリアスを編集するには
- エイリアスを選択します。
 - 更新**を入力して**保存**をクリックします。
- ステップ 5** エイリアスを削除するには、エイリアスを選択して**[選択内容を削除 (Delete Selected)]** をクリックします。

次のタスク

- Cisco XCP Text Conference Manager をオンにする。

チャットノードエイリアスのトラブルシューティングのヒント

- どのチャットノードのエイリアスも一意でなければなりません。システムはクラスタ全体に重複したチャットノードのエイリアスを作成することを防ぎます。

- チャット ノードのエイリアス名を IM and Presence ドメイン名と同じにすることはできません。
- 古いエイリアスでチャットルームのアドレスを維持する必要がなくなった場合に限り古いエイリアスを削除します。
- 外部ドメインとフェデレーションすると、エイリアスに変更され、新しいエイリアスが使用可能であることをフェデレーション相手に通知する場合があります。すべてのエイリアスを外部にアドバタイズするには、DNS を設定し、DNS レコードとしてエイリアスをパブリッシュします。
- チャット ノードのエイリアス設定のいずれかを更新したら、Cisco XCP Text Conference Manager を再起動します。

常設チャット用の外部データベースの消去

外部データベースを監視し、期限切れのレコードを削除するジョブを設定します。これにより、新しいレコード用に常に十分なディスク容量が確保されます。

常設チャットのデータベーステーブルを消去するには、必ず**機能テーブル**の下にある**テキスト会議 (TC)** を選択します。

手順

-
- ステップ 1** データベース パブリッシャ ノードで Cisco Unified CM IM and Presence Administration にログインします。
- ステップ 2** [メッセージング (Messaging)] > [外部データベースの設定 (External Server Setup)] > [外部データベース ジョブ (External Databases Jobs)] を選択します。
- ステップ 3** 外部 DB を消去しますをクリックします。
- ステップ 4** 次のいずれかを実行します。
- パブリッシャノードに接続する外部データベースを手動でクリーンアップするには、**SameCup ノード** を選択します。
 - 加入者ノードに接続する外部データベースを手動でクリーンアップするには、**その他の CupNode** を選択してから、外部データベースの詳細を選択します。
 - 外部データベースを自動的に監視および消去するようにシステムを設定している場合は、**自動クリーンアップラジオボタン** をチェックします。
- (注) 自動クリーンアップを設定する前に手動クリーンアップを実行することをお勧めします。
- ステップ 5** ファイル削除のために戻りたい**日数**を設定します。たとえば、90 と入力すると、システムは 90 日以上経過したレコードを削除します。
- ステップ 6** **スキーマを更新**をクリックしてデータベースのインデックスとストアードプロシージャを作成します。

(注) スキーマを更新する必要があるのは、ジョブを初めて実行したときだけです。

ステップ7 ファイル削除のために戻りたい日数を設定します。たとえば、**90** と入力すると、システムは 90 日以上経過したレコードを削除します。

ステップ8 機能テーブルセクションで、レコードをクリーンアップするための各機能を選択します。

- **テキスト会議 (TC)** - 常設チャット機能のデータベーステーブルを消去するには、このオプションを選択します。
- **メッセージアーカイバ (MA)** - Message Archiver 機能のデータベーステーブルを消去するには、このオプションを選択します。
- **非同期ファイル転送 (AFT)** - Managed File Transfer 機能のデータベーステーブルを消去するには、このオプションを選択します。

ステップ9 [クリーンアップジョブを送信 (Submit Clean-up Job)] をクリックします。

(注) [自動 (Automatic)] オプションが有効になっていて、それを無効にする場合は、[自動クリーンアップジョブの無効化 (Disable Automatic Clean-up Job)] ボタンをクリックします。

チャット相互作用の管理

チャット ノードのエイリアスを変更すると、データベースのチャットルームのアドレス指定が不可能になり、ユーザが既存のチャットルームを検索できなくなることがあります。

エイリアスまたは他のノードの依存関係の構成部分を変更する前にこれらの結果に注意してください。

- **クラスタ ID** : この値は完全修飾クラスタ名 (FQDN) の一部です。クラスタ ID を変更 ([システム (System)] [プレゼンス トポロジの設定 (Presence Topology Settings)] を選択) すると、FQDN はクラスタ全体で自動的に変更される新しい値およびシステム管理されたエイリアスを組み込みます。手動管理されたエイリアスでは、クラスタ ID が変更された場合、手動でエイリアス リストを更新するのは管理者の責任です。
- **ドメイン** : この値は FQDN の一部です。ドメインを変更 ([プレゼンス (Presence)] [プレゼンスの設定 (Presence Settings)] を選択) すると、FQDN はクラスタ全体で自動的に変更される新しい値およびシステム管理されたエイリアスを組み込みます。手動管理されたエイリアスでは、ドメインが変更された場合、手動でエイリアス リストを更新するのは管理者の責任です。
- **チャット ノードと外部データベース間の接続** : 永続的なチャットが有効で、外部データベースとの適切な接続が維持されていない場合、チャット ノードは起動しません。
- **チャット ノードの削除** : プレゼンス トポロジから既存のエイリアスに関連付けられているノードを削除した場合、それ以上の処理を行わない限り、その古いエイリアスを使用して作成したチャットルームをアドレス指定できないことがあります。

変更の広い影響を考慮せずに既存のエイリアスを変更しないことを推奨します。つまり、次のようにします。

- ユーザが必要に応じて古いエイリアスによって既存のチャットルームを検索できるように、データベースに古いチャット ノードのアドレスを維持します。
- 外部ドメインとのフェデレーションがある場合、DNS エイリアスをパブリッシュして、エイリアスが変更され、新しいアドレスが使用可能であることをそのドメインのユーザに通知する必要があります。これはすべてのエイリアスを外部にアドバタイズするかどうかによって異なります。



第 24 章

マネージド ファイル転送管理

- [マネージドファイル転送管理の概要 \(317 ページ\)](#)
- [マネージドファイル転送管理の前提条件 \(318 ページ\)](#)
- [マネージドファイル転送管理のタスクフロー \(318 ページ\)](#)

マネージド ファイル転送管理の概要

IM and Presence サービスの管理者として、あなたはマネージドファイル転送機能のためのファイルストレージとディスク使用量を管理する責任があります。この章を使用して、ファイルストレージとディスク使用量のレベルを監視し、レベルが定義済みのしきい値を超えたときに知らせるためのカウンタと警告を設定します。

外部ファイルサーバとデータベースサーバの管理

外部データベースのサイズを管理するときは、指定に応じてファイルをデータベースから自動的に消去するように、クエリとシェルスクリプトを組み合わせることができます。クエリを作成するには、ファイル転送メタデータを使用します。これには転送タイプ、ファイルタイプ、タイムスタンプ、ファイルサーバ上のファイルの絶対パスなどの情報が含まれます。

1 対 1 の IM やグループチャットは通常、一時的なものなので、転送されたファイルをすぐに削除できる可能性があります。IM やグループチャット内でのファイル転送の処理方法を選択する際には、そのことを考慮に入れてください。ただし、次の点に注意してください。

- オフラインユーザに配信される IM のために、ファイルに対する遅延要求が発生する可能性があります。
- 永続的なチャットの転送は、長期間保持される必要がある可能性があります。



- (注)
- 現在の UTC 時間中に作成されたファイルは消去しないでください。
 - ファイル サーバ構成（ファイル サーバそのものではない）の名前は、ファイル サーバが割り当てられた後で変更できます。
 - マネージドファイル転送がすでに設定済みで、設定を変更した場合には、Cisco XCP Router サービスを再起動すると、マネージドファイル転送機能が再開されます。
 - （ファイルサーバ自体での設定の変更を伴うことなく）他のいずれかの設定を変更した場合、ファイル転送機能が停止し、Cisco XCP Router サービスを再起動するよう促す通知を受け取ります。
 - データベースまたはファイルサーバに障害が発生した場合、その障害を明記するメッセージが生成されます。ただし、エラー応答では、データベースの障害、ファイルサーバの障害、他の何らかの内部障害が区別されません。データベースまたはファイルサーバに障害が発生した場合も、リアルタイム監視ツールはアラームを生成します。このアラームは、ファイル転送が行われているかどうかとは無関係です。

マネージド ファイル転送管理の前提条件

マネージド ファイル転送機能の設定

マネージド ファイル転送管理のタスクフロー

手順

	コマンドまたはアクション	目的
ステップ 1	AFT_LOG テーブル例クエリおよび出力 (319 ページ)	次の手順では、次の手順で実行できるクエリの例を示します。AFT_LOG 表と、ファイルサーバから不要なファイルを削除するための出力の使用方法
ステップ 2	サービスパラメータのしきい値の設定 (321 ページ)	マネージド ファイル転送サービス パラメータを設定して、外部ファイルサーバのディスク領域に関する RTMT アラームが生成されるしきい値を定義します。
ステップ 3	XCP File Transfer Manager のアラームの設定 (322 ページ)	マネージド ファイル転送のアラームを設定して、定義されたしきい値に達したときに知らせる。

	コマンドまたはアクション	目的
ステップ 4	マネージド ファイル転送の外部データベースを消去する (324 ページ)	これはオプションです。外部データベースを監視し、期限切れのレコードを削除するジョブを設定するには、外部データベースクリーンアップユーティリティを使用します。これにより、新しいレコード用に常に十分なディスク容量が確保されます。

AFT_LOG テーブル例クエリおよび出力

次の手順では、次の手順で実行できるクエリの例を示します。AFT_LOG 表と、ファイルサーバから不要なファイルを削除するための出力の使用方法

このクエリは、指定された日付以降にアップロードされたすべてのファイルのレコードを返します。



(注) サンプル SQL コマンドについては、[外部データベースのディスク使用量 \(320 ページ\)](#) を参照してください。

手順

ステップ 1 IM and Presence サービスのコマンドラインインターフェイス (CLI) で、次のコマンドを入力します。

file_path を選択します

```
FROM aft_log
```

```
WHERE method = 'Post' AND timestampvalue > '2014-12-18 11:58:39';
```

以下の出力が得られた。

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name1
```

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name2
```

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name3
```

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name4
```

...

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name99
```

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name100
```

ステップ 2 `rm` コマンドとこの出力を使用して、外部ファイル サーバから上記のファイルを削除するスクリプトを作成します。サンプル SQL クエリについては、『*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

(注) ファイルに関連するレコードが外部データベースからすでに消去されていても、そのファイルが外部ファイルサーバからまだ消去されていなければ、そのファイルを引き続きアクセス/ダウンロードできます。

次のタスク

[サービスパラメータのしきい値の設定 \(321 ページ\)](#)

外部データベースのディスク使用量

ディスクやテーブルスペースが満杯にならないようにする必要があります。満杯になると、マネージドファイル転送機能が動作を停止することがあります。以下は、外部データベースからレコードを消去するために使用できるサンプル SQL コマンドです。追加クエリについては、『*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。



(注) ファイルに関連するレコードが外部データベースからすでに消去されていても、そのファイルが外部ファイルサーバからまだ消去されていなければ、そのファイルを引き続きアクセス/ダウンロードできます。

操作	コマンド例
アップロードされたファイルのすべてのレコードを削除します。	<pre>DELETE FROM aft_log WHERE method = 'Post';</pre>
特定のユーザによってダウンロードされたすべてのファイルの記録を削除します。	<pre>DELETE FROM aft_log WHERE jid LIKE '<userid>@<domain>%' AND method = 'Get';</pre>
特定の時刻の後にアップロードされたすべてのファイルのレコードを削除するには、次のコマンドを実行します。	<pre>DELETE FROM aft_log WHERE method = 'Post' AND timestampvalue > '2014-12-18 11:58:39';</pre>

さらに、データベースのディスク使用量を管理するのに役立つカウンタおよびアラームがあります。詳細については、[マネージドファイル転送のアラームとカウンタ \(322 ページ\)](#) を参照してください。

サービスパラメータのしきい値の設定

マネージドファイル転送サービスパラメータを設定して、外部ファイルサーバのディスク領域に関する RTMT アラートが生成されるしきい値を定義します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [サービスパラメータ (Service Parameters)] を選択します。

ステップ 2 ノードの [Cisco XCP File Transfer Manager] サービスを選択します。

ステップ 3 次のサービスパラメータの値を入力します。

- **外部ファイルサーバの使用可能領域の下限しきい値 (External File Server Available Space Lower Threshold)** : 外部ファイルサーバパーティションで使用可能な領域の割合 (パーセンテージ) がこの値以下になると、XcpMFTEExtFsFreeSpaceWarn アラームが生成されます。デフォルト値は 10% です。
- **外部ファイルサーバの使用可能領域の上限しきい値 (External File Server Available Space Upper Threshold)** : 外部ファイルサーバパーティションで使用可能な領域の割合 (パーセンテージ) がこの値以上になると、XcpMFTEExtFsFreeSpaceWarn アラームが解除されます。デフォルト値は 15% です。

(注) 下限しきい値を上限しきい値より大きい値に設定しないでください。設定された場合、Cisco XCP Router サービスを再起動しても Cisco XCP File Transfer Manager サービスが起動しません。

ステップ 4 [保存 (Save)] をクリックします。

ステップ 5 Cisco XCP Router サービスを再起動します。

- a) [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
- b) [サーバ (Server)] ドロップダウンから、IM and Presence パブリッシャーを選択し、[移動 (Go)] をクリックします。
- c) [IM and Presence サービス (IM and Presence Services)] の下で、[Cisco XCP ルータ (Cisco XCP Router)] を選択し、[リスタート (Restart)] をクリックします

次のタスク

[XCP File Transfer Manager のアラームの設定 \(322 ページ\)](#)

XCP File Transfer Manager のアラームの設定

マネージド ファイル転送のアラームを設定して、定義されたしきい値に達したときに知らせる。

手順

- ステップ 1 Cisco Unified IM and Presence のサービスアビリティにサインインします。
- ステップ 2 [アラーム (Alarm)] > [設定 (Configuration)] を選択します。
- ステップ 3 [サーバ (Server)] ドロップダウンから、サーバ (ノード) を選択して、[移動 (Go)] をクリックします。
- ステップ 4 [サービス グループ (Service Group)] ドロップダウンリストから、[IM and Presence サービス (IM and Presence Services)] を選択し、[移動 (Go)] を選択します。
- ステップ 5 [サービス (Service)] ドロップダウンリストから [Cisco XCP File Transfer Manager (アクティブ) (Cisco XCP File Transfer Manager (Active))] を選択し、[移動 (Go)] をクリックします。
- ステップ 6 お好みのアラーム設定を行います。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。
- ステップ 7 [保存 (Save)] をクリックします。

次のタスク

利用可能なアラームとカウンタの詳細については、を参照してください。 [マネージド ファイル転送のアラームとカウンタ \(322 ページ\)](#)

マネージド ファイル転送のアラームとカウンタ

マネージドファイル転送では、転送されたファイルがユーザへ配信されるのは、これらのファイルが外部ファイルサーバに正常にアーカイブされ、しかもファイルのメタデータが外部データベースに記録された後になります。IM and Presence Service ノードが外部ファイルサーバまたは外部データベースとの接続を失った場合、IM and Presence Service は受信者にファイルを配信しません。

マネージド ファイル転送のアラーム

接続が失われたときに通知を受け取るようにするには、以下のアラームが Real-Time Tool で正しく設定されていることを確認する必要があります。



- (注) 外部ファイルサーバへの接続が失われる前にアップロードされたファイル、および受信者にダウンロード中であったファイルは、ダウンロードに失敗します。ただし、失敗した転送のレコードが外部データベースに残ります。これらのファイルを特定するには、外部データベースフィールド file_size と bytes_transferred の不一致を調べることができます。

表 30: マネージド ファイル転送のアラーム

アラーム	問題	解決方法
XcpMFTextFsMountError	Cisco XCP File Transfer Manager で外部ファイルサーバとの接続が失われました。	External File Server Troubleshooter で詳細を確認してください。 外部ファイルサーバが正常に動作していることを確認します。 外部ファイルサーバとのネットワーク接続に問題があるかどうか確認します。
XcpMFTextFsFreeSpaceWarn	Cisco XCP File Transfer Manager は、外部ファイルサーバの空きディスク領域が少ないことを検出しました。	ファイル転送に使われるパーティションから不要なファイルを削除して、外部ファイルサーバの領域を解放します。
XcpMFTDBConnectError	Cisco XCP データ アクセスレイヤがデータベースに接続できませんでした。	システムトラブルシュータで詳細を確認してください。 外部データベースが正常に動作していること、および外部データベースサーバとのネットワーク接続に問題があるかどうか確認します。
XcpMFTDBFullError	Cisco XCP File Transfer Manager は、ディスクまたはテーブルスペースのいずれかがいっぱいであるため、外部データベースにデータを挿入または変更できません。	データベースを確認し、ディスクスペースを解放または回復できるかどうか評価します。 データベース容量を追加することも検討してください。

マネージド ファイル転送のカウンタ

マネージド ファイル転送を管理しやすくするために、Real-Time Monitoring Tool を介して以下のカウンタを監視できます。これらのカウンタは、Cisco XCP MFT Counters フォルダに保存されています。

表 31: マネージド ファイル転送のカウンタ

カウンタ	説明
MFTBytesDownloadedLastTimeslice	このカウンタは、最後のレポートインターバル（通常は 60 秒）の間にダウンロードされたバイト数を表します。

カウンタ	説明
MFTBytesUpoadedLastTimeslice	このカウンタは、最後のレポートインターバル（通常は60秒）の間にアップロードされたバイト数を表します。
MFTFilesDownloaded	このカウンタは、ダウンロードされたファイルの総数を表します。
MFTFilesDownloadedLastTimeslice	このカウンタは、最後のレポートインターバル（通常は60秒）の間にダウンロードされたファイル数を表します。
MFTFilesUploaded	このカウンタは、アップロードされたファイルの総数を表します。
MFTFilesUploadedLastTimeslice	このカウンタは、最後のレポートインターバル（通常は60秒）の間にアップロードされたファイル数を表します。

マネージドファイル転送の外部データベースを消去する

外部データベースを監視し、期限切れのレコードを削除するジョブを設定します。これにより、新しいレコード用に常に十分なディスク容量が確保されます。

マネージドファイル転送用のデータベーステーブルを消去するには、必ず**機能テーブル**の下にある**非同期ファイル転送 (AFT)** を選択してください。

手順

- ステップ1 データベース パブリッシャ ノードで Cisco Unified CM IM and Presence Administration にログインします。
- ステップ2 [メッセージング (Messaging)] > [外部データベースの設定 (External Server Setup)] > [外部データベース ジョブ (External Databases Jobs)] を選択します。
- ステップ3 外部 DB を消去しますをクリックします。
- ステップ4 次のいずれかを実行します。

- パブリッシャノードに接続する外部データベースを手動でクリーンアップするには、**SameCup ノード**を選択します。
- 加入者ノードに接続する外部データベースを手動でクリーンアップするには、**その他の CupNode** を選択してから、外部データベースの詳細を選択します。
- 外部データベースを自動的に監視および消去するようにシステムを設定している場合は、**自動クリーンアップラジオボタン**をチェックします。

(注) 自動クリーンアップを設定する前に手動クリーンアップを実行することをお勧めします。

- ステップ5** ファイル削除のために戻りたい日数を設定します。たとえば、**90** と入力すると、システムは 90 日以上経過したレコードを削除します。
- ステップ6** **スキーマを更新**をクリックしてデータベースのインデックスとストアードプロシージャを作成します。
- (注) スキーマを更新する必要があるのは、ジョブを初めて実行したときだけです。
- ステップ7** ファイル削除のために戻りたい日数を設定します。たとえば、**90** と入力すると、システムは 90 日以上経過したレコードを削除します。
- ステップ8** **機能テーブルセクション**で、レコードをクリーンアップするための各機能を選択します。
- **テキスト会議 (TC)** - 常設チャット機能のデータベーステーブルを消去するには、このオプションを選択します。
 - **メッセージアーカイバ (MA)** - Message Archiver 機能のデータベーステーブルを消去するには、このオプションを選択します。
 - **非同期ファイル転送 (AFT)** - Managed File Transfer 機能のデータベーステーブルを消去するには、このオプションを選択します。
- ステップ9** [クリーンアップジョブを送信 (Submit Clean-up Job)] をクリックします。
- (注) [自動 (Automatic)] オプションが有効になっていて、それを無効にする場合は、[自動クリーンアップジョブの無効化 (Disable Automatic Clean-up Job)] ボタンをクリックします。

■ マネージドファイル転送の外部データベースを消去する



第 25 章

エンドユーザの管理

- エンドユーザの管理の概要 (327 ページ)
- エンドユーザーのタスクフローを管理する (329 ページ)
- プレゼンスの連携動作と制限事項 (341 ページ)

エンドユーザの管理の概要

IM and Presence Service ノードへユーザを割り当てて、エンドユーザを IM and Presence Service 用に設定する手順については、次のガイドを参照してください。

エンドユーザを管理するための管理タスクの一部として、次のタスクを管理しなければならない場合があります。

- プレゼンス要求を承認するためのデフォルトポリシーを設定する
- 重複または無効なユーザー ID とディレクトリ URI に対するスケジュールされたシステムチェックを設定する
- ユーザー ID とディレクトリ URI の問題が発生したらそれらを修正

エンドユーザーをインポートして設定する方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure End Users」のセクションを参照してください。

ユーザ連絡先リストの一括インポートおよびエクスポートの完了については、[連絡先リストの一括管理 \(427 ページ\)](#) を参照してください。

プレゼンス認証の概要

プレゼンスサブスクリプション要求にはシステム認証ポリシーを割り当てる必要があります。プレゼンス認証ポリシーは、システムレベルで、プレゼンスが要求されているエンドユーザの認証を必要とせずに、システム上のエンドユーザが他のエンドユーザのプレゼンスステータスを表示できるかどうかを決定します。この設定は**プレゼンス設定**設定ウィンドウにある**承認を求められることなくユーザが他のユーザの在席状況を確認できる**チェックボックス経由で設定できます。空き時間の設定は展開されているプロトコルによって部分的に異なります。

- SIP ベースのクライアントの場合、すべてのプレゼンス登録要求を自動的に承認するように IM and Presence サービスを設定する必要があります。そうしないと、プレゼンスは正しく機能しません（これがデフォルト設定です）。このオプションが設定されている場合、IM and Presence サービスは1つの例外を除いてすべての要求を自動的に承認します:参加がリクエストされているユーザーが、そのリクエストをしたユーザーを含む Cisco Jabber クライアントに設定されたブロック済みリストを持っている場合。この場合、ユーザはプレゼンス要求を承認するように促されます。
- XMPP ベースのクライアントの場合、IM and Presence サービスで他のユーザからのプレゼンス要求を承認するようにユーザに要求するかどうか、またはそれらのプレゼンス要求を自動的に承認するかどうかを設定できます。



(注) 認証システム設定は、エンドユーザが Cisco Jabber クライアント内で設定できるユーザポリシー設定によって上書きされる可能性があります。

Jabber のユーザポリシー設定

プレゼンス要求を承認するとき、IM and Presence サービスは、ユーザが Cisco Jabber クライアント内で設定したユーザポリシーも参照します。エンドユーザは他のユーザをブロックリストに追加して他のユーザが許可なしにプレゼンス状態を表示できないようにしたり、許可リストに追加して自分のプレゼンス状態の表示を許可することができます。これらの設定はシステムのデフォルト設定を上書きします。

エンドユーザは、Cisco Jabber クライアント内で次のものを設定できます。

- ブロックリスト - ユーザは他のユーザ（ローカルユーザと外部のユーザーの両方）をブロックリストに追加できます。拒否されているユーザの任意のユーザがプレゼンスを見る場合、ユーザの実際のステータスに関係なくユーザのプレゼンスステータスは常に空いていないと表示されます。ユーザはフェデレーションドメイン全体を拒否することもできます。
- 許可リスト - ユーザは、他のローカルユーザおよび外部のユーザーがいつでも自分の在席状況を表示できるようにすることができます。外部（フェデレーション）ドメイン全体を許可することもできます。
- [デフォルトポリシー（Default policy）] : そのユーザのデフォルトポリシー設定。ユーザは、すべてのユーザを拒否するか、すべてのユーザを許可するようにポリシーを設定できます。

ユーザー ID とディレクトリ URI の検証

単一クラスタ展開の場合、同じクラスタ内で重複を割り当てることはできないため、重複したユーザー ID とディレクトリ URI は問題になりません。ただし、クラスタ間配置では、異なるクラスタの異なるユーザに意図せずに同じユーザー ID またはディレクトリ URI 値を割り当てる可能性があります。

IM and Presence サービスには、重複するユーザー ID と重複するディレクトリ URI を確認するための次の検証ツールがあります。

- **Cisco IM and Presence データモニタサービス**：このサービスを使用して継続的なシステムチェックを設定できます。Cisco IM and Presence Data Monitor サービスは、Active ディレクトリ エントリで、すべての IM and Presence Service クラスタの重複ユーザー ID および重複、または、空のディレクトリ URI をチェックします。管理者にはアラームまたはアラートで通知されます。Cisco Unified Real-Time モニタリングツールを使用して、アラームを監視し、Duplicate UserID および DuplicateDirectoryURI エラーに関する電子メールアラートを設定できます。
- システムトラブルシューティングツール-ディレクトリの URI やユーザー ID の重複など、アドホックにシステムのエラーチェックを実行する場合は、システムトラブルシューティングツールを使用します。Troubleshooter は、最大 10 人のユーザにのみ詳細を提供します。システムトラブルシュータには Cisco Unified CM IM and Presence の管理インターフェイスから、**[診断 (Diagnostics)] > [システムトラブルシュータ (System Troubleshooter)]** からアクセスできます。
- コマンドラインインターフェイス - 重複した URI とユーザー ID の完全で詳細なレポートを入手するには、utils ユーザがすべて検証する CLI コマンドを実行します。

エンドユーザーのタスクフローを管理する

手順

	コマンドまたはアクション	目的
ステップ 1	プレゼンス認証ポリシーを割り当てる (330 ページ)	プレゼンスサブスクリプション要求にシステム認証ポリシーを割り当てます。
ステップ 2	ユーザデータに対するデータモニタチェックの設定 (331 ページ)	重複ディレクトリ URI およびユーザー ID に対して定期チェックを実行するように Cisco IM and Presence データモニタサービスを設定します。問題が見つかったら、システムアラームまたは警告が発生します。
ステップ 3	システムトラブルシューターを介してユーザデータを検証する (333 ページ)	重複したディレクトリ URI やユーザー ID など、システムの問題について特別チェックを実行する場合は、システムトラブルシュータを実行します。
ステップ 4	CLI を介してユーザー ID とディレクトリ URI を検証する (334 ページ)	CLI コマンドを実行して、重複するディレクトリ URI とユーザー ID の詳細レポートを取得します。

	コマンドまたはアクション	目的
ステップ 5	ユーザのプレゼンス設定を表示 (338 ページ)	IM and Presence 対応のエンドユーザのプレゼンス設定を表示したい場合は、プレゼンスビューアを使用してそれらの設定を表示できます。

プレゼンス認証ポリシーを割り当てる

プレゼンスサブスクリプション要求にシステム認証ポリシーを割り当てます。



- (注) Cisco Jabber クライアントでは、エンドユーザは他のユーザが自分のプレゼンスステータスを表示できるようにするかどうかを設定できます。このユーザポリシーはシステム許可設定を上書きします。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[プレゼンス (Presence)] > [設定 (Settings)] を選択します。

ステップ 2 [承認を求められることなくユーザが他のユーザの在席状況を確認できる (Allow users to view the availability of other users without being prompted for approval)] チェックボックスにチェックする、またはチェックを外します。

- チェック済 - IM and Presence は、ローカル企業内で受信するすべてのプレゼンス登録要求を許可します。
- 未チェック - IM and Presence は、プレゼンスが要求されているクライアントに対して、すべてのプレゼンス購読要求を参照します。ユーザは、要求を受諾または拒否できます。

(注) SIP ベースのクライアントを展開している場合は、このチェックボックスをオンにする必要があります。チェックボックスをオフのままにした場合、展開はXMPPクライアントのみをサポートします。

ステップ 3 [保存 (Save)] をクリックします。

ステップ 4 Cisco XCP Router サービスを再起動します。

次のタスク

IM and Presence サービスの SIP パブリッシュ トランクの設定に進みます。

ユーザデータに対するデータモニタチェックの設定

スケジュールされた間隔でディレクトリ URI とユーザー ID を検証するように Cisco IM and Presence データモニタを設定するには、次の作業を実行してください。エラーが発生した場合は、アラームまたはアラートを介して Cisco Unified Real-Time Monitoring Tool に通知されます。



(注) ディレクトリ URI の重複とユーザー ID の重複のエラーは、クラスタ間展開でのみ問題になります。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザー ID とディレクトリ URI 検証チェックのスケジュール設定 (331 ページ)	Cisco IM and Presence データモニタチェックのスケジュール間隔を設定します。このサービスは、重複するディレクトリ URI やユーザー ID を含む、アクティブディレクトリエントリのエラーをチェックします。
ステップ 2	電子メールアラート用の電子メールサーバをセットアップします。 (332 ページ)	これはオプションです。Data Monitor サービスが重複するディレクトリ URI またはユーザー ID を検出したときに Eメールアラートを受信したい場合は、リアルタイム監視ツールを使用して Eメールサーバを設定する必要があります。
ステップ 3	電子メールアラートの有効化 (333 ページ)	これはオプションです。DuplicateDirectoryURI および DuplicateUserid アラームの電子メール警告を有効にするには、この手順を実行します。Cisco IM and Presence データモニタサービスがこれらのアラームのいずれかを返すと、電子メールが管理者に送信されます。

ユーザー ID とディレクトリ URI 検証チェックのスケジュール設定

Cisco IM and Presence データモニタサービスのスケジュール間隔を設定します。このサービスは、重複するディレクトリ URI やユーザー ID など、データエラーについてスケジュールされた間隔でシステムをチェックします。このサービスは、エラーが見つかったときはいつでもリアルタイム監視ツールを介して表示できるアラームまたは警告を発します。

電子メールアラート用の電子メールサーバをセットアップします。

始める前に

Cisco IM and Presence データモニタネットワークサービスが実行されている必要があります。デフォルトにより、このサービスは実行されます。このサービスが Cisco Unified IM and Presence Serviceability インターフェースの [コントロールセンター - ネットワークサービス (Control Center - Network Services)] ウィンドウから実行されていることを確認できます。

手順

-
- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。
 - ステップ 2 [サービス (Service)] ドロップダウンで、[Cisco IM and Presence データ モニタ (Cisco IM and Presence Data Monitor)] を選択します。
 - ステップ 3 [User Check Interval] フィールドで、時間間隔を入力します。5 から 1440 (分) までの整数を入力できます。デフォルト値は 30 分です。
 - ステップ 4 [保存 (Save)] をクリックします。
-

次のタスク

これはオプションです。DuplicateDirectoryURI または DuplicateUserid アラームが発生したときに電子メール警告を設定したい場合は、[電子メールアラート用の電子メールサーバをセットアップします。](#) (332 ページ)

電子メールアラート用の電子メールサーバをセットアップします。

データモニタの検証チェックでディレクトリ URI とユーザー ID の重複エラーが検出された場合は、管理者に電子メールによる警告を受信させると便利です。その場合は、このオプションの手順を使用して、E メールアラート用に E メールサーバをセットアップします。

手順

-
- ステップ 1 Real-Time Monitoring Tool のシステム ウィンドウで、[アラート セントラル (Alert Central)] をクリックします。
 - ステップ 2 [システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [電子メールサーバの設定 (Config Email Server)] の順に選択します。
 - ステップ 3 [メールサーバ設定 (Mail Server Configuration)] ポップアップで、メールサーバの詳細を入力します。
 - ステップ 4 OK をクリックします。
-

次のタスク

[電子メールアラートの有効化 \(333 ページ\)](#)

電子メールアラートの有効化

この手順を使用して、DuplicateUserID または DuplicateDirectoryURI システムアラートが発生したときに管理者に電子メールを送信するようにリアルタイム監視ツールを設定します。

始める前に

[電子メールアラート用の電子メールサーバをセットアップします。 \(332 ページ\)](#)

手順

-
- ステップ 1 Real-Time Monitoring Tool の [システム (System)] 領域で、[アラート セントラル (Alert Central)] をクリックします。
 - ステップ 2 クリック **IM** と **プレゼンスタブ**。
 - ステップ 3 E メールアラートを追加したいアラートをクリックします。例えば、**DuplicateDirecctoryURI** または **DuplicateUserid** システムアラート
 - ステップ 4 [ツール (Tools)] > [アラート (Alert)] > [アラート アクションの設定 (Config Alert Action)] の順に選択します。
 - ステップ 5 [アラート アクション (Alert Action)] ポップアップで、[デフォルト (Default)] を選択して、[編集 (Edit)] をクリックします。
 - ステップ 6 [アラート アクション (Alert Action)] ポップアップで、受信者を追加します。
 - ステップ 7 ポップアップ ウィンドウで、電子メールアラートを送信するアドレスを入力して、[OK] をクリックします。
 - ステップ 8 [アラート アクション (Alert Action)] ポップアップで、アドレスが [受信者 (Recipients)] に表示されていることと、[有効 (Enable)] チェックボックスがオンになっていることを確認します。
 - ステップ 9 **OK** をクリックします。
 - ステップ 10 この手順、電子メール警告を有効にしたいシステム警告ごとに繰り返します。
-

システムトラブルシューターを介してユーザデータを検証する

Cisco Unified CM IM and Presence 管理 GUI のシステムトラブルシューターを使用することで、重複ユーザー ID および重複または無効なディレクトリ URI の展開をチェックします。トラブルシューターツールは、展開内のすべてのノードとクラスタを確認します。

手順

ステップ 1 Cisco Unified CM IM and Presence Administration で、[診断 (Diagnostics)] > [システムトラブルシュータ (System Troubleshooter)] を選択します。

ステップ 2 ユーザー ID とディレクトリ URI のステータスを [ユーザトラブルシュータ (User Troubleshooter)] 領域で監視します。システムチェックで何らかの問題が検出された場合は、[問題 (Problem)] 列に表示されます。

- すべてのユーザに一意のユーザー ID が設定されていることを確認します。
- すべてのユーザにディレクトリ URI が設定されていることを確認します。
- すべてのユーザに一意のディレクトリ URI が設定されていることを確認します。
- すべてのユーザに有効なディレクトリ URI が設定されていることを確認します。
- すべてのユーザに一意のメール ID が設定されていることを確認します。

(注) 重複したメール ID は、フェデレーションと Exchange Calendar の統合機能の両方のメールアドレスに影響を与えます。

ステップ 3 問題が生じたら、[ソリューション (Solution)] 列の [修正 (fix)] リンクをクリックすると、Cisco Unified Communications Manager の管理 (Cisco Unified Communications Manager Administration) の [エンドユーザの設定 (End User Configuration)] ウィンドウにリダイレクトされます。このウィンドウで、ユーザプロフィールを再設定することができます。

(注) ユーザプロフィールでのユーザー ID とディレクトリ URI フィールドは、LDAP Directory にマップされる場合があります。この場合は、LDAP Directory サーバで修正を行います。

次のタスク

何らかの問題が生じたら、ユーザー設定を Cisco Unified Communications Manager の [エンドユーザの設定 (End User Configuration)] ウィンドウで編集します。ユーザが LDAP ディレクトリから同期されている場合は、編集を LDAP ディレクトリで行う必要があります。

もっと詳細なレポートが必要な場合は、[CLI を介してユーザー ID とディレクトリ URI を検証する \(334 ページ\)](#)。

CLI を介してユーザー ID とディレクトリ URI を検証する

コマンド行インターフェースを使用して、重複したユーザー ID と重複したディレクトリ URI についてデプロイメントの詳細な検査を実行します。

手順

ステップ 1 コマンドラインインターフェイスにログインします。

ステップ2 次のコマンドを実行します。

- `utils` ユーザがすべて検証する - 重複したユーザー ID と重複したディレクトリ URI の両方についてシステムをチェックします。
- `utils` ユーザは `userid` を検証します - システムで重複するユーザー ID を確認します。
- `utils` ユーザが `uri` を検証します - システムで重複するディレクトリ URI を確認します。

CLI は、重複したディレクトリ URI やユーザー ID のレポートを返します。サンプルレポートについては、[ユーザー ID と ディレクトリ URI CLI 検証の例 \(335 ページ\)](#)

次のタスク

何らかの問題が生じたら、ユーザー設定を Cisco Unified Communications Manager の [エンドユーザの設定 (End User Configuration)] ウィンドウで編集します。ユーザが LDAP ディレクトリから同期されている場合は、編集を LDAP ディレクトリで行う必要があります。

ユーザー ID と ディレクトリ URI CLI 検証の例

重複ユーザー ID と重複または無効なディレクトリ URI が設定されたユーザを識別する IM and Presence サービスのユーザを確認するための CLI コマンドは、`utils users validate { all | userid | uri }` です。

ディレクトリ URI は、ユーザ毎に一意である必要があります。複数のユーザに同じディレクトリ URI を使用することはできません。大文字と小文字の違いがある場合でも、使用できません。たとえば、`aaa@bbb.ccc` と `AAA@BBB.CCC` のように、大文字と小文字の違いはあっても、これらで 2 つの異なるディレクトリ URI を作成することはできません。

CLI とコマンドの説明の使用方法の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

ユーザー ID エラーを表示する CLI 出力例

```
Users with Duplicate User IDs
-----
User ID: user3
Node Name
cucm-imp-1
cucm-imp-2
```

ディレクトリ URI エラーを表示する CLI 出力例

```
Users with No Directory URI Configured
-----
Node Name: cucm-imp-2
User ID
user4

Users with Invalid Directory URI Configured
-----
Node Name: cucm-imp-2
```

```
User ID   Directory URI
user1    asdf@ASDF@asdf@ADSF@cisco
```

```
Users with Duplicate Directory URIs
```

```
-----
Directory URI: user1@cisco.com
```

```
Node Name  User ID
cucm-imp-1 user4
cucm-imp-2 user3
```

ユーザー ID とディレクトリ URI のエラー

Cisco IM and Presence Data Monitor サービスは、Active ディレクトリ エントリで、すべての IM and Presence Service クラスタの重複ユーザー ID および空または重複ディレクトリ URI をチェックします。重複ユーザー ID またはディレクトリ URI はクラスタ内では無効です。ただし、誤ってクラスタ間展開の異なるクラスタのユーザに同じユーザー ID またはディレクトリ URI 値を割り当てる可能性があります。

次の一覧は、発生する可能性があるエラーを示しています。これらのエラーを **Real-Time Monitoring Tool** で確認することができます。これにより、これらのそれぞれについてアラームまたは警告が発生します。

DuplicateDirectoryURI

このアラートは、ディレクトリ URI IM アドレス スキームが設定されている時、同じディレクトリ URI 値が割り当てられているクラスタ間展開内に複数のユーザが設定されていることを示します。

DuplicateDirectoryURIWarning

この警告は userID @ Default_Domain IM アドレス スキームが設定されている時、同じディレクトリ URI 値が割り当てられているクラスタ間展開内に複数のユーザが設定されていることを示します。

DuplicateUserid

このアラートは、クラスタ間展開内の別のクラスタで 1 人以上のユーザに割り当てられた重複ユーザー ID が設定されていることを示します。

InvalidDirectoryURI

この警告は、ディレクトリ URI IM アドレス スキームが設定されている時、クラスタ間展開内の 1 つ以上のユーザに空または無効なディレクトリ URI 値が割り当てられていることを示します。

InvalidDirectoryURIWarning

このアラートは userID@ Default_Domain IM Address スキームが設定されている時、クラスタ間展開内の 1 つ以上のユーザに空または無効なディレクトリ URI 値が割り当てられていることを示します。

これらのアラーム条件に関連するユーザの特定情報を収集するには、**Command Line Interface** を使用して、その完全な一覧を確認してください。システムアラームは、影響を受けるユーザの詳細を提供しません。また、システム トラブルシュータは最大で 10 ユーザのみの詳細を表

示します。Command Line Interface を使用してユーザを確認し、アラームが発生しているユーザに関する情報を収集します。詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。



注意 影響を受けているユーザの通信の中断を避けるために、重複ユーザー ID および重複しているか無効なディレクトリ URI を解決するための適切な処置をとります。ユーザの連絡先情報を変更するには、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

エラーと推奨処置

次の表は、重複ユーザおよび重複または無効なディレクトリ URI のシステム確認をクラスタ間展開で実行するとき起こる可能性のあるユーザー ID とディレクトリ URI のエラー状態を示します。発生するアラームとそのエラーを修正するための推奨措置が一覧表示されます。

表 32: ユーザー ID とディレクトリ URI のエラー状態および推奨されるアクション

エラー状態	説明	推奨措置
重複ユーザー ID	<p>重複ユーザー ID は、クラスタ間展開内で別のクラスタの 1 人以上のユーザに割り当てられます。影響を受けるユーザが、クラスタ間ピアに配置されている場合があります。</p> <p>関連アラーム :</p> <p>DuplicateUserid</p>	DuplicateUserid アラームが発生したら、問題を修正するために即時に対処してください。クラスタ間展開内の各ユーザは一意的なユーザー ID が必要です。

エラー状態	説明	推奨措置
重複したディレクトリ URI	<p>クラスタ間展開内の複数のユーザに同じディレクトリ URI 値が割り当てられます。影響を受けるユーザが、クラスタ間ピアに配置されている場合があります。</p> <p>関連アラーム：</p> <ul style="list-style-type: none"> • DuplicateDirectoryURI • DuplicateDirectoryURIWarning 	<p>ディレクトリ URI IM アドレススキームを使用するようにシステムが設定されていて、DuplicateDirectoryURI アラームが発生した場合、問題を修正するために即時に対処してください。各ユーザは一意のディレクトリ URI が割り当てられる必要があります。</p> <p><i>userID@Default_Domain</i> IM アドレススキームを使用するように設定されていて、重複ディレクトリ URI が検出されると、DuplicateDirectoryURIWarning の警告が発生します。即時に対処する必要はありませんが、問題を解決することを推奨します。</p>
無効なディレクトリ URI	<p>展開内の 1 人以上のユーザに無効または空のディレクトリ URI 値が割り当てられます。<i>user @ domain</i> 形式でない URI は無効なディレクトリ URI です。影響を受けるユーザが、クラスタ間ピアに配置されている場合があります。</p> <p>関連アラーム：</p> <ul style="list-style-type: none"> • InvalidDirectoryURI • InvalidDirectoryURIWarning 	<p>ディレクトリ URI IM アドレススキームを使用するように設定がされていて、次のアラームが発生した場合、問題を修正するために即時に対処します。InvalidDirectoryURI。</p> <p><i>userID@Default_Domain</i> IM アドレススキームを使用するための設定がされており、無効なディレクトリ URI が検出された場合、InvalidDirectoryURIWarning の警告が発生します。即時に対処する必要はありませんが、問題を解決することを推奨します。</p>

ユーザのプレゼンス設定を表示

プレゼンスビューアを使用して、IM and Presence 対応のエンドユーザのプレゼンス設定の概要を表示します。プレゼンスビューアは、プレゼンスサーバの割り当て、連絡先、ウォッチャーなどの情報を提供します。

始める前に

Cisco AXL Web サービス、Cisco SIP Proxy サービス、および Cisco プレゼンスエンジンサービスはすべて Cisco Unified Serviceability で実行されている必要があります。

手順

- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] で、[ユーザの管理 (User Management)] > [エンド ユーザ (End Users)] を選択します。
- ステップ 2** [検索 (Find)] をクリックして、プレゼンス設定を表示するエンドユーザーを選択します。
- ステップ 3** [サービス設定 (Service Settings)] で、[ユーザのプレゼンスビューア (Presence Viewer for User)] リンクをクリックすると、エンド ユーザ プレゼンス ビューアが表示されます。ビューをカスタマイズしたい場合は、次の表を参照してください。

表 33: エンド ユーザ プレゼンス ビューアのフィールド

プレゼンスの設定	説明
[ユーザステータス (User Status)]	次のような、ユーザのプレゼンス ステータスを識別します。 <ul style="list-style-type: none"> • 応答可能 (Available) • 不在 • 取り込み中 • 連絡不可能 • [カスタム (Custom)]
[ユーザー ID (User ID)]	選択したユーザー ID を識別します。使用可能な場合は、ユーザの写真を表示します。 [送信 (Submit)] をクリックして、別のユーザー ID を選択することができます。
[プレゼンスステータスを見るユーザ (View From Perspective of)]	ユーザの視点からプレゼンス ステータスを見る際のユーザを指定します。これにより、指定されたユーザのプレゼンス ステータスが別のユーザ (ウォッチャ) にどのように見えるのか確認できます。この機能は、デバッグ シナリオで役立ちます (ユーザがプライバシー ポリシーを設定した場合など)。 最大 128 文字を使用できます。

プレゼンスの設定	説明
[連絡先(Contacts)]	<p>該当ユーザの連絡先リストの連絡先の数を表示します。</p> <p>[連絡先およびウォッチャ(Contacts and Watchers)] リスト領域の [連絡先(Contacts)] 見出しの横にある矢印をクリックして、特定ユーザの連絡先のプレゼンス ステータスを表示します。グループ名の横にある矢印をクリックして、グループ内の連絡先のリストを展開します。</p> <p>グループの一部ではない連絡先（グループのない連絡先）は、連絡先グループリストの下に表示されます。連絡先は複数のグループに属する場合がありますが、そのユーザの連絡先リストのサイズとしては1回しかカウントされません。</p> <p>エンドユーザに対して設定された連絡先の最大数を超えると、警告メッセージが表示されます。IM and Presence サービスの設定と連絡先の最大数の設定については、『<i>IM and Presence Administration Online Help</i>』を参照してください。</p>
[ウォッチャ(Watchers)]	<p>ウォッチャと呼ばれるユーザのリストを表示します。ウォッチャは、連絡先リストのユーザのプレゼンス ステータスを表示するために登録されます。</p> <p>[連絡先およびウォッチャ(Contacts and Watchers)] リスト領域の [ウォッチャ(Watchers)] 見出しの横にある矢印をクリックして、特定ウォッチャの連絡先のプレゼンス ステータスを表示します。グループ名の横にある矢印をクリックして、グループ内のウォッチャのリストを展開します。</p> <p>ウォッチャは複数のグループに属する場合がありますが、そのユーザのウォッチャリストのサイズとしては1回しかカウントされません。</p> <p>エンドユーザに対して設定されたウォッチャの最大数を超えると、警告メッセージが表示されます。IM and Presence サービスの設定とウォッチャの最大数の設定については、『<i>IM and Presence Administration Online Help</i>』を参照してください。</p>
[プレゼンス サーバの割り当て(Presence Server Assignment)]	<p>ユーザが割り当てられている IM and Presence サービス サーバを識別します。ハイパーリンクを利用してサーバの設定ページにハイパーリンクで直接移動し、詳細を確認できます。</p>
[プレゼンス アクセス アイコンの有効化(Enable accessible presence icons)]	<p>チェックボックスをオンにして、エンドユーザのプレゼンス アクセス アイコンを有効にします。</p>

プレゼンスの設定	説明
[送信(Submit)]	<p>選択すると、プレゼンス ビューアが実行されます。</p> <p>有効なプレゼンス情報を使用するには、ユーザがIM and Presence ノードに割り当てられている必要があります。これを機能させるためには、AXL、プレゼンス エンジン、プロキシ サービスのすべてを IM and Presence サーバで実行している必要があります。</p>

プレゼンスの連携動作と制限事項

機能	制約事項
自動プレゼンス認証をオフにする	<p>プレゼンスリクエストの自動許可をオフにした場合、IM and Presence サービスは他のユーザの連絡先リストに存在するユーザの登録要求を自動的に許可することに注意してください。これは、同じドメイン内のユーザおよび異なるドメイン内のユーザ（フェデレーション ユーザ）に適用されます。次に例を示します。</p> <ul style="list-style-type: none"> ユーザ A はユーザ B の在席状況の表示を登録します。自動許可は IM and Presence サービスでオフであり、ユーザ B はユーザ A の許可リストまたは拒否リストにありません IM and Presence サービスは UserB のクライアント アプリケーションにプレゼンス登録要求を送信し、クライアント アプリケーションは登録を許可または拒否するように UserB に求めます。 UserB は、プレゼンス登録要求を受け入れ、UserB は UserA の連絡先リストに追加されます。 UserA は、プレゼンス登録を許可するように求められることなく、UserB の連絡先リストに自動的に追加されます。これは、ユーザ B のポリシーが外部ドメインをブロックしている場合や、ユーザ B が「私に質問」している場合でも発生します。ユーザプロファイルで設定します。
ドメイン間フェデレーション - 外部ドメインから受信したプレゼンス要求	<p>IM and Presence は、プレゼンスステータスが要求されているユーザのユーザポリシー設定にのみ依存します。ユーザが[私に質問]を選択した場合ユーザポリシーで、外部連絡先またはドメインの許可リストまたはブロックリストが追加されていない場合、IM and Presence はプレゼンス要求をエンドユーザに送信して承認します。</p>



第 26 章

ユーザを集中展開に移行する

- [集中展開のユーザ移行概要 \(343 ページ\)](#)
- [中央クラスタ移行のための前提作業 \(343 ページ\)](#)
- [中央クラスタタスクフローへの移行 \(345 ページ\)](#)

集中展開のユーザ移行概要

この章では、既存の IM and Presence サービスユーザを標準の分散型 IM and Presence 展開 (Cisco Unified Communications Manager の IM and Presence サービス) から集中型展開に移行する手順について説明します。集中型展開では、IM and Presence 展開およびテレフォニー展開を別々のクラスタに展開できます。

中央クラスタ移行のための前提作業

すべてのユーザが既存の分散型クラスタから移行する先の新しい IM and Presence 中央クラスタを設定している場合は、次の前提条件の手順に従って移行用にクラスタを設定します。



- (注) 移行の一部ではない新しいユーザを追加する場合は、[集中展開の設定 \(115 ページ\)](#) の手順に従って新規ユーザーで中央クラスタを設定することができます。構成が正常に機能することを確信した後にのみ、既存のユーザを中央クラスタに移行します。

表 34: 移行前の作業

	移行前の作業
ステップ 1	<p>新しい中央クラスタを移行クラスタに接続します。</p> <ol style="list-style-type: none"> 1. IM and Presence サービスの集中型クラスタでデータベース パブリッシャ ノードにログインします。 2. Cisco Unified CM IM and Presence Administration から、[システム (System)]> [集中展開 (Centralized Deployment)]を選択します。 3. [検索(Find)] をクリックして、次のいずれかを実行します。 <ul style="list-style-type: none"> • 既存のクラスタを選択して、選択したものを編集する をクリックします。 • [新規追加 (Add New)] をクリックして、移行クラスタを追加します。 4. 追加する移行クラスタ毎に、以下のフィールドに入力を行います。 <ul style="list-style-type: none"> • [ピアアドレス (Peer Address)]: リモート Cisco Unified Communications Manager のテレフォニー クラスタ上のパブリッシャ ノードの FQDN、ホスト名、IPv4 アドレス、または IPv6 アドレス。 • [AXL ユーザ名 (AXL Username)]: リモート クラスタ上の AXL アカウントのログイン ユーザ名。 • [AXL パスワード (AXL Password)]: リモート クラスタ上の AXL アカウントのパスワード。 5. [保存 (Save)] をクリックします。
ステップ 2	<p>新しい中央クラスタが IM and Presence クラスタ間ネットワークの一部になる場合は、中央クラスタと、移行の一部ではない IM and Presence ピアクラスタ間のクラスタ間ピアリングを設定します。次のガイドラインが適用されます。</p> <ul style="list-style-type: none"> • 中央クラスタと移行クラスタ間でクラスタ間ピアリングを設定する必要はありません。ただし、移行しているクラスタに、移行時に任意の数の非移行クラスタが設定されているクラスタ間ピア接続がある場合は、これらのクラスタ間ピア接続が中央クラスタで設定されている必要があります。移行または移行は機能しません。 • クラスタ間ピアリングを設定した後は、クラスタ間ピアリングステータスを確認して、設定が正しく機能することを確認してください。 <p>詳細については、クラスタ間ピアの設定 (183 ページ) を参照してください。</p>

中央クラスタタスクフローへの移行

これらのタスクを実行して、既存のユーザを分散型クラスタ（Cisco Unified Communications Manager の IM and Presence サービス）から集中型 IM and Presence クラスタに移行します。このタスクフローでは：

- **IM and Presence 中央クラスタ** ユーザの移行先となるクラスタを指します。移行後、このクラスタは IM and Presence だけを処理します。
- **移行元クラスタ** とは IM and Presence ユーザの移行元のクラスタを指します。移行後、このクラスタはテレフォニーのみを処理します。

事前準備

IM and Presence 中央クラスタが新しくインストールされたクラスタで、まだユーザがない場合は、[中央クラスタ移行のための前提作業（343 ページ）](#) を完了してからユーザの移行を完了します。

表 35: 中央クラスタタスクフローへの移行

	IM and Presence 中央クラスタ	移行元クラスタ	目的
ステップ 1		移行元クラスタから連絡先リストをエクスポートする (347 ページ)	移行元クラスタ内のユーザ連絡先リストを csv ファイルにエクスポートします。
ステップ 2		移行元クラスタで高可用性を無効にする (348 ページ)	移行元クラスタ内のすべてのプレゼンス冗長グループ（サブクラスタ）に対して高可用性を無効にします。
ステップ 3		IM and Presence UC サービスの設定 (349 ページ)	移行元クラスタで、IM and Presence 中央クラスタを指す IM and Presence UC サービスを設定します。
ステップ 4:		IM and Presence のサービスプロファイルの作成 (350 ページ)	移行元クラスタで、設定した IM and Presence UC サービスを使用するサービスプロファイルを作成します。
ステップ 5:		テレフォニークラスタでの Presence ユーザーの無効化 (350 ページ)	ユーザの IM and Presence を無効にするには、移行元クラスタで一括管理を使用します。

	IM and Presence 中央クラスタ	移行元クラスタ	目的
ステップ 6:		中央クラスタの OAuth 認証を有効にする (352 ページ)	オプション。移行元クラスタで、OAuth 更新ログインを有効にします。これにより、中央クラスタの機能も有効になります。
ステップ 7	中央クラスタで高可用性を無効にする (352 ページ)		IM and Presence 中央クラスタのすべてのプレゼンス冗長グループ (サブクラスタ) でハイ アベイラビリティを無効にします。
ステップ 8	中央および移行クラスタのピア関係の削除 (353 ページ)		クラスタ間ピアリングが中央クラスタと移行クラスタの間に存在する場合は、両方のクラスタでピア接続を削除します。
ステップ 9	Cisco クラスタ間同期エージェントの停止 (354 ページ)		IM and Presence 中央クラスタ内の Cisco Intercluster Sync Agent を停止します。
ステップ 10	IM and Presence を Feature Group Template から有効化 (354 ページ)		中央クラスタで、IM and Presence サービスを有効にする機能グループ テンプレートを設定します。
ステップ 11	中央クラスタでの LDAP 同期の完了 (355 ページ)		LDAP ディレクトリ同期への機能グループテンプレートの追加同期を使用して、移行元クラスタからユーザを追加します。
ステップ 12	連絡先を中央クラスタにインポート (357 ページ)		一括管理と、前の手順で作成した csv エクスポート ファイルを使用して、連絡先リストを中央クラスタにインポートします。
ステップ 13	Cisco Intercluster Sync Agent (358 ページ)		中央クラスタで Cisco Intercluster Sync Agent を起動します。

	IM and Presence 中央クラスタ	移行元クラスタ	目的
ステップ 14	中央クラスタで高可用性を有効にする (359 ページ)		中央クラスタ内のすべてのプレゼンス冗長グループでハイアベイラビリティを有効にします。
ステップ 15	クラスタを移行する残りのピアの削除 (359 ページ)		移行クラスタ (現在はテレフォニークラスタ) とその他のピアクラスタ間の残りのクラスタ間ピア接続を削除します。

移行元クラスタから連絡先リストをエクスポートする

この手順は、分散型 IM and Presence 展開から集中型展開に移行する場合にのみ使用してください。移行元クラスタで、ユーザの連絡先リストを csv ファイルにエクスポートします。このファイルは後で中央クラスタにインポートできます。2 種類の連絡先リストをエクスポートできます。

- 連絡先リスト：このリストは、IM and Presence の連絡先で構成されています。IM アドレスを持たない連絡先は、このリストと一緒にエクスポートされません (プレゼンス以外の連絡先リストをエクスポートする必要があります)。
- 不在連絡先リスト：このリストは、IM アドレスを持たない連絡先で構成されています。

手順

- ステップ 1** 古いクラスタの Cisco Unified CM Administration および Presence Administration にログインします。
- ステップ 2** エクスポートする連絡先リストの種類に応じて、次のいずれかのオプションを選択します。
 - 連絡先リストのエクスポートの場合は、一括管理 > 連絡先リスト > 連絡先リストのエクスポートを選択します
 - 存在しない連絡先リストのエクスポートの場合は、一括管理 > 不在連絡先リスト > 不在連絡先リストのエクスポートを選択し、次のステップを飛ばしてください。
- ステップ 3** 担当者リストのみ。連絡先リストをエクスポートするユーザを選択します。
 - a) 連絡先リストのエクスポートオプションで、連絡先リストをエクスポートするユーザのカテゴリを選択します。デフォルトのオプションはクラスタ内のすべてのユーザです。
 - b) [検索 (Find)] をクリックしてユーザのリストを表示し、[次へ (Next)] をクリックします。
- ステップ 4** [ファイル名 (File Name)] を入力します。

ステップ 5 求人情報で、このジョブを実行するタイミングを設定します。

- **すぐに実行** - 連絡先リストをすぐにエクスポートするには、このボタンをオンにします。
- **[後で実行 (Run Later)]** - ジョブを実行する時間をスケジュールしたい場合は、このボタンをチェックしてください。

ステップ 6 [送信 (Submit)] をクリックします。

- (注) **すぐに実行**を選択すると、エクスポートファイルはすぐに生成されます。**[後で実行 (Run Later)]**を選択すると、(一括管理>ジョブスケジューラ)にあるジョブスケジューラーを使用して、ジョブを選択して実行する時間をスケジュールすることができます。

ステップ 7 エクスポートファイルが生成されたら、csv ファイルをダウンロードします。

- a) **[一括管理(Bulk Administration)]>[ファイルのアップロード/ダウンロード(Upload/Download Files)]**の順に選択します。
- b) **[検索(Find)]** をクリックします。
- c) ダウンロードするエクスポート ファイルを探し、**[選択をダウンロード (Download Selected)]** 選択します。
- d) 安全な場所にファイルを保存します。

ステップ 8 別の CSV エクスポートファイルを作成する場合は、この手順を繰り返します。たとえば、連絡先リスト用のエクスポートファイルを作成する場合は、不在連絡先リスト用に別のファイルを作成することができます。

次のタスク

[移行元クラスタで高可用性を無効にする \(348 ページ\)](#)

移行元クラスタで高可用性を無効にする

集中展開への移行では、移行中のテレフォニークラスタの各プレゼンス冗長グループ (サブクラスタ) で高可用性を無効にします。



- (注) **[プレゼンス冗長グループの詳細]**ページには、クラスタで高可用性が無効になっている場合でも、すべてのアクティブな JSM セッションが表示されます。

手順

ステップ 1 古いクラスタで Cisco Unified Communications Manager のパブリッシャ ノードにログインします。

- ステップ 2** Cisco Unified CM の管理から、[システム (System)] > [プレゼンス冗長グループ (Presence Redundancy Groups)] を選択します。
- ステップ 3** 検索をクリックしてサブクラスタを選択します。
- ステップ 4** [ハイ アベイラビリティを有効にする (Enable High Availability)] チェックボックスのチェックを外します。
- ステップ 5** [保存 (Save)] をクリックします。
- ステップ 6** 各クラスタで、この手順を繰り返します。

(注) すべてのサブクラスタに対してこの手順を完了したら、このクラスタで追加の設定を完了する前に少なくとも 2 分待ってください。

次のタスク

[IM and Presence UC サービスの設定 \(349 ページ\)](#)

IM and Presence UC サービスの設定

リモートテレフォニー クラスタでこの手順を使用して、IM and Presence サービスの中央クラスタを指す UC サービスを設定します。テレフォニー クラスタ内のユーザは、IM and Presence センtralクラスタから IM and Presence サービスを受けます。

手順

- ステップ 1** テレフォニー クラスタで Cisco Unified CM の管理インターフェイスにログインします。
- ステップ 2** [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [UC サービス (UC Service)] を選択します。
- ステップ 3** 次のいずれかを実行します。
- [検索 (Find)] をクリックし、編集する既存のサービスを選択します。
 - [新規追加 (Add New)] をクリックして、新しい UC サービスを作成します。
- ステップ 4** [UC サービスタイプ (UC Service Type)] ドロップダウンリスト ボックスから、[IM and Presence] を選択し、[次へ (Next)] をクリックします。
- ステップ 5** [製品タイプ (Product type)] ドロップダウン リスト ボックスから、[IM and Presence サービス (IM and Presence Service)] を選択します。
- ステップ 6** クラスタの一意の [名前 (Name)] を入力します。これはホスト名である必要はありません。
- ステップ 7** [ホスト名/IP アドレス (HostName/IP Address)] に、IM and Presence 集中型クラスタ データベースのパブリッシャ ノードのホスト名、IPv4 アドレス、または IPv6 アドレスを入力します。
- ステップ 8** [保存 (Save)] をクリックします。

ステップ 9 推奨。この手順を繰り返して、2 番目の IM and Presence サービスを作成します。ホスト名/IP アドレス field は、中央クラスタ内の加入者ノードを指します。

次のタスク

[IM and Presence のサービス プロファイルの作成 \(350 ページ\)](#)

IM and Presence のサービス プロファイルの作成

リモート テレフォニー クラスタでこの手順を使用して、IM and Presence 中央クラスタを指す サービス プロファイルを作成します。テレフォニー クラスタ内のユーザは、このサービス プロファイルを使用して、中央クラスタから IM and Presence サービスを取得します。

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [サービス プロファイル (Service Profile)] を選択します。

ステップ 2 次のいずれかを実行します。

- [検索 (Find)] をクリックし、編集する既存のサービス プロファイルを選択します。
- [新規追加 (Add New)] をクリックして、新しいサービス プロファイルを作成します。

ステップ 3 の中に **IM とプレゼンス プロファイル** セクションで、前のタスクで設定した IM and Presence サービスを設定します。

- [プライマリ (Primary)] ドロップダウン リストからデータベース パブリッシャ ノードを選択します。
- [セカンダリ (Secondary)] ドロップダウン リストから、サブスクリバノード サービスを選択して下さい。

ステップ 4 [保存 (Save)] をクリックします。

次のタスク

[テレフォニー クラスタでの Presence ユーザーの無効化 \(350 ページ\)](#)

テレフォニー クラスタでの Presence ユーザーの無効化

テレフォニー 展開で LDAP 同期が既に完了している場合は、一括管理 ツールを使用して IM and Presence ユーザ用のテレフォニー クラスタのユーザ設定を編集します。この設定では、プレゼンス ユーザが IM and Presence サービスの中央クラスタを参照するようになります。



(注) この手順は、テレフォニー クラスタで LDAP 同期が既に完了していることを前提としています。ただし、最初の LDAP 同期がまだ完了していない場合は、Presence ユーザの Central Deployment 設定を最初の同期に追加できます。この場合は、テレフォニー クラスタで次の手順を実行します。

- 設定したサービス プロファイルを含む機能グループ テンプレートを設定します。それが あることを確認してくださいホーム クラスタ オプションを選択して **Unified CM の IM and Presence** に対して **ユーザを有効にする** オプションが選択されていません。
- に LDAP ディレクトリ 設定追加する機能グループ テンプレート LDAP ディレクトリに同期します。
- 初期同期を完了してください。

機能グループ テンプレート および LDAP ディレクトリを設定する方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure End Users」を参照してください。

手順

- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] から、[クエリ (Query)] > [一括管理 (Bulk Administration)] > [ユーザ (Users)] > [ユーザの更新 (Update Users)] > [クエリ (Query)] の順に選択します。
- ステップ 2** フィルタから、**ホーム クラスタが有効になっている**を選択し**検索**をクリックします。ウィンドウに、これが自分のホーム クラスタであるすべてのエンドユーザが表示されます。
- ステップ 3** [次へ (Next)] をクリックします。
の中に**ユーザ設定の更新**ウィンドウの左端のチェックボックスは、このクエリでこの設定を編集するかどうかを示します。左のチェックボックスをオンにしないと、クエリはそのフィールドを更新しません。右側のフィールドは、このフィールドの新しい設定を示しています。2つのチェックボックスが表示される場合は、左側のチェックボックスをオンにしてフィールドを更新し、右側のチェックボックスに新しい設定を入力する必要があります。
- ステップ 4** **サービス設定**で、次の各フィールドの左端のチェックボックスをオンにしてこれらのフィールドを更新するように指定してから、隣接する設定を次のように編集します。
 - **ホーム クラスタ** - テレフォニー クラスタをホーム クラスタとして有効にするには、右側のチェックボックスをオンにします。
 - **[Unified IM and Presenceでのユーザの有効化 (Enable User for Unified IM and Presence)]** - 右チェックボックスをオフにします。この設定は、テレフォニー クラスタを IM and Presence のプロバイダーとして無効にします。
 - **UC サービス概要** - ドロップダウンから、前のタスクで設定したサービスプロファイルを選択します。この設定では、IM and Presence セントラル クラスタが IM and Presence サービスのプロバイダーになります。

(注) Expressway モバイルおよびリモートアクセスの構成の詳細については、<https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>で『*Mobile and Remote Access via Cisco Expressway Deployment Guide*』を参照してください。

ステップ 5 必要な残りのフィールドをすべて入力してください。フィールドとその設定を含むヘルプは、オンラインヘルプを参照してください。

ステップ 6 [ジョブ情報 (Job Information)] で、[今すぐ実行 (Run Immediately)] を選択します。

ステップ 7 [送信 (Submit)] をクリックします。

次のタスク

[中央クラスタの OAuth 認証を有効にする \(352 ページ\)](#)

中央クラスタの OAuth 認証を有効にする

この手順を使用して、テレフォニークラスタで OAuth 認証を有効にします。これにより、IM and Presence 中央クラスタでの OAuth 認証も有効になります。

手順

ステップ 1 テレフォニー クラスタで Cisco Unified CM の管理にログインします。

ステップ 2 [システム (System)] > [エンタープライズ パラメータ (Enterprise Parameters)] と選択します。

ステップ 3 [SSO設定 (SSO Configuration)] で、[更新ログインフローによるOAuth (OAuth with Refresh Login Flow)] エンタープライズ パラメータを [有効 (Enabled)] に設定します。

ステップ 4 パラメータ設定を編集した場合は、**保存する** をクリックします。

中央クラスタで高可用性を無効にする

IM and Presence 中央クラスタの各プレゼンス冗長グループ (サブクラスタ) で高可用性が無効になっていることを確認します。設定の適用またはユーザの移行前に、これを実行する必要があります。



(注) [プレゼンス冗長グループの詳細] ページには、クラスタで高可用性が無効になっている場合でも、すべてのアクティブな JSM セッションが表示されます。

手順

- ステップ 1 中央クラスタで Cisco Unified CM の管理インスタンスにログインします。
- ステップ 2 [システム(System)] > [プレゼンス冗長グループ(Presence Redundancy Groups)] を選択します。
- ステップ 3 [検索 (Find)] をクリックし、既存の電話機を選択します。
- ステップ 4 [ハイ アベイラビリティを有効にする (Enable High Availability)] チェックボックスのチェックを外します。
- ステップ 5 [保存 (Save)] をクリックします。
- ステップ 6 各サブクラスタに対してこの手順を繰り返します。

次のタスク

[Cisco クラスタ間同期エージェントの停止 \(354 ページ\)](#)

中央および移行クラスタのピア関係の削除

IM and Presence 中央クラスタと移行クラスタの間にクラスタ間ピアリングが存在する場合は、そのピア関係を削除します。

手順

- ステップ 1 IM およびプレゼンスサービスの中央クラスタのパブリッシャ ノードにログインします。
- ステップ 2 Cisco Unified CM IM and Presence 管理で、**プレゼンス(Presence) > クラスタ間(Inter-Clustering)** を選択します。
- ステップ 3 **検索(Find)** をクリックして移行クラスタを選択します。
- ステップ 4 [削除 (Delete)] をクリックします。
- ステップ 5 **Cisco XCP ルータ** を再起動します：
 - a) Unified IM and Presence Serviceability にログインして、**ツール(Tools) > コントロール センター - ネットワーク サービス(Control Center - Network Services)** を選択します。
 - b) サーバリストから、データベース パブリッシャ ノードを選択して、**移動(Go)** をクリックします。
 - c) [IM and Presence サービス (IM and Presence Services)] の下で、[Cisco XCP ルータ (Cisco XCP Router)] を選択し、[リスタート(Restart)] をクリックします
- ステップ 6 移行クラスタでこれらの手順を繰り返します。

Cisco クラスタ間同期エージェントの停止

IM and Presence 中央クラスタを設定する前に、**Cisco Intercluster Sync Agent** サービスが中央クラスタで停止していることを確認します。

手順

- ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
- ステップ 2 [サーバ (Server)] ドロップダウンから、中央クラスタ データベース パブリッシャー ノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3 **Cisco Intercluster Sync Agent** サービスのステータスを確認します。サービスが実行中またはアクティブ化されている場合は、隣のラジオボタンを選択して [停止 (Stop)] をクリックします。

次のタスク

[IM and Presence を Feature Group Template から有効化 \(354 ページ\)](#)

IM and Presence を Feature Group Template から有効化

この手順を使用して、中央クラスタの IM and Presence 設定を使用して機能グループテンプレートを設定します。機能グループテンプレートを LDAP ディレクトリ設定に追加して、同期されたユーザに IM and Presence を設定できます。



- (注) 機能グループテンプレートは、初期同期がまだ行われていない LDAP ディレクトリ設定にのみ適用できます。中央クラスタから LDAP 設定を同期した後は、Cisco Unified Communications Manager で LDAP 設定を編集することはできません。ディレクトリをすでに同期している場合は、一括管理を使用して IM and Presence をユーザに設定する必要があります。詳細については、[一括管理経由で IM and Presence を有効にする \(125 ページ\)](#) を参照してください。

手順

- ステップ 1 IM and Presence 集中型クラスタの Cisco Unified CM の管理インターフェイスにログインします。このサーバにはテレフォニーが設定されてはいけません。
- ステップ 2 [ユーザ管理 (User Management)] > [ユーザ電話/追加 (User Phone/Add)] > [機能グループテンプレート (Feature Group Template)] を選択します。
- ステップ 3 次のいずれかを実行します。

- [検索 (Find)] をクリックし、既存のテンプレートを選択します。
- [新規追加 (Add New)] をクリックして新しいテンプレートを作成します。

ステップ 4 次の両方のチェックボックスをオンにします。

- [ホームクラスタ (Home Cluster)]
- [Unified CM IM and Presence のユーザを有効にする (Enable User for Unified CM IM and Presence)]

ステップ 5 [機能グループテンプレートの設定 (Feature Group Template Configuration)] ウィンドウの残りのフィールドに入力します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 6 [保存 (Save)] をクリックします。

次のタスク

設定をユーザに伝達するには、最初の同期がまだ行われていない LDAP ディレクトリ構成に機能グループテンプレートを追加してから、最初の同期を完了する必要があります。

[中央クラスタでの LDAP 同期の完了 \(355 ページ\)](#)

中央クラスタでの LDAP 同期の完了

リモート Cisco Unified Communications Manager のテレフォニー クラスタでこの手順を使用し、LDAP 同期を使用して、IM and Presence 集中型設定を Cisco Unified Communications Manager の展開に展開します。



(注) LDAP ディレクトリ同期の設定方法については、『Cisco Unified Communications Manager システム構成ガイド』の「エンドユーザの構成」の部分を参照してください。

手順

ステップ 1 Cisco Unified CM の管理で、[システム (System)] > [LDAP (LADP)] > [LDAP ディレクトリ (LDAP Directory)] を選択します。

ステップ 2 次のいずれかを実行します。

- [検索 (Find)] をクリックし、既存の LDAP ディレクトリ同期を選択します。
- [新規追加 (Add New)] をクリックして、新しい LDAP ディレクトリ同期を作成します。

ステップ 3 [機能グループテンプレート (Feature Group Template)] ドロップダウンリストボックスから、前のタスクで作成した機能グループテンプレートを選択します。IM and Presence は、このテンプレートで無効にする必要があります。

ステップ 4 [LDAPディレクトリ (LDAP Directory)] ウィンドウで残りのフィールドを設定します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 5 [保存 (Save)] をクリックします。

ステップ 6 [完全同期を実施 (Perform Full Sync)] をクリックします。

Cisco Unified Communications Manager は、データベースを LDAP ディレクトリと同期させ、更新された IM and Presence 設定を割り当てます。

次のタスク

[連絡先を中央クラスタにインポート \(357 ページ\)](#)

一括管理経由で IM and Presence を有効にする

ユーザをすでに中央クラスタに同期させていて、それらのユーザが IM and Presence サービスに対して有効になっていない場合は、一括管理の [ユーザの更新 (Update Users)] 機能を使用して IM and Presence サービスを有効にします。



(注) 一括管理の [ユーザのインポート] または [ユーザの挿入] 機能を使用して、csv ファイルを介して新規ユーザーをインポートすることもできます。手順については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。インポートしたユーザで、下記のオプションが選択されていることを確認します。

- [ホームクラスタ (Home Cluster)]
- [Unified CM IM and Presence のユーザを有効にする (Enable User for Unified CM IM and Presence)]

手順

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] から、[一括管理 (Bulk Administration)] > [ユーザ (Users)] > [ユーザの更新 (Update Users)] > [クエリ (Query)] の順に選択します。

ステップ 2 フィルタから、ホームクラスタが有効になっているを選択し、検索をクリックします。ウィンドウに、これが自分のホームクラスタであるすべてのエンドユーザが表示されます。

ステップ 3 [次へ (Next)] をクリックします。

の中にユーザ設定の更新ウィンドウの左端のチェックボックスは、このクエリでこの設定を編集するかどうかを示します。左のチェックボックスをオンにしないと、クエリはそのフィールドを更新しません。右側のフィールドは、このフィールドの新しい設定を示しています。2つのチェックボックスが表示される場合は、左側のチェックボックスをオンにしてフィールドを更新し、右側のチェックボックスに新しい設定を入力する必要があります。

ステップ 4 サービス設定で、次の各フィールドの左側のチェックボックスをオンにしてこれらのフィールドを更新することを示し、次に隣接するフィールド設定を次のように編集します。

- **ホームクラスタ** - このクラスタをホームクラスタとして有効にするには、右側のチェックボックスをオンにします。
- **[Unified CM IM and Presence でのユーザの有効化 (Enable User for Unified CM IM and Presence)]** - 右チェックボックスをオンにします。この設定により、中央クラスタがこれらのユーザの IM and Presence サービスのプロバイダーとして有効になります。

ステップ 5 更新したい残りのフィールドをすべて入力します。フィールドとその設定を含むヘルプは、オンラインヘルプを参照してください。

ステップ 6 [ジョブ情報 (Job Information)] で、[今すぐ実行 (Run Immediately)] を選択します。

ステップ 7 [送信 (Submit)] をクリックします。

連絡先を中央クラスタにインポート

ユーザを IM and Presence Central クラスタに移行した場合は、この手順を使用してユーザの連絡先リストを IM and Presence 中央クラスタにインポートできます。次の種類の連絡先リストのいずれかをインポートできます。

- **連絡先リスト** : このリストには、IM and Presence の連絡先が含まれています。
- **不在連絡先リスト** : このリストには、IM アドレスを持たない連絡先が含まれています。

始める前に

古いクラスタ (テレフォニークラスタ) からエクスポートした連絡先リストの csv ファイルが必要です。

手順

ステップ 1 IM and Presence 中央クラスタの Cisco Unified CM IM and Presence Administration にログインします。

ステップ 2 テレフォニークラスタからエクスポートした csv ファイルをアップロードします。

- a) [一括管理(Bulk Administration)]>[ファイルのアップロード/ダウンロード(Upload/Download Files)] の順に選択します。
- b) [新規追加 (Add New)] をクリックします。
- c) [選択 (Choose)] をクリックして、インポートする CSV ファイルを選択します。
- d) **ターゲットを選択**から、次のいずれかをドロップダウンリストから選択します。インポートしている連絡先リストのタイプによって**連絡先リスト**または**不在連絡先リスト**。
- e) **取引タイプの選択**から、インポートジョブを選択します。
- f) [保存 (Save)] をクリックします。

ステップ 3 csv 情報を中央クラスタにインポートします。

- a) Cisco Unified CM の IM and Presence の管理から、次のいずれかを実行します。
 - 連絡先リストのインポートの場合は、**一括管理 > 連絡先リスト > 連絡先リストの更新**を選択します。
 - 不在連絡先リストのインポートの場合は、**一括管理 > 不在連絡先リスト > 不在連絡先リストのインポート**を選択します。
- b) [ファイル名 (File Name)] ドロップダウンから、アップロードした csv ファイルを選択します。
- c) ジョブ情報で、いつジョブを実行したいかによって[**すぐに実行 (Run Immediately)**]または[**後で実行 (Run Later)**]のいずれかを選択します。
- d) [送信 (Submit)] をクリックします。 **すぐに実行**を選択すると、連絡先リストはすぐにインポートされます。

(注) [後で実行 (Run Later)] を実行すると、**一括管理 > ジョブスケジューラ**に進み、ジョブを選択して実行する時間をスケジュールすることができます。

ステップ 4 インポートする 2 番目の csv ファイルがある場合は、この手順を繰り返します。

次のタスク

[Cisco Intercluster Sync Agent \(358 ページ\)](#)

Cisco Intercluster Sync Agent

設定または移行が完了したら、IM and Presence 中央クラスタにある **Cisco Intercluster Sync Agent** を起動します。このサービスは、クラスタ間ピアリングを使用している場合に必要です。

手順

- ステップ 1** [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] を選択します。
- ステップ 2** [サーバ (Server)] ドロップダウンから、IM and Presence パブリッシャーノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3** **IM and Presence Services** で、**Cisco Intercluster Sync Agent** サービスを選択して、**再起動** をクリックします。

次のタスク

[中央クラスタで高可用性を有効にする \(359 ページ\)](#)

中央クラスタで高可用性を有効にする

設定またはユーザの移行が完了したら、IM and Presence 中央クラスタのプレゼンス冗長グループ（サブクラスタ）で高可用性を有効にします。

手順

- ステップ 1 IM and Presence 中央クラスタの Cisco Unified CM Administration インスタンスにログインします。
- ステップ 2 [システム(System)] > [プレゼンス冗長グループ(Presence Redundancy Groups)] を選択します。
- ステップ 3 [検索 (Find)] をクリックし、既存の電話機を選択します。
- ステップ 4 [ハイ アベイラビリティを有効にする (Enable High Availability)] チェックボックスをチェックします。
- ステップ 5 [保存 (Save)] をクリックします。
- ステップ 6 IM and Presence 中央クラスタ内の各サブクラスタでこの手順を繰り返します。

クラスタを移行する残りのピアの削除

移行クラスタ (現在はテレフォニークラスタ) とその他の IM and Presence サービスピアクラスタ間のクラスタ間ピア関係を削除します。



- (注) クラスタ間接続の削除は、メッシュ全体での Cisco XCP ルータの再起動の可用性に応じて、後の日付に延期することができます。テレフォニークラスタと任意の数のピアクラスタの間に既存のクラスタ間接続がある限り、現在 Cisco XCP ルータサービスを実行している場合は、テレフォニークラスタで**実行状態のままにする**必要があります。

手順

- ステップ 1 移行クラスタの IM and Presence データベース パブリッシャ ノードにログインします。
- ステップ 2 Cisco Unified CM IM and Presence 管理で、**プレゼンス(Presence) > クラスタ間(Inter-Clustering)** を選択します。
- ステップ 3 **検索(Find)** をクリックしてピアクラスタを選択します。
- ステップ 4 [削除 (Delete)] をクリックします。
- ステップ 5 **Cisco XCP ルータ**を再起動します：
 - a) Unified IM and Presence Serviceability にログインして、**ツール(Tools) > コントロール センター - ネットワーク サービス(Control Center - Network Services)**を選択します。

- b) サーバリストから、データベース パブリッシャ ノードを選択して、**移動(Go)**をクリックします。
- c) [IM and Presenceサービス (IM and Presence Services)] の下で、[Cisco XCPルータ (Cisco XCP Router)] を選択し、[リスタート(Restart)] をクリックします

ステップ 6 IM and Presence サービス ピア クラスタでこれらの手順を繰り返します。

- (注) 移行クラスタに複数のクラスタへのクラスタ間ピア接続がある場合は、クラスタ間ネットワークに残っている各ピアクラスタに対してこの手順を繰り返す必要があります。つまり、移行するクラスタでは、破損しているピアクラスタ接続があるため、**Cisco XCP ルータ**が再起動するサイクルは多数あります。
-



第 27 章

ユーザの移行

- [ユーザ移行の概要 \(361 ページ\)](#)
- [ユーザ移行の前提条件 \(361 ページ\)](#)
- [ユーザの移行タスクフロー \(361 ページ\)](#)

ユーザ移行の概要

ここでは、IM and Presence Service クラスタ間でユーザを移行する方法について説明します。

ユーザ移行の前提条件

- 現在のクラスタと移行先クラスタの両方のフルバックアップを実行します。詳細については、[システムのバックアップ \(395 ページ\)](#) を参照してください。
- 移行されるユーザに現在のホーム クラスタ上の Cisco Unified Presence または Cisco Jabber のライセンスが供与されていることを確認します。これらのユーザがプレマイグレーションクラスタ以外のクラスタでライセンスされている場合は、移行作業を進める前に完全にライセンスを取得しておく必要があります。

ユーザの移行タスクフロー

IM and Presence ユーザを新しいクラスタに移行するには、これらのタスクを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	古いエントリの削除 (363 ページ)	ユーザを移行する前に、古い名簿、グループ エントリ、および非プレゼンス契約レコードをすべて削除します。

	コマンドまたはアクション	目的
ステップ 2	移行のための必須サービスの起動 (365 ページ)	移行する前に、以下のサービスが実行されていることを確認してください。 <ul style="list-style-type: none"> • Cisco AXL Web Service • Cisco Sync Agent • Cisco Intercluster Sync Agent
ステップ 3	Intercluster Sync Errors を確認 (364 ページ)	トラブルシュータを実行し、クラスタ間同期の問題がないことを確認します。
ステップ 4	移行の標準プレゼンスの設定 (364 ページ)	ユーザを移行する前に、これらの標準プレゼンス設定を構成してください。
ステップ 5	ユーザ連絡先リストのエクスポート (365 ページ)	次の手順を完了して、現在のクラスタから移行するユーザの連絡先リストをエクスポートします。
ステップ 6	ユーザを新しいクラスタに移動するには、次のいずれかのミニタスクフローを実行します。 <ul style="list-style-type: none"> • LDAP を介してユーザを移行する (367 ページ) • 新しいクラスタへのユーザの手動での移動 (369 ページ) • 一括管理からのユーザの移行 (371 ページ) 	新しいクラスタへのユーザの移動LDAPを使用して新しいクラスタにユーザをプロビジョニングする、ユーザを手動で移動する、または一括管理を使用してユーザを新しいクラスタに移行することができます。
ステップ 7	ホーム クラスタでの連絡先リストのインポート (376 ページ)	ユーザを新しいクラスタに移行したら、移行されたユーザの連絡先リストのデータを復元するために、連絡先リストをインポートします。
ステップ 8	古いクラスタのユーザの更新 (377 ページ)	新しいクラスタですべてが正常に動作していることを確認するまで、古いクラスタからユーザを削除したくない場合があります。一括管理の [ユーザの更新 (Update Users)] 機能を使用して古いクラスタから IM and Presence 機能を削除するには、この手順を使用します。

古いエントリの削除

ユーザーを移行する前に、古い名簿、グループエントリ、およびプレゼンス以外の取引先担当者レコードを削除します。これは、ユーザがプレゼンスを無効にしたパブリッシャ IM & P ノードで実行されます。



(注) 2000 のバッチで必要に応じてこれらの手順を繰り返します。CLI を介して大量の古いエントリを削除するのに時間がかかりすぎる場合は、このセクションの最後にあるルートアクセスを必要とする古いリストスクリプトを活用するために TAC ケースを開きます。

手順

ステップ 1 CLI セッションを開始します。CLI セッションを開始する方法の詳細については、『*Cisco Unified Communications* ソリューション コマンドライン インターフェイス リファレンス ガイド』の「CLI セッションの開始」の項を参照してください。

ステップ 2 古い名簿エントリを確認して削除します。これを行うには、次のクエリを実行します。

a) 古い名簿エントリを確認します。

```
run sql select count(*) from rosters where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)
```

b) 古い名簿エントリを削除します。

```
run sql delete from rosters where pkid in (select * from (select first 2000 pkid from rosters where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

ステップ 3 古いグループレコードを確認および削除します。これを行うには、次のクエリを実行します。

a) 古いグループレコードを確認する:

```
run sql select count(*) from groups where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)
```

b) 古いグループレコードを削除します。

```
run sql delete from groups where pkid in (select * from (select first 2000 pkid from groups where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

ステップ 4 古い非連絡先レコードを確認して削除します(順番に)。これを行うには、次のクエリを実行します。

a) 古い非連絡先レコードを(順番に)確認します。

```
run sql select count(*) from nonpresencecontacts where fkenduser in (select pkid from enduser where primarynodeid is null)
```

b) 古い非連絡先レコードを削除(順番に):

```
run sql delete from nonpresencecontacts where pkid in (select * from (select first 2000 pkid from nonpresencecontacts where fkenduser in (select pkid from enduser where primarynodeid is null)))
```

- c) ルートアクセス権がある場合は、このクエリを使用します。

```
run sql delete from epascontactaddinfo where pkid in (select * from (select first
2000 pkid from epascontactaddinfo where pkid not in (select fkepascontactaddinfo from
nonpresencecontacts)))
```

移行の標準プレゼンスの設定

ユーザを移行する前に、これらのプレゼンス設定を構成してください。

手順

- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で [プレゼンス (Presence)] > [設定 (Settings)] > [標準設定 (Standard Configuration)] を選択します。
- ステップ 2 [承認を求められることなくユーザが他のユーザの在席状況を確認できる (Allow users to view the availability of other users without being prompted for approval)] チェックボックスにチェックします。
- ステップ 3 [連絡先リストの最大サイズ (ユーザごと) (Maximum Contact List Size (per user))] 設定では、[制限なし (No Limit)] チェックボックスをオンにします。
- ステップ 4 [ウォッチャの最大数 (ユーザごと) (Maximum Watchers (per user))] では、[制限なし (No Limit)] チェックボックスをオンにします。
- ステップ 5 [保存 (Save)] をクリックします。

次のタスク

[Intercluster Sync Errors を確認 \(364 ページ\)](#)

Intercluster Sync Errors を確認

移行する前に、クラスタ間同期エラーがないことを確認してください。

手順

- ステップ 1 Cisco Unified CM IM and Presence Administration から、[診断 (Diagnostics)] > [システムトラブルシュータ (System Troubleshooter)] を選択します。
- ステップ 2 クラスタ間同期エラーがないことを確認してください。エラーがある場合は、先に進む前にそれらを修正してください。

次のタスク

[移行のための必須サービスの起動 \(365 ページ\)](#)

移行のための必須サービスの起動

Cisco Unified IM and Presence Serviceability で、移行に不可欠な次のサービスが実行されていることを確認します。

- Cisco AXL Web Service
- Cisco Sync Agent
- Cisco Intercluster Sync Agent

手順

- ステップ 1** [Cisco Unified IM and Presenceのサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンター-機能サービス (Control Center - Feature Services)] を選択します。
- ステップ 2** [サーバ (Server)] ドロップダウンメニューから、IM and Presence ノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3** データベースと管理サービスで、**Cisco AXL Web** サービスが開始していることを確認します。サービスが実行されていない (デフォルト設定が実行されていない) 場合は、サービスを選択して**開始**をクリックします。
- ステップ 4** [ツール (Tools)] > [コントロールセンター-ネットワーク サービス (Control Center - Network Services)] を選択します。
- ステップ 5** [サーバ (Server)] ドロップダウンメニューから、IM and Presence ノードを選択し、[移動 (Go)] をクリックします。
- ステップ 6** IM and Presence サービスで、**Cisco Sync Agent** および **Cisco Intercluster Sync Agent** サービスが実行中であることを確認します。実行されていない場合、**開始**します。

次のタスク

[ユーザ連絡先リストのエクスポート \(365 ページ\)](#)

ユーザ連絡先リストのエクスポート

次の手順を完了して、現在のクラスターから移行するユーザの連絡先リストをエクスポートします。

手順

- ステップ 1** 現在のホーム クラスタから移行ユーザの連絡先リストをエクスポートします。
- [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[一括管理 (Bulk Administration)] > [連絡先リスト (Contact List)] > [エクスポート (Export)] を選択します。
 - [クラスタ内のすべての未割り当てユーザ (All unassigned users in the cluster)] を選択し、[Find (検索)] をクリックします。
 - 結果を確認し、必要に応じて [および/また (AND/OR)] フィルタを使用して検索結果をフィルタリングします。
 - リストが完了すると、[次へ (Next)] をクリックします。
 - エクスポートされた連絡先リストデータのファイル名を選択します。
 - 任意でジョブの説明を更新します。
 - [今すぐ実行 (Run Now)] をクリックするか、ジョブを後で実行するようにスケジュールします。
- ステップ 2** 連絡先リストのエクスポート ジョブのステータスをモニタします。
- [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[一括管理 (Bulk Administration)] > [ジョブ スケジューラ (Job Scheduler)] を選択します。
 - [検索 (Find)] をクリックして、すべての BAT ジョブをリストします。
 - 連絡先リストのエクスポート ジョブを検索し、それが完了と報告された場合はジョブを選択します。
 - [CSV ファイル名 (CSV FileName)] リンクを選択して、連絡先リストのエクスポートファイルの内容を表示します。タイムスタンプがファイル名に追加されます。
 - [ジョブの結果 (Job Results)] セクションから、アップロードされた内容の要約を表示するログファイルを選択します。ログファイルには、ジョブの開始時刻と終了時刻、および結果の要約が含まれています。
- ステップ 3** 後でユーザの移行が完了したときに使用できるように、連絡先リストのエクスポートファイルをダウンロードし、保存します。
- [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[一括管理 (Bulk Administration)] > [ファイルのアップロード/ダウンロード (Upload/Download Files)] を選択します。
 - [検索 (Find)] をクリックします。
 - 連絡先リストのエクスポート ファイルを選択し、[選択項目のダウンロード (Download Selected)] を選択します。
 - 後の手順でアップロードできるように CSV ファイルをローカルに保存します。
-

次のタスク

次のタスクフローのいずれかに移動して、新しいクラスタにユーザを割り当てます。

- [LDAP を介してユーザを移行する \(367 ページ\)](#)
- [新しいクラスタへのユーザの手動での移動 \(369 ページ\)](#)

LDAP を介してユーザを移行する

ユーザがLDAPディレクトリと同期していて、新しいクラスタに移行したい場合は、これらのタスクを完了してください。



- (注) LDAPディレクトリ設定を新しいクラスタに追加する必要があります。これには、サービスプロファイル、ユーザプロファイル、および機能グループテンプレートが含まれます。機能グループテンプレートの設定で、**Unified CM の IM and Presence に対するユーザの有効化**チェックボックスがオンになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	外部 LDAP ディレクトリの更新 (367 ページ)	展開でクラスタごとに別々の LDAP 構造を使用し、ユーザが自分のホームクラスタに対してのみ同期される場合は、外部 LDAP ディレクトリを更新する必要があります。
ステップ 2	新しいクラスタでの LDAP の設定 (368 ページ)	Cisco Unified Communications Manager で LDAP が有効になっている場合は、新しいクラスタを更新された LDAP ディレクトリと同期させて、ユーザを新しいクラスタにインポートします。

次のタスク

[ホーム クラスタでの連絡先リストのインポート \(376 ページ\)](#)

外部 LDAP ディレクトリの更新

展開でクラスタごとに別々の LDAP 構造を使用し、ユーザが自分のホームクラスタに対してのみ同期される場合は、外部 LDAP ディレクトリを更新する必要があります。



- (注) 展開でフラットな LDAP 構造を使用する場合、つまり、すべてのユーザがすべての Cisco Unified Communications Manager および IM and Presence サービス クラスタに同期され、ユーザが 1 つのクラスタにのみライセンスされている場合は、ユーザを移動する必要はありません。



- (注) 新旧のクラスタで LDAP ディレクトリ同期をどのように設定しているかに応じて、外部 LDAP ディレクトリ内でユーザを移動すると、次の同期が発生したときにそれらのユーザを自動的に新しい IM and Presence サービスクラスタに移行することがあります。

手順

- ステップ 1** 外部 LDAP ディレクトリのユーザを更新します。
- ステップ 2** ユーザの移動後、古い LDAP のクラスタから LDAP エントリを削除します。

次のタスク

[新しいクラスタでの LDAP の設定 \(368 ページ\)](#)

新しいクラスタでの LDAP の設定

始める前に

新しいクラスタに LDAP ディレクトリをプロビジョニングします。LDAP ディレクトリ同期にユニバーサル回線テンプレート、デバイステンプレート、および機能グループテンプレートが含まれている場合は、これらのテンプレートを新しいクラスタで設定する必要があります。機能グループテンプレートに次のオプションがチェックされていることを確認してください。

- [ホームクラスタ (Home Cluster)]
- [Unified CM IM and Presence のユーザを有効化 (Enable User for Unified CM IM and Presence)]

LDAP ディレクトリ同期の設定方法については、『*Cisco Unified Communications Manager システム構成ガイド*』の「エンドユーザの構成」の部分を参照してください。

手順

- ステップ 1** Cisco Unified CM の管理で、[システム (System)] > [LDAP (LADP)] > [LDAP ディレクトリ (LDAP Directory)] を選択します。
- ステップ 2** [検索 (Find)] をクリックし、設定した LDAP ディレクトリを選択します。
- ステップ 3** [Perform Full Sync Now (完全同期を今すぐ実施)] をクリックします。

次のタスク

[ホーム クラスタでの連絡先リストのインポート \(376 ページ\)](#)

新しいクラスタへのユーザの手動での移動

これらのタスクを完了して、ユーザを新しいクラスタに手動で移動します。



- (注) 多数のユーザがいる場合は、Cisco Unified Communications Manager の一括管理ツールを使用して、csv ファイルを介して多数のユーザを更新します。詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザの IM and Presence の手動での無効化 (369 ページ)	現在のホーム クラスタでの IM and Presence Service および Cisco Jabber のユーザ移行を無効にします。
ステップ 2	ユーザの手動インポート (370 ページ)	新しいクラスタで LDAP 同期が設定されていない場合は、新しい Cisco Unified Communications Manager クラスタに手動でユーザをプロビジョニングします。
ステップ 3	新しいクラスタの IM and Presence Service のユーザの有効化 (370 ページ)	新しいホーム クラスタでユーザが同期されている場合、または手動でプロビジョニングされている場合は、手動で IM and Presence サービスおよび Cisco Jabber のユーザを有効にする必要があります。

次のタスク

[ホーム クラスタでの連絡先リストのインポート \(376 ページ\)](#)

ユーザの IM and Presence の手動での無効化

次の手順では、現在のホーム クラスタの IM and Presence Service および Cisco Jabber の移行ユーザを無効にする方法について説明します。



- (注) 一度に多数のユーザを移行する場合は、Cisco Unified Communications Manager の一括管理ツールを使用することをお勧めします。詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

始める前に

[ユーザ連絡先リストのエクスポート \(365 ページ\)](#)

手順

-
- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] で、[ユーザの管理 (User Management)] > [エンド ユーザ (End User)] を選択します。
 - ステップ 2 フィルタを使用して、IM and Presence Service を無効にするユーザを検索します。
 - ステップ 3 [エンド ユーザの設定 (End User Configuration)] 画面で、[Unified CM IM and Presence にユーザを有効にします (Enable User for Unified CM IM and Presence)] チェックボックスをオフにします。
 - ステップ 4 [保存 (Save)] をクリックします。
-

次のタスク

[ユーザの手動インポート \(370 ページ\)](#)

ユーザの手動インポート

新しいクラスタでLDAP同期が設定されていない場合は、新しい Cisco Unified Communications Manager クラスタにユーザを手動でインポートしてください。

詳細については、[ユーザ設定値の設定 \(77 ページ\)](#) を参照してください。

次のタスク

[新しいクラスタの IM and Presence Service のユーザの有効化 \(370 ページ\)](#)

新しいクラスタの IM and Presence Service のユーザの有効化

新しいホームクラスタでユーザが同期されている場合、または手動でプロビジョニングされている場合は、手動で IM and Presence サービスおよび Cisco Jabber のユーザを有効にする必要があります。

手順

-
- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] で、[ユーザの管理 (User Management)] > [エンド ユーザ (End User)] を選択します。
 - ステップ 2 フィルタを使用して、IM and Presence サービスを有効にするユーザを検索します。
 - ステップ 3 [エンド ユーザの設定 (End User Configuration)] 画面で、[Unified CM IM およびプレゼンスにユーザを有効にします (Enable User for Unified CM IM and Presence)] をオンにします。
 - ステップ 4 [保存 (Save)] をクリックします。

- ステップ 5** 電話機および CSF の Cisco Unified Communications Manager のユーザをプロビジョニングします。詳細については、『*Upgrade Guide for the Cisco Unified Communications Manager*』を参照してください。

次のタスク

[ホーム クラスタでの連絡先リストのインポート \(376 ページ\)](#)

一括管理からのユーザの移行

一括管理ツールを使用して、ユーザを新しいクラスタに移動します（たとえば、クラスタ 1 からクラスタ 2 への移行）。

始める前に

Cisco Bulk Provisioning Service は両方のクラスタで実行されている必要があります。



- (注) IM and Presence クラスタで移行元から移行先に移動するユーザ数が 100 未満の場合は、Cisco Intercluster Sync Agent サービスを開始または停止しないでください。

いずれかの移行元/移行先クラスタから 100 ~ 1,000 ユーザを移動する場合は、移行元と移行先の両方のクラスタで Intercluster Sync Agent サービスを停止して、次の手順を実行します。

移行するユーザ数が 1,000 を超える場合、たとえば 16,000 ユーザを移動する必要がある場合は、まず次の手順に従って Intercluster Sync Agent サービスを停止し、8,000 ユーザを 1,000 ユーザ単位で移動します。その後、残りの 8,000 ユーザを 1,000 ユーザ単位に分散させて順番に移動します。

移行元からユーザが移動される IM and Presence クラスタでの手順：

ステップ 1 IM and Presence パブリッシャのプレゼンス冗長グループ (PRG) ペアとして関連付けられているパブリッシャ ノードで、Intercluster Sync Agent サービスを停止します。

ステップ 2 パブリッシャ IM and Presence プレゼンス冗長グループ ペアのパブリッシャ ノードで、Intercluster Sync Agent サービスを停止します。

移行先からユーザが移動される IM and Presence クラスタでの手順：

ステップ 3 パブリッシャ Presence Redundancy Group ペアのセカンダリ ノードで、Intercluster Sync Agent サービスを停止します。

ステップ 4 パブリッシャ Presence Redundancy Group ペアのパブリッシャ ノードで、Intercluster Sync Agent サービスを停止します。



(注) これら以外のクラスタ ノードでは、Intercluster Sync Agent サービスを停止する必要はありません。

ステップ 5 「一括管理によるユーザの移行」で説明されている手順を実行します。

ステップ 6 移行先と移行元の両方のクラスタの IM and Presence パブリッシャ ノードおよびサブスクリバノードで、Intercluster Sync Agent サービスを開始します。

ステップ 7 他のすべてのクラスタで移行先クラスタとの同期が完了するまで、最大で 30 分ほどかかる可能性があります。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザーをCSVファイルにエクスポート (372 ページ)	元のクラスタ (クラスタ 1) で、移行中のユーザを CSV ファイルにエクスポートします。
ステップ 2	CSVエクスポートファイルをダウンロードします (373 ページ)	CSVエクスポートファイルをダウンロードします。
ステップ 3	CSV エクスポートファイルを新しいクラスタにアップロードします (374 ページ)	CSV ファイルを宛先クラスタ (クラスタ 2) にアップロードします。
ステップ 4	ユーザ テンプレートの設定 (374 ページ)	移行先クラスタで、ユーザ設定を使用してユーザテンプレートを構成します。
ステップ 5	ユーザを新しいクラスタにインポート (375 ページ)	一括管理の [ユーザの挿入] メニューを使用して、CSV ファイルからユーザをインポートします。
ステップ 6	一括管理によるユーザー移行の確認 (375 ページ)	一括管理によるユーザの移行を検証します。

ユーザーをCSVファイルにエクスポート

元のクラスタで、一括管理ツールを使用して、移行するユーザを CSV ファイルにエクスポートします。

注：ジョブの実行後、ジョブスケジューラに進みジョブのステータスを確認し、ファイルが作成されたことを確認できます。[後で実行]を選択した場合は、ジョブスケジューラを使用してジョブを実行する時間を設定できます。

手順

- ステップ 1** Cisco Unified CM Administration から、[一括管理 (Bulk Administration)] > [ユーザ (Users)] > [ユーザのエクスポート (Export Users)] の順に選択します。
- ステップ 2** フィルタツールを使用して移行したいユーザを検索して選択するために、**検索**をクリックします。
- ステップ 3** [次へ (Next)] をクリックします。
- ステップ 4** ファイルの**ファイル名**を入力します。
ツールはファイルの末尾に .txt 拡張子を追加します。例えば、 <csvfilename> .txt
- ステップ 5** **ファイルフォーマットドロップダウン**から、エクスポートファイルの形式を選択します。
- ステップ 6** すぐにジョブを実行するには、[すぐに実行 (Run Immediately)] を選択して [送信 (Submit)] をクリックします。

次のタスク

ジョブが終わったら、**ジョブスケジューラ**に進みジョブの状況を確認し、ファイルが作成されたことを確認できます。[後で実行] を選択した場合は、ジョブスケジューラを使用してジョブを実行する時間を設定できます。

ファイルが作成されたことを確認したら、[CSV エクスポートファイルをダウンロードします \(373 ページ\)](#)

CSV エクスポートファイルをダウンロードします

エクスポートファイルが作成されたことを確認したら、ファイルをダウンロードします。

手順

- ステップ 1** Cisco Unified CM の管理ページから、[一括管理 (Bulk Administration)] > [ファイルのアップロード/ダウンロード (Upload/Download Files)] の順に選択します。
- ステップ 2** [検索 (Find)] をクリックします。
- ステップ 3** 作成したファイルを選択してクリック **選択をダウンロード** をクリックします。
- ステップ 4** ファイルをダウンロードします。

次のタスク

[CSV エクスポートファイルを新しいクラスタにアップロードします \(374 ページ\)](#)

CSV エクスポートファイルを新しいクラスタにアップロードします

宛先クラスタ（クラスタ 2）で、クラスタ 1 からエクスポートした csv ファイルをアップロードします。

手順

- ステップ 1 Cisco Unified CM の管理ページから、[一括管理(Bulk Administration)]>[ファイルのアップロード/ダウンロード(Upload/Download Files)] の順に選択します。
- ステップ 2 [新規追加 (Add New)] をクリックします。
- ステップ 3 [Choose File] をクリックします。他のシステムからエクスポートファイルを参照して選択します。
- ステップ 4 からターゲットドロップダウンメニューから、ファイルの内容をインポートするために使用する一括管理メニューを選択します。例えば、**ユーザ**または**電話とユーザ**
- ステップ 5 **取引タイプ**ドロップダウンから、ファイルの内容をインポートするために使用するサブメニューを選択します。例えば、**ユーザを挿入**または**電話機/ユーザを挿入**。
- ステップ 6 [保存 (Save)] をクリックします。

次のタスク

[ユーザテンプレートの設定 \(374 ページ\)](#)

ユーザテンプレートの設定

移行先クラスタで、インポートしたユーザに適用する設定を使用してユーザテンプレートを構成します。

手順

- ステップ 1 Cisco Unified CM Administration から、[一括管理 (Bulk Administration)]>[ユーザ (Users)]>[ユーザテンプレート (User Templates)] の順に選択します。
- ステップ 2 次のいずれかを実行します。
 - [検索 (Find)] をクリックし、既存のテンプレートを選択します。
 - [新規追加 (Add New)] をクリックして新しいテンプレートを作成します。
- ステップ 3 インポートしたユーザに適用するユーザ設定を構成します。例えば、以下のフィールドがチェックされていることを確認します。
 - [ホームクラスタ (Home Cluster)]
 - [Unified CM IM and Presence のユーザを有効にする (Enable User for Unified CM IM and Presence)]

- ステップ4 ユーザが Microsoft Outlook とのカレンダー統合ができるように設定したい場合は、**会議情報をプレゼンスチェックボックスに含める**をチェックします。
- ステップ5 残りのフィールドを設定します。
- ステップ6 **[保存 (Save)]** をクリックします。

次のタスク

[ユーザを新しいクラスタにインポート \(375 ページ\)](#)

ユーザを新しいクラスタにインポート

一括管理の**[ユーザの挿入]**メニューを使用して、エクスポートしたユーザを新しいクラスタにインポートします。

手順

- ステップ1 Cisco Unified CM Administration から、**[一括管理 (Bulk Administration)]** > **[ユーザ (Users)]** > **[ユーザの挿入 (Insert Users)]** の順に選択します。
- ステップ2 ファイル名から、他のシステムからエクスポートされたファイルを選択します。
- ステップ3 ユーザテンプレート名から、作成したユーザテンプレートを選択します。
- ステップ4 エクスポートユーザで作成された**ファイルチェックボックス**をチェックします。
- ステップ5 **[今すぐ実行 (Run Immediately)]** をチェックして、**[送信 (Submit)]** をクリックします。

次のタスク

[ホーム クラスタでの連絡先リストのインポート \(376 ページ\)](#)

一括管理によるユーザー移行の確認

一括管理によるユーザの移行が完了し、移行元および移行先のクラスタで Cisco Intercluster Sync Agent サービスが開始されたら、移行元と移行先以外のクラスタで、ユーザの移動が発生したという通知が受信されたことを確認する必要があります。

他のすべてのクラスタで移行先クラスタとの同期が完了するまでには、最大で 30 分ほどかかる可能性があります。待機中は、変更に含まれていない（移行元または移行先ではない）サンプル (5) IMP パブリッシャへのターミナルセッションを並行して開いて、CiscoSyslogs を監視することができます。

手順

- ステップ1 一括管理によるユーザの移行が完了し、移行元および異国先のクラスタで Cisco Intercluster Sync Agent サービスが開始された後、以下のコマンドを実行して、サンプル IMP パブリッシャ ノー

ドの同期がすでに完了したかどうかを確認します。この時点のタイムスタンプを記録します。次の構文の例では、`dst-name`が移行先のクラスタ名です。これを実際の移行先クラスタ名に置き換えてください。

```
admin:file search activelog syslog/CiscoSyslog ".*InterClusterSyncAgentStatus:.*dst-name.*"
```

ステップ2 記録されたタイムスタンプよりも ICSA ステータスのタイムスタンプが古い場合は、同期が成功するまで最大 30 分間、次のコマンドを実行します。

```
admin:file tail activelog syslog/CiscoSyslog regexp
".*InterClusterSyncAgentStatus:.*dst-name.*"
```

選択したサンプル クラスタ/ノードで ICSA の同期失敗ステータス アラームが表示された場合は、同期成功ステータス アラームが表示されるまで 5 ~ 10 分間待機します。ICSA は 5 分ごとに再試行します。同期成功のアラームが生成されない場合、または同期に失敗し続ける場合は、TAC サービス リクエストを開いてください。

この時点で、一括管理によるユーザの移行が完了し、移行元および移行先のクラスタで Cisco Intercluster Sync Agent サービスが開始された後に記録されたタイムスタンプと比較して、現在の時刻が 30 分後であるとする、5 つのリモート サンプル クラスタを確認したことになります。これで次の移動プロセスを続行できます。これ以上移動する必要がない場合は完了です。

ホーム クラスタでの連絡先リストのインポート

ユーザを新しいクラスタに移行したら、移行されたユーザの連絡先リストのデータを復元するために、連絡先リストをインポートします。

手順

ステップ1 前にエクスポートされた連絡先リストの CSV ファイルをアップロードします。

- a) [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[一括管理 (Bulk Administration)] > [ファイルのアップロード/ダウンロード (Upload/Download Files)] を選択します。
- b) [新規追加 (Add New)] をクリックします。
- c) 連絡先リストの CSV ファイルを選択するには、[参照 (Browse)] をクリックします。
- d) ターゲットとして [連絡先リスト (Contact Lists)] を選択します。
- e) トランザクションタイプとして [ユーザの連絡先のインポート-カスタムファイル (Import Users' Contacts - Custom File)] を選択します。
- f) 必要に応じて [ファイルが存在する場合は上書きする (Overwrite File if it exists)] をオンにします。
- g) [保存 (Save)] をクリックし、ファイルをアップロードします。
- h) [保存 (Save)] をクリックし、ファイルをアップロードします。

ステップ2 連絡先リスト ジョブのインポートを実行します。

- a) [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[一括管理 (Bulk Administration)] > [連絡先リスト (Contact List)] > [更新 (Update)] を選択します。
- b) ステップ 1 でアップロードした CSV ファイルを選択します。
- c) 任意でジョブの説明を更新します。
- d) ジョブを今すぐ実行するには、[今すぐ実行 (Run Immediately)] をクリックします。後で更新をスケジュールするには、[後で実行 (Run Later)] を選択します。
- e) [送信 (Submit)] をクリックします。

ステップ 3 連絡先リストのインポート ステータスをモニタします。

- a) [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[一括管理 (Bulk Administration)] > [連絡先リスト (Contact List)] > [ジョブスケジューラ (Job Scheduler)] を選択します。
- b) [検索 (Find)] をクリックして、すべての BAT ジョブをリストします。
- c) ステータスが完了と報告されたら、連絡先リストのインポート ジョブのジョブ ID を選択します。
- d) 連絡先リスト ファイルの内容を表示するには、[CSV ファイル名 (CSV File Name)] にリストされているファイルを選択します。
- e) [ログ ファイル名 (Log File Name)] リンクをクリックし、ログを開きます。
ジョブの開始時刻と終了時刻が表示され、結果の要約も表示されます。

古いクラスタのユーザの更新

新しいクラスタですべてが正常に動作していることを確認するまで、古いクラスタからユーザを削除したくない場合があります。一括管理の [ユーザの更新 (Update Users)] 機能を使用して古いクラスタから IM and Presence 機能を削除するには、この手順を使用します。

手順

- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] から、[一括管理 (Bulk Administration)] > [ユーザ (Users)] > [ユーザの更新 (Update Users)] > [クエリ (Query)] の順に選択します。
- ステップ 2** フィルタツールを使用して、移行中のユーザを検索します。たとえば、次の条件を満たすすべてのユーザを検索できます。**IM and Presence** が有効になっている。
- ステップ 3** [次へ (Next)] をクリックします。
- ステップ 4** 次の2つのフィールドのそれぞれについて、一番左のボックスをチェックし、右隣のボックスはオフのままにします。左側のボックスはフィールドを更新することを示し、右側のボックスは新しい設定 (チェックされていない) を示します。
 - [ホームクラスタ (Home Cluster)]

- [Unified CM IM and Presence のユーザを有効にする (Enable User for Unified CM IM and Presence)]

ステップ 5 [ジョブ情報 (Job Information)] で、[今すぐ実行 (Run Immediately)] を選択します。

ステップ 6 [送信 (Submit)] をクリックします。

次のタスク

移行がうまくいったこと、およびすべてのユーザが新しいクラスタで正しく構成されたことを確認したら、古いクラスタで移行したユーザを削除できます。



第 28 章

ロケールの管理

- [ロケールの管理の概要 \(379 ページ\)](#)
- [ロケールの管理の前提条件 \(380 ページ\)](#)
- [IM and Presence Service へのロケール インストーラのインストール \(381 ページ\)](#)

ロケールの管理の概要

複数の言語をサポートする Cisco Unified Communications Manager と IM and Presence サービスを設定できます。インストール可能なサポート言語の数に制限はありません。

www.cisco.com には、ロケール固有のバージョンの Cisco Unified Communications Manager のロケール インストーラと IM and Presence サービスのロケール インストーラが用意されています。このロケール インストーラはシステム管理者がインストールします。このインストーラを使用すると、ユーザがサポートされているインターフェイスを使用するときに、選択した翻訳済みテキストまたはトーン（使用可能な場合）を表示または受信できます。

Cisco Unified Communications Manager または IM and Presence Service をアップグレードした後で、すべてのロケールを再インストールする必要があります。Cisco Unified Communications Manager ノードまたは IM and Presence Service ノードの major.minor バージョン番号と一致する、最新バージョンのロケールをインストールしてください。

クラスタの各ノードに Cisco Unified Communications Manager をインストールし、データベースをセットアップしてから、ロケールをインストールします。IM and Presence Service ノードで特定のロケールをインストールする場合は、最初に Cisco Unified Communications Manager のクラスタで同じ国の Cisco Unified Communications Manager のロケール ファイルをインストールする必要があります。

ソフトウェアのアップグレードが完了した後に、Cisco Unified Communications Manager のノードと IM and Presence サービス ノードでロケールをインストールするには、次の項の情報を使用します。

ユーザ ロケール

ユーザ ロケール ファイルは、特定の言語と国に関する言語情報が含まれます。ユーザ ロケール ファイルは、ユーザが選択したロケールの電話機表示用の翻訳済みテキストとボイス プロンプト（使用可能な場合）、ユーザ アプリケーション、および Web ページを提供します。これらのファイル名の表記は、次のとおりです。

- `cm-locale-language-country-version.cop` (Cisco Unified Communications Manager)
- `ps-locale-language_country-version.cop` (IM and Presence Service)

システムでユーザ ロケールのみが必要な場合は、CUCM ロケールをインストールした後でそれをインストールします。

ネットワーク ロケール

ネットワーク ロケール ファイルは、電話トーン、アナウンサー、ゲートウェイ トーンなど、さまざまなネットワーク項目の国固有のファイルを提供します。複合ネットワーク ロケール ファイル名の表記は、次のとおりです。

- `cm-locale-combinednetworklocale-version.cop` (Cisco Unified Communications Manager)

1つのロケール インストーラに複数のネットワーク ロケールが組み合されている場合があります。



(注) シスコ承認の Cisco Unified Communications Manager および IM and Presence Service では、顧客が提供するサーバは複数のロケールをサポートできます。複数のロケール インストーラをインストールすることにより、ユーザは複数のロケールから選択できるようになります。

ロケール ファイルは、ソフトウェア アップグレードをインストールする場合と同じプロセスを使用して、ローカル ソースまたはリモート ソースからインストールできます。クラスタの各ノードに、複数のロケール ファイルをインストールできます。クラスタ内のすべてのノードをリブートしないと、変更は有効になりません。クラスタ内のすべてのノードですべてのロケールのインストールが終了するまで、ノードをリブートしないように強くお勧めします。通常の業務時間後にノードをリブートして、コール処理の中断を最小限にとどめてください。

ロケールの管理の前提条件

ロケールのインストールに関する考慮事項

- ロケールをインストールする前に、すべての Cisco Unified Communications Manager と IM and Presence サービスのクラスタノードをインストールし、データベースを設定します。

- IM and Presence Service ノードで特定のロケールをインストールする場合は、最初に Cisco Unified Communications Manager のクラスタで同じ国の Cisco Unified Communications Manager のロケール ファイルをインストールする必要があります。
- クラスタの各ノードに、複数のロケール ファイルをインストールできます。新しいロケールをアクティブにするには、インストール後にクラスタの各ノードを再起動する必要があります。
- ロケール ファイルは、ソフトウェア アップグレードをインストールする場合と同じプロセスを使用して、ローカルソースまたはリモートソースからインストールできます。ローカルソースまたはリモートソースからのアップグレードの詳細については、『*Upgrade Guide for Cisco Unified Communications Manager*』を参照してください。

IM and Presence Service へのロケール インストーラのインストール

- IM and Presence Service にロケールをインストールしてから、Cisco Unified Communications Manager にロケールをインストールします。英語以外のロケールを使用する場合は、Cisco Unified Communications Manager と IM and Presence Service の両方に適切な言語インストーラをインストールする必要があります。
- IM and Presence Service クラスタに複数のノードがある場合は、ロケールインストーラがクラスタ内のすべてのノードにインストールされていることを確認します（サブスクライバノードの前に IM and Presence データベース パブリッシュャ ノードにインストールします）。
- 適切なすべてのロケール インストーラが両方のシステムにロードされるまで、ユーザ ロケールを設定しないでください。ロケールインストーラが Cisco Unified Communications Manager にロードされた後であっても、IM and Presence Service にロードされる前にユーザがユーザロケールを設定してしまうと、問題が発生することがあります。問題が報告された場合は、各ユーザに対し、Cisco Unified Communications Self Care Portal にサインインし、ロケールを現在の設定から [英語 (English)] に変更してから適切な言語に戻すように指示することを推奨します。BAT ツールを使用してユーザ ロケールを適切な言語に同期することもできます。

手順

- ステップ 1** cisco.com に移動し、IM and Presence Service のバージョンのロケールインストーラを選択します。 <http://software.cisco.com/download/navigator.html?mdfid=285971059>
- ステップ 2** 作業環境に適した IM and Presence ロケール インストーラのバージョンをクリックします。
- ステップ 3** ファイルをダウンロードしたら、ハードドライブに保存し、ファイルの保存場所をメモします。

- ステップ 4** SFTP をサポートするサーバにこのファイルをコピーします。
- ステップ 5** 管理者のアカウントとパスワードを使用して Cisco Unified IM and Presence オペレーティングシステムの管理にサインインします。
- ステップ 6** **[Software Upgrades (ソフトウェア アップグレード)] > [Install/Upgrade (インストール/アップグレード)]** を選択します。
- ステップ 7** ソフトウェアの入手先として **[リモート ファイル システム (Remote File System)]** を選択します。
- ステップ 8** **[ディレクトリ (Directory)]** フィールドにファイルの保存場所 (/tmp など) を入力します。
- ステップ 9** **[サーバ (Server)]** フィールドに IM and Presence Service のサーバ名を入力します。
- ステップ 10** **[ユーザ名 (User Name)]** フィールドと **[ユーザー パスワード (User Password)]** フィールドに自分のユーザ名とパスワードを入力します。
- ステップ 11** **[転送プロトコル (Transfer Protocol)]** で **[SFTP (SFTP)]** を選択します。
- ステップ 12** **[次へ (Next)]** をクリックします。
- ステップ 13** 検索結果のリストから IM and Presence サービス ロケール インストーラを選択します。
- ステップ 14** **[次へ (Next)]** をクリックして、インストーラ ファイルをロードし、検証します。
- ステップ 15** ロケールのインストールが完了したら、クラスタ内の各サーバを再起動します。
- ステップ 16** インストールされるロケールのデフォルト設定は、「英語 (米国) (English United States)」です。IM and Presence サービス ノードの再起動中に、必要に応じて、ダウンロードしたインストーラのロケールに合わせてブラウザの言語を変更してください。
- ステップ 17** ユーザがサポートされている製品のロケールを選択できることを確認します。
- ヒント** クラスタ内のすべてのサーバに同じコンポーネントをインストールしてください。

エラーメッセージロケールリファレンス

ロケールインストーラをアクティベーションするときに発生する可能性のあるメッセージの説明については、次の表を参照してください。エラーが発生した場合は、インストールログにあるメッセージを表示できます。

表 36: ロケールインストーラのエラーメッセージと説明

メッセージ (Message)	説明
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	データベースに追加するユーザ ロケール情報が格納されている CSV ファイルが見つからない場合にこのエラーが発生します。これはビルドプロセスのエラーを示しています。

メッセージ (Message)	説明
<p>[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.</p>	<p>データベースに追加するネットワーク ロケール情報が格納されている CSV ファイルが見つからない場合にこのエラーが発生します。これはビルドプロセスのエラーを示しています。</p>
<p>[LOCALE] CSV file installer installdb is not present or not executable</p>	<p>installdb と呼ばれるアプリケーションが存在することを確認する必要があります。このアプリケーションは CSV ファイルに含まれる情報を読み取り、それをターゲットデータベースに正しく適用します。このアプリケーションが見つからない場合、Cisco Unified Communications アプリケーションとともにインストールされなかった（ほとんどあり得ません）、削除された（可能性はあります）、またはノードに Cisco Unified Communications Manager や IM and Presence Service などの Cisco Unified Communications アプリケーションがインストールされていません（最も可能性があります）。データベースに適切なレコードが格納されていないとロケールは機能しないため、ロケールのインストールは中止されます。</p>
<p>[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum.</p> <p>[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum.</p> <p>[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum.</p> <p>[ロケール] /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum を作成できません。</p>	<p>これらのエラーは、システムがチェックサムファイルの作成に失敗した場合に発生します。原因としては、Java 実行ファイルの /usr/local/thirdparty/java/j2sdk/jre/bin/java が存在しない、Java アーカイブファイルの /usr/local/cm/jar/cmutil.jar が存在しないか損傷している、Java クラスの com.cisco.ccm.util.Zipper が存在しないか損傷していることなどが考えられます。これらのエラーが発生する場合でも、Cisco Unified Communications Manager Assistant を除いてロケールは引き続き正常に動作します。この場合、Cisco Unified Communications Manager Assistant では、ローカライズされた Cisco Unified Communications Manager Assistant ファイルの変化を検出できません。</p>
<p>[ロケール] /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information を検索できません。</p>	<p>このエラーは、適切な場所にファイルが見つからない場合に発生します。原因としては、ビルドプロセスのエラーが考えられます。</p>

メッセージ (Message)	説明
[LOCALE] Addition of <locale-installer-file-name> to the database has failed!	このエラーは、ロケールのインストール時に発生した何らかの失敗が累積されたために発生します。最終状態を示しています。
[LOCALE] Could not locate <locale-installer-file-name>	このロケールはアップグレード中移行されません。 ダウンロードされたロケール インストーラ ファイルは、ダウンロード ロケーションに置かれていません。移動または削除された可能性があります。このエラーの重大度は低く、Cisco Unified Communications アプリケーションのアップグレード後にロケール インストーラを再適用するか、新しいロケール インストーラをダウンロードして適用する必要があることを示します。
[LOCALE] Could not copy <locale-installer-file-name> to migratory path. This locale will not be migrated during an upgrade!	ダウンロードされたロケール インストーラ ファイルを移行パスにコピーできません。このエラーの重大度は低く、Cisco Unified Communications アプリケーションのアップグレード後にロケール インストーラを再適用するか、新しいロケール インストーラをダウンロードして適用する必要があることを示します。
[LOCALE] DRS unregistration failed	ロケール インストーラはディザスタリカバリ システムから登録解除できませんでした。バックアップまたはリストア レコードにはロケール インストーラは含まれません。インストールのログを記録して、Cisco TAC にお問い合わせください。
[LOCALE] Backup failed!	ディザスタリカバリ システムは、ダウンロードされたロケール インストーラ ファイルから tarball を作成できませんでした。バックアップを試みる前に、ローカル インストーラを再適用してください。 (注) システムの復元後にロケールを手動で再インストールすることもできます。

メッセージ (Message)	説明
[LOCALE] No COP files found in restored tarball!	バックアップファイルの破損によって、ロケールインストーラファイルの抽出が失敗した可能性があります。 (注) ロケールインストーラを手動で再適用すると、ロケールが完全に復元されます。
[LOCALE] Failed to successfully reinstall COP files!	バックアップファイルの破損によって、ロケールインストーラファイルが損傷した可能性があります。 (注) ロケールインストーラを手動で再適用すると、ロケールが完全に復元されます。
[LOCALE] Failed to build script to reinstall COP files!	プラットフォームで、ロケールの再インストールに使用されるスクリプトを動的に作成できませんでした。 (注) ロケールインストーラを手動で再適用すると、ロケールが完全に復元されます。インストールのログを記録して、TAC にお問い合わせください。

ローカライズされたアプリケーション

IM and Presence Service アプリケーションはさまざまな言語をサポートします。ローカライズされたアプリケーションおよび使用可能な言語のリストについては、次の表を参照してください。

表 37: ローカライズされたアプリケーションおよびサポートされる言語のリスト

インターフェイス (Interface)	サポートされる言語
管理アプリケーション	
Cisco Unified CM IM and Presence の管理	中国語 (中国)、英語、日本語 (日本)、韓国語 (韓国)
Cisco Unified IM and Presence オペレーティング システム	中国語 (中国)、英語、日本語 (日本)、韓国語 (韓国)



第 29 章

サーバの管理

- サーバの管理の概要 (387 ページ)
- サーバアドレスの変更 (387 ページ)
- クラスタからの IM and Presence ノードの削除 (388 ページ)
- 削除したサーバをクラスタに戻す (389 ページ)
- インストール前のクラスタへのノードの追加 (389 ページ)
- プレゼンス サーバのステータスの表示 (390 ページ)
- ハイ アベイラビリティでのサービスの再起動 (391 ページ)
- ホスト名の設定 (392 ページ)

サーバの管理の概要

この章では、展開されたシステムのサーバ詳細を編集する方法について説明します。これには、新しいノードのクラスタへの割り当て、クラスタからのノードの削除、プレゼンスステータスの表示、およびサーバアドレスの詳細の変更が含まれます。

サーバアドレスの変更

稼働中のシステムがあり、サーバのアドレス指定に対して以下の変更を加える必要がある場合は、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>で *Cisco Unified Communications Manager* および *IM and Presence* サービスの IP アドレスとホスト名の変更にある手順を参照してください。

これは、次の種類の住所変更に適用されます。

- サーバの IP アドレスの変更
- サーバのホスト名の変更
- ノード名の変更 (例えば、IP アドレスを使用してノード名を定義していて、代わりにホスト名を使用したい場合)。

- IM and Presence サービスのデフォルトドメインの変更

クラスタからの IM and Presence ノードの削除

プレゼンス冗長グループおよびクラスタから IM and Presence Service ノードを安全に削除する必要がある場合は、この手順に従います。



注意 ノードを削除すると、そのプレゼンス冗長グループの残りのノードで、ユーザに対するサービスが中断されます。この手順は、メンテナンス時間中のみ実行してください。

手順

- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] > [システム (System)] > [プレゼンス冗長グループ (Presence Redundancy Groups)] ページで、高可用性が有効な場合は無効にします。
- ステップ 2** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] > [ユーザ管理 (User Management)] > [プレゼンスユーザの割り当て (Assign Presence Users)] ページで、削除するノードからすべてのユーザの割り当てを解除するか、移動します。
- ステップ 3** プレゼンス冗長グループからノードを削除するには、プレゼンス冗長グループの [プレゼンス冗長グループの設定 (Presence Redundancy Group Configuration)] ページの [プレゼンスサーバ (Presence Server)] ドロップダウンリストから、[未選択 (Not-Selected)] を選択します。ノードの割り当て解除の結果として、プレゼンス冗長グループ内のサービスが再起動されることを示す警告ダイアログボックスが表示されたら、[OK] を選択します。

(注) プレゼンス冗長グループからパブリッシャノードを直接削除することはできません。パブリッシャノードを削除するには、まずパブリッシャノードからユーザの割り当てを解除し、プレゼンス冗長グループを完全に削除します。

ただし、削除した IM and Presence ノードをクラスタに再び追加することもできます。削除されたノードを追加する方法の詳細については、「[削除したサーバをクラスタに戻す \(389ページ\)](#)」を参照してください。この場合、削除されたパブリッシャノードが Cisco Unified CM 管理コンソールの [システム (System)] > [サーバ (Server)] 画面でサーバに再び追加されると、**DefaultCUPSubcluster** が自動的に作成されます。
- ステップ 4** Cisco Unified CM Administration で、[システム (System)] > [サーバ (Server)] から未割り当てのノードを削除します。この操作は取り消せないことを示す警告ダイアログボックスが表示されたら、[OK] をクリックします。
- ステップ 5** 割り当てを解除したノードのホスト VM またはサーバをシャットダウンします。
- ステップ 6** すべてのノードの **Cisco XCP Router** を再起動します。

削除したサーバをクラスタに戻す

Cisco Unified Communications Manager Administration から後続のノード（サブスライバ）を削除してそれをクラスタに戻す場合に、次の手順を実行します。

手順

-
- ステップ 1** Cisco Unified Communications Manager Administration で、[システム (System)] > [サーバ (Server)] を選択してサーバを追加します。
- ステップ 2** 後続のノードを Cisco Unified Communications Manager Administration に追加したら、シスコが提供しているお使いのバージョンのソフトウェア キットに付属しているディスクを使用して、サーバ上でインストールを実行します。
- ヒント** インストールするバージョンが、パブリッシャノードで動作しているバージョンと一致することを確認します。パブリッシャで実行されているバージョンがインストールファイルと一致しない場合は、インストールプロセス中に [Upgrade While Install] オプションを選択します。詳細は、*Cisco Unified Communications Manager* および *IM and Presence Service* リリース 11.5(1) インストール ガイドを参照してください。
- ステップ 3** Cisco UnifiedCM をインストールしたら、その Cisco UnifiedCM のバージョンをサポートしているインストール マニュアルの説明に従って、後続のノードを設定します。
- ステップ 4** Cisco Unified Reporting、RTMT、または CLI にアクセスして、データベース レプリケーションが既存のノード間で発生していることを確認します。必要に応じて、ノード間のデータベース レプリケーションを修復します。
-

インストール前のクラスタへのノードの追加

ノードをインストールする前に、Cisco Unified Communications Manager Administration を使用して、新しいノードをクラスタに追加します。ノードの追加時に選択するサーバタイプは、インストールしたサーバタイプと一致する必要があります。

新しいノードをインストールする前に、Cisco Unified Communications Manager Administration を使用して、最初のノードで新しいノードを設定する必要があります。クラスタにノードをインストールする方法については、『*Cisco Unified Communications Manager Installation Guide*』を参照してください。

Cisco Unified Communications Manager のビデオ/音声サーバでは、Cisco Unified Communications Manager ソフトウェアの初期インストール中に追加した最初のサーバがパブリッシャノードに指定されます。後続のすべてのサーバインストールまたは追加は、サブスライバノードに指定されます。クラスタに追加した最初の Cisco Unified Communications Manager IM and Presence ノードが、IM and Presence Service データベース パブリッシャノードに指定されます。



(注) サーバの追加後は、Cisco Unified Communications Manager Administration を使用して、サーバタイプを変更できなくなります。既存のサーバインスタンスを削除してから、再度、新しいサーバを追加して、正しいサーバタイプ設定を選択する必要があります。

手順

ステップ 1 [システム (System)] > [サーバ (Server)] を選択します。

[サーバの検索/一覧表示 (Find and List Servers)] ウィンドウが表示されます。

ステップ 2 [新規追加 (Add New)] をクリックします。

[サーバの設定 - サーバを追加 (Server Configuration - Add a Server)] ウィンドウが表示されます。

ステップ 3 [サーバタイプ (Server Type)] ドロップダウン リスト ボックスで、追加するサーバタイプを選択してから、[次へ (Next)] をクリックします。

- CUCM ビデオ/音声
- CUCM IM and Presence

ステップ 4 [サーバの設定 (Server Configuration)] ウィンドウで、適切なサーバ設定を入力します。

サーバ設定フィールドの説明については、「[Server Settings](#)」を参照してください。

ステップ 5 [保存 (Save)] をクリックします。

プレゼンス サーバのステータスの表示

IM and Presence Service ノードの重要なサービスのステータスと自己診断テスト結果を確認するには、Cisco Unified Communications Manager の管理を使用します。

手順

ステップ 1 [システム (System)] > [サーバ (Server)] を選択します。

[サーバの検索/一覧表示 (Find and List Servers)] ウィンドウが表示されます。

ステップ 2 サーバの検索パラメータを選択し、[検索 (Find)] をクリックします。

一致するレコードが表示されます。

ステップ3 [サーバの検索/一覧表示 (Find and List Servers)] ウィンドウに表示される IM and Presence サーバを選択します。

[サーバの設定 (Server Configuration)] ウィンドウが表示されます。

ステップ4 [サーバの設定 (Server Configuration)] ウィンドウの IM and Presence サーバ情報のセクションで、プレゼンスサーバステータスのリンクをクリックします。

サーバの [ノードの詳細 (Node Details)] ウィンドウが表示されます。

ハイアベイラビリティでのサービスの再起動

ハイアベイラビリティを無効にしてから Cisco XCP ルータ、Cisco Presence Engine、またはサーバ自体を再起動する必要がある、システムの設定変更またはシステムアップグレードを行う場合は、ハイアベイラビリティを有効にする前に Cisco Jabber セッションを再作成するのに十分な時間を確保する必要があります。十分な時間を確保しない場合、セッションが作成されていない Jabber クライアントでプレゼンスは機能しません。

次のプロセスに従います。

手順

- ステップ1** 変更を行う前に、[Cisco Unified CM IM and Presenceの管理 (Cisco Unified CM IM and Presence Administration)] ウィンドウの [プレゼンストポロジ (Presence Topology)] ウィンドウ ([システム (System)] > [プレゼンストポロジ (Presence Topology)]) を確認します。各プレゼンス冗長グループの各ノードに割り当てられたユーザ数を記録します。
- ステップ2** 各プレゼンス冗長グループでハイアベイラビリティを無効にし、新しいHA設定が同期されるまで少なくとも2分間待ちます。
- ステップ3** 更新に必要な次のいずれかを実行します。
- Cisco XCP ルータの再起動
 - Cisco Presence Engine の再起動
 - サーバを再起動します。
- ステップ4** 再起動後、すべてのノードでアクティブなセッションの数をモニタします。
- ステップ5** 各ノードで、show perf query counter "Cisco Presence Engine" ActiveJsmSessions CLI コマンドを実行し、各ノードでアクティブなセッションの数を確認します。アクティブなセッションの数は、手順1で記録した割り当てられているユーザの数と一致するはずですが、すべてのセッションが15分以内に再開します。
- ステップ6** すべてのセッションが作成されたら、プレゼンス冗長グループ内でハイアベイラビリティを有効にできます。

- (注) 30分が経過し、アクティブセッションがまだ作成されていない場合は、Cisco Presence Engineを再起動します。それでも問題が解決しない場合は、システムに修正すべき大きな問題があります。
- (注) Cisco XCP ルータまたは Cisco Presence Engine、あるいはその両方を連続して再起動することはお勧めできません。ただし、再起動が必要な場合は、最初のサービスを再起動し、すべてのJSMセッションが再作成されるのを待ちます。すべてのJSMセッションが作成されたら、2回目の再起動を行います。

ホスト名の設定

次の表に、Unified Communications Manager サーバのホスト名を設定できる場所、ホスト名として指定できる文字数、および推奨されるホスト名の先頭文字と最終文字を示します。ホスト名を正しく設定しないと、Unified Communications Manager の一部のコンポーネント（オペレーティングシステム、データベース、インストールなど）が期待通りに機能しない可能性があります。

表 38 : Cisco Unified Communications Manager におけるホスト名の設定

ホスト名の場所	可能な設定	指定できる文字数	推奨されるホスト名の先頭文字	推奨されるホスト名の最終文字
[ホスト名/IP アドレス (Host Name/IP Address)]フィールド Cisco Unified Communications Manager Administration の [システム (System)]>[サーバ (Server)]	クラスタ内のサーバのホスト名を追加または変更できます。	2 ~ 63	英字	英数字
[ホスト名 (Hostname)]フィールド Cisco Unified Communications Manager インストール ウィザード	クラスタ内のサーバのホスト名を追加できます。	1 ~ 63	英字	英数字
[ホスト名 (Hostname)]フィールド Cisco Unified Communications オペレーティング システム の [設定 (Settings)]>[IP]>[イーサネット (Ethernet)]	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1 ~ 63	英字	英数字

ホスト名の場所	可能な設定	指定できる文字数	推奨されるホスト名の先頭文字	推奨されるホスト名の最終文字
set network hostname hostname コマンドライン インターフェイス	クラスタ内のサーバのホスト名を変更できますが、追加できません。	1 ~ 63	英字	英数字



ヒント このホスト名は、ARPANET ホスト名の規則に従う必要があります。ホスト名の先頭文字と最終文字の間には、英数文字とハイフンを入力できます。

いずれかの場所でホスト名を設定する前に、次の情報を確認してください。

- [サーバの設定 (Server Configuration)] ウィンドウの [ホスト名/IP アドレス (Host Name/IP Address)] フィールドは、デバイスとサーバ間、アプリケーションとサーバ間、および異なるサーバ間の通信をサポートします。このフィールドには、ドット区切り形式の IPv4 アドレスまたはホスト名を入力できます。

Unified Communications Manager パブリッシャ ノードをインストールした後は、パブリッシャのホスト名がこのフィールドに自動的に表示されます。Unified Communications Manager サブスクライバ ノードをインストールする前に、Unified Communications Manager パブリッシャ ノードでこのフィールドにサブスクライバ ノードの IP アドレスまたはホスト名を入力してください。

このフィールドにホスト名を設定できるのは、Unified Communications Manager が DNS サーバにアクセスしてホスト名を IP アドレスに解決できる場合のみです。DNS サーバに Cisco Unified Communications Manager の名前とアドレスの情報が設定されていることを確認してください。



ヒント DNS サーバに Unified Communications Manager の情報を設定するのに加えて、Cisco Unified Communications Manager のインストール時に DNS 情報を入力します。

- Unified Communications Manager パブリッシャ ノードのインストール時に、ネットワーク情報を設定するために (つまり、スタティック ネットワークを使用する場合に) パブリッシャ サーバのホスト名 (必須) と IP アドレスを入力します。

Unified Communications Manager サブスクライバ ノードのインストール時には、Unified Communications Manager パブリッシャ ノードのホスト名と IP アドレスを入力して、Unified Communications Manager がネットワークの接続性およびパブリッシャ とサブスクライバ 間の検証を確認できるようにしてください。さらに、サブスクライバ ノードのホスト名と IP アドレスも入力する必要があります。Unified Communications Manager のインストール時にサブスクライバ サーバのホスト名の入力を求められた場合は、Cisco Unified Communications Manager Administration の ([ホスト名/IP アドレス (Host Name/IP Address)]

フィールドでサブスクライバサーバのホスト名を設定した場合に [サーバの設定 (Server Configuration)] ウィンドウに表示される値を入力します。



第 30 章

システムのバックアップ

- [バックアップの概要 \(395 ページ\)](#)
- [バックアップの前提条件 \(396 ページ\)](#)
- [バックアップタスクフロー \(396 ページ\)](#)
- [バックアップの連携動作と制限事項 \(403 ページ\)](#)

バックアップの概要

定期的にバックアップを行うことを推奨します。ディザスタリカバリシステム (DRS) を使用して、クラスタ内のすべてのサーバのデータを完全にバックアップできます。自動バックアップをセットアップすることも、任意の時点でバックアップを起動することもできます。

ディザスタリカバリシステムで実行するバックアップは、クラスタレベルであり、Cisco Unified Communications Manager クラスタ内のすべてのサーバのバックアップを 1 箇所に集め、バックアップデータを物理的なストレージデバイスにアーカイブします。バックアップファイルは暗号化され、システムソフトウェアによってだけ開くことができます。

DRS は、プラットフォームのバックアップ/復元の一環として、独自の設定 (バックアップデバイス設定およびスケジュール設定) を復元します。DRS は `drfDevice.xml` ファイルと `drfSchedule.xml` ファイルをバックアップおよび復元します。これらのファイルとともにサーバを復元するときは、DRS バックアップデバイスおよびスケジュールを再設定する必要があります。

システムデータを復元するときには、クラスタ内のどのノードを復元するかを選択できます。

ディザスタリカバリシステムには、次の機能があります。

- バックアップおよび復元タスクを実行するためのユーザインターフェイス。
- バックアップ機能を実行するための分散システムアーキテクチャ。
- スケジュールバックアップまたは手動 (ユーザが起動する) バックアップ。
- リモート SFTP サーバへのバックアップのアーカイブ。

バックアップの前提条件

- バージョンの要件を満たしていることを確認してください。
 - すべての Cisco Unified Communications Manager クラスタ ノードは、同じバージョンの Cisco Unified Communications Manager アプリケーションを実行している必要があります。
 - すべての IM and Presence Service クラスタ ノードは、同じバージョンの IM and Presence Service アプリケーションを実行している必要があります。
 - バックアップ ファイルに保存されているソフトウェア バージョンが、クラスタ ノードで実行されるバージョンと同じでなければなりません。

バージョンの文字列全体が一致している必要があります。たとえば、IM and Presence データベース パブリッシャ ノードがバージョン 11.5.1.10000-1 の場合、すべての IM and Presence サブスクリバ ノードは 11.5.1.10000-1 であり、バックアップ ファイルに保存されているバージョンも 11.5.1.10000-1 でなければなりません。現在のバージョンと一致しないバックアップ ファイルからシステムを復元しようすると、復元は失敗します。バックアップ ファイルに保存されているバージョンが、クラスタ ノードで実行されているバージョンと一致するよう、ソフトウェア バージョンをアップグレードしたら常にシステムをバックアップするようにしてください。

- DRS 暗号化は、クラスタ セキュリティ パスワードに依存することに留意してください。バックアップの実行中に、DRS は暗号化のためにランダム パスワードを生成し、そのランダム パスワードをクラスタ セキュリティ パスワードを使用して暗号化します。バックアップを実行した後、復元を行うまでの間にクラスタ セキュリティ パスワードが変更された場合、そのバックアップファイルを使用してシステムを復元するには、バックアップを実行した時点でのパスワードを把握していなければなりません。あるいは、セキュリティ パスワードを変更/リセットした直後にバックアップを作成するようにしてください。
- リモート デバイスをバックアップする必要がある場合は、必ず SFTP サーバを設定する必要があります。利用可能な SFTP サーバの詳細については、次の項を参照してください。
[リモート バックアップ用 SFTP サーバ \(404 ページ\)](#)

バックアップ タスク フロー

次のタスクを実行して、バックアップを設定して実行します。バックアップの実行中は OS 管理タスクを実行しないでください。これは、ディザスタ リカバリ システムがプラットフォーム API をロックすることにより、すべての OS 管理要求をブロックするためです。ただし、CLI ベースのアップグレード コマンドしかプラットフォーム API ロッキング パッケージを使用しないため、ディザスタ リカバリ システムはほとんどの CLI コマンドを妨害しません。

手順

	コマンドまたはアクション	目的
ステップ 1	バックアップデバイスの設定 (397 ページ)	データをバックアップするデバイスを指定します。
ステップ 2	バックアップ ファイルのサイズの予測 (398 ページ)	SFTP デバイス上で作成されるバックアップ ファイルのサイズを見積もります。
ステップ 3	次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> スケジュール バックアップの設定 (399 ページ) 手動バックアップの開始 (401 ページ) 	スケジュールに従ってデータをバックアップするためのバックアップ スケジュールを作成します。 または、手動バックアップを実行します。
ステップ 4	現在のバックアップ ステータスの表示 (402 ページ)	これはオプションです。バックアップのステータスをチェックします。バックアップの実行中、現在のバックアップジョブのステータスを確認できます。
ステップ 5	バックアップ履歴の表示 (402 ページ)	これはオプションです。バックアップ履歴の表示

バックアップ デバイスの設定

最大 10 個のバックアップデバイスを設定できます。バックアップ ファイルを保存する場所を設定するには、次の手順を実行します。

始める前に

- バックアップ ファイルを保存するために SFTP サーバにディレクトリ パスへの書き込みアクセス権があることを確認します。
- DRS マスターエージェントがバックアップデバイスの設定を検証するときに、ユーザ名、パスワード、サーバ名とディレクトリ パスが有効であることを確認します。



(注) バックアップはネットワークトラフィックが少なくなる時間帯にスケジューリングしてください。

手順

-
- ステップ1** ディザスタリカバリシステムから、[バックアップ (Backup)] > [バックアップ デバイス (Backup Device)] の順に選択します。
- ステップ2** [バックアップ デバイス リスト (Backup Device List)] ウィンドウで、次のいずれかを実行します。
- 新しいデバイスを設定するには、[新規追加 (Add New)] をクリックします。
 - 既存のバックアップ デバイスを編集するには、検索条件を入力し、[検索 (Find)]、次に [選択項目の編集 (Edit Selected)] をクリックします。
 - バックアップ デバイスを削除するには、[バックアップ デバイス (Backup Device)] リストでバックアップ デバイスを選択してから [選択項目の削除 (Delete Selected)] をクリックします。
- バックアップ スケジュールにバックアップ デバイスとして設定されているバックアップ デバイスは削除できません。
- ステップ3** [バックアップ デバイス名 (Backup device name)] フィールドにバックアップ名を入力します。バックアップ デバイス名には、英数字、スペース ()、ダッシュ (-)、およびアンダースコア (_) だけを使用します。それ以外の文字は使用しないでください。
- ステップ4** [接続先の選択 (Select Destination)] 領域の [ネットワーク ディレクトリ (Network Directory)] で、次を実行します。
- [ホスト名/IP アドレス (Host name/IP Address)] フィールドに、ネットワーク サーバのホスト名または IP アドレスを入力します。
 - [パス名 (Path name)] フィールドに、バックアップ ファイルを格納するディレクトリ パスを入力します。
 - [ユーザ名 (User name)] フィールドに、有効なユーザ名を入力します。
 - [パスワード (Password)] フィールドに、有効なパスワードを入力します。
 - [ネットワーク ディレクトリに保存するバックアップ数 (Number of backups to store on Network Directory)] ドロップダウン リストから、バックアップの必要数を選択します。
- ステップ5** [保存 (Save)] をクリックします。
-

次のタスク

[バックアップ ファイルのサイズの予測 \(398 ページ\)](#)

バックアップ ファイルのサイズの予測

1 つまたは複数の選択した機能のバックアップ履歴が存在する場合に限り、Cisco Unified Communications Manager は、バックアップ tar のサイズを予測します。

計算されたサイズは正確な値ではなく、バックアップ tar の予測サイズです。サイズは前のバックアップの実際のバックアップサイズに基づいて計算され、設定が前回のバックアップ以降変更された場合は異なることがあります。

この手順は、前回のバックアップが存在する場合にのみ使用でき、初めてシステムをバックアップする場合は使用できません。

SFTP デバイスに保存されているバックアップ tar のサイズを予測するには、次の手順に従ってください。

手順

ステップ 1 ディザスタリカバリシステムから、[バックアップ (Backup)] > [手動バックアップ (Manual Backup)] の順に選択します。

ステップ 2 [機能の選択 (Select Features)] 領域でバックアップする機能を選択します。

ステップ 3 選択した機能のバックアップの予測サイズを表示するには、[サイズの予測 (Estimate Size)] を選択します。

次のタスク

システムをバックアップするには、次のいずれかの手順を実行します。

- [スケジュールバックアップの設定 \(399 ページ\)](#)
- [手動バックアップの開始 \(401 ページ\)](#)

スケジュールバックアップの設定

最大 10 個のバックアップスケジュールを作成できます。各バックアップスケジュールには、自動バックアップのスケジュール、バックアップする機能セット、保存場所など、独自のプロパティがあります。

バックアップ .tar ファイルはランダムに生成されるパスワードで暗号化されるということに注意してください。このパスワードは、クラスタセキュリティパスワードで暗号化され、バックアップ .tar ファイルとともに保存されます。このセキュリティパスワードは忘れないように記憶しておくか、またはセキュリティパスワードを変更またはリセットしたらすぐにバックアップを作成する必要があります。



注意 コール処理が中断してサービスに影響が及ばないように、バックアップはオフピーク時間中にスケジュールしてください。

始める前に

[バックアップデバイスの設定 \(397 ページ\)](#)

手順

- ステップ 1** ディザスタリカバリシステムで、[バックアップスケジューラ (Backup Scheduler)] を選択します。
- ステップ 2** [スケジュールリスト (Schedule List)] ウィンドウで、新規スケジュールを追加するか、または既存のスケジュールを編集します。
- 新規スケジュールを作成するには、[新規追加 (Add New)] をクリックします。
 - 既存のスケジュールを設定するには、[スケジュールリスト (Schedule List)] 列でその名前をクリックします。
- ステップ 3** [スケジューラ (scheduler)] ウィンドウで、[スケジュール名 (Schedule Name)] フィールドにスケジュール名を入力します。
- (注) デフォルトのスケジュールの名前は変更できません。
- ステップ 4** [バックアップデバイスの選択 (Select Backup Device)] 領域でバックアップデバイスを選択します。
- ステップ 5** [機能の選択 (Select Features)] 領域でバックアップする機能を選択します。少なくとも1つの機能を選択する必要があります。
- ステップ 6** [バックアップの開始時刻 (Start Backup at)] 領域でバックアップを開始する日付と時刻を選択します。
- ステップ 7** [頻度 (Frequency)] 領域でバックアップを行う頻度を選択します。頻度は、[一度 (Once)]、[日次 (Daily)]、[週次 (Weekly)]、[月次 (Monthly)] に設定できます。[週次 (Weekly)] を選択した場合は、バックアップを行う週の曜日も選択できます。
- ヒント バックアップ頻度を火曜日から土曜日までの [週次 (Weekly)] に設定するには、[デフォルトの設定 (Set Default)] をクリックします。
- ステップ 8** これらの設定を更新するには、[保存 (Save)] をクリックします。
- ステップ 9** 次のいずれかのオプションを選択します。
- 選択したスケジュールをイネーブルにするには、[選択されたスケジュールの有効化 (Enable Selected Schedules)] をクリックします。
 - 選択したスケジュールをディセーブルにするには、[選択されたスケジュールの無効化 (Disable Selected Schedules)] をクリックします。
 - 選択したスケジュールを削除するには、[選択項目の削除 (Delete Selected)] をクリックします。
- ステップ 10** スケジュールを有効にするには、[スケジュールの有効化 (Enable Schedule)] をクリックします。
- 設定した時刻になると自動的に次のバックアップが実行されます。

- (注) クラスタ内のすべてのサーバが、同じバージョンの Cisco Unified Communications Manager または Cisco IM and Presence サービスを実行し、ネットワークから到達可能であることを確認します。スケジュールされたバックアップの時刻にサーバに到達できないと、そのサーバはバックアップされません。

次のタスク

次の手順を実行します。

- [バックアップ ファイルのサイズの予測 \(398 ページ\)](#)
- (オプション) [現在のバックアップ ステータスの表示 \(402 ページ\)](#)

手動バックアップの開始

始める前に

- バックアップ ファイルの格納場所としてネットワーク デバイスを使用していることを確認します。Unified Communications Manager の仮想化展開では、テープ ドライブによるバックアップ ファイルの保存はサポートされません。
- Cisco Unified Communications Manager または IM and Presence Service のインストールされているバージョンが、すべてのクラスタ ノードで同じであることを確認します。
- バックアップ プロセスは、リモート サーバに利用可能な容量がないためや、ネットワーク接続が中断されたために失敗することがあります。バックアップが失敗する原因となった問題に対処した後、新規のバックアップを開始する必要があります。
- ネットワークの中断がないことを確認してください。
- [バックアップ デバイスの設定 \(397 ページ\)](#)
- [バックアップ ファイルのサイズの予測 \(398 ページ\)](#)
- クラスタ セキュリティ パスワードのレコードがあることを確認します。このバックアップの完了後に、クラスタ セキュリティ パスワードを変更した場合は、パスワードを認識している必要があります。パスワードを認識していないと、バックアップファイルを使用してシステムを復元できなくなります。



- (注) バックアップが実行されている間は、Disaster Recovery System がプラットフォーム API をロックしてすべての要求をブロックするため、Cisco Unified OS の管理または Cisco Unified IM and Presence OS の管理でタスクを実行することはできません。ただし、CLI ベースのアップグレード コマンドしかプラットフォーム API ロッキング パッケージを使用しないため、ディザスタリカバリ システムはほとんどの CLI コマンドを妨害しません。

手順

- ステップ1 ディザスタリカバリシステムから、[バックアップ (Backup)] > [手動バックアップ (Manual Backup)] の順に選択します。
- ステップ2 [手動バックアップ (Manual Backup)] ウィンドウで、[バックアップデバイス名 (Backup Device Name)] 領域を選択します。
- ステップ3 [機能の選択 (Select Features)] 領域から機能を選択します。
- ステップ4 [バックアップの開始 (Start Backup)] をクリックします。

次のタスク

(オプション) [現在のバックアップステータスの表示 \(402 ページ\)](#)

現在のバックアップステータスの表示

現在のバックアップジョブのステータスを確認するには、次の手順を実行します。



注意 リモートサーバへのバックアップが20時間以内に完了しないとバックアップセッションがタイムアウトするため、新規バックアップを開始する必要があります。

手順

- ステップ1 ディザスタリカバリシステムから、[バックアップ (Backup)] > [現在のステータス (Current Status)] の順に選択します。
- ステップ2 バックアップログファイルを表示するには、ログファイル名リンクをクリックします。
- ステップ3 現在のバックアップをキャンセルするには、[バックアップのキャンセル (Cancel Backup)] をクリックします。

(注) 現在のコンポーネントがバックアップ操作を完了した後、バックアップがキャンセルされます。

次のタスク

[バックアップ履歴の表示 \(402 ページ\)](#)

バックアップ履歴の表示

バックアップ履歴を参照するには、次の手順を実行します。

手順

- ステップ1** ディザスタリカバリシステムから、[バックアップ (Backup)] > [履歴 (History)] の順に選択します。
- ステップ2** [バックアップ履歴 (Backup History)] ウィンドウで、ファイル名、バックアップデバイス、完了日、結果、バージョン、バックアップされている機能、失敗した機能など、実行したバックアップを表示できます。
- (注) [バックアップ履歴 (Backup History)] ウィンドウには、最新の20個のバックアップジョブだけが表示されます。

バックアップの連携動作と制限事項

バックアップの制約事項

バックアップには、次の制約事項が適用されます。

表 39: バックアップの制約事項

制約事項	説明
クラスタセキュリティパスワード	<p>クラスタセキュリティパスワードを変更したら、必ずバックアップを実行することを推奨します。</p> <p>バックアップ暗号化では、バックアップファイルのデータを暗号化する際にクラスタセキュリティパスワードを使用します。バックアップファイルの作成後にクラスタセキュリティパスワードを編集すると、古いパスワードを忘れてしまった場合に、そのバックアップファイルを使用してデータを復元できなくなります。</p>

制約事項	説明
証明書の管理	ディザスタリカバリシステム (DRS) は、マスターエージェントとローカルエージェントとの間で SSL ベースの通信を使用して、Cisco Unified Communications Manager クラスタ ノード間のデータの認証および暗号化を行います。DRS は、IPSec 証明書を使用して、公開キー/秘密キーの暗号化を行います。証明書管理ページから IPSEC 信頼ストア (hostname.pem) ファイルを削除すると、DRS が想定どおりに機能しなくなることに注意してください。IPSEC 信頼ファイルを手動で削除するときは、IPSEC 証明書を IPSEC 信頼に必ずアップロードしてください。詳細については、 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『 <i>Security Guide for Cisco Unified Communications Manager</i> 』の「証明書管理」の項を参照してください。

リモートバックアップ用 SFTP サーバ

データをネットワーク上のリモート デバイスにバックアップするには、SFTP サーバを用意して必要な設定を行う必要があります。内部テストでは、シスコが提供し、Cisco TAC がサポートしている Cisco Prime Collaboration Deployment (PCD) 上の SFTP サーバを使用します。SFTP サーバオプションの概要については、次の表を参照してください。

以下の表示に記載されている情報を参考に、システムで使用する SFTP サーバソリューションを決定してください。

表 40: SFTP サーバ情報

SFTP サーバ	情報
Cisco Prime Collaboration Deployment の SFTP サーバ	このサーバはシスコが提供およびテストした唯一の SFTP サーバであり、Cisco TAC が完全にサポートします。 バージョンの互換性は、使用している Unified Communications Manager および Cisco Prime Collaboration Deployment のバージョンに依存します。バージョン (SFTP) または Unified Communications Manager をアップグレードする前に、『 <i>Cisco Prime Collaboration Deployment Administration Guide</i> 』を参照して、互換性のあるバージョンであることを確認してください。

SFTP サーバ	情報
テクノロジー パートナーの SFTP サーバ	これらのサーバはサードパーティが提供およびテストしたものです。バージョンの互換性は、サードパーティによるテストに依存します。テクノロジーパートナーの SFTP サーバまたは Unified Communications Manager をアップグレードする場合、テクノロジーパートナーのページで、互換性のあるバージョンを確認してください。 https://marketplace.cisco.com
他のサードパーティの SFTP サーバ	これらのサーバはサードパーティが提供するものであり、Cisco TAC はこれらのサーバを正式にサポートしていません。 バージョンの互換性は、SFTP バージョンと Unified Communications Manager バージョンの互換性を確立するためのベストエフォートに基づきます。 (注) これらの製品はシスコによってテストされていないため、機能を保証することはできません。Cisco TAC はこれらの製品をサポートしていません。完全にテストされてサポートされる SFTP ソリューションとしては、Cisco Prime Collaboration Deployment またはテクノロジー パートナーの SFTP サーバを利用してください。

暗号サポート

Unified Communications Manager 11.5 の場合、Unified Communications Manager は SFTP 接続用に次の CBC および CRT 暗号を通知します。

- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr



(注) バックアップ SFTP サーバが Unified Communications Manager と通信するためにこれらの暗号のいずれかをサポートしていることを確認してください。

Unified Communications Manager 12.0 以降のリリースでは、CBC 暗号はサポートされていません。Unified Communications Manager は、次の CTR 暗号だけをサポートおよび通知します。

- aes256-ctr
- aes128-ctr
- aes192-ctr



(注) バックアップ SFTP サーバが Unified Communications Manager と通信するためにこれらの CTR 暗号のいずれかをサポートしていることを確認してください。



第 31 章

システムの復元

- [復元の概要 \(407 ページ\)](#)
- [復元的前提条件 \(408 ページ\)](#)
- [復元タスク フロー \(408 ページ\)](#)
- [データ認証 \(419 ページ\)](#)
- [アラームおよびメッセージ \(421 ページ\)](#)
- [復元の連携動作と制約事項 \(425 ページ\)](#)
- [トラブルシューティング \(426 ページ\)](#)

復元の概要

ディザスタ リカバリ システム (DRS) には、システムを復元するプロセスを実行するためのガイドとなるウィザードが用意されています。

バックアップ ファイルは暗号化されており、それらを開いてデータを復元できるのは DRS システムのみです。ディザスタ リカバリ システムには、次の機能があります。

- 復元タスクを実行するためのユーザ インターフェイス。
- 復元機能を実行するための分散システム アーキテクチャ。

マスター エージェント

クラスタの各ノードで自動的にマスター エージェント サービスが起動されますが、マスター エージェントはパブリッシャ ノード上でのみ機能します。サブスクリバノード上のマスター エージェントは、何の機能も実行しません。

ローカル エージェント

サーバには、バックアップおよび復元機能を実行するローカル エージェントが搭載されています。

マスターエージェントを含むノードをはじめ、Cisco Unified Communications Manager クラスタ内の各ノードには、バックアップおよび復元機能を実行するために独自のローカルエージェントが必要です。



(注) デフォルトでは、ローカルエージェントは IM and Presence ノードをはじめ、クラスタ内の各ノードで自動的に起動されます。

復元の前提条件

- バージョンの要件を満たしていることを確認してください。
 - すべての Cisco Unified Communications Manager クラスタ ノードは、同じバージョンの Cisco Unified Communications Manager アプリケーションを実行している必要があります。
 - すべての IM and Presence Service クラスタ ノードは、同じバージョンの IM and Presence Service アプリケーションを実行している必要があります。
 - バックアップ ファイルに保存されているバージョンが、クラスタ ノードで実行されるバージョンと同じでなければなりません。

バージョンの文字列全体が一致している必要があります。たとえば、IM and Presence データベースパブリッシャ ノードがバージョン 11.5.1.10000-1 の場合、すべての IM and Presence サブスクリバノードは 11.5.1.10000-1 であり、バックアップファイルに保存されているバージョンも 11.5.1.10000-1 でなければなりません。現在のバージョンと一致しないバックアップファイルからシステムを復元しようすると、復元は失敗します。

- サーバの IP アドレス、ホスト名、DNS 設定および導入タイプが、バックアップファイルに保存されている IP アドレス、ホスト名、DNS 設定および導入タイプと一致していることを確認します。
- バックアップを実行した後にクラスタセキュリティパスワードを変更した場合、元のパスワードの記録を記録しておきます。元のパスワードが分からなければ、復元は失敗します。

復元タスク フロー

復元プロセス中、[Cisco Unified CM の管理 (Cisco Unified Communications Manager OS Administration)] または [Cisco Unified CM IM and Presence OS の管理 (Cisco Unified IM and Presence OS Administration)] に関するタスクを実行しないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	最初のノードのみの復元 (409 ページ)	(オプション) クラスタ内の最初のパブリッシャノードだけを復元する場合は、この手順を使用します。
ステップ 2	後続クラスタ ノードの復元 (411 ページ)	(オプション) クラスタ内のサブスクライバノードを復元する場合は、この手順を使用します。
ステップ 3	パブリッシャの再構築後の1回のステップでのクラスタの復元 (413 ページ)	(オプション) パブリッシャがすでに再構築されている場合、1回のステップでクラスタ全体を復元するには、次の手順に従ってください。
ステップ 4	クラスタ全体の復元 (415 ページ)	(オプション) パブリッシャ ノードを含む、クラスタ内のすべてのノードを復元するには、この手順を使用します。主要なハード ドライブで障害またはアップグレードが発生した場合や、ハード ドライブを移行する場合には、クラスタ内のすべてのノードの再構築が必要になる場合があります。
ステップ 5	前回正常起動時の設定へのノードまたはクラスタの復元 (416 ページ)	(オプション) 前回正常起動時の設定にノードを復元する場合に限り、この手順を使用します。ハード ドライブ障害やその他のハードウェア障害の後には使用しないでください。
ステップ 6	ノードの再起動 (417 ページ)	ノードを再起動するには、この手順を使用します。
ステップ 7	復元ジョブステータスのチェック (418 ページ)	(オプション) 復元ジョブ ステータスを確認するには、この手順を使用します。
ステップ 8	復元履歴の表示 (418 ページ)	(オプション) 復元履歴を表示するには、この手順を使用します。

最初のノードのみの復元

再構築後に最初のノードを復元する場合は、バックアップ デバイスを設定する必要があります。

この手順は、Cisco Unified Communications Manager の最初のノード（パブリッシャ ノードとも呼ばれます）に対して実行できます。その他の Cisco Unified Communications Manager ノードおよびすべての IM and Presence サービス ノードは、セカンダリ ノードまたはサブスクリバと見なされます。

始める前に

クラスタ内に IM and Presence サービス ノードがある場合は、最初のノードを復元するときに、ノードが実行されており、アクセス可能であることを確認してください。これは、この手順の実行中に有効なバックアップ ファイルを見つけるために必須です。

手順

-
- ステップ 1** ディザスタ リカバリ システムから、**[復元 (Restore)] > [復元ウィザード (Restore Wizard)]** を選択します。
- ステップ 2** **[復元ウィザード ステップ 1 (Restore Wizard Step 1)]** ウィンドウの **[バックアップ デバイスの選択 (Select Backup Device)]** 領域で、復元する適切なバックアップ デバイスを選択します。
- ステップ 3** **[次へ (Next)]** をクリックします。
- ステップ 4** **[復元ウィザード ステップ 2 (Restore Wizard Step 2)]** ウィンドウで、復元するバックアップ ファイルを選択します。
- (注) バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。
- ステップ 5** **[次へ (Next)]** をクリックします。
- ステップ 6** **[復元ウィザード ステップ 3 (Restore Wizard Step 3)]** ウィンドウで、**[次へ (Next)]** をクリックします。
- ステップ 7** 復元する機能を選択します。
- (注) バックアップ対象として選択した機能が表示されます。
- ステップ 8** 復元するノードを選択します。
- ステップ 9** **[復元 (Restore)]** をクリックして、データを復元します。
- ステップ 10** **[次へ (Next)]** をクリックします。
- ステップ 11** 復元するノードの選択を求められたら、最初のノード（パブリッシャ）だけを選択します。
- 注意** このときに後続（サブスクリバ）ノードは選択しないでください。復元を試みても失敗します。
- ステップ 12** （オプション）**[サーバ名の選択 (Select Server Name)]** ドロップダウンリストから、パブリッシャデータベース復元のサブスクリバノードを選択します。選択したサブスクリバノードが稼働しており、クラスタに接続されていることを確認してください。ディザスタ リカバリ システムでバックアップ ファイルのすべてのデータベース以外の情報が復元され、選択した後続ノードから最新のデータベースが取り出されます。

(注) このオプションは、選択したバックアップファイルにCCMDBデータベースコンポーネントが含まれている場合にのみ表示されます。まず、パブリッシャノードだけが完全に復元されますが、ステップ14を実行し、後続のクラスタノードを再起動すると、ディザスタリカバリシステムはデータベースレプリケーションを実行し、完全にすべてのクラスタノードのデータベースが同期されます。これにより、すべてのクラスタノードに最新のデータを使用していることが保障されます。

ステップ13 [復元 (Restore)] をクリックします。

ステップ14 パブリッシャノードにデータが復元されます。復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

(注) 最初のノードを復元すると、Cisco Unified Communications Manager データベース全体がクラスタに復元されます。そのため、復元しているノードの数とデータベースのサイズによっては、数時間かかることがあります。復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

ステップ15 [復元ステータス (Restore Status)] ウィンドウの [完了率 (Percentage Complete)] フィールドに100%と表示されたら、サーバを再起動します。クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

(注) Cisco Unified Communications Manager ノードだけを復元する場合は、Cisco Unified Communications Manager and IM and Presence Service サービスクラスタを再起動する必要があります。

IM and Presence サービスのパブリッシャノードのみを復元する場合は、IM and Presence サービスクラスタを再起動する必要があります。

次のタスク

- (オプション) 復元のステータスを表示するには、次を参照してください。 [復元ジョブステータスのチェック \(418 ページ\)](#)
- ノードを再起動するには、次を参照してください： [ノードの再起動 \(417 ページ\)](#)

後続クラスタノードの復元

この手順は、Cisco Unified Communications Manager のサブスクリバ (後続) ノードにのみ適用されます。インストールされる最初の Cisco Unified Communications Manager ノードはパブリッシャノードです。その他すべての Cisco Unified Communications Manager ノードおよびすべての IM and Presence サービス ノードはサブスクリバノードです。

クラスタ内の1つ以上の Cisco Unified Communications Manager サブスクリバノードを復元するには、次の手順に従います。

始める前に

復元操作を実行する場合は事前に、復元のホスト名、IP アドレス、DNS 設定、および配置タイプが、復元するバックアップファイルのホスト名、IP アドレス、DNS 設定、および配置タイプに一致することを確認します。ディザスタリカバリシステムでは、ホスト名、IP アドレス、DNS 設定、および配置タイプが異なると復元が行われません。

サーバにインストールされているソフトウェアのバージョンが復元するバックアップファイルのバージョンに一致することを確認します。ディザスタリカバリシステムは、一致するソフトウェアバージョンのみを復元操作でサポートします。再構築後に後続ノードを復元している場合は、バックアップデバイスを設定する必要があります。

手順

-
- ステップ 1** ディザスタリカバリシステムから、**[復元 (Restore)] > [復元ウィザード (Restore Wizard)]** を選択します。
- ステップ 2** **[復元ウィザード ステップ 1 (Restore Wizard Step 1)]** ウィンドウの **[バックアップ デバイスの選択 (Select Backup Device)]** 領域で、復元するバックアップ デバイスを選択します。
- ステップ 3** **[次へ (Next)]** をクリックします。
- ステップ 4** **[復元ウィザード ステップ 2 (Restore Wizard Step 2)]** ウィンドウで、復元するバックアップファイルを選択します。
- ステップ 5** **[次へ (Next)]** をクリックします。
- ステップ 6** **[復元ウィザード ステップ 3 (Restore Wizard Step 3)]** ウィンドウで、復元する機能を選択します。
- (注) 選択したファイルにバックアップされた機能だけが表示されます。
- ステップ 7** **[次へ (Next)]** をクリックします。**[復元ウィザード ステップ 4 (Restore Wizard Step 4)]** ウィンドウが表示されます。
- ステップ 8** **[復元ウィザード ステップ 4 (Restore Wizard Step 4)]** ウィンドウで、復元するノードを選択するよう求められたら、後続ノードのみを選択します。
- ステップ 9** **[復元 (Restore)]** をクリックします。
- ステップ 10** 後続ノードにデータが復元されます。復元ステータスの確認方法については、「次の作業」の項を参照してください。
- (注) 復元プロセス中、**[Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)]** または **[ユーザ オプション (User Options)]** に関するタスクを実行しないでください。
- ステップ 11** **[復元ステータス (Restore Status)]** ウィンドウの **[完了率 (Percentage Complete)]** フィールドに 100% と表示されたら、復元した 2 次サーバを再起動します。クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

- (注) 最初の IM and Presence サービス ノードが復元されたら、IM and Presence サービスの後続ノードを再起動する前に、必ず最初の IM and Presence サービス ノードを再起動してください。

次のタスク

- (オプション) 復元のステータスを表示するには、次を参照してください。 [復元ジョブステータスのチェック \(418 ページ\)](#)
- ノードを再起動するには、次を参照してください: [ノードの再起動 \(417 ページ\)](#)

パブリッシャの再構築後の1回のステップでのクラスタの復元

復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。パブリッシャがすでに再構築されている場合、または新しくインストールされた場合に、1回のステップでクラスタ全体を復元する場合は、次の手順に従います。

手順

- ステップ 1** ディザスタリカバリ システムから、**[復元 (Restore)] > [復元ウィザード (Restore Wizard)]** を選択します。
- ステップ 2** [復元ウィザード ステップ 1 (Restore Wizard Step 1)] ウィンドウの [バックアップデバイスの選択 (Select Backup Device)] 領域で、復元するバックアップ デバイスを選択します。
- ステップ 3** [次へ (Next)] をクリックします。
- ステップ 4** [復元ウィザード ステップ 2 (Restore Wizard Step 2)] ウィンドウで、復元するバックアップ ファイルを選択します。
- バックアップファイル名から、バックアップファイルが作成された日付と時刻がわかります。クラスタ全体を復元するクラスタのバックアップ ファイルだけを選択します。
- ステップ 5** [次へ (Next)] をクリックします。
- ステップ 6** [復元ウィザード ステップ 3 (Restore Wizard Step 3)] ウィンドウで、復元する機能を選択します。
- 画面には、復元する機能のうち、バックアップ ファイルに保存された機能のみが表示されます。
- ステップ 7** [次へ (Next)] をクリックします。
- ステップ 8** [復元ウィザード ステップ 4 (Restore Wizard Step 4)] ウィンドウで、[1 ステップでの復元 (One-Step Restore)] をクリックします。

このオプションは、復元用に選択されたバックアップファイルがクラスタのバックアップファイルであり、復元用に選択された機能に、パブリッシャとサブスクライバの両方のノードに登

録された機能が含まれている場合にのみ [復元ウィザード ステップ 4 (Restore Wizard Step 4)] ウィンドウに表示されます。詳細については、[最初のノードのみの復元 \(409 ページ\)](#) および [後続クラスタ ノードの復元 \(411 ページ\)](#) を参照してください。

(注) 「パブリッシャがクラスタ対応になりませんでした。1 ステップでの復元を開始できません (*Publisher has failed to become cluster aware. Cannot start one-step restore*) 」というステータス メッセージが表示されたら、パブリッシャ ノードを復元してからサブスクリバノードを復元する必要があります。詳細については、「関連項目」を参照してください。

このオプションでは、パブリッシャがクラスタ対応になり、そのためには5分かかります。このオプションをクリックすると、ステータスメッセージに「「パブリッシャがクラスタ対応になるまで5分間待機してください。この期間にバックアップまたは復元処理を開始しないでください。(Please wait for 5 minutes until Publisher becomes cluster aware and do not start any backup or restore activity in this time period.) 」」と表示されます。

この待ち時間の経過後に、パブリッシャがクラスタ対応になると、「「パブリッシャがクラスタ対応になりました。サーバを選択し、[復元 (Restore)] をクリックしてクラスタ全体の復元を開始してください (Publisher has become cluster aware. Please select the servers and click on Restore to start the restore of entire cluster) 」」というステータスメッセージが表示されます。

この待ち時間の経過後、パブリッシャがクラスタ対応にならない場合、「パブリッシャがクラスタ対応にならなかったため、1 ステップでの復元を開始できません。通常の2ステップでの復元を実行してください。(Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore.) 」というステータス メッセージが表示されます。クラスタ全体を2ステップ (パブリッシャとサブスクリバ) で復元するには、[最初のノードのみの復元 \(409 ページ\)](#) と [後続クラスタ ノードの復元 \(411 ページ\)](#) で説明する手順を実行してください。

ステップ 9 復元するノードの選択を求められたら、クラスタ内のすべてのノードを選択します。

最初のノードを復元すると、ディザスタ リカバリ システムが自動的に後続ノードに Cisco Unified Communications Manager データベース (CCMDB) を復元します。そのため、復元しているノードの数とデータベースのサイズによっては、数時間かかることがあります。

ステップ 10 [復元 (Restore)] をクリックします。

クラスタ内のすべてのノードでデータが復元されます。

ステップ 11 [復元ステータス (Restore Status)] ウィンドウの [完了率 (Percentage Complete)] フィールドに 100% と表示されたら、サーバを再起動します。クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

次のタスク

- (オプション) 復元のステータスを表示するには、次を参照してください。 [復元ジョブステータスのチェック \(418 ページ\)](#)
- ノードを再起動するには、次を参照してください： [ノードの再起動 \(417 ページ\)](#)

関連トピック

- [最初のノードのみの復元 \(409 ページ\)](#)
- [後続クラスタ ノードの復元 \(411 ページ\)](#)

クラスタ全体の復元

主要なハード ドライブで障害またはアップグレードが発生した場合や、ハード ドライブを移行する場合には、クラスタ内のすべてのノードの再構築が必要です。クラスタ全体を復元するには、次の手順を実行します。

ネットワーク カードの交換やメモリの増設など他のほとんどのハードウェア アップグレードでは、次の手順を実行する必要はありません。

手順

-
- ステップ 1** ディザスタ リカバリ システムから、**[復元 (Restore)] > [復元ウィザード (Restore Wizard)]** を選択します。
 - ステップ 2** **[バックアップ デバイスの選択 (Select Backup Device)]** エリアで、復元する適切なバックアップ デバイスを選択します。
 - ステップ 3** **[次へ (Next)]** をクリックします。
 - ステップ 4** **[復元ウィザード ステップ 2 (Restore Wizard Step 2)]** ウィンドウで、復元するバックアップ ファイルを選択します。

(注) バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。
 - ステップ 5** **[次へ (Next)]** をクリックします。
 - ステップ 6** **[復元ウィザード ステップ 3 (Restore Wizard Step 3)]** ウィンドウで、**[次へ (Next)]** をクリックします。
 - ステップ 7** **[復元ウィザード ステップ 4 (Restore Wizard Step 4)]** ウィンドウで復元ノードの選択を求められたら、すべてのノードを選択します。
 - ステップ 8** **[復元 (Restore)]** をクリックして、データを復元します。

最初のノードを復元すると、ディザスタ リカバリ システムが自動的に後続ノードに Cisco Unified Communications Manager データベース (CCMDB) を復元します。そのため、ノードの数とデータベースのサイズによっては、最大数時間かかることがあります。

すべてのノードでデータが復元されます。

(注) 復元プロセス中、[Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] または [ユーザ オプション (User Options)] に関するタスクを実行しないでください。

復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

ステップ 9 復元プロセスが完了したら、サーバを再起動します。サーバの再起動方法の詳細については、「次の作業」セクションを参照してください。

(注) 必ず最初のノードを再起動してから、後続ノードを再起動してください。

最初のノードが再起動し、Cisco Unified Communications Manager の復元後のバージョンが実行されたら、後続ノードを再起動します。

ステップ 10 レプリケーションはクラスタのリブート後に自動的に設定されます。『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の説明に従って「`utils dbreplication runtimestate`」CLI コマンドを使用して、すべてのノードで [レプリケーション ステータス (Replication Status)] の値を確認します。各ノードの値は 2 になっているはずです。

(注) クラスタのサイズによっては、後続ノードの再起動後に、後続ノードでのデータベース レプリケーションが完了するまでに時間がかかる場合があります。

ヒント レプリケーションが正しくセットアップされない場合は、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の説明に従って「`utils dbreplication rebuild`」CLI コマンドを使用します。

次のタスク

- (オプション) 復元のステータスを表示するには、次を参照してください。 [復元ジョブステータスのチェック \(418 ページ\)](#)
- ノードを再起動するには、次を参照してください： [ノードの再起動 \(417 ページ\)](#)

前回正常起動時の設定へのノードまたはクラスタの復元

前回正常起動時の設定にノードまたはクラスタを復元するには、次の手順に従います。

始める前に

- 復元ファイルに、バックアップ ファイルで設定されているホスト名、IP アドレス、DNS 設定、および配置タイプが含まれていることを確認します。
- サーバにインストールされている Cisco Unified Communications Manager のバージョンが復元するバックアップ ファイルのバージョンに一致することを確認します。
- この手順は、前回正常起動時の設定にノードを復元する場合にのみ使用してください。

手順

- ステップ 1 ディザスタリカバリ システムから、**[復元 (Restore)] > [復元ウィザード (Restore Wizard)]** を選択します。
- ステップ 2 **[バックアップ デバイスの選択 (Select Backup Device)]** エリアで、復元する適切なバックアップ デバイスを選択します。
- ステップ 3 **[次へ (Next)]** をクリックします。
- ステップ 4 **[復元ウィザード ステップ 2 (Restore Wizard Step 2)]** ウィンドウで、復元するバックアップ ファイルを選択します。

(注) バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。
- ステップ 5 **[次へ (Next)]** をクリックします。
- ステップ 6 **[復元ウィザード ステップ 3 (Restore Wizard Step 3)]** ウィンドウで、**[次へ (Next)]** をクリックします。
- ステップ 7 復元ノードを選択するように求められたら、該当するノードを選択します。選択したノードにデータが復元されます。
- ステップ 8 クラスタ内のすべてのノードを再起動します。後続の Cisco Unified Communications Manager ノードを再起動する前に、最初の Cisco Unified Communications Manager ノードを再起動します。クラスタに Cisco IM and Presence ノードもある場合は、最初の Cisco IM and Presence ノードを再起動してから、後続の IM and Presence ノードを再起動します。詳細については、「次の作業」の項を参照してください。

ノードの再起動

データを復元したら、ノードを再起動する必要があります。

パブリッシャ ノード (最初のノード) を復元したら、最初にパブリッシャ ノードを再起動する必要があります。サブスクライバ ノードは必ず、パブリッシャ ノードが再起動し、ソフトウェアの復元されたバージョンを正常に実行し始めた後で再起動してください。



- (注) CUCM パブリッシャ ノードがオフラインの場合は、IM and Presence サブスクライバ ノードを再起動しないでください。このような場合は、サブスクライバ ノードが CUCM パブリッシャ に接続できないため、ノード サービスの開始に失敗します。



注意 この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

再起動する必要があるクラスタ内のすべてのノードでこの手順を実行します。

手順

-
- ステップ 1** [Cisco Unified OS の管理 (Cisco Unified OS Administration)] から、[設定 (Settings)] > [バージョン (Version)] を選択します。
- ステップ 2** ノードを再起動するには、[再起動 (Restart)] をクリックします。
- ステップ 3** レプリケーションはクラスタのリブート後に自動的に設定されます。 **utils dbreplication runcurrentstate** CLI コマンドを使用して、すべてのノードで [レプリケーション ステータス (Replication Status)] 値を確認します。各ノードの値は 2 になっているはずですが、CLI コマンドの詳細については、『[Cisco Unified Communications \(CallManager\) Command References](#)』をしてください。CLI コマンドに関する情報は、後述の「関連項目」の項を参照してください。
- レプリケーションが正しくセットアップされない場合は、『*Command Line Reference Guide for Cisco Unified Communications Solutions*』の説明に従って **utils dbreplication reset** CLI コマンドを使用します。CLI コマンドに関する情報は、後述の「関連項目」の項を参照してください。
- (注) クラスタのサイズによっては、後続ノードの再起動後に、後続ノードでのデータベースレプリケーションが完了するまでに数時間かかる場合があります。
-

次のタスク

(オプション) 復元のステータスを表示するには、[復元ジョブステータスのチェック \(418 ページ\)](#) を参照してください。

関連トピック

『[Cisco Unified Communications Manager \(CallManager\) Command References](#)』

復元ジョブステータスのチェック

次の手順に従って、復元ジョブステータスをチェックします。

手順

-
- ステップ 1** ディザスタ リカバリ システムで、[復元 (Restore)] > [現在のステータス (Current Status)] を選択します。
- ステップ 2** [復元ステータス (Restore Status)] ウィンドウで、ログファイル名のリンクをクリックし、復元ステータスを表示します。
-

復元履歴の表示

復元履歴を参照するには、次の手順を実行します。

手順

-
- ステップ 1** [Disaster Recovery System] で、[復元 (Restore)] > [履歴 (History)] を選択します。
- ステップ 2** [復元履歴 (Restore History)] ウィンドウで、ファイル名、バックアップデバイス、完了日、結果、バージョン、復元された機能、失敗した機能など、実行した復元を表示できます。
- [復元履歴 (Restore History)] ウィンドウには、最新の 20 個の復元ジョブだけが表示されます。
-

データ認証

トレース ファイル

トラブルシューティングを行う際、またはログの収集中には、トレースファイルの保存先として次の場所が使用されます。

マスター エージェント、GUI、各ローカル エージェント、および JSch ライブラリのトレースファイルは次の場所書き込まれます。

- マスター エージェントの場合、トレース ファイルは platform/drf/trace/drfMA0* にあります。
- 各ローカル エージェントの場合、トレース ファイルは platform/drf/trace/drfLA0* にあります。
- GUI の場合、トレース ファイルは platform/drf/trace/drfConfLib0* にあります。
- JSch の場合、トレース ファイルは platform/drf/trace/drfJSch* にあります。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』（<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html>）を参照してください。

コマンドライン インターフェイス

ディザスタ リカバリ システムでは、次の表に示すように、バックアップおよび復元機能のサブセットにコマンドラインからアクセスできます。これらのコマンドの内容とコマンドライン インターフェイスの使用法の詳細については、『*Command Line Interface (CLI) Reference Guide for Cisco Unified Presence*』（<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html>）を参照してください。

表 41: ディザスタリカバリシステムのコマンドラインインターフェイス

コマンド	説明
utils disaster_recovery estimate_tar_size	SFTP/Local デバイスからのバックアップ tar の概算サイズを表示し、機能リストのパラメータを 1 つ要求します。
utils disaster_recovery backup	ディザスタリカバリシステムのインターフェイスに設定されている機能を使用して、手動バックアップを開始します。
utils disaster_recovery jschLogs	JSch ライブラリのロギングを有効または無効にします。
utils disaster_recovery restore	復元を開始します。復元するバックアップ場所、ファイル名、機能、およびノードを指定するためのパラメータが必要です。
utils disaster_recovery status	進行中のバックアップジョブまたは復元ジョブのステータスを表示します。
utils disaster_recovery show_backupfiles	既存のバックアップファイルを表示します。
utils disaster_recovery cancel_backup	進行中のバックアップジョブをキャンセルします。
utils disaster_recovery show_registration	現在設定されている登録を表示します。
utils disaster_recovery device add	ネットワーク デバイスを追加します。
utils disaster_recovery device delete	デバイスを削除します。
utils disaster_recovery device list	すべてのデバイスを一覧表示します。
utils disaster_recovery schedule add	スケジュールを追加します。
utils disaster_recovery schedule delete	スケジュールを削除します。
utils disaster_recovery schedule disable	スケジュールを無効にします。
utils disaster_recovery schedule enable	スケジュールを有効にします。
utils disaster_recovery schedule list	すべてのスケジュールを一覧表示します。
utils disaster_recovery backup	ディザスタリカバリシステムのインターフェイスに設定されている機能を使用して、手動バックアップを開始します。

コマンド	説明
utils disaster_recovery restore	復元を開始します。復元するバックアップ場所、ファイル名、機能、およびノードを指定するためのパラメータが必要です。
utils disaster_recovery status	進行中のバックアップジョブまたは復元ジョブのステータスを表示します。
utils disaster_recovery show_backupfiles	既存のバックアップファイルを表示します。
utils disaster_recovery cancel_backup	進行中のバックアップジョブをキャンセルします。
utils disaster_recovery show_registration	現在設定されている登録を表示します。

アラームおよびメッセージ

アラームおよびメッセージ

ディザスタリカバリシステムは、バックアップまたは復元手順の実行時に発生するさまざまなエラーのアラームを発行します。次の表に、ディザスタリカバリシステムのアラームの一覧を記載します。

表 42: ディザスタリカバリシステムのアラームとメッセージ

アラーム名	説明	説明
DRFBackupDeviceError	DRF バックアッププロセスでデバイスへのアクセスに関する問題が発生しています。	DRS バックアッププロセスでデバイスへのアクセス中にエラーが発生しました。
DRFBackupFailure	シスコ DRF バックアッププロセスが失敗しました。	DRS バックアッププロセスでエラーが発生しました。
DRFBackupInProgress	別のバックアップの実行中は、新規バックアップを開始できません。	DRS は、別のバックアップの実行中は新規バックアップを開始できません。
DRFInternalProcessFailure	DRF 内部プロセスでエラーが発生しました。	DRS 内部プロセスでエラーが発生しました。
DRFLA2MAFailure	DRF ローカルエージェントが、マスターエージェントに接続できません。	DRS ローカルエージェントが、マスターエージェントに接続できません。

アラーム名	説明	説明
DRFLocalAgentStartFailure	DRF ローカルエージェントが開始されません。	DRS ローカルエージェントがダウンしている可能性があります。
DRFMA2LAFailure	DRF マスターエージェントがローカルエージェントに接続できません。	DRS マスターエージェントがローカルエージェントに接続できません。
DRFMABackupComponentFailure	DRF は、少なくとも1つのコンポーネントをバックアップできません。	DRS は、コンポーネントのデータをバックアップするように要求しましたが、バックアッププロセス中にエラーが発生し、コンポーネントはバックアップされませんでした。
DRFMABackupNodeDisconnect	バックアップされるノードが、バックアップの完了前にマスターエージェントから切断されました。	DRS マスターエージェントが Cisco Unified Communications Manager ノードでバックアップ操作を実行しているときに、そのノードはバックアップ操作が完了する前に切断されました。
DRFMARestoreComponentFailure	DRF は、少なくとも1つのコンポーネントを復元できません。	DRS は、コンポーネントのデータを復元するように要求しましたが、復元プロセス中にエラーが発生し、コンポーネントは復元されませんでした。
DRFMARestoreNodeDisconnect	復元されるノードが、復元の完了前にマスターエージェントから切断されました。	DRS マスターエージェントが Cisco Unified Communications Manager ノードで復元操作を実行しているときに、そのノードは復元操作が完了する前に切断されました。
DRFMasterAgentStartFailure	DRF マスターエージェントが開始されませんでした。	DRS マスターエージェントがダウンしている可能性があります。
DRFNoRegisteredComponent	使用可能な登録済みコンポーネントがないため、バックアップが失敗しました。	使用可能な登録済みコンポーネントがないため、DRS バックアップが失敗しました。

アラーム名	説明	説明
DRFNoRegisteredFeature	バックアップする機能が選択されませんでした。	バックアップする機能が選択されませんでした。
DRFRestoreDeviceError	DRF 復元プロセスでデバイスへのアクセスに関する問題が発生しています。	DRS 復元プロセスは、デバイスから読み取ることができません。
DRFRestoreFailure	DRF 復元プロセスが失敗しました。	DRS 復元プロセスでエラーが発生しました。
DRFSftpFailure	DRF SFTP 操作でエラーが発生しています。	DRS SFTP 操作でエラーが発生しています。
DRFSecurityViolation	DRF システムが、セキュリティ違反となる可能性がある悪意のあるパターンを検出しました。	DRF ネットワーク メッセージには、コードインジェクションやディレクトリ トラバーサルなど、セキュリティ違反となる可能性がある悪意のあるパターンが含まれています。DRF ネットワーク メッセージがブロックされています。
DRFTruststoreMissing	ノードで IPsec 信頼ストアが見つかりません。	ノードで IPsec 信頼ストアが見つかりません。DRF ローカルエージェントが、マスターエージェントに接続できません。
DRFUnknownClient	パブリッシャの DRF マスターエージェントが、クラスタ外部の不明なサーバからクライアント接続要求を受け取りました。要求は拒否されました。	パブリッシャの DRF マスターエージェントが、クラスタ外部の不明なサーバからクライアント接続要求を受け取りました。要求は拒否されました。
DRFBackupCompleted	DRF バックアップが正常に完了しました。	DRF バックアップが正常に完了しました。
DRFRestoreCompleted	DRF 復元が正常に完了しました。	DRF 復元が正常に完了しました。
DRFNoBackupTaken	現在のシステムの有効なバックアップが見つかりませんでした。	アップグレード/移行または新規インストール後に、現在のシステムの有効なバックアップが見つかりませんでした。

アラーム名	説明	説明
DRFComponentRegistered	DRF により、要求されたコンポーネントが正常に登録されました。	DRF により、要求されたコンポーネントが正常に登録されました。
DRFRegistrationFailure	DRF 登録操作が失敗しました。	内部エラーが原因で、コンポーネントに対する DRF 登録操作が失敗しました。
DRFComponentDeRegistered	DRF は正常に要求されたコンポーネントの登録をキャンセルしました。	DRF は正常に要求されたコンポーネントの登録をキャンセルしました。
DRFDeRegistrationFailure	コンポーネントの DRF 登録解除リクエストが失敗しました。	コンポーネントの DRF 登録解除リクエストが失敗しました。
DRFFailure	DRF バックアップまたは復元プロセスが失敗しました。	DRF バックアップまたは復元プロセスでエラーが発生しました。
DRFRestoreInternalError	DRF 復元オペレーションでエラーが発生しました。復元は内部的にキャンセルされました。	DRF 復元オペレーションでエラーが発生しました。復元は内部的にキャンセルされました。
DRFLogDirAccessFailure	DRF は、ログディレクトリにアクセスできませんでした。	DRF は、ログディレクトリにアクセスできませんでした。
DRFDeRegisteredServer	DRF がサーバのすべてのコンポーネントを自動的に登録解除しました。	サーバが Unified Communications Manager クラスタから切断されている可能性があります。
DRFSchedulerDisabled	設定された機能がバックアップで使用できないため、DRF スケジューラは無効になっています。	設定された機能がバックアップで使用できないため、DRF スケジューラは無効になっています
DRFSchedulerUpdated	機能が登録解除されたため、DRF でスケジュールされたバックアップ設定が自動的に更新されます。	機能が登録解除されたため、DRF でスケジュールされたバックアップ設定が自動的に更新されます

復元の連携動作と制約事項

復元の制約事項

ディザスタリカバリシステムを使用して Cisco Unified Communications Manager または IM and Presence Service を復元する場合、以下の制約事項が適用されます。

表 43: 復元の制約事項

制約事項	説明
エクスポートの制限	制限されたバージョンの DRS バックアップは、制限されたバージョンにのみ復元できます。また、制限されていないバージョンのバックアップは、制限されていないバージョンにのみ復元できます。Cisco Unified Communications Manager の米国輸出無制限バージョンにアップグレードした場合、その後、このソフトウェアの米国輸出制限バージョンへのアップグレード、または新規インストールを実行できなくなります。
プラットフォームの移行	ディザスタリカバリシステムを使用してプラットフォーム間で（たとえば、Windows から Linux へ、または Linux から Windows へ）データを移行することはできません。復元は、バックアップと同じ製品バージョンで実行する必要があります。Windows ベースのプラットフォームから Linux ベースのプラットフォームへのデータ移行については、『 <i>Data Migration Assistant User Guide</i> 』を参照してください。
HW の交換と移行	DRS 復元を実行してデータを新しいサーバに移行する場合、新しいサーバに古いサーバが使用していたのと同じ IP アドレスとホスト名を割り当てる必要があります。さらに、バックアップの取得時に DNS が設定されている場合、復元を実行する前に、同じ DNS 設定がある必要があります。 サーバの交換の詳細については、『 <i>Replacing a Single Server or Cluster for Cisco Unified Communications Manager</i> 』ガイドを参照してください。 また、ハードウェアの交換後は、証明書信頼リスト (CTL) クライアントを実行する必要もあります。後続ノード (サブスクリイバ) サーバを復元しない場合には、CTL クライアントを実行する必要があります。他の場合、DRS は必要な証明書をバックアップします。詳細については、『 <i>Cisco Unified Communications Manager Security Guide</i> 』の「 <i>Installing the CTL Client</i> 」と「 <i>Configuring the CTL Client</i> 」の手順を参照してください。

制約事項	説明
クラスタ間のエクステンション モビリティ	バックアップ時にリモートクラスタにログインしていた Extension Mobility Cross Cluster ユーザは、復元後もログインしたままとなります。



(注) DRS バックアップ/復元は CPU 指向の高いプロセスです。バックアップと復元の対象となるコンポーネントの 1 つに、スマートライセンスマネージャがあります。このプロセスの間、スマートライセンス マネージャ サービスが再起動します。リソース使用率が高い場合があります。メンテナンス期間中のスケジュールを設定してください。

Cisco Unified Communications サーバ コンポーネントの復元が正常に完了した後、Cisco Unified Communications Manager を Cisco Smart Software Manager または Cisco スマートソフトウェア マネージャ サテライトに登録してください。バックアップを作成する前に製品がすでに登録されていたとしても、その製品を再登録してライセンス情報を更新する必要があります。

製品を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録する方法の詳細については、お使いのリリース向けの *Cisco Unified Communications Manager* システムコンフィギュレーションガイドを参照してください。

トラブルシューティング

より小さい仮想マシンへの DRS 復元の失敗

問題

IM and Presence サービス ノードをディスク容量がより小さい VM に復元すると、データベースの復元が失敗することがあります。

原因

大きいディスクサイズから小さいディスクサイズに移行したときに、この障害が発生します。

解決方法

2 個の仮想ディスクがある OVA テンプレートから、復元用の VM を展開します。



第 32 章

連絡先リストの一括管理

- [一括管理の概要](#) (427 ページ)
- [一括管理の前提条件](#) (427 ページ)
- [一括管理のタスクフロー](#) (428 ページ)

一括管理の概要

IM and Presence サービス一括管理ツールを使用すると、次のような多くの IM and Presence サービスユーザに対してバルクトランザクションを実行できます。

- Microsoft の移行プロセスで使用するために、ユーザ連絡先 ID の名前を変更します。
- 特定のノードまたはプレゼンス冗長グループに属するユーザの連絡先リストや非プレゼンスリスト、および場所の小足を CSV データ ファイルにエクスポートします。



(注) 非プレゼンス連絡先は、IM アドレスを持たない連絡先であり、この手順でのみエクスポートできます。

- エクスポートしたユーザ連絡先リストおよび非プレゼンス連絡先リスト、およびユーザの場所移行の詳細を、別のクラスタ内の別のノードまたはプレゼンス冗長グループにインポートできます。新規ユーザの連絡先リストを事前に設定したり、既存の連絡先リストに追加したりできます。
- これらの機能により、クラスタ間でのユーザの移行が容易になります。

一括管理の前提条件

ユーザ連絡先リストをインポートする前に：

1. Cisco Unified Communications Manager でユーザをプロビジョニングします。

2. Cisco Unified Communications Manager でユーザに IM and Presence Service のライセンスが供与されていることを確認します。



(注) デフォルトの連絡先リストのインポート速度は、仮想マシン展開のハードウェアのタイプに基づいています。[Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] > [システム (System)] > [サービス パラメータ (Service Parameters)] > [Cisco Bulk Provisioning Service] を選択して、連絡先リストのインポート レートを変更できます。ただし、デフォルトのインポート レートを大きくすると、IM and Presence Service で CPU 使用率とメモリ使用率が高くなります。

一括管理のタスクフロー

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザ連絡先 ID の一括名前変更 (429 ページ)	CSV ファイルをアップロードして、ユーザのリストの連絡先 ID の名前を変更します。
ステップ 2	非プレゼンス連絡先リストの一括エクスポート (430 ページ)	この手順を使用して、ユーザの連絡先リストを CSV ファイルにエクスポートします。その後、一括管理を使用して、ユーザ連絡先リストを別のノードまたはクラスタに移動できます。
ステップ 3	ユーザの場所の詳細の一括エクスポート (431 ページ)	ユーザの場所の詳細を CSV ファイルにエクスポートするには、次の手順を使用します。その後、一括管理を使用して、ユーザの場所の詳細リストを別のノードまたはクラスタに移動できます。
ステップ 4	次の手順を実行して、ユーザ連絡先リストを IM and Presence Service にインポートします。 <ul style="list-style-type: none"> • 連絡先リストの最大サイズの確認 (435 ページ) • 入力ファイルのアップロード (435 ページ) • 新しい一括管理ジョブの作成 (440 ページ) 	

	コマンドまたはアクション	目的
	<ul style="list-style-type: none"> 一括管理ジョブの結果の確認 (441 ページ) 	

ユーザ連絡先 ID の一括名前変更



注意 連絡先 ID の一括名前変更は、Microsoft Server (たとえば Lync) から IM and Presence サービス サービスへのユーザの移行で使用されます。このツールのユーザ移行プロセスの一部としての使用方法についての詳しい手順については、Cisco.com の『Partitioned Intradomain Federation Guide』を参照してください。それ以外の状況での、このツールの使用はサポートされません。

CSV ファイルをアップロードして、ユーザのリストの連絡先 ID の名前を変更します。

手順

- ステップ 1** すべての連絡先リスト内で名前を変更する連絡先 ID のリストを含んだ CSV ファイルをアップロードします。
- IM and Presence サービスのデータベース パブリッシャ ノードに進みます。
 - [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[一括管理 (Bulk Administration)] > [ファイルのアップロード/ダウンロード (Upload/Download Files)] を選択します。
 - [新規追加 (Add New)] をクリックします。
 - [参照 (Browse)] をクリックして CSV ファイルを見つけて選択します。入力ファイルの詳細については、[ユーザ連絡先 ID の一括名前変更 \(430 ページ\)](#) を参照してください。
 - ターゲットとして [連絡先 (Contacts)] を選択します。
 - トランザクションタイプとして [連絡先の名前変更 - カスタム ファイル (Rename Contacts - Custom File)] を選択します。
 - [保存 (Save)] をクリックし、ファイルをアップロードします。
- ステップ 2** パブリッシャ ノードの [Cisco Unified CM IM and Presence 管理 (Cisco Unified CM IM and Presence Administration)] [一括管理 (Bulk Administration)] > [連絡先リスト (Contact List)] > [連絡先の名前変更 (Rename Contacts)] を選択します。
- ステップ 3** [ファイル名 (File Name)] フィールドで、アップロードしたファイルを選択します。
- ステップ 4** 次のいずれかのアクションを選択します。
- 一括管理ジョブをただちに実行するには、[今すぐ実行 (Run Immediately)] をクリックします。
 - 一括管理ジョブを実行する時間をスケジュールするには、[後で実行 (Run Later)] をクリックします。一括管理ツールのスケジューリングジョブの詳細については、Cisco Unified CM IM and Presence Administration のオンライン ヘルプを参照してください。

ステップ 5 [送信 (Submit)] をクリックします。

ジョブをただちに実行するように選択した場合は、[送信 (Submit)] をクリックするとジョブが実行されます。

次のタスク

[非プレゼンス連絡先リストの一括エクスポート \(430 ページ\)](#)

ユーザ連絡先 ID の一括名前変更

このジョブを実行する前にアップロードするファイルは、次の形式の CSV ファイルである必要があります。

<Contact ID>, <New Contact ID>

<Contact ID> が、既存の連絡先 ID であり、<New Contact ID> が連絡先 ID の新しい形式です。

[Presence トポロジのユーザー割り当て (Presence Topology User Assignment)] ウィンドウに表示されるため、<Contact ID> がユーザの IM アドレスです。

次に、1 つのエントリを持つ CSV ファイルのサンプルを示します。

```
Contact ID, New Contact ID
john.smith@example.com, jsmith@example.com
```

非プレゼンス連絡先リストの一括エクスポート

この手順を使用して、ユーザの連絡先リストを CSV ファイルにエクスポートします。その後、一括管理を使用して、ユーザ連絡先リストを別のノードまたはクラスタに移動できます。

- 連絡先リスト：このリストは、IM and Presence の連絡先で構成されています。IM アドレスを持たない連絡先はエクスポートされません（プレゼンス以外の連絡先リストをエクスポートする必要があります）。
- 不在連絡先リスト：このリストは、IM アドレスを持たない連絡先で構成されています。

手順

ステップ 1 Cisco Unified CM の IM and Presence の管理から、次のいずれかを実行します。

- 連絡先リストをエクスポートするには、**一括管理 > 連絡先リスト > 連絡先リストのエクスポート** を選択します。
- 不在連絡先リストをエクスポートするには、**一括管理 > 不在連絡先リスト > 不在連絡先リストのエクスポート** を選択し、次のステップを飛ばしてください。

ステップ 2 担当者リストのみ。連絡先リストをエクスポートするユーザを選択します。

- a) 連絡先リストのエクスポートオプションで、連絡先リストをエクスポートするユーザのカテゴリを選択します。デフォルトでは、すべてのユーザの連絡先リストがエクスポートされます。
- b) [検索 (Find)] をクリックしてユーザのリストを表示し、[次へ (Next)] をクリックします。

ステップ 3 [ファイル名 (File Name)] フィールドに、CSV ファイルの名前を入力します。

ステップ 4 求人情報で、このジョブを実行するタイミングを設定します。

- **すぐに実行** - 連絡先リストをすぐにエクスポートするには、このボタンをオンにします。
- **[後で実行 (Run Later)]** - ジョブの時間をスケジュールしたい場合は、このボタンをチェックしてください。このオプションでは、ジョブが実行する時間をスケジュールするには、一括管理 > ジョブスケジューラ のジョブスケジューラページを使用する必要があります。

ステップ 5 [送信 (Submit)] をクリックします。

すぐに実行を選択する場合は、エクスポートジョブはすぐに実行されます。

ステップ 6 エクスポートファイルを作成したら、エクスポートしたファイルをダウンロードします。

- a) [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] から、[一括管理 (Bulk Administration)] > [ファイルのアップロード/ダウンロード (Upload/Download Files)] を選択します。
- b) 検索をクリックして、エクスポートファイルを選択します。
- c) 選択をダウンロードをクリックして、アクセス可能な場所にファイルをダウンロードします。

ユーザの場所の詳細の一括エクスポート

ユーザの場所の詳細を CSV ファイルにエクスポートするには、次の手順を使用します。その後、一括管理を使用して、ユーザの場所の詳細を別のノードまたはクラスタに移動できます。

手順

ステップ 1 Cisco Unified CM IM and Presence の管理から、[一括管理] > [ユーザの場所移行] > [ユーザの場所の詳細のエクスポート] を選択します。

ステップ 2 [ユーザの場所の詳細のエクスポート] の [ファイル名] フィールドに、CSV ファイルの名前を入力します。

ステップ 3 求人情報で、このジョブを実行するタイミングを設定します。

- **すぐに実行 (Run Immediately)** : このボタンをオンにし、ユーザの場所の詳細をすぐにエクスポートします。
- **[後で実行 (Run Later)]** - ジョブの時間をスケジュールしたい場合は、このボタンをチェックしてください。このオプションでは、ジョブが実行する時間をスケジュールするには、ジョブスケジューラページから [一括管理] > [ジョブスケジューラ] を使用する必要があります。

ステップ 4 [送信 (**Submit**)] をクリックします。

[すぐに実行 (**Run Immediately**)] を選択すると、エクスポートジョブがすぐに実行されます。

ステップ 5 エクスポートファイルを作成したら、エクスポートしたファイルをダウンロードします。

- a) [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] から、[-一括管理 (**Bulk Administration**)] > [ファイルのアップロード/ダウンロード (**Upload/Download Files**)] を選択します。
- b) 検索をクリックして、エクスポートファイルを選択します。
- c) 選択をダウンロードをクリックして、アクセス可能な場所にファイルをダウンロードします。

エクスポート連絡先リストのファイルの詳細

次に、CSV ファイル エントリのサンプルを示します。

```
userA,example.com,userB,example.com,buddyB,General,0
```

BAT を使用すると、エクスポートする連絡先リストのユーザを検索して選択できます。ユーザ連絡先リストは次の形式の CSV ファイルにエクスポートされます。

```
<User ID>,<User Domain>,<Contact ID>,<Contact Domain>,<Nickname>,<Group Name>,<State>
```

次の表で、エクスポート ファイルのパラメータについて説明します。

パラメータ	説明
[ユーザー ID (User ID)]	IM and Presence サービス ユーザのユーザー ID。 (注) この値は、ユーザの IM アドレスのユーザ部分です。
ユーザのドメイン名 (User Domain)	IM and Presence サービス ユーザのプレゼンスドメイン。 (注) この値は、ユーザの IM アドレスのドメイン部分です。 例 1 : bjones@example.com : bjones はユーザー ID、example.com はユーザドメインです。 例 2 : bjones@usa@example.com : bjones@usa はユーザー ID、example.com はユーザドメインです。
コンタクト ID (Contact ID)	連絡先リスト エントリのユーザー ID。
連絡先ドメイン (Contact Domain)	連絡先リスト エントリのプレゼンスドメイン。

パラメータ	説明
ニックネーム (Nickname)	連絡先リスト エントリのニックネーム。 ユーザが連絡先のニックネームを指定しない場合、[ニックネーム (Nickname)]パラメータは空白です。
グループ名 (Group Name)	連絡先リスト エントリが追加されるグループの名前。 ユーザの連絡先がグループに分けられていない場合、デフォルトグループ名が、[グループ名 (Group Name)]フィールドに指定されます。
状態	名簿の状態は、名簿データベースに10進形式で保存されます。

非プレゼンス連絡先リストのーファイルの詳細

非プレゼンス ユーザ連絡先リストは次の形式の CSV ファイルにエクスポートされます。

```
<User JID>,<Contact JID>,<Group Name>,<Content Type>,<Version>,<Info>
```

次の表で、エクスポート ファイルのパラメータについて説明します。

パラメータ	説明
User JID	ユーザ JID。これはユーザの IM アドレスです。
Contact JID	連絡先リスト エントリのユーザ JID (利用できる場合)。それ以外の場合は UUID。
グループ名 (Group Name)	連絡先リスト エントリが追加されるグループの名前。
コンテンツ タイプ (Content Type)	情報フィールドで使用されるテキスト MIME タイプおよびサブタイプ。
Version	情報フィールドで使用されるコンテンツ タイプ。
情報 (Info)	vCard 形式の連絡先リスト エントリの連絡先情報。

次に、CSV ファイル エントリのサンプルを示します。

```
user2@cisco.com,ce463d44-02c3-4975-a37f-d4553e3f17e1,group01,text/directory,3,BEGIN:VCARD
ADR;TYPE=WORK:ADR\;WORK:\;123 Dublin rd\,\;Oranmore\;Galway\;\;Ireland
```

```
EMAIL;TYPE=X-CUSTOM1;X LABEL=Custom:testuser01@test.com N:test;user;;; NICKNAME:pizzaguy01
ORG:ABC TEL;TYPE=WORK,VOICE:5323534535 TITLE:QA VERSION:3.0 END:VCARD
```

ユーザの場所の詳細をエクスポートするファイルの詳細

ユーザの場所の詳細は次の形式の CSV ファイルにエクスポートされます。

```
<User JID>,<Access Type>,<Create Time>,<Item ID>,<Resource ID>,<Message Text>
```



注意 ファイル自体のサイズに関する問題が発生したりユーザのロケーション情報が破損するリスクがあることから、エクスポートした CSV ファイルは手動で変更しないことを推奨します。

次の表で、エクスポート ファイルのパラメータについて説明します。

パラメータ	説明
User JID	ユーザ JID。これはユーザの IM アドレスです。
アクセス タイプ (Access Type)	<p>アクセスタイプは、ユーザのアクセスタイプを定義します。</p> <p>アクセスタイプの値は次のとおりです。</p> <ul style="list-style-type: none"> • W: ホワイトリスト • R: 名簿グループ • O: オープン <p>(注) Jabber には「W」を使用します。</p>
作成時刻	作成時間には、アイテムが作成または更新された日時が表示されます。
品目 ID	項目 ID は、ユーザの特定のレコードを識別します。
リソース ID	リソース ID は Jabber インスタンス ID です。
メッセージ テキスト (Message Text)	メッセージテキストは、ユーザのロケーション情報です。

次に、CSV ファイル エントリのサンプルを示します。

```
userA@example.com,W,2021-01-22
10:11:18.000001,7d0ec34c-458f-4fd2-9d15-58accac4af00,jabber_7151,
<geoloc
xmlns="http://jabber.org/protocol/geoloc"><description>relocation104</description><street>104</street><mobile>0</mobile><enable>1</enable></geoloc>
```

ユーザ連絡先リストの一括インポート

連絡先リストの最大サイズの確認

IM and Presence Service での、連絡先リストの最大サイズとウォッチャの最大設定を確認します。[連絡先リストの最大サイズ (Maximum Contact List Size)] のシステム デフォルト値は 200、[ウォッチャの最大数 (Maximum Watchers)] のシステム デフォルト値は 200 です。

ユーザ連絡先リストをインポート中は[連絡先リストの最大サイズ (Maximum Contact List Size)] と [ウォッチャの最大数 (Maximum Watchers)] の設定値を [無制限 (Unlimited)] に設定することを推奨します。BAT を使用して連絡先リストをインポートするときにデータを失うことなく最大連絡先リストサイズを超える場合でも、この手順により、移行された各ユーザ連絡先リストが完全にインポートされます。すべてのユーザを移行した後は、[連絡先リストの最大サイズ (Maximum Contact List Size)] と [ウォッチャの最大数 (Maximum Watchers)] の設定値を必要な値にリセットできます。

連絡先をインポートするユーザを含むクラスタについてのみ、連絡先リストの最大サイズを確認する必要があります。プレゼンス設定を変更する場合、変更はクラスタ内のすべてのノードに適用されます。したがって、クラスタ内の IM and Presence データベース パブリッシュ ノードでのみこれらの設定を変更する必要があります。

次のタスク

[入力ファイルのアップロード \(435 ページ\)](#)

入力ファイルのアップロード

次の手順では、BAT を使用して連絡先および非プレゼンス連絡先の CSV 入力ファイルをアップロードする方法について説明します。

始める前に

[連絡先リストの最大サイズの確認 \(435 ページ\)](#)

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[一括管理 (Bulk Administration)] > [ファイルのアップロード/ダウンロード (Upload/Download Files)] を選択します。

ステップ 2 [新規追加 (Add New)] をクリックします。

ステップ 3 [参照 (Browse)] をクリックして CSV ファイルを見つけて選択します。

ステップ 4 目標設定用：

- 連絡先リストの入力ファイルをアップロードする場合は、**連絡先リスト** を選択します。ユーザ連絡先リスト入力ファイルの詳細については、[連絡先リストのインポートのファイル詳細 \(436 ページ\)](#) を参照してください。

- プレゼンス以外の連絡先リストの入力ファイルをアップロードする場合は、**不在連絡先リスト**を選択します。プレゼンス以外のユーザ連絡先リスト入力ファイルの詳細については、[非プレゼンス連絡先リストのインポートのファイル詳細 \(438 ページ\)](#) を参照してください。
- ユーザの場所移行の詳細を入力ファイルとしてアップロードする場合は、**[ユーザの場所移行]**を選択します。ユーザの場所の詳細入力ファイルの詳細については、[ユーザの場所の詳細をインポートするファイルの詳細 \(439 ページ\)](#) を参照してください。

ステップ 5 取引タイプ：取引タイプとして選択します。

- 連絡先リストの入力ファイルをアップロードする場合は、**ユーザの連絡先のインポート - カスタムファイル**を選択します。
- プレゼンス以外の連絡先リストの入力ファイルをアップロードする場合は、**ユーザの不在連絡先のインポート**を選択します。
- ユーザの場所移行の詳細を入力ファイルとしてアップロードする場合は、**[ユーザの場所の詳細のインポート]**を選択します。

ステップ 6 [保存 (Save)] をクリックし、ファイルをアップロードします。

次のタスク

[新しい一括管理ジョブの作成 \(440 ページ\)](#)

連絡先リストのインポートのファイル詳細

入力ファイルは次の形式の CSV ファイルである必要があります。

```
<User ID>,<User Domain>,<Contact ID>,<Contact Domain>,<Nickname>,<Group Name>,<State>
```

次に、CSV ファイル エントリのサンプルを示します。

```
userA,example.com,userB,example.com,buddyB,General,0
```

次の表に、入力ファイルのパラメータについて説明します。

パラメータ	説明
[ユーザー ID (User ID)]	これは必須パラメータです。 IM and Presence サービス ユーザのユーザー ID。これには、最大 132 文字を使用できます。 (注) この値は、ユーザの IM アドレスのユーザ部分です。

パラメータ	説明
ユーザのドメイン名 (User Domain)	<p>これは必須パラメータです。</p> <p>IM and Presence サービス ユーザのプレゼンスドメイン。これには、最大 128 文字を使用できます。</p> <p>(注) この値は、ユーザの IM アドレスのドメイン部分です。</p> <p>例 1 : bjones@example.com : bjones はユーザー ID、example.com はユーザドメインです。</p> <p>例 2 : bjones@usa@example.com : bjones@usa はユーザー ID、example.com はユーザドメインです。</p>
コンタクト ID (Contact ID)	<p>これは必須パラメータです。</p> <p>連絡先リストエントリのユーザー ID。これには、最大 132 文字を使用できます。</p>
連絡先ドメイン (Contact Domain)	<p>これは必須パラメータです。</p> <p>連絡先リストエントリのプレゼンスドメイン。次の制限は、ドメイン名の形式に適用されます。</p> <ul style="list-style-type: none"> • 長さは 128 文字以下である必要があります • 数字、大文字と小文字、およびハイフン (-) だけ含めます • ハイフン (-) で開始または終了してはいけません • ラベルの長さは 63 文字以下である必要があります • トップレベルドメインは文字だけで、少なくとも 2 文字にする必要があります
ニックネーム (Nickname)	<p>連絡先リストエントリのニックネーム。これには、最大 255 文字を使用できます。</p>

パラメータ	説明
グループ名 (Group Name)	グループ名は必須パラメータです。 連絡先リスト エントリが追加されるグループの名前。これには、最大 255 文字を使用できます。
状態	名簿の状態は、名簿データベースに 10 進形式で保存されます。

非プレゼンス連絡先リストのインポートのファイル詳細

入力ファイルは次の形式の CSV ファイルである必要があります。

```
<User JID>,<Contact JID>,<Group Name>,<Content Type>,<Version>,<Info>
```

次に、CSV ファイル エントリのサンプルを示します。

```
user2@cisco.com,ce463d44-02c3-4975-a37f-d4553e3f17e1,group01,text/directory,3,BEGIN:VCARD
ADR;TYPE=WORK:ADR\;WORK:\;\;123 Dublin rd\,\;Oranmore\;Galway\;\;Ireland
EMAIL;TYPE=X-CUSTOM1;X LABEL=Custom:testuser01@test.com N:test;user;;; NICKNAME:pizzaguy01
ORG:ABC TEL;TYPE=WORK,VOICE:5323534535 TITLE:QA VERSION:3.0 END:VCARD
```



注意 ファイル自体のサイズに関する問題が発生したり vCard 情報が破損するリスクがあることから、CSV ファイルは手動で変更しないことを推奨します。

次の表で、非プレゼンス連絡先の入力ファイルのパラメータについて説明します。

パラメータ	説明
User JID	ユーザ JID。これはユーザの IM アドレスです。
Contact JID	連絡先リスト エントリのユーザ JID (利用できる場合)。それ以外の場合は UUID。
グループ名 (Group Name)	連絡先リスト エントリが追加されるグループの名前。
コンテンツ タイプ (Content Type)	情報フィールドで使用されるテキスト MIME タイプおよびサブタイプ。
Version	情報フィールドで使用されるコンテンツ タイプ。
情報 (Info)	vCard 形式の連絡先リスト エントリの連絡先情報。

ユーザの場所の詳細をインポートするファイルの詳細

入力ファイルは次の形式の CSV ファイルである必要があります。

```
<User JID>,<Access Type>,<Item ID>,<Create Time>,<Resource ID>,<Message Text>
```

次に、CSV ファイル エントリのサンプルを示します。

```
userA@example.com,W,7d0ec34c-458f-4fd2-9d15-58accac4af00,2021-01-22
10:11:18.000001,jabber_7151,
```

```
<geoloc
```

```
xmlns="http://jabber.org/protocol/geoloc"><description>newlocation104</description><street>104</street><mobile>0</mobile><enable>1</enable></geoloc>
```



注意

ファイル自体のサイズに関する問題が発生したりユーザのロケーション情報が破損するリスクがあることから、CSV ファイルは手動で変更しないことを推奨します。

次の表で、ユーザの場所移行の入力ファイルのパラメータについて説明します。

パラメータ	説明
User JID	これは必須パラメータです。 ユーザ JID は、ユーザの IM アドレスです。これには、最大 255 文字を使用できます。
アクセス タイプ (Access Type)	これは必須パラメータです。アクセスタイプは、ユーザのアクセスタイプを定義します。これには、最大 128 文字を使用できます。 アクセスタイプの値は次のとおりです。 <ul style="list-style-type: none"> • W: ホワイトリスト • R: 名簿グループ • O: オープン (注) Jabber には「W」を使用します。
品目 ID	これは必須パラメータです。 項目 ID は、ユーザの特定のレコードを識別します。項目 ID の値は、「無視 (Ignore)」または英数字の値にする必要があります。連絡先リスト エントリのユーザー ID。これには、最大 50 文字を使用できます。
作成時刻	これは必須パラメータです。 作成時間には、アイテムが作成または更新された日時が表示されます。これには、最大 26 文字を使用できます。

パラメータ	説明
リソースID	これは必須パラメータです。 リソース ID は Jabber インスタンス ID です。 これには、最大 1023 文字を使用できます。
メッセージテキスト (Message Text)	これは必須パラメータです。 メッセージテキストは、ユーザのロケーション情報です。これには、最大 30000 文字を使用できます。

新しい一括管理ジョブの作成

連絡先リストおよび非プレゼンス連絡先リストの新しい一括管理ジョブを作成します。

始める前に

[入力ファイルのアップロード \(435 ページ\)](#)

手順

ステップ 1 Cisco Unified CM IM and Presence の管理で：

- 連絡先リスト用の新しい一括管理ジョブを作成する場合は、**一括管理 > 連絡先リスト > 更新**を選択します。
- 連絡先リスト用の新しい一括管理ジョブを作成する場合は、**一括管理 > 不在リストへの連絡 > 不在連絡先リストのインポート**を選択します。
- ユーザの場所移行用に新しい一括管理ジョブを作成する場合は、**[一括管理] > [ユーザの場所移行] > [ユーザの場所詳細のインポート]**を選択します。

ステップ 2 [ファイル名 (File Name)] ドロップダウン リストから、インポートするファイルを選択します。

ステップ 3 [ジョブの説明 (Job Description)] フィールドに、この一括管理コミッションの説明を入力します。

ステップ 4 次のいずれかを実行します。

- 一括管理ジョブをただちに実行するには、**[今すぐ実行 (Run Immediately)]**をクリックします。
- 一括管理ジョブを実行する時間をスケジュールするには、**[後で実行 (Run Later)]**をクリックします。BAT でジョブをスケジュールする方法の詳細については、Cisco Unified CM IM and Presence の管理のオンライン ヘルプを参照してください。

ステップ 5 [送信 (Submit)] をクリックします。ジョブをただちに実行するように選択した場合は、[送信 (Submit)] をクリックするとジョブが実行されます。

次のタスク

[一括管理ジョブの結果の確認 \(441 ページ\)](#)

一括管理ジョブの結果の確認

一括管理ジョブが完了すると、IM and Presence サービス BAT ツールは、連絡先リストのインポート ジョブの結果をログ ファイルに書き込みます。ログ ファイルには、次の情報が含まれています。

- 正常にインポートされた連絡先の数。
- 連絡先をインポートしようとした際に発生した内部サーバエラーの数。
- インポートされなかった（無視された）連絡先の数。ログ ファイルには、無視されたそれぞれの連絡先の理由がログ ファイルの末尾に記載されます。次に、連絡先がインポートされない理由を示します。
 - 無効な形式：無効な行形式。たとえば、必須フィールドが見つからないか、または空になっています
 - 無効なアクセスドメイン：連絡先ドメインの形式が無効です。連絡先ドメインの有効な形式については、ユーザの連絡先リストの一括インポートに関するトピックを参照してください
 - 連絡先として自身を追加できない：連絡先がユーザの場合、そのユーザの連絡先はインポートできません
 - ユーザの連絡先リストが制限を超えている：ユーザが連絡先リストの最大サイズに達したため、これ以上の連絡先をそのユーザに対してインポートできません
 - ユーザはローカル ノードに割り当てられない：ユーザはローカル ノードに割り当てられません
- BAT ジョブを早期に終了させたエラーが原因で処理されなかった CSV ファイル内の連絡先の数。このエラーは滅多に起こりません。

このログ ファイルにアクセスするには、次の手順を実行します。

始める前に

[新しい一括管理ジョブの作成 \(440 ページ\)](#)

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[一括管理 (Bulk Administration)] > [ジョブ スケジューラ (Job Scheduler)] を選択します。

ステップ 2 [検索 (Find)] をクリックして、連絡先リストのインポート ジョブのジョブ ID を選択します。

ステップ3 [ログ ファイル名 (Log File Name)] リンクをクリックし、ログを開きます。



第 33 章

システムのトラブルシューティング

- [トラブルシューティングの概要 \(443 ページ\)](#)
- [システムトラブルシューターを実行する \(443 ページ\)](#)
- [診断の実行 \(444 ページ\)](#)
- [トラブルシューティングのためのトレースログの使用 \(446 ページ\)](#)
- [ユーザー ID エラーおよびディレクトリ URI エラーのトラブルシューティング \(455 ページ\)](#)

トラブルシューティングの概要

この章の手順を使用して、IM and Presence の展開に関する問題をトラブルシューティングします。IM and Presence サービスを導入すると、次のことが可能になります。

- コマンドラインインタフェース (CLI) を使用して、問題を解決するために確認できるトレースログを作成します。
- システムの問題を確認するための診断の実行。
- システムの正常性を確認するためのしすシステムトラブルシュータの実行。
- 重複ディレクトリ URI 問題のトラブルシューティング。

システムトラブルシューターを実行する

トラブルシューターを実行して、IM and Presence サービスの展開に関する問題を診断します。トラブルシューターは、展開に関する以下のようなさまざまな問題を自動的にチェックします：

- システムに関する問題
- 同期エージェントの問題
- プレゼンスエンジンの問題
- SIP プロキシの問題

- Microsoft RCC の問題
- カレンダーの問題
- クラスタ間の問題
- トポロジの問題
- Cisco Jabber の冗長割り当て
- 外部データベースエントリ
- [サードパーティのコンプライアンスサーバ(Third-Party Compliance Server)]
- サードパーティの LDAP 接続
- LDAP 接続 (LDAP Connection)
- XCP スタウス
- ユーザの設定

手順

-
- ステップ 1** Cisco Unified CM IM and Presence Administration から、[診断 (Diagnostics)] > [システムトラブルシュータ (System Troubleshooter)] を選択します。
 トラブルシュータは、システムに対して一連の自動チェックを実行します。結果はシステム構成のトラブルシュータウィンドウに表示されます。
- ステップ 2** トラブルシュータが強調している問題を解決してください。
-

診断の実行

稼働中のシステムを管理するとき、システムの通常の稼働に影響する問題が発生する可能性があります。IM and Presence Service 診断ツールを使用して、これらの問題の根本的な原因を特定することができます。

この手順を使用して、IM and Presence Service の診断ツールにアクセスします。

これらのツールには **Cisco Unified CM の IM and Presence の管理** から **診断** をクリックし、以下のオプションから 1 つ選択することでアクセスできます。

手順

-
- ステップ 1** Cisco Unified CM IM and Presence Administration で、[診断 (Diagnostics)] を選択します。
- ステップ 2** ドロップダウンリストから使用する診断ツールをクリックします。

これらのツールの目的の詳細については、「診断ツールの概要」を参照してください。

診断ツールの概要

診断ツール	目的
システム ダッシュボード	システムコンポーネント（デバイスの数、ユーザの数、および連絡先、プライマリ内線といったユーザごとのデータ）の概要データビューが含まれるシステムの状態のスナップショットを取得するには、システム ダッシュボードを使用します。
システム トラブルシュータの設定	<p>初期設定や設定変更の後に、IM and Presence Service 設定の問題を診断するには、システム設定トラブルシュータを使用します。</p> <p>Troubleshooter は、IM and Presence Service クラスタとその両方で一連のテストを実行します。</p> <p>Cisco Unified Communications Manager Cluster は IM and Presence Service 設定を確認します</p> <p>トラブルシュータは、テストの完了後、考えられる3つの状態のいずれかをテストごとに報告します。</p> <ul style="list-style-type: none"> • テストに合格しました。 • テストに失敗しました • [テスト警告(設定に問題がある可能性を示しています)(Test Warning (indicates possible configuration issue))] <p>不合格または警告となった各テストには、トラブルシュータから問題の説明および考えられる解決策が示されます。不合格または警告となったテストごとに、解決策の列にある [fix] リンクをクリックし、[Cisco Unified Communications Manager IM and Presence Administration] ウィンドウに移動します。このウィンドウには、設定トラブルシュータで検出された問題が表示されます。検出された設定エラーを修正して、トラブルシュータを再実行してください。</p>

診断ツール	目的
Microsoft RCC トラブルシュータ	Microsoft Remote Call Control (RCC) を使用して、初期設定後や設定変更後に IM and Presence Service と Microsoft Lync または Microsoft Office クライアントアプリケーションの間の統合で発生した問題を診断します。トラブルシュータは、Microsoft Lync、LCS または OCS サーバと IM and Presence Service の間、および Microsoft Lync または Microsoft Office クライアントと IM and Presence Service の間で発生するユーザ関連および接続関連の問題を検証します。

トラブルシューティングのためのトレースログの使用

トレースを使用して、IM and Presence のサービスと機能に関するシステムの問題をトラブルシューティングします。さまざまなサービス、機能、およびシステムコンポーネントに対して自動システムトレースを設定できます。結果はシステムログに保存され、Cisco Unified Real-Time Monitoring Tool を使用して参照および表示できます。あるいは、コマンドラインインターフェースを使用してシステムログファイルのサブセットを取得し、それらを自分の PC またはラップトップにアップロードしてさらに分析することもできます。

トレースを使用するには、最初にトレース向けにシステムを構成する必要があります。システムトレースを設定する方法の詳細については、『*Cisco Unified Serviceability Administration Guide*』の「Traces」の章を参照してください。

トレースを設定したら、次の2つの方法のいずれかを使用してトレースファイルの内容を表示できます。

- リアルタイム監視ツール - リアルタイム監視ツールを使用すると、システムトレースの結果として作成された個々のログファイルを参照および表示できます。リアルタイム監視ツールの使用の詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。
- コマンドラインインターフェイス (CLI) : システムトレースが設定されている場合は、CLI を使用してシステムログからカスタマイズされたトレースを作成します。CLI を使用すると、カスタマイズしたトレースファイルに含める特定の日を指定できます。CLI はシステムから関連付けられているトレースファイルを取り出し、それらを圧縮された zip ファイルに保存します。これを PC またはラップトップにコピーしてさらに分析することで、システムによってログが上書きされないようにします。

このセクション以降の表と作業では、IM and Presence サービスのトレースログファイルを作成するための CLI コマンドの使用方法について説明します。

トレースによる一般的な IM and Presence の問題

次の表は、IM and Presence サービスに関する一般的な問題と、問題をトラブルシューティングするために実行できるトレースの一覧です。

表 44: IM and Presence の一般的な問題とトラブルシューティング

の問題	これらのサービスのトレースを表示する	追加の指示
ログインおよび認証トレース	Client Profile Agent Cisco XCP Connection Manager Cisco XCP Router Cisco XCP Authentication Service Cisco Tomcat Security Logs	ログおよび出力場所を作成するための CLI コマンドは CLI 経由の共通トレース (449 ページ) を参照してください。
応答可否ステータス	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine	ログおよび出力場所を作成するための CLI コマンドは CLI 経由の共通トレース (449 ページ) を参照してください。
IM の送受信	Cisco XCP Connection Manager Cisco XCP Router	ログおよび出力場所を作成するための CLI コマンドは CLI 経由の共通トレース (449 ページ) を参照してください。
担当者リスト	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine	ログおよび出力場所を作成するための CLI コマンドは CLI 経由の共通トレース (449 ページ) を参照してください。
チャット ルーム	Cisco XCP Connection Manager Cisco XCP Router Cisco XCP Text Conferencing Manager	ログおよび出力場所を作成するための CLI コマンドは CLI 経由の共通トレース (449 ページ) を参照してください。
パーティションイントラドメイン フェデレーション	Cisco XCP Router Cisco XCP SIP Federation Connection Manager Cisco SIP Proxy Cisco Presence Engine	ログおよび出力場所を作成するための CLI コマンドは CLI 経由の共通トレース (449 ページ) を参照してください。 (注) Cisco SIP Proxy デバッグロギングは、SIP メッセージ交換の確認に必要です。

の問題	これらのサービスのトレースを表示する	追加の指示
XMPP ベースのドメイン間フェデレーション連絡先の可用性および IM	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine Cisco XCP XMPP Federation Connection Manager	ログおよび出力場所を作成するための CLI コマンドは CLI 経由の共通トレース (449 ページ) を参照してください。 XMPP フェデレーションが有効な各 IM and Presence ノードでトレースを実行します。
SIP ドメイン間フェデレーション連絡先の可用性および IM	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine Cisco SIP Proxy Cisco XCP SIP Federation Connection Manager	ログおよび出力場所を作成するための CLI コマンドは CLI 経由の共通トレース (449 ページ) を参照してください。
カレンダー トレース	Cisco Presence Engine	ログおよび出力場所を作成するための CLI コマンドは CLI 経由の共通トレース (449 ページ) を参照してください。
クラスタ間同期トレースおよびクラスタ間設定トラブルシュータ	Cisco Intercluster Sync Agent Cisco AXL Web Service Cisco Tomcat Security Log Cisco Syslog Agent	診断 > システムトラブルシュータ でシステムトラブルシュータを実行して、クラスタ間エラーをチェックします。
SIP フェデレーション トレース	Cisco SIP Proxy Cisco XCP Router Cisco XCP SIP Federation Connection Manager	ログおよび出力場所を作成するための CLI コマンドは CLI 経由の共通トレース (449 ページ) を参照してください。
XMPP フェデレーション トレース	Cisco XCP Router Cisco XCP XMPP Federation Connection Manager	ログおよび出力場所を作成するための CLI コマンドは CLI 経由の共通トレース (449 ページ) を参照してください。

の問題	これらのサービスのトレースを表示する	追加の指示
高 CPU と低 VM のアラートのトラブルシューティング	Cisco XCP Router Cisco XCP SIP Federation Connection Manager Cisco SIP Proxy Cisco Presence Engine Cisco Tomcat Security Log Cisco Syslog Agent	追加のトラブルシューティングを行うには、次の CLI コマンドを実行してください。 <ul style="list-style-type: none"> • <code>show process using-most cpu</code> • <code>show process using-most memory</code> • <code>utils dbreplication runtimestate</code> • <code>utils service list</code> 次の CLI を実行して RIS (リアルタイム情報サービス) データを取得します。 <ul style="list-style-type: none"> • <code>file get activelog cm/log/ris/csv</code> また、Cisco Unified IM and Presence Serviceability のアラームを設定することで、実行時のステータスとシステムの状態に関する情報をローカルシステムのログに提供できます。

CLI 経由の共通トレース

コマンドラインインタフェースを使用して、システムのトラブルシューティングを行うためのトレースログファイルを作成します。CLIを使用すると、トレースを実行するコンポーネントを選択して、<duration>を指定できます。これは、ログファイルに含める今日からの過去の日数です。

次の2つの表には、トレースログファイルの作成に使用できる CLI コマンドとログ出力先が含まれています。

- IM and Presence サービス
- IM and Presence 機能



- (注) CLI は、Cisco Unified Real-Time Monitoring Tool (RTMT) で表示できるのと同じ個々のトレースファイルのサブセットを取得しますが、それらを単一の圧縮 zip ファイルにまとめて保存します。RTMT トレースについては、[RTMT 経由の共通トレース \(454 ページ\)](#) を参照してください。

表 45: CLI を使用した IM and Presence サービスの一般的なトレース

サービス	ログを作成するための CLI	CLI 出力ファイル
シスコの監査ログ	ファイルビルドログ cisco_audit_logs < duration>	/epas/trace/log_cisco_audit_logs_*.tar.gz
Cisco Client Profile Agent	ファイルビルドログ cisco_client_profile_agent < duration>	/epas/trace/log_cisco_client_profile_agent_*.tar.gz
Cisco Cluster Manager	ファイル構築ログ cisco_config_agent<duration>	/epas/trace/log_cisco_cluster_manager_*.tar.gz
Cisco Config Agent	ファイル構築ログ cisco_config_agent<duration>	/epas/trace/log_cisco_config_agent_*.tar.gz
Cisco Database Layer Monitor	ファイル構築ログ cisco_database_layer_monitor <duration>	/epas/trace/log_cisco_database_layer_monitor_*.tar.gz
Cisco Intercluster Sync Agent	ファイル構築ログ cisco_inter_cluster_sync_agent <duration>	/epas/trace/log_cisco_inter_cluster_sync_agent_*.tar.gz
Cisco OAM Agent	ファイル構築ログ cisco_oam_agent <duration>	/epas/trace/log_cisco_oam_agent_*.gz
Cisco Presence Engine	ファイル構築ログ cisco_presence_engine <duration>	/epas/trace/log_cisco_presence_engine_*.tar.gz
Cisco RIS (リアルタイム情報サービス) データコレクタ	ファイル構築ログ cisco_ris_data_collector <duration>	/epas/trace/log_cisco_ris_data_collector_*.tar.gz
シスコのサービス管理	ファイル構築ログ cisco_service_management <duration>	/epas/trace/log_cisco_service_management_*.tar.gz
Cisco SIP Proxy	ファイル構築ログ cisco_sip_proxy <duration>	/epas/trace/log_cisco_sip_proxy_*.tar.gz

サービス	ログを作成するための CLI	CLI 出力ファイル
Cisco Sync Agent	ファイル構築ログ cisco_sync_agent <duration>	/epas/trace/log_cisco_sync_agent_*.tar.gz
Cisco XCP Config Manager	ファイル構築ログ cisco_xcp_config_mgr <duration>	/epas/trace/log_cisco_xcp_config_mgr_*.tar.gz
Cisco XCP Router	ファイル構築ログ cisco_xcp_router <duration>	/epas/trace/log_cisco_xcp_router_*.tar.gz

表 46: CLI を使用した IM and Presence 機能の一般的なトレース

機能名	ログを作成するための CLI	CLI 出力ファイル
管理 GUI	ファイル構築ログ admin_ui <duration>	/epas/trace/log_admin_ui_*.tar.gz
一括管理	ファイル構築ログ bat <duration>	/epas/trace/log_bat_*.tar.gz
Bidirectional Streams over Synchronous HTTP	ファイル構築ログ bosh <duration>	/epas/trace/log_bosh_*.tar.gz
証明書 (Certificates)	ファイル構築ログ証明書 <duration>	/epas/trace/log_certificates_*.tar.gz
設定エージェント	ファイル構築ログ cfg_agent_core <duration>	/epas/trace/log_cfg_agent_core_*.tar.gz
Customer Voice Portal	ファイル構築ログ cvp <duration>	/epas/trace/log_cvp_*.tar.gz
ディレクトリ グループ	ファイル構築ログ directory_groups <duration>	/epas/trace/log_directory_groups_*.tar.gz
ディザスタ リカバリ	ファイル構築ログ disaster_recovery <duration>	/epas/trace/log_disaster_recovery_*.tar.gz
柔軟な IM アドレス	ファイル構築ログ flexable_im_address <duration>	/epas/trace/log_flexible_im_address_*.tar.gz
一般コア	ファイル構築ログ general_core <duration>	/epas/trace/log_general_core_*.tar.gz
高可用性	ファイル構築ログ ha <duration>	/epas/trace/log_ha_*.tar.gz
高い CPU	ファイル構築ログ high_cpu <duration>	/epas/trace/log_high_cpu_*.tar.gz

CLI 経由の共通トレース

機能名	ログを作成するための CLI	CLI 出力ファイル
高いメモリ	ファイル構築ログ high_memory <duration>	/epas/trace/log_high_memory_*.tar.gz
インスタントメッセージング データベースコア	ファイル構築ログ imdb <duration>	/epas/trace/log_imdb_core_*.tar.gz
クラスタ間ピアリング	ファイル構築ログ inter_cluster <duration>	/epas/trace/log_inter_cluster_*.tar.gz
マネージド ファイル転送	ファイル構築ログ managed_file_transfer <duration>	/epas/trace/log_managed_file_transfer_*.tar.gz
Microsoft Exchange	ファイル構築ログ msft_exchange <duration>	/epas/trace/log_msft_exchange_*.tar.gz
メッセージアーカイバ	ファイル構築ログ msg_archiver <duration>	/epas/trace/log_msg_archiver_*.tar.gz
プレゼンス エンジン コア	ファイル構築ログ pe_core <duration>	/epas/trace/log_pe_core_*.tar.gz
プレゼンスと IM メッセージ 交換	ファイル構築ログ presence_im_exchange <duration>	/epas/trace/log_presence_im_exchange_*.tar.gz
SIP ログインの問題	ファイル構築ログ pws <duration>	/epas/trace/log_pws_*.tar.gz
Remote Call Control; リモート 呼制御	ファイル構築ログ remote_call_control <duration>	/epas/trace/log_remote_call_control_*.tar.gz
セキュリティの脆弱性	ファイル構築ログ sec_vulnerability <duration>	/epas/trace/log_sec_vulnerability_*.tar.gz
サービスアビリティの GUI	ファイル構築ログ serviceability_ui <duration>	/epas/trace/log_serviceability_ui_*.tar.gz
SIP ドメイン間フェデレー ション	ファイル構築ログ sip_inter_federation <duration>	/epas/trace/log_sip_inter_federation_*.tar.gz
SIP パーティションイントラ ドメイン フェデレーション	ファイル構築ログ sip_partitioned_federation <duration>	/epas/trace/log_sip_partitioned_federation_*.tar.gz
SIP プロキシコア	ファイル構築ログ sipd_core <duration>	/epas/trace/log_sipd_core_*.tar.gz
常設チャットの高可用性	ファイル構築ログ tc_ha <duration>	/epas/trace/log_tc_ha_*.tar.gz

機能名	ログを作成するための CLI	CLI 出力ファイル
常設チャット	ファイル構築ログ text_conference <duration>	/epas/trace/log_text_conference_*.tar.gz
アップグレードの問題	ファイル構築ログ upgrade_issues <duration>	/epas/trace/log_upgrade_issues_*.tar.gz
ユーザ接続	ファイル構築ログ user_connectivity <duration>	/epas/trace/log_user_connectivity_*.tar.gz
名簿	ファイル構築ログ user_rosters <duration>	/epas/trace/log_user_rosters_*.tar.gz
XCP ルーターコア	ファイル構築ログ xcp_core <duration>	/epas/trace/log_xcp_core_*.tar.gz
XMPP ドメイン間フェデレーション	ファイル構築ログ xmpp_inter_federation <duration>	/epas/trace/log_xmpp_inter_federation_*.tar.gz
展開情報	ファイル構築ログ deployment_info <duration>	/epas/trace/log_deployment_info_*.tar.gz

CLI 経由でトレースを実行する

この手順を使用して、コマンドラインインタフェース (CLI) を介してカスタマイズされたトレースファイルを作成します。CLI を使用すると、`duration` パラメータを使用して、トレースに含める過去を振り返る日数を指定できます。CLI はシステムログのサブセットを取得します。



(注) SFTP サーバは必ずファイルの転送にのみ使用してください。

始める前に

システムにトレースを設定しておく必要があります。トレースを設定する方法の詳細については、『*Cisco Unified Serviceability Administration Guide*』の「Traces」の章を参照してください。実行できるトレースのリストについては [CLI 経由の共通トレース \(449 ページ\)](#) を確認します。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 ログを作成するには、ファイル構築ログ <name of service> <duration> CLI コマンドを実行します。ここで、duration はトレースに含める日数です。

例えば、ファイル構築ログ `cisco_cluster_manager 7` は過去 1 週間の Cisco Cluster Manager ログを表示します。

ステップ 3 ログを取得するには、トレースファイルを取得するための `file get activelog <ログファイルパス>` を実行します。

例えば、ファイル取得 `activelog epas / trace / log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz`。

ステップ 4 安定したシステムを維持するために、取得した後にログを削除します。ログを削除するには `file delete activelog <ファイルパス>` コマンドを実行します。

例えば、ファイル削除 `activelog epas / trace / log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz`。

RTMT 経由の共通トレース

次の表に、IM and Presence Service ノードと結果のログ ファイルで実行できる共通トレースを示します。Real-Time Monitoring Tool (RTMT) を使用してトレースログファイルを表示できます。



(注) CLI は、RTMT で表示できるのと同じ個々のトレースファイルのサブセットを取得するのに使用できますが、それらを単一の圧縮 zip ファイルにまとめて保存します。CLI トレースについては、[CLI 経由の共通トレース \(449 ページ\)](#) を参照してください。

表 47: IM and Presence ノードに共通のトレースとログ ファイル

サービス	トレース ログのファイル名
Cisco AXL Web サービス	/tomcat/logs/axl/log4j/axl*.log
Cisco Intercluster Sync Agent	/epas/trace/cupicsa/log4j/icSyncAgent*.log
Cisco Presence Engine	/epas/trace/epe/sdi/epe*.txt.gz
Cisco SIP Proxy	/epas/trace/esp/sdi/esp*.txt.gz
Cisco Syslog Agent	/cm/trace/syslogmib/sdi/syslogmib*.txt
Cisco Tomcat Security Log	/tomcat/logs/security/log4/security*.log
Cisco XCP Authentication Service	/epas/trace/xcp/log/auth-svc-1*.log.gz
Cisco XCP Config Manager	/epas/trace/xcpconfigmgr/log4j/xcpconfigmgr*.log

サービス	トレース ログのファイル名
Cisco XCP Connection Manager	/epas/trace/xcp/log/client-cm-1*.log.gz
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-1*.log.gz
Cisco XCP SIP Federation Connection Manager	/epas/trace/xcp/log/sip-cm-3*.log
Cisco XCP Text Conferencing Manager	/epas/trace/xcp/log/txt-conf-1*.log.gz
Cisco XCP XMPP Federation Connection Manager	/epas/trace/xcp/log/xmpp-cm-4*.log
Cluster Manager	/platform/log/clustermgr*.log
Cisco Client Profile Agent (CPA)	/tomcat/logs/epassoap/log4j/EPASSoap*.log
dbmon	/cm/trace/dbl/sdi/dbmon*.txt

ユーザー ID エラーおよびディレクトリ URI エラーのトラブルシューティング

重複したユーザー ID エラーの受信

問題 ユーザー ID が重複していることを示すアラームを受信しました。これらのユーザの連絡先情報を修正しなければなりません。

解決法 次のステップを実行します。

1. **utils users validate { all | userid | uri }** CLI コマンドを使用して全ユーザのリストを生成します。CLI の使用の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

ユーザー ID に続いて重複したユーザー ID の元となっているサーバのリストが、結果セットに表示されます。次の CLI 出力の例は、出力時のユーザー ID エラーを示しています。

```
Users with Duplicate User IDs
-----
User ID: user3
Node Name
cucm-imp-1
cucm-imp-2
```

2. 同じユーザが 2 台の別のクラスタに割り当てられている場合、いずれかのクラスタからそのユーザの割り当てを解除します。

3. 別のクラスターで異なるユーザに同じユーザー ID が割り当てられている場合、いずれかのユーザに対しユーザー ID 値の名前を変更して、重複がないようにします。
4. ユーザ情報が無効または空白の場合、Cisco Unified Communications Manager Administration の GUI を使用して、そのユーザのユーザー ID 情報を修正します。
5. Cisco Unified Communications Manager 内のユーザ レコードを修正できます。[エンドユーザの設定 (End User Configuration)] ウィンドウ ([ユーザの管理 (User Management)] > [エンドユーザ (EndUser)]) を使用することで、必要に応じて、全ユーザに有効なユーザー ID またはディレクトリ URI 値を確実に設定します。詳細については、『Cisco Unified Communications Manager Administration Guide』を参照してください。



(注) ユーザプロフィールでのユーザー ID とディレクトリ URI フィールドは、LDAP Directory にマップされる場合があります。この場合は、LDAP Directory サーバで修正を行います。

6. 重複したユーザー ID エラーがそれ以上ないことを確認するには、CLI コマンドをもう一度実行してユーザを検証します。

重複または無効なディレクトリ URI エラーの受信

問題 ユーザディレクトリ URI が重複または無効であることを示すアラームを受信しました。これらのユーザの連絡先情報を修正しなければなりません。

解決法 次のステップを実行します。

1. **utils users validate { all | userid | uri }** CLI コマンドを使用して全ユーザのリストを生成します。CLI の使用の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

ディレクトリ URI の値、続いて重複または無効なディレクトリ URI の元となっているサーバのリストが、結果セットに表示されます。次の CLI 出力の例は、検証チェック時に検出されたディレクトリ URI エラーを示しています。

```
Users with No Directory URI Configured
-----
Node Name: cucm-imp-2
User ID
user4

Users with Invalid Directory URI Configured
-----
Node Name: cucm-imp-2
User ID   Directory URI
user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
-----
Directory URI: user1@cisco.com
Node Name   User ID
cucm-imp-1  user4
cucm-imp-2  user3
```


2. 同じユーザが 2 台の別のクラスタに割り当てられている場合、いずれかのクラスタからそのユーザの割り当てを解除します。
3. 別のクラスタで異なるユーザに同じディレクトリ URI が割り当てられている場合、いずれかのユーザに対しディレクトリ URI 値の名前を変更して、重複がないようにします。
4. ユーザ情報が無効または空白の場合、ユーザのディレクトリ URI 情報を修正します。
5. Cisco Unified Communications Manager 内のユーザ レコードを修正できます。[エンド ユーザの設定 (End User Configuration)] ウィンドウ ([ユーザの管理 (User Management)] > [エンド ユーザ (EndUser)]) を使用することで、必要に応じて、全ユーザに有効なユーザ ID またはディレクトリ URI 値を確実に設定します。詳細については、『Cisco Unified Communications Manager Administration Guide』を参照してください。



(注) ユーザ プロファイルでのユーザー ID とディレクトリ URI フィールドは、LDAP Directory にマップされる場合があります。この場合は、LDAP Directory サーバで修正を行います。

6. 重複または無効なディレクトリ URI エラーがそれ以上ないことを確認するには、CLI コマンドをもう一度実行してユーザを検証します。



第 **V** 部

参考情報

- [Cisco Unified Communications Manager](#) での TCP および UDP ポートの使用 (461 ページ)
- [IM and Presence](#) サービスのポートの使用情報 (485 ページ)
- [追加の要件](#) (505 ページ)



第 34 章

Cisco Unified Communications Manager での TCP および UDP ポートの使用

この章では、Cisco Unified Communications Manager がクラスター内接続および外部アプリケーションまたはデバイスとの通信に使用する TCP ポートと UDP ポートの一覧を示します。また、IP Communications ソリューションの実装時に、ネットワークにファイアウォール、アクセスコントロールリスト（ACL）、および Quality of Service（QoS）を設定するために重要な情報も記載されています。

- [Cisco Unified Communications Manager の TCP と UDP ポートの使用に関する概要（461 ページ）](#)
- [ポート説明（463 ページ）](#)
- [ポート参照（482 ページ）](#)

Cisco Unified Communications Manager の TCP と UDP ポートの使用に関する概要

Cisco Unified Communications Manager の TCP および UDP ポートは、次のカテゴリに整理されます。

- Cisco Unified Communications Manager サーバ間のクラスター間ポート
- 共通サービス ポート
- Cisco Unified Communications Manager と LDAP ディレクトリとの間のポート
- CCMAAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求
- Cisco Unified Communications Manager から電話機への Web 要求
- 電話機と Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信
- ゲートウェイと Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信

- アプリケーションと Cisco Unified Communications Manager との間の通信
- CTL クライアントとファイアウォールとの通信
- HP サーバ上の特殊なポート

上記のそれぞれのカテゴリのポートの詳細については、「「ポートの説明」」を参照してください。



(注) シスコでは、これらのポートで想定されるすべての設定シナリオを検証しているわけではありません。この一覧を参考にした結果、設定に問題が発生した場合は、シスコのテクニカルサポートにお問い合わせください。

ポートの参照は、特に Cisco Unified Communications Manager に適用されます。リリースによってポートが異なる場合があります、今後のリリースで新しくポートが追加される可能性もあります。このため、インストールされている Cisco Unified Communications Manager のバージョンに一致するバージョンのマニュアルを使用していることを確認してください。

ほとんどすべてのプロトコルは双方向ですが、セッション送信元からみた方向性は想定されています。デフォルトのポート番号は、管理者が手動で変更できる場合がありますが、ベストプラクティスとしてこのような変更は推奨しません。Cisco Unified Communications Manager が内部使用に限って複数のポートを開くことに注意してください。

Cisco Unified Communications Manager ソフトウェアをインストールすると、デフォルトではサービスアビリティ用に次のネットワークサービスが自動的にインストールされてアクティブになります。詳細については、「「Cisco Unified Communications Manager サーバの間のクラスタ内ポート」」を参照してください。

- Cisco Log Partition Monitoring (共通パーティションを監視および消去します。このサービスは、カスタム共通ポートを使用しません)
- Cisco Trace Collection Service (TCTS ポート使用)
- Cisco RIS Data Collector (RIS サーバ ポート使用)
- Cisco AMC Service (AMC ポート使用)

ファイアウォール、ACL、または QoS の設定は、トポロジ、テレフォニー デバイスおよびテレフォニー サービスの配置とネットワーク セキュリティ デバイスの配置との関係、および使用中のアプリケーションとテレフォニー拡張機能によって異なります。また、デバイスやバージョンによって、ACL のフォーマットが異なることにも注意してください。



(注) Cisco Unified Communications Manager でマルチキャスト保留音 (MoH) ポートを設定することもできます。管理者が実際のポート値を指定するため、マルチキャスト MOH のポート値は提供されません。



- (注) システムの一時ポート範囲は 32768～61000 で、電話を登録したままにするには、ポートを開く必要があります。詳細については、<http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html> を参照してください。



- (注) ポート 22 への接続が開かれ、調整されないようにファイアウォールを設定してください。IM and Presence サブスクリバノードのインストール中に、Cisco Unified Communications Manager パブリッシャノードへの複数の接続が短時間で連続して開かれます。これらの接続を調整すると、インストールが失敗する可能性があります。

ポート説明

Cisco Unified Communications Manager サーバ間のクラスタ間ポート

表 48: Cisco Unified Communications Manager サーバ間のクラスタ間ポート

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
エンドポイント (Endpoint)	Unified Communications Manager	514 / UDP	システム ロギング サービス
Unified Communications Manager	RTMT	1090、1099 / TCP	RTMT パフォーマンス モニタ、データ収集、 ロギング、およびア ラート生成用の Cisco AMC サービス。
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1500、1501 / TCP	データベース接続 (1501 / TCP はセカン ダリ接続)
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1510 / TCP	CAR IDS DB。CAR IDS エンジンが、クラ イアントからの接続要 求を監視します。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1511 / TCP	CAR IDS DB。アップグレード時に、CAR IDS のインスタンスをもう1つ開始するために使用される代替ポート。
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1515 / TCP	インストール時のノード間でのデータベースレプリケーション
Cisco Extended Functions (QRT)	Unified Communications Manager (DB)	2552 / TCP	Cisco Unified Communications Manager データベース変更通知をサブスクライバが受信できるようにします。
Unified Communications Manager	Unified Communications Manager	2551 / TCP	アクティブ/バックアップ判別のための Cisco Extended Services 間のクラスタ間通信
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	2555 / TCP	Real-time Information Services (RIS) データベース サーバ
Unified Communications Manager (RTMT、AMC、またはSOAP)	Unified Communications Manager (RIS)	2556 / TCP	Cisco RIS 向け Real-time Information Services (RIS) データベース クライアント
Unified Communications Manager (DRS)	Unified Communications Manager (DRS)	4040 / TCP	DRS プライマリエージェント
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5001 / TCP	このポートは、SOAP モニタがリアルタイムモニタリングサービスに使用します。
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5002 / TCP	このポートは、SOAP モニタがパフォーマンスモニタ サービスに使用します。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5003 / TCP	このポートは、SOAP モニタがコントロールセンターサービスに使用します。
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5004 / TCP	このポートは、SOAP モニタがログコレクションサービスに使用します。
標準 CCM 管理ユーザ / 管理	Unified Communications Manager	5005 / TCP	このポートは SOAP CDROnDemand 2 サービスによって使用されます
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5007 / TCP	SOAP モニタ
Unified Communications Manager (RTMT)	Unified Communications Manager (TCTS)	エフェメラル / TCP	Cisco Trace Collection Tool Service (TCTS) : RTMT Trace and Log Central (TLC) 向けのバックエンドサービス
Unified Communications Manager (Tomcat)	Unified Communications Manager (TCTS)	7000、7001、7002 / TCP	このポートは、Cisco Trace Collection Tool Service と Cisco Trace Collection Servlet との通信に使用されます。
Unified Communications Manager (DB)	Unified Communications Manager (CDLM)	8001 / TCP	クライアントデータベース変更通知
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8002 / TCP	クラスタ間通信サービス
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8003 / TCP	クラスタ間通信サービス (CTI 対象)
Unified Communications Manager	CMI マネージャ	8004 / TCP	Cisco Unified Communications Manager と CMI マネージャとのクラスタ間通信

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8005 / TCP	Tomcat シャットダウンスクリプトで使用される内部リスニングポート
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8080 / TCP	診断テストのためのサーバ間の通信
ゲートウェイ	Unified Communications Manager	8090	CUCM と GW (Cayuga インターフェイス) が Gateway Recording 機能のための通信に使用する HTTP ポート
Unified Communications Manager	ゲートウェイ		
Unified Communications Manager (IPSec)	Unified Communications Manager (IPSec)	8500 / TCP および UDP	IPSec クラスタ マネージャによるシステムデータのクラスタ間複製
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	8888 ~ 8889 / TCP	RIS サービス マネージャのステータス要求と応答
Location Bandwidth Manager (LBM)	Location Bandwidth Manager (LBM)	9004 / TCP	LBM 間のクラスタ間通信
Unified Communications Manager パブリッシャ	Unified Communications Manager サブスクリイバ	22 / TCP	Cisco SFTP サービス。サブスクリイバを新しくインストールする場合は、このポートを開く必要があります。
Unified Communications Manager	Unified Communications Manager	8443 / TCP	ノード間のコントロールセンター機能とネットワークサービスへのアクセスを可能にします。

共通サービス ポート

表 49: 共通サービス ポート

送信元 (送信者)	送信先 (リスナー)	接続先ポート	目的
エンドポイント (Endpoint)	Unified Communications Manager	7	Internet Control Message Protocol (ICMP)。このプロトコル番号がエコー関連のトラフィックを伝送します。列見出しに示すようなポートとなるものではありません。
Unified Communications Manager	エンドポイント (Endpoint)		
Unified Communications Manager (DRS、CDR)	SFTP サーバ	22 / TCP	SFTP サーバにバックアップデータを送信します。(DRS ローカルエージェント) SFTP サーバに CDR データを送信します。
エンドポイント (Endpoint)	Unified Communications Manager (DHCP サーバ)	67 / UDP	DHCP サーバとして機能する Cisco Unified Communications Manager (注) Cisco Unified Communications Manager 上で DHCP サーバを実行することは推奨しません。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager	DHCP サーバ（DHCP Server）	68 / UDP	DHCP クライアントとして機能する Cisco Unified Communications Manager （注） Cisco Unified Communications Manager 上で DHCP クライアントを実行することは推奨しません。その代わりに、Cisco Unified Communications Manager には固定 IP アドレスを設定します。
エンドポイントまたはゲートウェイ	Unified Communications Manager	69、6969、次にエフェメラル / UDP	電話機およびゲートウェイに対する Trivial File Transfer Protocol（TFTP）サービス
エンドポイントまたはゲートウェイ	Unified Communications Manager	6970 / TCP	プライマリサーバとプロキシサーバ間のトリビアルファイル転送プロトコル（TFTP） 電話機とゲートウェイに対する TFTP サーバの HTTP サービス
Unified Communications Manager	NTP サーバ（NTP Server）	123 / UDP	ネットワーク タイム プロトコル（NTP）
SNMP サーバ	Unified Communications Manager	161 / UDP	SNMP サービス応答（管理アプリケーションからの要求）
CUCM サーバ SNMP プライマリエージェント アプリケーション	SNMP トラップの宛先	162 / UDP	SNMP トラップ

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
SNMP サーバ	Unified Communications Manager	199 / TCP	SMUX サポートのためのネイティブ SNMP エージェントリスニングポート
Unified Communications Manager	DHCP サーバ（DHCP Server）	546 / UDP	DHCPv6。IPv6 用の DHCP ポート。
Unified Communications Manager Serviceability	Location Bandwidth Manager（LBM）	5546 / TCP	Enhanced Location CAC Serviceability
Unified Communications Manager	Location Bandwidth Manager（LBM）	5547 / TCP	コールアドミッションの要求および帯域幅の縮小
Unified Communications Manager	Unified Communications Manager	6161 / UDP	プライマリエージェントとネイティブエージェント間の通信に使用され、ネイティブエージェントの MIB 要求を処理します。
Unified Communications Manager	Unified Communications Manager	6162 / UDP	プライマリエージェントとネイティブエージェント間の通信に使用され、ネイティブエージェントから生成された通知を転送します。
中央集中型 TFTP	代替 TFTP（Alternate TFTP）	6970 / TCP	中央集中型 TFTP ファイルロケータサービス
Unified Communications Manager	Unified Communications Manager	7161 / TCP	SNMP プライマリエージェントとサブエージェント間の通信に使用されます。
SNMP サーバ	Unified Communications Manager	7999 / TCP	Cisco Discovery Protocol（CDP）エージェントが、CDP 実行可能機器と通信します。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
エンドポイント （Endpoint）	Unified Communications Manager	443、8443/TCP	Cisco ユーザ データ サービス（UDS）の要 求に使用されます。
Unified Communications Manager	Unified Communications Manager	9050 / TCP	Cisco Unified Communications Manager にある TAPS を利用して CRS 要求 を処理します。
Unified Communications Manager	Unified Communications Manager	61441 / UDP	Cisco Unified Communications Manager アプリケー ションが、UDPでこの ポートにアラームを送 信します。Cisco Unified Communications Manager MIB エージェ ントが、Cisco Unified Communications Manager MIB 定義に 従って、このポートを 監視し、SNMPトラッ プを生成します。
Unified Communications Manager	Unified Communications Manager	5060、5061 / TCP	トランクベースの SIP サービスを提供しま す。
Unified Communications Manager	Unified Communications Manager	7501	クラスタ間検索サービ ス（ILS）の証明書 ベースの認証に使用さ れます。
Unified Communications Manager	Unified Communications Manager	7502	ILSのパスワードベー ス認証に使用されま す。
--	--	8000-48200	ASR および ISR G3 プ ラットフォームのデ フォルトポート範囲。
		16384 ~ 32766	ISR G2 プラットフォー ムのデフォルトポート 範囲。

Cisco Unified Communications Manager と LDAP ディレクトリとの間のポート

表 50: Cisco Unified Communications Manager と LDAP ディレクトリとの間のポート

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager	外部ディレクトリ	389、636、3268、3269 / TCP	外部ディレクトリ（Active Directory、Netscape Directory）への Lightweight Directory Access Protocol（LDAP）クエリ
外部ディレクトリ	Unified Communications Manager	エフェメラル	

CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求

表 51: CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
ブラウザ	Unified Communications Manager	80、8080 / TCP	ハイパーテキスト転送プロトコル（HTTP）
ブラウザ	Unified Communications Manager	443、8443 / TCP	Hypertext Transport Protocol over SSL（HTTPS）

Cisco Unified Communications Manager から電話機への Web 要求

表 52: Cisco Unified Communications Manager から電話機への Web 要求

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager <ul style="list-style-type: none"> • QRT • RTMT • [電話の検索と一覧表示 (Find and List Phones)] ページ • [電話の設定 (Phone Configuration)] ページ 	電話	80/TCP	ハイパーテキスト転送プロトコル (HTTP)

電話機と Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信

表 53: 電話機と Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
電話	Unified Communications Manager	53 / TCP	<p>Session Initiation Protocol (SIP) 電話機が、ドメインネームシステム (DNS) を使用して、完全修飾ドメイン名 (FQDN) を解決します。</p> <p>(注) デフォルトでは、一部のワイヤレスアクセスポイントは TCP の 53 番ポートをブロックし、FQDN を使用しながら CUCM を設定しているときに、ワイヤレス SIP 電話機が登録されないようにします。</p>
電話	Unified Communications Manager (TFTP)	69、次にエフェメラル / UDP	ファームウェアおよび設定ファイルのダウンロードに使用される Trivial File Transfer Protocol (TFTP)
電話	Unified Communications Manager	2000 / TCP	Skinnny Client Control Protocol (SCCP)
電話	Unified Communications Manager	2443 / TCP	Secure Skinnny Client Control Protocol (SCCPS)

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
電話	Unified Communications Manager	2445 / TCP	エンドポイントに信頼検証サービスを提供します。
電話	Unified Communications Manager (CAPF)	3804 / TCP	ローカルで有効な証明書 (LSC) を IP Phone に発行するための認証局プロキシ機能 (CAPF) リスニングポート
電話	Unified Communications Manager	5060 / TCP および UDP	Session Initiation Protocol (SIP) 電話機
Unified Communications Manager	電話		
電話	Unified Communications Manager	5061 TCP	Secure Session Initiation Protocol (SIPS) 電話機
Unified Communications Manager	電話		
電話	Unified Communications Manager (TFTP)	6970 TCP	ファームウェアおよび設定ファイルの HTTP ベースのダウンロード
電話	Unified Communications Manager (TFTP)	6971、6972 / TCP	TFTP への HTTPS インターフェイス。電話機が、TFTP からセキュアな設定ファイルをダウンロードするためにこのポートを使用します。
電話	Unified Communications Manager	8080 / TCP	XML アプリケーション、認証、ディレクトリ、サービスなどで電話機が使用する URL。サービスごとにこれらのポートを設定できます。
電話	Unified Communications Manager	9443 / TCP	電話機が、認証された連絡先検索にこのポートを使用します。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
電話	Unified Communications Manager	9444	電話機は、このポート番号を使用してヘッドセット管理機能を利用します。
IP VMS	電話	16384 ~ 32767 / UDP	Real-Time Protocol (RTP)、Secure Real-Time Protocol (SRTP) (注) 他のデバイスは全範囲を使用しますが、Cisco Unified Communications Manager は 24576 ~ 32767 だけを使用します。
電話	IP VMS		

ゲートウェイと Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信

表 54: ゲートウェイと Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
ゲートウェイ	Unified Communications Manager	47、50、51	Generic Routing Encapsulation (GRE)、Encapsulating Security Payload (ESP)、認証ヘッダー (AH)。これらのプロトコル番号は、暗号化された IPSec トラフィックを伝送します。列見出しに示すようなポートとなるものではありません。
Unified Communications Manager	ゲートウェイ		

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
ゲートウェイ	Unified Communications Manager	500 / UDP	IP Security (IPSec) プロトコル確立のためのインターネットキーエクステンジ (IKE)
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager (TFTP)	69、次にエフェメラル / UDP	トリビアルファイル転送プロトコル (TFTP)
Cisco Intercompany Media Engine (CIME) トランクを使用した Unified Communications Manager	CIME ASA	1024 ~ 65535 / TCP	ポート マッピング サービス。CIME オフパス導入モデルでのみ使用します。
Gatekeeper	Unified Communications Manager	1719 / UDP	ゲートキーパー (H.225) RAS
ゲートウェイ	Unified Communications Manager	1720 / TCP	H.323 ゲートウェイおよびクラスタ間トランク (ICT) 向けの H.225 シグナリングサービス
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	エフェメラル / TCP	ゲートキーパー制御トランク上の H.225 シグナリング サービス
Unified Communications Manager	ゲートウェイ		

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
ゲートウェイ	Unified Communications Manager	エフェメラル / TCP	音声、ビデオ、およびデータを確立するための H.245 シグナリングサービス (注) ゲートウェイの種類によって異なる、リモートシステムで使用される H.245 ポート。 IOS ゲートウェイでの H.245 ポート範囲は、11000 ~ 65535 です。
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	2000 / TCP	Skinny Client Control Protocol (SCCP)
ゲートウェイ	Unified Communications Manager	2001 / TCP	Cisco Unified Communications Manager の導入で使用する 6608 ゲートウェイ用アップグレードポート
ゲートウェイ	Unified Communications Manager	2002 / TCP	Cisco Unified Communications Manager の導入で使用する 6624 ゲートウェイ用アップグレードポート
ゲートウェイ	Unified Communications Manager	2427 / UDP	Media Gateway Control Protocol (MGCP) ゲートウェイコントロール
ゲートウェイ	Unified Communications Manager	2428 / TCP	Media Gateway Control Protocol (MGCP) バックホール

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
--	--	4000 ~ 4005 / TCP	Cisco Unified Communications Manager に音声、ビデオ、およびDチャンネルのポートがないときには、これらのポートがこのようなメディアのファントム Real-Time Transport Protocol (RTP) ポートおよび Real-Time Transport Control Protocol (RTCP) ポートとして使用されます。
ゲートウェイ	Unified Communications Manager	5060 / TCP および UDP	Session Initiation Protocol (SIP) ゲートウェイおよびクラスター間トランク (ICT)
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	5061 / TCP	Secure Session Initiation Protocol (SIPS) ゲートウェイおよびクラスター間トランク (ICT)
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	16384 ~ 32767 / UDP	Real-Time Protocol (RTP)、Secure Real-Time Protocol (SRTP) (注) 他のデバイスは全範囲を使用しますが、Cisco Unified Communications Manager は 24576 ~ 32767 だけを使用します。
Unified Communications Manager	ゲートウェイ		

アプリケーションと Cisco Unified Communications Manager との間の通信

表 55: アプリケーションと Cisco Unified Communications Manager との間の通信

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
CTL クライアント	Unified Communications Manager CTL プロバイダー	2444 / TCP	Cisco Unified Communications Manager の証明書信頼リスト (CTL) プロバイダー リスニング サービス
Cisco Unified Communications アプリケーション	Unified Communications Manager	2748 / TCP	CTI アプリケーション サーバ
Cisco Unified Communications アプリケーション	Unified Communications Manager	2749 / TCP	CTI アプリケーション (JTAPI/TSP) と CTI Manager 間の TLS 接続
Cisco Unified Communications アプリケーション	Unified Communications Manager	2789 / TCP	JTAPI アプリケーション サーバ
Unified Communications Manager Assistant Console	Unified Communications Manager	2912 / TCP	Cisco Unified Communications Manager Assistant サーバ (以前の IPMA)
Unified Communications Manager Attendant Console	Unified Communications Manager	1103 ~ 1129 / TCP	Cisco Unified Communications Manager Attendant Console (AC) JAVA RMI レジストリ サーバ
Unified Communications Manager Attendant Console	Unified Communications Manager	1101 / TCP	RMI サーバは、RMI コールバック メッセージをこれらのポートを使用するクライアントに送信します。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager Attendant Console	Unified Communications Manager	1102 / TCP	Attendant Console (AC) RMI サーババインドポート: RMI サーバは、これらのポートに RMI メッセージを送信します。
Unified Communications Manager Attendant Console	Unified Communications Manager	3223 / UDP	Cisco Unified Communications Manager Attendant Console (AC) サーバ回線状態ポートは、Attendant Console サーバから ping および登録メッセージを受信し、Attendant Console サーバに回線状態を送信します。
Unified Communications Manager Attendant Console	Unified Communications Manager	3224 / UDP	Cisco Unified Communications Manager Attendant Console (AC) クライアントは、回線状態情報およびデバイス状態情報のために AC サーバに登録されます。
Unified Communications Manager Attendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Communications Manager Attendant Console (AC) クライアントは、コール制御のために AC サーバに登録されます。
SAF/CCD を使用する Unified Communications Manager	SAF イメージを実行する IOS ルータ	5050 / TCP	EIGRP/SAF プロトコルを実行するマルチサービス IOS ルータ。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager	Cisco Intercompany Media Engine (IME) サーバ	5620 / TCP このポートでは、ポート番号 5620 の使用を推奨しますが、CLI コマンドの <code>add ime vapserver</code> または <code>set ime vapserver port</code> を Cisco IME サーバで実行することにより、値を変更できます。	VAP プロトコルは、Cisco Intercompany Media Engine サーバとの通信に使用されます。
Cisco Unified Communications アプリケーション	Unified Communications Manager	8443 / TCP	課金アプリケーションまたはテレフォニー管理アプリケーションなどのサードパーティが、Cisco Unified Communications Manager データベースに対してプログラムで読み書きするために使用する AXL/SOAP API。

CTL クライアントとファイアウォールとの通信

表 56: CTL クライアントとファイアウォールとの通信

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
CTL クライアント	TLS プロキシサーバ	2444 / TCP	ASA ファイアウォールの証明書信頼リスト (CTL) プロバイダーリスニングサービス

HP サーバ上の特殊なポート

表 57: HP サーバ上の特殊なポート

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
エンドポイント (Endpoint)	HP SIM	2301 / TCP	HP エージェントへの HTTP ポート

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
エンドポイント （Endpoint）	HP SIM	2381 / TCP	HP エージェントへの HTTPS ポート
エンドポイント （Endpoint）	Compaq 管理エー ジェント	25375、25376、25393 /UDP	COMPAQ 管理エー ジェント拡張 （cmaX）
エンドポイント （Endpoint）	HP SIM	50000 ~ 50004 / TCP	HP SIM への HTTPS ポート

ポート参照

ファイアウォールアプリケーションインスペクションガイド

ASA シリーズ参考情報

<http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html>

『PIX Application Inspection Configuration Guide』

<http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html>

『FWSM 3.1 Application Inspection Configuration Guide』

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fws31/configuration/guide/fws31_cfg/inspct_f.html

IETF TCP/UDP ポート割り当てリスト

Internet Assigned Numbers Authority (IANA) IETF 割り当てポート リスト

<http://www.iana.org/assignments/port-numbers>

IP テレフォニー設定とポート使用に関するマニュアル

『Cisco CRS 4.0 (IP IVR and IPCC Express) Port Utilization Guide』

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

『Port Utilization Guide for Cisco ICM/IPCC Enterprise and Hosted Editions』

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

『Cisco Unified Communications Manager Express Security Guide to Best Practices』

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

『Cisco Unity Express Security Guide to Best Practices』

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e31.html#wp41149

VMware ポート割り当てリスト

vCenter Server、ESX ホストおよびその他のネットワーク コンポーネント管理アクセス用の TCP および UDP ポート



第 35 章

IM and Presence サービスのポートの使用 情報

- [IM and Presence サービス ポートの使用方法の概要 \(485 ページ\)](#)
- [テーブルで照合する情報 \(486 ページ\)](#)
- [IM and Presence サービス ポート リスト \(486 ページ\)](#)

IM and Presence サービス ポートの使用方法の概要

このマニュアルには、IM and Presence Service が、クラスタ内接続用および、外部アプリケーションまたは外部デバイスとの通信用に使用する TCP および UDP ポートの一覧を示します。これは、IP Communications ソリューションの実装時に、ネットワークにファイアウォール、アクセスコントロールリスト (ACL)、および Quality of Service (QoS) を設定するうえで重要な情報となります。



(注) シスコでは、これらのポートで想定されるすべての設定シナリオを検証しているわけではありません。この一覧を参考にした結果、設定に問題が発生した場合は、シスコのテクニカルサポートにお問い合わせください。

事実上すべてのプロトコルが双方向で行われますが、このマニュアルではセッション開始側から見た方向を記載しています。デフォルトのポート番号は、管理者が手動で変更できる場合がありますが、ベストプラクティスとしてこのような変更は推奨しません。IM and Presence Service が内部使用に限って複数のポートを開くことに注意してください。

このドキュメントのポートは、IM and Presence サービスに特別に適用されます。リリースによってポートが異なる場合があり、今後のリリースで新しくポートが追加される可能性もあります。このため、インストールされている IM and Presence Service のバージョンに一致する正しいバージョンのマニュアルを使用していることを確認してください。

ファイアウォール、ACL、または QoS の設定内容は、トポロジ、ネットワークセキュリティデバイスの配置に対するデバイスとサービスの配置、および使用するアプリケーションとテレ

フォニー拡張機能の種類に応じて異なります。また、デバイスやバージョンによって、ACLのフォーマットが異なることにも注意してください。

テーブルで照合する情報

この表では、このドキュメントの表のそれぞれに照合する情報を定義します。

表 58: 表の内容

表の項目	説明
送信元 (From)	ポートに要求を送信するクライアント
移行後	ポートで要求を受信するクライアント
[役割 (Role)]	クライアントまたはサーバのアプリケーションまたはプロセス
[プロトコル (Protocol)]	通信の確立と終了に使用されるセッション層プロトコル、またはトランザクションの要求と応答に使用されるアプリケーション層プロトコルのどちらか。
トランスポートプロトコル	コネクション型 (TCP) またはコネクションレス型 (UDP) のトランスポート層プロトコル
宛先/リスナー	要求の受信に使用されるポート
ソース/送信元	要求の送信に使用されるポート

IM and Presence サービス ポート リスト

次のテーブルは、IM and Presence サービスがクラスタ内とクラスタ間のトラフィックに使用するポートを示します。

表 59: IM and Presence サービス ポート : SIP プロキシの要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
SIP ゲートウェイ ----- [IM and Presence]	[IM and Presence] ----- SIP ゲートウェイ	SIP	TCP/UDP	[5060]	エフェメラル	デフォルトの SIP プロキシの UDP および TCP リスナー

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
SIP ゲートウェイ	[IM and Presence]	SIP	TLS	5061	エフェメラル	TLS サーバ認証のリスナー ポート
[IM and Presence]	[IM and Presence]	SIP	TLS	5062	エフェメラル	TLS 相互認証のリスナー ポート
[IM and Presence]	[IM and Presence]	SIP	UDP/TCP	5049	エフェメラル	内部ポート。ローカルホスト トラフィック専用。
[IM and Presence]	[IM and Presence]	HTTP	[TCP]	8081	エフェメラル	設定の変更を示す設定のエージェントからの HTTP 要求に使用されます。
サードパーティ製クライアント	[IM and Presence]	HTTP	[TCP]	8082	エフェメラル	デフォルトの IM and Presence HTTP のリスナー。サードパーティ製クライアントからの接続に使用されます。
サードパーティ製クライアント	[IM and Presence]	HTTPS	TLS/TCP	8083	エフェメラル	デフォルトの IM and Presence HTTPS リスナー。サードパーティ製クライアントからの接続に使用されます。

表 60: IM and Presence サービス ポート : Presence エンジンの要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	IM and Presence (Presence Engine)	SIP	UDP/TCP	5080	エフェメラル	デフォルトの SIP UDP/TCP リスナー ポート

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence (Presence Engine)	IM and Presence (Presence Engine)	Livebus	UDP	50000	エフェメラル	内部ポート。ローカルホストトラフィック専用。LiveBus メッセージングポート。IM and Presence サービスは、このポートをクラスタ通信に使用します。

表 61 : IM and Presence サービス ポート : シスコの Tomcat WebRequests

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
ブラウザ	[IM and Presence]	HTTPS	[TCP]	8080	エフェメラル	Web アクセスに使用されます。
ブラウザ	[IM and Presence]	AXLHTTPS	TLS/TCP	8443	エフェメラル	SOAP によりデータベースおよびサービスアビリティへのアクセスを提供します。
ブラウザ	[IM and Presence]	HTTPS	TLS/TCP	8443	エフェメラル	Web 管理へのアクセスを提供します。
ブラウザ	[IM and Presence]	HTTPS	TLS/TCP	8443	エフェメラル	ユーザ オプションページへのアクセスを提供します。
ブラウザ	[IM and Presence]	SOAP	TLS/TCP	8443	エフェメラル	SOAP により Cisco Unified Personal Communicator、Cisco Unified Mobility Advantage、およびサードパーティ製の API クライアントへのアクセスを提供します。

表 62: IM and Presence サービス ポート : 外部社内ディレクトリ要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence] ----- 外部社内ディレクトリ	外部社内ディレクトリ ----- [IM and Presence]	LDAP	TCP	389 / 3268	エフェメラル	ディレクトリ プロトコルを外部社内ディレクトリと統合できるようにします。この LDAP ポートは、統合される社内ディレクトリによって異なります (デフォルトは 389)。Netscape Directory の場合は、別のポートで LDAP トラフィックを受信できるよう設定できます。 認証用に IM&P と LDAP サーバ間の通信を LDAP に許可します。
[IM and Presence]	外部社内ディレクトリ	LDAPS	TCP	636	エフェメラル	ディレクトリ プロトコルを外部社内ディレクトリと統合できるようにします。この LDAP ポートは、統合される社内ディレクトリによって異なります (デフォルトは 636)。

表 63: IM and Presence サービス ポート : リクエストの設定

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence (設定エージェント)	IM and Presence (設定エージェント)	[TCP]	[TCP]	8600	エフェメラル	設定エージェントの ハートビート ポート

表 64: IM and Presence サービス ポート : Certificate Manager の要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	証明書マネージャ	[TCP]	[TCP]	7070	エフェメラル	内部ポート。ローカルホスト トラフィック専用。

表 65: IM and Presence サービス ポート : IDSデータベースの要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence (データベース)	IM and Presence (データベース)	[TCP]	[TCP]	1500	エフェメラル	データベース クライアント用の内部 IDS ポート。ローカルホスト トラフィック専用。
IM and Presence (データベース)	IM and Presence (データベース)	[TCP]	[TCP]	1501	エフェメラル	内部ポート : アップグレード中に IDS の 2 次インスタンスを始動するための代替ポートです。ローカルホスト トラフィック専用。
IM and Presence (データベース)	IM and Presence (データベース)	XML	[TCP]	1515	エフェメラル	内部ポート。ローカルホスト トラフィック専用。DB レプリケーション ポート。

表 66: IM and Presence Service ポート : IPsec マネージャの要求

送信元 送信者	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence (IPSec)	IM and Presence (IPSec)	専用	UDP/TCP	8500	8500	内部ポート : ipsec_mgr デーモンがプラットフォーム データ (ホスト) の証明書のクラスタ レプリケーションに使用するクラスタ マネージャ ポートです。

表 67: IM and Presence サービス ポート : DRFにマスター エージェント サーバ要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence (DRF)	IM and Presence (DRF)	[TCP]	[TCP]	4040	エフェメラル	DRF Master Agent サーバポート。Local Agent、GUI、および CLIからの接続を受け入れます。

表 68: IM and Presence サービス ポート : RISDC要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence (RIS)	IM and Presence (RIS)	[TCP]	[TCP]	2555	エフェメラル	Real-time Information Services (RIS) データベースサーバ。クラスタ内の他の RISDC サービスに接続し、クラスタ全体のリアルタイム情報を提供します。
IM and Presence (RIMI/AMC/ SOAP)	IM and Presence (RIS)	[TCP]	[TCP]	2556	エフェメラル	Cisco RIS 向け Real-time Information Services (RIS) データベースクライアント。RISクライアント接続で、リアルタイム情報を取得できるようにする
IM and Presence (RIS)	IM and Presence (RIS)	[TCP]	[TCP]	8889	8888	内部ポート。ローカルホストトラフィック専用。サービスステータスの要求および応答用として、RISDC (システムアクセス) が TCP で servM にリンクするために使用します。

表 69: IM and Presence サービス ポート: SNMP の要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
SNMP サーバ	[IM and Presence]	SNMP	UDP	161、8161	エフェメラル	SNMP ベースの管理アプリケーションにサービスを提供
[IM and Presence]	[IM and Presence]	SNMP	UDP	6162	エフェメラル	SNMP マスター エージェントから転送される要求を受信するネイティブ SNMP エージェント。
[IM and Presence]	[IM and Presence]	SNMP	UDP	6161	エフェメラル	ネイティブ SNMP エージェントからのトラップ情報を受信し、管理アプリケーションに転送する SNMP マスター エージェント。
SNMP サーバ	[IM and Presence]	[TCP]	[TCP]	7999	エフェメラル	CDP Agent が CDP バイナリと通信するためにソケットとして使用します。
[IM and Presence]	[IM and Presence]	[TCP]	[TCP]	7161	エフェメラル	SNMP マスター エージェントとサブエージェント間の通信に使用されます。
[IM and Presence]	SNMP トラップ モニタ	SNMP	UDP	162	エフェメラル	SNMP トラップを管理アプリケーションに送信します。
[IM and Presence]	[IM and Presence]	SNMP	UDP	設定可能	61441	内部 SNMP トラップ レシーバ

表 70: IM and Presence サービス ポート : *Racoon* サーバ要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
ゲートウェイ ----- [IM and Presence]	[IM and Presence] ----- ゲートウェイ	Ipsec	UDP	500	エフェメラル	Internet Security Association and the KeyManagement Protocol (ISAKMP) を有効にします。

表 71: IM and Presence サービス ポート : システム サービス要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence (RIS)	IM and Presence (RIS)	XML	[TCP]	8888 および 8889	エフェメラル	内部ポート。ローカルホストトラフィック専用。RIS サービスマネージャ (servM) と通信するクライアントを受信するために使用します。

表 72: IM and Presence サービス ポート : *DNS* 要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	DNS サーバ	DNS	UDP	53	エフェメラル	DNS サーバが IM and Presence DNS 照会を受信するポート。 宛先:DNS サーバ 送信元:IM and Presence

表 73: IM and Presence サービス ポート: SSH/SFTP 要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	エンドポイント (Endpoint)	SSH/SFTP	[TCP]	22	エフェメラル	多くのアプリケーションが、サーバへのコマンドラインアクセスを行うために使用します。ノード間で証明書などのファイル交換 (sftp) にも使用されます。

表 74: IM and Presence サービス ポート: ICMP 要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence] ----- Cisco Unified Communications Manager	Cisco Unified Communications Manager ----- [IM and Presence]	ICMP	IP	N/A	エフェメラル	インターネット制御メッセージプロトコル (ICMP)。Cisco Unified Communications Manager サーバとの通信に使用されます。

表 75: IM and Presence サービス ポート: NTP 要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	NTP サーバ (NTP Server)	NTP	UDP	123	エフェメラル	Cisco Unified Communications Manager は NTP サーバとして動作します。サブスクリバノードが、パブリッシュノードと時刻を同期するために使用されます。

表 76: IM and Presence サービス ポート : Microsoft Exchange 通知要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
Microsoft Exchange	[IM and Presence]	HTTP (HTTPu)) WebDAV : HTTP /UDP/IP 通知 2) EWS - HTTP/TCP/ SOAP 通知	IM and Presence サーバ ポート (デフォルト 50020)	エフェメラル	Microsoft Exchange は、このポートを使用してカレンダー イベントの特定のサブスクリプション識別子に対する変更を示す通知 (NOTIFY メッセージによって示される) を送信します。ネットワーク構成内にある Exchange サーバと統合する場合に使用されます。どちらのポートも作成されます。送信されるメッセージの種類は、設定するカレンダー プレゼンス バックエンド ゲートウェイのタイプによって異なります。

表 77: IM and Presence サービス ポート : SOAP サービス リクエスト

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence (Tomcat)	IM and Presence (SOAP)	[TCP]	[TCP]	5007	エフェメラル	SOAP モニタ ポート

表 78: IM and Presence サービス ポート : AMC RMI 要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	RTMT	[TCP]	[TCP]	1090	エフェメラル	AMC RMI オブジェクトポート RTMT パフォーマンス モニタ、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。
[IM and Presence]	RTMT	[TCP]	[TCP]	1099	エフェメラル	AMC RMI レジストリポート RTMT パフォーマンス モニタ、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。

表 79: IM and Presence サービス ポート : XCP 要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
XMPP クライアント	[IM and Presence]	[TCP]	[TCP]	5222	エフェメラル	クライアント アクセス ポート
[IM and Presence]	[IM and Presence]	[TCP]	[TCP]	5269	エフェメラル	サーバ間接続 (S2S) ポート
サードパーティ製 BOSH クライアント	[IM and Presence]	[TCP]	[TCP]	7335	エフェメラル	XCP Web Connection Manager が、BOSH を使用するサードパーティ製 API との接続に使用する HTTP リスニング ポート

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence (XCP サービス)	IM and Presence (XCP ルータ)	[TCP]	[TCP]	7400	エフェメラル	XCP ルータ マスター アクセス ポート。オープンポート設定からルータに接続する XCP サービス (XCP 認証コンポーネント サービスなど) は、通常このポートを使用して接続します。
IM and Presence (XCP ルータ)	IM and Presence (XCP ルータ)	UDP	UDP	5353	エフェメラル	MDNS ポート。クラスタ内の XCP ルータはこのポートを使用してお互いを検出します。
IM and Presence (XCP ルータ)	IM and Presence (XCP ルータ)	[TCP]	[TCP]	7336	HTTPS	MFT ファイル転送 (オンプレミスのみ)。

表 80: IM and Presence サービスポート: 外部データベースのリクエスト

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	PostgreSQL データベース	[TCP]	[TCP]	5432 ¹	エフェメラル	PostgreSQL データベース リスニング ポート
[IM and Presence]	Oracle データベース	[TCP]	[TCP]	1521	エフェメラル	Oracle データベース リスニング ポート
IM and Presence	MSSQL database	[TCP]	[TCP]	1433	エフェメラル	MSSQL データベース リスニング ポート

¹ これがデフォルトのポートですが、任意のポートで受信するよう PostgreSQL データベースを設定できます。

表 81: IM and Presence サービス ポート: 高可用性の要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence (Server Recovery Manager)	IM and Presence (Server Recovery Manager)	[TCP]	[TCP]	20075	エフェメラル	Cisco Server Recovery Manager が管理 RPC 要求を行うために使用するポート。
IM and Presence (Server Recovery Manager)	IM and Presence (Server Recovery Manager)	UDP	UDP	21999	エフェメラル	Cisco Server Recovery Manager がピアとの通信に使用するポート。

表 82: IM and Presence サービス ポート: In Memory データベース レプリケーションのメッセージ

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	専用	[TCP]	6603*	エフェメラル	Cisco Presence Datastore
[IM and Presence]	[IM and Presence]	専用	[TCP]	6604*	エフェメラル	Cisco Login Datastore
[IM and Presence]	[IM and Presence]	専用	[TCP]	6605*	エフェメラル	Cisco SIP Registration Datastore
[IM and Presence]	[IM and Presence]	専用	[TCP]	9003	エフェメラル	Cisco Presence Datastore デュアル ノードプレゼンス冗長グループの複製。
[IM and Presence]	[IM and Presence]	専用	[TCP]	9004	エフェメラル	Cisco Login Datastore デュアル ノードプレゼンス 冗長グループの複製。
[IM and Presence]	[IM and Presence]	専用	[TCP]	9005	エフェメラル	Cisco SIP Registration Datastore デュアル ノードプレゼンス冗長グループの複製。

* 管理 CLI 診断ユーティリティを実行するには、`utils imdb_replication status` コマンドを使用します。これらのポートは、クラスタの IM and Presence Service ノード間で設定されているすべてのファイアウォールでオープンである必要があります。このセットアップは、通常の運用では必要ありません。

表 83: IM and Presence サービス ポート : In Memory データベース SQL メッセージ

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	専用	[TCP]	6603	エフェメラル	Cisco Presence Datastore SQL クエリ。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6604	エフェメラル	Cisco Login Datastore SQL クエリ。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6605	エフェメラル	Cisco SIP Registration Datastore SQL クエリ。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6606	エフェメラル	Cisco Route Datastore SQL クエリ。

表 84: IM and Presence サービス ポート : In Memory データベースの通知メッセージ

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	専用	[TCP]	6607	エフェメラル	Cisco Presence Datastore XML ベースの変更通知。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6608	エフェメラル	Cisco Login Datastore XML ベースの変更通知。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6609	エフェメラル	Cisco SIP Registration Datastore XML ベースの変更通知。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6610	エフェメラル	Cisco Route Datastore XML ベースの変更通知。

表 85: IM and Presence Service ポート : 強制手動同期/X.509 証明書更新要求

送信元 (送信者)	送信先 (リスナー)	[プロトコル (Protocol)]	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence (Intercluster Sync Agent)	IM and Presence (Intercluster Sync Agent)	[TCP]	[TCP]	37239	エフェメラル	Cisco Intercluster Sync Agent サービスは、このポートを使用してコマンドを処理するためのソケット接続を確立します。

表 86: IM and Presence サービス ポート : ICMP 要求

送信元 (送信者)	送信先 (リスナー)	接続先ポート	目的
エンドポイント/IM and Presence	[IM and Presence]	7	Internet Control Message Protocol (ICMP)。このプロトコル番号がエコー関連のトラフィックを伝送します。列見出しに示すようなポートとなるものではありません。
[IM and Presence]	エンドポイント/IM and Presence		

表 87: IM and Presence に使用されるポート - Cisco Unified CM コミュニケーションおよび IM and Presence の発行者 - サブスクリバコミュニケーション

送信元 (送信者)	送信先 (リスナー)	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[TCP]	1500	双方向	データベースクライアント用の内部 ID ポート。ローカルホストトラフィック専用。
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[TCP]	8443	双方向	Web 管理へのアクセスを提供します。
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[TCP]	1090	双方向	AMC RMI オブジェクトポート RTMT パフォーマンス モニタ、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。

送信元 (送信者)	送信先 (リッシー)	トランスポートプロトコル	宛先/リッシー	ソース/送信元	備考
Cisco Unified Communications Manager	IM and Presence パブリッシー	[TCP]	2555	双方向	Bi-directional Real-time Information Services (RIS) データベースサーバ。クラスタ内の他の RISDC サービスに接続し、クラスタ全体のリアルタイム情報を提供します。
Cisco Unified Communications Manager	IM and Presence パブリッシー	[TCP]	8500	双方向	内部ポート : ipsec_mgr デーモンがプラットフォームデータ (ホスト) の証明書のクラスタレプリケーションに使用するクラスタマネージャポートです。
Cisco Unified Communications Manager	IM and Presence パブリッシー	[TCP]	8600	双方向	設定エージェントのハートビートポート
Cisco Unified Communications Manager	IM and Presence パブリッシー	UDP	123	双方向	時間同期に使用されるネットワークタイムプロトコル (NTP)。
IM and Presence パブリッシー	IM and Presence サブスクライバ	UDP	50000	双方向	内部ポート。ローカルホストトラフィック専用。LiveBus メッセージングポート。IM and Presence サービスは、このポートをクラスタ通信に使用します。
IM and Presence パブリッシー	IM and Presence サブスクライバ	UDP	219999	双方向	Cisco Server Recovery Manager がピアとの通信に使用するポート。
IM and Presence パブリッシー	Cisco Unified Communications Manager	TCP	4040	双方向	DRF マスター エージェント サーバポートは、ローカルエージェントの GUI および CLI からの接続を受け入れます。

送信元 (送信者)	送信先 (リスナー)	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence パブリッシャ	Cisco Unified Communications Manager	TCP	8001	双方向	永続チャットの構成中に使用されます。
IM and Presence パブリッシャ	Cisco Unified Communications Manager	TCP	6379	双方向	マネージドファイル転送 (MFT) の構成時に使用されます。
IM and Presence パブリッシャ	IM and Presence サブスクライバ	[TCP]	7	双方向	外部データベース (MSSQL) の構成中に使用されます。
IM and Presence パブリッシャ	IM and Presence サブスクライバ	[TCP]	20075	双方向	Cisco Server Recovery Manager が管理 RPC 要求を行うために使用するポート。
IM and Presence パブリッシャ	IM and Presence サブスクライバ	[TCP]	8600	双方向	設定エージェントのハートビートポート
IM and Presence サブスクライバ	IM and Presence パブリッシャ	[TCP]	9005	双方向	Cisco SIP Registration Datastore デュアルノードプレゼンス冗長グループの複製。
IM and Presence サブスクライバ	IM and Presence パブリッシャ	[TCP]	9003	双方向	Cisco Presence Datastore デュアルノードプレゼンス冗長グループの複製。
IM and Presence サブスクライバ	IM and Presence パブリッシャ	[TCP]	20075	双方向	Cisco Server Recovery Manager が管理 RPC 要求を行うために使用するポート。
IM and Presence サブスクライバ	IM and Presence パブリッシャ	[TCP]	9004	双方向	Cisco Login Datastore デュアルノードプレゼンス冗長グループの複製。
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[TCP]	5070	双方向	コール設定で使用されます

送信元（送信者）	送信先（リシナー）	トランスポートプロトコル	宛先/リシナー	ソース/送信元	備考
IM and Presence パブリッシャ	IM and Presence サブスクライバ	[TCP]	44000	双方向	コール設定で使用されます

SNMP については、『Cisco Unified Serviceability アドミニストレーションガイド』を参照してください。



第 36 章

追加の要件

- [ハイ アベイラビリティ ログイン プロファイル \(505 ページ\)](#)
- [単一クラスタ コンフィギュレーション \(508 ページ\)](#)
- [XMPP 標準への準拠 \(515 ページ\)](#)
- [設定変更通知およびサービス再起動通知 \(516 ページ\)](#)

ハイ アベイラビリティ ログイン プロファイル

ハイ アベイラビリティ ログイン プロファイルに関する重要事項

- この項のハイ アベイラビリティ ログイン プロファイル テーブルを使用して、プレゼンス冗長グループのクライアント再ログインの上限値と下限値を設定できます。[Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] > [システム (System)] > [サービス パラメータ (Service Parameters)] を選択し、[サービス (Service)] メニューから [Cisco Server Recovery Manager] を選択して、クライアント ログインの上限値と下限値を設定します。
- ハイ アベイラビリティ クライアント ログイン プロファイルは、単一クラスタの展開でのみ適用されます。複数のクラスタが存在する場合、ハイ アベイラビリティ クライアント ログイン プロファイルには、冗長グループの上位および下位のクライアントの再ログイン値を設定することはできません。複数のクラスタ展開でハイ アベイラビリティ クライアント ログイン プロファイルを検出するには、さらにテストを実行する必要があります。
- Cisco XCP ルータ サービスのデバッグ ロギングが有効になっている場合は、CPU の使用率が増加し、IM and Presence Service に関して現在サポートされているログ レベルが低下することを予告する必要があります。
- ここに示すテーブルに基づいてプレゼンス冗長グループのクライアント再ログインの上限と下限を設定することで、展開のパフォーマンスの問題および高 CPU スパイクを回避できます。

- 各 IM and Presence Service ノードのメモリ サイズおよび各ハイアベイラビリティ展開タイプ（アクティブ/アクティブまたはアクティブ/スタンバイ）用にハイアベイラビリティログインプロファイルを提供します。
- ハイアベイラビリティログインプロファイルテーブルは、次の入力に基づいて計算されます。
 - クライアント再ログインの下限は、Server Recovery Manager のサービスパラメータ「重要なサービス停止遅延（Critical Service Down Delay）」に基づいており、デフォルトは90秒です。重要なサービス停止遅延（Critical Service Down Delay）が変更されると、下限も必ず変わります。
 - アクティブ/スタンバイ展開のプレゼンス冗長グループ内のユーザ合計数、またはアクティブ/アクティブ展開のユーザが最も多いノード。
- プレゼンス冗長グループ内の両方のノードで、クライアント再ログインの上限値と下限値を設定する必要があります。プレゼンス冗長グループの両方のノードでこれらの値をすべて手動で設定する必要があります。
- クライアント再ログインの上限値と下限値は、プレゼンス冗長グループの各ノードで同じである必要があります。
- ユーザを再平衡化する場合は、ハイアベイラビリティログインプロファイルテーブルに基づくクライアント再ログインの上限値と下限値を再設定する必要があります。

ハイアベイラビリティログインプロファイルテーブルの使用

ハイアベイラビリティログインプロファイルテーブルを使用して、次の値を取得します。

- [クライアント再ログインの下限（Client Re-Login Lower Limit）] サービスパラメータ値
- [クライアント再ログインの上限（Client Re-Login Upper Limit）] サービスパラメータ値

手順

- ステップ 1** 仮想ハードウェア設定およびハイアベイラビリティ展開タイプに基づいてプロファイルテーブルを選択します。
- ステップ 2** プロファイルテーブルで、展開内のユーザ数を選択します（最も近い値に切り上げ）。アクティブ/スタンバイ展開を使用している場合、ユーザが最も多いノードを使用します。
- ステップ 3** プレゼンス冗長グループの[ユーザ数（Number of Users）]の値に基づいて、プロファイルテーブル内の対応する再試行の下限値と上限値を取得します。
- ステップ 4** [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]> [システム（System）]> [サービスパラメータ（Service Parameters）]を選択し、[サービス（Service）]メニューから [Cisco Server Recovery Manager] を選択して、IM and Presence Service の再試行の下限値と上限値を設定します。

ステップ 5 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] > [システム (System)] > [サービス パラメータ (Service Parameters)] を選択し、[サービス (Service)] メニューから [Cisco Server Recovery Manager] を選択して [重要なサービス停止 (Critical Service Down Delay)] の値を確認します。デフォルト値は 90 秒です。再試行下限値はこの値に設定してください。

高可用性 ログイン設定の例

例 1 : ユーザ数 15,000 のフル UC プロファイル - アクティブ/アクティブ展開

プレゼンス冗長グループ内のユーザが 3,000 人で、あるノードに 2,000 人、2 台目のノードに 1,000 人のユーザがいます。非平衡型のアクティブ/アクティブ展開の場合、シスコはユーザが最も多いノード（この場合は、2,000 人のユーザが割り当てられているノード）を使用することを推奨します。ユーザ数 15,000 のフル米国 (4 vCPU 8 GB) アクティブ/アクティブプロファイルを使用して、次の再試行の下限値と上限値を取得します。

アクティブ ユーザの予想数	再試行下限値	再試行上限値
2000	120	253



(注) 再試行上限値は、フェールオーバー発生後にすべてのクライアントがバックアップノードにログインするまでのおおよその時間（秒）です。



(注) 120 の下限値は、[重要なサービス停止遅延 (Critical Service Down Delay)] サービスパラメータが 120 に設定されていることを前提としています。

例 2 : ユーザ数 5000 のフル UC プロファイル - アクティブ/アクティブ展開

プレゼンス冗長グループ内の各ノードに 4,700 人のユーザがいます。シスコは、最も近い値に切り上げ、ユーザ数 5,000 のフル米国 (4 vCPU 8 GB) アクティブ/アクティブプロファイルを使用して、ユーザ数 5,000 に基づいて、再試行の下限値と上限値を取得することを推奨します。

アクティブ ユーザの予想数	再試行下限値	再試行上限値
5000	120	953

単一クラスタ コンフィギュレーション

500 ユーザ フル UC (1vCPU 700MHz 2GB) のアクティブ/アクティブ プロファイル

表 88: 標準展開 (500 ユーザ フル UC のアクティブ/アクティブ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	187
250	120	287

500 ユーザ フル UC (1vCPU 700MHz 2GB) のアクティブ/スタンバイ プロファイル

表 89: 標準展開 (500 ユーザ フル UC のアクティブ/スタンバイ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	187
250	120	287
500	120	453

1000 ユーザ フル UC (1vCPU 1500MHz 2GB) のアクティブ/アクティブ プロファイル

表 90: 標準展開 (1000 ユーザ フル UC のアクティブ/アクティブ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153
250	120	203
500	120	287

1000 ユーザフル UC (1vCPU 1500MHz 2GB) のアクティブ/スタンバイ プロファイル

表 91: 標準展開 (1000 ユーザフル UC のアクティブ/スタンバイ) のユーザ ログイン再試行制限

アクティブユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153
250	120	203
500	120	287
750	120	370
[1000]	120	453

2000 ユーザフル UC (1vCPU 1500Mhz 4GB) のアクティブ/アクティブプロファイル

表 92: 標準展開 (2000 ユーザフル UC のアクティブ/アクティブ) のユーザ ログイン再試行制限

アクティブユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153
500	120	287
[1000]	120	453

2000 ユーザフル UC (1vCPU 1500Mhz 4GB) のアクティブ/スタンバイ プロファイル

表 93: 標準展開 (2000 ユーザフル UC のアクティブ/スタンバイ) のユーザ ログイン再試行制限

アクティブユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153
250	120	203

アクティブユーザの予想数	再試行下限値	再試行上限値
500	120	287
750	120	370
[1000]	120	453
1250	120	537
1500	120	620
1750	120	703
2000	120	787

5000 ユーザフル UC (4 GB 2vCPU) のアクティブ/アクティブ プロファイル

表 94: 標準展開 (5000 ユーザフル UC のアクティブ/アクティブ) のユーザログイン再試行制限

アクティブユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	137
500	120	203
[1000]	120	287
1500	120	370
2000	120	453
2500	120	537

5000 ユーザフル UC (4 GB 2vCPU) のアクティブ/スタンバイ プロファイル



注目 5000 ユーザシステムで最大のクライアントログインスループットを実現するために、シスコでは、少なくとも 2.6 GHz の CPU クロック速度を推奨しています。

表 95: 標準展開 (5000 ユーザフル UC のアクティブ/スタンバイ) のユーザログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	154
500	120	287
[1000]	120	453
1500	120	620
2000	120	787
2500	120	953
3000	120	1120
3500	120	1287
4000	120	1453
4500	120	1620
5000	120	1787

15000 ユーザフル UC (4 vCPU 8GB) のアクティブ/アクティブ プロファイル

注目 15000 ユーザ システムで最大のクライアント ログインスループットを実現するために、シスコでは、少なくとも 2.5GHz の CPU クロック速度を推奨しています。

表 96: 標準展開 (15000 ユーザフル UC のアクティブ/アクティブ) のユーザログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	127
500	120	153
[1000]	120	187
1500	120	220
2000	120	253
2500	120	287
3000	120	320

アクティブユーザの予想数	再試行下限値	再試行上限値
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
7500	120	620

15000 ユーザフル UC (4 vCPU 8GB) のアクティブ/スタンバイ プロファイル

注目 15000 ユーザ システムで最大のクライアントログインスループットを実現するために、シスコでは、少なくとも 2.5GHz の CPU クロック速度を推奨しています。

表 97: 標準展開 (15000 ユーザフル UC のアクティブ/スタンバイ) のユーザログイン再試行制限

アクティブユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	137
500	120	203
[1000]	120	287
1500	120	370
2000	120	453
2500	120	537
3000	120	620
3500	120	703
4000	120	787
4500	120	870
5000	120	953
6000	120	1120
7000	120	1287

アクティブ ユーザの予想数	再試行下限値	再試行上限値
8000	120	1453
9000	120	1620
10000	120	1787
11000	120	1953
12000	120	2120
13000	120	2287
14000	120	2453
15000	120	2620

25000 ユーザフル UC (6 vCPU 16GB) のアクティブ/アクティブ プロファイル



注目 25000 ユーザ システムで最大のクライアント ログインスループットを実現するために、システムでは、少なくとも 2.8GHz の CPU クロック速度を推奨しています。

表 98: アクティブ/アクティブ プロファイルのログイン率 : 9 ユーザが 45% の CPU を使用

アクティブ ユーザの予想数	再試行下限値	再試行上限値
100	120	131
500	120	176
[1000]	120	231
1500	120	287
2000	120	342
2500	120	398
3000	120	453
3500	120	509
4000	120	564
4500	120	620
5000	120	676

アクティブ ユーザの予想数	再試行下限値	再試行上限値
6000	120	787
7000	120	898
7500	120	953
8000	120	1009
9000	120	1120
10000	120	1231
11000	120	1342
12000	120	1453
12500	120	1509

25000 ユーザフル UC (6vCPU16GB) のアクティブ/スタンバイ プロファイル



注目 25000 ユーザ システムで最大のクライアント ログインスループットを実現するために、システムでは、少なくとも 2.5GHz の CPU クロック速度を推奨しています。

表 99: アクティブ/スタンバイプロファイルのログイン率 : 16 ユーザが 80% の CPU を使用

アクティブ ユーザの予想数	再試行下限値	再試行上限値
100	120	133
500	120	183
[1000]	120	245
1500	120	308
2000	120	370
2500	120	433
3000	120	495
3500	120	558
4000	120	620
4500	120	683

アクティブユーザの予想数	再試行下限値	再試行上限値
5000	120	745
6000	120	870
7000	120	995
8000	120	1058
9000	120	1120
10000	120	1245
11000	120	1370
12000	120	1495
13000	120	1620
14000	120	1870
15000	120	1995
16000	120	2120
17000	120	2245
18000	120	2370
19000	120	2495
20000	120	2620
21000	120	2745
22000	120	2870
23000	120	2995
24000	120	3120
25000	120	3245

XMPP 標準への準拠

IM and Presence サービスは次の XMPP 標準に準拠しています。

- RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core RFC 3921 Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence
 - XEP-0004 Data Forms
 - XEP-0012 Last Activity

- XEP-0013 Flexible Offline Message Retrieval
- XEP-0016 Privacy Lists
- XEP-0030 Service Discovery
- XEP-0045 Multi-User Chat
- XEP-0054 Vcard-temp
- XEP-0055 Jabber Search
- XEP-0060 Publish-Subscribe
- XEP-0065 SOCKS5 Bystreams
- XEP-0066 Out of Band Data Archive OOB requests
- XEP-0068 Field Standardization for Data Forms
- XEP-0071 XHTML-IM
- XEP-0082 XMPP Date and Time Profiles
- XEP-0092 Software Version
- XEP-0106 JID Escaping
- XEP-0114 Jabber Component Protocol
- XEP-0115 Entity Capabilities
- XEP-0124 Bidirectional Streams over Synchronous HTTP (BOSH)
- XEP-0126 Invisibility
- XEP-0128 Service Discovery Extensions
- XEP-0160 Best Practices for Handling Offline Messages
- XEP-0163 Personal Eventing Via PubSub
- XEP-0170 Recommended Order of Stream Feature Negotiation
- XEP-0178 Best Practices for Use of SASL EXTERNAL
- XEP-0220 Server Dialback
- XEP-0273 SIFT (Stanza Interception and Filtering Technology)

設定変更通知およびサービス再起動通知

サービスを再起動する必要がある場合は、[アクティブな通知 (Active Notifications)] ポップアップが表示されます。Cisco Unified CM IM and Presence Administration GUI ヘッダーの右上に、[アクティブな通知の概要 (Active Notifications Summary)] があります。

さらに、Cisco Unified CM IM and Presence の管理インターフェイスから [システム (System)]> [通知 (Notifications)] を選択することで、アクティブな通知リストにアクセスできます。

再起動が必要な設定の変更

多くの IM and Presence 設定の変更および更新では、Cisco XCP ルータ、Cisco SIP プロキシ、または Cisco Presence Engine を再起動する必要があります。

次の表に、これらのサービスの再起動が必要な設定の変更を示します。このリストには設定の変更が含まれていますが、インストールやアップグレードなどのプラットフォームの変更は含まれていません。

再起動を必要とする設定	再起動するサービス
アプリケーション リスナーの設定 ([システム (System)]>[アプリケーションリスナー (Application Listeners)]) アプリケーション リスナーの編集	Cisco SIP Proxy
コンプライアンス プロファイルの設定 ([メッセージング (Messaging)]>[コンプライアンス (Compliance)]>[コンプライアンス設定 (Compliance Settings)]) ([メッセージング (Messaging)]>[コンプライアンス (Compliance)]>[コンプライアンスプロファイル (Compliance Profiles)]) サードパーティのコンプライアンスサーバに割り当てられているイベントの設定を編集する場合	Cisco XCP Router
グループチャットのシステム管理者 ([メッセージング (Messaging)]>[グループチャットのシステム管理者 (Group Chat System Administrators)]) この設定を有効または無効にする場合	Cisco XCP Router
外部ファイルサーバの設定 ([メッセージング (Messaging)]>[外部サーバの設定 (External Server Setup)]>[外部ファイルサーバ (External File Servers)]) [ホスト/IPアドレス設定 (Host/IP Address Setting)] を編集する場合 [外部ファイルサーバパブリックキー (External File Server Public Key)] を再生成する場合	Cisco XCP Router

再起動を必要とする設定	再起動するサービス
グループチャットと持続チャットの設定 ([メッセージング (Messaging)] > [グループチャットと持続チャット (Group Chat and Persistent Chat)]) 起動時にチャットノードが外部DBに到達できない場合、Cisco XCP Text Conference Mgr サービスは実行されていません。	Cisco XCP Router
グループチャットサーバエイリアスマッピング ([メッセージング (Messaging)] > [グループチャットサーバエイリアスマッピング (Group Chat Server Alias Mapping)]) チャットエイリアスの追加	Cisco XCP Router
ACL 設定 ([システム (System)] > [セキュリティ (Security)] > [着信ACL (Incoming ACL)]) ([システム (System)] > [セキュリティ (Security)] > [発信ACL (Outgoing ACL)]) 着信または発信 ACL 設定の編集	Cisco SIP Proxy
コンプライアンス設定 [メッセージアーカイバ (Message Archiver)]: 設定の編集	Cisco XCP Router
LDAP サーバ (LDAP Server) ([アプリケーション (Application)] > [サードパーティクライアント (Third-Party Clients)] > [サードパーティLDAP設定 (Third-party LDAP Settings)]) [LDAP検索 (LDAP Search)]: LDAP 検索の編集 [LDAPからvCardを作成 (Build vCards from LDAP)] の編集 vCard FN に使用するための LDAP 属性の編集	Cisco XCP Router
メッセージ設定の構成 ([メッセージング (Messaging)] > [設定 (Settings)]) [インスタントメッセージの有効化 (Enable instant message)] の編集 オフライン中の相手へのインスタントメッセージの送信を無効にする	Cisco XCP Router

再起動を必要とする設定	再起動するサービス
<p>Microsoft RCC 設定</p> <p>([アプリケーション (Application)] > [Microsoft RCC] > [設定 (Settings)])</p> <p>このページのいずれかの設定の編集</p>	Cisco SIP Proxy
<p>プレゼンス ゲートウェイ (Presence Gateway)</p> <p>([プレゼンス (Presence)] > [ゲートウェイ (Gateways)])</p> <p>プレゼンス ゲートウェイの追加、編集、削除</p> <p>MS Exchange 証明書をアップロードした後</p>	Cisco Presence Engine
<p>プレゼンス設定の構成</p> <p>([プレゼンス (Presence)] > [設定 (Settings)] > [標準設定 (Standard Configuration)])</p> <p>[プレゼンスステータスの共有を有効にする (Enable Availability Sharing)] 設定の編集</p> <p>確認プロンプトなしで、ユーザが他のユーザのプレゼンスステータスを表示できるようにする</p> <p>連絡先リストの最大サイズ (ユーザごと) (Maximum Contact List Size (per user))</p> <p>[ウォッチャの最大数 (Maximum Watchers)]</p>	Cisco Presence Engine Cisco XCP Router
<p>プレゼンス設定の構成</p> <p>([プレゼンス (Presence)] > [設定 (Settings)] > [標準設定 (Standard Configuration)])</p> <p>[イントラドメインフェデレーションで電子メールアドレスのユーザを有効にする (Enable user of Email address for Interdomain Federation)] フィールドの編集</p>	Cisco XCP Router

再起動を必要とする設定	再起動するサービス
<p>パーティションイントラドメイン フェデレーションの設定</p> <p>[プレゼンス (Presence)]>[設定 (Settings)]>[標準設定 (Standard Configuration)] (チェックボックス)</p> <p>[プレゼンス (Presence)]>[イントラドメインフェデレーションのセットアップ (Intradomain Federation Setup)] (ウィザード)</p> <p>チェックボックスまたはウィザードを使用した [LCS/OCS/Lync とのパーティションイントラドメインフェデレーションを有効にする (Enable Partitioned Intradomain Federation with LCS/OCS/Lync)] の設定</p> <p>パーティションイントラドメインルーティングモード:[標準設定 (Standard Configuration)]ウィンドウまたはウィザードを使用した設定</p>	<p>これらの設定を編集すると、Cisco SIP プロキシが自動的に再起動します</p> <p>さらに、XCP ルータを再起動する必要があります</p>
<p>プロキシ設定</p> <p>([プレゼンス (Presence)]>[ルーティング (Routing)]>[設定 (Settings)])</p> <p>プロキシ設定へのいずれかの編集</p>	Cisco SIP Proxy
<p>セキュリティ設定</p> <p>([システム (System)]>[セキュリティ (Security)]>[設定 (Settings)])</p> <p>SIP イントラクラスタプロキシ間トランスポートプロトコルなどのいずれかの SIP セキュリティ設定の編集</p> <p>いずれかの XMPP セキュリティ設定の編集</p>	<p>Cisco SIP プロキシ (SIP セキュリティの編集の場合)</p> <p>Cisco XCP ルータ (XMPP セキュリティの編集の場合)</p>
<p>SIP フェデレーテッド ドメイン</p> <p>([プレゼンス (Presence)]>[ドメイン間フェデレーション (Interdomain Federation)]>[SIP フェデレーション (SIP Federation)])</p> <p>この設定の追加、編集、削除</p>	Cisco XCP Router
<p>サードパーティ製コンプライアンス サービス</p> <p>([アプリケーション (Application)]>[サードパーティクライアント (Third-Party Clients)]>[サードパーティLDAPサーバ (Third-Party LDAP Servers)])</p> <p>[ホスト名/IPアドレス (Hostname/IP Address)]、[ポート (Port)]、[パスワード/パスワードの確認 (Password/Confirm Password)] フィールドの編集</p>	Cisco XCP Router

再起動を必要とする設定	再起動するサービス
<p>TLS ピア サブジェクトの設定</p> <p>([システム (System)]>[セキュリティ (Security)]>[TLSピアサブジェクト (TLS Peer Subjects)])</p> <p>このページでのいずれかの編集</p>	<p>Cisco SIP Proxy</p>
<p>TLS コンテキスト (TLS Context)</p> <p>([システム (System)]>[セキュリティ (Security)]>[TLSコンテキスト設定 (TLS Context Configuration)])</p> <p>このページでのいずれかの編集</p>	<p>関連付けられているチャットサーバの再起動が必要な場合があります。</p>
<p>XMPP フェデレーション</p> <p>([プレゼンス (Presence)]>[ドメイン間フェデレーション (Interdomain Federation)]>[XMPPフェデレーション (XMPP Federation)]>[設定 (Settings)])</p> <p>([プレゼンス (Presence)]>[ドメイン間フェデレーション (Interdomain Federation)]>[XMPPフェデレーション (XMPP Federation)]>[ポリシー (Policy)])</p> <p>XMPP フェデレーションへのいずれかの編集</p>	<p>Cisco XCP Router</p>
<p>クラスタ間ピアリング</p> <p>(プレゼンス クラスタ間設定)</p> <p>クラスタ間ピア設定の編集</p>	<p>場合によっては、Cisco XCP ルータの再起動を求められる場合があります (右上のウィンドウに通知が表示されます)。</p>
<p>イーサネット設定</p> <p>([Cisco Unified IM and PresenceのOSの管理 (Cisco Unified IM and Presence OS Administration)]から、[設定 (Settings)]>[IP]>[イーサネット/イーサネットIPv6 (Ethernet/Ethernet IPv6)])</p> <p>いずれかのイーサネット設定の編集</p>	<p>システムが即時再起動されます</p>
<p>IPv6 設定 (IPv6 Configuration)</p> <p>([システム (System)]>[エンタープライズパラメータ (Enterprise Parameters)])</p> <p>[IPv6を有効化] エンタープライズパラメータの有効化の編集</p>	<p>Cisco XCP Router</p> <p>Cisco SIP Proxy</p> <p>Cisco Presence Engine</p>

再起動を必要とする設定	再起動するサービス
<p>トラブルシューティング</p> <p>サブスクライバがオフラインの間に IM and Presence パブリッシャが変更された場合</p> <p>サブスクライバからの [設定 (Settings)] > [IP] > [パブリッシャ (Publisher)] 設定の編集</p>	サブスクライバノードの再起動
IM and Presence をアップグレードすると、以前のバージョンに切り替える必要があります	システムを再起動する
cup 証明書の再生成	Cisco SIP Proxy Cisco Presence Engine
cup-xmpp の再生成	Cisco XCP Router
cup-xmpp-s2s 証明書の再生成	Cisco XCP Router
新しい証明書のアップロード	その証明書に関連するサービスを再起動します。 CUP 信頼証明書の場合は、Cisco SIP プロキシを再起動します。
<p>リモート監査ログの転送プロトコル</p> <p>utils remotesyslog set protocol * CLI コマンドのいずれかを実行した場合</p>	ノードの再起動
<p>次のアラートのいずれかを受け取った場合</p> <ul style="list-style-type: none"> • PEIDSQueryError • PEIDStoIMDBDatabaseSyncError • PEIDSSubscribeError • PEWebDAVInitializationFailure 	Cisco Presence Engine を再起動することを推奨します。
<p>次のアラートのいずれかを受け取った場合</p> <ul style="list-style-type: none"> • • XCPCConfigMgrJabberRestartRequired • XCPCConfigMgrR2RPasswordEncryptionFailed • XCPCConfigMgrR2RRequestTimedOut • XCPCConfigMgrHostNameResolutionFailed 	Cisco XCP ルータを再起動することを推奨します。

再起動を必要とする設定	再起動するサービス
PWSSCBIInitFailed	Cisco SIP プロキシを再起動することを推奨します。
いずれかの Exchange サービス パラメータの編集 <ul style="list-style-type: none"> • Microsoft Exchange 通知ポート (Microsoft Exchange Notification Port) • カレンダーの展開 (Calendar Spread) • Exchange タイムアウト (秒) (Exchange Timeout (seconds)) • Exchange キュー (Exchange Queue) • Exchange スレッド (Exchange Threads) • EWS ステータス頻度 (EWS Status Frequency) 	Cisco Presence Engine
Exchange 証明書のアップロード	Cisco SIP Proxy Cisco Presence Engine
ロケールのインストール	IM and Presence サービスの再起動
新しい MSSQL 外部データベースの作成	Cisco XCP Router
外部データベース設定の編集	Cisco XCP Router
外部データベースのマージ	Cisco XCP Router
TLS ピア サブジェクトの設定	Cisco SIP Proxy
ピア認証 TLS コンテキストの設定	Cisco SIP Proxy

再起動を必要とする設定	再起動するサービス
次の Cisco SIP プロキシ サービス パラメータの編集 <ul style="list-style-type: none"> • CUCMドメイン (CUCM Domain) • サーバ名 (補足) (Server Name (supplemental)) • HTTP ポート (HTTP Port) • ステートフルサーバ (トランザクションステートフル) (Stateful Server (transaction Stateful)) • 持続的TCP接続数 (Persist TCP Connections) • 共有メモリサイズ (バイト) (Shared memory size (bytes)) • フェデレーションルーティングIM/P FQDN (Federation Routing IM/P FQDN) • MicrosoftフェデレーションUser-Agentヘッダー (Microsoft Federation User-Agent Headers) (コンマ区切り) 	Cisco SIP Proxy
[ルーティング通信タイプ (Routing Communication Type)] サービスパラメータの編集	Cisco XCP Router
IM アドレス スキームの編集	Cisco XCP Router
デフォルト ドメインの割り当て	Cisco XCP Router
クラスタからのノードの削除	Cisco XCP Router
Cisco XCP ルータに影響するパラメータを編集する場合は、Cisco XCP ルータを再起動する必要があります	Cisco XCP Router
[ルーティング通信タイプ (Routing Communication Type)] サービスパラメータ	Cisco XCP Router
次のいずれかの [Cisco XCP File Transfer Manager] サービスパラメータの編集： <ul style="list-style-type: none"> • 外部ファイルサーバの使用可能領域の下限しきい値 (External File Server Available Space Lower Threshold) • 外部ファイルサーバの使用可能領域の上限しきい値 (External File Server Available Space Upper Threshold) 	Cisco XCP Router
[複数のデバイスメッセージングの有効化 (Enable Multiple Device Messaging)] サービスパラメータの編集	Cisco XCP Router
[ユーザあたりの最大ログオンセッション数 (Maximum number of logon sessions per user)] サービスパラメータの編集	Cisco XCP Router

再起動を必要とする設定	再起動するサービス
外部データベース上の <code>install_dir /data/pg_hba.conf</code> または <code>install_dir /data/postgresql.conf</code> 設定ファイルの更新	Cisco XCP Router
移行ユーティリティ： <ul style="list-style-type: none"> • [プレゼンスの設定 (Presence Settings)] ウィンドウでの [確認プロンプトなしで、ユーザが他のユーザのプレゼンスステータスを表示できるようにする (Allow users to view the availability of other users without being prompted for approval)] 設定の編集。 • [プレゼンスの設定 (Presence Settings)] 設定ウィンドウでの [連絡先リストの最大サイズ (ユーザごと) (Maximum Contact Lists Size (per user))] および [ウォッチャの最大数(ユーザごと) (Maximum Watchers (per user))] 設定の編集。 	Cisco XCP Router
クラスタからのノードの削除	Cisco XCP Router

