Cisco Unified Communications Manager IM and Presence Service リリース 12.0(1) 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 ガイド

初版：2017 年 8 月 17 日

最終更新：2019 年 9 月 20 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

マニュアルの変更履歴 xxi

第 I 部： 展開のプランニング 22

第 1 章 IM and Presence Service の機能 1

IM and Presence Service のコンポーネント 1

主要なコンポーネント 1

SIP インターフェイス 2

AXL/SOAP インターフェイス 3

LDAP インターフェイス 3

XMPP インターフェイス 3

CTI インターフェイス 4

Cisco IM and Presence Data Monitor 4

IM and Presence Service の機能展開オプション 5

展開モデル 8

シングルノード、マルチノード、および IM-Only での高可用性展開 8

プレゼンス冗長グループと高可用性 9

WAN 経由のクラスタリング 10

ユーザ割り当て 10

エンドユーザ管理 11

アベイラビリティとインスタントメッセージ 11

チャット（Chat） 11

IM 分岐 12

オフライン IM 12

ブロードキャスト IM 12
IM and Presence Service のチャット ルーム 12
チャット ルームの制限 13
ファイル転送 14
IM and Presence Service およびチャットに関する重要事項 14
IM コンプライアンス 14
プレゼンス データの概要 15
手動プレゼンス 15
システムが決定するプレゼンス 15
エンタープライズ グループ 16
LDAP 統合 17
サードパーティ統合 18
サードパーティ製クライアントの統合 19
サポートされているサードパーティ製 XMPP クライアント 19
サードパーティ製クライアントのライセンス要件 20
Cisco Unified Communications Manager での XMPP クライアント統合 20
XMPP 連絡先検索のための LDAP 統合 20
XMPP クライアントの DNS 設定 21
IPv6 のサポート 21
IM アドレス スキームとデフォルト ドメイン 22
UserID@Default_Domain を使用した IM アドレス 22
ディレクトリ URI を使用した IM アドレス 22
IM アドレスの例 23
Cisco Unified Communications Manager との IM アドレスの統合 24
Cisco Unified Communications Manager を使用した UserID@Default_Domain の統合 24
Cisco Unified Communications Manager を使用したディレクトリ URI の統合 25
複数の IM ドメインの管理 25
セキュリティ 25
SAML シングル サインオン 26

第 2 章 マルチノードの拡張性と WAN の展開 27

マルチノードの拡張性機能 27
マルチノードの拡張性要件 27
OVA 要件 28
展開の拡張性オプション 28
クラスタ全体の DNS SRV 30
ローカル フェールオーバー 31
プレゼンス冗長グループの障害検出 31
メソッド イベント ルーティング 31
外部データベースの推奨事項 32
クラスタ内およびクラスタ間展開における WAN 経由のクラスタリング 32
WAN 経由のクラスタ内展開 32
WAN 経由の展開のマルチノード設定 33
クラスタ間展開 33
WAN 経由のクラスタ間展開 33
クラスタ間ピア関係 34
クラスタ間ルータツールータ接続 34
クラスタ間展開のノード名の値 34
クラスタ間展開の IM and Presence のデフォルト ドメイン値 35
クラスタ間展開の IM アドレス スキーム 35
セキュアなクラスタ間ルータ ツー ルータ接続 36

第 3 章 **IM and Presence Service の計画の要件 37**
マルチノード ハードウェアの推奨事項 37
クラスタ間のハードウェアの推奨事項 38
サポートされているエンド ポイント 38
サポートされる LDAP ディレクトリ サーバ 39
WAN の帯域幅要件 39
WAN の帯域幅の考慮事項 40
マルチノードの拡張性とパフォーマンス 40
マルチノードの拡張性要件 40
マルチノード パフォーマンスの推奨事項 41

ユーザ ライセンスの要件 41
DNS ドメインとデフォルト ドメインの要件 41

第 4 章 ワークフロー 43
高可用性の基本的な展開のワークフロー 43
高可用性と IP Phone プレゼンスを備えた基本展開のワークフロー 46
フェデレーション展開のワークフロー 49

第 II 部 : システム設定（System Configuration） 53

第 5 章 IM and Presence Service と統合するための Cisco Unified Communications Manager の設定 55
統合前の Cisco Unified Communications Manager のユーザおよびデバイス設定のタスク リスト 55
プレゼンス グループ間登録パラメータの設定 58
Cisco Unified Communications Manager の SIP トランク設定 58
IM and Presence Service の SIP トランク セキュリティ プロファイルの設定 59
IM and Presence Service の SIP トランクの設定 59
クラスタ外の Unified Communications Manager の電話利用状況の設定 61
TLS ピア サブジェクトの設定 61
TLS コンテキストの設定 62
必要なサービスが Cisco Unified Communications Manager で実行されていることの確認 63

第 6 章 集中展開の設定 65
集中展開の概要 65
集中型クラスタの展開アーキテクチャ 68
集中型クラスタの使用例 69
集中展開の前提条件 69
集中展開設定のタスク フロー 71
機能グループ テンプレート経由の IM and Presence の有効化 73
IM and Presence 中央クラスタでの LDAP 同期の完了 74
一括管理を介した IM and Presence ユーザの有効化 75

リモート テレフォニー クラスタの追加 76
M and Presence UC Service の設定 77
IM and Presence のサービス プロファイルの作成 77
テレフォニー クラスタでのプレゼンス ユーザの無効化 78
OAuth 更新ログインの設定 79
ILS ネットワークの設定 80
ILS へのクラスタ ID の設定 81
テレフォニー クラスタでの ILS の有効化 81
ILS ネットワークが動作していることを確認する 83
MRA の設定 83
集中型の導入の相互作用および制限事項 85

第 7 章 **IM and Presence Service のネットワーク設定 87**
設定変更通知およびサービス再起動通知 87
サービス再起動通知 87
Cisco XCP Router の再起動 88
Cisco XCP Router サービスの再起動 88
高可用性でのサービスの再起動 88
DNS ドメイン コンフィギュレーション 89
別々の 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 90
別々の DNS ドメインまたはサブドメインに展開されたクラスタ内の IM and Presence Service ノード 91
関連する Cisco Unified Communications Manager クラスタとは異なる DNS ドメインに展開されているクラスタ内の IM and Presence Service ノード 91
Cisco Unified Communications Manager クラスタに関連付ける DNS ドメインの指定 92
IM and Presence Service のデフォルト ドメインの設定 93
IM アドレス設定 95
IM アドレスの設定要件 95
UserID @ Default_Domain IM アドレス インタラクションと制約事項 96
ディレクトリ URI IM アドレスの連携動作と制約事項 96
IM アドレス タスク フローの設定 97

サービスの停止 99
IM アドレス スキームの割り当て 100
サービスの再起動 101
IM and Presence Service クラスタのドメイン管理 102
IM ドメイン管理のインタラクションと制約事項 103
IM アドレス ドメインの表示 103
IM アドレス ドメインの追加または更新 104
IM アドレス ドメインの削除 105
IM and Presence Service のルーティング情報の設定 106
ルーティング通信の推奨事項 106
MDNS ルーティングとクラスタ ID の設定 106
ルーティング通信の設定 107
クラスタ ID の設定 108
アベイラビリティ状態変更メッセージのスロットル レートの設定 109
IPv6 設定（IPv6 Configuration） 110
IPv6 連携動作と制約事項 110
IM and Presence Service の Eth0 での IPv6 の有効化 111
IM and Presence Service の Eth0 での IPv6 の無効化 112
IPv6 エンタープライズ パラメータの有効化 113
プロキシ サーバの設定 114
IM and Presence Service のサービス 114
IM and Presence Service のサービスのオン 114

第 8 章 **IP Phone Presence の設定** 117
IM and Presence Service のスタティック ルート設定 117
ルート組み込みテンプレート 117
IM and Presence Service のルート組み込みテンプレートの設定 118
IM and Presence Service のスタティック ルートの設定 119
IM and Presence Service のプレゼンス ゲートウェイの設定 124
プレゼンス ゲートウェイの設定オプション 124
プレゼンス ゲートウェイの設定 125

IM and Presence Service の SIP パブリッシュ トランクの設定 126
SIP パブリッシュ トランクのクラスタ全体の DNS SRV 名の設定 126

第 9 章 LDAP ディレクトリ統合 129
LDAP サーバ名、アドレス、およびプロファイル設定 129
Cisco Unified Communications Manager との LDAP ディレクトリの統合のタスク リスト 129
Cisco Unified Communications Manager と LDAP ディレクトリとの間のセキュア接続 130
ユーザ プロビジョニングのための LDAP 同期の設定 131
LDAP 認証サーバ証明書のアップロード 132
LDAP 認証の設定 133
IM and Presence Service と LDAP ディレクトリ間のセキュア接続の設定 134
システム トラブルシュータを使用した LDAP ディレクトリ接続の検証 134
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 135
LDAP アカウント ロックの問題 136
XMPP クライアントの LDAP サーバの名前とアドレスの設定 137
XMPP クライアントの LDAP 検索設定 139
Cisco XCP ディレクトリ サービスのオン 141

第 10 章 IM and Presence Service のセキュリティ設定 143
セキュリティ設定のタスク リスト 143
ログイン バナーの作成 145
IM and Presence Service の拡張 TLS 暗号化 146
RSA セキュリティ証明書による、拡張されたキー長のサポート 147
マルチサーバ証明書の概要 148
IM and Presence Service の証明書タイプ 148
IM and Presence Service と Cisco Unified Communications Manager 間の証明書交換の設定 151
セキュリティを設定するための前提条件 151
IM and Presence Service への Cisco Unified Communications Manager 証明書のインポート 151
SIP Proxy サービスの再起動 152
IM and Presence Service からの証明書のダウンロード 153

Cisco Unified Communications Manager への IM and Presence Service 証明書のアップロード 153
Cisco Unified Communications Manager サービスの再起動 154
IM and Presence Service へのマルチサーバ CA 署名付き証明書のアップロード 154
IM and Presence Service への単一サーバ CA 署名付き証明書のアップロード 155
CA 署名付きの Tomcat 証明書のタスク リスト 155
署名を行う認証局のルート証明書および中間証明書のアップロード 156
Cisco Intercluster Sync Agent サービスの再起動 156
他のクラスタに CA 証明書が同期されていることの確認 157
各 IM and Presence Service ノードへの署名付き証明書のアップロード 158
Cisco Tomcat サービスの再起動 159
クラスタ間同期の確認 159
CA 署名付き cup-xmpp 証明書のアップロード 160
署名を行う認証局のルート証明書および中間証明書のアップロード 160
Cisco Intercluster Sync Agent サービスの再起動 161
他のクラスタに CA 証明書が同期されていることの確認 162
各 IM and Presence Service ノードへの署名付き証明書のアップロード 163
すべてのノードの Cisco XCP Router サービスの再起動 164
CA 署名付き cup-xmpp-s2s 証明書のアップロード 164
署名を行う認証局のルート証明書および中間証明書のアップロード 164
他のクラスタに CA 証明書が同期されていることの確認 165
フェデレーション ノードへの署名付き証明書のアップロード 166
Cisco XCP XMPP Federation Connection Manager サービスの再起動 167
自己署名の信頼証明書の削除 168
IM and Presence Service からの自己署名信頼証明書の削除 168
Cisco Unified Communications Manager からの自己署名 Tomcat 信頼証明書の削除 169
IM and Presence Service での SIP セキュリティの設定 170
TLS ピア サブジェクトの設定 170
TLS コンテキストの設定 171
TLS 暗号のマッピングの設定 172
IM and Presence Service での XMPP セキュリティの設定 173

XMPP セキュリティ モード 173
IM and Presence Service と XMPP クライアント間のセキュア接続の設定 175
IM and Presence Service のオンによる XMPP クライアントのサポート 176
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 177

第 11 章 クラスタ間ピアの設定 179
クラスタ間展開の前提条件 179
クラスタ間ピアの設定 180
クラスタ間ピアの設定 180
Intercluster Sync Agent のオン 181
クラスタ間ピア ステータスの確認 182
Intercluster Sync Agent の Tomcat 信頼証明書の更新 183
クラスタ間ピア接続を削除する 183
クラスタ間ピアリングの連携動作と制限事項 184

第 III 部 : 機能設定 185

第 12 章 IM and Presence Service 設定のアベイラビリティとインスタント メッセージ 187
IM and Presence Service のアベイラビリティの設定 187
IM and Presence Service クラスタのプレゼンス ステータス共有のオン/オフ 187
一時的（アドホック）プレゼンス登録の設定 188
ユーザごとの連絡先リストの最大サイズの設定 189
ユーザごとの最大ウォッチャ数の設定 190
IM and Presence Service での IM 設定 191
IM and Presence Service クラスタのインスタント メッセージのオン/オフ 191
オフライン インスタント メッセージのオン/オフ 192
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 192
インスタント メッセージでのカット アンド ペーストの許可 193
アベイラビリティおよびインスタント メッセージング連携動作および制限事項 194

第 13 章 アドホック チャットおよび常設チャットの設定 195

グループ チャットルームの概要 195
グループ チャットの要件 196
グループ チャットおよび常設チャットのタスク フロー 197
グループ チャット システム管理の設定 197
常設チャット ルームの設定 198
Cisco XCP Text Conference Manager の再起動 199
常設チャット用の外部データベースの設定 200
外部データベース接続の追加 201
グループ チャットと常設チャットのインタラクションと制限 201
常設チャットの例（高可用性なし） 205
IM and Presence での常設チャットの境界 206

第 14 章 IM and Presence Service での常設チャットの高可用性 211
常設チャットにおける高可用性の概要 211
常設チャットにおける高可用性のフロー 212
常設チャットにおける高可用性のフェールオーバー フロー 213
常設チャット ルームの高可用性フォールバック フロー 214
常設チャットにおける高可用性の有効化と確認 215
常設チャットの高可用性のための外部データベース 216
外部データベースのテーブルのマージ 217
外部データベースのマージ ツール 217

第 15 章 マネージド ファイル転送 219
マネージド ファイル転送 219
サポート対象のソフトウェア 219
ファイル転送のフロー 220
特記事項 221
外部データベース 222
特記事項 223
外部データベースのディスク使用量 223
外部ファイル サーバ 224

外部ファイル サーバの要件 225
ユーザ認証 226
パブリック キーとプライベート キー 226
ファイル サーバ ディレクトリ 227
ファイル サーバの管理 228
マネージド ファイル転送サービスのパラメータ 230
Cisco XCP File Transfer Manager RTMT のアラームとカウンタ 230
XCP File Transfer Manager のアラームの設定 232
マネージド ファイル転送のワークフロー 233
IM and Presence Service での外部データベース インスタンスの設定 233
外部ファイル サーバのセットアップ 236
前提条件 236
ユーザの設定 237
ディレクトリの設定 238
パブリック キーの取得 239
IM and Presence Service での外部ファイル サーバ インスタンスの設定 240
ファイル サーバのトラブルシューティング テスト 242
IM and Presence Service でのマネージド ファイル転送の有効化 243
マネージド ファイル転送のトラブルシューティング 247
Cisco Jabber クライアントの相互運用性 247
単一ノード - マネージド ファイル転送 248
単一ノード - マネージドおよびピアツーピア ファイル転送 249
単一クラスタ - 混合ノード 251
複数のクラスタ - 混合ノード 252
グループ チャット 253
Jabber クライアント用のモバイルおよびリモート アクセス 254

第 16 章 **Multiple Device Messaging** 257
Multiple Device Messaging の概要 257
Multiple Device Messaging のフロー 258
Multiple Device Messaging における静音モードのフロー 258

Multiple Device Messaging の有効化 259
複数のデバイスのメッセージングのカウンタ 260
Multiple Device Messaging のインタラクションと制限 260

第 17 章 **iPhone および iPad での Cisco Jabber のプッシュ通知の設定** 261
プッシュ通知の概要 261
プッシュ通知の設定 264

第 IV 部 : **管理** 265

第 18 章 **チャットの設定と管理** 267
チャットの展開 267
チャットの展開シナリオ 1 267
チャットの展開シナリオ 2 268
チャットの展開シナリオ 3 268
チャットの展開シナリオ 4 269
チャット管理の設定 270
IM ゲートウェイ設定の変更 270
サインイン セッション数の制限 271
常設チャット ルームの設定 271
常設チャットの有効化 273
グループ チャット システム管理の設定 276
グループ チャットと常設チャットのデフォルト設定と復帰 277
チャット ノード エイリアスの管理 277
チャット ノードのエイリアス 277
重要な考慮事項 278
システムで生成されたチャット ノード エイリアスのオン/オフの切り替え 279
チャット ノードのエイリアスの手動管理 280
Cisco XCP Text Conference Manager のオン 282
チャット ルーム管理 283
チャット ルーム数の設定 283

メンバーの設定 283
アベイラビリティの設定 284
招待の設定 285
利用者数の設定 286
チャット メッセージの設定 287
モデレータが管理するルームの設定 288
履歴の設定 288
グループ チャットと常設チャットのインタラクションと制限 289

第 19 章 エンド ユーザの設定と処理 295
IM and Presence Service のエンド ユーザの設定と処理 295
IM and Presence Service の許可ポリシーの設定 295
IM and Presence Service の自動許可 295
ユーザ ポリシーおよび自動許可 296
IM and Presence Service の許可ポリシーの設定 297
ユーザ連絡先 ID の一括名前変更 298
ユーザ連絡先リストの一括エクスポート 300
非プレゼンス連絡先リストの一括エクスポート 302
ユーザ連絡先リストの一括インポート 303
連絡先リストの最大サイズの確認 305
BAT を使用した入力ファイルのアップロード 306
新しい一括管理ジョブの作成 307
一括管理ジョブの結果の確認 307
ユーザ非プレゼンス連絡先リストの一括インポート 308
BAT を使用した非プレゼンス連絡先の入力ファイルのアップロード 310
非プレゼンス連絡先リストの新しい一括管理ジョブの作成 310
重複するユーザ ID とディレクトリ URI の管理 311
ユーザ ID と ディレクトリ URI モニタリング 311
ユーザ ID と ディレクトリ URI のエラー状態 312
ユーザ ID と ディレクトリ URI の確認と変更 313
ユーザ ID と ディレクトリ URI CLI 検証の例 314

ユーザ チェック間隔の設定 314
システム トラブルシュータを使用したユーザ ID とディレクトリ URI の検証 315

第 20 章 ユーザの移行 317
IM and Presence Service クラスタ間のユーザの移行 317
古いエントリを削除する 318
ユーザ連絡先リストのエクスポート 319
IM and Presence Service のユーザの無効化 321
新しいクラスタへのユーザの移動 321
Cisco Unified Communications Manager で有効な LDAP 同期 321
Cisco Unified Communications Manager で有効ではない LDAP 同期 322
新しいクラスタの IM and Presence Service のユーザの有効化 322
ホーム クラスタでの連絡先リストのインポート 323

第 21 章 ユーザの中央展開への移動 325
ユーザの中央展開への移動の概要 325
中央クラスタ マイグレーションの要件となるタスク 325
中央クラスタ タスク フローへの移行 327
移行元クラスタからの連絡先リストのエクスポート 329
移行元クラスタの高可用性の無効化 330
IM and Presence の UC Service の設定 331
IM and Presence のサービス プロファイルの作成 332
テレフォニー クラスタでのプレゼンス ユーザの無効化 332
中央クラスタの OAuth 認証を有効にする 334
中央および移行クラスタのピア関係を削除する 334
Cisco Intercluster Sync Agent 335
機能グループ テンプレート経由の IM and Presence の有効化 335
中央クラスタでの LDAP 同期の完了 336
一括管理を介した IM and Presence ユーザの有効化 337
中央クラスタへの連絡先リストのインポート 338
Cisco Intercluster Sync Agentを起動する 339

中央クラスタの高可用性の有効化 340
移行クラスタの残りのピアを削除する 340

第 22 章 IM and Presence Service の多言語サポート設定 343
ロケールのインストール 343
ロケールのインストールに関する考慮事項 344
ロケール ファイル 345
IM and Presence Service へのロケール インストーラのインストール 345
エラー メッセージ 347
ローカライズされたアプリケーション 350

第 23 章 ブランディングのカスタマイズ 351
ブランディングの概要 351
ブランディングの前提条件 351
ブランディングの有効化 351
ブランディングの無効化 352
ブランディング ファイルの要件 353

第 V 部： IM and Presence Service のトラブルシューティング 357

第 24 章 高可用性のトラブルシューティング 359
手動によるフェールオーバー、フォールバック、リカバリ 359
手動フェールオーバーの開始 360
手動フォールバックの開始 360
手動リカバリの開始 361
プレゼンス冗長グループのノードのステータスの表示 362
ノード状態の定義 362
ノードの状態、原因、および推奨処置 364
高可用性でのサービスの再起動 372

第 25 章 UserID 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 375

重複したユーザ ID エラーの受信 375
重複または無効なディレクトリ URI エラーの受信 376

第 26 章 IM and Presence Service のトラブルシューティングに使用するトレース 379
トラブルシューティングでのトレースログの使用 379
トレースを使用した一般的な IM and Presence の問題 380
CLIを介した共通トレース 382
CLI 経由のトレースの実行 386
RTMT を介した共通トレース 387

第 VI 部 : 参考情報 389

第 27 章 Cisco Unified Communications Manager での TCP および UDP ポートの使用 391
Cisco Unified Communications Manager の TCP と UDP ポートの使用に関する概要 391
ポートの説明 393
Cisco Unified Communications Manager サーバがクラスタ間で使用するポート 393
共通サービス ポート 397
Cisco Unified Communications Manager と LDAP ディレクトリとの間のポート 401
CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求 401
Cisco Unified Communications Manager から電話機への Web 要求 402
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 403
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 405
アプリケーションと Cisco Unified Communications Manager との間の通信 408
CTL クライアントとファイアウォールとの通信 411
HP サーバ上の特殊なポート 411
ポート参照 411
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 411
IETF TCP/UDP ポート割り当てリスト 412
IP テレフォニー設定とポート使用に関するマニュアル 412

VMware ポート割り当てリスト 412

第 28 章 IM and Presence Service のポート使用状況の情報 413

IM and Presence Service ポートの使用方法の概要 413

テーブルで照合する情報 414

IM and Presence Service ポート リスト 414

付録 A： 高可用性 クライアント ログイン プロファイル 431

高可用性ログイン プロファイル 431

高可用性ログイン プロファイルに関する重要事項 431

高可用性ログイン プロファイル テーブルの使用 432

高可用性ログイン設定の例 433

単一クラスタ コンフィギュレーション 434

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 434

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 434

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 434

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 435

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 435

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 435

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 436

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 436

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 437

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 438

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 439

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 440

付録 B： 追加の要件 443

高可用性ログイン プロファイル 443

高可用性ログイン プロファイルに関する重要事項 443

高可用性ログイン プロファイル テーブルの使用 444

高可用性ログイン設定の例 445

単一クラスタ コンフィギュレーション 446
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 446
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 446
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 446
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 447
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 447
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 447
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 448
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 448
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 449
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 450
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 451
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 452
XMPP 標準への準拠 453
設定変更通知およびサービス再起動通知 454

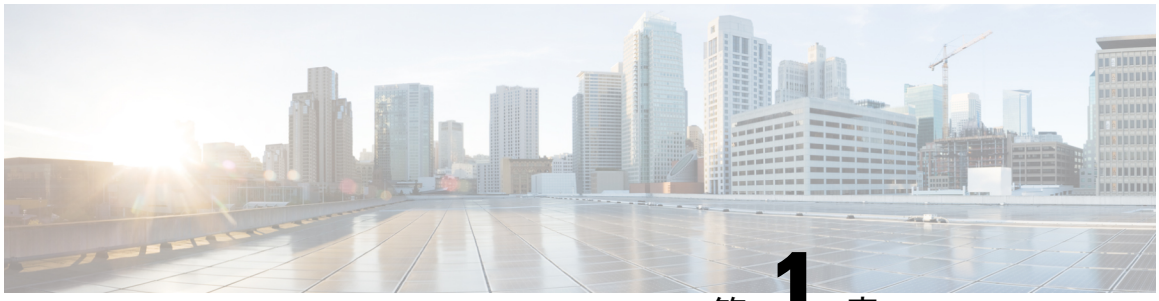
マニュアルの変更履歴

日付（**Date**）	リビジョン
2018 年 3 月 28 日	IM and Presence 集中型展開機能の前提条件を更新しました。
2018 年 4 月 12 日	制限されたバージョン要件を伴う管理ファイル転送機能が、MRA 経由の管理ファイル転送を使用するように更新されました。

第 I 部

展開のプランニング

- IM and Presence Service の機能 （1 ページ）
- マルチノードの拡張性と WAN の展開 （27 ページ）
- IM and Presence Service の計画の要件 （37 ページ）
- ワークフロー （43 ページ）



第 1 章

IM and Presence Service の機能

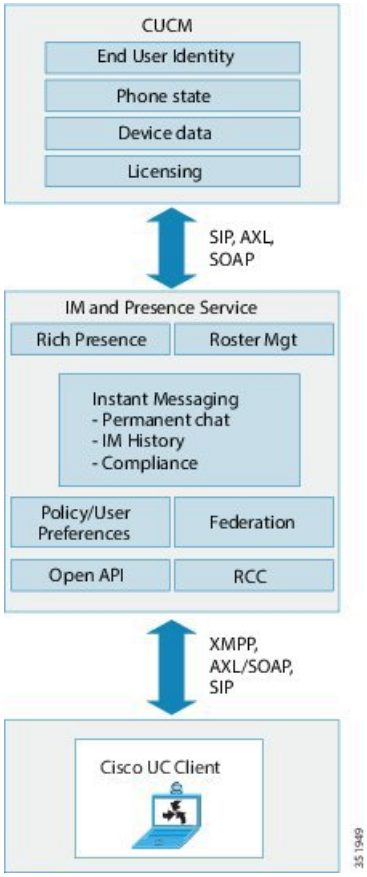
- IM and Presence Service のコンポーネント （1 ページ）
- IM and Presence Service の機能展開オプション （5 ページ）
- 展開モデル （8 ページ）
- ユーザ割り当て （10 ページ）
- エンド ユーザ管理 （11 ページ）
- アベイラビリティとインスタント メッセージ （11 ページ）
- エンタープライズ グループ （16 ページ）
- LDAP 統合 （17 ページ）
- サードパーティ統合 （18 ページ）
- サードパーティ製クライアントの統合 （19 ページ）
- IM アドレス スキームとデフォルト ドメイン （22 ページ）
- セキュリティ （25 ページ）
- SAML シングル サインオン （26 ページ）

IM and Presence Service のコンポーネント

主要なコンポーネント

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 接続は、Cisco Unified Communications Manager と Cisco Unified Presence 間のプレゼンス情報交換を処理します。Cisco Unified Communications Manager の SIP 接続を有効にするには、Cisco Unified 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。

Cisco Unified 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、Cisco Unified Presence は、SIP トランク経由で、SIP サブスクライブ メッセージを Cisco Unified Communications Manager に送信できます。

（注） Cisco Unified Presence は、TLS 経由で SIP/SIMPLE インターフェイスを使用することで Cisco Unified Presence に接続しているクライアント（シスコ クライアントまたはサードパーティ）をサポートしません。TCP 経由の SIP 接続だけがサポートされます。

関連トピック

Cisco Unified Communications Manager の SIP トランク設定 （58 ページ）
プレゼンス ゲートウェイの設定オプション （124 ページ）

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化するには、IM and Presence Service で Sync Agent サービスを起動する必要があります。

Sync Agent は、デフォルトでは M and Presence Service クラスタ内のすべてのノードにすべてのユーザを等しくロードバランシングします。また、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係動作がサポートされていません。

関連トピック

http://www.cisco.com/go/designzone

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。

関連トピック

LDAP ディレクトリ統合 （129 ページ）
LDAP サーバ名、アドレス、およびプロファイル設定 （129 ページ）
Cisco Unified Communications Manager と LDAP ディレクトリとの間のセキュア接続 （130 ページ）
XMPP クライアントの LDAP サーバの名前とアドレスの設定 （137 ページ）

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 Service は、XMPP ベースのクライアントの一時的（アドホック）および常設チャット ルームをサポートします。IM ゲートウェイは、IM and Presence

Service 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。

関連トピック

IM and Presence Service と XMPP クライアント間のセキュア接続の設定 （175 ページ）

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 Office Communicator クライアントの IM and Presence Service リモート コール制御機能にも使用されます。リモート コール制御機能の設定については、「*Microsoft Office Communicator Call Control with Microsoft OCS for IM and Presence Service on Cisco Unified Communications Manager*」を参照してください。

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

Cisco IM and Presence Data Monitor は、IM and Presence Service の IDS の複製の状態を監視します。他の IM and Presence サービスは、IM and Presence Data Monitor に依存します。これらの依存サービスは、シスコのサービスを使用して、IDS の複製が安定した状態になるまで起動を遅らせます。

また、Cisco IM and Presence Data Monitor は Cisco Sync Agent の同期のステータスを Cisco Unified Communications Manager から確認します。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 PresenceData Monitor は機能サービスの起動を遅らせます。Cisco IM and Presence Data Monitor のみがクラスタ内の問題のあるサブスクライバ ノードの機能サービスの起動を遅らせます。問題のある 1 個のノードのためにすべてのサブスクライバ ノードの機能サービスの起動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、ソフトウェア更新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。

- 次の CLI コマンドを使用します。

  utils dbreplication runtimestate

- 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。

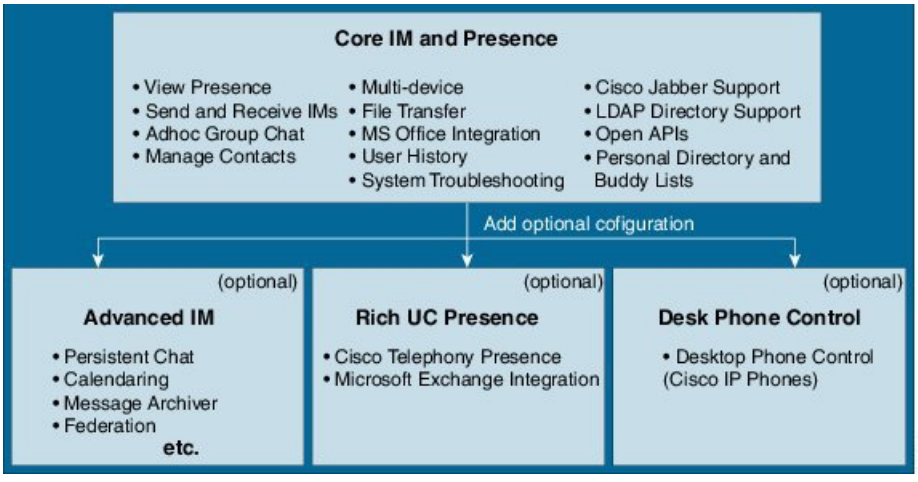
Cisco Sync Agent のステータスを確認するには、Cisco Unified CM IM and Presence の管理インターフェイスに移動し、**[診断（Diagnostics）]>[システム ダッシュボード（System Dashboard）]** を選択します。CUCM Publisher の IP アドレスと同期ステータスを検索します。

IM and Presence Service の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。

図 *2 : IM and Presence Service* の機能展開オプション



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 Service* 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 Exchange サーバの統合	リモート Cisco IP Phone 制御 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）
	常設チャット マネージド ファイル転送 メッセージ アーカイバ カレンダー サードパーティ製 XMPP クライアントのサポート 高可用性 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 クラスタ間のピアリング 企業の連携（B2B）： • Cisco Unified Presence との統合 • Cisco Webex の統合 • Mircosoft Lync/OCS サーバの統合（ドメイン間とパーティション化されたドメイン内のフェデレーション） • IBM SameTime の統合 • Cisco Jabber XCP パブリック フェデレーション（B2C）： • Google Talk、AOL の統合 • XMMP サービスまたは BOT • サードパーティの Exchange サービスの統合		

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）
	IM コンプライアンス シングル サインオン カスタム ログイン バナー		

展開モデル

シングルノード、マルチノード、および IM-Only での高可用性展開

IM and Presence Service は、シングルノード、マルチノード、をサポートしています。

クラスタ内のシングルノード展開では、そのノードに割り当てられているユーザに対して、高可用性のフェールオーバー保護は提供されません。プレゼンス冗長グループを使用しているマルチノード展開では、グループに対して高可用性を有効にできるため、ユーザにはフェールオーバー保護が提供されます。

シスコでは、IM and Presence Service 展開を高可用性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、高可用性と非高可用性の両方を、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に対して、Cisco Unified CM Administration インターフェイスを使用して、高可用性を手動で有効にする必要があります。高可用性の設定方法の詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

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。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。

平衡型とアクティブ/スタンバイの 2 種類の異なる設定を使用することで、高可用性を実現できます。バランス モードでは、連動するようにプレゼンス冗長グループ内のノードを設定できます。コンポーネントの障害や停電により、いずれかのノードが停止すると、ユーザのロードバランシングとユーザのフェールオーバーが自動的に有効になり、冗長高可用性が提供されます。アクティブ/スタンバイの設定では、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。

プレゼンス冗長グループ、高可用性モード、およびユーザの割り当ての詳細や設定手順については、次のガイドを参照してください。

- 『Cisco Unified Communications Manager アドミニストレーション ガイド』
- 『Cisco Unified Communications Manager 一括管理ガイド』

- 『*Cisco Unified Communications Manager* 機能およびサービス ガイド』
- 『Cisco Unified Communications Manager インストール ガイド』
- 『*Cisco Unified Communications Manager* システム ガイド』

プレゼンス冗長グループと高可用性

プレゼンス冗長グループは、同じクラスタの 2 つの IM and Presence Service ノードから構成され、IM and Presence Service のクライアントとアプリケーションに冗長化とリカバリを提供します。[Cisco Unified CMの管理（Cisco Unified CM Administration）] を使用して、ノードをプレゼンス冗長グループに割り当て、高可用性を可能にします。

- フェールオーバー：プレゼンス冗長グループ内の IM and Presence Service 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、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 Service 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（コマンドライン インターフェイス）または Cisco Unified Communications Manager から発行されると行われます。
  - 障害が発生した IM and Presence Service 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。そのグループ内のフェールオーバーしていたクライアントは、回復したノードが使用可能になると、その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 Service 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。

自動フォールバック。IM and Presence Service は、フェールオーバー後のプライマリ ノードへの自動フォールバックをサポートしています。自動フォールバックは、手動による介入を必要とすることなく、フェールオーバー後にユーザをプライマリ ノードに戻す処理です。自動フォールバックは、Cisco Unified CM IM and Presence の管理インターフェイス上で [自動フォールバックの有効化（Enable Automatic Fallback）] サービス パラメータを使用して有効にできます。自動フォールバックは次のシナリオで実行されます。

- ノード A の重要なサービスが失敗する：重要なサービス（たとえば、Presence Engine）がノード A で失敗します。自動フェールオーバーが発生し、すべてのユーザはノード B に移動します。ノード A は [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）]「」 と呼ばれる状態です。重要なサービスが回復すると、ノードの状態は [フェールオーバー済み（Failed Over）] に変わります。これが発生すると、ノード B は 30 分間ノード A の状態を追跡します。ハートビートがこの期間に欠落しておらず、各ノードの状態が変更されずに残っている場合、自動フォールバックが実行されます。
- ノード A がリブートされる：自動フェールオーバーが発生し、すべてのユーザがノード B に移動します。ノード A は正常な状態に戻り、30 分間その状態のままになると、自動フォールバックが発生します。

- ノードAのノードBとの通信が失われる：自動フェールオーバーが発生し、すべてのユーザがノードBに移動します。通信が再確立され、30分間変化がなければ、自動フォールバックが発生します。

フェールオーバーがここに示した3とおりのシナリオ以外の理由で実行された場合、ノードを手動で回復する必要があります。自動フォールバックまで30分間待たない場合は、プライマリ ノードへの手動フォールバックを実行できます。たとえば、ローカルのIM and Presence Service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、プレゼンス冗長グループを使用してバックアップ用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オンラインに戻ると、クライアントはローカルのIM and Presence Serviceノードに自動的に再接続します。障害が発生したノードがオンラインに戻ったときに、自動フォールバック オプションを設定していない場合は、手動のフォールバック操作を行う必要があります。

プレゼンス冗長グループのIM and Presence Serviceノードのノード フェールオーバー、フォールバック、および回復は手動で開始できます。自動フォールバック オプションを設定していない場合は、手動のフォールバック操作を行う必要があります。

プレゼンス冗長グループおよび高可用性を設定する方法については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

WAN 経由のクラスタリング

IM and Presence Service は WAN 経由のクラスタリング展開をサポートします。

関連トピック

クラスタ内およびクラスタ間展開における WAN 経由のクラスタリング （32 ページ）

ユーザ割り当て

ユーザがIM and Presence Serviceの可用性サービスとインスタント メッセージ（IM）サービスを利用できるようにするには、IM and Presence Service展開でノードとプレゼンス冗長グループにユーザを割り当てる必要があります。IM and Presence展開では、手動または自動でユーザを割り当てることができます。**User Assignment Mode for Presence Server** の [エンタープライズ パラメータ（Enterprise Parameter）] 設定を使用してユーザ割り当てを管理します。このパラメータは、Sync Agentがクラスタ内のノードにユーザを分散させるモードを指定します。

[バランス（Balanced）]モード（デフォルト）では、ユーザをプレゼンス冗長グループの各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。デフォルトモードは [バランス（Balanced）] です。

[アクティブ スタンバイ（Active-Standby）]モードでは、プレゼンス冗長グループ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 ノードをバックアップのままにします。

[なし（None）]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。

手動のユーザ割り当てを選択した場合は、Cisco Unified Communications Manager Administration を使用してノードとプレゼンス冗長グループに手動でユーザを割り当てる必要があります。詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

エンド ユーザ管理

次のエンドユーザの管理タスクを実行するには、IM and Presence Service GUI を使用できます。

- 重複しているか無効なエンド ユーザ インスタンスの有無を展開の全体にわたって確認します。
- 連絡先リストをエクスポートします。
- ホーム クラスタで連絡先リストをインポートします。

IM and Presence Service ユーザを移行する手順については、クラスタ間のユーザ移行、ユーザ管理、および管理に関するトピックを参照してください。

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。

- 『Cisco Unified Communications Manager アドミニストレーション ガイド』
- 『Cisco Unified Communications Manager 一括管理ガイド』
- 『Cisco Unified Communications Manager のインストール』

アベイラビリティとインスタント メッセージ

チャット（Chat）

ポイントツーポイント インスタント メッセージ（IM）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。ユーザは、ポイントツーポイント IM を交換するために IM クライアントでオンラインである必要があります。

IM and Presence Service でチャットとアベイラビリティの両方の機能を無効にできます。

関連トピック

IM and Presence Service クラスタのインスタント メッセージのオン/オフ （191 ページ）
IM and Presence Service クラスタのプレゼンス ステータス共有のオン/オフ （187 ページ）

IM 分岐

複数の IM クライアントにサイン インしている連絡先に、ユーザが IM を送信すると、IM and Presence Service は各クライアントに IM を配信します。この機能は、IM 分岐と呼ばれます。IM and Presence Service は、連絡先が応答するまで IM 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 IM を配信します。

オフライン インスタント メッセージは、IM and Presence Service で無効にできます。

関連トピック

オフライン インスタント メッセージのオン/オフ （192 ページ）

オフライン IM

オフライン IM は、オフラインの連絡先に IM を送信する機能です。ユーザがオフラインの連絡先に IM を送信すると、IM and Presence Service は IM を保存し、オフラインの連絡先が IM クライアントにサイン インすると IM を配信します。

ブロードキャスト IM

ブロードキャスト IM は、同時に複数の連絡先に IM を送信する機能です。たとえば、ユーザは、連絡先の大きなグループに通知を送信できます。すべての IM クライアントがこの機能をサポートしているとは限りません。

IM and Presence Service のチャット ルーム

IM and Presence Service は、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 IM 交換をサポートします。デフォルトで、IM and Presence Service の Text Conference（TC）コンポーネントは、アドホック チャット ルームの IM 交換を処理するように設定されています。このモジュールで説明するように、常設チャット ルームをサポートするには、追加要件の設定が必要になります。

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 IM セッションで、最後のユーザがルームを離れるとシステムから削除されます。IM 会話のレコードは永続的に維持されません。

アドホック チャット ルームは、デフォルトではパブリック ルームですが、プライベートに再設定できます。ただし、ユーザ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 のユーザがアドホック チャットルーム（パブリックまたはプライベート）に参加するには、ルームのオーナーまたは管理者からの招待を受ける必要があります。
- サードパーティ XMPP クライアントのユーザは、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）に参加するために招待されるか、またはパブリックのみのアドホック ルームを検索し、ルーム検出サービスを介して参加することができます。

常設チャット ルーム

常設チャット 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、アドホック グループ チャット セッションのように終了することはありません。その目的は、ユーザが後で常設チャットルームに戻って、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参加したりできるようにすることです。管理者は、そのルームのメンバーだけがアクセスできるように常設チャットルームへのアクセスを制限することもできます。メンバーの設定（283ページ）と、Cisco Unified Communications Manager および IM and Presence Service Release 11.0(1) のリリース ノートにある「Important Notes」セクションの「IM and Presence Service Ad Hoc Group Chat Rooms Privacy Policy」を参照してください。

IM and Presence Service の TC コンポーネントにより、ユーザは次の操作を実行できます。

- 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。
- 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。

また、IM and Presence Serviceの常設チャット機能により、ユーザは次の操作を実行できます。

- 既存のチャット ルームを検索し、そのルームに入室します。
- チャットの音声テキスト変換を保存し、メッセージ履歴を検索できるようにします。

（注） クラスタ間接続を介してチャット ルームを検索するユーザの場合、検索結果では、リリース11.5(1)SU2より古いクラスタからのアドホック チャットルームが検出されますが、このリリース以上のクラスタからは検出されません。リリース 11.5(1) SU2 のクラスタ以上のアドホック チャット ルームは、チャット ルームのオーナーまたは管理者のみが検出できます。

チャット ルームの制限

次の表に、IM and Presence Service のチャット ルームの制限値を示します。

表 *2 : IM and Presence Service* のチャット ルームの制限

項目	最大数
ノードごとの常設チャット ルーム	1500 ルーム
ノードあたりのルームの合計（アドホックおよび常設）	16500 ルーム
ルームごとの利用者	1000 利用者

項目	最大数
アーカイブから取得されたメッセージ これは、ユーザがルーム履歴を問い合わせたときに返されるメッセージの最大数です。	100 メッセージ
デフォルトで表示されるチャット履歴のメッセージ これは、ユーザがチャット ルームに入室したときに表示されるメッセージの数です。	15 メッセージ

ファイル転送

IM and Presence Service は、XEP-0096（http://xmpp.org/extensions/xep-0096.html）に準拠した XMPP クライアント間のポイントツーポイントおよびマネージドファイル転送をサポートします。

関連トピック

ファイル転送の有効化

IM and Presence Service およびチャットに関する重要事項

SIP 間の IM 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 から XMPP への IM 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

IM コンプライアンス

IM and Presence Service におけるインスタント メッセージ（IM）のコンプライアンスの設定については、次のマニュアルを参照してください。

- 『Cisco Unified Communications Manager の IM and Presence Service インスタント メッセージ コンプライアンス ガイド』

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

- 『Cisco Unified Communications Manager の IM and Presence Service データベース セットアップ ガイド』

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

プレゼンス データの概要

IM and Presence Service は、プレゼンス更新が行われるたびに、ユーザの高度なプレゼンスを再構成します。プレゼンス更新には、次の 2 つのメイン カテゴリがあります。

- システムが決定するプレゼンス
- 手動プレゼンス

手動プレゼンス

手動プレゼンスは、ユーザによって明示的に設定されます。これは通常、システムが決定するプレゼンスをオーバーライドします。手動プレゼンスの設定には次のものが含まれます。

- IM クライアントでのユーザ設定 [応答不可（Do Not Disturb）]
- IM クライアントでのユーザ設定 [退席中（Away）]
- 電話機/カレンダーのプレゼンスなど、システムが決定したステータスを上書きするための IM クライアントでのユーザ設定 [使用可能（Available）]
- サード パーティ製アプリケーションからの上記いずれかのユーザ設定

ユーザは 1 つの手動プレゼンス ステータスしか持つことができません。これは、次のいずれかの場合にクリアされます。

- ユーザが明示的にクリアする（または新しい手動ステータスで置き換える）。
- ユーザのクライアントがログアウト時にクリアする。
- ユーザがすべての IM デバイスからログアウトされた場合に、IM and Presence サーバがクリアする。

システムが決定するプレゼンス

システムが決定するプレゼンスは、ユーザとシステム間のいくつかの相互作用に基づいてプレゼンス ソースによって自動的に公開されます。

- 電話をかける
- 会議への参加
- IM デバイスへのサインインとサインアウト
- 一定期間の非アクティブ後に IM デバイスがアイドル状態になる
- 電話を応答不可に設定する

システムが決定するプレゼンスには 4 つのカテゴリがあります。

- IM デバイスのステータス

  ユーザに属する個々の IM デバイスの特定のステータス。ユーザに複数の IM デバイスがある場合、IM and Presence Service は、そのようなすべてのデバイス全体でユーザのステータスを最もよく表す全体的なユーザ ステータスを構成します。

- カレンダーのステータス

  カレンダー上のユーザの空き時間情報を表す特定のステータス。IM and Presence Service は、そのようなカレンダーのステータスを全体的なユーザ ステータスに組み込みます。

- 電話機のステータス

  これは、ユーザの電話アクティビティ（オンフック/オフフック）を表します。各ユーザのライン アピアランスごとに個別の入力があります。IM and Presence Service によって組み込まれます。

- サード パーティ製アプリケーションのステータス

  これにより、SIP、XMPP、BOSH、またはプレゼンス Web サービスなどのオープン インターフェイスを介して、プレゼンス更新を IM and Presence Service にプッシュできます。これらのプレゼンス ステータスは、全体的に構成されたユーザ ステータスに組み込まれます。

エンタープライズ グループ

Cisco Unified Communications Manager リリース 11.0 では、Cisco Jabber ユーザが Microsoft Active Directory の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。連絡先リストにすでに追加されているグループが更新された場合は、連絡先リストが自動的に更新されます。Cisco Unified Communications Manager のデータベースは、指定された間隔で Microsoft Active Directory グループと同期されます。

Cisco Jabber ユーザが連絡先リストにグループを追加すると、IM and Presence Service は各グループ メンバーに関する次の情報を提供します。

- 表示名
- ユーザ ID
- タイトル
- 電話番号
- メール ID

IM and Presence Service ノードに割り当てられているグループ メンバーのみを、連絡先リストに追加することができます。他のグループ メンバは廃棄されます。

（注） 現在、エンタープライズ グループ機能は Microsoft Active Directory サーバでのみサポートされています。その他の企業ディレクトリではサポートされません。

エンタープライズ グループ機能は、Cisco Unified Communications Manager の [Cisco IM and Presence でのディレクトリ グループ操作（Directory Group Operations on Cisco IM and Presence）] エンタープライズ パラメータにより、システム全体で有効にされます。エンタープライズ グループの詳細については、『Cisco Unified Communications Manager 機能設定ガイド』を参照してください。

エンタープライズ グループの検証済 OVA 情報

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。

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。

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。

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。

（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。

LDAP 統合

いくつかの異なる要件を満たすために、この統合に社内 LDAP ディレクトリを設定できます。

- **ユーザ プロビジョニング**：Cisco Unified Communications Manager データベースに LDAP ディレクトリからユーザを自動的にプロビジョニングできます。Cisco Unified Communications Manager は、LDAP ディレクトリの内容と同期するため、変更が LDAP ディレクトリで発生するたびにユーザ情報を手動で追加、削除、または修正する必要はありません。
- **ユーザ認証**：LDAP ディレクトリの資格情報を使用してユーザを認証できます。IM and Presence Service は Cisco Unified Communications Manager からすべてのユーザ情報を同期し、Cisco Jabber クライアントおよび IM and Presence Service ユーザ インターフェイスのユーザ認証を提供します。

シスコは、ユーザの同期化と認証のために、Cisco Unified Communications Manager と Directory サーバの統合を推奨しています。

（注） Cisco Unified Communications Manager を LDAP と統合しない場合は、IM and Presence Service を展開する前に、ユーザ名が Active Directory と Cisco Unified Communications Manager でまったく同じであることを確認する必要があります。

関連トピック

Cisco Unified Communications Manager との LDAP ディレクトリの統合のタスク リスト （129 ページ）

サードパーティ統合

サードパーティ統合については、次の表の参照資料を参照してください。

マニュアルのタイトル	このマニュアルの構成
『Microsoft Exchange for IM and Presence Service on Cisco Unified Communications Manager』	• Microsoft Exchange 2007、2010、および 2013 との統合 • この統合のための Microsoft Active Directory の設定
『Microsoft Office Communicator Call Control with Microsoft OCS for IM and Presence Service on Cisco Unified Communications Manager』	• Microsoft Office Communicator クライアントからのリモート コール制御用 CSTA ゲートウェイとしての IM and Presence Service の設定 • この統合のための Microsoft Active Directory の設定 • TCP 経由のデュアル ノード IM and Presence Service 展開での MOC 要求のロード バランシング • TLS 経由のデュアル ノード IM and Presence Service 展開での MOC 要求のロード バランシング
『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』	• Microsoft OCS と AOL による SIP プロトコルを介したドメイン間フェデレーションと、IBM Sametime、Googletalk、Webex Connect、および別の IM and Presence Service リリース 9.x エンタープライズによる XMPP プロトコルを介したドメイン間フェデレーション用の IM and Presence Service の設定。

マニュアルのタイトル	このマニュアルの構成
『Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager』	• パーティション化されたドメイン内フェデレーション用の IM and Presence Service の設定 • パーティション化されたドメイン内フェデレーション用の Microsoft OCS の設定 • パーティション化されたドメイン内フェデレーション用の Microsoft LCS の設定 • ユーザの移行
『Remote Call Control with Microsoft Lync Server for IM and Presence Service on Cisco Unified Communications Manager』	• Microsoft Lync と統合するための Cisco Unified Communications Manager および IM and Presence Service の設定 • Microsoft Active Directory の設定 • 正規化ルールの設定 • IM and Presence Service と Microsoft Lync 間のセキュリティの設定

サードパーティ製クライアントの統合

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/

（注） IM and Presence Service は、サードパーティ Web クライアントの高可用性をサポートしていません。高可用性機能が設定されているかどうかにかかわらず、プライマリ ノードに障害が発生すると、サードパーティ クライアントは接続を失い、再接続できなくなります。サードパーティ クライアントに冗長性を持たせるには、プライマリ ノードに障害が発生した場合にサードパーティ クライアントがバックアップ ノードにフェールオーバーできるように、事前にクライアントにバックアップ ノードをプロビジョニングする必要があります。

（注） サポートされるクライアントは、IM and Presence Service ノードに設定された IM アドレス スキームによって異なる場合があります。

サードパーティ製クライアントのライセンス要件

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。詳細については、『Cisco Unified Communications Manager Enterprise License Manager ユーザ ガイド』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。

関連トピック

ユーザ ライセンスの要件 （41 ページ）
統合前の Cisco Unified Communications Manager のユーザおよびデバイス設定のタスク リスト （55 ページ）

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 Service で XMPP クライアントの LDAP 設定を実行します。

関連トピック

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 （135 ページ）

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。

IPv6 のサポート

IM and Presence Service は、インターネット プロトコル バージョン 6（IPv6）をサポートしています。したがって、デジタルネットワーク上で、データ、音声、および動画のトラフィックを交換する際に、パケットを使用します。また、IPv6 では、ネットワーク アドレス ビット数が 32 ビット（IPv4 の場合）から 128 ビットに増やされています。IM and Presence Service ネットワークでの IPv6 の展開は、IPv4 と IPv6 のデュアル スタックな環境で透過的に機能します。デフォルトのネットワーク設定は IPv4 です。

IPv6 が有効な場合、IPv6 の発信トラフィックが可能です。たとえば、スタティック ルートまたは DNS クエリのいずれかを使用するように SIP S2S を設定できます。スタティック ルートを設定し、IPv6 を有効にしている場合は、IPv6 IP トラフィックが発生すると、SIP プロキシは IPv6 接続を確立しようとします。IM and Presence Service と Cisco Unified Communications Manager 間の接続に IPv4 を使用していても、外部データベース、LDAP サーバ、Exchange サーバへの接続、および IM and Presence Service でのフェデレーション接続には IPv6 を使用できます。

サービスで（XMPP S2S などで）DNS 要求を使用する場合、DNS クエリの結果として IP アドレスのリストを受信した後に、サービスはリストの各 IP アドレスに 1 つずつ接続しようとします。リストされた IP アドレスが IPv6 の場合、サーバは IPv6 接続を確立します。IPv6 接続の確立要求が失敗した場合、サービスはリストの次の IP アドレスに進みます。

IM and Presence Service ノードで、エンタープライズ パラメータまたは ETH0 のいずれかに対して、何らかの理由で IPv6 が無効になった場合でも、IM and Presence Service で設定されているサーバのホスト名が解決可能な IPv6 アドレスならば、ノードは内部 DNS クエリを実行し、外部の LDAP やデータベース サーバに接続できます。

IPv6 の補足情報とネットワークのガイドラインについては、次のマニュアルを参照してください。

- 『Cisco Unified Communications Manager アドミニストレーション ガイド』
- 『*Cisco Unified Communications Manager* 機能およびサービス ガイド』

- 『Cisco Unified Communications Solutions コマンドライン インターフェイス ガイド』
- 『*Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*』
- 『Cisco Unified Communications Manager の IM and Presence Service 設定および管理ガイド』

IM アドレス スキームとデフォルト ドメイン

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 をインストールした場合の、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。

（注） 選択した IM アドレス スキームは、すべての IM and Presence Service クラスタ全体で一致している必要があります。

UserID@Default_Domain の IM アドレス スキームを使用している場合、IM アドレスの一部として使用されているデフォルトのドメインは、クラスタ全体の設定になります。

UserID@Default_Domain を使用した IM アドレス

UserID@Default_Domain の IM アドレス スキームは、IM and Presence Service を新規インストールまたは以前のバージョンからアップグレードする場合の、デフォルトのオプションです。デフォルトのドメインを設定するには、**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [詳細設定（Advanced Configuration）]** を選択します。

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。

Cisco Unified CM の IM and Presence の管理 GUI を使用してディレクトリ URI を設定するには、次の 2 つの方法があります。

- LDAP ディレクトリ ソースからディレクトリ URI を同期します。

  Cisco Unified Communications Manager で LDAP ディレクトリ ソースを追加する場合、ディレクトリ URI の値を設定できます。その後で、ディレクトリ ソースからユーザ データを同期するときに、Cisco Unified Communications Manager はディレクトリ URI を追加します。

  （注） Cisco Unified Communications Manager で LDAP ディレクトリとの同期が有効な場合は、電子メール アドレス（mailid）または Microsoft OCS/Lync SIP URI（msRTCSIP-PrimaryUserAddress）にディレクトリ URI をマップできます。

- Cisco Unified Communications Manager でディレクトリ URI の値を手動で指定します。

  Cisco Unified Communications Manager で LDAP ディレクトリ ソースを追加しない場合、ディレクトリ URI を自由形式の URI として手動で入力できます。

注意 ディレクトリ URI を IM アドレス スキームとして使用するようにノードを設定する場合、シスコはディレクトリ 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。

LDAP ディレクトリでディレクトリ URI を設定する場合の詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

IM アドレスの例

次の表は、IM and Presence Service で使用可能な IM アドレス オプションの例を示しています。

IM and Presence Service Default Domain: cisco.com **User**: John Smith **Userid**: js12345 **Mailid**: 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

IM アドレスの設定の詳細については、『*Cisco Unified Communications Manager* における *IM and Presence Service* の設定と管理』を参照してください。

Cisco Unified Communications Manager との IM アドレスの統合

Cisco Unified Communications Manager を使用した UserID@Default_Domain の統合

デフォルト IM アドレス スキームは *UserID @ Default_Domain* です。次の条件を満たすすべてのクラスタに対してこの IM アドレス スキームを使用します。

- すべての IM and Presence Service クラスタがリリース 10.0 よりも前のソフトウェア リリースと一緒に展開されます。
- 展開されたクライアントはすべてディレクトリ URI IM アドレス スキームをサポートしません。

名前が示すように、すべての IM アドレスが単一デフォルト IM ドメインの一部です。すべての IM and Presence Service クラスタ全体で一貫したドメインを設定するために Cisco Unified CM IM and Presence 管理 GUI を使用します。

IM and Presence Service の IM アドレス（JID）は常に *UserID@Default_Domain* です。*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

ユーザ ID は電子メール アドレスにマッピングできますが、それが 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 Service 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。

Cisco Unified Communications Manager を使用したディレクトリ URI の統合

単一 IM ドメインに限定される *UserID@Default_Domain* IM アドレス スキームとは異なり、Directory URI IM アドレス スキームは複数の IM ドメインをサポートします。ディレクトリ URI に指定されたドメインは IM and Presence Service によってホストされているものとして処理されます。ユーザの IM アドレスを使用して、Cisco Unified Communications Manager で設定されているとおりにそれらのユーザのディレクトリ URI に合わせます。

ディレクトリ URI の形式は自由であり、LDAP から同期することもできます。LDAP 同期が無効になっている場合は、ディレクトリ URI を自由形式の URI として設定することができます。LDAP ディレクトリ同期が有効になっている場合は、次のフィールドにディレクトリ URI をマッピングできます。

- email address（電子メール アドレス）（mailid）
- Microsoft OCS/Lync SIP URI (msRTCSIP-PrimaryUserAddress)

LDAP の有効化については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

複数の IM ドメインの管理

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。Cisco Unified CM IM and Presence の管理 GUI を使用して、管理者がローカルに管理するドメインを手動で追加、更新、削除し、システムがローカルに管理するすべてのドメインを表示します。

Cisco Expressway と連携させる場合は、ドメインに関する制限の詳細について、『Cisco Expressway (X8.2) 管理者ガイドhttp://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html』を参照してください。

セキュリティ

証明書を交換することにより、IM and Presence Service と Cisco Unified Communications Manager、XMPP クライアント、および SIP クライアントの間にセキュアな接続を設定できます。証明書は自己署名するか、認証局（CA）によって生成されます。

詳細については、セキュリティ設定に関するトピックを参照してください。

SAML シングル サインオン

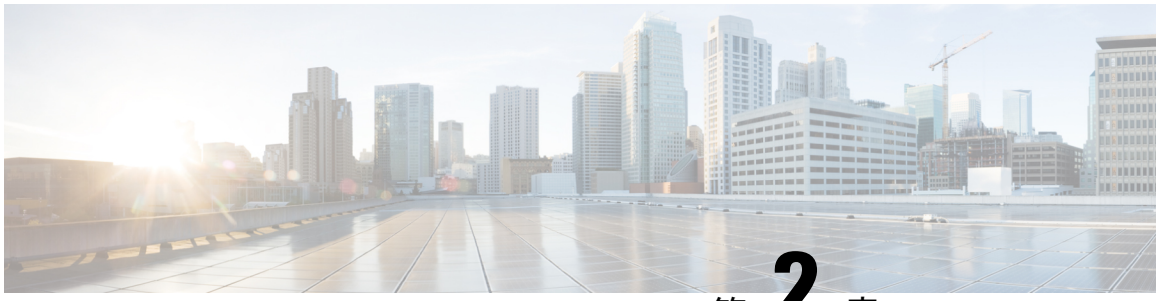
Security Assertion Markup Language（SAML）のシングル サインオン機能を使用すると、管理ユーザは再度ログインせずに次の Cisco Unified Communications Manager および IM and Presence Service の Web アプリケーションにアクセスすることができます。

- Cisco Unified CM IM and Presence の管理
- Cisco Unified IM and Presence Service アビリティ
- Cisco Unified IM and Presence のレポート
- Cisco Unified CM の管理
- Cisco Unified のレポート
- Cisco Unified サービスアビリティ
- ユニファイド コミュニケーション セルフ ケア ポータル

（注） LDAP 同期されたユーザのみが、SAML SSO 対応の Web アプリケーションにアクセスできます。ローカル エンド ユーザとアプリケーション ユーザはアクセスできません。

Cisco Unified Communications Manager および IM and Presence Service Web アプリケーション用に SAML SSO を有効にする方法の詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』（リンク）を参照してください。

SAML SSO について、およびいくつかの Unified Communications アプリケーションで SAML SSO を有効にする方法の詳細については、『Cisco Unified Communications アプリケーション SAML SSO 導入ガイド』（リンク）を参照してください。



第 2 章

マルチノードの拡張性と WAN の展開

- マルチノードの拡張性機能 （27 ページ）
- クラスタ全体の DNS SRV （30 ページ）
- ローカル フェールオーバー （31 ページ）
- プレゼンス冗長グループの障害検出 （31 ページ）
- メソッド イベント ルーティング （31 ページ）
- 外部データベースの推奨事項 （32 ページ）
- クラスタ内およびクラスタ間展開における WAN 経由のクラスタリング （32 ページ）

マルチノードの拡張性機能

マルチノードの拡張性要件

IM and Presence Service 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ごとに最大 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、および高可用性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 Service 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。

拡張性は、展開内のクラスタの数によって異なります。詳細な 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。http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CM_IM_and_Presence

OVA 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 Service 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 パブリッシャ 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 パブリッシャ 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ャ 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は、以下の URL の *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 *3:* マルチノードの拡張性オプション

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	新しいプレゼンス冗長グループへの新しいノードの追加
平衡型非冗長高可用性展開	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高可用性を提供します。	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高可用性を提供しません。平衡型高可用性を実現するには、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。
平衡型冗長高可用性展開	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高可用性を提供します。 （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。	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高可用性を提供しません。平衡型高可用性を実現するには、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	新しいプレゼンス冗長グループへの新しいノードの追加
アクティブ/スタンバイ冗長高可用性展開	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、プレゼンス冗長グループの既存のノードのユーザに高可用性が提供されます。これは、高可用性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。	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高可用性を提供しません。高可用性を実現するには、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。

クラスタ全体の DNS SRV

DNS 設定では、クラスタ全体の IM and Presence Service アドレスを定義できます。

Cisco Unified Communications Manager の SIP パブリッシュ トランクは、クラスタ全体の IM and Presence Service アドレスを使用して、Cisco Unified Communications Manager からの SIP パブリッシュ メッセージをクラスタのすべてのノードにロード バランシングします。とりわけ、この設定にすると、初期 SIP パブリッシュ メッセージがクラスタのすべてのノードにロード バランシングされるようになります。また、ノードで障害が発生した場合には、Cisco Unified Communications Manager によって SIP パブリッシュ メッセージが残りのノードに転送されるため、高可用性展開を実現できます。

クラスタ全体の DNS 設定は必須の設定ではありません。クラスタ内のすべてのノードに対して初期 SIP パブリッシュ メッセージをロード バランスする方法としてこの設定方法を推奨します。IM and Presence Service は、各デバイスの後続の SIP パブリッシュ メッセージを IM and Presence Service でユーザが配置されているノードに送信します。

IM and Presence Service が複数のドメインをサポートするとしても、単一のクラスタ全体の DNS SRV レコードのみが必要です。Cisco Unified Communications Manager SIP トランクを設定したときに DNS SRV レコードを指定します。DNS SRV レコードの宛先アドレスとして IM and Presence Service のデフォルト ドメインを使用することを推奨します。

（注） DNS SRV レコードの宛先アドレスとして任意のドメイン値を指定できます。ただし、IM and Presence Service で SRV クラスタ名を呼び出した SIP プロキシ サービス パラメータが、DNS SRV レコードに指定するドメイン値と一致していることを確認します。指定するドメインにユーザを割り当てる必要はありません。

詳細については、IM and Presence Service および DNS SRV レコードを統合するための Cisco Unified Communications Manager の設定に関するトピックを参照してください。

関連トピック

SIP パブリッシュ トランクのクラスタ全体の DNS SRV 名の設定 （126 ページ）

ローカル フェールオーバー

1 つのプレゼンス冗長グループが 1 つの地理的なサイトにあり、2 番目のプレゼンス冗長グループが別の地理的なサイトにある WAN 経由で IM and Presence Service を展開することもできます。プレゼンス冗長グループにはローカル ノード間の高可用性のために単一ノードまたはデュアル ノードを含めることができます。このモデルは、地理的なサイト間のフェールオーバーを提供しません。

プレゼンス冗長グループの障害検出

IM and Presence Service は、プレゼンス冗長グループの障害検出メカニズムをサポートします。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 でハートビート接続とハートビート間隔を設定するには、**[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）]** > **[Server Recovery Manager（service）]** を選択します。[一般的な Server Recovery Manager パラメータ（クラスタ全体）（General Server Recovery Manager Parameters (Clusterwide)）] セクションで、次のパラメータを設定します。

- [ハートビート間隔（Heart Beat Interval）]：このパラメータは、Server Recovery Manager が同じ冗長グループのピア Server Recovery Manager にハートビート メッセージを送信する間隔を秒単位で指定します。ハートビートは、ネットワークのアベイラビリティを判断するために使用されます。デフォルト値は 60 秒です。
- [接続タイムアウト（Connect Timeout）]：このパラメータは、Server Recovery Manager がピア Server Recovery Manager への接続要求から応答を受信するために待つ時間を秒単位で指定します。デフォルト値は 30 秒です。

（注） シスコは、これらの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。

メソッド イベント ルーティング

WAN 経由で IM and Presence Service を展開する場合は、IM and Presence Service に TCP メソッド イベント ルーティングを設定することを推奨します。メソッド イベント ルートを設定するには、**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence**

Administration）]>[プレゼンス（Presence）]>[ルーティング（Routing）]>[メソッド/イベント ルーティング（Method/Event Routing）] を選択します。

外部データベースの推奨事項

WAN 展開を介してクラスタリングの外部データベース サーバを設定する場合は、外部データベース サーバを、外部データベース サーバを使用する IM and Presence Service ノードに共存させることを推奨します。

IPv4 または IPv6 のいずれかを使用する外部データベース サーバ にIM and Presence Service ノードを接続できます。

外部データベース サーバおよび IM and Presence Service の詳細については、『Cisco Unified Communications Manager の IM and Presence Service データベース セットアップ ガイド』を参照してください。

クラスタ内およびクラスタ間展開における WAN 経由のクラスタリング

IM and Presence Service は、クラスタ内およびクラスタ間展開における WAN 経由のクラスタリング展開をサポートします。

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 パブリッシャ 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、クライアントの高可用性をサポートし、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 レベルの高可用性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 ソリューション リファレンス ネットワーク デザイン（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 経由の高可用性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。この高可用性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。

関連トピック

WAN 経由のクラスタ内展開 （32 ページ）
http://www.cisco.com/go/designzone

クラスタ間展開

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。

関連トピック

WAN の帯域幅要件 （39 ページ）

クラスタ間ピア関係

クラスタ間ピアと呼ばれる、スタンドアロンの IM and Presence Service 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。あるクラスタからクラスタ間ピアを削除した場合は、リモートクラスタの対応するピアも削除する必要があります。

IM and Presence Service は、ホーム クラスタ アソシエーションのユーザ情報の検索に AXL/SOAP インターフェイスを使用します。IM and Presence Service は、このユーザ情報を使用して、ユーザがローカル ユーザ（ホーム クラスタのユーザ）であるのか、それとも同じドメイン内のリモート IM and Presence Service クラスタのユーザであるのかを検出します。

IM and Presence Service は登録および通知トラフィックに XMPP インターフェイスを使用します。IM and Presence Service が同じドメイン内のリモート クラスタのユーザを検出すると、IM and Presence Service はリモート クラスタにメッセージを再ルーティングします。

注意 最初の同期で大量の帯域幅と CPU が使用されるため、クラスタ間ピアは時間をずらして設定することを推奨します。複数のピアを同時に設定すると、同期の時間が極端に長くなる可能性があります。

クラスタ間ルータ ツールータ接続

デフォルトでは、IM and Presence Service は、クラスタ間ルータツールータ 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ツールータ コネクタ ノードからの情報を同期化します。

IM and Presence Service がクラスタ間ルータツールータ コネクタ ノード間の接続を確立するには、ローカル クラスタとリモート クラスタの両方のノードすべてで Cisco XCP Router サービスを再起動する必要があります。一方のクラスタの各クラスタ間ルータツールータ コネクタは、もう一方のクラスタのルータツールータ コネクタとのクラスタ間接続を開始するか、または受け入れます。

（注） クラスタ間展開では、クラスタに新しいノードを追加すると、ローカル クラスタとリモートクラスタの両方のノードすべてで Cisco XCP Router を再起動する必要があります。

関連トピック

セキュアなクラスタ間ルータ ツー ルータ接続 （36 ページ）

クラスタ間展開のノード名の値

任意の IM and Presence Service 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 Service 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。

（注） ノード名としてのホスト名の指定がサポートされるのは、すべてのクラスタのすべてのノードが同じ DNS ドメインを共有している場合だけです。

注目 Cisco Jabber クライアントを使用している場合、IP アドレスを IM and Presence Service のノード名として設定すると、証明書の警告メッセージが表示されることがあります。Cisco Jabber で証明書の警告メッセージの生成を防止するには、ノード名として FQDN を使用する必要があります。IM and Presence Service のノード名の値を設定する手順については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

関連トピック

クラスタ間展開の IM and Presence のデフォルト ドメイン値 （35 ページ）

クラスタ間展開の IM and Presence のデフォルト ドメイン値

クラスタ間展開を設定する場合は、次の点に注意してください。

- クラスタ間機能を正常に動作させるには、ローカル クラスタとリモート クラスタの両方で、IM and Presence のデフォルト ドメイン値が一致している必要があります。

詳細な手順については、IM and Presence のデフォルト ドメインの設定に関するトピックを参照してください。

関連トピック

IM and Presence Service のデフォルト ドメインの設定
クラスタ間展開のノード名の値 （34 ページ）

クラスタ間展開の 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。

詳細については、IM アドレス スキームの設定に関するトピックを参照してください。

関連トピック

IM アドレス スキームの設定
UserID@Default_Domain を使用した IM アドレス （22 ページ）
ディレクトリ URI を使用した IM アドレス （22 ページ）

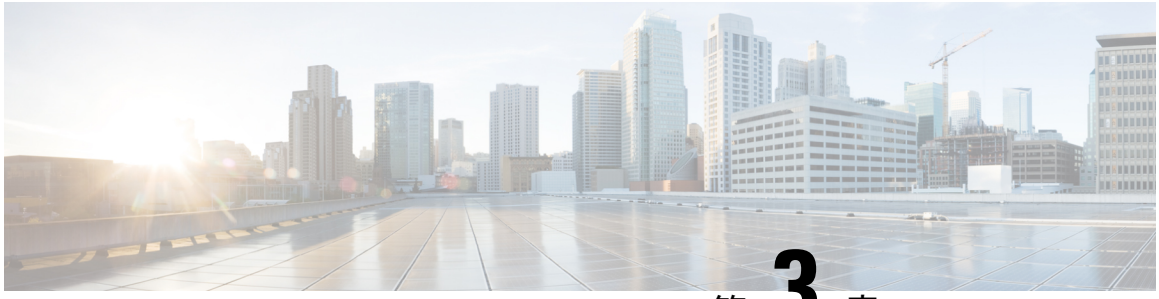
セキュアなクラスタ間ルータ ツー ルータ接続

クラスタ間とクラスタ間のルータツールータ接続の組み合わせである、IM and Presence Service 展開内のすべてのルータツールータ コネクタ間にセキュアな XMPP 接続を設定できます。**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [設定（Settings）] > を選択し、[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）]** をオンにします。

XMPP ルータツールータ接続のセキュア モードをオンにすると、IM and Presence Service は XMPP 信頼証明書を使用してセキュアな SSL 接続を適用します。クラスタ間展開では、IM and Presence Service は、ローカル クラスタ内にある各ルータツールータ コネクタ ノードとリモート クラスタ内にある各ルータ コネクタ ノード間にセキュアな SSL 接続を適用します。

関連トピック

クラスタ間ルータツールータ接続 （34 ページ）



第 3 章

IM and Presence Service の計画の要件

- マルチノード ハードウェアの推奨事項 （37 ページ）
- クラスタ間のハードウェアの推奨事項 （38 ページ）
- サポートされているエンド ポイント （38 ページ）
- サポートされる LDAP ディレクトリ サーバ （39 ページ）
- WAN の帯域幅要件 （39 ページ）
- マルチノードの拡張性とパフォーマンス （40 ページ）
- ユーザ ライセンスの要件 （41 ページ）
- DNS ドメインとデフォルト ドメインの要件 （41 ページ）

マルチノード ハードウェアの推奨事項

マルチノード機能を設定するときには、次の点を考慮してください。

- シスコは、展開で高可用性をオンにすることを推奨します。
- シスコは、Cisco Unified Computing System サーバまたはシスコ認定サードパーティ サーバ設定のみで、IM and Presence Service の仮想化した展開をサポートしています。シスコは、Cisco Media Convergence Server（MCS）サーバでは、IM and Presence の展開をサポートしません。仮想化環境での IM and Presence Service の展開の詳細については、http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment を参照してください。
- 展開の数を最小限に抑えます。たとえば、仮想マシンを 5 台使用して計 2,000 人のユーザをサポートするのではなく、仮想マシンを 2 台使用して計 5,000 人のユーザをサポートします。
- 同世代のサーバ ハードウェアを使用します。
- 展開のどのノードにも同種のハードウェアを使用します。同種のハードウェアの世代をいくつか混在させる必要がある場合は、古いハードウェアの同世代のものを同じプレゼンス冗長グループにまとめ、このプレゼンス冗長グループのユーザ数を、高性能の世代を配置したプレゼンス冗長グループよりも少なくします。ただし、このような展開にすることはお勧めしません。

（注） 混在ハードウェア（たとえば、UCS、MCS、またはVMware）を使用したマルチノード展開の場合は、同じサブクラスタ内の IM and Presence Service サブスクライバ ノードとデータベース パブリッシャ ノードで、データベース サイズを同様にすることを強く推奨します。2台のノード間でデータベース サイズが大きく異なると、サブスクライバ ノードのインストール中にエラーを受信します。

（注） マルチノード展開の場合、混在仮想マシンの展開サイズを使用するのではなく、同じプレゼンス冗長グループ内の IM and Presence Service サブスクライバ ノードとデータベース パブリッシャ ノードで、データベース サイズを同様にすることを強く推奨します。2 台のノード間でデータベース サイズが大きく異なると、サブスクライバ ノードのインストール中にエラーを受信します。

マルチノード機能に対応したサポート対象のハードウェアのリストおよびマルチノード機能のハードウェア ユーザ割り当てガイドラインについては、次の URL にある IM and Presence Service の互換性マトリクスを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

クラスタ間のハードウェアの推奨事項

クラスタ間の展開では、最小サイズの 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 の OVA を実行している限り、複数のクラスタで異なるサイズの OVA を実行できます。

（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 15,000 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 3 万ユーザのキャパシティが必要となります。

サポートされているエンド ポイント

マルチノードのスケーラビリティ機能は、次のエンドポイントをサポートします。

- Cisco Unified Communications Manager（デスクフォン）
- Cisco Jabber
- サードパーティ XMPP クライアント
- Cisco Unified Mobile Communicator

- Microsoft Office Communicator（Microsoft ソフト クライアント）
- Lotus Sametime（Lotus ソフト クライアント）

（注） Lotus クライアントは、リモート コール制御用 IM and Presence Service と連動する Microsoft サーバで使用されます。

- サードパーティ インターフェイス クライアント
- Lync 2010 および 2013 クライアント（Microsoft Office Communicator）

サードパーティのクライアントだけが、ディレクトリ URI IM アドレス スキームをサポートします。他のすべてのクライアントは *USERID @ Default_Domain* IM アドレス スキームを使用する必要があります。詳細については、IM and Presence Service の IM アドレス スキームに関連する項目を参照してください。

サポートされる LDAP ディレクトリ サーバ

IM and Presence Service は次の LDAP ディレクトリ サーバと統合されます。

- Microsoft Active Directory 2000、2003、2008、2012、2016
- Netscape Directory Server
- Sun ONE Directory Server 5.2
- OpenLDAP

関連トピック

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html
http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

WAN の帯域幅要件

最低でも、ラウンドトリップ遅延が 80 ミリ秒以内となるように、各 IM and Presence Service のプレゼンス冗長グループに 5 Mbps の帯域幅を専用にする必要があります。これらの帯域幅の推奨事項は、クラスタ間およびクラスタ間 WAN 展開に適用されます。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。

（注） WAN 展開経由のクラスタリングに追加する各 IM and Presence Service のプレゼンス冗長グループは追加（専用）の 5 Mbps の帯域幅が必要です。

WAN の帯域幅の考慮事項

WAN 上のクラスタリング展開に必要な帯域幅を計算する場合は、次の点を考慮します。

- 帯域幅を考慮する場合、Cisco Unified Communications Manager クラスタの通常の帯域幅使用量を含める必要があります。マルチノードを設定した場合、Cisco Unified Communications Manager はラウンドロビン メカニズムを使用して SIP/SIMPLE メッセージをロード バランシングしますが、より多くの帯域幅が消費されます。パフォーマンスを改善し、トラフィックを減らすために、IM and Presence Service と Cisco Unified Communications Manager との間で送信されるすべての SIP/SIMPLE メッセージに対して単一の専用の Cisco Unified Communications Manager ノードをプロビジョニングできます。
- 帯域幅を考慮する場合、Cisco Unified Personal Communicator ユーザの連絡先リストにおける連絡先の数および IM and Presence のユーザ プロファイルのサイズを考慮することを推奨します。WAN 経由で IM and Presence を展開する場合の連絡先リストのサイズに関する推奨事項については、IM and Presence SRND を参照してください。IM and Presence Service の連絡先リストの最大サイズが 200 であるため、多数のユーザを含むシステムの帯域幅については、この点を考慮する必要があることにも注意してください。

詳細については、『IM and Presence Service ソリューション リファレンス ネットワーク デザイン（SRND）』を参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html

マルチノードの拡張性とパフォーマンス

マルチノードの拡張性要件

IM and Presence Service 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ごとに最大 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、および高可用性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 Service 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。

拡張性は、展開内のクラスタの数によって異なります。詳細な 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。http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CM_IM_and_Presence

マルチノード パフォーマンスの推奨事項

次の場合はマルチノード機能で最適なパフォーマンスを実現できます。

- すべての IM and Presence Service ノードのリソースは、メモリ、ディスク サイズ、および保持時間の観点からは同等です。仮想サーバのハードウェアのクラスが混在していると、ノードの能力が十分に発揮されず、良好なパフォーマンスが得られません。
- 仮想サーバのハードウェア推奨事項に準拠したハードウェアを展開します。
- バランス モードの展開モデルを設定します。この場合、ユーザの総数は、すべてのプレゼンス冗長グループ内のすべてのノードに均等に分散されます。最適なパフォーマンスを実現するために、IM and Presence Service はデフォルトでバランス モードのユーザ割り当てを行います。

関連トピック

マルチノード ハードウェアの推奨事項 （37 ページ）
平衡型ユーザ割り当て冗長高可用性展開

ユーザ ライセンスの要件

IM and Availability 機能にノード ライセンスまたはソフトウェア バージョン ライセンスは必要ありません。ただし、各 IM and Presence Service ユーザに IM and Availability 機能を割り当てる必要があります。

各ユーザに関連付けられているクライアントの数に関係なく、ユーザ単位で IM and Availability を割り当てることができます。IM and Availability をユーザに割り当てると、そのユーザは IM の送受信が可能になり、アベイラビリティのアップデートも送受信できます。ユーザで IM and Availability が有効になっていない場合、そのユーザはアベイラビリティの更新が許可されません。

Cisco Unified Communications Manager の [エンド ユーザの設定（End User Configuration）] ウィンドウでユーザの IM and Presence Service 機能を有効にできます。詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

IM and Availability 機能は、User Connect Licensing（UCL）と Cisco Unified Workspace Licensing（CUWL）の両方に含まれています。詳細については、『Cisco Unified Communications Manager Enterprise License Manager ユーザ ガイド』を参照してください。

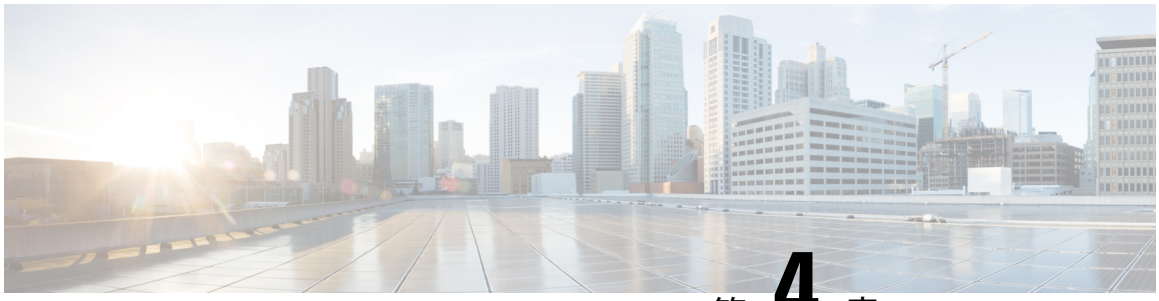
DNS ドメインとデフォルト ドメインの要件

次の DNS ドメインと IM and Presence Service のデフォルト ドメインの条件が適用されます。ドメイン関連の展開の問題を解決するため、クラスタ内のすべての IM and Presence Service のノード名をホスト名ではなく、FQDN または IP アドレスに設定することを推奨します。

- クラスタ間 IM and Presence Service の展開の場合、各 IM and Presence Service クラスタは基礎となっている同じ DNS ドメインを共有している必要があります。
- 任意のクライアント デバイスに関連付けられている DNS ドメインは、 IM and Presence Service DNS ドメインにマッピングする必要があります。
- DNS ドメインが IM and Presence Service のデフォルト ドメインに合っていることを確認します。

  IM and Presence Service のデフォルト ドメイン値は、インストール中に DNS ドメインにデフォルトで設定されます。インストール時に IM and Presence Service のデフォルト ドメインは変更できません。DNS ドメインとは異なる値にデフォルト ドメインを変更するには、Cisco Unified CM IM and Presence の管理 GUI を使用する必要があります。

注意 クラスタ内のすべての IM and Presence Service ノード名をホスト名ではなく FQDN または IP アドレスに設定できない場合は、クラスタ内のノード間の通信障害になる可能性があります。関連する機能には、SIP および XMPP ベースのクラスタ間通信、高可用性、クライアント サインイン、および SIP ベースのリスト サブスクリプションが含まれます。



第 4 章

ワークフロー

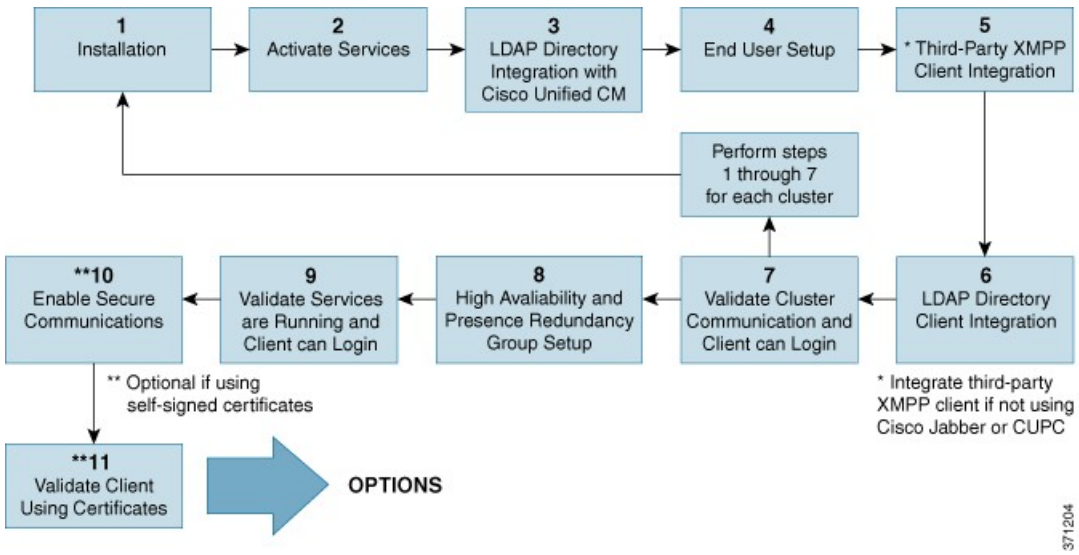
- 高可用性の基本的な展開のワークフロー （43 ページ）
- 高可用性と IP Phone プレゼンスを備えた基本展開のワークフロー （46 ページ）
- フェデレーション展開のワークフロー （49 ページ）

高可用性の基本的な展開のワークフロー

次のワークフロー図に、高可用性の基本的な IM and Presence Service 展開を設定するためのおおまかな手順を示します。基本設定後は、ユーザは基本的な IM 機能、プレゼンス、およびアドホック グループ チャットなどの IM およびアベイラビリティの中心的な機能にアクセスできます。オプション機能は、ユーザ機能を強化するように設定できます。

より高度な展開シナリオとワークフローについては、電話利用状況の設定およびフェデレーションを含むワークフローに関するトピックを参照してください。

図 *3* : 高可用性の *IM and Presence Service* の基本的な展開のワークフロー



次の表に、ワークフローの各タスクについて説明します。

ヒント IM and Presence Service ノードをインストールまたは設定する場合は、次のすべての準備タスクを実行します。展開オプションおよび計画要件に関連するトピックを確認します。

表 *4:* 高可用性の基本的なワークフローのタスク リスト

	タスク	説明
1	インストール	詳細なインストール手順については、『Cisco Unified Communications Manager のインストール』を参照してください。
2	サービスのアクティブ化	ノードをインストールした後に手動で機能サービスをアクティブ化する必要があります。詳細な手順については、『Cisco Unified Communications Manager のインストール』を参照してください。 ヒント ネットワーク サービスは、ノードのインストール後に自動的に起動します。
3	Cisco Unified Communications Manager との LDAP ディレクトリの統合	IM and Presence Service ノードの LDAP ディレクトリ統合をセットアップします。 • Cisco Unified Communications Manager と LDAP ディレクトリの接続を保護します。 • IM and Presence Service および LDAP サーバ間の接続を保護します。 ヒント Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。
4	エンド ユーザのセットアップ	IM and Presence Service 展開のノードおよびプレゼンス冗長グループにユーザを割り当てます。IM and Presence Service 展開のノードには手動または自動でユーザを割り当てることができます。ユーザを割り当てる手順については『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。User Assignment Mode for Presence Server の [エンタープライズ パラメータ（Enterprise Parameter）] を使用して、ユーザ割り当てモードを、バランス、アクティブ/スタンバイ、またはなしに設定します。 ヒント 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します。
5	サードパーティ製 XMPP クライアントの統合	（任意）Cisco Jabber を使用しない場合は、サードパーティ製 XMPP クライアントを統合します。

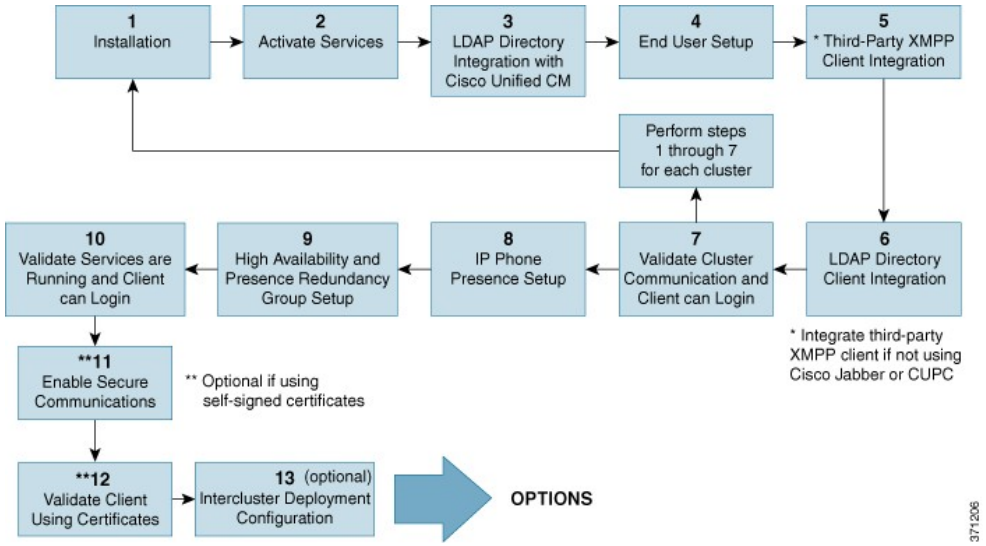
	タスク	説明
6	LDAP ディレクトリのクライアントの統合	LDAP ディレクトリとのユーザの統合の設定： • ユーザ プロビジョニングのための LDAP 同期を設定します。 • LDAP サーバ証明書をアップロードします。 • LDAP ユーザ認証を設定します。 ヒント Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。
7	クラスタ通信とクライアントのログインが可能かどうかの検証	クラスタ内で IM とアベイラビリティをやりとりできることを確認します。IM が送受信でき、ユーザのアベイラビリティの変化が確認できることを確認します。複数のクラスタを設定する場合は、クラスタ全体の基本的な IM とアベイラビリティを検証します。
8	高可用性とプレゼンス冗長グループの設定	高可用性とプレゼンス冗長性グループを設定する手順については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。
9	サービスが実行されていること、およびクライアントがログインできることの検証	サービスが実行中であることを確認する検証タスクを実行します。クライアントが IM and Presence Service にログインできること、そしてアベイラビリティがあることを確認します。
10	セキュア通信の有効化	IM and Presence Service ノードのセキュア通信を有効化する次のタスクを実行します。 • IM and Presence Service および Cisco Unified Communications Manager 間での証明書の交換を設定します。 • IM and Presence Service に CA 署名付き証明書をアップロードします。 • TLS ピア サブジェクト用に IM and Presence Service の SIP セキュリティを設定します。 • （任意）IM and Presence Service の XMPP セキュリティを設定します。
11	証明書を使用してクライアントを検証します。	クライアントが IM and Presence Service にログインできること、そしてアベイラビリティがあることを確認します。

高可用性と IP Phone プレゼンスを備えた基本展開のワークフロー

次のワークフローの図は、高可用性と IP Phone プレゼンスを備えた、IM and Presence Service の基本展開を設定するおおまかな手順です。基本設定後に、ユーザは、基本的な IM 機能、プレゼンス、アドホック グループ チャットなど、コア IM とアベイラビリティの機能にアクセスできます。オプション機能を設定することで、ユーザ機能を強化することができます。

オプション機能を設定することで、ユーザ機能を強化することもできます。機能オプションやその他の展開ワークフローの詳細については、IM and Presence Service および高可用性展開設定の機能やオプションに関連するトピックを参照してください。

図 *4*: 高可用性と *IP Phone* プレゼンスを備えた *IM and Presence Service* の基本ワークフロー



次の表で、ワークフローでの各タスクについて説明します。

表 *5*: 高可用性と *IP Phone* プレゼンスを備えた基本ワークフローのタスク リスト

	タスク	説明
1	インストール	詳細なインストール手順については、『Cisco Unified Communications Manager のインストール』を参照してください。
2	サービスのアクティブ化	ノードをインストールした後に手動で機能サービスをアクティブ化する必要があります。詳細な手順については、『Cisco Unified Communications Manager のインストール』を参照してください。 **ヒント** ネットワーク サービスは、ノードのインストール後に自動的に起動します。

	タスク	説明
3	Cisco Unified Communications Manager との LDAP ディレクトリの統合	IM and Presence Service ノードの LDAP ディレクトリ統合をセットアップします。 • Cisco Unified Communications Manager と LDAP ディレクトリの接続を保護します。 • IM and Presence Service および LDAP サーバ間の接続を保護します。 ヒント Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。
4	エンドユーザのセットアップ	IM and Presence Service 展開のノードおよびプレゼンス冗長グループにユーザを割り当てます。IM and Presence Service 展開のノードには手動または自動でユーザを割り当てることができます。ユーザを割り当てる手順については『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。User Assignment Mode for Presence Server の [エンタープライズ パラメータ（Enterprise Parameter）] を使用して、ユーザ割り当てモードを、バランス、アクティブ/スタンバイ、またはなしに設定します。 ヒント ユーザの移行や連絡先リストのエクスポート/インポートを行う場合は、IM and Presence Service の GUI を使用します。
5	サードパーティ製 XMPP クライアントの統合	（任意）Cisco Jabber を使用しない場合は、サードパーティ製 XMPP クライアントを統合します。
6	LDAP ディレクトリのクライアントの統合	LDAP ディレクトリとのユーザの統合の設定： • ユーザ プロビジョニングのための LDAP 同期を設定します。 • LDAP サーバ証明書をアップロードします。 • LDAP ユーザ認証を設定します。 ヒント Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。

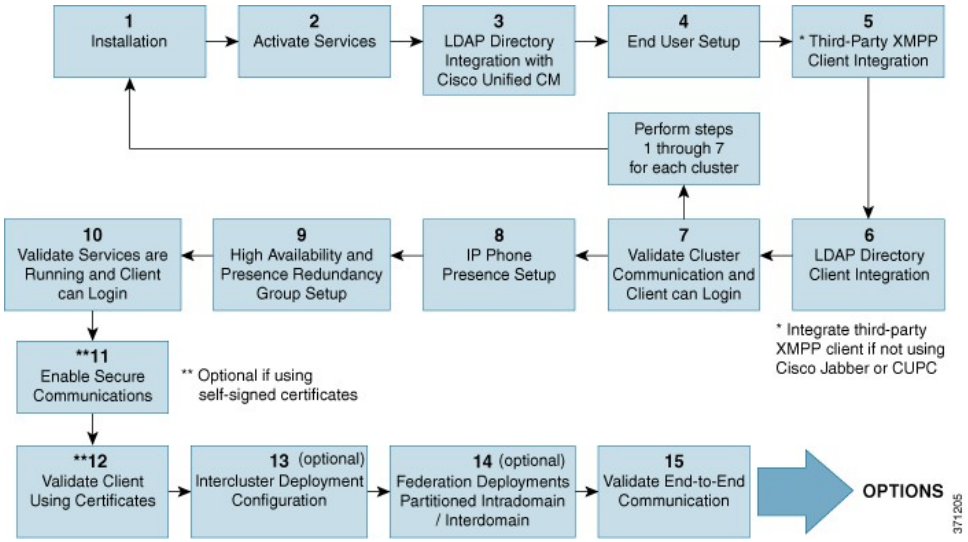
	タスク	説明
7	クラスタ通信とクライアントのログインが可能かどうかの検証	クラスタ内でIMとアベイラビリティをやりとりできることを確認します。IMが送受信でき、ユーザのアベイラビリティの変化が確認できることを確認します。複数のクラスタを設定する場合は、クラスタ全体の基本的なIMとアベイラビリティを検証します。
8	IP Phone Presence の設定	IM and Presence Service ノードで、次を設定します。 • スタティック ルート • プレゼンス ゲートウェイ • SIP パブリッシュ トランク • SIP パブリッシュ トランクのクラスタ全体での DNS SRV 名
9	高可用性とプレゼンス冗長グループの設定	高可用性とプレゼンス冗長グループを設定する手順については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。
10	サービスが実行されていること、およびクライアントがログインできることの検証	サービスが実行中であることを確認する検証タスクを実行します。クライアントが IM and Presence Service にログインできること、そしてアベイラビリティがあることを確認します。
11	セキュア通信の有効化	IM and Presence Service ノードのセキュア通信を有効化する次のタスクを実行します。 • IM and Presence Service および Cisco Unified Communications Manager 間での証明書の交換を設定します。 • IM and Presence Service に CA 署名付き証明書をアップロードします。 • TLS ピア サブジェクト用に IM and Presence Service の SIP セキュリティを設定します。 • （オプション）IM and Presence Service で XMPP セキュリティを設定します。
12	証明書を使用したクライアントの検証	クライアントが IM and Presence Service にログインできること、そしてアベイラビリティがあることを確認します。
13	クラスタ間展開の設定	クラスタ間ピア関係、ルータツールータ接続、ノード名、および IM アドレス スキームを設定します。

フェデレーション展開のワークフロー

次のワークフローの図は、フェデレーション展開用に、高可用性とIP Phoneプレゼンスを備えた、IM and Presence Serviceの展開を設定する場合の基本的な手順を示しています。フェデレーションの詳細な設定手順については、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』ガイドおよび『*Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』ガイドを参照してください。

基本設定後は、ユーザは基本的なIM機能、プレゼンス、およびアドホック グループ チャットなどのIMおよびアベイラビリティの中心的な機能にアクセスできます。オプション機能を設定することで、ユーザ機能を強化することができます。機能オプションの詳細については、IM and Presence Serviceの機能やオプションに関連するトピックを参照してください。

図 *5 : IM and Presence Service* のフェデレーション展開用ワークフロー



次の表で、ワークフローでの各タスクについて説明します。

表 *6 : IM and Presence Service* のフェデレーション用ワークフローのタスク リスト

	タスク	説明
1	インストール	詳細なインストール手順については、『Cisco Unified Communications Manager のインストール』を参照してください。
2	サービスのアクティブ化	ノードをインストールした後に手動で機能サービスをアクティブ化する必要があります。詳細な手順については、『Cisco Unified Communications Manager のインストール』を参照してください。 **ヒント** ネットワーク サービスは、ノードのインストール後に自動的に起動します。

	タスク	説明
3	Cisco Unified Communications Manager との LDAP ディレクトリの統合	IM and Presence Service ノードの LDAP ディレクトリ統合をセットアップします。 • Cisco Unified Communications Manager と LDAP ディレクトリの接続を保護します。 • IM and Presence Service および LDAP サーバ間の接続を保護します。 ヒント Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。
4	エンド ユーザのセットアップ	IM and Presence Service 展開のノードおよびプレゼンス冗長グループにユーザを割り当てます。IM and Presence Service 展開のノードには手動または自動でユーザを割り当てることができます。ユーザを割り当てる手順については『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。User Assignment Mode for Presence Server の [エンタープライズ パラメータ（Enterprise Parameter）] を使用して、ユーザ割り当てモードを、バランス、アクティブ/スタンバイ、またはなしに設定します。 ヒント ユーザの移行や連絡先リストのエクスポート/インポートを行う場合は、IM and Presence Service の GUI を使用します。
5	サードパーティ製 XMPP クライアントの統合	（オプション）Cisco Jabber または Cisco Unified Communications Manager を使用していない場合は、サードパーティ製 XMPP クライアントを統合します。
6	LDAP ディレクトリのクライアントの統合	LDAP ディレクトリとのユーザの統合の設定： • ユーザ プロビジョニングのための LDAP 同期を設定します。 • LDAP サーバ証明書をアップロードします。 • LDAP ユーザ認証を設定します。 ヒント Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。
7	クラスタ通信の検証	クラスタ内で IM とアベイラビリティをやりとりできることを確認します。IM が送受信でき、ユーザのアベイラビリティの変化が確認できることを確認します。複数のクラスタを設定する場合は、クラスタ全体の基本的な IM とアベイラビリティを検証します。

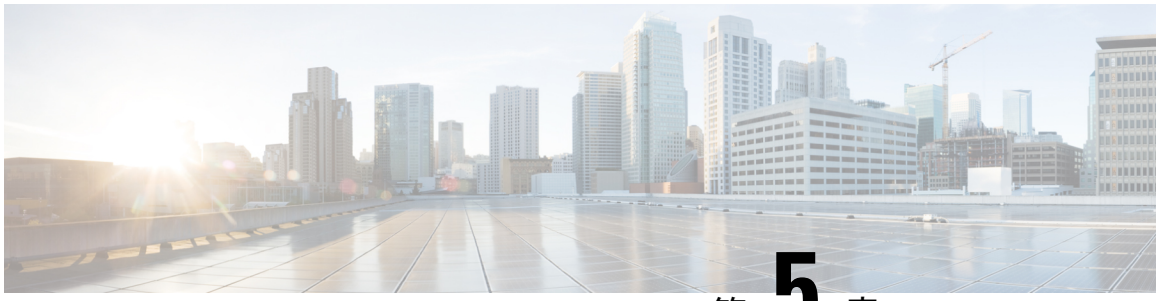
	タスク	説明
8	IP Phone Presence の設定	IM and Presence Service ノードで、次を設定します。 • スタティック ルート • プレゼンス ゲートウェイ • SIP パブリッシュ トランク • SIP パブリッシュ トランクのクラスタ全体での DNS SRV 名
9	高可用性とプレゼンス冗長グループの設定	高可用性とプレゼンス冗長グループを設定する手順については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。
10	サービスが実行されていること、およびクライアントがログインできることの検証	サービスが実行中であることを確認する検証タスクを実行します。クライアントが IM and Presence Service にログインできること、そしてアベイラビリティがあることを確認します。
11	セキュア通信の有効化	IM and Presence Service ノードのセキュア通信を有効化する次のタスクを実行します。 • IM and Presence Service および Cisco Unified Communications Manager 間での証明書の交換を設定します。 • IM and Presence Service に CA 署名付き証明書をアップロードします。 • TLS ピア サブジェクト用に IM and Presence Service の SIP セキュリティを設定します。 • （オプション）IM and Presence Service で XMPP セキュリティを設定します。
12	証明書を使用したクライアントの検証	クライアントが IM and Presence Service にログインできること、そしてアベイラビリティがあることを確認します。
13	クラスタ間展開の設定	クラスタ間ピア関係、ルータツールータ接続、ノード名、および IM アドレス スキームを設定します。
14	フェデレーション展開	ドメイン間フェデレーションまたはパーティション化されたドメイン内フェデレーションを展開に設定します。手順と要件については、『Cisco Unified Communications Manager の IM and Presence Service におけるドメイン間フェデレーション』および『Cisco Unified Communications Manager の IM and Presence Service におけるパーティション ドメイン間フェデレーション』を参照してください。

	タスク	説明
15	エンドツーエンド通信の検証	エンドツーエンド通信を確認する検証タスクを実行します。クラスタ全体で IM とアベイラビリティをやりとりできることを確認します。IM が送受信できること、ユーザのアベイラビリティでその変更が表示できることを確認します。

第 II 部

システム設定（System Configuration）

- IM and Presence Service と統合するための Cisco Unified Communications Manager の設定 （55 ページ）
- 集中展開の設定 （65 ページ）
- IM and Presence Service のネットワーク設定 （87 ページ）
- IP Phone Presence の設定 （117 ページ）
- LDAP ディレクトリ統合 （129 ページ）
- IM and Presence Service のセキュリティ設定 （143 ページ）
- クラスタ間ピアの設定 （179 ページ）



第 5 章

IM and Presence Service と統合するための Cisco Unified Communications Manager の設定

- 統合前の Cisco Unified Communications Manager のユーザおよびデバイス設定のタスク リスト （55 ページ）
- プレゼンス グループ間登録パラメータの設定 （58 ページ）
- Cisco Unified Communications Manager の SIP トランク設定 （58 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の確認 （63 ページ）

統合前の Cisco Unified Communications Manager のユーザおよびデバイス設定のタスク リスト

IM and Presence Service と統合するように Cisco Unified Communications Manager を設定する前に、次のユーザおよびデバイス設定が Cisco Unified Communications Manager で完了していることを確認します。

表 *7 : IM and Presence Service* と統合する前に、*Cisco Unified Communications Manager* のユーザとデバイスを設定するためのタスク リスト

タスク	説明
ユーザ クレデンシャル ポリシーを修正する	この手順は、Cisco Unified Communications Manager リリース 6.0 以降と統合する場合にだけ適用されます。 ユーザのクレデンシャル ポリシーの有効期限を設定することを推奨します。クレデンシャル 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。 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ャルポリシーを使用しません。 **[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [ユーザ管理（User Management）] > [クレデンシャル ポリシーのデフォルト（Credential Policy Default）]**
電話機を設定し、各電話機に電話番号（DN）を関連付ける	**[CTI からデバイスを制御可能（Allow Control of Device from CTI）]** チェックボックスをオンにして、電話が クライアントと相互運用できるようにします。 **[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [デバイス（Device）] > [電話機（Phone）]**
ユーザを設定し、各ユーザにデバイスを関連付ける	ユーザ ID 値が各ユーザで一意になっていることを確認します。 **[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）]**
ユーザをライン アピアランスに関連付ける	この手順は、Cisco Unified Communications Manager リリース 6.0 以降だけに適用されます。 **[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [デバイス（Device）] > [電話機（Phone）]**

タスク	説明
CTI 対応ユーザ グループにユーザを追加する	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。 **[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）]**
（任意）ユーザの directoryURI 値を設定する	IM and Presence Service ノードが Directories URI IM アドレス スキームを使用している場合は、ユーザの directoryURI 値を設定する必要があります。ユーザのディレクトリ URI 値は、Cisco Unified Communications Manager LDAP ディレクトリに同期化するか、または手動で更新できます。 LDAP が有効になっていない場合に LDAP を有効にする、またはユーザのディレクトリ URI 値を手動で編集する手順については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

（注） IM and Presence Service 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 Service から解決可能である必要があります。IM and Presence Service 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。

（注） メニュー オプションおよびパラメータは、Cisco Unified Communications Manager リリースごとに異なる可能性があるため、リリースに適用される Cisco Unified Communications Manager のマニュアルを参照してください。

関連トピック

LDAP ディレクトリ統合 （129 ページ）

プレゼンス グループ間登録パラメータの設定

あるプレゼンス グループのユーザが別のプレゼンス グループのユーザのアベイラビリティ情報に登録することを許可するには、プレゼンス グループ間登録パラメータを有効にします。

制約事項

プレゼンス グループ間登録パラメータを有効にできるのは、デフォルトの標準プレゼンス グループまたは新しいプレゼンス グループの登録権限が [システム デフォルトの使用（Use System Default）] に設定されている場合のみです。プレゼンス グループを設定するには、**[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [プレゼンス グループ（Presence Groups）]** を選択します。

手順

ステップ 1 **[Cisco Unified CMの管理（Cisco Unified CM Administration）] > [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）] メニューから [Cisco Unified Communications Manager] ノードを選択します。

ステップ 3 [サービス（Service）] メニューから **[Cisco CallManager]** を選択します。

ステップ 4 [クラスタ全体のパラメータ（システム - プレゼンス）（Clusterwide Parameters （System - Presence））] セクションでデフォルトのプレゼンス グループ間登録に対して **[登録の許可（Allow Subscription）]** を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

ヒント Cisco Unified Communications Manager で IM and Presence Service をアプリケーション サーバとして手動で追加する必要はありません。

次のタスク

Cisco Unified Communications Manager の SIP トランクを設定します。

Cisco Unified Communications Manager の SIP トランク設定

SIP トランクに設定するポート番号は、展開する IM and Presence Service のバージョンによって異なります。IM and Presence Service リリース 9.0(x) 以降では、SIP トランクにポート番号 5060 を設定します。

IM and Presence Service の SIP トランク セキュリティ プロファイルの設定

手順

ステップ 1 **[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [セキュリティ（Security）] > [SIP トランプ セキュリティ プロファイル（SIP Trunk Security Profile）]** 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 [Non Secure SIP Trunk Profile] をクリックします。

ステップ 4 **[コピー（Copy）]** をクリックして、**[ファイル名（Name）]** フィールドにCUP トランクを入力してください。

ステップ 5 [デバイス セキュリティ モード（Device Security Mode）] の設定が [非セキュア] であることを確認します。

ステップ 6 [着信転送タイプ（Incoming Transport Type）] の設定が [TCP+UDP] であることを確認します。

ステップ 7 [発信転送タイプ（Outgoing Transport Type）] の設定が [TCP] であることを確認します。

ステップ 8 次の項目をオンにして有効にします。

- **[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 9 **[保存（Save）]**をクリックします。

次のタスク

Cisco Unified Communications Manager の SIP トランクの設定に進みます。

IM and Presence Service の SIP トランクの設定

Cisco Unified Communications Manager クラスタと IM and Presence Service クラスタの間には、1 個の SIP トランクのみを設定します。SIP トランクを設定した後、**[Cisco Unified CMの管理（Cisco Unified CM Administration）] > [システム（System）] > [サービスパラメータ（Service Parameters）]** を選択することにより、Cisco Unified Communications Manager でその SIP トランクを IM and Presence PUBLISH トランクとして割り当てる必要があります。

[宛先アドレス（Destination Address）] フィールドで、次の形式の 1 つを使用して値を入力してください。

- ドット付き IP アドレス
- 完全修飾ドメイン名（FQDN）
- DNS SRV

高可用性が IM and Presence クラスタに設定されている場合、クラスタ内の複数のノードを識別するために、複数のエントリをドット付き IP アドレスまたは FQDN で入力する必要があります。高可用性を設定する場合は、DNS SRVは IM and Presence のクラスタに使用できません。

始める前に

- Cisco Unified Communications Manager の SIP トランク セキュリティ プロファイルを設定します。
- プレゼンス ゲートウェイの設定オプションのトピック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）] > [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）] メニューから **[SIP トランク（SIP Trunk）]** を選択します。

ステップ 4 [デバイス プロトコル（Device Protocol）] メニューから **[SIP（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）] で **[なし（None）]** を選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [デバイス名（Device Name）] に「**CUPS-SIP-Trunk**」と入力します。

ステップ 8 [デバイス プール（Device Pool）] メニューからデバイス プールを選択します。

ステップ 9 ウィンドウの下部にある [SIP 情報（SIP Information）] セクションで、次の値を設定します。

a) [宛先アドレス（Destination Address）] フィールドに、ドット付き IP アドレスまたは DNS で解決可能で、IM and Presence ノードで設定された SRV クラスタ名に一致する必要がある FQDN を入力します。

b) マルチノード展開を設定した場合は、**[宛先アドレスはSRVです（Destination Address is an SRV）]** をオンにします。

このシナリオでは、Cisco Unified Communications Manager は名前（たとえば、*_sip._tcp.hostname.tld*）を解決するために DNS SRV レコード クエリを実行します。シングル ノード展開を設定する場合は、このチェックボックスをオフのままにし、Cisco Unified Communications Manager は名前（たとえば、*hostname.tld*）を解決するために DNS A レコード クエリを実行します。

DNS SRV レコードの宛先アドレスとして IM and Presence Service のデフォルト ドメインを使用することを推奨します。

（注） DNS SRV レコードの宛先アドレスとしてドメイン値を指定できます。指定されたドメインにユーザを割り当てる必要はありません。入力したドメイン値が IM and Presence Service のデフォルト ドメインと異なる場合、IM and Presence Service の SRV クラスタ名である SIP Proxy サービス パラメータが DNS SRV レコードで指定するドメイン値に一致することを確認する必要があります。デフォルト ドメインを使用する場合は、SRV クラスタ名パラメータの変更は必要ありません。

いずれの場合も、Cisco Unified Communications SIP トランクの宛先アドレスは DNS によって解決し、IM and Presence のノードで設定された SRV クラスタ名に一致する必要があります。

c) [接続先ポート（Destination Port）] に「`5060`」と入力します。
d) [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] メニューから **[非セキュアな SIP トランク プロファイル（Non Secure SIP Trunk Profile）]** を選択します。
e) [SIP プロファイル（SIP Profile）] メニューから **[標準 SIP プロファイル（Standard SIP Profile）]** を選択します。

ステップ 10 **[保存（Save）]** をクリックします。

トラブルシューティングのヒント

ポート番号または IP アドレスを変更することで Publish SIP trunk SRV レコードの DNS エントリを修正する場合は、そのアドレスに以前にパブリッシュしたデバイスをすべて再起動し、どのデバイスも正しい IM and Presence Service の連絡先を指していることを確認する必要があります。

関連トピック

SIP パブリッシュ トランクのクラスタ全体の DNS SRV 名の設定 （126 ページ）
IM and Presence Service の SIP トランク セキュリティ プロファイルの設定 （59 ページ）
IM and Presence Service の SIP パブリッシュ トランクの設定 （126 ページ）
プレゼンス ゲートウェイの設定オプション （124 ページ）

クラスタ外の Unified Communications Manager の電話利用状況の設定

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。クラスタ外にある Cisco Unified Communications Manager からのデフォルトの要求は、IM and Presence Service では受け付けられません。また、Cisco Unified Communications Manager の SIP トランクも設定できます。

TLS ピア サブジェクトを設定する前に、TLS コンテキストを設定する必要があります。

TLS ピア サブジェクトの設定

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 の管理（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）]** 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（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 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

TLS コンテキストを設定するには、次の手順を使用します。

始める前に

TLS ピア サブジェクトを設定します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [TLS コンテキストの設定（TLS Context Configuration）] 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 [Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context] をクリックします。

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 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 [保存（Save）]をクリックします。

ステップ 7 OAMAgent を再起動します。

ステップ 8 Cisco Presence Engine を再起動します。

ヒント 次の順序で再起動し、変更を有効にします。

必要なサービスが Cisco Unified Communications Manager で実行されていることの確認

Cisco Unified Communications Manager サービスは、Cisco Unified Communications Manager ノード、またはIM and Presence Service ノードから表示、起動、停止できます。次の手順には、Cisco Unified Communications Manager ノードで従う手順が示されています。Cisco Unified Communications Manager サービスを IM and Presence Service ノードから表示するには、**[Cisco Unified IM and Presence の有用性（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [サービスのアクティブ化（Service Activation）]** を選択します。

手順

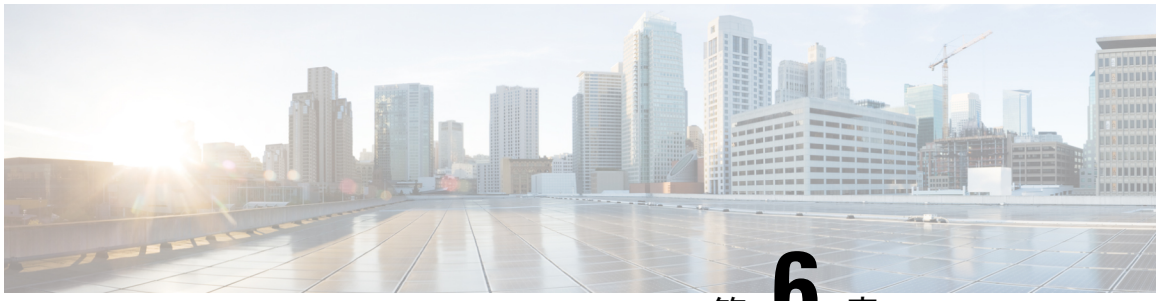
ステップ 1 Cisco Unified Communications Manager で、**[Cisco Unified Serviceability] > [ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 2 [サーバ（Server）] メニューから [Cisco Unified Communications Manager] ノードを選択します。

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。

- 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）

ヒント Cisco Unified Communications Manager のサービスを有効にするには、**[Cisco Unified Serviceability] > [ツール（Tools）] > [サービスのアクティブ化（Service Activation）]** を選択します。



第 6 章

集中展開の設定

- 集中展開の概要 （65 ページ）
- 集中展開の前提条件 （69 ページ）
- 集中展開設定のタスク フロー （71 ページ）
- 集中型の導入の相互作用および制限事項 （85 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 Service 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 Service 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ユニファイド コミュニケーション マネージャ 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 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 Service 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ャノードでは、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ャ 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 パブリッシャ 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（非集中型）展開との比較

次の表では、IM and Presence Service 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。

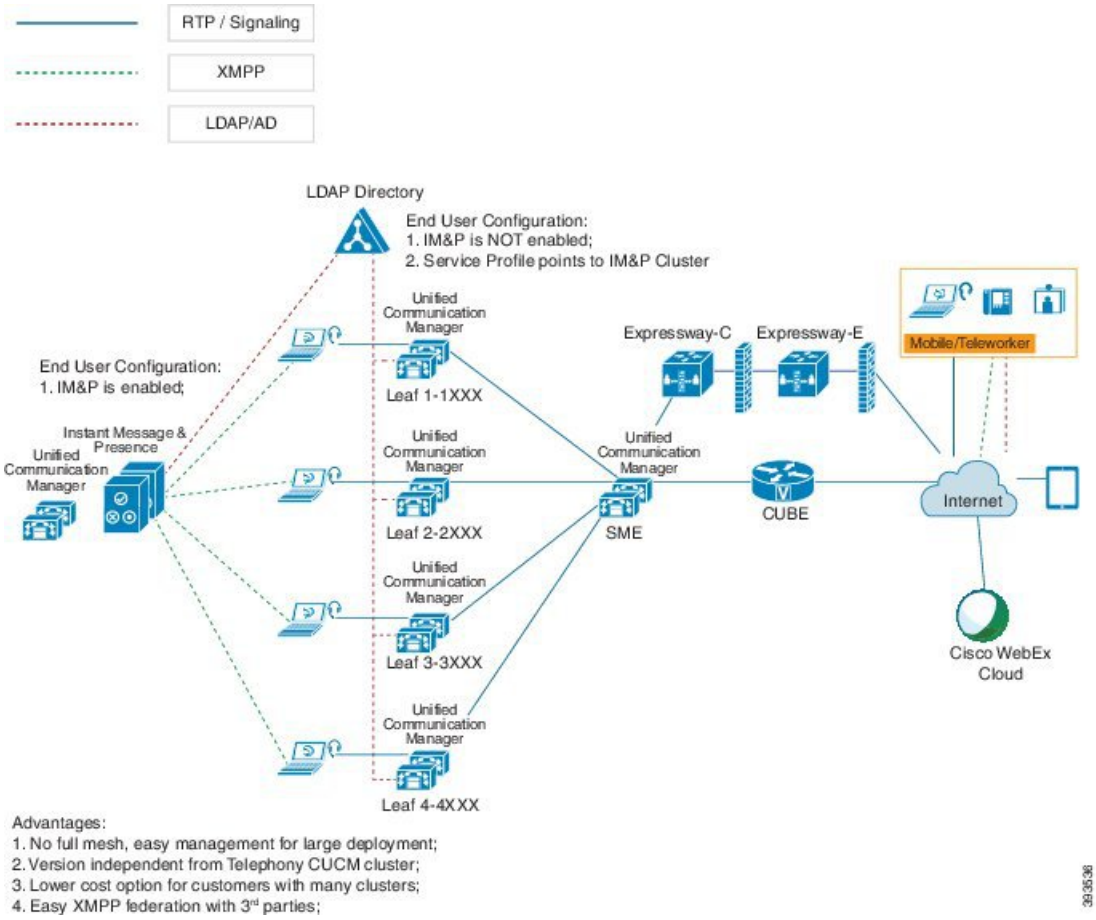
設定段階	標準展開との違い
インストールフェーズ	IM and Presence 中央展開のインストールプロセスは、標準展開と同じです。ただし、中央展開では、IM and Presence 中央クラスタはテレフォニークラスタとは別にインストールされ、別のハードウェアサーバ上に配置される場合があります。トポロジの計画方法によっては、IM and Presence の中央クラスタをテレフォニークラスタとは別の物理ハードウェアにインストールすることができます。 IM and Presence の中央クラスタの場合は、引き続き Cisco Unified Communications Manager をインストールしてから、IM and Presence Service 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ユニファイド コミュニケーション マネージャ 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 コールを処理しません。
設定フェーズ	標準（非集中型）展開と比較すると、IM およびプレゼンスサービスの中央展開を設定するには、以下の追加設定が必要となります。 • テレフォニー クラスタと IM and Presence Service 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 Service 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 Service 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ユニファイド コミュニケーション マネージャ のテレフォニー クラスタ ピアを追加します。 IM およびプレゼンスサービス の標準展開で使用される以下の設定は、集中型展開では必要ありません。 • プレゼンス ゲートウェイは必要ありません。 • SIP パブリッシュ トランクは必要ありません。 • 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ユニファイド コミュニケーション マネージャ 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 およびプレゼンスサービス 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 *6 : IM and Presence Service* の集中型クラスタ アーキテクチャ

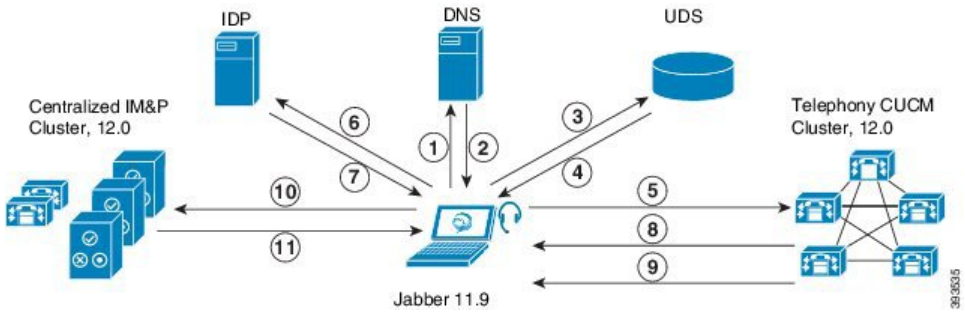


集中型クラスタの使用例

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 に問い合わせて、SRV レコードを取得します。
- [3]-[4]：UDS に問い合せて、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 *7 : IM and Presence Service* の集中型クラスタの使用例



集中展開の前提条件

IM およびプレゼンスサービス の集中展開には、以下の前提条件が必要です。

- IM およびプレゼンスサービス の集中クラスタは、リリース 11.5 SU4 (1) 以降を実行している必要があります。
- IM and Presence の集中クラスタを使用して実行されるローカルの Ciscoユニファイドコミュニケーション マネージャ インスタンスは、IM and Presence の集中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。
- リモートの Ciscoユニファイドコミュニケーションマネージャ 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 以降で実行され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のサポートについては、IMおよびプレゼンスサービス は、少なくとも 11.5 (1) SU4 を実行している必要があります。
- Ciscoユニファイド コミュニケーション マネージャ の機能は、IM and Presence 集中クラスタで動作しているローカル インスタンスではなく、リモート テレフォニー クラスタ上で実行されているCiscoユニファイドコミュニケーションマネージャ のバージョンに依存します。次に例を示します。
  - プッシュ通知の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 更新ログインのサポートについては、リモートの Ciscoユニファイド コミュニケーション マネージャ テレフォニー クラスタは、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 サポートについては、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ブ化（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。
- 集中型展開では、高度なプレゼンスは Cisco Jabber によって処理されます。ユーザの電話でのプレゼンス表示は、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 集中クラスタが接続する Ciscoユニファイド コミュニケーション マネージャ 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」を参照している必要があります。

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の識別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 コントローラの特定に使用されます。ドメイン コントローラの SRV ロケーター リソース レコードを確認するには、以下の方法を使用します。

Active Directory は、以下のフォルダーに SRV レコードを作成します。ドメイン名は、インストールされたドメイン名を表示します。

- 前方参照ゾーン/ドメイン名/_msdcs/dc/_sites/Default-First-Site-Name/_tcp
- 前方参照ゾーン/ドメイン名/_msdcs/dc/_tcp

これらのロケーションには、以下のサービス用のための SRV レコードが表示されます。

- _kerberos
- _ldap

- _cisco_uds : indicates the SRV record

以下のパラメータは、SRV レコードの作成時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（0 が最優先）
- 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：

```
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

新しい IM and Presence の集中型クラスタ展開オプションを構成する場合は、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 およびプレゼンスサービス を展開する場合にのみ使用します。既存の分散 IM and Presence クラスタからすべてのユーザを移行する場合は、ユーザの中央展開への移動 （325 ページ）を参照してください。

表 *8 :* 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	機能グループテンプレート経由の IM and Presence の有効化 （73 ページ）		IM and Presence 中央クラスタで、IM and Presence Service 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 （74 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。

	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 3：	一括管理を介した IM and Presence ユーザの有効化 （75 ページ）		オプション。すでに LDAP 同期を完了している場合は、一括管理を使用して、ユーザの 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 （76 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		M and Presence UC Service の設定 （77 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 （77 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プレゼンス ユーザの無効化 （78 ページ）	テレフォニークラスタで、IM and Presence中央クラスタをポイントするプレゼンスユーザ設定を編集します。
ステップ 8		OAuth 更新ログインの設定 （79 ページ）	テレフォニー クラスタに OAuth を設定すると、集中クラスタの機能が有効になります。
ステップ 9		ILS ネットワークの設定 （80 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。

次の作業

クラスタ間ネットワークの一部として、集中クラスタを別の IM and Presence クラスタに接続する場合は、クラスタ間のピアリングを設定します。

機能グループ テンプレート経由の IM and Presence の有効化

この手順で、集中クラスタの IM and Presence の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 ディレクトリの設定に追加して、同期ユーザに IM and Presence を設定することができます。

（注） 初回同期がまだ行われていない場合にのみ、LDAP ディレクトリ同期に機能グループ テンプレートの編集内容を適用することができます。集中クラスタから LDAP 設定を同期した後は、Ciscoユニファイド コミュニケーション マネージャ の LDAP 設定に編集を適用することはできません。すでにディレクトリを同期している場合は、一括管理を使用して、ユーザの IM and Presence を設定する必要があります。詳細については、一括管理を介した IM and Presence ユーザの有効化 （75 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いてはいけません。

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 [保存（Save）] をクリックします。

次のタスク

設定をユーザに適用するには、初期同期がまだ行われていない場合は、機能グループ テンプレートを LDAP ディレクトリの設定に追加してから初期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 （74 ページ）

IM and Presence 中央クラスタでの LDAP 同期の完了

IM and Presence Service の集中クラスタで 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 Service を持つユーザを設定します。

（注） 初期同期の実行後に、LDAP 同期設定の編集を適用することはできません。初期同期が既に行われている場合には、その代わりに一括管理を使用します。LDAP ディレクトリ同期を設定する方法の詳細については、『Cisco Unified Communications Manager システム コンフィギュレーション ガイド』の「エンド ユーザの設定」を参照してください。

始める前に

機能グループ テンプレート経由の IM and Presence の有効化 （73 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いてはいけません。

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 [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 Service 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 （76 ページ）

一括管理を介した IM and Presence ユーザの有効化

ユーザをすでに中央クラスタに同期させており、それらのユーザが IM and Presence Service 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（Administration's Update）] 機能を使用して、それらのユーザを IM and Presence Service に対して有効にします。

（注） 一括管理の [ユーザのインポート（Administration's Import ）] または [ユーザの挿入（Insert Users）] 機能を使用して、CSVファイルを介して新しいユーザをインポートすることもできます。手順は、*Cisco Unified Communications Manager* 一括管理ガイド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（Filter）] で、[ホーム クラスタが有効になっている（Has Home Cluster Enabled）] を選択して、[検索（Find）]をクリックします。このウィンドウには、ここをホーム クラスタとするすべてのエンド 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。
ユーザ設定の更新 ウィンドウの一番左のチェック ボックスで、この設定をこのクエリで編集するかどうかが表示されます。左側のチェック ボックスをチェックしないと、フィールドはクエリによって更新されません。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ている場合は、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 ボックスには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、以下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、隣接するフィールドの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**：右のチェックボックスを確認します。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 Service のプロバイダーとして有効となります。

ステップ 5 更新が必要な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**の下の**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 Service クラスタに追加します。

（注） 複数のテレフォニー クラスタがある場合は、ILS を導入する必要があります。この場合、IM and Presence 集中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 Service 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の管理（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ユニファイド コミュニケーション マネージャ 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ユニファイドコミュニケーション マネージャ 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 Service が、キーをリモート クラスタと同期させます。

次のタスク

M and Presence UC Service の設定 （77 ページ）

M and Presence UC Service 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 Service 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 クラスタのユーザは、IM and Presence 集中クラスタから IM and Presence Service を取得します。

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**で、IM and Presence の集中型クラスタ 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、あるいは 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、**ホスト名 / IP アドレス** フィールドが集中クラスタのサブスクライバ ノードを指す 2 番目の IM and Presence Service を作成します。

次のタスク

IM and Presence のサービス プロファイルの作成 （77 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 Service 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 **IM and Presence Profile** セクションで、以前のタスクで設定した IM and Presence Service を設定します。

a) **プライマリ** ドロップダウンでデータベース パブリッシャ ノード サービスを選択します。
b) **セカンダリ** ドロップダウンで、サブスクライバ ノード サービスを選択します。

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 クラスタでのプレゼンス ユーザの無効化 （78 ページ）

テレフォニー クラスタでのプレゼンス ユーザの無効化

テレフォニー展開で既に LDAP 同期が完了している場合は、一括管理ツールを使用して、IM and Presence ユーザのテレフォニー クラスタ内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 およびプレゼンスサービス の集中クラスタを指します。

（注） この手順は、テレフォニークラスタのLDAP同期がすでに完了していることを前提としています。ただし、LDAPの初期同期が未完了の場合は、最初の同期にプレゼンスユーザの集中導入設定を追加することができます。この場合は、テレフォニークラスタに対して以下の操作を実行します。

- 先ほど設定した **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。**ホーム クラスタ** オプションが選択されていること、**Unified CM IM and Presence のユーザを有効にする** 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。
- **LDAP ディレクトリ設定**で、**機能グループ テンプレート** を LDAP ディレクトリ同期に追加します。
- 最初の同期を完了します。

機能グループ テンプレートおよびLDAP ディレクトリ同期の設定の詳細は、*Cisco Unified Communications Manager*システム設定ガイドの「エンドユーザの設定(Configure End Users)」セクションを参照してください。

手順

ステップ 1 Cisco Unified CM Administration で、**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)**を選択します。

ステップ 2 フィルタで、**ホーム クラスタが有効(Home Cluster Enabled)**を選択し、**検索(Find)**をクリックします。このウィンドウには、ここをホーム クラスタとするすべてのエンド 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。
ユーザ設定の更新 ウィンドウの一番左のチェック ボックスで、この設定をこのクエリで編集するかどうかが表示されます。左側のチェック ボックスをチェックしないと、フィールドはクエリによって更新されません。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ている場合は、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 ボックスには新しい設定を入力する必要があります。

ステップ 4 **サービスの設定** で、以下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てから、隣の設定を以下に従って編集します。

- **ホーム クラスタ**：ホーム クラスタとしてテレフォニー クラスタを有効にするには、右側のチェック ボックスをオンにします。
- **Unified CM IM and Presence のユーザを有効にする**：右のチェックボックスはオンにしません。この設定では、IM and Presenceのプロバイダーとしてテレフォニー クラスタを無効にします。
- **UC サービス プロファイル**—ドロップ ダウンから、先ほど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およびプレゼンスサービスのプロバイダーとなる IM and Presenceの集中クラスタがユーザに表示されます。

（注） Expressway MRA 構成の詳細は、https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html の *Cisco Expressway* を介したモバイルおよび*Remote Access*導入ガイドを参照してください。

ステップ 5 残りのすべてフィールドの入力を完了します。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**の下の**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 更新ログインの設定 （79 ページ）

OAuth 更新ログインの設定

テレフォニー クラスタ内の OAuth 更新ログインを有効にします。これで、集中クラスタでこ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 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 と OAuth の設定** の下で、**更新ログイン フローを使用した OAuth** のエンタープライズ パラメータを **有効**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（Save）**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することができます。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、『Cisco Unified Communications Manager システム設定ガイド』の「ダイヤル プランの設定」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 ソリューション リファレンス ネットワーク デザイン』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 （81 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。

	コマンドまたはアクション	目的
ステップ 2	テレフォニー クラスタでの ILS の有効化 （81 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 （83 ページ）	ILS が動作している場合、使用するテレフォニー クラスタの [ILS設定（ILS Configuration）] ウィンドウで、「最新」同期ステータスのすべてのリモート クラスタを確認することができます。

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 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 [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 （81 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を含むヘルプは、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 （81 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、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「証明書の管理」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 （83 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。

MRA 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ユニファイド コミュニケーション マネージャ 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 サービスを使用することができます。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。

ソリューション全体で提供されるものは以下の通りです。

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

Configuration

すべてのテレフォニー リーフ クラスタ上の MRA を Expressway-C. で設定するには、**設定 → Unified Communications → Unified CM Servers**を選択します。

集中 IM and Presence ノード上の MRA を Expressway-C. で設定するには、**設定→ Unified Communications →IM およびプレゼンスサービス ノード**を選択します。

モバイルおよびRemote Accessを有効にするには、**設定 →「モバイルおよびRemote Access」の有効化** を選択して、以下の表に従って制御オプションを選択します。

表 *9 : 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（On）
OAuth トークンによる承認	オン（On）
ユーザ クレデンシャルによる承認	いいえ（No）
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	いいえ（No）
内部認証の可用性の確認（Check for internal authentication availability）	はい（Yes）

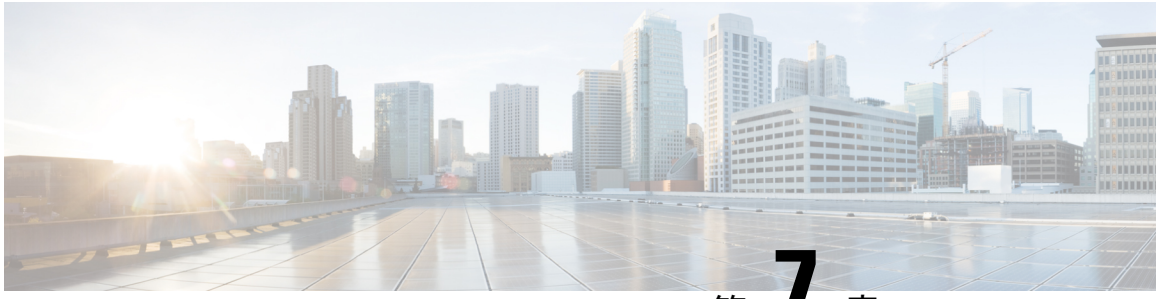
表 *10 : OAuth* 無効化設定

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（Off）
ユーザ クレデンシャルによる承認	オン（On）
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（Off）
内部認証の可用性の確認（Check for internal authentication availability）	はい（Yes）

（注） **基本的な MRA の設定については、以下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

集中型の導入の相互作用および制限事項

機能	データのやり取り
ILS ハブ クラスタ	ILS ハブ クラスタがダウンしており、複数のテレフォニー クラスタが存在する場合、集中クラスタ機能は動作しません。
ILS の展開	IM and Presence 集中クラスタを使用しており、ILS も導入している場合は、ILS をテレフォニー クラスタに導入することもできます。IM and Presence クラスタ用の Ciscoユニファイド コミュニケーション マネージャ のインスタンスでは、ILS を展開することはできません。このインスタンスは、プロビジョニングのためのもので、テレフォニーを処理するものではありません。
高度なプレゼンス	集中型展開では、ユーザのリッチプレゼンスが 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。	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。 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。 （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。



第 7 章

IM and Presence Service のネットワーク設定

- 設定変更通知およびサービス再起動通知 （87 ページ）
- DNS ドメイン コンフィギュレーション （89 ページ）
- IM and Presence Service のデフォルト ドメインの設定 （93 ページ）
- IM アドレス設定 （95 ページ）
- IM and Presence Service クラスタのドメイン管理 （102 ページ）
- IM and Presence Service のルーティング情報の設定 （106 ページ）
- IPv6 設定（IPv6 Configuration） （110 ページ）
- プロキシ サーバの設定 （114 ページ）
- IM and Presence Service のサービス （114 ページ）

設定変更通知およびサービス再起動通知

サービス再起動通知

Cisco Unified CM IM and Presence の管理で IM and Presence XCP サービスに影響する設定変更を行う場合は、変更を有効にするために XCP サービスを再起動する必要があります。IM and Presence Service は、設定変更が影響する正確なノードおよび再起動する必要があるサービスを通知します。アクティブな通知のポップアップ ウィンドウが Cisco Unified CM IM and Presence の管理の各ページに表示され、サービスを再起動する必要があることを視覚的に示します。マウスをダイアログ バブル アイコンに合わせると、アクティブな通知（存在する場合）および関連する重大度の一覧が表示されます。アクティブな通知のリストから Cisco Unified IM and Presence Serviceability に直接アクセスして、必要なサービスを再起動できます。

特にネットワークに IM and Presence Service を展開した後で設定変更を行う場合は、サービス再起動通知のサービス再起動ポップアップ ウィンドウをモニタすることを推奨します。付属マニュアルのほとんどのタスクでは、サービスの再起動が必要かどうかが示されます。

サービス通知のタイプおよびサービス通知のセキュリティ レベルに関する情報については、サービス再起動通知のオンライン ヘルプ トピックを参照してください。

（注） Cisco XCP Routerや Cisco Presence Engine、あるいはその両方を連続して再起動することは推奨しません。ただし、以下のように再起動する必要がある場合は、最初のサービスを再起動し、JSM のすべてのセッションが再作成されるまで待機します。JSM セッションがすべて作成されたら、2 つ目の再起動を実行します。

Cisco XCP Router の再起動

すべてのアベイラビリティおよびメッセージング サービスが IM and Presence Service で適切に機能するには、Cisco XCP Router を実行する必要があります。これは、SIP ベースと XMPP ベースの両方のクライアント メッセージングに適用されます。Cisco XCP Routerを再起動すると、IM and Presence Service によりすべてのアクティブな XCP サービスが自動的に再起動されます。

このモジュールのトピックは、設定変更後に Cisco XCP Router を再起動する必要があるかどうかを示します。Cisco XCP Routerは、停止して再開するのではなく、再起動する必要があります。Cisco XCP Router を再起動するのではなく停止した場合、IM and Presence Service により他のすべての XCP サービスが停止されます。その後 XCP ルータを起動しても、IM and Presence Service により他の XCP サービスは自動的に起動されません。手動で他の XCP サービスを起動する必要があります。

Cisco XCP Router サービスの再起動

手順

ステップ 1 IM and Presence Service で、**[Cisco Unified IM and Presence Serviceability（Cisco Unified IM and Presence Serviceability）] > [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 ノードを [サーバ（Server）] リストボックスから選択して、**[進む（Go）]** を選択します。

ステップ 3 [IM and Presence Service（IM and Presence Service）] セクションで、[Cisco XCP Router（Cisco XCP Router）] サービスの横にあるオプション ボタンをクリックします。

ステップ 4 [再起動（Restart）] をクリックします。

ステップ 5 再起動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。

高可用性でのサービスの再起動

高可用性を無効にしてから Cisco XCP Router、Cisco Presence Engine、またはサーバ自体を再起動する必要のある、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、高可用性を有効にする前に 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高可用性を無効にし、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 Router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。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高可用性を有効にできます。

（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 RouterやCisco Presence Engine、あるいはその両方を連続して再起動することは推奨しません。ただし、以下のように再起動する必要がある場合は、最初のサービスを再起動し、JSM のすべてのセッションが再作成されるまで待機します。JSM セッションがすべて作成されたら、2 つ目の再起動を実行します。

DNS ドメイン コンフィギュレーション

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 Service 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。いくつかのサンプル ノード展開オプションは、次のとおりです。

（注） ある IM and Presence Service ノード名がホスト名だけに基づいている場合、すべての IM and Presence Service 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 Service 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 Service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。

詳細情報については、『Cisco Unified Communications Manager および IM and Presence Service における IP アドレスとホスト名の変更』を参照してください。

関連トピック

Cisco Unified Communications Manager クラスタに関連付ける DNS ドメインの指定 （92 ページ）

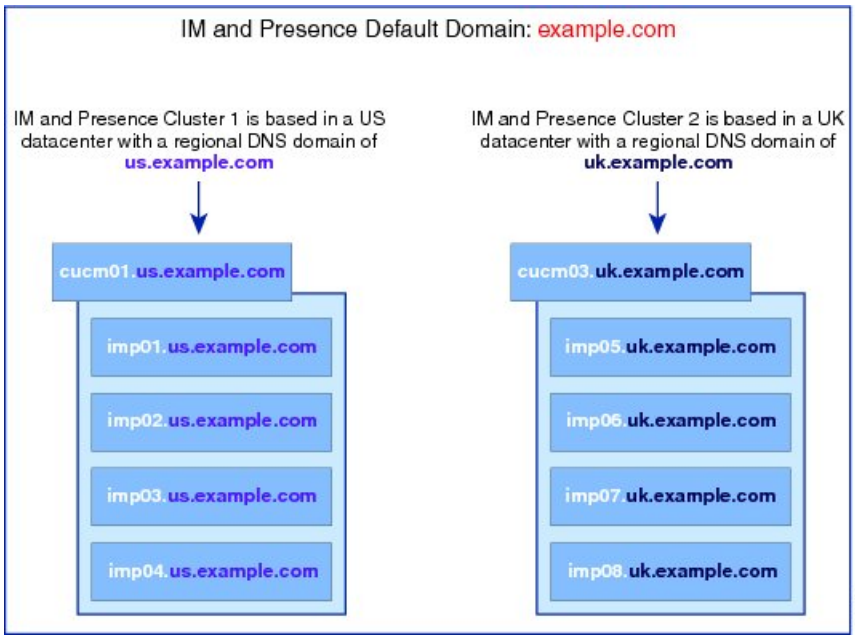
IM and Presence Service のデフォルト ドメインの設定

ノード名の推奨事項

別々の 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

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。

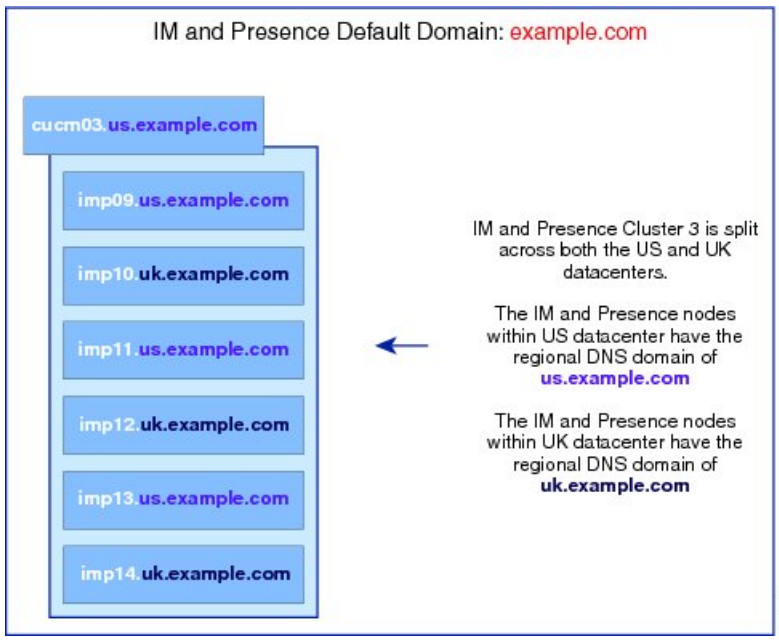
図 *8 :* 別々の *DNS* ドメインまたはサブドメインに展開された *IM and Presence Service* クラスタ



別々の DNS ドメインまたはサブドメインに展開されたクラスタ内の IM and Presence Service ノード

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。

図 *9*：別々の *DNS* ドメインまたはサブドメインに展開されたクラスタ内の *IM and Presence Service* ノード

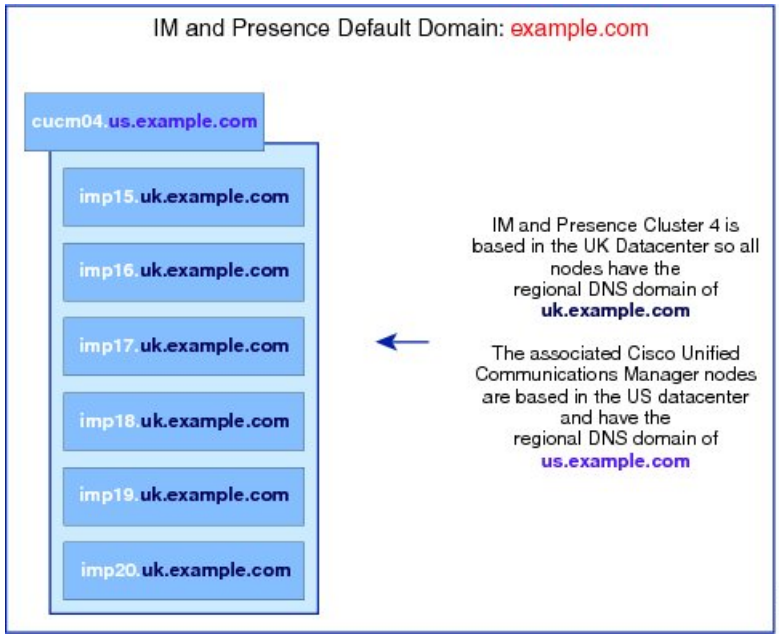


（注） 高可用性は、プレゼンス冗長グループ内の 2 台のノードが別々の DNS ドメインまたはサブドメインにあるシナリオでも完全にサポートされます。

関連する Cisco Unified Communications Manager クラスタとは異なる DNS ドメインに展開されているクラスタ内の IM and Presence Service ノード

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。

図 *10 :* 関連する *Cisco Unified Communications Manager* クラスタとは異なる *DNS* ドメインに展開されているクラスタ内の *IM and Presence Service* ノード



（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。

デフォルトでは、CUCM ドメインの SIP Proxy 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。したがって、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、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 の管理 GUI を使用してこのサービス パラメータを更新する必要があります。詳細については、トピック「*Specify DNS domain associated with Cisco Unified Communications Manager*」を参照してください。

Cisco Unified Communications Manager クラスタに関連付ける DNS ドメインの指定

（注） この手順は、IM and Presence データベース パブリッシャ ノードの DNS ドメインが Cisco Unified Communications Manager ノードの DNS ドメインとは異なる場合にのみ必要です。

IM and Presence Service はクラスタ内のすべての Cisco Unified Communications Manager ノード用の アクセス コントロール リスト（ACL）エントリを維持します。これにより、ノード間での

アベイラビリティのシームレス共有が可能になります。これらの ACL エントリは FQDN ベースであり、Cisco Unified Communications Manager のホスト名を IM and Presence データベース パブリッシャ ノードの DNS ドメインに付加することによって生成されます。

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 ノードの DNS ドメインとは異なる場合、無効な ACL エントリが追加されます。これを回避するには、IM and Presence データベース パブリッシャ ノードの Cisco Unified CM IM and Presence の管理 GUI で次の手順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 Service（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 リストから、[Cisco SIP Proxy（Cisco SIP Proxy）] を選択します。

ステップ 4 Cisco Unified Communications Manager ノードの DNS ドメインと一致するように [一般的なプロキシ パラメータ（クラスタ全体）（General Proxy Parameters（Clusterwide））] セクションの **[CUCM ドメイン（CUCM Domain）]** フィールドを編集します。

デフォルトで、このパラメータは 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。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

DNS ドメイン コンフィギュレーション （89 ページ）

IM and Presence Service のデフォルト ドメインの設定

クラスタ内で IM and Presence Service のデフォルト ドメイン 値を変更する場合、この手順に従ってください。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。

注意 この手順の一環として、サービスを停止する前に、プレゼンス冗長グループの高可用性を無効にします。高可用性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。高可用性を無効にする前に、[プレゼンス トポロジ（Presence Topology）] ウィンドウに表示される各ノードに割り当てられたユーザ数を記録します。

高可用性を無効にした後、さらに設定を変更する前に、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。

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 Service ノードの DNS ドメインを変更する方法の手順については、『Cisco Unified Communications Manager および IM and Presence Service における IP アドレスとホスト名の変更』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。

手順

ステップ 1 表示された順番で、クラスタ内のすべての IM and Presence Service ノードで次のサービスを停止します。

- Cisco Client Profile Agent
- Cisco XCP Router

  （注） Cisco XCP Routerを停止すると、すべての XCP 機能サービスは自動的に停止します。

- Cisco Sync Agent
- Cisco SIP Proxy
- Cisco Presence Engine

ステップ 2 IM and Presence Service データベース パブリッシャ ノードで、新しいドメイン値を設定するには、次のステップを実行します。

a) **[Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [詳細設定（Advanced Configuration）]** を選択します。
b) [デフォルトドメイン（Default Domain）] を選択します。
c) [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。

ステップ 3 クラスタ内のすべてのノードで、手動でこの手順の初めで停止したすべてのサービスを起動します。

クラスタ内のすべてのノードで、前に実行されていた、XCP機能サービスを手動で再起動します。

次のタスク

更新前に高可用性が有効になっていた場合は、高可用性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。確認しない場合、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。

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、高可用性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。すべてのJabberセッションが 30 分経っても再作成されない場合、システムに大きな問題があります。Jabberセッションがアクティブになったら、プレゼンス冗長グループ内で高可用性を再度有効にします。

IM アドレス設定

IM アドレスの設定要件

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。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。

次のサービスは、IM アドレス スキームを設定する前に、クラスタ内のすべてのノードで停止させる必要があります。

- Cisco Client Profile Agent
- Cisco XCP Router
- Cisco Sync Agent
- Cisco SIP Proxy
- Cisco Presence Engine

IM and Presence Service で IM アドレスを設定する前に、各 IM アドレスに固有の詳細な要件については連動操作と制約事項についてのトピックを、追加情報については IM アドレス設定の計画のトピックを参照してください。

UserID @ Default_Domain IM アドレス インタラクションと制約事項

次の制約事項は *USERID @ Default_Domain* IM アドレス スキームに適用します。

- UserID@Default_Domain IM アドレスは一意である必要があり、既存の IM アドレス、ディレクトリ URI、またはユーザ ID と一致していてはなりません。一意になっていないと、エラーが発生します。
- ユーザ ID がすでに UPN 形式である場合、IM and Presence Service は最初の @ をエスケープします（たとえば、ユーザ ID が `alice@cisco.com` の場合、IM アドレスは `alice%20%cisco.com@cisco.com` となります）。
- すべての 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。
- IM アドレス スキームは、すべての IM and Presence Service クラスタ全体で一貫している必要があります。
- 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。
- *userid* が Cisco Unified Communications Manager の LDAP フィールドにマップされる場合、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。

ディレクトリ URI IM アドレスの連携動作と制約事項

複数のドメイン設定をサポートするには、IM and Presence Service の IM アドレス スキームとしてディレクトリ URI を設定する必要があります。

注意 IM アドレス スキームとしてディレクトリ URI を使用するように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 スキームを使用する場合は、次の制約事項および連係動作を順守します。

- ディレクトリ URI は一意である必要があり、既存の IM アドレス、ディレクトリ URI、またはユーザ ID と一致していてはなりません。一意になっていないと、エラーが発生します。
- ユーザ ID が UPN 形式（UserID が `alice@cisco.com` など）で、ディレクトリ URI が IM アドレス方式に使用されている場合、ディレクトリ URI はユーザ ID と異なっている必要があります。異なっていないと、エラーが発生します。
- すべてのユーザに Cisco Unified Communications Manager に有効なディレクトリ URI 値が設定されています。

- 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。

（注） 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。

- IM アドレス スキームは、すべての IM and Presence Service クラスタ全体で一貫している必要があります。
- すべてのクラスタが、ディレクトリ URI アドレス スキームをサポートする Cisco Unified Communications Manager のバージョンを実行している必要があります。
- LDAP 同期が無効になっている場合は、ディレクトリ URI を自由形式の URI として設定することができます。LDAP ディレクトリ同期が有効になっている場合は、ディレクトリ URI を電子メール アドレス（mailid）または Microsoft OCS/Lync SIP URI（msRTCSIP-PrimaryUserAddress）にマップできます。
- 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。
- ディレクトリ URI を IM アドレス形式として設定する場合、ユーザには有効なディレクトリ URI が必要です。そうしないと、Jabber クライアントはログインできません。URI のドメイン部分は数字で始めることはできず、IP アドレスを含むことはできないことに注意してください。

  たとえば、`joe@5.cisco.com`、`joe@cisco.5com`、および `joe@10.10.10.1` はすべて無効なディレクトリ URI です。

  `joe5@.cisco.com` または `5joe@.cisco.com` は、有効なディレクトリ URI です。

IM アドレス タスク フローの設定

システムの IM アドレスを設定するには、次のタスクを完了します。

（注） 既存の IM ユーザ アドレスを編集するだけで、デフォルト ドメインまたは IM アドレス スキームを変更しない場合は、手順 4 に進むことができます。

手順

	コマンドまたはアクション	目的
ステップ 1	サービスの停止 （99 ページ）	IM アドレスの設定を更新する前に、基本の IM and Presence Service を停止する必要があります。
ステップ 2	IM アドレス スキームの割り当て （100 ページ）	デフォルト ドメイン、IM アドレス スキームなどの新しい設定によって IM アドレスの設定を更新します。
ステップ 3	サービスの再起動 （101 ページ）	基本の IM and Presence Service を再起動します。ユーザ アドレスを更新したりユーザをプロビジョニングしたりする前に、サービスを再起動する必要があります。
ステップ 4	IM ユーザ アドレスの更新	Cisco Unified Communications Manager で対応するユーザ設定を設定することにより、IM ユーザ アドレスを更新します。設定した IM アドレス スキームによって、どのエンドユーザ情報が IM アドレスを取得するかが決まります。 • 新しい IM ユーザのプロビジョニングについては、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『Cisco Unified Communications Manager システム コンフィギュレーション ガイド』の「エンド ユーザの設定」のパートを参照してください。 • 既存のユーザ設定の編集については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『Cisco Unified Communications Manager アドミニストレーション ガイド』の「エンド ユーザの管理」の章を参照してください。

サービスの停止

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

サービスを停止する前に高可用性（HA）を無効にします（設定している場合）。そのようにしないと、システム フェールオーバーが発生します。手順は次のとおりです。

- IM and Presence Service の [プレゼンストポロジ（Presence Topology）] ウィンドウで、各クラスタ ノードに割り当てられたユーザ数を記録します。
- Cisco Unified Communications Manager の [プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウで、サブクラスタ内の高可用性を無効にします。
- 変更後、サービスを停止する前に HA 設定がクラスタ間で同期するまで少なくとも 2 分間待ちます。

高可用性の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『Cisco Unified Communications Manager システム コンフィギュレーション ガイド』の「プレゼンス冗長グループ」の章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 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

サービスが停止したら、IM アドレス スキームを更新できます。

IM アドレス スキームの割り当て （100 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

アドレス スキームを設定する前にサービスを停止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。

サービスの停止 （99 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。これがデフォルトの設定です。
- **[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。

ステップ 4 [保存（Save）] をクリックします。

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。

（注） ディレクトリ URI またはユーザ ID が重複していないことをさらに確認するには、次の手順を実行します。

- `utils users validate all` CLI コマンドを実行し、重複しているディレクトリ URI およびユーザ ID がないかシステムをチェックします。
- **Cisco IM and Presence Data Monitor** ネットワーク サービスが実行されていることを確認します（サービスはデフォルトで実行されています）。このサービスは、重複しているディレクトリ URI およびユーザ ID がないかどうか自動的に定期的にチェックします。チェック間隔を設定するには、を参照してください。 ユーザ チェック間隔の設定 （314 ページ）

次のタスク

アドレス スキームが割り当てられると、サービスを再起動できます。

サービスの再起動 （101 ページ）

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しい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。

始める前に

IM アドレス スキームの割り当て （100 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

更新前に高可用性を有効にしていた場合は、すべての Cisco Jabber セッションを再作成した後で高可用性を再度有効にできます。サービスが再起動してから 30 分経っていない場合は、すべてのクラスタ ノードで `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI コマンドを実行して、Jabber セッションが再作成されていることを確認します。アクティブセッションの数は、アップグレード前に高可用性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。セッションの再開に 30 分以上かかる場合、システムに大きな問題があります。Jabber セッションがアクティブになったら、プレゼンス冗長グループ内で高可用性を再度有効にします。

サービスが起動したら、エンド ユーザ IM アドレスを更新できます。IM アドレスは、設定されている IM アドレス スキームに応じて Cisco Unified Communications Manager でプロビジョニングされるユーザ ID またはディレクトリ URI から取得されます。

- 新しい IM ユーザのプロビジョニングについては、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『Cisco Unified Communications Manager システム コンフィギュレーション ガイド』の「エンド ユーザの設定」のパートを参照してください。
- 既存のユーザ設定の編集については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『Cisco Unified Communications Manager アドミニストレーション ガイド』の「エンド ユーザの管理」の章を参照してください。

IM and Presence Service クラスタのドメイン管理

Cisco Unified CM IM and Presence の管理 GUI を使用して、ローカル IM アドレス ドメインを手動で追加、更新、削除できます。

[IM and Presence ドメイン（IM and Presence Domain）] ウィンドウに次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、手動で追加されたが、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。有効化または無効化するドメインはありません。

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がそのドメインに割り当てられると、そのドメインは管理者が管理するドメインからシステムが管理するドメインに変更されます。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。

（注） 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 Service クラスタ内のすべてのノードがリリース 10.0 以降を使用して実行しており、ディレクトリ URI IM アドレッシングが設定されていることを確認します。

IM ドメイン管理のインタラクションと制約事項

- ローカル クラスタに関連付けられている管理者が管理するドメインのみを追加または削除できます。
- システムが管理するドメインは編集できません。
- 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。
- 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ます。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 クラスタで使用中であると識別されます。
- 一部のセキュリティ証明書は、手動でドメインを追加、更新、または削除した後で再作成することが必要になる場合があります。自己署名証明書または証明書署名要求（CSR）を生成すると、サブジェクト共通名（CN）がノードの FQDN に設定されます。また、ローカルの IM and Presence のデフォルト ドメインおよび システムがホストするすべての追加ドメインが、サブジェクトの別名（SAN）として証明書に追加されます。
- TLS による XMPP フェデレーションでは、IM アドレス ドメインを追加または削除する場合、TLS 証明書を再作成する必要があります。

IM アドレス ドメインの表示

IM and Presence Service の展開全体で、システムおよび管理者によって管理されるすべてのプレゼンス ドメインは、[プレゼンス（Presence）] > [ドメイン（Domains）] > [ドメインの検索/一

覧表示（Find and List Domains）] ウィンドウに表示されます。いずれかの情報フィールドのチェック マークは、ドメインがローカル クラスタに、または任意のピアのクラスタに関連付けられてるかどうかを示します。管理者が管理するプレゼンス ドメインに関して、次の情報フィールドが表示されます。

- ドメイン
- ローカル クラスタに設定されている
- ピアのクラスタに設定されている

システムが管理するプレゼンス ドメインに関して、次の情報フィールドが表示されます。

- ドメイン
- ローカル クラスタで使用中
- ピアのクラスタで使用中

手順

[Cisco Unified CM IM and Presence Administration] > **[プレゼンス（Presence）]** > **[ドメイン（Domains）]** を選択します。[ドメインの検索と一覧表示（Find and List Domains）] ウィンドウが表示されます。

IM アドレス ドメインの追加または更新

Cisco Unified CM IM Presence 管理 GUI を使用して、ローカル クラスタに手動で IM アドレス ドメインを追加し、ローカル クラスタにある既存の IM アドレスのドメインを更新できます。

最大255文字のドメイン名を入力でき、各ドメインはクラスタ全体で一意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。

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。IM アドレス ドメインを持つシステムでユーザが設定されていない場合（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。

手順

ステップ 1 **[Cisco Unified CM IM and Presence Administration]** > **[プレゼンス（Presence）]** > **[ドメイン（Domains）]** 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。

ヒント 警告メッセージが表示されます。TLS XMPP フェデレーションを使用した場合、新しい TLS 証明書を生成する手順に進みます。

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す。

（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。

手順

ステップ 1 **[Cisco Unified CM IM and Presence Administration] > [プレゼンス（Presence）] > [ドメイン（Domains）]** 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。

IM and Presence Service のルーティング情報の設定

ルーティング通信の推奨事項

ルータ間通信は、IM and Presence Service で XCP ルート ファブリックを確立するためのデフォルトのメカニズムです。この場合、IM and Presence Service は動的にクラスタ内のノード間のすべてのルータ間接続を設定します。クラスタのすべてのノードが同じマルチキャスト ドメイン内にあるわけではない場合は、このルーティング設定タイプを選択します。ルータ間通信を選択する場合は、次のことに注意してください。

- 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。
- 新しいノードを追加するときは、展開内のすべてのノードで Cisco XCP Router を再起動する必要はありません。
- ノードを削除する場合は、展開内のすべてのノードで Cisco XCP Router を再起動する必要があります。

または、MDNS を展開に選択できます。MDNS ルーティングの要件は、クラスタのすべてのノードが同じマルチキャスト ドメインにあることです。MDNS ルーティングは、XCP ルート ファブリックに参加する新しい XCP ルーターをシームレスにサポートできます。

ルーティング通信として MDNS を選択する場合は、ネットワークでマルチキャスト DNS を有効にする必要があります。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（クラスタを構成するノードが含まれている領域など）で有効です。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 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。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。

MDNS ルーティングとクラスタ ID の設定

インストール時に、システムは固有のクラスタ ID を IM and Presence データベース パブリッシャ ノードに割り当てます。システムはクラスタ ID を配布して、クラスタ内のすべてのノー

ドが同じクラスタ ID 値を共有できるようにします。クラスタ内のノードは、クラスタ ID を使用して、MDNS を使用するマルチキャスト ドメインにある他のノードを識別します。MDNS ルーティングの要件は、1 つのスタンドアロンの IM and Presence Service クラスタにあるノードが別のスタンドアロン クラスタ内のノードとのルータ間接続を確立することを防ぐために、クラスタ ID 値が一意であることです。スタンドアロン クラスタはクラスタ間ピア接続上でのみ通信します。

クラスタのクラスタ ID 値を表示または設定するには、**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）]** を選択します。クラスタ ID 値を変更する場合は、値が IM and Presence Service 展開に固有であることを確認します。

（注） チャット機能を導入する場合は、IM and Presence Service がチャット ノードのエイリアスを定義するクラスタ ID を使用します。クラスタ ID 値の変更が必要になる可能性がある特定の設定シナリオがあります。詳細については、グループ チャット モジュールを参照してください。

関連トピック

チャットの設定と管理 （267 ページ）

ルーティング通信の設定

クラスタ内のノードがメッセージを相互にルーティングできるようにするには、ルーティング通信タイプを設定する必要があります。この設定により、クラスタ内のノード間のルータ接続を確立するためのメカニズムが決定されます。IM and Presence データベース パブリッシャ ノードでルーティングの通信タイプを設定し、IM and Presence Service はクラスタのすべてのノードにこのルーティング設定を適用します。

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、MDNS がネットワーク内で有効になっていることを確認します。
- ルータ間通信を使用する必要があり、DNS がネットワークで使用できない場合は、ノードごとにクラスタ トポロジでノード名として IP アドレスを設定する必要あります。ノード名を編集するには、**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [プレゼンス トポロジ（Presence Topology）]** を選択し、ノードの [編集（edit）] リンクをクリックします。この設定は、

IM and Presence Service のインストール後、すべてのノードで Cisco XCP Router を再起動する前に実行します。

注目 Cisco Jabber クライアントを使用する時、証明書の警告メッセージは、IP アドレスが IM and Presence Service ノード名として設定されると発生する場合があります。Cisco Jabber で証明書の警告メッセージの生成を防止するには、ノード名として FQDN を使用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）] > [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 Service（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 リストから [Cisco XCP Router（Cisco XCP Router）] を選択します。

ステップ 4 メニューから次の [ルーティング通信タイプ（Routing Communication Types）] のいずれかを選択します。

- [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、マルチキャスト DNS 通信を選択します。マルチキャスト DNS 通信は、IM and Presence Service でデフォルトで有効になっています。
- [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 ドメイン内にない場合、ルータツールータ通信を選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 展開内のすべてのノードで Cisco XCP Router サービスを再起動します。

関連トピック

Cisco XCP Router サービスの再起動 （88 ページ）

クラスタ ID の設定

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 IM and Presence データベース パブリッシャ ノードに割り当てます。クラスタ内の複数のノードを設定する場合、システムはクラスタの各ノードが同じクラスタ ID 値を共有するようにクラスタ ID を配布します。

クラスタ ID 値をデフォルト設定のままにすることを推奨します。クラスタ ID 値を変更する場合は、次の点に注意してください。

- MDNS ルーティングを選択した場合は、すべてのノードにマルチキャスト ドメインにある他のノードを識別できるようにするために同じクラスタ ID が必要です。
- グループ チャット機能を展開する場合、IM and Presence Service は、チャット ノードのエイリアス マッピングにクラスタ ID 値を使用し、クラスタ ID 値の変更が必要になる可能

性がある特定の設定シナリオがあります。詳細については、グループ チャット モジュールを参照してください。

デフォルトのクラスタ ID 値を変更する場合は、IM and Presence データベース パブリッシャ ノードでのみこの変更を行う必要があります。システムはクラスタ内の他のノードに新しいクラスタ ID 値を複製します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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 ID 値を表示または編集します。

（注） デフォルトでは、IM and Presence Service はクラスタにクラスタ ID 値の「StandaloneCluster」 を割り当てます。

ステップ 3 [保存（Save）] をクリックします。

ヒント IM and Presence Service 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。

関連トピック

チャットの設定と管理 （267 ページ）

アベイラビリティ状態変更メッセージのスロットル レートの設定

IM and Presence Service の過負荷を防ぐために、メッセージで Cisco XCP Router に送信される可用性（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 Service 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。

手順

ステップ 1 **[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）]** を選択します。

ステップ 2 [サーバ（Server）] メニューから [IM and Presence Service（IM and Presence Service）] ノードを選択します。

ステップ 3 [サービス（Service）] メニューから **[Cisco Presence エンジン（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（Clusterwide Parameters）] 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）]** パラメータを編集します。このパラメータは、秒当たりのプレゼンス更新の数を定義します。

ステップ 5 [保存（Save）] をクリックします。

IPv6 設定（IPv6 Configuration）

IM and Presence Service に対して IPv6 を有効にするには、次のタスクを実行する必要があります。

- Cisco Unified IM and Presence OS Administration の GUI またはコマンドライン インターフェイスのどちらかを使用して、クラスタ内の各 IM and Presence Service ノードの Eth0 に IPv6 を設定します。
- 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します。

IM and Presence Service の企業ネットワークと Eth0 の両方に対して、各 IM and Presence Service ノードで IPv6 を使用するように設定する必要があります。そのようにしないと、システムは IP トラフィック向けに IPv4 を使おうとします。たとえば、エンタープライズ パラメータが IPv6 に設定され、クラスタ内の 2 つのノードのうちの 1 つだけで Eth0 ポートが IPv6 に設定されている場合、ポートを IPv6 に設定したノードのみが IPv6 に対して有効になります。他のノードは IPv4 を使おうとします。

IPv6 エンタープライズ パラメータへの設定変更を有効にするには、IM and Presence Service で次のサービスを再起動する必要があります。

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router

IM and Presence Service に IPv6 を設定する手順については、「*Cisco Unified Communications Manager* における *IM and Presence Service* の設定と管理」を参照してください。

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、『Cisco Unified Communications Manager アドミニストレーション ガイド』および『Cisco Unified Communications Solutions コマンドライン インターフェイス ガイド』を参照してください。

関連トピック

特記事項 （223 ページ）

IPv6 連携動作と制約事項

IM and Presence Service で IPv6 を設定する場合、および外部の IPv6 デバイスやネットワークとのインタラクションを行う場合は、次のインタラクションと制限事項に注意してください。

- 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 の企業ネットワークと Eth0 の両方に対して、各 IM and Presence Service ノードで IPv6 を使用するように設定する必要があります。そのようにしないと、システムは外部インターフェイス上で IP トラフィック向けに IPv4 を使おうとします。たとえば、エンタープライズ パラメータが IPv6 に設定され、クラスタ内の 2 つのノードのうちの 1 つだけで Eth0 ポートが IPv6 に設定されている場合、ポートを IPv6 に設定したノードのみが IPv6 に対して有効になります。他のノードは IPv4 を使おうとします。

（注） IM and Presence Service ノードで、エンタープライズ パラメータまたは ETH0 のいずれかに対して、何らかの理由で IPv6 が無効になった場合でも、IM and Presence Service で設定されているサーバのホスト名が解決可能な IPv6 アドレスならば、ノードは内部 DNS クエリを実行し、外部の LDAP やデータベース サーバに接続できます。

- 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。
- 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。IPv4 を使用するには、次の項目が展開に存在する場合、これらが IPv4 に設定されていることを確認する必要があります。
  - 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。

IM and Presence Service の Eth0 での IPv6 の有効化

IPv6 を使用するクラスタの各 IM and Presence Service 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 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 設定を完了するには、Eth0 を設定しノードをリブートした後に、クラスタの IPv6 エンタープライズ パラメータを有効にし、IPv6 Name パラメータも設定する必要があります。

手順

ステップ 1 **[Cisco Unified IM and Presence の OS の管理（Cisco Unified IM and Presence OS Administration）] > [設定（Settings）] > [IP（IP）] > [Ethernet IPv6（Ethernet IPv6）]** を選択します。[Ethernet IPv6 の設定（Ethernet IPv6 Configuration）] ウィンドウが表示されます。

ステップ 2 **[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにします。

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

- ルータ 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 必須: **[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

Cisco Unified CM IM and Presence の管理を使用して 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設定し、次に共通トポロジ（Common Topology）を使用して IPv6 名のパタメータを設定します。

IM and Presence Service の Eth0 での IPv6 の無効化

IPv6 を使用しないクラスタで各 IM and Presence Service ノードの Eth0 ポートの IPv6 を無効にするには、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 の管理（Cisco Unified CM IM and Presence OS Administration）] > [設定（Settings）] > [IP（IP）] > [Ethernet IPv6（Ethernet IPv6）]** を選択します。[Ethernet IPv6 の設定（Ethernet IPv6 Configuration）] ウィンドウが表示されます。

ステップ 2 **[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオフにします。

ステップ 3 必須: **[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 4 **[保存（Save）]** を選択します。

[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。

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。変更を適用するには、次のサービスを再起動する必要があります。

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router

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

サービスを再起動する前に、IPv6 が次のように設定されていることを確認します。

- [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] を使用して各 IM and Presence Service ノードの ETH0 の IPv6 を有効にします。
- 共通のトポロジを使用して IPv6 Name パラメータを設定します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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。[エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウが表示されます。

ステップ 2 **[IPv6]** パネルで **[True]** を選択します。

ステップ 3 **[保存（Save）]** を選択します。

次のタスク

変更を適用するには、IM and Presence Service ノードのサービスを再起動します。

プロキシ サーバの設定

手順

ステップ 1 **[Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] > [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。

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 のサービス

IM and Presence Service のサービスのオン

次の手順は、基本的な IM and Presence Service 設定を導入するときにオンにする必要のあるサービスを一覧表示します。IM and Presence Service クラスタの各ノードで次のサービスをオンにします。

IM and Presence Service で導入する追加機能によって他の任意サービスをオンにする必要があります。詳細については、固有の機能に関連する IM and Presence Service のマニュアルを参照してください。特定のシステム コンポーネントまたは機能を設定できるようにサービスを手動で停止した場合は、この手順を使用して、手動でこれらのサービスを再起動します。

Cisco XCP Router サービスを、基本的な IM and Presence Service 展開のために実行する必要があります。IM and Presence Service は、デフォルトで Cisco XCP Router をオンにします。**[Cisco Unified IM and Presence Serviceability（Cisco Unified IM and Presence Serviceability）] > [コントロールセンター - ネットワークサービス（Control Center - Network Services）]** を選択して、このネットワーク サービスがオンになっていることを確認します。

手順

ステップ 1 **[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。

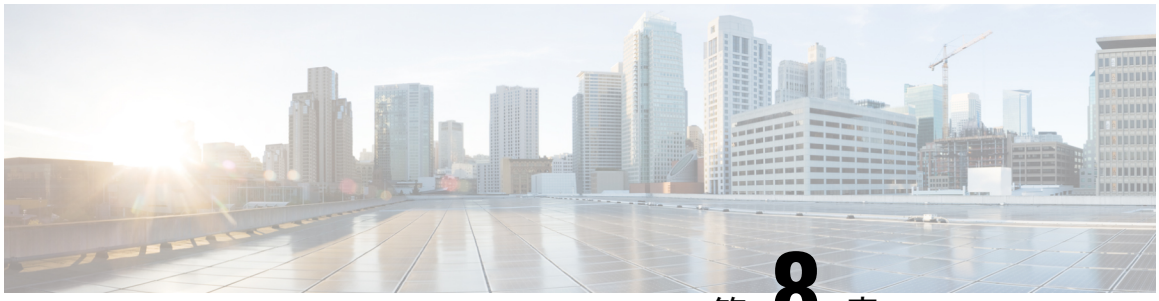
ステップ 2 [サーバ（Server）] メニューから [IM and Presence Service（IM and Presence Service）] ノードを選択します。

このメニューから [Cisco Unified Communications マネージャー（Cisco Unified Communications Manager）] ノードを選択して、Cisco Unified Communications Manager サービスのステータスを変更することもできます。

ステップ 3 基本的な IM and Presence Service 展開では、次のサービスをオンにします。

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

ステップ 4 [保存（Save）] をクリックします。



第 8 章

IP Phone Presence の設定

- IM and Presence Service のスタティック ルート設定 （117 ページ）
- IM and Presence Service のプレゼンス ゲートウェイの設定 （124 ページ）
- IM and Presence Service の SIP パブリッシュ トランクの設定 （126 ページ）
- SIP パブリッシュ トランクのクラスタ全体の DNS SRV 名の設定 （126 ページ）

IM and Presence Service のスタティック ルート設定

SIP プロキシ サーバ トラフィック用のスタティック ルートを設定する場合は、次の点を考慮してください。

- ダイナミック ルートは、ルーティング プロトコルとルーティング更新メッセージに従って自動的に計算されるネットワーク経由のパスを表します。
- スタティック ルートは、明示的に設定するネットワーク経由の固定パスを表します。
- スタティック ルートは、ダイナミック ルートよりも優先されます。

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。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 *11 :* 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 *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 *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 のルート組み込みテンプレートの設定

最大 5 つのルート組み込みテンプレートを定義できます。ただし、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。

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。

手順

ステップ 1 **[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）]** を選択します。

ステップ 2 IM and Presence Service ノードを選択します。

ステップ 3 Cisco SIP Proxy サービスを選択します。

ステップ 4 [ルーティング パラメータ（クラスタ全体）（Routing Parameters (Clusterwide)）] セクションの [ルート組み込みテンプレート（RouteEmbedTemplate）] フィールドでルート埋め込みテンプレートを定義します。最大 5 つのルート組み込みテンプレートを定義できます。

ステップ 5 [保存（Save）] を選択します。

次のタスク

IM and Presence Serviceのスタティック ルートの設定に進みます。

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

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 *13 : 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	

フィールド	説明
	着信番号のパターンを 255 文字以内で指定します。 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。 ワイルドカードの使用方法 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。 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。 電話機の場合： • 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、パターンの最後だけに使用できます。 IP アドレスおよびホスト名の場合： • 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。 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。

フィールド	説明
説明（Description）	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。
ネクスト ホップ（Next Hop）	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。 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。
ネクスト ホップ ポート（Next Hop Port）	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。 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。
ルート タイプ（Route Type）	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。 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。
プロトコル タイプ（Protocol Type）	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。

フィールド	説明
プライオリティ（Priority）	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。 値の範囲：1 ～ 65535
重み（Weight）	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。 値の範囲：1 ～ 65535 **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。 • 1、20 • 1、10 • 2、50 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。
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。 このパラメータを使用すると、管理者は効率的にルートをアウトオブサービスにすることができます（完全に削除してから再度追加する必要がありません）。

フィールド	説明
[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。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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 スタティック ルートを設定します。

ステップ 4 [保存（Save）] をクリックします。

IM and Presence Service のプレゼンス ゲートウェイの設定

プレゼンス ゲートウェイの設定オプション

Cisco Unified Communications Manager と IM and Presence Service との間でアベイラビリティ情報交換を処理する SIP 接続を有効にするには、IM and Presence Service で Cisco Unified Communications Manager をプレゼンス ゲートウェイとして設定する必要があります。

プレゼンス ゲートウェイを設定するときは、関連する Cisco Unified Communications Manager ノードの FQDN（完全修飾ドメイン名）または IP アドレスを指定します。この値は、使用中のネットワークに応じて次のいずれかになります。

- Cisco Unified Communications Manager データベース パブリッシャ ノードの FQDN アドレス
- Cisco Unified Communications Manager サブスクライバ ノードに解決される DNS SRV FQDN
- Cisco Unified Communications Manager データベース パブリッシャ ノードの IP アドレス

DNS SRV がネットワークのオプション場合は、次の設定を行います。

1. Cisco Unified Communications Manager サブスクライバ ノード（重み付けは均等）の DNS SRV FQDN で IM and Presence Service ノードのプレゼンス ゲートウェイを設定します。これにより、IM and Presence Service では、アベイラビリティ情報交換に使用するすべてのノード間でアベイラビリティ メッセージを均等に共有できます。

2. Cisco Unified Communications Manager で、IM and Presence Service ノードの SIP トランクを IM and Presence Service データベース パブリッシャ ノードとサブスクライバ ノードの DNS SRV FQDN で設定します。

DNS SRV がネットワークのオプションではなく、関連付けられた Cisco Unified Communications Manager ノードの IP アドレスを使用している場合、IP アドレスが単一のサブスクライバ ノードを指すため、複数のサブスクライバ ノードでプレゼンス メッセージング トラフィックを均等に共有できません。

関連トピック

Cisco Unified Communications Manager の SIP トランク設定 （58 ページ）

プレゼンス ゲートウェイの設定

始める前に

- プレゼンス ゲートウェイの設定オプションのトピックを参照してください。
- 設定要件に応じて、関連する Cisco Unified Communications Manager ノードの FQDN、DNS SRV FQDN、または IP アドレスを取得します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]** > **[プレゼンス（Presence）]** > **[ゲートウェイ（Gateways）]** 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 ゲートウェイ タイプ（Presence Gateway Type）] で **[CUCM（CUCM）]** を選択します。

ステップ 4 [説明（Description）] フィールドにプレゼンス ゲートウェイの説明を入力します。

ステップ 5 [プレゼンス ゲートウェイ（Presence Gateway）] フィールドに、関連付ける Cisco Unified Communications Manager ノードの FQDN、DNS SRV FQDN、または IP アドレスを指定します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

IM and Presence Service の許可ポリシーを設定します。

関連トピック

IM and Presence Service の許可ポリシーの設定 （297 ページ）
プレゼンス ゲートウェイの設定オプション （124 ページ）

IM and Presence Service の SIP パブリッシュ トランクの設定

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。

この手順は、Cisco Unified Communications Manager のサービス パラメータで SIP トランクを CUP PUBLISH トランクとして割り当てる操作と同じです。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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 SIP パブリッシュ トランク（CUCM SIP Publish Trunk）]** ドロップダウン リストから [SIP トランク（SIP Trunk）] を選択します。

ステップ 3 [保存（Save）] をクリックします。

SIP パブリッシュ トランクのクラスタ全体の DNS SRV 名の設定

IM and Presence データベース パブリッシャ ノードのクラスタ全体の IM and Presence Service アドレスを設定すると、IM and Presence Service はクラスタのすべてのノードのアドレスを複製します。

クラスタ全体の IM and Presence Service のアドレスを設定すると、SRV ポート値を 5060 に設定します。

（注） IM and Presence Service のデフォルト ドメインがクラスタ全体の DNS SRV レコードで使用される場合、この手順で SRV クラスタ名の値を変更しないでください。これ以上の操作は必要ありません。

始める前に

クラスタ全体の DNS SRV トピック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）]** > **[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）]** メニューから [IM and Presence Service （IM and Presence Service）] ノードを選択します。

ステップ 3 [サービス（Service）] メニューから [Cisco SIP Proxy（Cisco SIP Proxy）] を選択します。

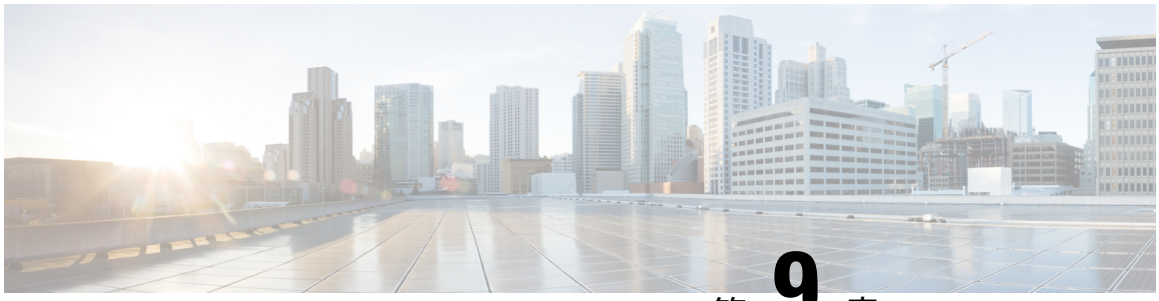
ステップ 4 [一般的なプロキシ パラメータ（クラスタ全体）（General Proxy Parameters（Clusterwide））] セクションの **[SRV クラスタ名（SRV Cluster Name）]** フィールドを編集します。

このパラメータはデフォルトでは空です。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

クラスタ全体の DNS SRV （30 ページ）
展開の拡張性オプション （28 ページ）



第 9 章

LDAP ディレクトリ統合

- LDAP サーバ名、アドレス、およびプロファイル設定 （129 ページ）
- Cisco Unified Communications Manager との LDAP ディレクトリの統合のタスク リスト （129 ページ）
- 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 （135 ページ）

LDAP サーバ名、アドレス、およびプロファイル設定

IM and Presence Service の *LDAP* サーバ名、アドレス、およびプロファイル設定は、*Cisco Unified Communications Manager* に移動されました。詳細については、『*Cisco Unified Communications Manager* リリース *9.0(1)* ガイド』を参照してください。

Cisco Unified Communications Manager との LDAP ディレクトリの統合のタスク リスト

次のワークフロー図に、Cisco Unified Communications Manager と LDAP ディレクトリを統合するためのおおまかな手順を示します。

図 *11 : Cisco Unified Communications Manager* との *LDAP* ディレクトリの統合のワークフロー

次の表に、タスクを Cisco Unified Communications Manager との LDAP ディレクトリの統合を実行するためのタスクを示します。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 *14 : LDAP* ディレクトリを統合するためのタスク リスト

タスク	説明
セキュアな Cisco Unified Communications Manager と LDAP ディレクトリとの接続	Cisco Unified Communications Manager の LDAP サーバで Secure Socket Layer（SSL）接続をイネーブルにします。 **ヒント** Cisco Unified Communications Manager リリース 8.x 以降では、LDAP の SSL 証明書を tomcat-trust 証明書としてアップロードする必要があります。
ユーザプロビジョニングのための LDAP 同期の設定	Cisco Unified Communications Manager で Cisco Directory Synchronization（DirSync）ツールを有効にし、社内ディレクトリからユーザを自動的にプロビジョニングするか、ユーザ ディレクトリ情報を手動で同期することができます。 **ヒント** LDAP 同期は Cisco Unified Communications Manager のアプリケーション ユーザに適用されません。Cisco Unified CM Administration の GUI を使用して、アプリケーション ユーザを手動でプロビジョニングします。
LDAP サーバ証明書のアップロード	Cisco Unified Communications Manager LDAP 認証がセキュア モード（ポート 363 または 3269）に対して設定されている場合、すべての LDAP 認証サーバ証明書と中間証明書を 「tomcat-trust」 として IM and Presence Service ノードにアップロードする必要があります。
LDAP サーバ認証の設定	Cisco Unified Communications Manager を有効にして、ユーザ パスワードを社内 LDAP ディレクトに対して認証します。 **ヒント** LDAP 認証は、アプリケーション ユーザのパスワードには適用されません。
IM and Presence Service と LDAP ディレクトリ間のセキュア接続の設定	Cisco Unified Communications Manager と LDAP ディレクトリ間にセキュアな接続を設定した場合は、クラスタのすべての IM and Presence Service ノード上でこのタスクを実行します。

Cisco Unified Communications Manager と LDAP ディレクトリとの間のセキュア接続

Cisco Unified Communications Manager ノードと LDAP ディレクトリ サーバとの間の接続をセキュリティで保護するには、Cisco Unified Communications Manager で LDAP サーバの Secure Socket Layer（SSL）接続を有効にし、SSL 証明書を Cisco Unified Communications Manager に

アップロードします。Cisco Unified Communications Manager リリース 8.x 以降では、LDAP の SSL 証明書を tomcat-trust 証明書としてアップロードする必要があります。

LDAP の SSL 証明書をアップロードしたら、Cisco Unified Communications Manager で次のサービスを再起動する必要があります。

- ディレクトリ サービス
- Tomcat サービス

Cisco Unified Communications Manager への証明書のアップロードの詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。

ユーザ プロビジョニングのための LDAP 同期の設定

LDAP 同期は Cisco Unified Communications Manager で Cisco Directory Synchronization（DirSync）ツールを使用して、社内 LDAP ディレクトリから情報を（手動または定期的に）同期します。DirSync サービスを有効にすると、Cisco Unified Communications Manager が自動的に社内ディレクトリからのユーザをプロビジョニングします。Cisco Unified Communications Manager は引き続きローカル データベースを使用しますが、そのファシリティを無効にしてユーザ アカウントの作成を可能にします。LDAP ディレクトリ インターフェイスを使用して、ユーザ アカウントを作成および管理します。

始める前に

- Cisco Unified Communications Manager で LDAP 固有の設定を試行する前に、LDAP サーバがインストールされていることを確認してください。
- Cisco Unified Communications Manager で Cisco DirSync サービスをアクティブにします。

制約事項

LDAP 同期は Cisco Unified Communications Manager のアプリケーション ユーザに適用されません。Cisco Unified CM の管理インターフェイスでアプリケーション ユーザを手動でプロビジョニング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）] > [システム（System）] > [LDAP（LDAP）] > [LDAP システム（LDAP System）]** 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 サーバのタイプおよび属性を設定します。

ステップ 4 **[LDAP サーバからの同期を有効にする（Enable Synchronizing from LDAP Server）]** を選択します。

ステップ 5 **[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [LDAP（LDAP）] > [LDAP ディレクトリ（LDAP Directory）]** を選択します。

ステップ 6 次の項目を設定します。

a) LDAP ディレクトリ アカウント設定
b) 同期対象のユーザ属性
c) 同期スケジュール
d) LDAP サーバ ホスト名または IP アドレスおよびポート番号

ステップ 7 Secure Socket Layer（SSL）を使用して LDAP ディレクトリと通信するには、**[SSL を使用（Use SSL）]** をオンにします。

ヒント
- LDAP over SSL を設定するには、LDAP ディレクトリ証明書を Cisco Unified Communications Manager にアップロードします。
- 特定の LDAP 製品のアカウント同期メカニズムおよび LDAP 同期の一般的なベスト プラクティスの詳細については、Cisco Unified Communications Manager SRND の LDAP ディレクトリの情報を参照してください。

次のタスク

LDAP 認証サーバ証明書のアップロードに進みます。

関連トピック

http://www.cisco.com/go/designzone

LDAP 認証サーバ証明書のアップロード

Cisco Unified Communications Manager LDAP 認証をセキュア モード（ポート 636 または 3269）に設定する場合は、認証局（CA）のルート証明書や他のすべての中間証明書などの LDAP 認証サーバ証明書を、「tomcat-trust」 として個別に IM and Presence Service ノードにアップロード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）]** > **[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 **[証明書のアップロード（Upload Certificate）]** をクリックします。
ステップ 3 **[証明書名（Certificate Name）]** メニューから **[tomcat-trust]** を選択します。
ステップ 4 ローカル コンピュータから LDAP サーバ ルート証明書を参照し、選択します。
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。
ステップ 6 他のすべての中間証明書に対して上記の手順を繰り返します。

次のタスク

LDAP 認証の設定に進みます。

LDAP 認証の設定

LDAP 認証機能を使用すると、社内 LDAP ディレクトリに対して Cisco Unified Communications Manager でユーザ パスワードを認証できます。

始める前に

Cisco Unified Communications Manager で LDAP 同期を有効にします。

制約事項

LDAP 認証は、アプリケーション ユーザのパスワードには適用されません。Cisco Unified Communications Manager は、内部データベースのアプリケーション ユーザを認証します。

手順

ステップ 1 **[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [LDAP（LDAP）] > [LDAP 認証（LDAP Authentication）]** を選択します。

ステップ 2 ユーザに対する LDAP 認証を有効にします。

ステップ 3 LDAP 認証設定を指定します。

ステップ 4 LDAP サーバ ホスト名または IP アドレスおよびポート番号を設定します。

（注） Secure Socket Layer（SSL）を使用して LDAP ディレクトリと通信するには、[SSL を使用（Use SSL）] をオンにします。

[SSL を使用（Use SSL）] チェックボックスをオンにした場合、IP アドレスまたはホスト名または LDAP サーバの証明書のサブジェクト CN と一致する FQDN を入力します。LDAP サーバの証明書のサブジェクト CN は、IP アドレス、ホスト名、または FQDN である必要があります。この条件を満たさない場合は、Cisco Unified CM IM and Presence の管理、Cisco Unified IM and Presence Serviceability、Cisco Unified IM and Presence リポーティング、Cisco Jabber ログイン、サードパーティ製 XMPP クライアントおよび Cisco Unified Communications Manager の他のアプリケーション、さらにユーザ認証を実行するLDAPに接続している IM and Presence Service のログインの失敗を招くので、[SSL を使用（Use SSL）] のチェックボックスをオンにしないでください。

ヒント LDAP over SSL を設定するには、LDAP ディレクトリ証明書を Cisco Unified Communications Manager にアップロードします。

次のタスク

IM and Presence Service と LDAP ディレクトリ間のセキュア接続を設定します。

IM and Presence Service と LDAP ディレクトリ間のセキュア接続の設定

このトピックは、Cisco Unified Communications Manager と LDAP ディレクトリとの間のセキュア接続を設定する場合にのみ適用されます。

（注） クラスタ内のすべての IM and Presence Service ノードでこの手順を実行します。

始める前に

Cisco Unified Communications Manager で LDAP の SSL を有効にし、LDAP ディレクトリ証明書を Cisco Unified Communications Manager にアップロードします。

手順

ステップ 1 **[Cisco Unified IM and Presence OS の管理（Cisco Unified IM and Presence OS Administration）] > [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 **[証明書のアップロード（Upload Certificate）]** をクリックします。

ステップ 3 [証明書の名前（Certificate Name）] メニューから [tomcat-trust] を選択します。

ステップ 4 ローカル コンピュータから LDAP サーバ証明書を参照し、選択します。

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。

ステップ 6 コマンド `utils service restart Cisco Tomcat` を使用して、CLI から Tomcat サービスを再起動します。

次のタスク

Cisco Jabber と LDAP ディレクトリを統合します。

システム トラブルシュータを使用した LDAP ディレクトリ接続の検証

システムのステータスを表示して、LDAP サーバへの接続が正常に機能していることを確認するには、**Cisco Unified CM IM and Presence Administration** の UI のシステム トラブルシュータを使用します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]** > **[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 LDAP サーバへの接続のステータスを [LDAP トラブルシュータ（LDAP 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。

- LDAP サーバに接続できることを確認します。
- LDAP サーバが接続をリッスンしていることを確認します。
- LDAP サーバの認証に成功したことを確認します。

接続に関する問題が検出された場合は、推奨ソリューションを実行します。

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

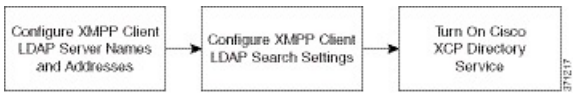
次のトピックでは、サードパーティ製 XMPP クライアントのユーザが LDAP ディレクトリから連絡先を検索および追加できるように IM and Presence Service で LDAP 設定を行う方法について説明します。

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 *12 : 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 *15 : 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 xmpp-trust-certificate 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って入力し、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。

関連トピック

Cisco Unified Communications Manager と LDAP ディレクトリとの間のセキュア接続 （130 ページ）

IM and Presence Service と LDAP ディレクトリ間のセキュア接続の設定 （134 ページ）

XMPP クライアントの LDAP 検索設定

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しすると、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 Service 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 Service 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 *16 : 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。 • 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。

フィールド	設定
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（ユーザ属性）	LDAP サーバ タイプに適切なユーザ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。
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 Service 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 Service 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 - 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 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 Service（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 10 章

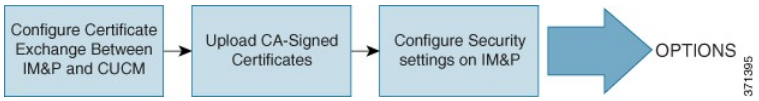
IM and Presence Service のセキュリティ設定

- セキュリティ設定のタスク リスト （143 ページ）
- ログイン バナーの作成 （145 ページ）
- IM and Presence Service の拡張 TLS 暗号化 （146 ページ）
- マルチサーバ証明書の概要 （148 ページ）
- IM and Presence Service の証明書タイプ （148 ページ）
- IM and Presence Service と Cisco Unified Communications Manager 間の証明書交換の設定 （151 ページ）
- IM and Presence Service へのマルチサーバ CA 署名付き証明書のアップロード （154 ページ）
- IM and Presence Service への単一サーバ CA 署名付き証明書のアップロード （155 ページ）
- 自己署名の信頼証明書の削除 （168 ページ）
- IM and Presence Service での SIP セキュリティの設定 （170 ページ）
- IM and Presence Service での XMPP セキュリティの設定 （173 ページ）

セキュリティ設定のタスク リスト

次のワークフローの図は、IM and Presence Service ノードの展開のセキュリティを設定するための手順の概要を示します。

図 *13* : セキュリティ設定のワークフロー



次の表は、IM and Presence Service ノードの展開のセキュリティ設定をするためのタスクを示します。手順の詳細については、ワークフローで説明されているタスクに関連する手順を参照してください。

（注） オプションで、IM and Presence Service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。

表 *17 : IM and Presence Service* のセキュリティ設定のタスク リスト

タスク	説明
IM and Presence Service と Cisco Unified Communications Manager 間の証明書交換の設定	次の作業を実行します。 • IM and Presence Service ノードへの Cisco Unified Communications Manager 証明書のインポート後、SIP プロキシ サービスを再起動します。 ヒント **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** から [証明書インポート ツール（Certificate Import Tool）] または手動で [Cisco Unified IM and Presence OS の管理（Cisco Unified IM and Presence OS Administration）] を使用して証明書をインポートできます。 • IM and Presence Serviceから証明書をダウンロード後、Cisco Unified Communications Manager で証明書を Callmanager-trust にアップロードします。 • Cisco Unified Communications Manager サービスを再起動します。 （注） Cisco Unified Communications Manager と IM and Presence Service 間の証明書交換を設定する前に、IM and Presence Service の SIP セキュリティ プロファイルと SIP トランクを設定する必要があります。 （注） IM and Presence Service 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 Service から解決可能である必要があります。IM and Presence Service 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。

タスク	説明
CA-Signed 証明書のアップロード	単一サーバまたは複数サーバの展開のために、IM and Presence Service に認証局（CA）署名付き証明書をアップロードします。サービスの再起動が必要です。詳細については、関連タスクを参照してください。 • tomcat または tomcat-ECDSA 証明書 • cup-xmpp または cup-xmpp-ECDSA 証明書 • cup-xmpp-s2s または cup-xmpp-s2s-ECDSA 証明書 ヒント　クラスタのすべてのIM and Presence Service ノードで証明書をアップロードできます。証明書のアップロードが完了すると、証明書と関連の署名証明書はクラスタ内の他のすべての IM and Presence Service ノードに自動的に配布されます。
IM and Presence Service でのセキュリティの設定	IM and Presence Service 証明書をインポートすると、IM and Presence Service 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。 IM and Presence Service は XMPP ベースの設定でセキュリティが強化されています。**[システム（System）] > [セキュリティ（Security）] > [設定（Settings）]** から [Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] を使用して IM and Presence Service の XMPP セキュア モードを設定できます。

ログイン バナーの作成

ユーザが IM and Presence Service 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 Service 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 Service ノードに個別にアップロードする必要があります。

IM and Presence Service の拡張 TLS 暗号化

このリリースでは、TLS バージョン 1.2 接続で Tomcat、SIP プロキシ、および XMPP インターフェイスに関して楕円曲線デジタル署名アルゴリズム（ECDSA）がサポートされます。

証明書を作成する際は、RSA ベースの証明書と ECDSA ベースの証明書の両方を設定することを推奨します。たとえば、Tomcat 証明書を設定する場合、Tomcat-ECDSA 証明書も設定する必要があります（その逆も同様）。

（注） IM and Presence Service ピアが TLS バージョン 1.2 をサポートしない場合は、接続が TLS バージョン 1.0 にフォールバックされ、既存の動作が保持されます。

（注） RSA 証明書については、**キー長**の値が 3072 または 4096 の証明書のみを選択できます。これらのオプションは、ECDSA 証明書については使用できません。

（注） Tomcat インターフェイスの EC 暗号はデフォルトで無効になっています。Cisco Unified Communications Manager または IM and Presence Service で [HTTPS 暗号（HTTPS Ciphers）] のエンタープライズパラメータを使用して、これらを有効にできます。このパラメータを変更すると、すべてのノードで Cisco Tomcat サービスを再起動する必要があります。

このサポートの一部として、Tomcat、SIP プロキシおよび XMPP インターフェイスをサポートする TLS 接続で使用するために 4 つの新しい暗号方式が導入されました。これらの新しい暗号方式のうちの 2 つは RSA ベースで、残りの 2 つは ECDSA ベースです。

ECDSA ベース暗号方式のサポートの詳細については、Cisco Unified Communications Manager および IM and Presence Service Release 11.0(1) のリリース ノートの「ECDSA Support for Common Criteria for Certified Solutions」を参照してください。

導入された新しい暗号方式は次のとおりです。

- ECDHE ECDSA 暗号方式
  - **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**
  - **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**
- ECDHE RSA 暗号方式
  - **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**
  - **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**

RSA ベースの暗号方式については、既存のセキュリティ証明書が使用されます。ただし、ECDSA ベースの暗号方式には次の追加のセキュリティ証明書が必要です。

- `cup-ECDSA`
- `cup-xmpp-ECDSA`
- `cup-xmpp-s2s-ECDSA`
- `tomcat-ECDSA`

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。EC 証明書の共通名（CN）はホスト名に `-EC` が追加されます。また、EC 証明書の SAN フィールドにはサーバの FQDN またはホスト名が含まれます。

（注） RSA ベースの証明書（Tomcat、XMPP、XMPP-s2s、および CUP）の共通名（CN）フィールドには EC を使用しないことを推奨します。使用すると、既存の EC ベースの証明書が上書きされます。

IM and Presence Service でのセキュリティ証明書の設定の詳細については、「IM and Presence Service の証明書タイプ」、「IM and Presence Service へのマルチサーバ CA 署名付き証明書のアップロード」、および「IM and Presence Service への単一サーバ CA 署名付き証明書のアップロード」を参照してください。

TLS 暗号の設定については、「TLS 暗号のマッピングの設定」を参照してください。

RSA セキュリティ証明書による、拡張されたキー長のサポート

このリリース以降では、RSA 証明書/キー タイプの自己署名証明書および CSR 証明書に関して、3072 ビットおよび 4096 ビットの新しい**キー長**サイズが導入されています。

マルチサーバ証明書の概要

IM and Presence Service は、tomcat/tomcat-ECDSA、cup-xmpp/cup-xmpp-ECDSA、および cup-xmpp-s2s/cup-xmpp-s2s-ECDSA の証明について、マルチサーバ SAN ベースの証明書をサポートしています。単一サーバ、またはマルチサーバの配布から選択し、証明書署名要求（CSR）を生成し、マルチサーバ証明書のサポートを承認することができます。最終的な署名付きのマルチサーバ証明書と、署名を行う証明書の関連チェーンが、クラスタ内の個々のサーバのいずれかにマルチサーバ証明書をアップロードするときにクラスタ内の他のサーバに分配されます。マルチサーバ証明書の詳細については、『*Release Notes for Cisco Unified Communications Manager Release 10.5(1)*』の新機能と変更された機能に関する章を参照してください。

IM and Presence Service の証明書タイプ

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 *18 :* 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。
cup cup-ECDSA	Cisco SIP Proxy Cisco Presence Engine	cup-trust	なし	

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-xmpp cup-xmpp-ECDSA	Cisco XCP Connection Manager Cisco XCP Web Connection Manager Cisco XCP Directory サービス 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。

関連トピック

IM and Presence Service での XMPP セキュリティの設定 （173 ページ）
IM and Presence Service と LDAP ディレクトリ間のセキュア接続の設定 （134 ページ）

IM and Presence Service と Cisco Unified Communications Manager 間の証明書交換の設定

このモジュールでは、Cisco Unified Communications Manager ノードと IM and Presence Service ノード間における自己署名証明書の交換について説明します。IM and Presence Service で証明書インポート ツールを使用して、Cisco Unified Communications Manager 証明書を IM and Presence Service に自動的にインポートできます。ただし、手動で Cisco Unified Communications Manager に IM and Presence Service 証明書をアップロードする必要があります。

IM and Presence Service および Cisco Unified Communications Manager 間にセキュア接続が必要な場合にのみ、次の手順を実行します。

セキュリティを設定するための前提条件

Cisco Unified Communications Manager で次の項目を設定します。

- IM and Presence Service の SIP セキュリティ プロファイルを設定します。
- 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。

関連トピック

Cisco Unified Communications Manager の SIP トランク設定 （58 ページ）

IM and Presence Service への Cisco Unified Communications Manager 証明書のインポート

手順

ステップ 1 **[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。

ステップ 2 **[Certificate Trust Store（証明書信頼ストア）]** メニューから **[IM and Presence（IM/P）Service Trust（IM and Presence（IM/P）サービス信頼）]** 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が報告されます。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。

次のタスク

SIP プロキシ サービスの再起動に進みます。

SIP Proxy サービスの再起動

始める前に

IM and Presence Service に Cisco Unified Communications Manager 証明書をインポートします。

手順

ステップ 1 IM and Presence Service で **[Cisco Unified IM and Presence Serviceability（Cisco Unified IM and Presence Serviceability）]** > **[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 [Cisco SIP Proxy（Cisco SIP Proxy）] を選択します。

ステップ 3 [再起動（Restart）] をクリックします。

次のタスク

IM and Presence Service から証明書をダウンロードする手順に進みます。

IM and Presence Service からの証明書のダウンロード

手順

ステップ 1 IM and Presence Service で、**[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 Service 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

Cisco Unified Communications Manager に IM and Presence Service 証明書をアップロードします。

Cisco Unified Communications Manager への IM and Presence Service 証明書のアップロード

始める前に

IM and Presence Service から証明書をダウンロードします。

手順

ステップ 1 Cisco Unified Communications Manager で **[Cisco Unified OS の管理（Cisco Unified OS Administration）] > [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 **[証明書のアップロード（Upload Certificate）]** をクリックします。

ステップ 3 [証明書名（Certificate Name）] メニューから **[Callmanager-trust]** を選択します。

ステップ 4 IM and Presence Service から以前にダウンロードした証明書（.pem ファイル）を参照し、選択します。

（注） ECDSA 証明書を使用する場合は、`-ECDSA.pem` で終わる証明書を選択します。

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。

次のタスク

Cisco Unified Communications Manager CallManager サービスの再起動に進みます。

Cisco Unified Communications Manager サービスの再起動

始める前に

Cisco Unified Communications Manager に IM and Presence Service 証明書をアップロードします。

手順

ステップ 1 Cisco Unified Communications Manager で、**[Cisco Unified Serviceability（Cisco Unified Serviceability）] > [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 [Cisco CallManager（Cisco CallManager）] を選択します。

ステップ 3 [再起動（Restart）] をクリックします。

次のタスク

IM and Presence Service の SIP セキュリティ設定に進みます。

関連トピック

IM and Presence Service での SIP セキュリティの設定 （170 ページ）

IM and Presence Service へのマルチサーバ CA 署名付き証明書のアップロード

ここでは、マルチサーバ CA 署名付き証明書の次の種類のアップロードについて詳しく説明します。

- tomcat および tomcat-ECDSA 証明書
- cup-xmpp および cup-xmpp-ECDSA 証明書
- cup-xmpp-s2s および cup-xmpp-s2s-ECDSA 証明書

クラスタ内の任意の IM and Presence Service ノードでこのような証明書をアップロードできます。これを行うと、証明書と関連の署名を行う証明書はクラスタ内のその他すべての M and Presence Service ノードに自動的に配布されます。特定の認証（たとえば、tomcat、cup-xmpp、

またはcup-xmpp-s2s）を行うために自己署名証明書がノードに既に存在する場合、その証明書は新しいマルチサーバ証明書によって上書きされます。

特定のマルチサーバ証明書と関連の署名を行う証明書が配布されるIM and Presence Serviceノードは、証明書の目的によって異なります。cup-xmpp/cup-xmpp-ECDSA および cup-xmpp-s2s/cup-xmpp-s2s-ECDSA マルチサーバ証明書は、クラスタ内のすべてのIM and Presence Service ノードに配布されます。tomcat マルチサーバ証明書は、クラスタ内のすべての IM and Presence Service ノードと、クラスタ内のすべての Cisco Unified Communications Manager ノードに配布されます。マルチサーバSAN証明書の詳細については、『*Release Notes for Cisco Unified Communications Manager Release 10.5(1)*』の新機能と変更された機能に関する章を参照してください。

IM and Presence Service への単一サーバ CA 署名付き証明書のアップロード

ここでは、IM and Presence Service に次のタイプの CA 署名付き証明書をアップロードする方法について説明します。

- tomcat および tomcat-ECDSA 証明書
- cup-xmpp および cup-xmpp-ECDSA 証明書
- cup-xmpp-s2s および cup-xmpp-s2s-ECDSA 証明書

CA 署名付きの Tomcat 証明書のタスク リスト

CA 署名付き Tomcat または Tomcat-ECDSA 証明書を IM and Presence Service にアップロードするためのおおまかな手順は次のとおりです。

1. 署名を行う認証局のルート証明書および中間証明書をIM and Presence Serviceにアップロードします。
2. Cisco Intercluster Sync Agent サービスを再起動します。
3. CA 証明書が他のクラスタに正しく同期されていることを確認します。
4. 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します。
5. すべてのノードで Cisco Tomcat サービスを再起動します。
6. 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。

（注） EC ベースの CA によって署名された Tomcat CSR または RSA ベースの CA によって署名された Tomcat-ECDSA CSR を取得すると、Tomcat インターフェイスを介した TLS 接続が失敗します。Tomcat-ECDSA 証明書の署名については EC ベースの CA、Tomcat 証明書の署名については RSA ベースの CA を使用することを推奨します。

署名を行う認証局のルート証明書および中間証明書のアップロード

ルート証明書および中間証明書をアップロードする場合は、証明書チェーンの各証明書をルート証明書から中間証明書の順に IM and Presence Service へアップロードする必要があります。

root > intermediate-1 > intermediate-2 > … > intermediate-N

チェーンでアップロードする各証明書ごとに、以前にアップロードしたどの証明書が署名したかを指定する必要があります。次に例を示します。

- intermediate-1 の場合は、署名にルート証明書が使用されました。
- intermediate-2 の場合は、署名に intermediate-1 が使用されました。

IM and Presence データベース パブリッシャ ノードで関連のリーフ証明書の信頼ストアにルート証明書および中間証明書（存在する場合）をアップロードする必要があります。署名を行う認証局（CA）のルート証明書および中間証明書を展開された IM and Presence Service にアップロードするには、次の手順を実行します。

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 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 [証明書名（Certificate Name）] ドロップダウン リストで、**[tomcat-trust]** を選択します。

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 **[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 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 [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。

次のタスク

Cisco Intercluster Sync Agent サービスを再起動します。

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 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 Intercluster Sync Agent**

（注） また、Cisco Unified Serviceability GUI からCisco Intercluster Sync Agent サービスを再起動できます。

次のタスク

CA 証明書が他のクラスタに同期したことを確認します。

他のクラスタに CA 証明書が同期されていることの確認

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 の管理（Cisco Unified CM IM and Presence Administration）] > [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。

各 IM and Presence Service ノードへの署名付き証明書のアップロード

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。

（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。

手順

ステップ 1 **[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 [証明書名（Certificate Name）] ドロップダウン リストで、**[tomcat]** を選択します。

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。

証明書の管理の詳細については、『Cisco Unified Communications オペレーティング システム アドミニストレーション ガイド』を参照してください。

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 Service 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。

クラスタ間同期の確認

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 の管理（Cisco Unified CM IM and Presence Administration）] > [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（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す。

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。

CA 署名付き cup-xmpp 証明書のアップロード

CA 署名付き cup-xmpp 証明書または cup-xmpp-ECDSA 証明書を IM and Presence Service にアップロードするためのおおまかな手順は次のとおりです。

1. 署名を行う認証局のルート証明書および中間証明書を IM and Presence Service にアップロードします。
2. Cisco Intercluster Sync Agent サービスを再起動します。
3. CA 証明書が他のクラスタに正しく同期されていることを確認します。
4. 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します。
5. すべてのノードで Cisco XCP Router サービスを再起動します。

署名を行う認証局のルート証明書および中間証明書のアップロード

ルート証明書および中間証明書をアップロードする場合は、証明書チェーンの各証明書をルート証明書から中間証明書の順に IM and Presence Service へアップロードする必要があります。

root > intermediate-1 > intermediate-2 > … > intermediate-N

チェーンでアップロードする各証明書ごとに、以前にアップロードしたどの証明書が署名したかを指定する必要があります。次に例を示します。

- intermediate-1 の場合は、署名にルート証明書が使用されました。
- intermediate-2 の場合は、署名に intermediate-1 が使用されました。

IM and Presence データベース パブリッシャ ノードで **cup-xmpp-trust** ストアにルート証明書および中間証明書（存在する場合）をアップロードする必要があります。署名を行う認証局（CA）のルート証明書および中間証明書を展開された IM and Presence Service にアップロードするには、次の手順を実行します。

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 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 [証明書名（Certificate Name）] ドロップダウン リストから **[cup-xmpp-trust]** を選択します。

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 **[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 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 [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。

次のタスク

Cisco Intercluster Sync Agent サービスを再起動します。

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 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 Intercluster Sync Agent`**

（注） また、Cisco Unified Serviceability GUI からCisco Intercluster Sync Agent サービスを再起動できます。

次のタスク

CA 証明書が他のクラスタに同期したことを確認します。

他のクラスタに CA 証明書が同期されていることの確認

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 の管理（Cisco Unified CM IM and Presence Administration）] > [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。

各 IM and Presence Service ノードへの署名付き証明書のアップロード

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 cup-xmpp 証明書をアップロードできます。

（注） クラスタに必要なすべての cup-xmpp 証明書に署名し、それらの証明書を同時にアップロードして、サービスへの影響が単一のメンテナンス時間帯内で管理できるようにすることを推奨します。

（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 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 [証明書名（Certificate Name）] ドロップダウン リストから **[cup-xmpp]** を選択します。

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。

証明書の管理の詳細については、『Cisco Unified Communications オペレーティング システム アドミニストレーション ガイド』を参照してください。

次のタスク

すべてのノードで Cisco XCP Router サービスを再起動します。

すべてのノードの Cisco XCP Router サービスの再起動

注意 Cisco XCP Router の再起動はサービスに影響を与えます。

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。

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。

（注） また、Cisco Unified IM and Presence Serviceability GUI から Cisco XCP Router サービス を再起動できます。

CA 署名付き cup-xmpp-s2s 証明書のアップロード

CA 署名付き cup-xmpp-s2s 証明書または cup-xmpp-s2s-ECDSA 証明書を IM and Presence Service にアップロードするためのおおまかな手順は次のとおりです。

1. 署名を行う認証局のルート証明書および中間証明書を IM and Presence Service にアップロードします。
2. CA 証明書が他のクラスタに正しく同期されていることを確認します。
3. 適切な署名付き証明書を IM and Presence Service フェデレーション ノードにアップロードします（この証明書はフェデレーションに使用する IM and Presence Service ノードにのみ必要であり、すべてのノードに必要なわけではありません）。
4. 影響を受けるすべてのノードで Cisco XCP XMPP Federation Connection Manager サービスを再起動します。

署名を行う認証局のルート証明書および中間証明書のアップロード

ルート証明書および中間証明書をアップロードする場合は、証明書チェーンの各証明書をルート証明書から中間証明書の順に IM and Presence Service へアップロードする必要があります。

root > intermediate-1 > intermediate-2 > … > intermediate-N

チェーンでアップロードする各証明書ごとに、以前にアップロードしたどの証明書が署名したかを指定する必要があります。次に例を示します。

- intermediate-1 の場合は、署名にルート証明書が使用されました。
- intermediate-2 の場合は、署名に intermediate-1 が使用されました。

IM and Presence データベース パブリッシャ ノードで **cup-xmpp-trust** ストアにルート証明書および中間証明書（存在する場合）をアップロードする必要があります。署名を行う認証局（CA）のルート証明書および中間証明書を展開された IM and Presence Service にアップロードするには、次の手順を実行します。

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 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 [証明書名（Certificate Name）] ドロップダウン リストから **[cup-xmpp-trust]** を選択します。

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 **[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 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 [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。

次のタスク

CA 証明書が他のクラスタと同期されたことを確認します。

他のクラスタに CA 証明書が同期されていることの確認

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 の管理（Cisco Unified CM IM and Presence Administration）] > [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。

フェデレーション ノードへの署名付き証明書のアップロード

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 フェデレーション 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。すべてのノードに証明書をアップロードする必要はありません。フェデレーション用のノードにだけアップロードします。

（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。

（注） クラスタに必要なすべての cup-xmpp-s2s 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。

手順

ステップ 1 **[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 [証明書名（Certificate Name）] ドロップダウン リストから **[cup-xmpp]** を選択します。

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 フェデレーション ノードで繰り返します。

証明書の管理の詳細については、『Cisco Unified Communications オペレーティング システム アドミニストレーション ガイド』を参照してください。

次のタスク

影響を受けるノードで Cisco XCP XMPP Federation Connection Manager サービスを再起動します。

Cisco XCP XMPP Federation Connection Manager サービスの再起動

各 IM and Presence Service 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 コマンド **`utils service restart Cisco XCP XMPP Federation Connection Manager`** を実行します。

ステップ 3 各フェデレーション ノードで繰り返します。

自己署名の信頼証明書の削除

（注） この項の情報は、-ECDSA で終わる証明書にも適用されます。

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 Service 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。

IM and Presence Service または Cisco Unified Communications Manager のいずれかで元の自己署名信頼証明書を置き換えるために CA 署名付き証明書が生成されても、元の自己署名信頼証明書は、両方のノードのサービス信頼ストアで保持されます。自己署名信頼証明書を削除する場合には、IM and Presence Service および Cisco Unified Communications Manager の両方のノードでこれらの証明書を削除する必要があります。

IM and Presence Service からの自己署名信頼証明書の削除

始める前に

重要 ここまでで、CA 署名付き証明書で IM and Presence Service ノードを設定し、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 分待機しました。

手順

ステップ 1 [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 Operating System Administration）] ユーザ インターフェイスにログインし、**[セキュリティ（Security）] > [証明書管理（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、削除する権限を持っている証明書に関してのみ表示されます。

次のタスク

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。

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 （169 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オペレーティングシステムの管理（Cisco Unified Operating System Administration）] ユーザインターフェイスにログインし、**[セキュリティ（Security）] > [証明書管理（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。

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 Service 証明書をインポートすると、IM and Presence Service 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 の管理（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）]** 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 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

IM and Presence Service 証明書をインポートすると、IM and Presence Service 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。

始める前に

IM and Presence Service の TLS ピア サブジェクトを設定します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [TLS コンテキスト設定（TLS Context Configuration）]** 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 **[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 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 [保存（Save）] をクリックします。

ステップ 7 **[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 8 Cisco SIP Proxy サービスを再起動します。

トラブルシューティングのヒント

TLS コンテキストに対する変更を有効にするには、SIP Proxy サービスを再起動する必要があります。

関連トピック

SIP Proxy サービスの再起動 （152 ページ）

TLS 暗号のマッピングの設定

TLS コンテキスト用の TLS 暗号スイートを設定します。

現在のリリースから、次の新しい RSA ベースと ECDSA ベースの暗号化が追加されました。

- ECDHE ECDSA 暗号方式
  - **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**
  - **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**
- ECDHE RSA 暗号方式
  - **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**
  - **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**

TLS 暗号の詳細については、「IM and Presence Service の拡張 TLS 暗号化」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）] > [システム（System）] > [セキュリティ（Security）] > [TLS コンテキスト設定（TLS Context Configuration）]** 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 リストからコンテキスト設定を選択します。

ステップ 4 選択した TLS 暗号のスイートに使用可能な暗号を追加するには、[TLS 暗号のマッピング（TLS Cipher Mapping）] ペインで、[使用可能な TLS 暗号（Available TLS Ciphers）] リストの暗号を選択し、右矢印をクリックしてその暗号を [選択済みの TLS 暗号（Selected TLS Ciphers）] リストに移動させます。

左矢印をクリックして暗号を [選択済みの TLS 暗号（Selected TLS Ciphers）] リストから [使用可能な TLS 暗号（Available TLS Ciphers）] リストに戻すことにより、TLS 暗号の選択を解除できます。

ステップ 5 [選択済みの TLS 暗号（Selected TLS Ciphers）] リスト内の暗号の優先順位を変更するには、リストの右側にある上下の矢印を使用します。

（注） このコンテキストのデフォルト設定に戻す場合は、[デフォルトにリセット（Reset To Default）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

IM and Presence Service での XMPP セキュリティの設定

XMPP セキュリティ モード

IM and Presence Service はXMPPベースの設定でセキュリティが強化されています。次の表は、これらの XMPP のセキュリティ モードについて説明します。IM and Presence Service の XMPP セキュリティ モードを設定するには、**[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）] > [設定（Settings）]** を選択します。

表 *19 : XMPP* セキュア モードの説明

セキュア モード	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）	この設定をオンにすると、IM and Presence Service は、クラスタ内の IM and Presence Service ノードと XMPP クライアント アプリケーション間にセキュアな TLS 接続を確立します。IM and Presence Service は、このセキュア モードをデフォルトでオンにします。 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 Service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 Service 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。

セキュア モード	説明
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 Service は、IM and Presence Service 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 Service の cup-xmpp-trust 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。 **注意** ネットワークおよび IM and Presence Service ノードが IPv6をサポートし、XMPP ベースの API クライアント アプリケーションへのセキュアな TLS 接続の有効にする場合、ノードの 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、Cisco Unified IM and Presence Operating System Administration を使用して各IM and Presence Service ノードで Eth0 の IPv6 Ethernet IP 設定を有効にする必要があります。それ以外の場合は、IP トラフィックにIPv4 を使用しようとします。IPv6 アドレスを使用する XMPP ベースの API クライアント アプリケーションから受信するパケットは配信されません。 外部データベース、LDAP サーバ、または Exchange サーバへの IPv6 接続を使用するためにノードが設定されている場合、またはIPv6 を使用するフェデレーション配置がノードで設定されている場合、ノードを IPv4 を使用するように戻すことはできません。

XMPP のセキュリティ設定を更新した場合は、サービスを再起動します。次のいずれかの操作を行います。

- [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）] を編集した場合は、Cisco XCP Connection Manager 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 - 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。

- [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）] を編集した場合は、Cisco XCP Router 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 - ネットワーク サービス（Control Center - Network Services）]** を選択して、このサービスを再起動します。
- [Web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 Web Client to IM/P Service Secure Mode）] を編集した場合は、Cisco XCP Web Connection Manager 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 - 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。

関連トピック

IM and Presence Service と XMPP クライアント間のセキュア接続の設定 （175 ページ）

IM and Presence Service と XMPP クライアント間のセキュア接続の設定

手順

ステップ 1 **[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）] > [設定（Settings）]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

- クラスタの IM and Presence Service と XMPP client アプリケーションの間のセキュアな TLS 接続を確立するには、[Enable XMPP Client To IM/P Service Secure Mode（XMPP クライアント ツー IM/P サービス セキュア モードを有効にする）] を選択します。

  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。

- クラスタの IM and Presence Service 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 接続を確立するには、[WebクライアントツーIM/Pサービスセキュア モードを有効にする（Enable Web Client To IM/P Service Secure Mode）] を選択します。

  この設定をオンにする場合は、IM and Presence の cup-xmpp-trust 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てください。

注意 ネットワークと IM and Presence Service ノードが IPv6 をサポートし、XMPP ベースの API クライアント アプリケーションへのセキュアな TLS 接続を有効にする場合は、ノードのIPv6 エンタープライズ パラメータを有効にし、クラスタの各 IM and Presence Service ノードで Eth0 の IPv6 Ethernet IP 設定を有効にする必要があります。エンタープライズ パラメータと Eth0 で IPv6 の設定がされていない場合は、ノードは XMPP ベースの API クライアント アプリケーションから受信する IPv6 パケットに対して IPv4 を使用するようにし、それらの IPv6 パケットは配信されません。

外部データベース、LDAP サーバ、またはエクスチェンジ サーバへの IPv6 接続を使用するようにノードが設定されている場合、または、IPv6 を使用するフェデレーション 展開がノードで設定されている場合は、ノードをIPv4 を使用するように戻すことはできません。

ステップ 3 **[保存（Save）]**をクリックします。

XMPP のセキュリティ設定を更新した場合は、次の手順の 1 つを使用して次のサービスを再起動します。

- [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）] を編集した場合は、Cisco XCP Connection Manager 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 - 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。
- **[Web 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 Web Client to IM/P Service Secure Mode）]** を編集した場合は、Cisco XCP Web Connection Manager 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 - 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

IM and Presence Service ノードの XMPP クライアントをサポートするサービスをオンに設定します。

関連トピック

サードパーティ製クライアントの統合 （19 ページ）

IM and Presence Service のオンによる XMPP クライアントのサポート

IM and Presence Service クラスタ内の各ノードでこの手順を実行します。

手順

ステップ 1 **[Cisco Unified IM and Presence Serviceability（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 Service（IM and Presence Service）] ノードを選択します。

ステップ 3 次のサービスをオンにします。

- Cisco XCP Connection Manager：XMPP クライアントまたはIM and Presence Service の XMPP ベースの API クライアントを統合する場合は、このサービスをオンします。
- Cisco XCP Authentication Service：XMPP クライアント、XMPP ベースの API クライアント、または IM and Presence Service の XMPP ベースの API クライアントを統合する場合は、このサービスをオンにします。
- Cisco XCP Web Connection Manager：XMPP クライアント、または IM and Presence Service の XMPP ベースの API クライアントを統合する場合は、このサービスを任意でオンにします。

ステップ 4 [保存（Save）] をクリックします。

ヒント XMPP クライアントが正常に機能するように、クラスタ内のすべてのノードで Cisco XCP Router がオンになっていることを確認します。

関連トピック

サードパーティ製クライアントの統合 （19 ページ）

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 Service の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 Service 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」

ヒント　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、[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生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 Service 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。

第 11 章

クラスタ間ピアの設定

- クラスタ間展開の前提条件 （179 ページ）
- クラスタ間ピアの設定 （180 ページ）
- クラスタ間ピアリングの連携動作と制限事項 （184 ページ）

クラスタ間展開の前提条件

スタンドアロンの IM and Presence Service クラスタ内で、IM and Presence データベース パブリッシャ ノード間にクラスタ間ピアを設定します。クラスタ内の IM and Presence Service サブスクライバ ノードには、クラスタ間ピア接続を設定する必要はありません。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。

- クラスタ間ピアをそれぞれ別の Cisco Unified Communications Manager と統合する必要があります。
- ホームの IM and Presence Service クラスタとリモートの IM and Presence Service クラスタの両方で、必要なマルチノード設定を完了する必要があります。
    - 必要に応じてシステム トポロジを設定し、ユーザを割り当てます。
    - クラスタ内の各 IM and Presence Service ノードでサービスをアクティブにします。
- すべてのローカル IM and Presence ノード、およびすべてのリモート IM and Presence ノードで AXL インターフェイスを有効にする必要があります。IM and Presence Service は、デフォルトでは 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。クラスタ間ピアを設定するには、リモートの IM and Presence Service ノードの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。
- ローカルの IM and Presence データベース パブリッシャ ノードとリモートの IM and Presence データベース パブリッシャ ノードで Sync Agent をオンにする必要があります。クラスタ間ピアを設定する前に、Sync Agent が Cisco Unified Communications Manager からのユーザの同期化を完了できるようにします。

プレゼンス ユーザ プロファイルの特定など、クラスタ間展開のサイジングおよびパフォーマンスに関する推奨事項については、IM and Presence Service の SRND を参照してください。

クラスタ間ピアの設定

クラスタ間ピアの設定

ローカルの IM and Presence Service クラスタのデータベース パブリッシャ ノードと（ピア関係を形成するローカル クラスタを有する）リモートの IM and Presence Service 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実行します。

始める前に

- すべてのローカル IM and Presence Service ノードで AXL インターフェイスをアクティブにして、すべてのリモート IM and Presence Service ノードで AXL インターフェイスがアクティブであることを確認します。
- Sync Agent がローカル クラスタおよびリモート 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。
- リモートの IM and Presence Service 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ます。
- ネットワークで DNS を使用しない場合は、IM and Presence Serviceのデフォルトドメインとクラスタ間展開のノード名の値に関するトピックを参照してください。
- この手順を続行する前に、無効なユーザ ID または重複したユーザ ID を解決します。詳細については、エンド ユーザの管理および処理に関するトピックを参照してください。

（注） 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）

手順

ステップ 1 **[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）]** を選択します。

ステップ 2 リモートの IM and Presence Service クラスタのデータベース パブリッシャ ノードの IP アドレス、FQDN、またはホスト名を入力します。

ステップ 3 AXL 権限を持つリモートの IM and Presence Service ノードのアプリケーション ユーザのユーザ名を入力します。

ステップ 4 AXL 権限を持つリモートの IM and Presence Service ノードのアプリケーション ユーザの関連付けられたパスワードを入力します。

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 Service クラスタのクラスタ間トランク転送として **TCP** 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 Router** を再起動するよう通知が表示された場合は、すべてのクラスタ ノードで **Cisco XCP Router** を再起動します。それ以外の場合は、このステップを省略できます。

ステップ 8 リモート クラスタ間ピアのデータベース パブリッシャ ノードでこの手順を繰り返します。

ヒント Sync Agent が（ローカル クラスタまたはリモート クラスタの）Cisco Unified Communications Manager からの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。

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 Service 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ます。IM and Presence Service 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

続いて Intercluster Sync Agent をオンに設定します。

関連トピック

Cisco XCP Router サービスの再起動 （88 ページ）
クラスタ間展開のノード名の値 （34 ページ）
クラスタ間展開の IM and Presence のデフォルト ドメイン値 （35 ページ）
クラスタ間展開のデフォルトのドメイン値

Intercluster Sync Agent のオン

デフォルトでは、IM and Presence Service は Intercluster Sync Agent パラメータをオンにします。Intercluster Sync Agent パラメータがオンになっていることを確認するか、または手動でこのサービスをオンにするには、この手順を使用します。

Intercluster Sync Agent は、次の処理のために AXL/SOAP インターフェイスを使用します。

- ユーザが（ローカル クラスタ上の）ローカル ユーザであるか、それとも同じドメイン内のリモート IM and Presence Service クラスタ上のユーザであるかを IM and Presence Service が判断できるように、ユーザ情報を取得します。
- ローカル ユーザへのリモートIM and Presence Service クラスタの変更をクラスタに通知します。

（注） ローカル IM and Presence データベース パブリッシャ ノードからリモート IM and Presence データベース パブリッシャ ノードへのユーザ情報の同期に加えて、Intercluster Sync Agent はクラスタのすべてのノード間のセキュリティも処理するため、IM and Presence Service クラスタ内のすべてのノードで Intercluster Sync Agent をオンにする必要があります。

手順

ステップ 1 **[Cisco Unified IM and Presence Serviceability（Cisco Unified IM and Presence Serviceability）] > [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 Service（IM and Presence Service）] ノードを選択します。

ステップ 3 **[Cisco クラスタ間同期エージェント（Cisco Intercluster Sync Agent）]** を選択します。

ステップ 4 [開始（Start）] をクリックします。

次のタスク

クラスタ間ピアの状態を確認する手順に進みます。

関連トピック

マルチノードの拡張性機能 （27 ページ）

クラスタ間ピア ステータスの確認

手順

ステップ 1 **[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（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 表示するピア アドレス エントリを選択します。

ステップ 5 [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どうかが示されます。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 6 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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 7 [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。

Intercluster Sync Agent の Tomcat 信頼証明書の更新

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、このエラーは、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発生します。具体的には、既存の [クラスタ間ピア設定（Inter-cluster Peer Configuration）] ウィンドウで、新しいリモート クラスタを指すように [ピア アドレス（Peer Address）] 値を変更します。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。

この手順では、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に Tomcat 信頼証明書を更新する方法について説明します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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） 自動的に同期しなかった証明書がある場合は、[クラスタ間ピアの設定（Intercluster Peer Configuration）] ウィンドウに移動します。x のマークが付けられたすべての証明書が存在していないため、手動でコピーする必要があります。

クラスタ間ピア接続を削除する

クラスタ間ピア関係を削除する場合は、次の手順を使用します。

手順

ステップ 1 IM and Presence Service 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の管理（Cisco Unified CM IM and Presence Administration）] から、**[プレゼンス（Presence）] > [クラスタ間設定（Inter-Clustering）]** を選択します。

ステップ 3 [検索（Find）] をクリックして、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 **Cisco XCP Router** 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の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 Router（Cisco XCP Router）] を選択し、[再起動（Restart）] をクリックします

ステップ 6 ピア クラスタでこれらの手順を繰り返します。

（注） 複数のクラスタがあるクラスタ間ネットワークからクラスタ間ピアを削除する場合は、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。これは、削除されているクラスタでは、破損しているピア クラスタ接続と同じ数の **Cisco XCP Router** の再起動サイクルが発生することを意味します。

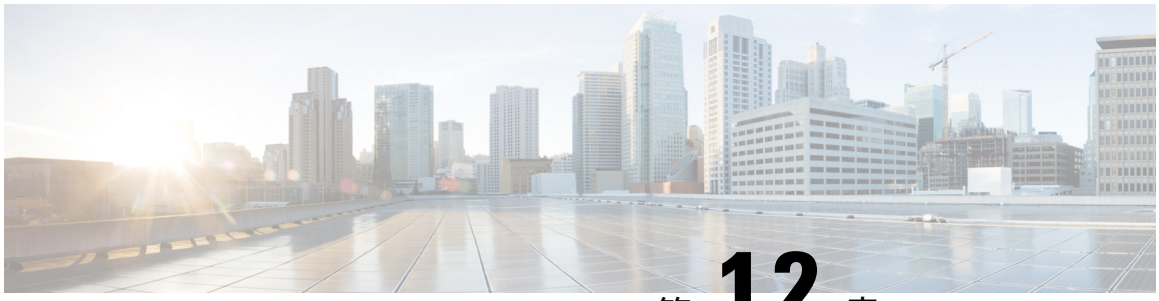
クラスタ間ピアリングの連携動作と制限事項

機能	連携動作と制限事項
Cisco Business Edition 6000	Cisco Business Edition 6000 サーバ上で IM and Presence Service が導入されている場合、クラスタ間ピアリング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、クラスタが集中型であるか、または分散型であるかに関係なく、最大 30 個の IM and Presence Service クラスタをクラスタ間のメッシュに導入できます。

第 III 部

機能設定

- IM and Presence Service 設定のアベイラビリティとインスタント メッセージ （187 ページ）
- アドホック チャットおよび常設チャットの設定 （195 ページ）
- IM and Presence Service での常設チャットの高可用性 （211 ページ）
- マネージド ファイル転送 （219 ページ）
- Multiple Device Messaging （257 ページ）
- iPhone および iPad での Cisco Jabber のプッシュ通知の設定 （261 ページ）



第 12 章

IM and Presence Service 設定のアベイラビリティとインスタント メッセージ

- IM and Presence Service のアベイラビリティの設定 （187 ページ）
- IM and Presence Service での IM 設定 （191 ページ）
- アベイラビリティおよびインスタントメッセージング連携動作および制限事項 （194 ページ）

IM and Presence Service のアベイラビリティの設定

IM and Presence Service クラスタのプレゼンス ステータス共有のオン/オフ

この手順では、IM and Presence Service クラスタのすべてのクライアント アプリケーションにおけるプレゼンス ステータス共有をオンまたはオフにする方法について説明します。

プレゼンス ステータス共有は、IM and Presence Service でデフォルトでオンになっています。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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 プレゼンス ステータスを設定します。次のいずれかの操作を実行します。

- IM and Presence Service クラスタでのプレゼンス ステータス共有をオンするために、[プレゼンスステータス共有の有効化（Enable availability sharing）] のチェックボックスをオンにしてください。この設定をオンにすると、IM and Presence Service では、ユーザのポリシー設定に基づいて、クラスタ内のすべてのユーザ間でそのユーザのプレゼンス ステータス情報が共有されます。

ユーザのデフォルトのポリシー設定では、他のすべてのユーザがそのプレゼンス ステータスを表示できます。ユーザは、Cisco Jabber クライアントから、ポリシー設定をします。

- IM and Presence Service クラスタですべてのクライアントのプレゼンス ステータスの共有をオフにするために、[プレゼンス ステータスの共有を有効にする（Enable availability sharing）] をオフにしてください。この設定をオフにすると、IM and Presence Service では、IM and Presence Service クラスタ内の他のユーザとプレゼンス ステータスが共有されません。また、クラスタ外から受信したプレゼンス ステータス情報も共有されません。ユーザは自分のプレゼンス ステータスだけを表示できます。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 次のサービスを再起動します。

a) Cisco XCP Router
b) Cisco Presence Engine

ヒント
- プレゼンス ステータス共有をオフにすると、ユーザは、クライアント アプリケーションで自分のプレゼンス ステータスを表示できます。その他のすべてのユーザのプレゼンス ステータスはグレー表示されます。
- プレゼンス ステータス共有をオフにして、ユーザがチャット ルームに入ると、そのプレゼンス ステータスは、緑色のアイコンで 「不明」 ステータスを示します。

一時的（アドホック）プレゼンス登録の設定

（注） これらの設定で、ユーザ連絡先リストにないユーザに一時的（アドホック）プレゼンス登録を開始できます。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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 Cisco Jabber ユーザ用の一時的（アドホック）プレゼンス登録をオンにするために、[一時的（アドホック） プレゼンス登録を有効にする（Enable ad-hoc presence subscriptions）] のチェックボックスをオンにします。

ステップ 3 IM and Presence Service が一度に指定する実行中の一時的（アドホック）プレゼンス登録の最大数を設定します。ゼロの値を設定する場合、IM and Presence Service は実行中の一時的（アドホック）プレゼンス登録を無制限に許可します。

ステップ 4 一時的（アドホック）プレゼンス登録の存続可能時間値（秒単位）を設定します。

この存続可能時間値が経過すると、IM and Presence Service は一時的（アドホック）プレゼンス登録をドロップし、そのユーザのプレゼンス ステータスを一時的にモニタしなくなります。

（注） ユーザがまだ一時的（アドホック）プレゼンス登録からのインスタント メッセージを表示している間に存続可能時間値が経過した場合は、表示されるプレゼンス ステータスが最新でないことがあります。

ステップ 5 [保存（Save）] をクリックします。

この設定のために IM and Presence Service のどのサービスも再起動する必要はありません。ただし、Cisco Jabber ユーザは、サインアウトしてからサインインし直して、IM and Presence Service の最新の一時的（アドホック）プレゼンス登録設定を取得する必要があります。

ユーザごとの連絡先リストの最大サイズの設定

ユーザの連絡先リストの最大サイズを設定できます。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と、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。

IM and Presence Service にユーザを移行する場合は、ユーザ連絡先リストのインポート中に連絡先リストの最大サイズと最大のウォッチャの設定を無制限に設定することを推奨します。これにより、移行し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。

手順

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

ステップ 2 [連絡先リストの最大サイズ（ユーザごと）（Maximum Contact List Size （per user））] 設定の値を編集します。

デフォルト値は 200 です。

ヒント　連絡先リストのサイズを無制限にするには、**[無制限（No Limit）]** チェックボックスをオンにします。

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。

関連トピック

Cisco XCP Router サービスの再起動 （88 ページ）

ユーザごとの最大ウォッチャ数の設定

ユーザのウォッチャの数、特にユーザのプレゼンス ステータスを表示するために登録できるユーザの最大数を設定できます。この設定は、Cisco Jabber クライアントとサードパーティ クライアントの連絡先リストに適用されます。

IM and Presence Service にユーザを移行する場合は、ユーザ連絡先リストのインポート中に連絡先リストの最大サイズと最大のウォッチャの設定を無制限に設定することを推奨します。これにより、移行し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。

手順

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

ステップ 2　**[ウォッチャの最大数（ユーザごと）（Maximum Watchers （per user））]** 設定の値を編集します。

デフォルト値は 200 です。

ヒント　ウォッチャの無制限の監視を許可するには、**[無制限 （No Limit）]** チェックボックスをオンにします。

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。

IM and Presence Service での IM 設定

IM and Presence Service クラスタのインスタント メッセージのオン/オフ

この手順では、IM and Presence Service クラスタのすべてのクライアント アプリケーションにおけるインスタントメッセージ機能をオンまたはオフにする方法について説明します。インスタント メッセージ機能は、IM and Presence Service でデフォルトでオンになっています。

⚠

注意 IM and Presence Service のインスタント メッセージ機能をオフにすると、すべてのグループ チャット機能（アドホックおよび常設チャット）が IM and Presence Service で動作しません。Cisco XCP Text Conference サービスをオンにしないか、IM and Presence Service の常設チャットの外部データベースを設定しないことを推奨します。

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** にログインし、**[メッセージング（Messaging）]** > **[設定（Settings）]** を選択します。

ステップ 2 インスタント メッセージングを設定します。次のいずれか 1 つの処理を実行します。

- IM and Presence Service クラスタのクライアント アプリケーションにおけるインスタント メッセージ機能をオンにするには、[インスタントメッセージを有効にする（Enable instant messaging）] のチェックボックスをオンにします。この設定をオンにすると、クライアント アプリケーションのローカル ユーザはインスタント メッセージを送受信できます。
- IM and Presence Service クラスタのクライアント アプリケーションにおけるインスタント メッセージ機能をオフにするには、[インスタントメッセージを有効にする（Enable instant messaging）] のチェックボックスをオフにします。

  （注） この設定をオフにすると、クライアント アプリケーションのローカル ユーザはインスタント メッセージを送受信できません。ユーザは、プレゼンス ステータスおよび電話操作にのみインスタント メッセージ アプリケーションを使用できます。この設定をオフにすると、ユーザはクラスタの外部からインスタントメッセージを受信しません。

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。

オフライン インスタント メッセージのオン/オフ

デフォルトでは、IM and Presence Serviceはユーザがオフラインのときにユーザに送信されたインスタント メッセージを（ローカルに）保存し、ユーザが次にクライアント アプリケーションにサインインしたときに、IM Presence Service はこれらのインスタント メッセージをユーザに配信します。この機能をオフに（抑制）して、IM and Presence Service がオフライン インスタント メッセージを保存しないようにすることができます。

（注） IM and Presence Service はオフライン メッセージを 1 ユーザあたり 100 個、1 ノードあたり最大 30000 個に制限します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [メッセージング（Messaging）] > [設定（Settings）]** を選択します。

ステップ 2 オフライン インスタント メッセージングを設定します。次のいずれかの操作を実行します。

- IM and Presence Serviceのオフライン インスタント メッセージ のストレージをオフにするには、**[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（Suppress Offline Instant Messaging）]** のチェックボックスをオンにします。この設定をオンにすると、IM and Presence Service はユーザがオフラインのときにユーザに送信されたインスタント メッセージを、ユーザが次にクライアント アプリケーションにサインインしたときにユーザに配信しません。
- IM and Presence Serviceのオフライン インスタント メッセージのストレージをオンにするには、**[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（Suppress Offline Instant Messaging）]** のチェックボックスをオフにします。この設定をオフにすると、IM and Presence Service はユーザがオフラインのときにユーザに送信されたインスタント メッセージを、ユーザが次にクライアント アプリケーションにサインインしたときにユーザに配信します。

ステップ 3 [保存（Save）] をクリックします。

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 の管理（Cisco Unified CM IM and Presence Administration）]** > **[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 Service 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 Service 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。

インスタント メッセージでのカット アンド ペーストの許可

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 の管理（Cisco Unified CM IM and Presence Administration）]** > **[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 メッセージでのカット アンド ペーストの設定を行います。

- インスタント メッセージでカット アンド ペーストすることをクライアント アプリケーションのユーザに許可する場合は、**[インスタント メッセージのカット アンド ペーストの許可（Allow cut & paste in instant messages）]** をオンにします。
- インスタント メッセージでカット アンド ペーストすることをクライアント アプリケーションのユーザに許可しない場合は、**[インスタント メッセージのカット アンド ペーストの許可（Allow cut & paste in instant messages）]** をオフにします。

ステップ 3 [保存（Save）] をクリックします。

アベイラビリティおよびインスタントメッセージング連携動作および制限事項

機能	連携動作と制限事項
全員をブロック	Cisco Jabber ユーザが Cisco Jabber ポリシー設定から [全員をブロック（Block everyone）] 機能を有効にすると、ブロック機能により、他の Jabber ユーザは IM and Presence を表示したり、ブロックするユーザと IM and Presence を交換したりできなくなります。ただしブロックするユーザの連絡先リストに連絡先として登録されている場合を除きます。 たとえば、Cisco Jabber ユーザ（Andy）が Jabber の個人設定で [全員をブロック（Block everyone）] を有効にしたとします。Andy の個人用連絡先リストに含まれている Jabber ユーザと含まれていない Jabber ユーザに対して Andy のブロックがどのように影響するかを以下に説明します。Andy は、ブロックの他に、次のような個人用連絡先リストを持っています。 • Bob が含まれている：Bob は Andy の個人用連絡先リストに含まれているので、ブロックに関わらず、IM を送信し、Andy のプレゼンスを確認できます。 • Carol が除外されている：ブロックに基づき Carol は Andy のプレゼンスを確認できず、IM を送信できません。 • Deborah は個人連絡先から除外されています。ただし Deborah は、Andy が連絡先としてリストに含めたエンタープライズ グループのメンバーです。ブロック機能により、Deborah は Andy のプレゼンスの確認も Andy への IM 送信も実行できません。 Deborah は Andy の連絡先リストのエンタープライズ グループのメンバーであるにもかかわらず、Andy のプレゼンスの確認や Andy への IM の送信がブロックされる点に注意してください。エンタープライズ グループの連絡先の動作の詳細については、CSCvg48001 を参照してください。

第 13 章

アドホック チャットおよび常設チャットの設定

- グループ チャットルームの概要 （195 ページ）
- グループ チャットの要件 （196 ページ）
- グループ チャットおよび常設チャットのタスク フロー （197 ページ）
- グループ チャットと常設チャットのインタラクションと制限 （201 ページ）
- 常設チャットの例（高可用性なし） （205 ページ）
- IM and Presence での常設チャットの境界 （206 ページ）

グループ チャットルームの概要

グループ チャットとは、3 人以上のユーザ間でのインスタント 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 ルームおよび常設チャット ルームをサポートします。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 ルームのサポートがデフォルトで有効になります。ただし、常設チャット ルームのサポートについては、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 チャット セッションであり、最後のユーザがルームを離れると、システムから削除されます。アドホック チャット ルームは、最後のユーザがルームを離れると、システムから削除されます。インスタントメッセージの会話の記録は永続的に維持されることはありません。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 ルームはデフォルトで有効化されます。

アドホック チャット ルームは、デフォルトではパブリック ルームですが、プライベートに再設定できます。ただし、ユーザ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 のユーザは、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）に参加するために出席を依頼する必要があります。

- サードパーティ XMPP クライアントのユーザは、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）に参加するために招待されるか、またはパブリックのみのアドホック ルームを検索し、ルーム検出サービスを介して参加することができます。

常設チャット ルーム

常設チャット 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、アドホック グループ チャット セッションと違い、終了することはありません。ユーザは、ディスカッションを続行するために、時間が経過しても同じ会議室に戻ることが求められます。

常設チャット ルームの目的は、ユーザが後で常設チャット ルームに戻って、協力し合い、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参加したりできるようにすることです。

常設チャットルームにはシステムの設定が必要です。また、常設チャットでは、外部データベースを導入する必要があります。

グループ チャットの要件

アドホック チャットの要件

アドホック チャットルームを展開する場合は、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 メッセージの有効化を参照してください。

常設チャットの要件

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 メッセージの有効化を参照してください。
- 外部データベースを導入する必要があります。データベースのセットアップおよび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の*IM and Presence* 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。この導入タイプにより、常設チャットルームに冗長性およびフェール オーバーが追加されます。ただし、外部データベースの要件は、高可用性を持たない機能を導入した場合と若干異なります。
- 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 チャットおよび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 システム管理の設定（197 ページ）	システム管理者を追加して、常設チャット システムを管理します。
ステップ 2	常設チャット ルームの設定 （198 ページ）	常設チャット ルームの基本設定を行います。オプションとして、常設チャットを有効にします。
ステップ 3	Cisco XCP Text Conference Manager の再起動 （199 ページ）	常設チャットを導入する場合は、Cisco XCP Text Conference Manager サービスが実行され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 （200 ページ）	常設チャット ルームを使用するには、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） 常設チャットに高可用性を導入している場合は、高可用性の展開時のデータベース要件が若干異なるため、この章の残りのタスクはスキップすることができます。
ステップ 5	外部データベース接続の追加 （201 ページ）	IM and Presence Serviceで、外部データベースへの接続をセットアップします。

グループ チャット システム管理の設定

システム管理者を追加して、常設チャット システムを管理します。

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。

設定が有効化または無効化する場合、Cisco XCP Routerを再起動する必要があります。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

常設チャット ルームの設定 （198 ページ）

常設チャット ルームの設定

ルーム メンバーおよび収容人数の設定などの基本的なチャット ルームの設定と、ルームあたりのユーザの最大人数の設定を行います。

必要に応じて、**常設チャットを有効にする** チェック ボックスをオンにして、常設チャットを有効に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）] 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 **プライマリグループチャットサーバのエイリアスをシステムで自動的に管理する**チェック ボックスをオンあるいはオフにして、システムがチャット ノードのエイリアスを管理するかどうかを設定します。

- オン：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。
- オフ：管理者がチャット ノードのエイリアスを割り当てることができます。

ステップ 3 すべての参加者がルームから退室した後もチャットルームが存続し続けるようにするには、**常設チャットを有効にする**チェックボックスをオンにします。

（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常設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 クラスタ上のユーザは、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 ルームを検出することができます。

ステップ 4 常設チャットを有効にするように選択した場合は、それぞれの値を以下のフィールドに設定します。

- 許可される常設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)）
- 常設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 **ルームの設定**で、ルームの最大数を割り当てます。

ステップ 6 **グループチャットおよび常設チャットの設定** ウィンドウで、残りの設定を入力します。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 7 [保存（Save）] をクリックします。

次のタスク

Cisco XCP Text Conference Manager の再起動 （199 ページ）

Cisco XCP Text Conference Manager の再起動

チャットの設定を編集したり、チャット ノードに複数のエイリアスを追加している場合は、**Cisco XCP Text Conference Manager** サービスを再起動します。

手順

ステップ 1 **Cisco Unified IM and Presence Serviceability**で、**ツール** > **コントロール センター - 機能サービス**を選択します。

ステップ 2 **サーバ** 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**をクリックします

ステップ 3 **IM and Presence Service** セクションで、**Cisco XCP Text Conference Manager** オプション ボタンをクリックして、**起動** あるいは **再起動**をクリックします。

ステップ 4 再起動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

常設チャットに高可用性を導入する場合は、このガイドの「常設チャットのための高可用性」の章に進み、に進みます。

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（200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、高可用性を備えていない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導入する場合は、外部のデータベース設定情報ではなく、この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各ノードに対して、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。

- 常設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。
- 常設チャットログ出力に外部データベースを使用する場合は、データベースが情報量を処理するのに十分な容量があることを確認します。チャットルームのすべてのメッセージのアーカイブはオプションであり、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ることになります。
- 外部データベースのクリーンアップ ユーティリティを使用して、データベース サイズを監視するジョブを設定し、期限切れのレコードは自動的に削除します。
- 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。UI 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可能です。

外部データベース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 にある『IM and Presence Service 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

外部データベース接続の追加 （201 ページ）

外部データベース接続の追加

IM and Presence Serviceから常設チャットの外部データベースへの接続を設定します。IM and Presence Service 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の管理（Cisco Unified CM IM and Presence Administration）] から、**[メッセージング（Messaging）]** > **[外部サーバのセットアップ（Exernal Servers 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、データベースの名前を入力します。

ステップ 4 [データベースタイプ（Database Type）] ドロップダウンから、導入する外部データベースのタイプを選択します。

ステップ 5 データベースの [ユーザ名（User Name）] および [パスワード情報（Password information）] を入力します。

ステップ 6 [ホスト名（Hostname）] フィールドにホストの DNS 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（External Database Settings）] ウィンドウで残りの設定を入力します。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 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、外部データベース インスタンスへの各接続を作成します。

グループチャットと常設チャットのインタラクションと制限

表 *20 :* グループ チャットと常設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。

機能の相互作用	制約事項
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 チャットまたは常設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常設ルームを作成できません。
OVA 要件	常設チャットまたはクラスタ間のピアリングを導入している場合、これらの機能が導入可能な OVA サイズは 5000 ユーザ OVA になります。最低でも 15000 ユーザ OVA の導入を推奨します。集中型展開では、ユーザ ベースの規模に応じて、25000 ユーザ 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、以下のサイトを参照してください。 （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。 https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html
Microsoft SQL Server での常設チャットの文字数制限	メッセージ本文（HTML タグ+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。こういった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 をリリース 11.5 (1) SU3 を外部データベースとして使用した場合に発生します。詳細は、CSCvd89705 を参照してください。

機能の相互作用	制約事項
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 の常設チャット	Jabber モバイル用の常設チャットは、11.5 (1) SU5 で導入されています。それ以前の 11.5 (1) SU リリースではサポートされていません。この機能は、12.0 (1) または 12.0 (1) の SU1 においてもサポートされていません。 Jabber の常設チャットは今回のリリースで導入されています。Jabber Mobile 用の常設チャットルームをサポートしていないピア クラスタを使用して、クラスタのトランクリングを設定している場合は、Jabber Mobile クライアントに対して以下の条件が適用されます。 常設チャット ルームが、サポートされていないリリース（11.5 (1) など）でホストされている場合： • サポートされるクラスタをホームとする 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することができます。ただし、ルームをミュートするオプションは提供されません。グローバル ミュート オプションは表示されますが、機能しません。 • サポートされていないピア クラスタをホームとする Jabber モバイルクライアントは、常設チャットルームに参加することができません。 11.5 (1) SU5 など、常設チャットルームがサポートされるリリースでホストされている場合： • サポートされるクラスタをホームとする Jabber モバイル クライアントの参加者は、すべての常設チャットをモバイル機能に備えています。 • サポートされないピア クラスタからの Jabber モバイルクライアントは、常設チャットルームに参加することができません。 （注） 常設チャット用の検索機能は、IM 履歴が無効に設定されている Jabber 設定ファイル（*jabber-config.xml*）の場合は機能しません。
外部データベース接続および Cisco XCP Text Conferencing サービス	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。 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。

機能の相互作用	制約事項
高可用性が設定されている場合にサポートされる常設チャット ルームの数	IM&P の導入でサポートされる常設チャット ルームの最大数は、サブクラスタあたり 5000 です。 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。 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 Collaboration Sizing Tool を使用して、常設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。Collaboration Sizing Tool の詳細については、次を参照してください。 https://cucst.cloudapps.cisco.com/landing サブクラスタ内の両方のノード間で均等にルームのバランスを取ることを推奨します。また、IM&P クラスタに複数のサブクラスタがある場合は、すべてのサブクラスタにわたってルームをロードバランシングすることを推奨します。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に選択していることを確認する必要があります。

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します	アドホックチャットルームは、デフォルトではパブリックですが、次の設定のメンバーのみに対して設定できます。 **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.** [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）] 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（高可用性なし）

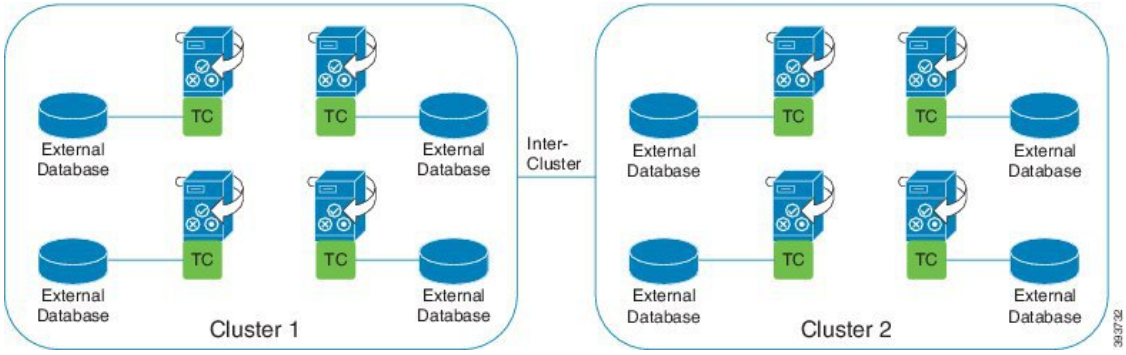
以下の2つの例は、常設チャットの高可用性が展開されていないクラスタ間のピアリングおよび常設チャットの機能を示しています。

（注） 常設チャットを導入する場合は、常設チャットの高可用性を提供して、常設チャットルームに冗長性を追加することが推奨されます。

すべてのクラスタ間ノードで有効にされた常設チャット（高可用性なし）

常設チャット（高可用性なし） は、クラスタ ネットワーク内のすべてのノードで有効になっています。すべてのノードには、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、すべてのノードで同一のチャット ルームをホストすることができます。

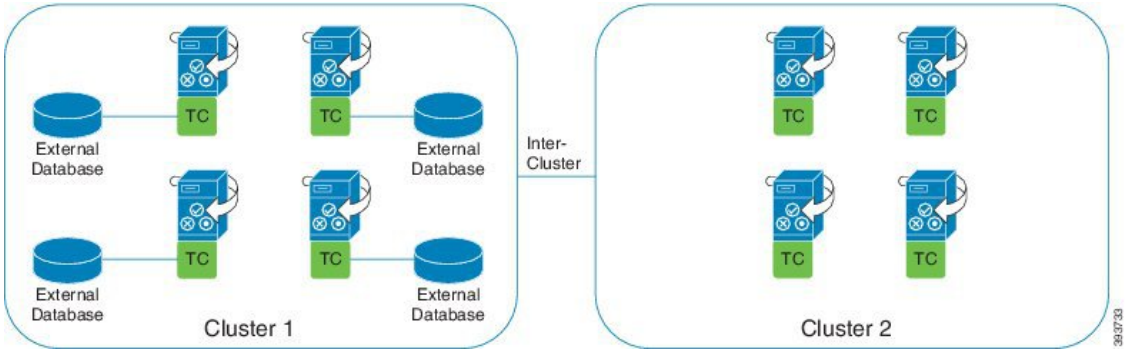
Cisco Text Conferencing サービスは、いずれかのクラスタ内のすべてのノード上で実行されています。これらのクラスタ内のすべてのユーザは、いずれかのクラスタのノードでホストされている常設チャットルームに参加することができます。



クラスタ間ネットワークの単一クラスタで有効にされた常設チャット（高可用性なし）

クラスタ 1 のノードのみの外部データベースを伴う常設チャット（高可用性なし）クラスタ 2 では、常設チャットルームをホスト用にノードが設定されていないため、外部データベースは必要ありません。

ただし、Cisco Text Conference Manager サービスはいずれかのクラスタ内のすべてのノード上で実行されるため、いずれかのクラスタ内のすべてのユーザは、クラスタ 1 でホストされる常設チャットルームに参加することができます。



IM and Presence での常設チャットの境界

ここでは、IM and Presence での常設チャット（PChat）の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ための例を示します。

次の前提は、常設チャットの境界を派生させるために作成されたものです。

1. エイリアス/サーバ/サブクラスタ/クラスタあたりのルームの数に対して、次のようになります。
    1. サーバには、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（ノード）が含まれています。
    3. クラスタは最大 3 つのサブクラスタを持つことができます。

2. 高可用性（HA）が有効な場合は、サポートされているすべてのルーム番号が半分になります。**常設チャットルームの最大数として許可される最大値** は 2500 です。
3. 例：ルームごとに平均 100 ユーザを想定した場合、IM and Presence Service は、次の機能をサポートしています。
    1. HA のないサーバーごとに 3500 の常設チャットルーム、または
    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 ルームあたり 1 つのメッセージを保持しているとします。1 台のサーバにつき、最大 273 の常設チャットルームをアクティブにできます。

次に、これらの依存関係を明確にするいくつかの例を示します。

次の式を使用すると、タイムスライスごとにサポートされるルームは、サポートされるルームの総数を犠牲にして増加することができます。

サポートされるルーム数 = 現在サポートされているルーム数 * タイムスライスごとに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ルーム（%）

表 *21 : 25K OVA* 常設チャット キャパシティ の表（サーバあたり）

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数 = 10

メッセージの頻度 = 3/分

現在サポートされているルーム数 = 5000

タイムスライスごとにサポートされている現在のルーム = 33%

タイムスライスごとにサポートされるルーム = 50%

結果：

サポートされるルーム = 5000 * 33/50 = 3300

表 *22 : 15K OVA* 常設チャット キャパシティの表（サーバあたり）

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

メッセージの頻度 = 3/分

現在サポートされているルーム数 = 5000

タイムスライスごとにサポートされている現在のルーム = 41%

タイムスライスごとにサポートされるルーム = 50%

結果：

サポートされるルーム = 5000 * 41/50 = 4100

表 *23 : 5K OVA* 常設チャット キャパシティの表（サーバあたり）

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

メッセージの頻度 = 3/分

現在サポートされているルーム数 = 5000

タイムスライスごとにサポートされている現在のルーム = 31%

タイムスライスごとにサポートされるルーム = 50%

結果：

サポートされるルーム = 5000 * 31/50 = 3100

第 14 章

IM and Presence Service での常設チャットの高可用性

- 常設チャットにおける高可用性の概要 （211 ページ）
- 常設チャットにおける高可用性のフロー （212 ページ）
- 常設チャットにおける高可用性の有効化と確認 （215 ページ）
- 常設チャットの高可用性のための外部データベース （216 ページ）

常設チャットにおける高可用性の概要

現在のリリースから、常設チャット機能は高可用性に対応しています。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 ノードの 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、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。

高可用性の詳細については、Ciscoユニファイドコミュニケーション マネージャ のシステム設定ガイドから、プレゼンス冗長グループの設定に関する章を参照してください。

この例では、3 人のユーザ（A、B、C）と 3 つの IM and Presence Service ノード（1A、2A、1B）があります。ノード 1A と 1B は同じプレゼンス冗長グループの一部で、高可用性（HA）ペアを形成します。ユーザは、次のノードに割り当てられます。

- ユーザ A = ノード 1A
- ユーザ B = ノード 2A
- ユーザ C = ノード 1B

1. ユーザ A、B、C はノード 1A にホストされているチャット ルームにいます。
2. テキスト会議（TC）サービスがノード 1A で失敗します。
3. IM and Presence Service 管理者は、手動フォールバックを開始します。

4. ノード 1B は、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、HA の状態 [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。
5. HA フェールオーバー モデルに沿ってユーザ A 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。
6. ユーザ B および C に変更はありませんが、ノード 2A 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送信できます。
7. ノード 1A は**テイクバック中**に移行して、ノード 2A は**フォールバック中**に移行します。
8. ユーザ A はノード 1B からサインアウトします。ユーザ B および C 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 [テイクバック中（Taking 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 [フェールオーバー中（Failing Over）] から [正常（Normal）] に遷移し、pubalias.cisco.com に関連付けられているルームをリロードします。
11. ユーザ A はノード 1A に再度サインインし、常設チャット 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。

表 *24* : グループ チャットと常設チャットの制限

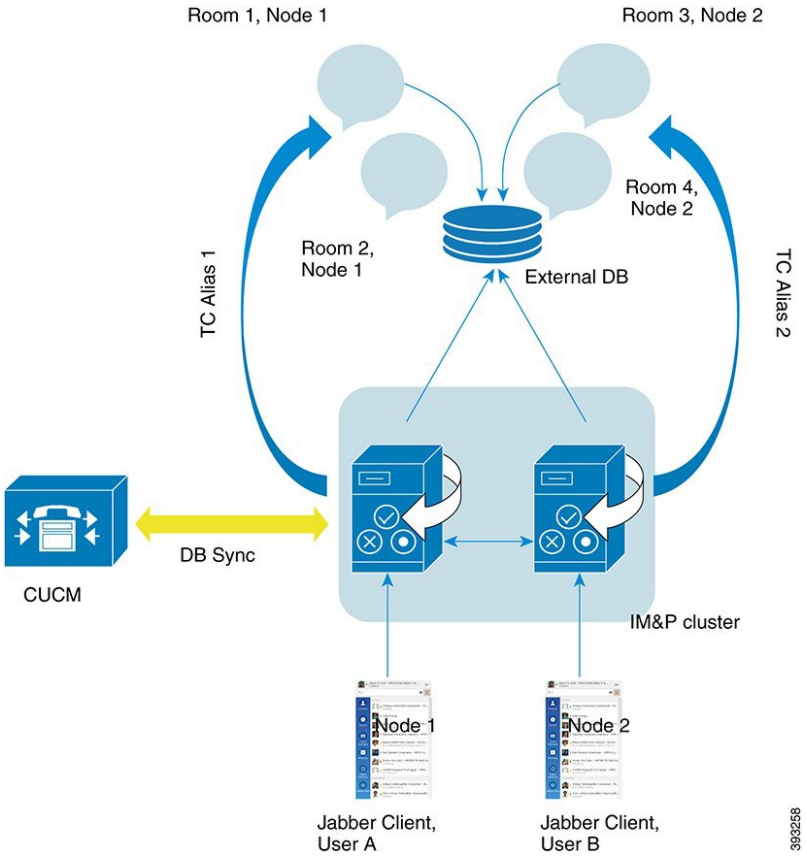
機能	制約事項
匿名ルームでのチャット	Cisco Jabber 経由でチャットを展開する場合（グループ チャットまたは常設チャットのいずれか）は、[グループチャットとパーシステントチャットの設定（Group Chat and Persistent Chat Settings）] ウィンドウで [デフォルトで、ルームは匿名です（Rooms are anonymous by default）] および [ルームのオーナーは、ルームを匿名にするかどうかを変更できます（Room owners can change whether or not rooms are anonymous）] オプションが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。

常設チャットにおける高可用性のフロー

次に、フェールオーバーとフェールバックにおける常設チャットの高可用性フローを示します。

（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 Router 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 *14* : 常設チャットにおける高可用性の構造



常設チャットにおける高可用性のフェールオーバー フロー

この例では、4 人のユーザが、2 つの高可用性（HA）ペアあるいはサブクラスタを持つ 4 つの IM and Presence Service ノードを持っています。ユーザは以下のように割り当てられます。

サブクラスタ 1	サブクラスタ 2
• 山田 はノード 1A 存在：ノード 1A はチャット ルームをホストしています。 • 髙橋 はノード 1B 上に	• 斎藤はノード 2A 上に存在する • 小川はノード 2B 上に存在する

1. 4 人のユーザすべてが、ノード 1A でホストされる同一のチャット ルーム内でチャットを行っています。
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、1A からユーザを引き継ぎ、**フェールオーバー済み（重要なサービスは非実行）**の状態に移行させてから、**バックアップモードで実行中** のHAの状態に移行させます。
5. HA フェールオーバー モデルに沿って、山田が自動的にログアウトし、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。ノード 1B でホストされるチャット ルームへのメッセージは引き続き投稿されます。
7. ユーザ A は常設チャット 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。

常設チャット ルームの高可用性フォールバック フロー

この例では、4 人のユーザが、2 つの高可用性（HA）ペアあるいはサブクラスタのある 4 つの IM and Presence Service ノードを持っています。ユーザは以下のように割り当てられます。

サブクラスタ 1	サブクラスタ 2
• 山田 はノード 1A 存在：ノード 1A はチャット ルームをホストしています。 • 髙橋 はノード 1B 上に	• 斎藤はノード 2A 上に存在する • 小川はノード 2B 上に存在する

1. 4 人のユーザすべてが、ノード 1A でホストされる同一のチャット ルーム内でチャットを行っています。
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、1A からユーザを引き継ぎ、**フェールオーバー済み（重要なサービスは非実行）**に移行させてから、**バックアップモードで実行中** のHAの状態に移行させます。
4. HA フェールオーバー モデルに沿って、山田が自動的にログアウトし、バックアップ ノード 1B にサインインします。
5. 髙橋、斎藤 および 小川は影響を受けません。ノード 1B でホストされるチャット ルームへのメッセージは引き続き投稿されます。
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**に移行して、ノード 2A は **フォールバック中**に移行します。

8. 山田 はノード 1B からログアウトします。髙橋、斎藤、小川は、常設チャット ルームの使用を継続し、**フォール バック** が起こると、ルームはノード 1Aに戻ります。
9. ノード1Bは、HAの状態から、**正常**に**フォールバック**し、ピア ノードルームをアンロードします。
10. ノード 1B は、**テイクバック中**のHA の状態から **正常**に移行し、ピア ノード ルームをリロードします。
11. ユーザAは常設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。

常設チャットにおける高可用性の有効化と確認

常設チャットの高可用性を有効にし、正しく動作していることを確認するには、次の手順を実行します。

手順

ステップ 1 高可用性がプレゼンス冗長グループで有効なことを確認するには、以下を実行します。

a) [Cisco Unified CM 管理（Cisco Unified CM Administration）] **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。
b) [プレゼンス冗長グループの検索/一覧表示（Find and List Presence Redundancy Groups）] ウィンドウで [検索（Find）] をクリックして、オンにするプレゼンス冗長グループを選択します。
c) [プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウで、[高可用性の有効化（Enable High Availability）] 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 2 常設チャットがプレゼンス冗長グループで有効なことを確認するには、以下を実行します。

a) [Cisco Unified CM IM and Presenceの管理UI（Cisco Unified CM IM and Presence Administration UI）]**で、** >**[Messaging（メッセージング）]** > **[Group Chat and Persistent Chat（グループチャットと常設チャット）]** を選択します。
b) [グループチャットと常設チャット（Group Chat and Persistent Chat）] ウィンドウで、[常設チャットの有効化（Enable Persistent Chat）] 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 3 プレゼンス冗長グループ ノードがどちらも同じ外部データベースに割り当てられていることを確認します。画像を参照してください。

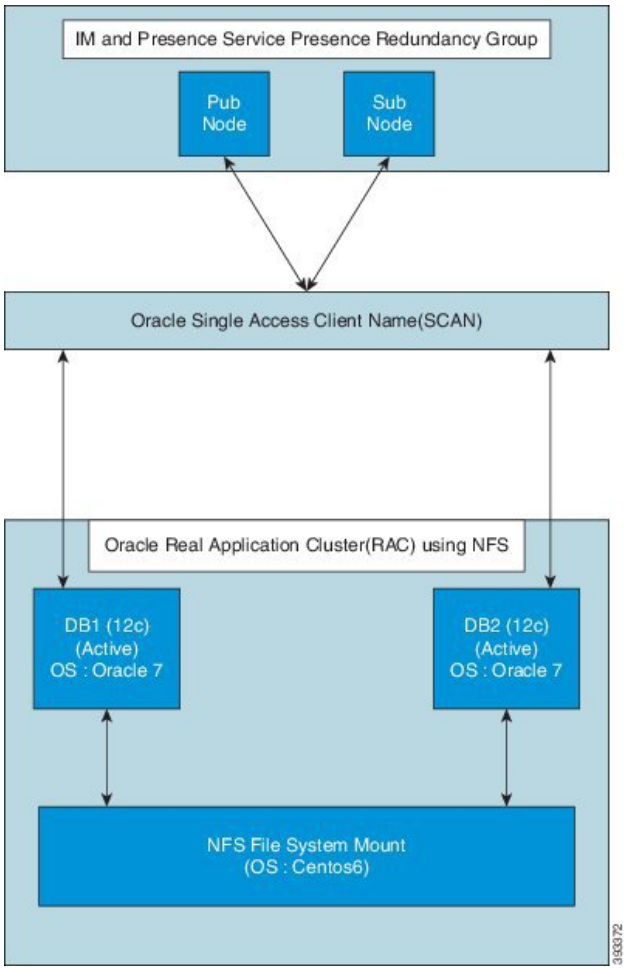
ステップ 4 常設チャットの高可用性が有効であることを確認するには、**[システム（System）]**>**[プレゼンス トポロジ（Presence Topology）]** ウィンドウを確認します。[ノードの詳細（Node Detail）] ペインの [ノードのステータス（Node Status）] セクションの [サービス列（Service Column）] で、[Cisco XCP Text Conference Manager] エントリの [モニタ対象（Monitored）] 列が [Yes] であることを確認します。

これがモニタ対象サービスである場合は、これが重要なサービスであり、高可用性が正常に有効にされていることを意味します。モニタ対象サービスでない場合は、プレゼンス冗長グループが正しく設定されていることを確認します。

常設チャットの高可用性のための外部データベース

サポートされているバージョンについては、『IM and Presence Service データベース セットアップ ガイド』の「外部データベースのセットアップ要件http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/database_setup/11_5_1/cup0_b_database-setup-guide-imp-115/cup0_b_database-setup-guide-imp-115_chapter_00.html#reference_6CA83246733D800138FE3F8DCD3FCFA9」の項を参照してください。

図 *15 : Oracle* 高可用性設定



外部データベースのテーブルのマージ

外部データベースのマージ ツールでは、複数の外部データベース パーティションに保存されている常設チャット データを 1 つのデータベースにマージできます。

以前のバージョンでは、プレゼンス冗長グループの各 IM and Presence Service ノードに固有の外部データベースが割り当てられていました。現在のリリースからは、常設チャットの高可用性を有効にする際はプレゼンス冗長グループのノードを 1 つの外部データベースにのみ割り当てる必要があります。外部データベースのマージ ツールにより、これらの 2 つのデータベースをすばやく連結することができます。

外部データベースのマージ ツールは、Oracle と Postgres データベースで使用できます。

（注） Oracle データベースで外部データベース マージ ツールを使用するには、[Oracle SID] フィールドに [データベース名（Database Name）] フィールドと同じ値を設定する必要があります。そうしないと、マージは失敗します。詳細については、CSCva08935 を参照してください。

外部データベースのマージ ツール

IM and Presence Service のプレゼンス冗長グループで 2 つのデータベースをマージするには、次の手順を使用します。

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。
  - `GRANT CREATE TABLE TO <user_name>;`
  - `GRANT CREATE PUBLIC DATABASE LINK TO <user_name>;`

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。

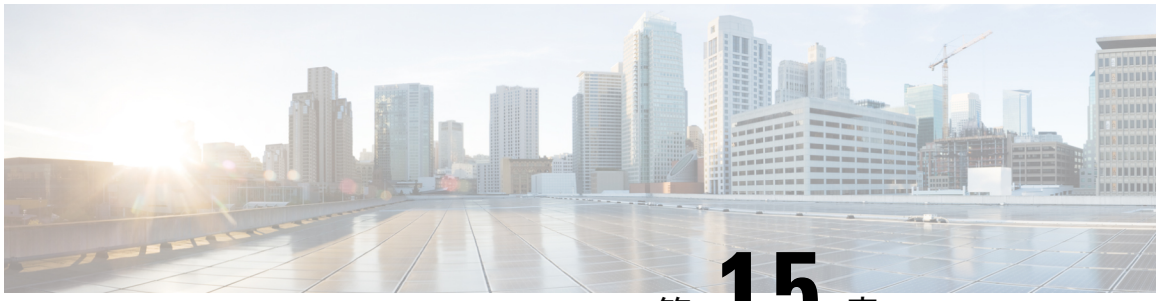
ステップ 9 マージが正常に完了したら、[外部データベースの検索と一覧表示（Find And List External Database Jobs）] ウィンドウがロードされます。ウィンドウを更新し、新しいジョブを表示するには、[検索（Find）] をクリックします。

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。



第 15 章

マネージド ファイル転送

- マネージド ファイル転送 （219 ページ）
- 外部データベース （222 ページ）
- 外部ファイル サーバ （224 ページ）
- Cisco XCP File Transfer Manager RTMT のアラームとカウンタ （230 ページ）
- マネージド ファイル転送のワークフロー （233 ページ）
- マネージド ファイル転送のトラブルシューティング （247 ページ）
- Cisco Jabber クライアントの相互運用性 （247 ページ）

マネージド ファイル転送

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 Service 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、常設チャット 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。

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。

サポート対象のソフトウェア

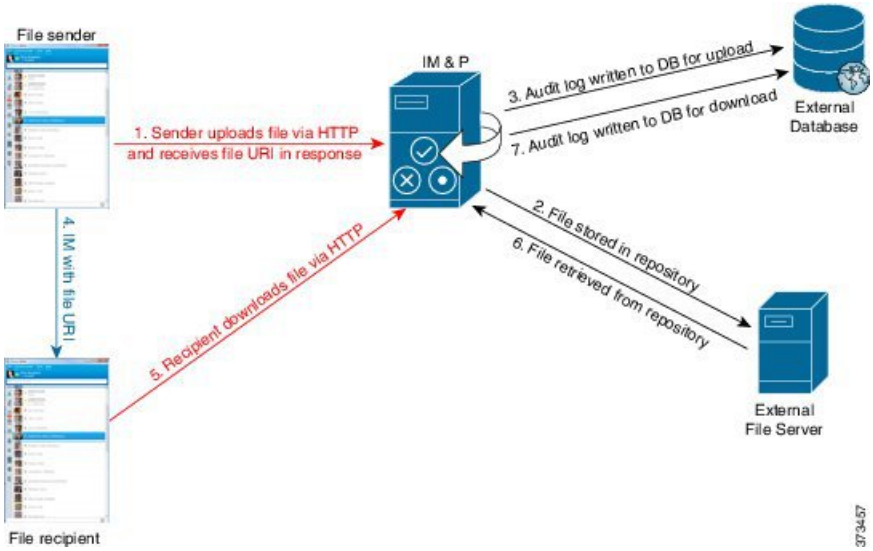
マネージド ファイル転送でサポートされているデータベースの詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html の『IM and Presence Service のデータベース セットアップ ガイド』で「外部データベースを使用する場合の要件」の章を参照してください。

関連トピック

PostgreSQL のマニュアル

Oracle のマニュアル

ファイル転送のフロー



1. 送信者のクライアントは HTTP 経由でファイルをアップロードし、サーバはファイルの URI を応答として返します。
2. ファイルは、ファイル サーバのリポジトリに格納されます。
3. 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が書き込まれます。
4. 送信者のクライアントが受信者に IM を送信します。IM にはファイルの URI が含まれます。
5. 受信者のクライアントが HTTP 経由でファイルを要求します。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、ファイルが受信者にダウンロードされます。

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。

特記事項

IM and Presence Service ノードでマネージドファイル転送を有効にする前に、次の点を考慮してください。

- IM and Presence Service ノードで、常設グループ チャット機能、メッセージ アーカイバ機能、マネージドファイル転送機能を組み合わせて配置する場合は、これらの機能すべてに、同一の物理外部データベース インストールと外部ファイル サーバを割り当てることができます。ただし、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。マネージドファイル転送機能が機能するためには、クライアントがホスト名を解決できるだけでは不十分です。FQDNを解決できる必要もあります。
- 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。

次のいずれかのオプションを [ファイル転送（File Transfer）] ウィンドウで設定できます。

- [無効（Disabled）]：クラスタに関してファイル転送が無効。
- [ピアツーピア（Peer-to-Peer）]：1対1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（Managed File Transfer）]：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。
- [マネージドおよびピアツーピアファイル転送（Managed and Peer-to-Peer File Transfer）]：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。

外部データベース

IM and Presence Service クラスタ内の各 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。外部データベースは、ファイル転送に関連する以下のメタデータをログに記録します。

- AFT インデックス：トランザクションを特定するシーケンス番号。
- JID：ファイルをアップロードまたはダウンロードしたユーザの Jabber ID。
- 宛先 JID：ファイル転送の宛先であるユーザ、グループ チャット、常設ルームの Jabber ID。
- ファイル名：アップロードされたファイルに割り当てられる、自動生成のエンコード化されたリソース名。
- 実際のファイル名：アップロードされたファイルの実際の名前。
- ファイル サーバ：ファイルが保存されているファイル サーバのホスト名または IP アドレス。
- ファイル パス：ファイル サーバ上のファイルへの絶対パス（ファイル名を含む）。
- ファイル サイズ：ファイルのサイズ（バイト単位）。
- タイム スタンプ値：ファイルがアップロードまたはダウンロードされた日時（UTC）。

（注） 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*』（リンク）を参照してください。

特記事項

- 外部データベースの要件と制約事項は、IM and Presence Service で展開する機能によって異なります。
  - マネージドファイル転送：IM and Presence Service クラスタ内の各 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。
  - 常設グループ チャット：IM and Presence Service クラスタ内の各 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。

  （注） 各ノードに固有の論理データベース インスタンスが必要ですが、それぞれのノードは同じ物理データベース インストールを共有できます。

  - メッセージ アーカイバ：IM and Presence Service クラスタに対して、少なくとも 1 つの論理外部データベース インスタンスを設定することを強く推奨します。ただし、IM トラフィックとサーバの容量によっては、クラスタに対して複数の外部データベースが必要になることもあります。

- IM and Presence Service が IPv6 を使用して外部データベース サーバに接続する場合は、エンタープライズ パラメータが IPv6 用に設定され、配置内の各ノードでイーサネット インターフェイスが IPv6 用に設定されていることを確認してください。そうしないと、外部データベース サーバへの接続に失敗し、Cisco XCP Message Archiver と Cisco XCP Text Conference Manager のサービスは、外部データベースに接続することができず、失敗します。IM and Presence Service で IPv6 を設定する方法の詳細については、関連トピックを参照してください。
- マネージドファイル転送機能のデータベース サイズとスケーラビリティについては、http://www.cisco.com/c/en/us/solutions/enterprise/unified-communication-system/index.html で『Cisco Collaboration System ソリューション リファレンス ネットワーク デザイン（SRND）』を参照してください。

関連トピック

IPv6 設定（IPv6 Configuration） （110 ページ）

外部データベースのディスク使用量

データベースのディスク使用量を管理する必要があります。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。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トがあります。Cisco XCP File Transfer Manager RTMT のアラームとカウンタ （230 ページ）を参照してください。

以下は、外部データベースからレコードを消去にするために使用できるサンプル SQL コマンドです。

- 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するには、次のコマンドを実行します。

  DELETE

  FROM *aft_log*

  WHERE *method* = **'Post'**;

- 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レコードを削除するには、次のコマンドを実行します。

  DELETE

  FROM *aft_log*

  WHERE *jid* LIKE **'<userid>@<domain>%'** AND *method* = **'Get'**;

- 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。

  DELETE

  FROM *aft_log*

  WHERE *method* = **'Post'** AND *timestampvalue* > **'2014-12-18 11:58:39'**;

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クエリについては、『*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*』（リンク）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。

外部ファイル サーバ

ファイル サーバはマネージドファイル転送機能によって転送されるファイルのリポジトリです。マネージドファイル転送に関連するメタデータは外部データベースに保存されます。

（注） ファイルは、IM and Presence Service ノードではなく、外部の Linux ファイル サーバに保存されます。

外部ファイル サーバの要件

外部サーバに関する次の要件に注意してください。

- ファイル サーバの容量に応じて、各 IM and Presence Service ノードは自身の論理ファイル サーバ 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 インストールを共有できます。
- 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 OpenSSH 4.9 以降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 60 MB を超えている必要があります。

  ファイル サーバの転送スピードを判別するために、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、システムの稼動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、『Cisco Unified Communications Solutions コマンドライン インターフェイス ガイド』（リンク）を参照してください。

ファイル ストレージ パーティションの推奨事項

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 4 GB 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 100 KB のファイルを 2 つ転送すると、1 日 8 時間では 19.2 GB になります。

特記事項

- お客様は外部ファイル サーバを提供して管理する必要があります。
- お客様の責任でファイル ストレージとディスク使用量を管理する必要があります。ファイル サーバ管理の詳細については、関連資料を参照してください。

ファイル サーバのディスク使用状況の管理に役立つカウンタとアラートが用意されています。マネージドファイル転送のアラームとカウンタの詳細については、関連資料を参照してください。

- 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。
- ファイル サーバへの接続は SSHFS を使用して暗号化されるため、すべてのファイルの内容が暗号化されます。

関連トピック

前提条件 （236 ページ）
ファイル サーバの管理 （228 ページ）
Cisco XCP File Transfer Manager RTMT のアラームとカウンタ （230 ページ）

ユーザ認証

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。
- 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。

パブリック キーとプライベート キー

サーバのプライベート/パブリック キー ペアが生成されるとき、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。

1. 次のコマンドを入力します。

   ```
   $ ssh-keygen -t rsa -b 2048
   ```

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。

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ライバ ノードへのステータスを確認する際、また逆を確認する際に、この外部ファイルサーバに関する情報「そのメッセージがここから実行される場合があります。」のメッセージが表示されます。

このログには、「 -7 」つまり外部ファイル サーバが設定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示す、「 ping 」が表示されます。

パブリッシャーノードでは外部ファイル サーバを設定し、パブリッシャ ノードの公開キーは外部ファイルサーバの「Authorized_key」ファイルで共有されます。

ファイル サーバ ディレクトリ

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。

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 ノードでパス */opt/mftFileStore/node_1/* を作成します。[1].
- ディレクトリ `/files/` が自動生成されます。

[1] マネージド ファイル転送を有効にする他のすべてのノード上で、このディレクトリ構造を必ず作成してください。

- 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。

ファイル サーバの管理

ファイル ストレージとディスク使用量を管理する必要があります。外部データベースのサイズを管理するには、クエリをシェル スクリプトと組み合わせることで、ファイルを自動的に消去できます。クエリでは、ファイルの転送時に作成されるメタデータ（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）を使用できます。

（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。

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。
- 常設チャットの転送は、長期間保持される必要がある可能性があります。

サンプル クエリおよび出力

AFT_LOG テーブルに対してクエリを実行し、そのクエリの出力を使用して、外部ファイル サーバから不要なファイルを消去できます。

たとえば、次のクエリは、特定の日付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返します。

SELECT *file_path*

FROM *aft_log*

WHERE *method* = **'Post'** AND *timestampvalue* > **'2014-12-18 11:58:39'**;

このクエリの出力は次のようになります。

```
/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
```

その後、rm コマンドとこの出力を使用して、外部ファイル サーバからこれらのファイルを削除するスクリプトを作成できます。外部ファイル サーバからレコードを消去にするために使用できるその他のサンプル SQL クエリについては、『*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*』（リンク）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。

マネージド ファイル転送サービスのパラメータ

外部ファイル サーバのディスク領域の管理を容易にするために、次のサービス パラメータを使用して、RTMT アラームが生成されるしきい値を設定することができます（Cisco XCP File Transfer Manager サービスの場合）。

- 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、XcpMFTExtFsFreeSpaceWarn アラームが生成されます。このサービス パラメータのデフォルト値は 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、XcpMFTExtFsFreeSpaceWarn アラームが解除されます。このサービス パラメータのデフォルト値は 15% です。

これらのパラメータのいずれかを変更した後は、Cisco XCP Router サービスを再起動する必要があります。これらのパラメータを設定するには、[Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] インターフェイスにログインし、**[システム（System）] > [サービスパラメータ（Service Parameters）]** と選択し、各ノードに関する [Cisco XCP File Transfer Manager] サービスを選択します。

ヒント　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。

関連トピック

Cisco XCP File Transfer Manager RTMT のアラームとカウンタ （230 ページ）

Cisco XCP File Transfer Manager RTMT のアラームとカウンタ

アラート（Alerts）

IM and Presence Service ノードが、マネージドファイル転送用に外部サーバおよび外部データベースに統合されている場合、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。

接続が失われたときに通知を受け取るようにするには、RTMTアラームが次のように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。

アラーム	問題	ソリューション
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。

Cisco XCP MFT カウンタ

マネージドファイル転送の管理を容易にするために、新しく 1 つのフォルダ（Cisco XCP MFT Counters）と 6 個のカウンタが RTMT に追加されました。

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。
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。

XCP File Transfer Manager のアラームの設定

手順

ステップ 1 **Cisco Unified IM and Presence Serviceability** にログインします。

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 リストから、アラームを設定するサーバ（ノード）を選択し、[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 アラーム設定を適切に設定し、[保存（Save）] をクリックします。

マネージド ファイル転送のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	外部データベースをセットアップします。「*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*」（リンク）を参照してください。	外部データベースは、アーカイブされたファイルに関連付けられたメタデータを格納するリポジトリです。
ステップ 2	IM and Presence Service での外部データベース インスタンスの設定 （233 ページ）	IM and Presence Service ノードを外部データベースに接続するのに必要な手順を説明します。
ステップ 3	外部ファイル サーバのセットアップ （236 ページ）	外部 Linux ファイル サーバを設定するための手順を説明します。
ステップ 4	IM and Presence Service での外部ファイル サーバインスタンスの設定 （240 ページ）	IM and Presence Service ノードを外部ファイル サーバに接続するのに必要な手順を説明します。
ステップ 5	IM and Presence Service でのマネージド ファイル転送の有効化 （243 ページ）	IM and Presence Service ノードでマネージド ファイル転送機能を有効にするための一連の指示が含まれています。ノードを外部データベースにリンクし、ノードを外部ファイル サーバにリンクするための方法を説明します。

IM and Presence Service での外部データベース インスタンスの設定

クラスタの IM and Presence Service データベースのパブリッシャ ノードで、この設定を実行します。

始める前に

- 外部データベースをインストールして設定します。「*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*」（リンク）を参照してください。
- 外部データベースのホスト名または IP アドレスを取得します。
- データベースとして Oracle を使用する場合、テーブルスペースの値を取得します。

  Oracle データベースのテーブルスペースが取得できるかを判断するには、sysdba として次のクエリを実行します。

```
SELECT DEFAULT_TABLESPACE FROM DBA_USERS WHERE USERNAME = 'UPPER_CASE_USER_NAME';
```

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** のユーザ インターフェイスにログインします。**[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（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 [外部データベース設定（External Database Settings）] ウィンドウで次のフィールドに入力し、[保存（Save）] をクリックします。

フィールド	説明
データベース名（Database Name）	外部データベースのインストール中に定義されたデータベースの名前を入力します。 （注） Oracle を使用している場合、この値は Windows のサービス名と一致する必要があります。
データベース タイプ	ドロップダウン リストからデータベースのタイプとして [Postgres] または [Oracle] を選択します。 （注） データベース タイプとして Oracle を選択した場合、[SSL の有効化（Enable SSL）] チェックボックスと [テーブルスペース（Tablespace）] フィールドがアクティブになります。
テーブルスペース（Tablespace）	テーブルスペースの値を入力します。
ユーザ名（User Name）	外部データベースのインストール中に定義した、データベースユーザ（所有者）のユーザ名を入力します。
[パスワード（Password）]	データベース ユーザのパスワードを入力して確認します。
ホストネーム（Hostname）	外部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。
部品番号（Port Number）	外部データベースのポート番号を入力します。 （注） Postgres（5432）、Oracle（1521）、SSL が有効な Oracle（2484）のデフォルトのポート番号が、**[ポート番号（Port Number）]** フィールドにあらかじめ追加されています。必要に応じて、別のポート番号を入力することを選択できます。

フィールド	説明
SSL の有効化（Enable SSL）	SSL を有効にする場合は、このチェックボックスをオンにします。 • データベース タイプとして Oracle が選択されている場合、このチェックボックスが有効になります。Postgres データベースではこのオプションを使用できません。 • [SSLの有効化（Enable SSL）] チェックボックス、または [証明書の名前（Certificate Name）] ドロップダウン フィールドのいずれか、あるいは両方を変更すると、外部データベースに割り当てられている該当するサービス（Cisco XCP Message Archiver または Cisco XCP Text Conference Manager）を再起動するよう求める通知が送信されます。
証明書の名前（Certificate Name）	ドロップダウン リストから証明書を選択します。 • [SSLの有効化（Enable SSL）] チェックボックスをオンにすると、ドロップダウン リストがアクティブになります。 • SSL を有効にする必要がある証明書は、cup-xmpp-trust ストアにアップロードする必要があります。 • 証明書が cup-xmpp-trust ストアにアップロードされた後、証明書が IM and Presence Service クラスタのすべてのノードに伝達されるまで、15 分間待機する必要があります。待機しなければ、証明書が伝達されていないノードで SSL 接続は失敗します。 • 証明書がないか、または cup-xmpp-trust ストアから削除された場合は、Cisco Unified Communications Manager Real Time Monitoring Tool（RTMT）で XCPExternalDatabaseCertificateNotFound のアラームが発生します。

[保存（Save）] をクリックすると、IM and Presence Service は外部データベースについて次のステータス情報を示します。

- データベースの到達可能性：IM and Presence Service が外部データベースを ping できることを検証します。
- データベースの接続性：IM and Presence Service が外部データベースとの Open Database Connectivity（ODBC）接続を正常に確立したことを検証します。
- データベース スキーマの検証：外部データベース スキーマが有効であることを検証します。

Postgres のみ：外部データベースを割り当てた後で `install_dir/data/pg_hba.conf` ファイルまたは `install_dir/data/postgresql.conf` ファイルで設定を変更した場合は、外部データベースの接続を検証する必要があります。

次のタスク

外部ファイル サーバのセットアップ （236 ページ）

関連トピック

http://www.postgresql.org/docs/manuals/
http://www.oracle.com/pls/db111/portal.portal_db?selected=11

外部ファイル サーバのセットアップ

前提条件

外部ファイルサーバのセットアップを始める前に実行しておく必要のあるタスクは、次のとおりです。

- 外部データベースをインストールして設定します。「*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*」（リンク）を参照してください。
- IM and Presence Service での外部データベース インスタンスの設定 （233 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、次の手順を実行しておきます。

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 *yes* に設定されていることを確認します。

- RSAAuthentication *yes*
- PubkeyAuthentication *yes*

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。詳細については、「*External File Server Requirements*」のトピックを参照してください。

次のタスク

ユーザの設定 （237 ページ）

関連トピック

外部ファイル サーバの要件 （225 ページ）

ユーザの設定

手順

ステップ 1 ファイル サーバ上で root として、ファイル ストレージのディレクトリ構造を所有するユーザ（この例では *mftuser* を使用）を作成し、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 *mftuser* 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

ディレクトリの設定 （238 ページ）

ディレクトリの設定

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およびパスは、「*IM and Presence Service* での外部ファイル サーバの展開」タスクで入力する [外部ファイルサーバディレクトリ（External File Server Directory）] フィールドで使用します。
- 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

パブリック キーの取得 （239 ページ）

パブリック キーの取得

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。

（注）
- 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` ファイルの場所に移動し、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 AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs...

...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。これは、「*IM and Presence Service* でのマネージド ファイル転送の有効化」の手順で使用されます。

次のタスク

IM and Presence Service での外部ファイル サーバ インスタンスの設定 （240 ページ）

IM and Presence Service での外部ファイル サーバ インスタンスの設定

次の手順では、IM and Presence Service 上で外部ファイル サーバ インスタンスを設定する方法について説明します。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

- 外部データベースをインストールして設定します。「*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*」（リンク）を参照してください。
- IM and Presence Service での外部データベース インスタンスの設定 （233 ページ）
- 外部ファイル サーバのセットアップ （236 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 Administration] ユーザ インターフェイスにログインします。**[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）]** 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	説明
名前（Name）]	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。
ホスト/IP アドレス（Host/IP Address）	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。 （注） • [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。

フィールド	説明
外部ファイルサーバパブリックキー（External File Server Public Key）	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。 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。 `$ ssh-keyscan -t rsa host`（ファイル サーバ上で）*host* は、ファイル サーバの IP アドレス、ホスト名、または FQDN です。 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、次のようにコピーします。 extFileServer.cisco.com ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs... ...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ== （... を追加）。 **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 extFileServer が使用されている場合は、このフィールドの先頭部分は extFileServer となり、その後に rsa キー全体が続きます。
外部ファイルサーバディレクトリ（External File Server Directory）	ファイル サーバ ディレクトリ階層の最上位のパス（例：`/opt/mftFileStore/node_1/`）。
ユーザ名（User Name）	外部ファイル サーバ管理者のユーザ名。

ステップ 4 マネージド ファイル転送が有効になるクラスタの各ノードに対して 1 つの外部ファイル サーバ インスタンスを作成するために、これらの手順を繰り返してください。

ステップ 5 [保存（Save）] をクリックします。

ファイル サーバのトラブルシューティング テスト

ファイルサーバが割り当てられた後、次のテストが自動的に実行されます。これは、次の手順（IM and Presence Service でのマネージドファイル転送の有効化（243 ページ））で、マネージドファイル転送を有効にしたときに発生します。ファイル サーバが割り当てられ、Cisco XCP

File Transfer Manager サービスが開始したら、このセクションに戻ってファイル サーバへの接続に問題がないことを確認する必要があります。

[外部ファイル サーバのステータス（External File Server Status）] 領域にファイル サーバのテストと結果がリストで表示されます。

- 外部ファイルサーバの到達可能性（ping 可能性）を確認します
- 外部ファイル サーバが接続をリッスンしていることを確認します。
- 外部ファイル サーバ公開キーが正しいことを確認します。
- ノードの公開キーが外部ファイル サーバで正しく設定されていることを確認します。
- 外部ファイル サーバ ディレクトリが有効であることを確認します。
- 外部ファイル サーバが正常に配置されたことを確認します。
- ファイル サーバ上に使用可能な空きディスク領域があることを確認します。

ヒント

- 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、既存の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。また、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にRTMTはアラームを生成しますが、このアラームは、ファイル転送が発生しているかどうかとは無関係です。

次の作業

IM and Presence Service でのマネージド ファイル転送の有効化 （243 ページ）

IM and Presence Service でのマネージド ファイル転送の有効化

始める前に

マネージド ファイル転送を有効にする前に、以下のタスクを完了してください。

- 外部データベースをセットアップします。「*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*」（リンク）を参照してください。

- IM and Presence Service での外部データベース インスタンスの設定 （233 ページ）
- 外部ファイル サーバのセットアップ （236 ページ）
- IM and Presence Service での外部ファイル サーバ インスタンスの設定 （240 ページ）

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** にログインし、**[メッセージング（Messaging）] > [ファイル転送（File Transfer）]** を選択します。

ステップ 2 [ファイル転送（File Transfer）] ウィンドウの [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。

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
yc2EAAAABIwAAAQEAp2g+S2XDEzptN11S5h5nwVleKBnfG2pdW6KiLfzu/sFLegioIIqA8jBguNY/...

...5s+tusrtBBuciCkH5gfXwrsFS0O0AlfFvwnfq1xmKmIS9W2rf0Qp+A+G4MVpTxHgaonw==
imp@imp_node

（... を追加）。

（注）
- マネージドファイル転送機能が設定されいる場合、[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 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 File Transfer Manager サービスがアクティブであることを確認します。

このサービスが開始するのは、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。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 File Transfer Manager サービスがアクティブであることを確認するには、次の手順を完了します。

a) 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。
b) **[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。
c) サーバ（ノード）を選択して [移動（Go）] をクリックします。
d) [Cisco XCP File Transfer Manager] の隣のチェックボックスがオンになっており、[アクティベーションステータス（Activation Status）] が [アクティブ（Actived）] になっていることを確認します。

上記の条件が満たされていない場合は、[更新（Refresh）] をクリックします。[更新（Refresh）] をクリックしても [アクティベーションステータス（Activation Status）] が変わらない場合は、手順 8 に進みます。

e) 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、手順 c および d を繰り返します。

ステップ 8 ノードでマネージド ファイル転送機能を初めて設定している場合は、次のようにして Cisco XCP File Transfer Manager サービスを手動で開始する必要があります。

a) 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。
b) **[ツール（Tools）]** > **[コントロールセンタ - 機能の有効化（Control Center - Feature Activation）]** を選択します。
c) サーバ（ノード）を選択して [移動（Go）] をクリックします。

d) [IM and Presenceサービス（IM and Presence Services）] エリアで、[Cisco XCP File Transfer Manager] の隣にあるラジオ ボタンをクリックします。
e) [開始（Start）] をクリックします。
f) 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、手順 c ～ e を繰り返します。これは、下記の手順 9 の f) と同じです。

ステップ 9 （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。

a) ノードの [Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] ユーザ インターフェイスにログインします。
b) **[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。
c) ノードの [Cisco XCP File Transfer Manager] サービスを選択します。
d) [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）] および [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）] サービス パラメータで、必要な値（割合）を入力します。
e) **[保存（Save）]** を選択します。

ステップ 10 Cisco XCP Router サービスを再起動します。

a) 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。
b) **[ツール（Tools）] > [コントロール センタのネットワーク サービス（Control Center - Network Services）]** を選択します。
c) サーバ（ノード）を選択して [移動（Go）] をクリックします。
d) [IM and Presenceサービス（IM and Presence Services）] エリアで、[Cisco XCP Router] の隣にあるラジオ ボタンをクリックします。
e) [再起動（Restart）] をクリックします。
f) 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、手順 c ～ e を繰り返します。

ステップ 11 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：
  1. ノードの [Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] ユーザ インターフェイスにログインします。
  2. **[メッセージング（Messaging）] > [外部サーバの設定（External Server Setup）] > [外部データベース（External Databases）]** を選択します。
  3. [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。
- 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ノードで、次のようにします。
  1. ノードの [Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] ユーザ インターフェイスにログインします。

2. **[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）]** を選択します。
3. [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ます。

マネージド ファイル転送のトラブルシューティング

マネージドファイル転送が開始されない場合、またはこの機能で問題が発生する場合は、次の手順に従ってください。

1. Cisco XCP File Transfer Manager のサービス ログを確認します。IM and Presence Service のコマンドライン インターフェイス（CLI）にアクセスし、`file view activelog epas/trace/xcp/log/AFTStartup.log` コマンドを入力します。
2. Cisco RTMT プラグインがインストールされている場合は、そのトレースと syslog メッセージを確認します。

Cisco Jabber クライアントの相互運用性

ファイル転送について、いくつかの設定オプションがあります。IM and Presence Service では、次のファイル転送タイプのいずれかを設定できます。

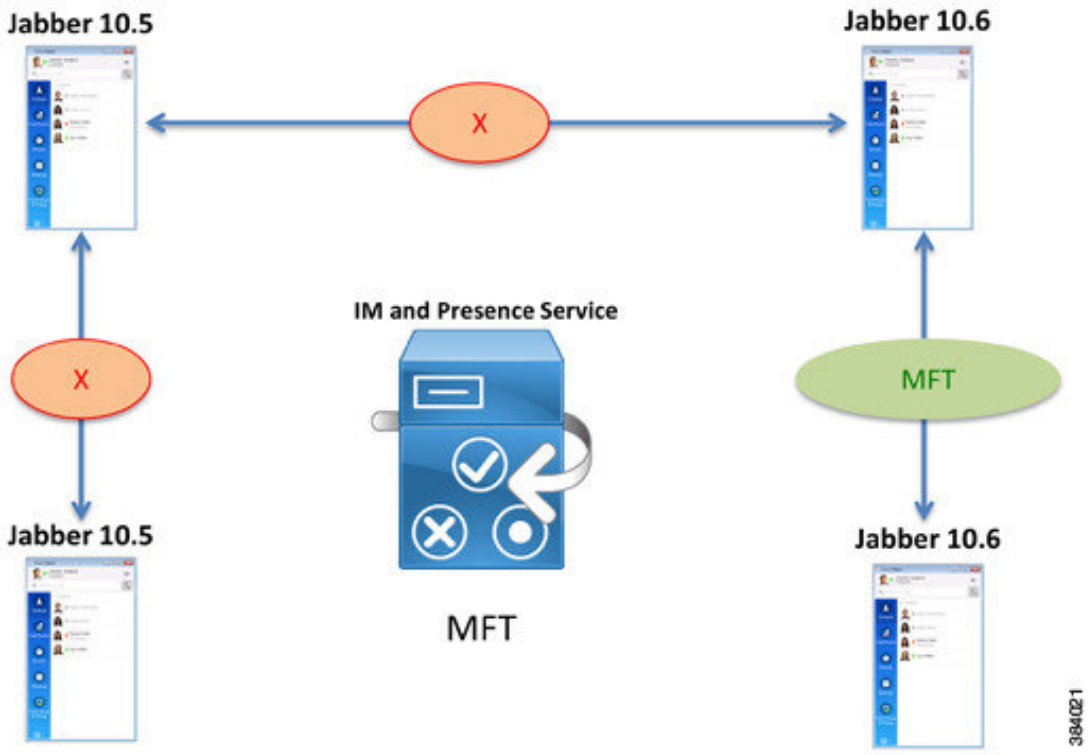
- [無効（Disabled）]：ファイル転送が許可されません。
- [ピアツーピア（Peer-to-Peer）]：1 対 1 のファイル転送は許可されますが、サーバではファイルのアーカイブや保存が行われません。グループ チャットのファイル転送はサポートされません。
- [マネージドファイル転送（Managed File Transfer）]：1 対 1 およびグループのファイル転送が許可されます。ファイル転送がデータベースのログに記録され、転送されたファイルはサーバに保存されます。クライアントがマネージドファイル転送をサポートしている必要もあります。そうでない場合、ファイル転送は許可されません。
- [マネージドおよびピアツーピアファイル転送（Managed and Peer-to-Peer File Transfer）]：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。

このセクションでは、以下のシナリオにおける Cisco Jabber 10.6 より前のクライアントまたはサードパーティ クライアントと、Cisco Jabber 10.6 以降のクライアントの間のファイル転送機能について説明します。

- 単一ノードの展開（[マネージドファイル転送（Managed File Transfer）] が有効になっている）。
- 単一ノードの展開（[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）] が有効になっている）。
- 2 ノードからなるクラスタの展開（1 つのノードでは [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）] が有効になっており、他方のノードでは [ピアツーピア（Peer-to-Peer）] が有効になっている）。
- 2 つのクラスタの展開（1 つのクラスタのノードでは [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）] が有効になっており、他方のクラスタのノードでは [ピアツーピア（Peer-to-Peer）] が有効になっている）。簡潔にするために、このシナリオでは 1 つのクラスタにつき 1 つのノードを仮定します。
- 2 クラスタ展開におけるグループ チャット（1 つのクラスタのノードで [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）] が有効になっており、他方のクラスタのノードでは [ピアツーピア（Peer-to-Peer）] が有効になっている）。簡潔にするために、このシナリオでは 1 つのクラスタにつき 1 つのノードを仮定します。

単一ノード - マネージド ファイル転送

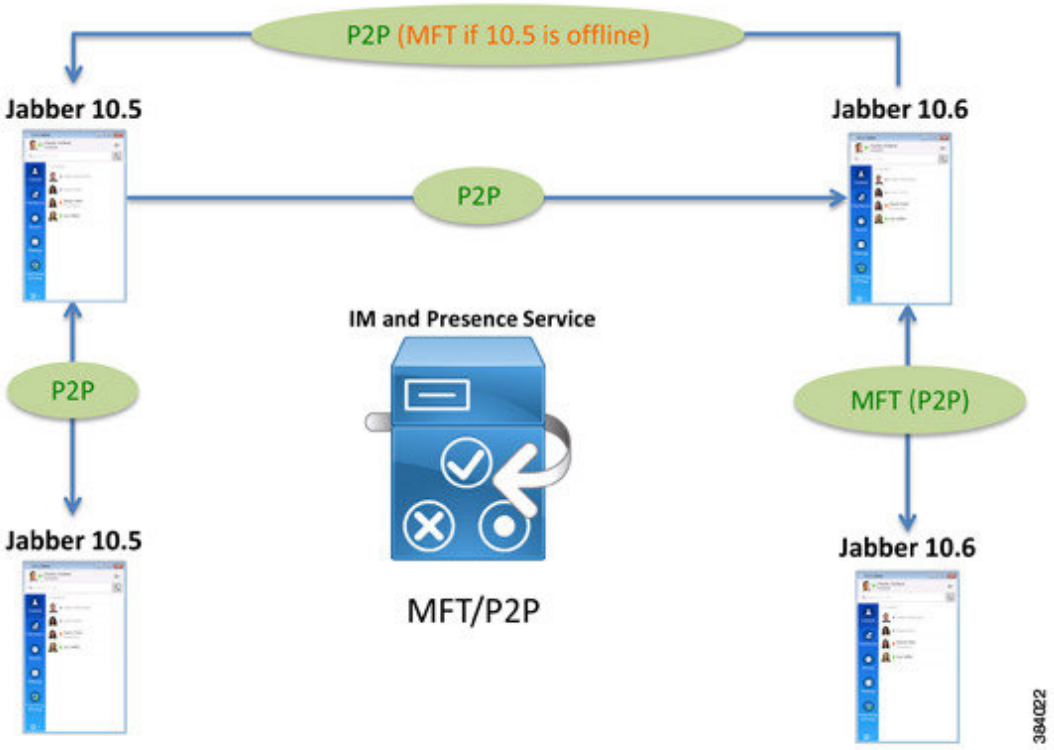
次の図は、マネージドファイル転送（MFT）が有効になっている単一の IM and Presence Service ノードを示しています。Cisco Jabber リリース 10.5 クライアントおよび Cisco Jabber リリース 10.6 クライアントが IM and Presence Service ノードに登録されています。



この展開モデルでは、マネージド ファイル転送は Cisco Jabber リリース 10.6 クライアント間でのみサポートされます。ピアツーピア ファイル転送は、クライアント リリースに関係なく、許可されていません。

単一ノード - マネージドおよびピアツーピア ファイル転送

次の図は、**マネージドおよびピアツーピア ファイル転送**（MFT/P2P）ノードが有効になっている単一の IM and Presence Service ノードを示しています。Cisco Jabber リリース 10.5 クライアントおよび Cisco Jabber リリース 10.6 クライアントが IM and Presence Service ノードに登録されています。

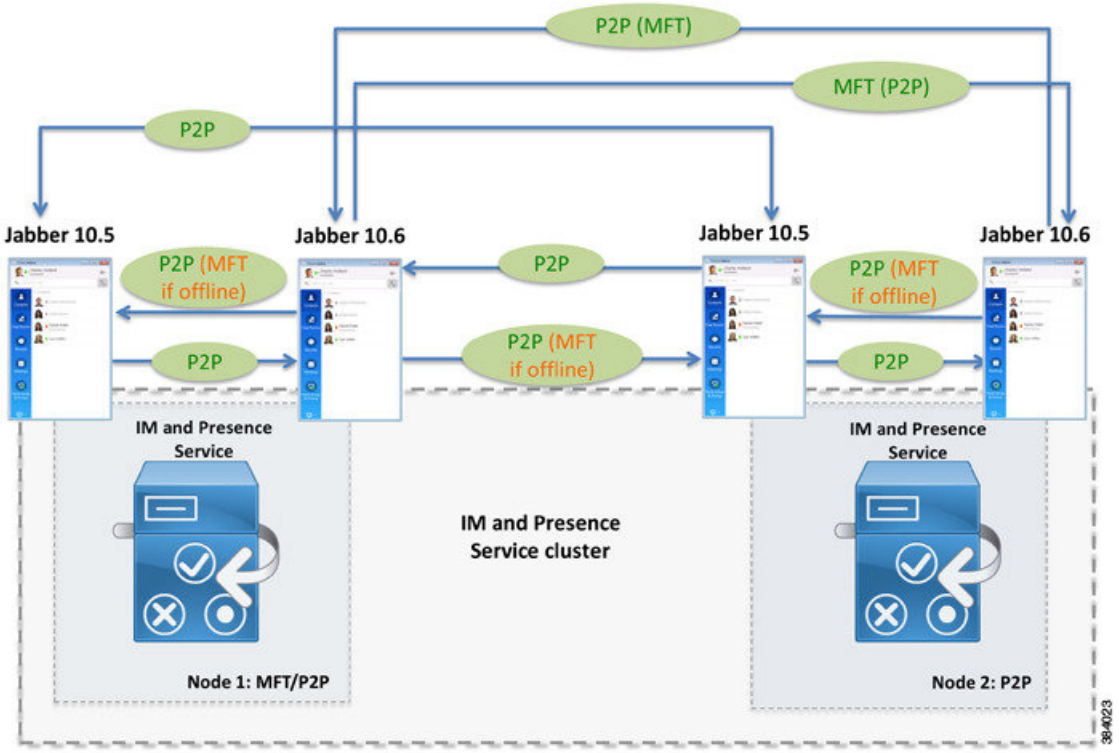


この展開モデルではファイル転送が許可されており、次のようにクライアントに応じてマネージド ファイル転送またはピアツーピアファイル転送のいずれかとして扱われます。

- Cisco Jabber 10.5 クライアント間のファイル転送は、ピアツーピア転送として処理されます。
- Cisco Jabber 10.6 クライアント間のファイル転送は、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よう設定されている場合、マネージドファイル転送として処理されます。ただし、ファイル転送をピアツーピア転送として処理するよう、クライアントの設定を変更することができます。
- Cisco Jabber 10.5 クライアントが Cisco Jabber 10.6 クライアントへファイルを送信すると、ピアツーピア ファイル転送として処理されます。
- Cisco Jabber 10.6 クライアントが Cisco Jabber 10.5 クライアントへファイルを送信した場合は、デフォルトのクライアント プリファレンスがピアツーピアで、Cisco Jabber 10.5 クライアントがオンラインであれば、ピアツーピア ファイル転送として処理されます。10.5 クライアントがオフラインの場合、ファイル転送はマネージドファイル転送として処理されますが、10.5 クライアントはこのファイルを受信できません。

単一クラスタ - 混合ノード

次の図は、2 つの IM and Presence Service ノードを含むクラスタを示しています。ノード 1 ではマネージドおよびピアツーピアファイル転送（MFT/P2P）が有効で、ノード 2 ではピアツーピア（P2P）が有効になっています。これらの両方のノードに、Cisco Jabber リリース 10.5 クライアントと Cisco Jabber リリース 10.6 クライアントが登録されています。



この展開モデルではファイル転送が許可されており、クライアントに応じてマネージドファイル転送またはピアツーピアファイル転送のいずれかとして扱われます。さまざまなファイル転送の動作を理解するには、次の凡例を参照してください。

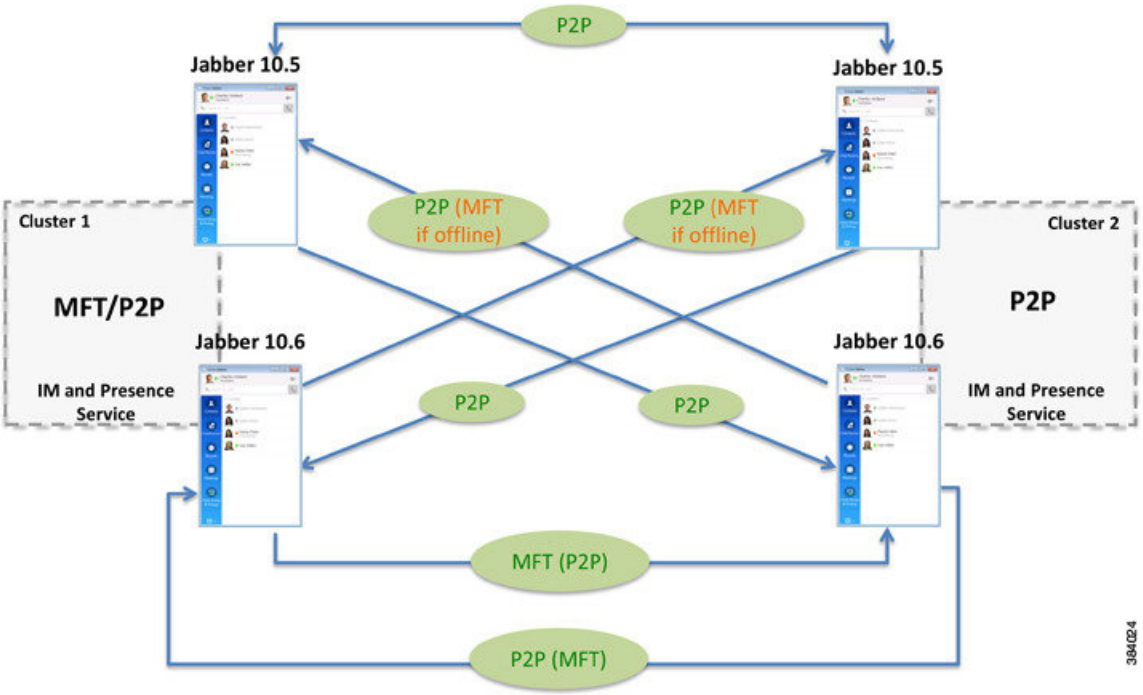
- P2P：ファイル転送はピアツーピア ファイル転送として処理されます。
- MFT（P2P）：マネージドファイル転送が、デフォルトのクライアントプリファレンスです。ただしピアツーピアファイル転送を使用するようにクライアントを設定し直すことができます。
- P2P（MFT）：ピアツーピアがデフォルトのクライアントプリファレンスです。ただし、マネージド ファイル転送を使用するようにクライアントを設定し直すことができます。

- P2P（オフラインの場合はMFT）：ピアツーピアがデフォルトのクライアントプリファレンスで、受信者はオンラインです。受信者がオフラインの場合は、送信者によってマネージド ファイル転送として処理されますが、受信者はそれを受信できません。

（注） [マネージド ファイル転送（Managed File Transfer）]が有効になっているノードを、[ピアツーピア（Peer-to-Peer）]が有効になっているノードを含むクラスタに展開しないでください。 推奨される移行パスは、[ピアツーピア（Peer-to-Peer）] ノードをマネージドおよび [ピアツーピア（Peer-to-Peer）] ファイル転送ノードとして設定した後、それらのノードを[マネージド ファイル転送（Managed File Transfer）] ノードに変更することです。

複数のクラスタ - 混合ノード

次の図は、2 つのクラスタを含む展開を示しています。クラスタ 1 のノードでは [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）]（MFT）が有効になっていて、クラスタ 2 のノードでは [ピアツーピア（Peer-to-Peer）]（P2P） が有効になっています。これらの両方のノードに、Cisco Jabber リリース 10.5 クライアントと Cisco Jabber リリース 10.6 クライアントが登録されています。

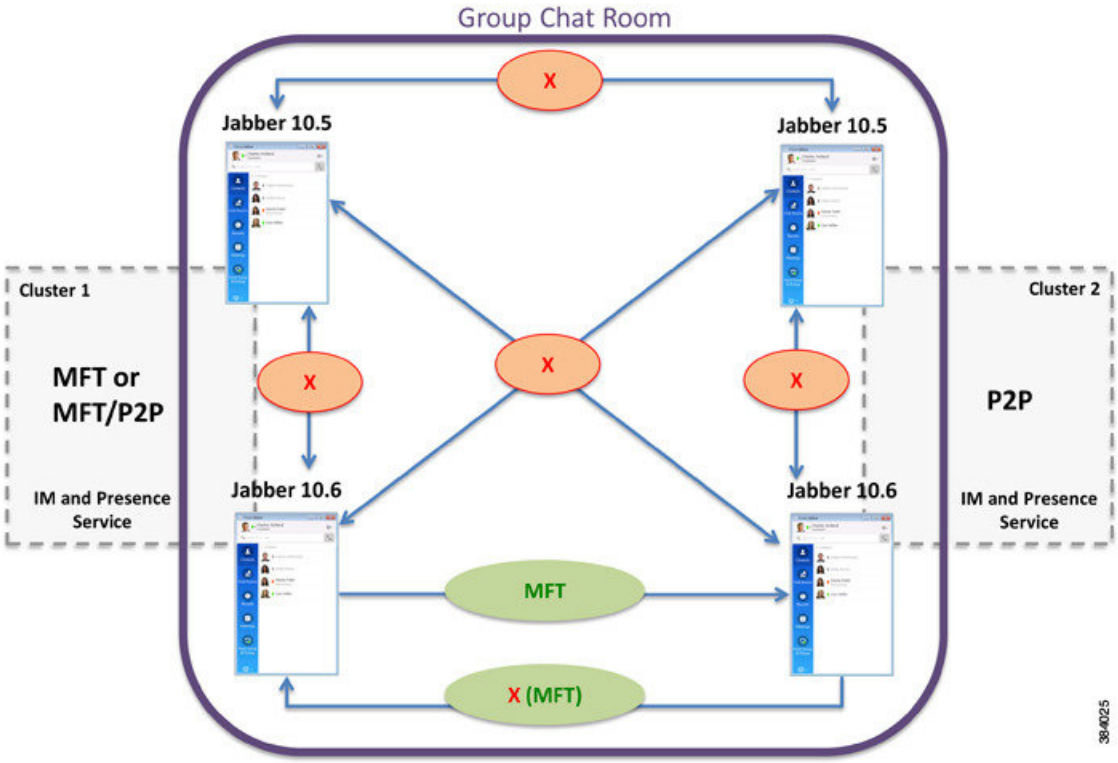


この展開モデルではファイル転送が許可されており、クライアントに応じてマネージドファイル転送またはピアツーピアファイル転送のいずれかとして扱われます。さまざまなファイル転送の動作を理解するには、次の凡例を参照してください。

- P2P：ファイル転送はピアツーピア ファイル転送として処理されます。
- MFT（P2P）：マネージドファイル転送が、デフォルトのクライアントプリファレンスです。ただしピアツーピア ファイル転送を使用するようにクライアントを設定し直すことができます。
- P2P（MFT）：ピアツーピアがデフォルトのクライアントプリファレンスです。ただし、マネージド ファイル転送を使用するようにクライアントを設定し直すことができます。
- P2P（オフラインの場合はMFT）：ピアツーピアがデフォルトのクライアントプリファレンスで、受信者はオンラインです。受信者がオフラインの場合は、送信者によってマネージド ファイル転送として処理されますが、受信者はそれを受信できません。

グループ チャット

次の図は、2 つのクラスタ間のグループ チャットのシナリオを表しています。クラスタ 1 のノードでは、**マネージドファイル転送**（MFT）または **マネージドおよびピアツーピアファイル転送**（MFT/P2P）が有効で、クラスタ 2 のノードでは、**ピアツーピア**（P2P）が有効になっています。これらの両方のノードに、Cisco Jabber リリース 10.5 クライアントと Cisco Jabber リリース 10.6 クライアントが登録されています。



このシナリオでは、マネージドファイル転送は Cisco Jabber リリース 10.6 クライアント間でのみサポートされています。ピアツーピア ファイル転送は、クライアント リリースに関係なく、許可されていません。さまざまなファイル転送の動作を理解するには、次の凡例を参照してください。

- MFT：マネージドファイル転送がサポートされ、ファイルのアップロードとすべてのファイルダウンロードには、受信者のホームがどのノードにあるかに関係なく、送信者のホーム ノードの外部ファイル サーバが使用されます。
- X（MFT）：クライアントのデフォルト設定では、ファイル転送がまったく許可されません。ただし、マネージドファイル転送をサポートするようにクライアントを設定し直すことができます。

Jabber クライアント用のモバイルおよびリモート アクセス

オンプレミス展開の場合、モバイルおよびリモートアクセス クライアントでサポートされる唯一のファイル転送オプションは、マネージド ファイル転送です。マネージド ファイル転送または MRA を使用するには、IM and Presence Service の制限付きバージョンを実行している必要があります。制限されていないバージョンの IM and Presence Service を実行している場合は、MRA 上でマネージド ファイル転送が機能しません。

モバイルおよびリモートアクセスの詳細については、このリンクを参照してください。
http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html

第 16 章

Multiple Device Messaging

- Multiple Device Messaging の概要 （257 ページ）
- Multiple Device Messaging の有効化 （259 ページ）
- 複数のデバイスのメッセージングのカウンタ （260 ページ）
- Multiple Device Messaging のインタラクションと制限 （260 ページ）

Multiple Device Messaging の概要

Multiple Device Messaging（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。

たとえばデスクトップ コンピュータから IM 交換を開始しても、デスクから移動した後はモバイル デバイスで交換を続けることができます。Multiple Device Messaging のフロー （258 ページ）を参照してください。

MDM は、モバイル デバイスのバッテリ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。

MDM は、Cisco XCP Message Archiver サービスなどの、MDM をサポートしていないサードパーティ クライアントとの互換性があります。

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。

次の制限が適用されます。

- クライアントはサインインしている必要があります。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。
- ファイル転送は、ファイルを送受信したアクティブ デバイスでのみ使用できます。
- 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。

- MDM は、バージョン X8.8 以前の Cisco Expressway 経由でクラウドから IM and Presence Service に接続するクライアントではサポートされません。

MDM の操作方法の詳細については、次の 2 つのフローを参照してください。

Multiple Device Messaging のフロー

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斉送信されます。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。

Multiple Device Messaging における静音モードのフロー

このフローでは、モバイル デバイス上で Multiple Device Messaging 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。

Multiple Device Messaging の有効化

Multiple Device Messaging はデフォルトで有効になっています。次の手順を使用して、この機能を有効または無効にすることができます。

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 Router（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 メッセージングの有効化（Enable Multi-Device Messaging）] ドロップダウンリストから [有効（Enabled）] または [無効（Disabled）] 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。

複数のデバイスのメッセージングのカウンタ

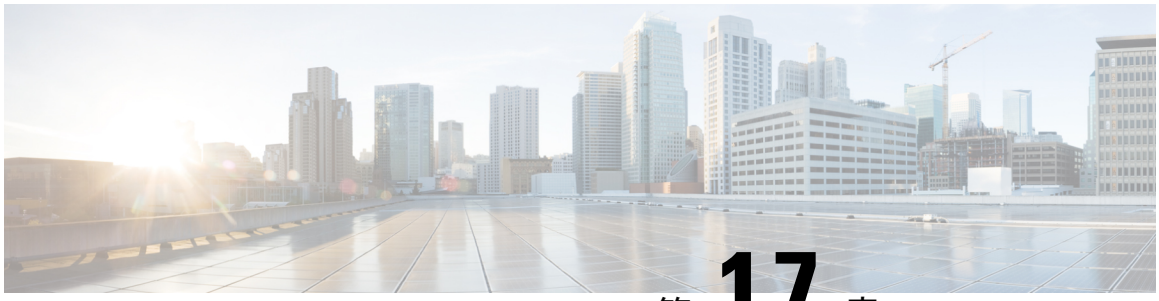
Multiple Device Messaging（MDM）は、Cisco XCP MDM カウンタ グループから次のカウンタを使用します。

表 *25 :* カウンタ グループ：*Cisco XCP MDM* カウンタ

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）。

Multiple Device Messaging のインタラクションと制限

機能	データのやり取り
Server Recovery Manager	フェールオーバーが発生した場合、Multiple Device Messaging 機能により、IM and Presence Service でサーバ回復に遅延が発生します。Multiple Device Messaging 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、フェールオーバーの時間は通常、**Cisco Server Recovery Manager** サービス パラメータで指定された時間の 2 倍になります。



第 17 章

iPhone および iPad での Cisco Jabber のプッシュ通知の設定

- プッシュ通知の概要 （261 ページ）
- プッシュ通知の設定 （264 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と、Cisco Unified Communications Manager と IM and Presence Service は、Apple のクラウドベースのプッシュ通知サービスを使用して、音声コール、ビデオ コール、インスタント メッセージ通知、および Cisco Webex 招待状を、保留モードで実行されている iPhone および iPad 版 Cisco Jabber クライアントにプッシュします。プッシュ通知を使用すると、システムは Cisco Jabber と永続的な通信を維持することができます。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 Cisco Jabber for iPhone and iPad クライアントと、Expressway のモバイルおよびリモート アクセス（MRA）機能を使用してオンプレミス展開に登録しているクライアントの両方に必要です。

（注） プッシュ通知は、Cisco Jabber for iPhone and iPad クライアントにのみ必要です。この機能は Android ではサポートされておらず、Windows および Mac ユーザには適用されません。

プッシュ通知の仕組み

起動時に、iPhone および iPad デバイスにインストールされている Cisco Jabber クライアントは、Cisco Unified Communications Manager、IM and Presence Service 、および Apple クラウドに登録されます。MRA の導入により、Cisco Jabber for iPhone または iPad のクライアントは、Expressway 経由でオンプレミス サーバに登録されます。Jabber クライアントがフォアグラウンド モードのままであれば、Cisco Unified Communications Manager と IM and Presence Service は Jabber クライアントにコールとインスタント メッセージを直接送信できます。

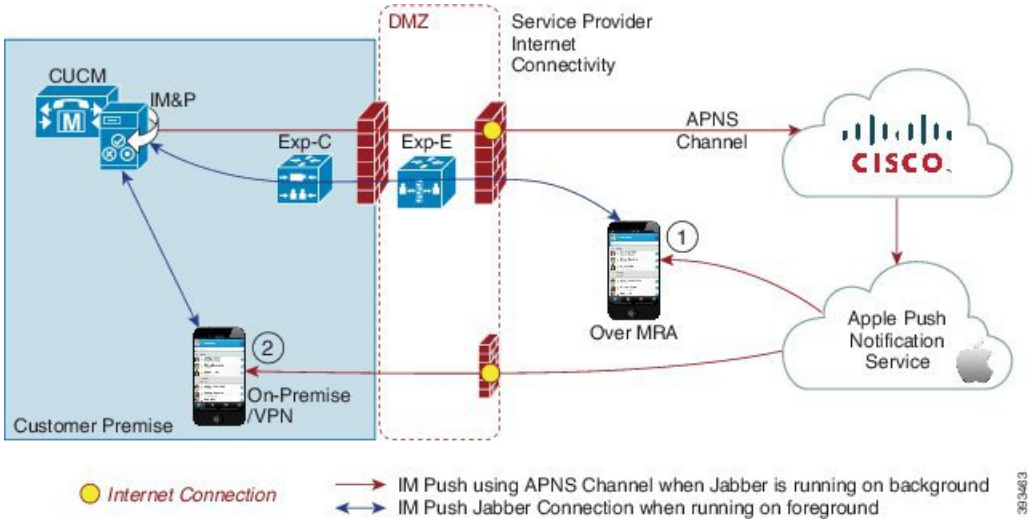
ただし、Cisco Jabber クライアントが保留モードに移行すると、標準の通信チャネルは使用できなくなり、Cisco Unified Communications Manager と IM and Presence Service はクライアントと

直接通信することができなくなります。プッシュ通知は、Cisco と Apple のクラウドを介して Jabber クライアントに到達するための別のチャネルを提供します。

（注） 次のいずれかの条件が当てはまる場合、Cisco Jabber は保留モードで動作しているとみなされます。

- Cisco Jabber 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
- iPhone または iPad がロックされている
- iPhone または iPad の画面がオフになっている

図 *16 : iPhone* および *iPad* 版 *Cisco Jabber* のプッシュ通知アーキテクチャ



上記の図は、iPhone および iPad 版 Cisco Jabber クライアントがバックグラウンドで実行されているか、または停止しているときにどうなるかを示しています。この図には、（1）Cisco Jabber 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 の展開に接続している MRA 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 Cisco Jabber for iPhone または iPad のクライアントが示されています。

それぞれの使用例で起こることの詳細については、次の表を参照してください。

表 *26 :* プッシュ通知が有効な場合の *Cisco Jabber for iPhone and iPad* のメッセージ フロー

Jabberクライアントの実行モード	Cisco Unified Communications Manager と IM and Presence Service によるプッシュ通知の送信先
フォアグラウンド モード	音声、ビデオ、IM and Presence には標準的な通信チャネルが使用されます。 • オンプレミスのモバイル クライアントの場合、Cisco Unified Communications Manager と IM and Presence Service は、コールまたはインスタント メッセージを Jabber クライアントに直接送信します。 • MRA クライアントの場合、コールまたは IM 通知は、Expressway 経由で Jabber クライアントに送信されます。 （注） 音声コールおよびビデオ コールの場合、プッシュ通知は引き続きプッシュ通知チャネルを介して送信されますが、Cisco Jabber クライアントは標準チャネルを使用します。
保留モード	**音声コールまたはビデオ コール** 標準的な通信チャンネルは使用できません。Cisco Unified Communications Manager は、プッシュ通知チャネルを使用します。 通知を受信すると、Jabber クライアントは自動的に再びフォアグラウンド モードに戻り、クライアントが呼び出し音を鳴らします。 **インスタント メッセージ** 標準的な通信チャンネルは使用できません。IM and Presence Service はプッシュ通知チャネルを使用して、次のように IM 通知を送信します。 1. IM and Presence Service 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 IM 通知を Jabber クライアントにプッシュし、Jabber 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、Jabber クライアントはフォアグラウンドに戻ります。Jabber 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。 （注） Cisco Jabber クライアントが保留モードの間、ユーザのプレゼンス ステータスは [退席中（Away）] と表示されます。

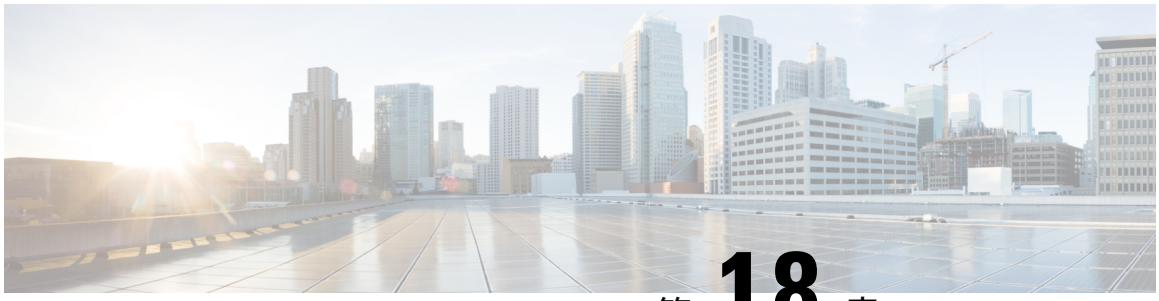
プッシュ通知の設定

プッシュ通知の設定および導入の方法の詳細は、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『iPhone および iPad での Cisco Jabber のプッシュ通知の導入』を参照してください。

第 IV 部

管理

- チャットの設定と管理 （267 ページ）
- エンド ユーザの設定と処理 （295 ページ）
- ユーザの移行 （317 ページ）
- ユーザの中央展開への移動 （325 ページ）
- IM and Presence Service の多言語サポート設定 （343 ページ）
- ブランディングのカスタマイズ （351 ページ）



第 18 章

チャットの設定と管理

- チャットの展開 （267 ページ）
- チャット管理の設定 （270 ページ）
- チャット ノード エイリアスの管理 （277 ページ）
- チャット ルーム管理 （283 ページ）
- グループ チャットと常設チャットのインタラクションと制限 （289 ページ）

チャットの展開

異なる展開シナリオに合わせてチャットを設定できます。展開シナリオの例を使用できます。

チャットの展開シナリオ 1

展開シナリオ：	チャット ノードのエイリアスにクラスタ ID を含めません。システムで生成されたエイリアス `conference-1-mycup.cisco.com` ではなく、エイリアス `primary-conf-server.cisco.com` を使用します。
設定手順：	**1.** **[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）]** を選択して、システムで生成されたエイリアスをオフにします（これはデフォルトでオンになっています）。 **2.** エイリアスを編集し、`primary-conf-server.cisco.com` に変更します。
（注）	システムで生成された古いエイリアスをオフにすると、`conference-1-mycup.cisco.com` は、[グループチャットサーバのエイリアス （Group Chat Server Alias）] の下に表示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。

チャットの展開シナリオ 2

展開シナリオ：	目的： • ドメインを cisco.com から linksys.com に変更し、conference-1-mycup.cisco.com ではなく、conference-1-mycup.linksys.com を使用します。 • ユーザがまだ xxx@conference-1-mycup.cisco.com というタイプの古いチャットルームを検索できるように、データベース内の既存の常設チャットルームのアドレスを維持します。
設定手順：	1. **Cisco Unified CM IM and Presence Administration** にログインして、**[プレゼンス（Presence）] > [トポロジの設定（Settings Topology）] > [詳細設定（Advanced Configuration）]** を選択します。 2. デフォルトの IM and Presence Service ドメインの編集方法の詳細については、関連するトピックを参照してください。
（注）	ドメインを変更すると、完全修飾クラスタ名（FQDN）が conference-1-mycup.cisco.com から conference-1-mycup.linksys.com に自動的に変更されます。システムで生成された古いエイリアス conference-1-mycup.cisco.com は、[グループ チャット サーバのエイリアス（Group Chat Server Aliases）] の下に表示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。

関連トピック

IM and Presence Service のデフォルト ドメインの設定

チャットの展開シナリオ 3

展開シナリオ：	目的： • mycup から ireland にクラスタ ID を変更し、conference-1-mycup.cisco.com ではなく、conference-1-ireland.cisco.com を使用します。 • データベース内の既存の常設チャットルームのアドレスを維持する必要はありません。
設定手順：	1. **[Cisco Unified CM IM and Presence の管理 （Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）]** を選択します。 2. クラスタ ID を編集し、ireland に変更します。 3. **[メッセージング（Messaging）] > [グループ チャット サーバ エイリアスのマッピング（Group Chat Server Alias Mapping）]** を選択します。

	4. 古いエイリアス conference-1-mycup.cisco.com を削除します。
（注）	クラスタ ID を変更すると、完全修飾クラスタ名（FQDN）が conference-1-mycup.cisco.com から conference-1-ireland.cisco.com に自動的に変更されます。システムで生成された古いエイリアス conference-1-mycup.cisco.com は、[グループ チャット サーバ エイリアス（Group Chat Server Aliases）] の下に表示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。（この例では）管理者は古いエイリアス アドレスを維持する必要がないため、これを削除するのが適切です。

チャットの展開シナリオ 4

展開シナリオ：	目的： • 既存のエイリアスに関連付けられたノード（たとえば、conference-3-mycup.cisco.com）をシステム トポロジから削除します。 • 新しいノード ID（ノード ID：7）を持つ新しいノード（たとえば、conference-7-mycup.cisco.com）をシステム トポロジに追加します。 • 古いエイリアスを使用して作成されたチャット ルームのアドレスを維持します。
設定手順：	オプション 1 **1.** **[Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] > [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。 **2.** [新規追加（Add New）] を選択して、追加エイリアス conference-3-mycup.cisco.com を追加します。 オプション 2 **1.** **[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、システムで生成されたデフォルト エイリアス conference-7-mycup.cisco.com をオフにします（これはデフォルトでオンになっています）。 **2.** エイリアスを編集し、conference-3-mycup.cisco.com に変更します。
（注）	システム トポロジに新しいノードを追加すると、システムはノードに自動的にこのエイリアス（conference-7-mycup.cisco.com）を割り当てます。 オプション 1

	• 追加エイリアスを追加すると、ノードは両方のエイリアス（conference-7-mycup.cisco.com と conference-3-mycup.cisco.com）によってアドレス指定可能です。 オプション 2 • システムで生成された古いエイリアスをオフにすると、conference-7-mycup.cisco.com は、[グループ チャット サーバのエイリアス（Group Chat Server Alias）] の下に表示される標準の編集可能なエイリアスに戻ります。

チャット管理の設定

IM ゲートウェイ設定の変更

IM and Presence Service の IM ゲートウェイを設定できます。

IM and Presence Service の IM Gateway の SIP ツー XMPP 接続（SIP-to-XMPP connection）はデフォルトで有効です。SIP と XMPP クライアント間の IM の相互運用性を実現することで、SIP IM クライアントのユーザが XMPP IM クライアントのユーザと二方向 IM を交換できるようになります。IM ゲートウェイ ステータス パラメータをオンにしておくことを推奨します。ただし、XMPP と SIP クライアントの相互通信を防ぐために、IM ゲートウェイ ステータス パラメータをオフにすることもできます。

IM会話のデフォルトの非アクティブタイムアウト間隔も変更でき、IMが送信に失敗した場合に表示されるエラー メッセージも選択できます。

制約事項

SIP クライアントは、XMPP 固有の機能であるチャット ルームに参加できません。

手順

ステップ 1 **[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 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウでサービスとして [Cisco SIP Proxy（Cisco SIP Proxy）] を選択します。

ステップ 4 次のいずれか 1 つの処理を実行します。

a) この機能を有効にするために、[SIP XMPP IMゲートウェイ（クラスタ全体）（SIP XMPP IM Gateway（Clusterwide））] セクションの [IMゲートウェイステータス（IM Gateway Status）] を [オン（ON）] に設定します。

b) この機能を無効にするために、[SIP XMPP IM ゲートウェイ（クラスタ全体）（SIP XMPP IM Gateway（Clusterwide））] セクションの [IM ゲートウェイ ステータス（IM Gateway Status）] を [オフ（Off）] に設定します。

ステップ 5 ゲートウェイによって維持される IM 会話の非アクティブなタイムアウト間隔（秒単位）を設定します。ほとんどの環境に適したデフォルト設定は 600 秒です。

ステップ 6 IM が配信に失敗した場合に、ユーザに表示するエラー メッセージを指定します。デフォルトのエラー メッセージは「Your IM could not be delivered（IM を配信できませんでした）」です。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

常設チャット ルームの設定に進みます。

サインイン セッション数の制限

管理者は Cisco XCP Router のユーザごとのサインイン セッションの数を制限できます。このパラメータは、XMPP クライアントのみに適用されます。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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）] メニューから [IM and Presence Service（IM and Presence Service）] ノードを選択します。

ステップ 3 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウでサービスとして [Cisco XCP Router（Cisco XCP Router）] を選択します。

ステップ 4 [XCP Manager 設定パラメータ（クラスタ全体）（XCP Manager Configuration Parameters（Clusterwide））] 領域の [ユーザごとのログオン セッションの最大数（Maximum number of logon sessions per user）] にパラメータ値を入力します。

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。

関連トピック

Cisco XCP Router サービスの再起動 （88 ページ）

常設チャット ルームの設定

一時的な（アドホック）チャット ルームではなく常設チャット ルームを使用する場合にのみ常設チャットの設定を行う必要があります。この設定は、常設チャットに固有で、法規制の遵守のための IM アーカイブに影響しません。

制約事項

SIP クライアントは、XMPP 固有の機能であるチャット ルームに参加できません。

始める前に

- 常設チャット ルームを使用するには、ノードごと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。
- 常設チャットのロギングに外部データベースを使用する場合は、データベースのサイズを考慮します。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、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。大規模な展開では、ディスク領域はただちに消費される可能性があります。データベースを、情報の量を処理するのに十分な大きさにしてください。
- 外部データベースへの接続数を設定する前に、オフラインで書き込む 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。UI 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。
- 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。Cisco 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。

手順

ステップ 1 **[Cisco Unified Communications Manager IM and Presenceの管理（Cisco IM and Presence Administration）]>[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 2 [常設チャットの有効化（Enable Persistent Chat）] をオンにします。

（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常設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 クラスタ上のユーザは、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ルームを検出できます。

ステップ 3 （任意） チャット ルーム メッセージの保存方法を必要に応じて指定します。

a) ルームに送信されたすべてのメッセージをアーカイブする場合は、[すべてのルーム メッセージのアーカイブ（Archive all room messages）] をオンにします。これはすべての常設チャット ルームに適用されるクラスタ全体の設定です。
b) 要求を処理するために使用するデータベースへの接続の数を入力します。これは、チャット ノードと関連するデータベース間のすべての接続に適用されるクラスタ全体の設定です。
c) データベース接続を何秒後に更新するかを入力します。これは、チャット ノードと関連するデータベース間のすべての接続に適用されるクラスタ全体の設定です。

ステップ 4 事前設定された外部データベースのリストから選択し、チャット ノードに適切なデータベースを割り当てます。

ヒント [クラスタ トポロジの詳細（Cluster Topology Details）] ウィンドウでチャット ノードの詳細を編集する必要がある場合は、ハイパーリンクをクリックします。

ステップ 5 Cisco Jabber を導入する場合は、[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）] チェックボックスをオフのままにします。いずれかのオプションが選択されていると、Cisco Jabber でのチャットは失敗します。

ステップ 6 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 Serviceability（Cisco Unified IM and Presence Serviceability）] > [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。

- [ルーム内のすべてのメッセージをアーカイブ（Archive all messages in a room）] 設定をオンにする場合は、常設チャットに使用する各外部データベースのパフォーマンスをモニタすることを推奨します。データベース サーバで負荷が高くなることを予測する必要があります。
- 常設チャット ルームを有効にし、外部データベースとの適切な接続を確立しない場合、TC サービスはシャットダウンします。このような状況では、すべてのチャット ルームの機能（一時的および常設の両方）が失われます。チャット ノードが接続を確立すると（他のチャット ノードが失敗しても）、そのノードは起動します。

次のタスク

[Cisco XCP テキスト会議マネージャ（Cisco XCP Text Conference Manager）] をオンに設定します。

関連トピック

IM ゲートウェイ設定の変更 （270 ページ）
チャット ノード エイリアスの管理 （277 ページ）

常設チャットの有効化

一時的な（アドホック）チャットルームではなく常設チャットルームを使用する場合にのみ、常設（パーシステント）チャットの設定を行います。この設定は、常設チャットに固有で、法規制の遵守のための IM アーカイブに影響しません。

始める前に

- 常設チャット ルームを使用するには、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。

重要 各ノードに外部データベースを割り当てておく必要があります。

- Oracle外部データベースを使用している場合は、既知のOracleの欠陥：ORA-22275のパッチを更新する必要があります。これが行われないと、常設チャットルームが正常に動作しません。
- 常設チャットのロギングに外部データベースを使用する場合は、データベースのサイズを考慮します。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、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。大規模な展開では、ディスク領域はただちに消費される可能性があります。データベースを、情報の量を処理するのに十分な大きさにしてください。
- ルームの入退室をすべてアーカイブすると、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。
- 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。UI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。
- 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。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。

手順

ステップ1 **[Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）]>[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2 [常設チャットの有効化（Enable Persistent Chat）]チェックボックスをオンにします。

ステップ3 （任意） ルームに入退室するユーザのすべてのインスタンスをログに記録するには、[すべてのルームの参加および終了をアーカイブ（Archive all room joins and exits）]チェック ボックスをオンにします。これはすべての常設チャットルームに適用されるクラスタ全体の設定です。

ステップ4 （任意）ルームに送信されたすべてのメッセージをアーカイブするには、[すべてのルームメッセージのアーカイブ（Archive all room messages）]チェック ボックスをオンにします。これはすべての常設チャット ルームに適用されるクラスタ全体の設定です。

ステップ5 （任意） グループ チャット システム管理者だけが常設（永続的）チャット ルームを作成できるようにするには、[グループチャットのシステム管理者のみの常設チャットルームの作成を許可する（Allow only group chat system administrators to create persistent chat rooms）]チェックボックスをオンにします。これはすべての常設チャットルームに適用されるクラスタ全体の設定です。

グループ チャット システムの管理者を設定するには、**[メッセージング（Messaging）]>[グループ チャット システム管理者（Group chat system administrators）]**を選択します。

ステップ 6 常設チャット ルームの許容最大数を [許可された常設チャットルームの最大数（Maximum number of persistent chat rooms allowed）] フィールドに入力します。デフォルト値は 1500 に設定されています。

重要 外部データベースに十分な容量があることを確認する必要があります。多くのチャット ルームを所有すると、外部データベースのリソースに影響を及ぼします。

ステップ 7 要求の処理に使用するデータベースへの接続数を [データベースへの接続数（Number of connections to the database）] フィールドに入力します。デフォルトでは 5 に設定されています。これは、チャット ノードと関連するデータベース間のすべての接続に適用されるクラスタ全体の設定です。

ステップ 8 データベース接続を更新するまでの秒数を [データベース接続ハートビート間隔（秒）（Database connection heartbeat interval (seconds)）] フィールドに入力します。デフォルトでは 300 に設定されています。これは、チャット ノードと関連するデータベース間のすべての接続に適用されるクラスタ全体の設定です。

ステップ 9 チャット ルームをタイムアウトにするまでの分数を [常設チャット ルームのタイムアウト値（分）（Timeout value for persistent chat rooms (minutes)）] フィールドに入力します。デフォルトでは 0 に設定されています。タイムアウトを使用して、チャット ルームがアイドルか空かを確認します。ルームがアイドルまたは空であると判明した場合は、そのルームは閉じられます。デフォルト値が 0 に設定されている場合は、アイドル チェックが無効になります。

ステップ 10 事前設定された外部データベースのリストから選択し、チャット ノードに適切なデータベースを割り当てます。

- [ルームのすべての入退室をアーカイブ（Archive all room joins and exits）] 設定をオンにした場合は、常設チャット ルームに使用されている各外部データベースのパフォーマンスを監視することを推奨します。データベース サーバの負荷が高くなると考えられます。
- [すべてのルーム メッセージをアーカイブ（Archive all room messages）] 設定をオンにした場合は、常設チャット ルームに使用されている各外部データベースのパフォーマンスを監視することを推奨します。データベース サーバの負荷が高くなると考えられます。
- 常設チャット ルームを有効にし、外部データベースとの適切な接続を確立しない場合、チャット ノードは失敗します。このような状況では、すべてのチャット ルームの機能（一時的および常設の両方）が失われます。チャット ノードが接続を確立すると（他のチャット ノードが失敗しても）、そのノードは起動します。
- [クラスタ トポロジの詳細（Cluster Topology Details）] ウィンドウで Cisco Unified Communications Manager の IM and Presence Service ノードの詳細を編集するには、ハイパーリンクをクリックします。

ステップ 11 [保存（Save）] をクリックします。

ステップ 12 **[Cisco Unified CM 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 - ネットワーク サービス（Control Center - Network Services）]** を選択して、クラスタ内のすべてのノードの Cisco XCP Router を再起動します。

次の点に注意してください。

- Cisco XCP Text Conference Manager サービスがすでに実行されていた場合は、Cisco XCP Router を再起動すると、それも自動的に再起動します。
- Cisco XCP Text Conference Manager サービスがまだ実行されていなかった場合は、Cisco XCP Router が再起動した後にそれを手動で開始する必要があります。Cisco XCP Text Conference Manager サービスを開始するには、**[Cisco Unified CM 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 - 機能サービス（Control Center - Feature Services）]** を選択します。

（注） 常設チャットを有効にした後で、引き続き常設チャットの設定を更新する場合は、次の非動的設定にのみ、Cisco XCP Text Conference Manager の再起動が必要になります。

- 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）

関連トピック

Cisco XCP Text Conference Manager サービスの再起動

グループ チャット システム管理の設定

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 Routerを再起動する必要があります。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 ニックネームを入力します。

ステップ 6 説明を入力します。

ステップ 7 [保存（Save）] をクリックします。

グループ チャットと常設チャットのデフォルト設定と復帰

強化されたデフォルトのアドホックと常設チャットの設定を変更できます。すべての設定をデフォルト値に戻すには、[デフォルトに設定（Set to Default）] をクリックします。

（注） チャット ルームの所有者が設定を変更できるようにするには、ノードで [ルーム所有者が変更できる（Room owners can change）] チェック ボックスを選択します。ルームの所有者は、希望する設定や、作成しているルームに適用可能な設定を行えるようになります。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。

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

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。

（注） このチャット ノードのエイリアス（たとえば、conference-3-mycup.cisco.com）は、そのノードで作成された各チャット ルームの一意の ID 部分になります（roomjid@conference-3-mycup.cisco.com）。

次の方法で、クラスタ全体にエイリアスを割り当てることができます。

- システム生成：システムは一意のエイリアスを各チャット ノードに自動的に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を有効にする場合、チャット ノードに対処するためにさらに実行することはありません。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：ハードコードされたキーワード
  - x：ノード ID を示す一意の整数値
  - 例：conference-3-mycup.cisco.com
- 手動：conference-x-clusterid.domain の命名規則が適さない場合、たとえば、チャット ノードのエイリアスにクラスタ ID を含めない場合は、システムで生成されたデフォルトのエイリアスを上書きすることもできます。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。

- 追加エイリアス：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。これは、システムによって生成されるエイリアスを割り当てるか、またはエイリアスを手動で管理するかに関係なく適用されます。

重要な考慮事項

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：常設チャットが有効で、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。
- ユーザがすべての古いチャットルームにアクセスできるようにするには、ノードを削除する前に、既存のすべてのエイリアスのバックアップを取得し、新しいノードに同じエイリアスを割り当てます。

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。

関連トピック

チャットの展開シナリオ 1 （267 ページ）

システムで生成されたチャット ノード エイリアスのオン/オフの切り替え

チャット ノード エイリアスを使用すると、任意のドメイン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、それらのチャット ルームに入室できます。デフォルトでは、IM and Presence Service によって、各ノードにシステムで生成された一意のエイリアスが自動的に割り当てられます。システムで生成されたエイリアスを使用する場合は、チャット ノードに対応するための設定はこれ以上必要ありません。システムは、デフォルトの命名規則である `conference-x-clusterid.domain` を使用して、チャット ノードごとに 1 個のエイリアスを自動的に生成します。

手動でチャット ノード エイリアスを割り当てる場合は、システムで生成されたデフォルトのエイリアス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 エイリアスの下にリストされる標準的な編集可能エイリアスに戻ります。詳細については、手動管理のチャット ノード エイリアスに関するトピックを参照してください。ベスト プラクティスのガイドラインについては、サンプルのチャット展開シナリオを参照してください。

始める前に

- チャット ノード エイリアスと重要な考慮事項に関するトピックを参照してください。
- システムで生成されたエイリアス（`conference-3-mycup.cisco.com` など）は編集または削除できません。

手順

ステップ 1 [Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] にログインし、**[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 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。

a) システムでルーム チャット エイリアスを命名規則 `conference-x-clusterid.domain` を使用してノードに自動的に割り当てるようにするには、**[システムでプライマリ グループ チャット サーバのエイリアスを自動的に管理する（System Automatically Manages Primary Group Chat Server Aliases）]** チェックボックスをオンにします。

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。

b) システムで生成されたエイリアスを無効にするには、**[システムでプライマリ グループ チャット サーバのエイリアスを自動的に管理する（System Automatically Manages Primary Group Chat Server Aliases）]** チェックボックスをオフにします。

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。
- 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 を再起動します。**[Cisco Unified IM and Presence の有用性（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択して、このサービスを再起動します。

関連トピック

チャットの展開シナリオ 1 （267 ページ）
常設チャット ルームの設定 （271 ページ）

チャット ノードのエイリアスの手動管理

手動でチャット ノードのエイリアスを追加、編集、または削除できます。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 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に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）] で **[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 ノードのエイリアスと重要な考慮事項に関するトピック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）] にログインし、**[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 2 **[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。

ステップ 3 すべての既存のチャット ノードのエイリアスはグループ チャット サーバのエイリアスの下に一覧表示されます。エイリアス リストを表示するには、次の操作を実行します。

a) **[メッセージング（Messaging）]** > **[グループ チャット サーバ エイリアスのマッピング（Group Chat Server Alias Mapping）]** を選択します。
b) **[検索（Find）]** をクリックします。

ステップ 4 必要に応じて、次の 1 つまたは複数の操作を実行します。

既存のエイリアス（古いシステム生成またはユーザ定義のエイリアス）を編集します

a) 編集する既存のエイリアスのハイパーリンクをクリックします。
b) [グループ チャットサーバのエイリアス（Group Chat Server Alias）] フィールドでノードのエイリアスを編集します。ノードのエイリアスが一意であることを確認します。
c) この変更されたエイリアスを割り当てる適切なノードを選択します。

新しいチャット ノードのエイリアスを追加します

a) **[新規追加（Add New）]** をクリックします。
b) [グループ チャットサーバのエイリアス（Group Chat Server Alias）] フィールドにノードの一意のエイリアスを入力します。
c) 新しいエイリアスを割り当てる適切なノードを選択します。

既存のエイリアスを削除します

a) 削除するエイリアスのチェックボックスをオンにします。
b) **[選択項目の削除（Delete Selected）]** をクリックします。

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。

次のタスク

- Cisco XCP Text Conference Manager をオンにします。

関連トピック

チャットの展開 （267 ページ）

Cisco XCP Text Conference Manager のオン

この手順は、常設チャット ルームの設定を行うか、チャット ノードに手動で 1 つまたは複数のエイリアスを追加した場合に適用されます。また、ノードでアドホック チャットを有効にする場合もこのサービスをオンにする必要があります。

始める前に

常設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。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常設ルームを作成できません。

手順

ステップ 1 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 - 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 Service] セクションの [Cisco XCP Text Conference Manager サービス（Cisco XCP Text Conference Manager service）] の横にあるオプション ボタンをクリックしてサービスをオンにするか、**[再起動（Restart）]** をクリックしてサービスを再起動します。

ステップ 4 再起動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。

関連トピック

常設チャット ルームの設定 （271 ページ）

チャット ルーム管理

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 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 2 [保存（Save）] をクリックします。

メンバーの設定

メンバー設定では、チャット ルームのメンバーシップをシステム レベルで制御できます。このような制御は、禁止などの管理操作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 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、[デフォルトでルームはメンバー専用です（Rooms are for members only by default）] 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ホワイト 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） ホワイト 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。

ステップ 2 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、[ルームがメンバー専用かどうかをルーム所有者が設定できます（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。

ステップ 3 モデレータ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、[モデレータのみがメンバー専用ルームにユーザを招待できます（Only moderators can invite people to members-only rooms）] 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。

ステップ 4 ルーム所有者がメンバーに他のユーザを招待できるように設定する場合は、[モデレータがユーザをメンバー専用ルームに招待できるかどうかをルーム所有者が変更できます（Room owners can change whether or not only moderators can invite people to members-only rooms）] 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 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、[ユーザは自分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）] 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。

ステップ 6 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、[ユーザが自分をメンバーとしてルームに追加できるかどうかをルーム所有者が変更できます（Room owners can change whether users can add themselves to rooms as members）] 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。

アベイラビリティの設定

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 ユーザが現在、オフラインであっても、ユーザをルームの参加者として保持する場合は、[メンバーと管理者はルームに入室していなくてもルームに表示されます（Members and administrators who are not in a room are still visible in 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 2 メンバーまたは管理者の可視性をルーム所有者が変更できるようにする場合は、[ルームに入室していないメンバーと管理者をルームに表示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 members and administrators who are not in a room are still visible in 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 以前の Group Chat 1.0 クライアントでサービスを正常に動作させるには、[ルームに古いクライアントとの下位互換性があります（Rooms are backwards-compatible with older clients）] 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 チャット ルームの下位互換性をルーム所有者が管理できるようにする場合は、[ルームに古いクライアントとの下位互換性があ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 backwards-compatible with older clients）] 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 5 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、[デフォルトでルームは匿名になっています（Rooms are anonymous 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 6 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、[ルームが匿名かどうかをルーム所有者が変更できます（Room owners can change whether or not rooms are anonymous）]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。

招待の設定

招待の設定によって、誰がユーザの役割に基づいてユーザをルームに招待できるかを決定します。役割は、モデレータからビジターへの階層に存在するため、たとえば、参加者はビジターができることは何でも実行でき、モデレータは参加者ができることは何でも実行できます。

手順

ステップ 1 [他のユーザをルームに招待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 invite others to 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、およびモデレータは他のユーザをルームに招待できます。

- **[参加者（Participant）]** を選択すると、参加者およびモデレータは他のユーザをルームに招待できます。これがデフォルトの設定です。
- **[モデレータ（Moderator）]** を選択すると、モデレータのみが他のユーザをルームに招待できます。

ステップ 2 招待状を送信できる最小参加者レベルの設定をルーム所有者が変更できるようにするには、[他のユーザをルームに招待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 invite others to the room）]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 3 [保存（Save）] をクリックします。

利用者数の設定

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、モデレータは参加者ができることはすべて実行できます。

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。これがデフォルトの設定です。
- [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。これがデフォルトの設定です。
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。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 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。

モデレータが管理するルームの設定

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しする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。

グループチャットと常設チャットのインタラクションと制限

表 *27*: グループ チャットと常設チャットのインタラクションと制限

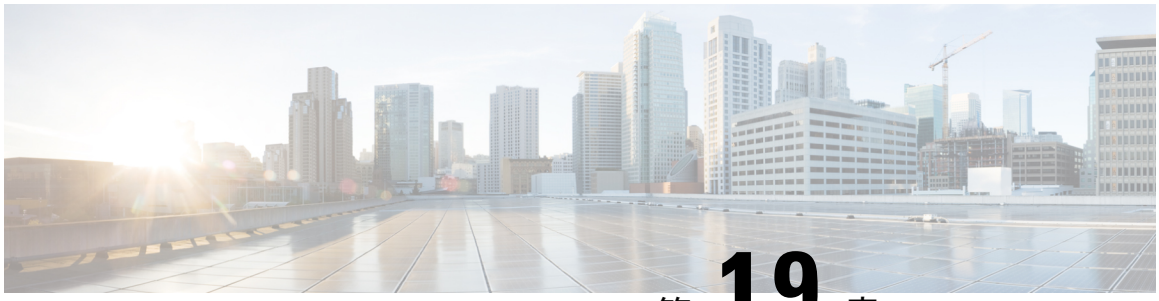
機能の相互作用	制約事項
ルームへの参加のアーカイブ	ルームの入退室をアーカイブすると、トラフィックが増加し、外部データベース サーバの領域が消費されるため、これを行うかどうかは任意です。
匿名ルームでのチャット	Cisco Jabber 経由でチャットを展開する場合（グループ チャットまたは常設チャットのいずれか）は、[グループチャットとパーシステントチャットの設定（Group Chat and Persistent Chat Settings）] ウィンドウで [デフォルトで、ルームは匿名です（Rooms are anonymous by default）]および[ルームのオーナーは、ルー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常設ルームを作成できません。

機能の相互作用	制約事項
OVA 要件	常設チャットまたはクラスタ間のピアリングを導入している場合、これらの機能が導入可能な OVA サイズは 5000 ユーザ OVA になります。最低でも 15000 ユーザ OVA の導入を推奨します。集中型展開では、ユーザ ベースの規模に応じて、25000 ユーザ 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、以下のサイトを参照してください。 （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。 https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html
Microsoft SQL Server での常設チャットの文字数制限	メッセージ本文（HTML タグ+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。こういった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 をリリース 11.5 (1) SU3 を外部データベースとして使用した場合に発生します。詳細は、CSCvd89705 を参照してください。

機能の相互作用	制約事項
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 の常設チャット	Jabber モバイル用の常設チャットは、11.5 (1) SU5 で導入されています。それ以前の 11.5 (1) SU リリースではサポートされていません。この機能は、12.0 (1) または 12.0 (1) の SU1 においてもサポートされていません。 Jabber の常設チャットは今回のリリースで導入されています。Jabber Mobile 用の常設チャットルームをサポートしていないピア クラスタを使用して、クラスタのトランクリングを設定している場合は、Jabber Mobile クライアントに対して以下の条件が適用されます。 常設チャット ルームが、サポートされていないリリース（11.5 (1) など）でホストされている場合： • サポートされるクラスタをホームとする 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することができます。ただし、ルームをミュートするオプションは提供されません。グローバル ミュート オプションは表示されますが、機能しません。 • サポートされていないピア クラスタをホームとする Jabber モバイルクライアントは、常設チャットルームに参加することができません。 11.5 (1) SU5 など、常設チャットルームがサポートされるリリースでホストされている場合： • サポートされるクラスタをホームとする Jabber モバイル クライアントの参加者は、すべての常設チャットをモバイル機能に備えています。 • サポートされないピア クラスタからの Jabber モバイルクライアントは、常設チャットルームに参加することができません。 （注） 常設チャット用の検索機能は、IM 履歴が無効に設定されている Jabber 設定ファイル（*jabber-config.xml*）の場合は機能しません。
外部データベース接続および Cisco XCP Text Conferencing サービス	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。 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。

機能の相互作用	制約事項
高可用性が設定されている場合にサポートされる常設チャット ルームの数	IM&P の導入でサポートされる常設チャット ルームの最大数は、サブクラスタあたり 5000 です。 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。 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 Collaboration Sizing Tool を使用して、常設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。Collaboration Sizing Tool の詳細については、次を参照してください。 https://cucst.cloudapps.cisco.com/landing サブクラスタ内の両方のノード間で均等にルームのバランスを取ることを推奨します。また、IM&P クラスタに複数のサブクラスタがある場合は、すべてのサブクラスタにわたってルームをロードバランシングすることを推奨します。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に選択していることを確認する必要があります。

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します	アドホックチャットルームは、デフォルトではパブリックですが、次の設定のメンバーのみに対して設定できます。 **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.** [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）] 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。



第 19 章

エンドユーザの設定と処理

- IM and Presence Service のエンドユーザの設定と処理 （295 ページ）
- IM and Presence Service の許可ポリシーの設定 （295 ページ）
- ユーザ連絡先 ID の一括名前変更 （298 ページ）
- ユーザ連絡先リストの一括エクスポート （300 ページ）
- 非プレゼンス連絡先リストの一括エクスポート （302 ページ）
- ユーザ連絡先リストの一括インポート （303 ページ）
- ユーザ非プレゼンス連絡先リストの一括インポート （308 ページ）
- 重複するユーザ ID とディレクトリ URI の管理 （311 ページ）

IM and Presence Service のエンドユーザの設定と処理

IM and Presence Service エンドユーザ用の許可ポリシーを設定し、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を実行するだけでなく、重複しているエンドユーザ インスタンスや無効なエンドユーザ インスタンスを管理できます。

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。

- 『Cisco Unified Communications Manager アドミニストレーション ガイド』
- 『Cisco Unified Communications Manager 一括管理ガイド』
- 『Cisco Unified Communications Manager のインストール』

IM and Presence Service の許可ポリシーの設定

IM and Presence Service の自動許可

IM and Presence Service は、ローカル企業の SIP ベースのクライアントから受信するすべてのプレゼンス登録要求を許可します。SIP ベースのクライアントを実行するローカル ユーザは、ク

ライアントでこれらの登録を許可するよう求められることなく、ローカル企業の連絡先のアベイラビリティステータスを自動的に受信します。IM and Presence Service は、連絡先がユーザの拒否リストに存在する場合にのみ、ローカル企業の連絡先の登録を許可するようにユーザに求めます。これは、IM and Presence Service における SIP ベースのクライアントのデフォルト許可動作であり、この動作を設定することはできません。

XMPP ネットワークでは、クライアントにすべてのプレゼンス登録を送信するのがノードの標準動作で、クライアントは登録を許可または拒否するようにユーザに求めます。SIP ベースのクライアントと XMPP ベースのクライアントが混在する IM and Presence Service を（両方のクライアント タイプの許可ポリシーに合わせて）企業が展開できるように、シスコは IM and Presence Service に次の自動許可設定を提供しています。

- 自動許可をオンにすると、IM and Presence Service は、ローカル企業で XMPP ベースのクライアントおよび SIP ベースのクライアントの両方から受信したすべてのプレゼンス登録要求を自動的に許可します。これは、IM and Presence Service におけるデフォルト設定です。
- 自動許可をオフにすると、IM and Presence Service は XMPP ベースのクライアントのみをサポートします。XMPP ベースのクライアントでは、IM and Presence Service はクライアントにすべてのプレゼンス登録を送信し、クライアントはユーザにプレゼンス登録を許可または拒否するよう求めます。SIP ベースのクライアントは、自動許可をオフにすると、IM and Presence で正しく動作しません。

注意 自動許可をオフにした場合、SIP ベースのクライアントはサポートされません。自動承認をオフにしたときの XMPP ベースのクライアントだけがサポートされます。

ユーザ ポリシーおよび自動許可

自動許可ポリシーの読み取りに加えて、IM and Presence Service はプレゼンス登録要求の処理方法を判断するためにユーザのポリシー設定を読み取ります。ユーザは Cisco Jabber クライアントからポリシー設定をします。ユーザ ポリシーには次の設定オプションがあります。

- [拒否リスト（Blocked list）]：ユーザの実際のステータスに関係なく使用不可としてユーザのプレゼンス ステータスを常に表示するローカルおよび外部（フェデレーション）ユーザのリスト。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（Allowed list）]：アベイラビリティを表示することをユーザが許可したローカルおよび外部ユーザのリスト。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）]：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。

自動許可をオフにした場合、IM and Presence Service 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。

- UserA は UserB のプレゼンス ステータスの表示を登録することを望んでいます。自動許可が IM and Presence Service でオフであり、UserB は UserA の許可リストまたは拒否リストにありません。
- IM and Presence Service 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。

IM and Presence Service は、UserB のポリシーが (i) 外部ドメインを拒否する場合、(ii) ユーザのデフォルト ポリシーがすべて拒否の場合、または (iii) 「確認（Ask me）」 が選択されている場合でも、UserB の連絡先リストに自動的に UserA を追加します。

ローカル IM and Presence Service エンタープライズとサポートされる外部エンタープライズとの間にドメイン間フェデレーションを展開すると、IM and Presence Service は、外部連絡先から受信したプレゼンス登録要求に自動許可設定を適用しません。ただし、ユーザがその外部連絡先またはドメインにポリシーを適用した場合を除きます。外部連絡先からプレゼンス登録要求を受信すると、ユーザが [確認（Ask me）]「」 を選択して外部連絡先の独自の許可/拒否ポリシーを設定するように求められた場合、および外部連絡先またはドメインがユーザの許可リストまたは拒否リストにない場合にのみ、IM and Presence Service はクライアント アプリケーションに登録要求を送信します。クライアント アプリケーションは、ユーザに登録を許可または拒否するように求めます。

（注） IM and Presence Service は、可用性とインスタント メッセージの両方に共通ユーザ ポリシーを使用します。

関連トピック

http://www.cisco.com/en/US/products/ps6837/products_user_guide_list.html

IM and Presence Service の構成ガイド

IM and Presence Service の許可ポリシーの設定

IM and Presence Service がローカル エンタープライズで XMPP ベースのクライアントおよび SIP ベースのクライアントの両方から受信したすべてのプレゼンス登録要求を自動的に許可するようにするには、自動許可をオンにします。自動許可をオフにする場合、IM and Presence Service が XMPP ベースのクライアントのみをサポートし、プレゼンス登録の許可または拒否を求めるユーザ クライアントにすべてのプレゼンス登録を送信します。

ヒント　このウィンドウ内のすべてのパラメータの定義については Cisco Unified CM IM and Presence の管理インターフェイスのオンライン ヘルプ トピック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）] > [プレゼンス（Presence）] > [設定（Settings）]** を選択します。

ステップ 2　認可ポリシーを設定します。次のいずれかの操作を実行します。

- 自動許可をオンにするには、[確認プロンプトなしで他のユーザのアベイラビリティ表示を許可する（Allow users to view the availability of other users without being prompted for approval）] のチェックボックスをオンにします。
- 自動許可をオフにするには、[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）] のチェックボックスをオフにします。

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 Service の SIP パブリッシュ トランクの設定に進みます。

関連トピック

Cisco XCP Router サービスの再起動 （88 ページ）
IM and Presence Service での IM 設定 （191 ページ）

ユーザ連絡先 ID の一括名前変更

IM and Presence Service の一括割り当てツール（BAT）により、ある形式から別の形式にユーザ連絡先リストのコンタクト ID（JID）の名前変更ができます。たとえば、firstname.lastname @ domain.com から userid @ domain.com にユーザの連絡先 ID の名前変更ができます。また、一括管理ツールは新しいコンタクト ID で各ユーザの連絡先リストを更新します。

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 Service 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『パーティションドメイン間フェデレーション ガイド』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。

このジョブを実行する前に、連絡先 ID のリストおよびそれらの連絡先 ID の対応する新しい形式を含むファイルをアップロードする必要があります。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。

リリース 10.0 より、**<Contact ID>** は [プレゼンス トポロジ ユーザ 管理（Presence Topology User Assignment ）] ウィンドウで表示されるユーザの 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
```

CSV ファイルをアップロードして、ユーザのリストのコンタクト ID の名前を変更するには、次の手順を実行します。

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。次の手順を実行します。

a) 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 管理（Cisco Unified CM IM and Presence Administration）] > [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) [参照（Browse）] をクリックして、CSV ファイルを検索し選択します。
d) ターゲットとして [連絡先（Contacts）] を選択します。
e) 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。
f) **[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 ノードで、**[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。

ユーザ連絡先リストの一括エクスポート

IM and Presence Service の一括管理ツール（BAT）を使用すると、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を CSV データ ファイルにエクスポートできます。その後、BAT を使用して、ユーザ連絡先リスト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。BAT のユーザ連絡先リストのエクスポートおよびインポート機能を使用すると、クラスタ間でのユーザの移動が容易になります。詳細については、ユーザ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。

IM and Presence Service リリース 11.5(0) 以降では、非プレゼンス連絡先リストをエクスポートすることもできます。詳細については、非プレゼンス連絡先リストの一括エクスポート （302 ページ）を参照してください。

（注） 連絡先リスト上の、IM アドレスを持たないユーザは、エクスポートされません。

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>
```

次の表に、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ID（User ID）]	IM and Presence Service ユーザのユーザ 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 Service 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 ID であり、example.com は、ユーザのドメインです。 **例 2** ： bjones @ usa @ example.com ： bjones @ usa はユーザ ID であり、example.com は、ユーザのドメインです。
コンタクト ID（Contact ID）	連絡先リスト エントリのユーザ 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
Nickname（ニックネーム）	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。

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
```

次の手順を実行して、BAT でユーザ連絡先リストをエクスポートし、エクスポート ファイルをダウンロードします。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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。

ステップ 2 連絡先リストをエクスポートするユーザを検索するには、選択基準を使用します。ユーザの検索および選択の詳細については、Cisco Unified CM IM and Presence の管理インターフェイスのオンライン ヘルプ トピックを参照してください。

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 5 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 6 [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。

ステップ 7 ジョブの実行後、エクスポート ファイルをダウンロードするには、**[Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] > [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 8 ダウンロードするエクスポート ファイルを探し、選択します。

ステップ 9 [選択項目のダウンロード（Download Selected）] をクリックします。

非プレゼンス連絡先リストの一括エクスポート

BAT を使用して、すべてのローカル クラスタ ユーザの非プレゼンス連絡先リストを CSV データ ファイルにエクスポートできます。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。

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
```

手順

ステップ 1 **[Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）] > [連絡先（Contact）] > [非プレゼンス連絡先リストのエクスポート（Export Non-presence Contact List）]** を選択します。

ステップ 2 [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 3 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 4 [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。

ステップ 5 ジョブの実行後、エクスポート ファイルをダウンロードするには、**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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 6 ダウンロードするエクスポート ファイルを探し、選択します。

ステップ 7 [選択項目のダウンロード（Download Selected）] をクリックします。

ユーザ連絡先リストの一括インポート

IM and Presence Service の一括割り当てツール（BAT）を使用して、ユーザ連絡先リストを IM and Presence Service にインポートできます。このツールを使用すると、新しい IM and Presence Service クライアント 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。ユーザ連絡先リストをインポートするには、ユーザ連絡先リストを含む入力ファイルを BAT に指定する必要があります。

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>
```

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
```

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。

表 *28* : 入力ファイルのパラメータの説明

パラメータ	説明
[ユーザ ID（User ID）]	これは必須パラメータです。 IM and Presence Service ユーザのユーザ 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）	これは必須パラメータです。 IM and Presence Service 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。 （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 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 ID、example.com はユーザ ドメインです。
コンタクト ID（Contact ID）	これは必須パラメータです。 連絡先リスト エントリのユーザ ID。これには、最大 132 文字を使用できます。
Contact Domain（連絡先ドメイン）	これは必須パラメータです。 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。 • 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）	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。
グループ名（Group Name）	これ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。

（注） 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ユーザを移動する場合は、BAT を使用して、選択したユーザの CSV ファイルを生成できます。詳細については、ユーザ連絡先リストの一括エクスポートに関するトピックを参照してください。

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。

- 連絡先リストの最大サイズを確認します。
- BAT を使用して入力ファイルをアップロードします。
- 新しい一括管理ジョブを作成します。
- 一括管理ジョブの結果を確認します。

はじめる前に

ユーザ連絡先リストをインポートする前に、次の手順を実行する必要があります。

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。

連絡先リストの最大サイズの確認

連絡先リストを IM and Presence Service にインポートする前に、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 IM and Presence Service にインポート中は [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。これにより、移行し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。

（注） 連絡先リストのインポート時に BAT を使用するとデータを損失することなく連絡先リストの最大サイズを超過できますが、[連絡先リストの最大サイズ（Maximum Contact List Size）] の設定値を一時的に大きくするか、値を [無制限（Unlimited）] に設定してインポートすることを推奨します。インポートが完了した後に、最大値をリセットできます。

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 パブリッシャ ノードでのみこれらの設定を変更する必要があります。

次の作業

BAT を使用して入力ファイルをアップロードします。

関連トピック

ユーザごとの連絡先リストの最大サイズの設定 （189 ページ）
ユーザごとの最大ウォッチャ数の設定 （190 ページ）

BAT を使用した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 CSV ファイルをアップロードする方法について説明します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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 ターゲットとして **[連絡先リスト（Contact Lists）]** を選択します。

ステップ 5 トランザクション タイプとして **[ユーザの連絡先 - カスタム ファイル（Import Users' Contacts – Custom File）]** 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を作成します。

新しい一括管理ジョブの作成

次の手順では、Cisco Unified CM IM and Presence の管理の新しい一括管理ジョブを作成する方法について説明します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）] > [連絡先リスト（Contact List）] > [更新（Update）]** 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を確認します。

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 Service 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。

手順

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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。

ユーザ非プレゼンス連絡先リストの一括インポート

IM and Presence Service の一括割り当てツール（BAT）を使用して、ユーザ非プレゼンス連絡先リストを IM and Presence Service にインポートできます。このツールを使用すると、新しい IM and Presence Service クライアント ユーザの連絡先リストを事前に設定したり、既存の非プレゼンス連絡先リストに追加したりできます。ユーザ非プレゼンス連絡先リストをインポートするには、ユーザ連絡先リストを含む入力ファイルを BAT に指定する必要があります。

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。

表 *29*：非プレゼンス連絡先リストの入力ファイルのパラメータの説明

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。

（注） 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ユーザを移動する場合は、BAT を使用して、選択したユーザの CSV ファイルを生成できます。詳細については、ユーザ連絡先リストの一括エクスポートに関するトピックを参照してください。

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。

- BAT を使用して非プレゼンス連絡先リストの入力ファイルをアップロードします。BAT を使用した非プレゼンス連絡先の入力ファイルのアップロード（310 ページ）を参照してください
- 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。非プレゼンス連絡先リストの新しい一括管理ジョブの作成（310 ページ）を参照してください
- 一括管理ジョブの結果を確認します。一括管理ジョブの結果の確認（307 ページ）を参照してください

BAT を使用した非プレゼンス連絡先の入力ファイルのアップロード

次の手順では、BAT を使用して非プレゼンス連絡先の CSV ファイルをアップロードする方法について説明します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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 ターゲットとして [非プレゼンス連絡先リスト（Non-presence Contact Lists）] を選択します。

ステップ 5 トランザクション タイプとして [ユーザの非プレゼンス連絡先のインポート（Import Users' Non Presence Contacts）] 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。

非プレゼンス連絡先リストの新しい一括管理ジョブの作成

次の手順では、Cisco Unified CM IM and Presence の管理の新しい一括管理ジョブを作成する方法について説明します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）] > [非プレゼンス連絡先リスト（Contact Non-presence List）] > [非プレゼンス連絡先リストのインポート（Import Non-presence Contact List）]** 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。

重複するユーザ ID とディレクトリ URI の管理

Cisco IM and Presence Data Monitor サービスは、すべての IM and Presence Service クラスタ間ノードで重複するユーザ ID と、空または重複するディレクトリ UIR を確認します。何らかのエラーが検出された場合、M and Presence Service はソフトウェアでアラームを生成します。それらのエラーを修正するための対策をすぐに講じて、ユーザに対する通信の中断を回避することを推奨します。

Cisco Unified CM IM and Presence の管理 GUI を使用して、システム トラブルシュータから重複するユーザ ID やディレクトリ URI のチェックの状態を監視できます。また、GUI を使用して、ユーザ ID と ディレクトリ URI のチェック間隔を設定できます。

これらのアラームの原因となったユーザに関する特定の情報を収集するには、コマンドライン インターフェイスを使用します。システム アラームやアラートを監視するには、リアルタイム監視ツール（RTMT）を使用します。

コマンドライン インターフェイスを使用したユーザ ID またはディレクトリ URI の検証の詳細については、『Cisco Unified Communications Solutions コマンドライン インターフェイス』を参照してください。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 アドミニストレーション ガイド』を参照してください。

ユーザ ID と ディレクトリ URI モニタリング

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 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 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 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。

Cisco Unified CM IM and Presence 管理 GUI のシステム トラブルシュータを使用することで、重複ユーザ ID とディレクトリ URI チェックのステータスを監視することができます。これらのユーザ ID とディレクトリ URI チェックの間隔は、Cisco Unified CM IM and Presence 管理 GUI を使用して設定されます。有効な範囲は、5 ～ 1440 分（12 時間）です。デフォルトは 30 分です。

エラーが検出された場合、IM and Presence Service ではソフトウェア アラームが発生します。

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 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 Adress 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、『Cisco Unified Communications Solutions コマンドライン インターフェイス ガイド』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 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 アドミニストレーション ガイド』を参照してください。

ユーザ ID と ディレクトリ URI のエラー状態

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に起こる可能性のあるユーザ 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 *30* : ユーザ *ID* と ディレクトリ *URI* のエラー状態

エラー状態	説明	推奨措置
重複ユーザ ID	重複ユーザ 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。 **関連アラーム：** `DuplicateUserid`	`DuplicateUserid` アラートが発生したら、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なユーザ 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	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。 **関連アラーム**： • DuplicateUserid • DuplicateDirectoryURIWarning	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 アラートが発生した場合、問題を修正するために即時に対処をしてください。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。 *userID@Default_Domain* 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。
無効なディレクトリ URI	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。user @ domain 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。 **関連アラーム**： • InvalidDirectoryURI • InvalidDirectoryURIWarning	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、次のアラートが発生した場合、問題を修正するために即時に対処します。 InvalidDirectoryURI。 *userID@Default_Domain* 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。

ユーザ ID と ディレクトリ URI の確認と変更

特に、新しいユーザを追加した後や連絡先リストを移行した場合は、システムでアラームが発生するのを待たずに、重複ユーザ情報のチェックを実行することを推奨します。

Cisco Unified CM IM and Presence の管理 GUI のシステム トラブルシュータを使用すると、ユーザ ID とディレクトリ URI のエラーの概要を表示できます。詳細および包括的なレポートについては、CLI コマンドを使用し、IM and Presence Service ユーザを検証します。

ユーザに重複または無効な情報があると特定された場合は、[エンド ユーザ設定（End User Configuration）] ウィンドウ（**[ユーザ管理（User Management）] > [エンド ユーザ（EndUser）]**）を使用して、Cisco Unified Communications Manager のユーザ レコードを変更できます。必要に応じて、すべてのユーザに有効なユーザ ID またはディレクトリ URI 値があることを確認します。詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

ユーザ ID と ディレクトリ URI CLI 検証の例

重複ユーザ 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 Service 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、『Cisco Unified Communications Solutions コマンドライン インターフェイス ガイド』を参照してください。

ユーザ 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 チェック間隔の設定

Cisco Unified CM IM and Presence の管理を使用して、重複ユーザ ID とディレクトリ URI の展開ですべてのノードとクラスタを確認するために Cisco IM and Presence Data Monitor サービスの間隔を設定します。

整数を使用して間隔を分単位で入力します。値の範囲は 5 ～ 1440 です。デフォルトは 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）]** > **[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）]** フィールドの **[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 **[ユーザ確認間隔（User Check Interval）]** として 5 ～ 1440 の整数を入力し、**[保存（Save）]** をクリックします。

システム トラブルシュータを使用したユーザ ID とディレクトリ URI の検証

Cisco Unified CM IM and Presence Administration の GUI のシステム トラブルシュータを使用して、展開されているすべてのノードおよびクラスタ全体にわたって重複するユーザ ID や、重複または無効なディレクトリ URI を特定するシステム チェックのステータスを表示します。

詳細および包括的なレポートについては、CLI コマンドを使用し、IM and Presence Service ユーザを検証します。CLI の使用方法およびコマンドの詳細については、『Cisco Unified Communications Solutions コマンドライン インターフェイス ガイド』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）]** > **[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 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。

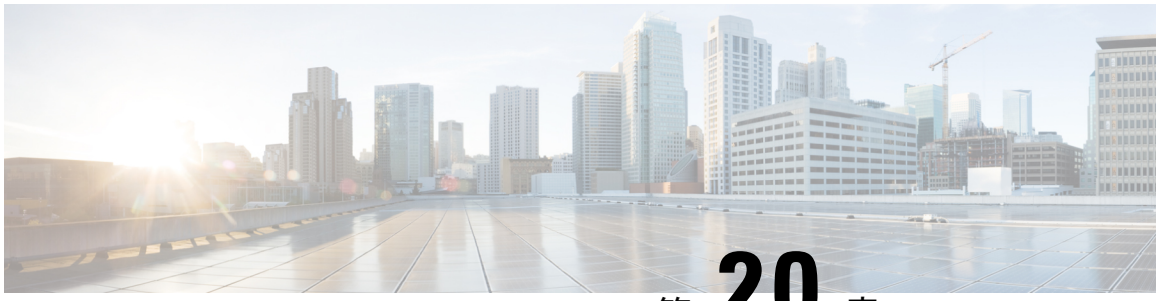
重複または無効なユーザ情報が検出された場合は、推奨ソリューションを実行します。ユーザ ID およびディレクトリ URI のエラーのトラブルシューティングを行うには、トラブルシューティングに関するトピックを参照してください。

ヒント **[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、ユーザプロファイルを見つけ、再設定することができます。詳細なユーザ検証情報については、CLI コマンドを使用してユーザを検証します。

（注） ユーザ プロファイルの [ユーザ ID（User ID）] フィールドと [ディレクトリ URI（Directory URI）] フィールドが LDAP ディレクトリにマップされている場合があります。その場合は、LDAP ディレクトリ サーバで修正を適用します。

関連トピック

重複したユーザ ID エラーの受信 （375 ページ）
重複または無効なディレクトリ URI エラーの受信 （376 ページ）



第 20 章

ユーザの移行

• IM and Presence Service クラスタ間のユーザの移行 （317 ページ）

IM and Presence Service クラスタ間のユーザの移行

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。次の手順を記述されている順に完了する必要があります。

1. 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。
2. 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。
3. Cisco Unified Communications Manager から現在のホーム クラスタの IM and Presence Service および Cisco Jabber の移行ユーザを無効にします。
4. LDAP 同期が Cisco Unified Communications Manager で有効になっている場合：
   - 新しいクラスタが情報を同期する新しい組織ユニットにユーザを移動します。
   - 新しいホーム Cisco Unified Communications Manager にユーザを同期します。
5. LDAP 同期が Cisco Unified Communications Manager で有効になっていない場合は、手動で Cisco Unified Communications Manager の移行ユーザをプロビジョニングします。
6. IM and Presence Service および Cisco Jabber のユーザを有効にします。
7. 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、新しいホーム クラスタに連絡先リストをインポートします。

はじめる前に

次のタスクを実行します。

- 現在のクラスタおよび新しいホーム クラスタの完全な DRS を実行します。詳細については、『Disaster Recovery System アドミニストレーション ガイド』を参照してください。
- 次のサービスが実行されていることを確認します。

- Cisco Intercluster Sync Agent
- Cisco AXL Web Service
- Cisco Sync Agent

- トラブルシュータを実行し、Intercluster Sync Agent の問題が報告されないことを確認します。この手順を続行する前に、トラブルシュータで報告されたすべての Intercluster Sync Agent の問題を解決する必要があります。
- **[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）]** 設定を有効にすることを推奨します。この設定を有効にするには、**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）]** を選択します。この設定の変更には、Cisco XCP Router を再起動する必要があります。
- 次の設定を [無制限（No Limit）] に設定することを推奨します。
  - 連絡先リストの最大サイズ（ユーザごと）（Maximum Contact List Size (per user)）
  - ウォッチャの最大数（ユーザごと）（Maximum Watchers (per user)）

  これらの設定を行うには、**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）]** を選択します。
- 移行されるユーザに現在の（移行前）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。これらのユーザに他のクラスタでライセンスが供与されている場合、次の手順に進む前に完全ライセンスが供与されている必要はありません。

古いエントリを削除する

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の IM&P ノードで行われます。

（注） 必要に応じて、2000 のバッチでこれらの手順を繰り返します。CLI 経由で大量の古いエントリを削除するには時間がかかりすぎる場合は、TAC サービス リクエストを開いて、ルート アクセスが必要なこのセクションの最後にある古い名簿スクリプトを活用してください。

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、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する：

```
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する：

```
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 レコードを削除する：

```
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 連絡先以外の古いレコードを（順に）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) 連絡先以外の古いレコードを（順に）確認する：

```
run sql select count(*) from nonpresencecontacts where fkenduser in (select pkid from
 enduser where primarynodeid is null)
```

b) 連絡先以外の古いレコードを（順に）削除する：

```
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 アクセスを持っている場合は、次のクエリを使用する：

```
run sql delete from epascontactaddinfo where pkid in (select * from (select first
2000 pkid from epascontactaddinfo where pkid not in (select fkepascontactaddinfo from
 nonpresencecontacts)))
```

ユーザ連絡先リストのエクスポート

現在のクラスタから移行の連絡先リストをエクスポートするには、次の手順を実行します。

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。

a) **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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。
b) **[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。
c) 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。
d) リストが完了すると、**[次へ（Next）]** をクリックします。
e) 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。
f) 任意でジョブの説明を更新します。
g) **[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。

a) **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）] > [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) 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。
d) [CSV ファイル名（CSV File Name）] 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付加されることに注意してください。
e) **[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。ジョブの開始時刻と終了時刻が一覧表示され、ジョブの結果の要約が表示されます。

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。

a) **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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（Find）]** をクリックします。
c) 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。
d) 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

ユーザを非ライセンスに設定します。

IM and Presence Service のユーザの無効化

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。

ユーザを一括更新する方法については、『Cisco Unified Communications Manager 一括管理ガイド』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）]** > **[ユーザ管理（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。

新しいクラスタへのユーザの移動

新しいクラスタにユーザを移動する手順は、LDAP 同期が Cisco Unified Communications Manager で有効になっているかどうかによって異なります。

Cisco Unified Communications Manager で有効な LDAP 同期

LDAP 同期が Cisco Unified Communications Manager で有効になっている場合は、新しい組織ユニットにユーザを移動し、新しいホーム クラスタにユーザを同期する必要があります。

新しい組織ユニットへのユーザの移動

LDAP 同期が Cisco Unified Communications Manager で有効になっている場合は、展開でクラスタごとに異なる LDAP 構造が使用されるときに（OU 分割）、新しいクラスタの同期元となる新しい組織ユニット（OU）にユーザを移動する必要があります。この場合、ユーザは LDAP からそのホーム クラスタにのみ同期されます。

（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 Service 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。

新しいホーム クラスタの関連する OU に移行ユーザを移動する方法の詳細については、LDAP 管理マニュアルを参照してください。

ユーザの移動後、古い LDAP のクラスタから LDAP エントリを削除する必要があります。

次のタスク

新しいホーム クラスタへのユーザの同期に進みます。

新しいホーム クラスタへのユーザの同期

LDAP が Cisco Unified Communications Manager になっている場合、新しいホーム Cisco Unified Communications Manager クラスタにユーザを同期する必要があります。Cisco Unified Communications Manager でこれを手動で同期するか、Cisco Unified Communications Manager でスケジュールされた同期化が行われるまで待機できます。

Cisco Unified Communications Manager で、同期を手動で強制するには、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 [完全同期を今すぐ実施（Perform Full Sync Now）] をクリックします。

次のタスク

IM and Presence Service のユーザを有効にし、新しいクラスタのユーザにライセンスを供与する手順に進みます。

関連トピック

新しいクラスタの IM and Presence Service のユーザの有効化 （322 ページ）

Cisco Unified Communications Manager で有効ではない LDAP 同期

LDAP 同期が Cisco Unified Communications Manager で有効になっていない場合、新しい Cisco Unified Communications Manager クラスタでユーザを手動でプロビジョニングする必要があります。詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

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 Service 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 Service 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、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

ユーザを一括更新する方法については、『Cisco Unified Communications Manager 一括管理ガイド』を参照してください。

次のタスク

新しいホーム クラスタの連絡先リストのインポートに進みます。

ホーム クラスタでの連絡先リストのインポート

移行されたユーザの連絡先データを復元するには、連絡先リストをインポートする必要があります。

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）] > [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。

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）] > [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。

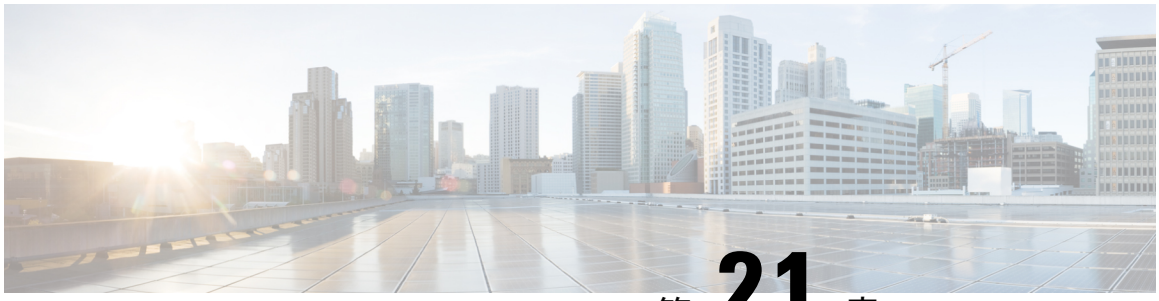
c) 任意でジョブの説明を更新します。

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）] > [一括管理（Bulk Administration）] > [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。



第 21 章

ユーザの中央展開への移動

- ユーザの中央展開への移動の概要 （325 ページ）
- 中央クラスタ マイグレーションの要件となるタスク （325 ページ）
- 中央クラスタ タスク フローへの移行 （327 ページ）

ユーザの中央展開への移動の概要

この章では、既存の IM およびプレゼンスサービスを使用しているユーザを標準の分散 IM およびプレゼンスサービスの導入（Cisco Unified Communications Manager 上の IM and Presence Service）から展開に移行する手順について説明します。集中展開では、IM and Presence 展開とテレフォニー展開は、別々のクラスタに位置します。

中央クラスタ マイグレーションの要件となるタスク

すべてのユーザを既存の分散クラスタから移行させる新たな IM and Presence 中央クラスタを設定する場合は、以下の必須手順を実行して、移行用クラスタを設定します。

（注） 移行に含まれない新しいユーザを追加する場合は、集中展開の設定 （65 ページ）の手順に従って、新しいユーザに中央クラスタを設定することができます。設定が正常に動作してい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 *31* : 移行前のタスク

	移行前のタスク
ステップ 1	新しい中央クラスタを移行クラスタに接続します。 **1.** IM and Presence Service 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の管理（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。 • 既存のクラスタを選択して、[選択したものを編集する（Edit Selected）] 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。 • **ピア アドレス（Peer Address）**：リモート テレフォニーのパブリッシャ 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	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。 • 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。 詳細については、クラスタ間ピアの設定 （179 ページ）を参照してください。

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クラスタ（Ciscoユニファイド コミュニケーション マネージャ の IM and Presence Service）から中央管理の IM and Presence クラスタに移行します。このタスク フローに含まれるタスク：

- **IM and Presence Central Cluster** は、ユーザの移行先クラスタを参照します。移行後は、このクラスタは IM and Presence のみを処理します。
- **移行元 クラスタ**とは、IM and Presence ユーザの移行元 クラスタを指します。このクラスタは移行後は、テレフォニーのみを処理します。

はじめる前に

IM and Presence の中央クラスタが新たにインストールされたクラスタであり、まだユーザを持っていない場合は、ユーザを移行する前に 中央クラスタ マイグレーションの要件となるタスク （325 ページ） を完了します。

表 *32 :* 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	クラスタの移行	目的
ステップ 1		移行元クラスタからの連絡先リストのエクスポート （329 ページ）	移行クラスタ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		移行元クラスタの高可用性の無効化 （330 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）の高可用性を無効にします。
ステップ 3		IM and Presence の UC Service の設定 （331 ページ）	移行元クラスタで、IM and Presence 中央クラスタをポイントする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 （332 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 クラスタでのプレゼンス ユーザの無効化 （332 ページ）	移行元クラスタの一括管理を使用して、ユーザの IM and Presence を無効にします。

	IM and Presence 中央クラスタ	クラスタの移行	目的
ステップ 6		中央クラスタの OAuth 認証を有効にする （334 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。これで、中央クラスタの機能も有効になります。
ステップ 7	#unique_394		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）で高可用性を無効にします。
ステップ 8	中央および移行クラスタのピア関係を削除する （334 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 Intercluster Sync Agent （335 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	機能グループテンプレート経由の IM and Presence の有効化 （335 ページ）		中央クラスタで、IM and Presence Service 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 （336 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移行元クラスタから、この同期を使用して、ユーザを追加します。
ステップ 12	中央クラスタへの連絡先リストのインポート （338 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 を起動する （339 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	クラスタの移行	目的
ステップ 14	中央クラスタの高可用性の有効化 （340 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高可用性を有効にします。
ステップ 15		移行クラスタの残りのピアを削除する （340 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の連絡先リストのエクスポート

この手順は、分散 IM and Presence 展開から集中配置に移行する場合にのみ使用します。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て、後で中央クラスタにインポートします。以下の 2 種類の連絡先リストをエクスポートすることができます。

- 連絡先リスト：このリストは、IM and Presence 連絡先で構成されます。IM アドレスがない連絡先は、このリストにエクスポートされません（非プレゼンス連絡先リストをエクスポートする必要があります）。
- 非プレゼンス連絡先リスト：このリストは、IM アドレスを持っていない連絡先で構成されます。

手順

ステップ 1 古いクラスタ（テレフォニークラスタ）で Cisco Unified CM のIM and Presence 管理にログインします。

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、以下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は、**[一括管理（Bulk Administration）] > [連絡先リスト（Contact List）] > [連絡先リストのエクスポート（Export Contact List）]** を選択します。
- 非プレゼンス連絡先リストのエクスポートの場合は、**一括管理(Bulk Administration) > 非プレゼンス連絡先リスト(Non-presence Contact List) > 非プレゼンス連絡先リストのエクスポート(Export Non-presence Contact List)** を選択し、次のステップはスキップします。

ステップ 3 連絡先リストのみ。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) [連絡先リストのオプションのエクスポート（Export Contact List Options）] の下で、連絡先リストのエクスポート先とな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（All users in the cluster）]です。

b) [検索（Find）] をクリックして、ユーザ リストを表示して、[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 [ジョブ情報（Job Information）] の下で、このジョブをいつ実行するかを設定します。

- [すぐに実行（Run Immediately）]：連絡先のリストを即座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する場合は、このボタンをオンにします。

ステップ 6 [送信（Submit）] をクリックします。

（注） **[すぐに実行（Run Immediately）]を選択した場合、エクスポート ファイルは即時に生成されます。[後で実行する（Run Later）]>を選択した場合は、このジョブを実行する時間をスケジュールするために、（>[一括管理（Bulk Administration）]>[ジョブ スケジューラ（Job Scheduler）]）**でジョブ スケジューラを使用しなければなりません。

ステップ 7 エクスポート ファイルが生成された後のCSV ファイルのダウンロード：

a) **[一括管理（Bulk Administration）]>[ファイルをアップロード/ダウンロード（Upload/Download Files）]** を選択します。
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 ファイルを選択して、[選択したファイルをダウンロード（Download Selected）] をクリックします。
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、連絡先リストのエクスポートファイルを作成する場合は、非プレゼンスの連絡先リストとして別のファイルを作成することができます。

次のタスク

移行元クラスタの高可用性の無効化 （330 ページ）

移行元クラスタの高可用性の無効化

集中展開型への移行の場合は、移行元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。

手順

ステップ 1 古いクラスタで、Ciscoユニファイド コミュニケーション マネージャ 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 Administration 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（Find）] をクリックします。

ステップ 4 [高可用性の有効化（Enable High Availability）]のチェック ボックスをオフにします。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 サブクラスタ毎に、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、少なくとも2分待ってから、このクラスタで追加の設定を完了に進みます。

次のタスク

IM and Presence の UC Service の設定 （331 ページ）

IM and Presence の UC Service 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 Service 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 クラスタのユーザは、IM and Presence 集中クラスタから IM and Presence Service を取得します。

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**で、IM and Presence の集中型クラスタ 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、あるいは 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、**ホスト名 / IP アドレス** フィールドが集中クラスタのサブスクライバ ノードを指す 2 番目の IM and Presence Service を作成します。

次のタスク

IM and Presence のサービス プロファイルの作成 （332 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 Service 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 **IM and Presence Profile** セクションで、以前のタスクで設定した IM and Presence Service を設定します。

a) **プライマリ** ドロップダウンでデータベース パブリッシャ ノード サービスを選択します。

b) **セカンダリ** ドロップダウンで、サブスクライバ ノード サービスを選択します。

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 クラスタでのプレゼンス ユーザの無効化 （332 ページ）

テレフォニー クラスタでのプレゼンス ユーザの無効化

テレフォニー展開で既に LDAP 同期が完了している場合は、一括管理ツールを使用して、IM and Presence ユーザのテレフォニー クラスタ内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 およびプレゼンスサービス の集中クラスタを指します。

（注） この手順は、テレフォニークラスタのLDAP同期がすでに完了していることを前提としています。ただし、LDAPの初期同期が未完了の場合は、最初の同期にプレゼンスユーザの集中導入設定を追加することができます。この場合は、テレフォニー クラスタに対して以下の操作を実行します。

- 先ほど設定した**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。**ホーム クラスタ** オプションが選択されていること、**Unified CM IM and Presence のユーザを有効にする** 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。
- **LDAP ディレクトリ設定**で、**機能グループ テンプレート** を LDAP ディレクトリ同期に追加します。
- 最初の同期を完了します。

機能グループ テンプレートおよびLDAP ディレクトリ同期の設定の詳細は、『Cisco Unified Communications Managerシステム設定ガイド』の「エンドユーザの設定」セクションを参照してください。

手順

ステップ 1 Cisco Unified CM Administration で、**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)**を選択します。

ステップ 2 フィルタで、**ホーム クラスタが有効(Home Cluster Enabled)**を選択し、**検索(Find)**をクリックします。このウィンドウには、ここをホーム クラスタとするすべてのエンド 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。
ユーザ設定の更新 ウィンドウの一番左のチェック ボックスで、この設定をこのクエリで編集するかどうかが表示されます。左側のチェック ボックスをチェックしないと、フィールドはクエリによって更新されません。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ている場合は、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 ボックスには新しい設定を入力する必要があります。

ステップ 4 **サービスの設定** で、以下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てから、隣の設定を以下に従って編集します。

- **ホーム クラスタ**：ホーム クラスタとしてテレフォニー クラスタを有効にするには、右側のチェック ボックスをオンにします。
- **Unified CM IM and Presence のユーザを有効にする**：右のチェックボックスはオンにしません。この設定では、IM and Presenceのプロバイダーとしてテレフォニー クラスタを無効にします。
- **UC サービス プロファイル**—ドロップ ダウンから、先ほど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およびプレゼンスサービスのプロバイダーとなる IM and Presenceの集中クラスタがユーザに表示されます。

（注） Expressway MRA 構成の詳細は、https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html の *Cisco Expressway* を介したモバイルおよび*Remote Access*導入ガイドを参照してください。

ステップ 5 残りのすべてフィールドの入力を完了します。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**の下の**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 （334 ページ）

中央クラスタの OAuth 認証を有効にする

テレフォニー クラスタの OAuth 認証を有効にするには、以下の手順を使用します。これで、IM and Presence 中央クラスタでも OAuth 認証が可能になります。

手順

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

ステップ 2 **システム** > **エンタープライズ パラメータ**を選択する

ステップ 3 **SSO と OAuth の設定** の下で、**更新ログイン フローを使用した OAuth** のエンタープライズ パラメータを **有効**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（Save）**をクリックします。

中央および移行クラスタのピア関係を削除する

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の管理（Cisco Unified CM IM and Presence Administration）] から、**[プレゼンス（Presence）]** > **[クラスタ間設定（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 Router** 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の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）] 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 Services（IM and Presence Services）] の下で、[Cisco XCP Router（Cisco XCP Router）] を選択し、[再起動（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 Intercluster Sync Agent

IM and Presence の中央クラスタを設定する前に、中央クラスタで**Cisco Intercluster Sync Agent** サービスが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から、**ツール > コントロールセンタ - ネットワークサービス**を選択します。

ステップ 2 **サーバ** 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、**移動(Go)** をクリックします。

ステップ 3 **Cisco Intercluster Sync Agent** のステータスを確認します。サービスが開始されているか、アクティブである場合は、隣接するオプション ボタンを選択して、**停止(Stop)**をクリックします。

次のタスク

機能グループ テンプレート経由の IM and Presence の有効化 （335 ページ）

機能グループ テンプレート経由の IM and Presence の有効化

この手順で、集中クラスタの IM and Presence の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 ディレクトリの設定に追加して、同期ユーザに IM and Presence を設定することができます。

（注） 初回同期がまだ行われていない場合にのみ、LDAP ディレクトリ同期に機能グループ テンプレートの編集内容を適用することができます。集中クラスタから LDAP 設定を同期した後は、Ciscoユニファイド コミュニケーション マネージャ の LDAP 設定に編集を適用することはできません。すでにディレクトリを同期している場合は、一括管理を使用して、ユーザの IM and Presence を設定する必要があります。詳細については、一括管理を介した IM and Presence ユーザの有効化 （75 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いてはいけません。

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 [保存（Save）] をクリックします。

次のタスク

設定をユーザに適用するには、初期同期がまだ行われていない場合は、機能グループ テンプレートを LDAP ディレクトリの設定に追加してから初期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 （336 ページ）

中央クラスタでの LDAP 同期の完了

リモート Ciscoユニファイド コミュニケーション マネージャ のテレフォニー クラスタでこの手順を使用して、LDAP 同期を使用して、IM and Presence 集中型設定を Ciscoユニファイド コミュニケーション マネージャ 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** > **LDAP** > **LDAPディレクトリ** 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。

ステップ 6 [完全同期を実施（Perform Full Sync）] をクリックします。
Ciscoユニファイド コミュニケーション マネージャ 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

中央クラスタへの連絡先リストのインポート （338 ページ）

一括管理を介した IM and Presence ユーザの有効化

ユーザをすでに中央クラスタに同期させており、それらのユーザが IM and Presence Service 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（Administration's Update）] 機能を使用して、それらのユーザを IM and Presence Service に対して有効にします。

（注） 一括管理の [ユーザのインポート（Administration's Import ）] または [ユーザの挿入（Insert Users）] 機能を使用して、CSVファイルを介して新しいユーザをインポートすることもできます。手順は、*Cisco Unified Communications Manager* 一括管理ガイド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（Filter）] で、[ホーム クラスタが有効になっている（Has Home Cluster Enabled）] を選択して、[検索（Find）] をクリックします。このウィンドウには、ここをホーム クラスタとするすべてのエンド 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。
ユーザ設定の更新 ウィンドウの一番左のチェック ボックスで、この設定をこのクエリで編集するかどうかが表示されます。左側のチェック ボックスをチェックしないと、フィールドはクエリによって更新されません。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ている場合は、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 ボックスには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、以下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、隣接するフィールドの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**：右のチェックボックスを確認します。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 Service のプロバイダーとして有効となります。

ステップ 5 更新が必要な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**の下の**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。

中央クラスタへの連絡先リストのインポート

ユーザーを 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することができます。以下のいずれかのタイプの連絡先グループがインポート可能です。

- 連絡先リスト：このリストは、IM and Presence 連絡先で構成されます。
- 非プレゼンス連絡先リスト：このリストは、IM アドレスを持っていない連絡先で構成されます。

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 ファイルが必要となります。

手順

ステップ 1 IM and Presence セントラル クラスタ上の Cisco Unified CM IM and Presence 管理にログインします。

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)** > **ファイルをアップロード/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) **ファイルの選択(Choose File)** 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) **対象の選択** ドロップダウンで、インポートする連絡先リストの種類に応じて、以下のいずれかを選択します。**連絡先リスト** または **非プレゼンス連絡先リスト**。
e) **トランザクション タイプの選択**で、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 IM and Presence 管理で、以下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(Bulk Administration)** > **連絡先リスト(Contact Lists)** > **連絡先リストの更新(Update Contact Lists)**を選択します。
- 非プレゼンス連絡先リストインポートの場合は、**一括管理(Bulk Administration)** > **非プレゼンス連絡先リスト(Non-presence Contact Lists)** > **非プレゼンス連絡先リストのインポート(Import Non-presence Contact Lists)**を選択します。

b) **ファイル名** ドロップダウンで、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**の下で、ジョブを実行したい時期に合わせて、**すぐに実行する** または **後で実行する** を選択します。
d) [送信（Submit）] をクリックします。**すぐに実行する** を選択した場合、連絡先リストはすぐにインポートされます

（注） 。**後で実行する**を選択した場合、**一括管理** > **ジョブ スケジューラ** を開き、ジョブを選択して、実行する時間をスケジュールします。

ステップ 4 2 個目の csv ファイルをインポートする場合は、この手順を繰り返します。

次のタスク

Cisco Intercluster Sync Agentを起動する （339 ページ）

Cisco Intercluster Sync Agentを起動する

設定または移行が完了したら、IM and Presence 中央クラスタで **Cisco Intercluster Sync Agent** を開始します。クラスタ間ピアリングを使用している場合、このサービスが必要です。

手順

ステップ 1 [Cisco Unified IM and Presence Serviceability（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** ドロップダウンから 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 およびプレゼンスサービス** の下の **Cisco Intercluster Sync Agent** を選択して、**起動(Start)**をクリックします。

次のタスク

中央クラスタの高可用性の有効化 （340 ページ）

中央クラスタの高可用性の有効化

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 セントラル クラスタ上の Cisco Unified CM 管理インスタンスにログインします。

ステップ 2 **[System（システム）]** > **[Presence Redundancy Groups（プレゼンス冗長グループ）]** を選択します。

ステップ 3 [検索（Find）] をクリックして、既存のサブクラスタを選択します。

ステップ 4 [高可用性の有効化（Enable High Availability）]の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 中央クラスタの各クラスタに対してこの手順を繰り返します。

移行クラスタの残りのピアを削除する

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 Service 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 Router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 Router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の管理（Cisco Unified CM IM and Presence Administration）] から、**[プレゼンス（Presence）]** > **[クラスタ間設定（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 Router** 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の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）] 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 Router（Cisco XCP Router）] を選択し、[再起動（Restart）] をクリックします

ステップ 6 IM and Presence Service 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 Router** が再起動するサイクルは多数あります。

第 22 章

IM and Presence Service の多言語サポート設定

- ロケールのインストール （343 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 （345 ページ）
- エラー メッセージ （347 ページ）
- ローカライズされたアプリケーション （350 ページ）

ロケールのインストール

複数の言語をサポートする Cisco Unified Communications Manager と IM and Presence Service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 Service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 Service 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。これらのファイルは、次のファイル名の表記を使用します。

- 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、アナンシエータ、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 の仮想化導入の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。

ロケールのインストールに関する考慮事項

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。

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、『Cisco Unified Communications Manager アップグレード ガイド』を参照してください。

ロケール ファイル

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。

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。

ノードでロケールをインストールする時は、次のファイルをインストールします。

- ユーザ ロケール ファイル：これらのファイルには、特定の言語と国の言語情報が含まれています。次の表記法が使用されます。

  `cm-locale-language-country-version.cop`（Cisco Unified Communications Manager）

  ps-locale-language_country-version.cop（IM and Presence Service）

- 複合ネットワーク ロケール ファイル：すべての国に対応した、さまざまなネットワーク項目（電話機のトーン、アナンシエータ、およびゲートウェイ トーンなど）の国固有のファイルが格納されています。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）

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

始める前に

- Cisco Unified Communications Manager にロケール インストーラ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。
- 変更を有効にするためには、サーバを再起動する必要があります。ロケールのインストール手順がすべて完了したら、クラスタ内の各サーバを再起動してください。クラスタ内のすべてのサーバを再起動するまで、システム内で更新は行われません。サーバの再起動後にサービスが再開されます。

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 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 Service 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 Service 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

ロケールインストーラをアクティブ化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 *33 :* 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	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。
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	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。
[LOCALE] CSV file installer installdb is not present or not executable	*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。

メッセージ	説明
[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum.	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。
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information.	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。
[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。

メッセージ	説明
[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。
[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。

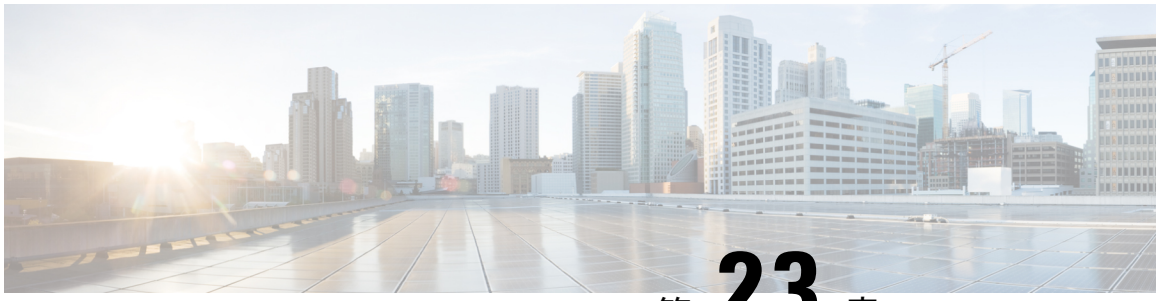
メッセージ	説明
[LOCALE] Failed to build script to reinstall COP files!	プラットフォームで、ロケールの再インストールに使用されるスクリプトを動的に作成できませんでした。 （注） ロケールインストーラを手動で再適用すると、ロケールが完全に復元されます。インストールのログを記録して、TAC にお問い合わせください。

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 *34 :* 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 23 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 （351 ページ）
- ブランディングの前提条件 （351 ページ）
- ブランディングの有効化 （351 ページ）
- ブランディングの無効化 （352 ページ）
- ブランディング ファイルの要件 （353 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 Service 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。詳細は、ブランディング ファイルの要件 （353 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 Service 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 Service 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） また、**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 Service 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 Service 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） また、**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 Service 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、フォルダー構造に2つのオプションがあります。

表 *35* : 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	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。
	
	`Branding (folder)`
	`  cup (folder)`
	`  BrandingProperties.properties (properties file)`
	`  brandingHeader.gif (652*1 pixel)`
	`  ciscoLogo12pxMargin.gif (44*44 pixel)`

勾配ヘッダー オプション	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。
	
	`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)`

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 *17 :* 管理ログイン画面のブランディング オプション

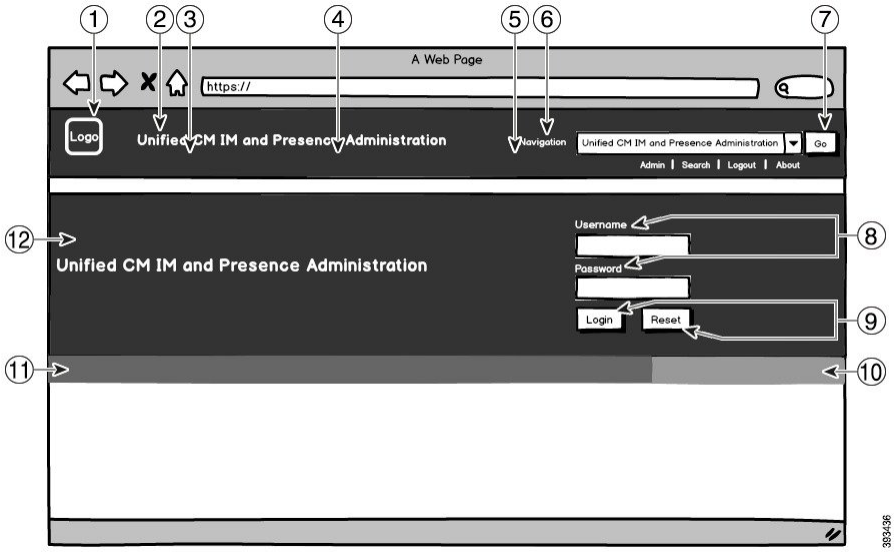
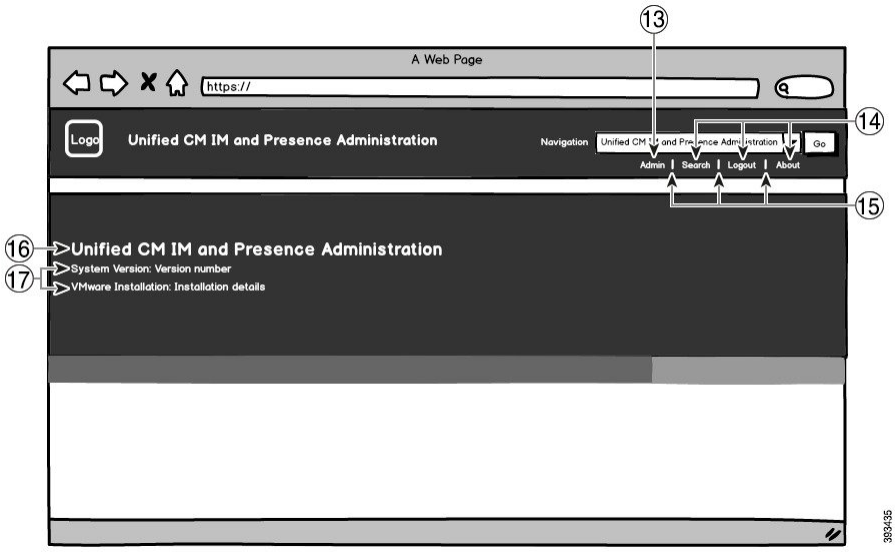


図 *18 :* 管理ログイン中の画面のブランディング オプション



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 *36 :* ユーザ 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		

項目	説明	ブランディングの編集
1	企業ロゴ	IM and Presence Service 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。 • `brandingHeaderBegLTR.gif`（652 x 1 ピクセル） • `brandingHeaderBegLTR.gif`（652 x 1 ピクセル）
4	ヘッダーの背景	ヘッダーの 1 つのイメージを使用する場合： • `brandingHeaderMidLTR.gif`（652 x 1 ピクセル） 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。 • `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）	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。 • `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

項目	説明	ブランディングの編集
7	[移動（Go）] ボタン	header.go.font.color header.go.background.color header.go.border.color
8	ユーザ名およびパスワードのテキスト	splash.login.text.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
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 ディバイダ	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。

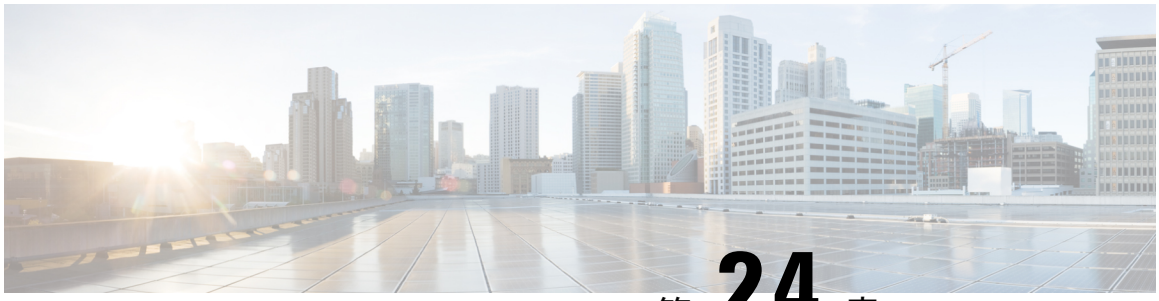
```
header.navigation.color="#FF0000"
```

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 V 部

IM and Presence Service のトラブルシューティング

- 高可用性のトラブルシューティング （359 ページ）
- UserID 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 （375 ページ）
- IM and Presence Service のトラブルシューティングに使用するトレース （379 ページ）



第 24 章

高可用性のトラブルシューティング

- 手動によるフェールオーバー、フォールバック、リカバリ （359 ページ）
- プレゼンス冗長グループのノードのステータスの表示 （362 ページ）
- ノード状態の定義 （362 ページ）
- ノードの状態、原因、および推奨処置 （364 ページ）
- 高可用性でのサービスの再起動 （372 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

Cisco Unified Communications Manager Administrationを使用して、プレゼンス冗長グループの IM and Presence Service ノードの手動フェールオーバー、手動フォールバック、手動リカバリを開始します。CLI を使用して Cisco Unified Communications Manager または IM and Presence Service からこれらのアクションを開始することもできます。詳細は、*Cisco Unified Communications Solutions* コマンドライン インターフェイス ガイドを参照してください。

- 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 は障害が発生したノードで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の接続は切断され、再度バックアップ ノードにログインする必要があります。

  （注） 手動フェールオーバーの後、手動ロールバックを呼び出すまで、重要なサービスは再起動されません。

- 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。これらのユーザは、割り当てられたノードに再度ログインする必要があります。

- 手動リカバリ：プレゼンス冗長グループの両方のノードで障害が発生した状態になって手動リカバリを起動すると、IM and Presence Service がプレゼンス冗長グループの両方のノードの Cisco Server Recovery Manager サービスを再起動します。

手動フェールオーバーの開始

Cisco Unified Communications Manager Administration を使用して、プレゼンス冗長グループの IM and Presence Service ノードのフェールオーバーを手動で実行することができます。

手順

ステップ 1 **[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。

[プレゼンス冗長グループの検索/一覧表示（Find and List Presence Redundancy Groups）] ウィンドウが表示されます。

ステップ 2 プレゼンス冗長グループの検索パラメータを選択して、[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 [プレゼンス冗長グループの検索/一覧表示（Find and List Presence Redundancy Groups）] ウィンドウに一覧表示されたプレゼンス冗長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 4 [サーバアクション（ServerAction）] フィールドで、[フェールオーバー（Failover）] をクリックします。

（注） このボタンは、サーバとプレゼンス冗長グループが正しい状態にある場合にのみ表示されます。

手動フォールバックの開始

Cisco Unified Communications Manager Administration を使用して、フェールオーバーしたプレゼンス冗長グループの IM and Presence Service ノードのフォールバックを手動で実行します。プレゼンス冗長グループ ノードのステータスの詳細については、ノードの状態、状態変更の原因、推奨処置に関するトピックを参照してください。

手順

ステップ 1 **[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。

[プレゼンス冗長グループの検索/一覧表示（Find and List Presence Redundancy Groups）] ウィンドウが表示されます。

ステップ 2 プレゼンス冗長グループの検索パラメータを選択して、[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 [プレゼンス冗長グループの検索/一覧表示（Find and List Presence Redundancy Groups）] ウィンドウに一覧表示されたプレゼンス冗長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 4 [サーバアクション（ServerAction）] フィールドで、[フォールバック（Fallback）] をクリックします。

（注） このボタンは、サーバとプレゼンス冗長グループが正しい状態にある場合にのみ表示されます。

手動リカバリの開始

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で障害が発生した状態の場合に必要となります。障害が発生した状態にあるプレゼンス冗長グループ内の IM and Presence Service ノードのリカバリを手動で開始するには、Cisco Unified Communications Manager Administration を使用します。

プレゼンス冗長グループ ノードのステータスの詳細については、ノードの状態、状態変更の原因、推奨処置に関するトピックを参照してください。

始める前に

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で障害が発生した状態の場合に必要となります。障害が発生した状態にあるプレゼンス冗長グループ内の IM and Presence Service ノードのリカバリを手動で開始するには、Cisco Unified Communications Manager Administration を使用します。

手順

ステップ 1 **[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。

[プレゼンス冗長グループの検索/一覧表示（Find and List Presence Redundancy Groups）] ウィンドウが表示されます。

ステップ 2 プレゼンス冗長グループの検索パラメータを選択して、[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 [プレゼンス冗長グループの検索/一覧表示（Find and List Presence Redundancy Groups）] ウィンドウに一覧表示されたプレゼンス冗長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 4 [回復（Recover）] をクリックします。

（注） このボタンは、サーバとプレゼンス冗長グループが正しい状態にある場合にのみ表示されます。

プレゼンス冗長グループのノードのステータスの表示

[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、プレゼンス冗長グループのメンバーになっている IM and Presence Service ノードのステータスを表示します。

手順

ステップ 1 **[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。

[プレゼンス冗長グループの検索/一覧表示（Find and List Presence Redundancy Groups）] ウィンドウが表示されます。

ステップ 2 プレゼンス冗長グループの検索パラメータを選択して、[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 検索結果に一覧表示されているプレゼンス冗長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。そのグループ内で2つのノードが設定され、高可用性が有効になっている場合、[高可用性（High Availability）] 領域にそのグループ内のノードのステータスが表示されます。

ノード状態の定義

表 *37*: 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。

状態	説明
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 Serviceはアイドル状態になります。アイドル状態では、IM and Presence Service ノードは可用性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 Service 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 Service 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 Service 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 Service 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。
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 Service 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 Service 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 Service 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 Service 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。

状態	説明
不明	ノード状態は不明です。 原因として、IM and Presence Service ノード上で高可用性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。

ノードの状態、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 *38 :* プレゼンス冗長グループ ノードの高可用性状態、原因、および推奨されるアクション

ノード 1		ノード 2		
状態	理由（Reason）	状態	理由（Reason）	原因/推奨処置
標準	標準	標準	標準	標準
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）	管理者からの要求時	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）	管理者からの要求時	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）	管理者からの要求時	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。

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

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（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）	Critical Service Down	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。 • ノード 1 のリブートにより、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。 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。
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）	Critical Service Down	バックアップモードで実行中（Running in Backup Mode）	Critical Service Down	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 Service 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**： **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。

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）	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 Service 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**： **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。
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（Start of Critical Services Failed）	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	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。 **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。 **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。

ノード 1		ノード 2		
状態	理由（Reason）	状態	理由（Reason）	原因/推奨処置
障害モードで実行中（Running in Failed Mode）	Critical Service Down	障害モードで実行中（Running in Failed Mode）	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。両方のノードが失敗状態に入ります。 **推奨処置**： **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、ノードをリブートします。

ノード 1		ノード 2		
状態	理由（Reason）	状態	理由（Reason）	原因/推奨処置
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	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 Service 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。**ノード 1 が起動したら、次の操作を実行します。 **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		
状態	理由（Reason）	状態	理由（Reason）	原因/推奨処置
（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	ノード 1 上で次のような条件が発生したため、IM and Presence Service はノード 2 への自動フェールオーバーを実行しました。 • ハードウェア障害 • 電源切断 • 再起動 • shutdown **推奨処置**： **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）] 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	起動中、ノード 2 はノード 1 を参照しません。 **推奨処置**： 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。

ノード 1		ノード 2		
状態	理由（Reason）	状態	理由（Reason）	原因/推奨処置
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		
状態	理由（Reason）	状態	理由（Reason）	原因/推奨処置
[バックアップがアクティブ化済み（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 Service ノード上で高可用性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。

高可用性でのサービスの再起動

高可用性を無効にしてから Cisco XCP Router、Cisco Presence Engine、またはサーバ自体を再起動する必要のある、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、高可用性を有効にする前に 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高可用性を無効にし、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 Routerの再起動
- Cisco Presence Engine の再起動
- サーバを再起動します。

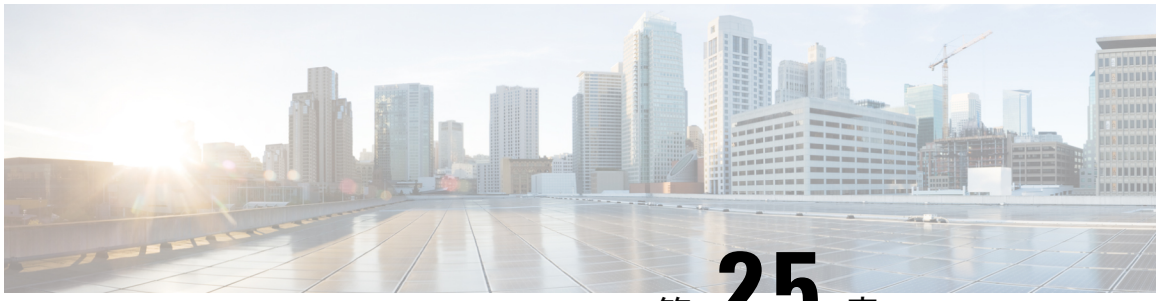
ステップ 4 再起動後、すべてのノードでアクティブなセッションの数をモニタします。

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。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高可用性を有効にできます。

（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 Routerや Cisco Presence Engine、あるいはその両方を連続して再起動することは推奨しません。ただし、以下のように再起動する必要がある場合は、最初のサービスを再起動し、JSM のすべてのセッションが再作成されるまで待機します。JSM セッションがすべて作成されたら、2 つ目の再起動を実行します。



第 25 章

UserID 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 ID エラーの受信 （375 ページ）
- 重複または無効なディレクトリ URI エラーの受信 （376 ページ）

重複したユーザ ID エラーの受信

問題 ユーザ 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 command を使用して、すべての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、『Cisco Unified Communications Solutions コマンドライン インターフェイス ガイド』を参照してください。

   ユーザ ID に続いて重複したユーザ 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 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. 別のクラスタで異なるユーザに同じユーザ 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 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 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 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 アドミニストレーション ガイド』を参照してください。

（注） ユーザ プロファイルでのユーザ 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 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 command を使用して、すべての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、『Cisco Unified Communications Solutions コマンドライン インターフェイス ガイド』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。

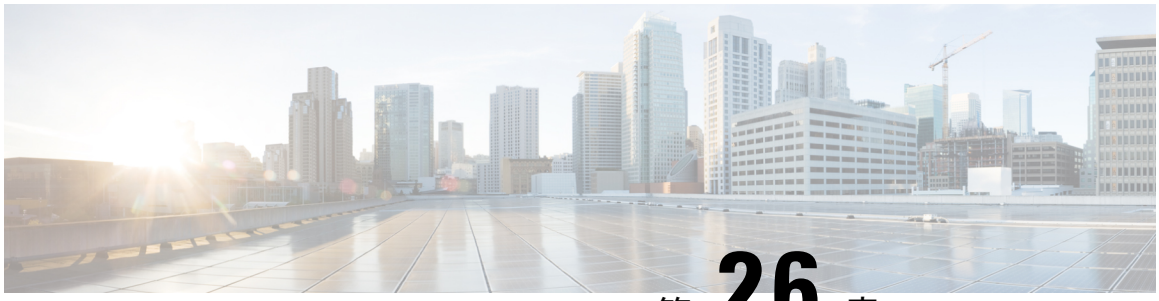
```
Users with No Directory URI Configured
------------------------------------------------------
 Node Name: cucm-imp-2
 User ID
 user4

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 アドミニストレーション ガイド』を参照してください。

（注） ユーザ プロファイルでのユーザ 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 26 章

IM and Presence Service のトラブルシューティングに使用するトレース

- トラブルシューティングでのトレースログの使用 （379 ページ）

トラブルシューティングでのトレースログの使用

トレースを使用して IM and Presence Service および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 トレースを設定することができます。結果は、Cisco Unified Real-Time Monitoring Tool を使用して参照および表示ができるシステム ログに保存されます。また、コマンドライン インターフェイスを使用して、システム ログ ファイルのサブセットを取得し、自分の PC またはラップトップにアップロードして詳細な分析を行うことも可能です。

トレースを使用するには、まずシステムをトレース用に設定する必要があります。トレースを設定する方法の詳細については、*Cisco Unified Serviceability* 管理ガイドの「トレース」の章を参照してください。

トレースの設定後、以下の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することができます。

- Real-Time Monitoring Tool：Real-Time Monitoring Tool を使用して、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することができます。Real-Time Monitoring Tool の使用法の詳細については、『Cisco Unified Real-Time Monitoring Tool アドミニストレーション ガイド』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、カスタマイズされたトレース ファイルに含める特定の日付の指定が可能です。CLI はシステムから関連付けられたトレース ファイルを取得して、圧縮 zip ファイルに保存して、後で分析するために、PC またはらっぷトップにコピーすることができるため、システムによってログが上書きされることはありません。

  このセクションの以降の表およびタスクでは、IM and Presence Service 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。

トレースを使用した一般的な IM and Presence の問題

以下の表では、IM and Presence Service に関する一般的な問題および、問題をトラブルシューティングするために実行することができるトレースの一覧が説明されています。

表 *39 :* 一般的な *IM and Presence* の問題のトラブルシューティング

問題個所 ...	これらのサービスのトレースの表示	追加手順
ログイン認証	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 を介した共通トレース （382 ページ） を参照してください。
アベイラビリティ 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 を介した共通トレース （382 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 を介した共通トレース （382 ページ） を参照してください。
連絡先リスト	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 を介した共通トレース （382 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 を介した共通トレース （382 ページ） を参照してください。

問題個所 ...	これらのサービスのトレースの表示	追加手順
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 を介した共通トレース （382 ページ）を参照してください。 （注） SIP メッセージ交換を確認するには、Cisco SIP Proxy デバッグ ログ機能が必要
XMPP ベースのドメイン間フェデレーション連絡先のアベイラビリティおよびIMの問題のトレース	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 を介した共通トレース （382 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 Service ノードで、このトレースを実行する
SIP ドメイン間フェデレーション連絡先のアベイラビリティおよび IM の問題のトレース	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 を介した共通トレース （382 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 を介した共通トレース （382 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トラブルシューティング	Cisco Intercluster Sync Agent Cisco AXL Web Service Cisco Tomcat Security Log Cisco Syslog Agent	クラスタ間のエラーを確認するには、**診断** > **システム トラブルシューティング**で、システムトラブルシューティングを実行します。

問題個所 ...	これらのサービスのトレースの表示	追加手順
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を介した共通トレース （382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を介した共通トレース （382ページ）を参照してください。
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	その他のトラブルシューティングを行うには、以下のCLIコマンドを実行します。 • `show process using-most cpu` • `show process using-most memory` • `utils dbreplication runtimestate` • `utils service list` 以下のCLIを実行して、RIS（Real-Time Information Servic）データを取得します。 • `file get activelog cm/log/ris/csv` 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を介した共通トレース

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を使用して、トレースを実行するコンポーネント

を選択して、<duration>を指定することができます。これは、ログ ファイルに含める、その日から過去にさかのぼる日数です。

以下の 2 つの表に、トレース ログ ファイルおよびログ出力場所の作成に使用できる CLI コマンドが提示されています。

- IM and Presence Service
- IM and Presence 機能

（注） CLI は、Cisco Unified Real-Time Monitoring Tool（RTMT）で表示可能であ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、グループ化して単一の圧縮 zip ファイルに格納します。RTMT トレースの詳細は、RTMT を介した共通トレース （387 ページ）を参照してください。

表 *40 : CLI* を使用した*IM and Presence Servic* の共通トレース

サービス	ログを作成するための CLI	CLI 出力ファイル
Cisco 監査ログ	file build log cisco_audit_logs <duration>	/epas/trace/log_cisco_audit_logs_*.tar.gz
Cisco Client Profile Agent	file build log cisco_client_profile_agent <duration>	/epas/trace/log_cisco_client_profile_agent_*.tar.gz
Cisco Cluster Manager	file build log cisco_config_agent <duration>	/epas/trace/log_cisco_cluster_manager_*.tar.gz
Cisco Config Agent	file build log cisco_config_agent<duration>	/epas/trace/log_cisco_config_agent_*.tar.gz
Cisco Database Layer Monitor	file build log cisco_database_layer_monitor <duration>	/epas/trace/log_cisco_database_layer_monitor_*.tar.gz
Cisco Intercluster Sync Agent	file build log cisco_inter_cluster_sync_agent <duration>	/epas/trace/log_cisco_inter_cluster_sync_agent_*.tar.gz
Cisco OAM Agent	file build log cisco_oam_agent <duration>	/epas/trace/log_cisco_oam_agent_*.gz
Cisco Presence Engine	file build log cisco_presence_engine <duration>	/epas/trace/log_cisco_presence_engine_*.tar.gz
Cisco RIS（Real-time Information Service）データ コレクタ	file build log cisco_ris_data_collector <duration>	/epas/trace/log_cisco_ris_data_collector_*.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 サービス管理（CSM）	file build log cisco_service_management <duration>	/epas/trace/log_cisco_service_management_*.tar.gz
Cisco SIP Proxy	file build log cisco_sip_proxy <duration>	/epas/trace/log_cisco_sip_proxy_*.tar.gz
Cisco Sync Agent	file build log cisco_sync_agent <duration>	/epas/trace/log_cisco_sync_agent_*.tar.gz
Cisco XCP Config Manager	file build log cisco_xcp_config_mgr <duration>	/epas/trace/log_cisco_xcp_config_mgr_*.tar.gz
Cisco XCP Router	file build log cisco_xcp_router <duration>	/epas/trace/log_cisco_xcp_router_*.tar.gz

表 *41 : CLI* を使用した *IM* およびプレゼンス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	file build log admin_ui <duration>	/epas/trace/log_admin_ui_*.tar.gz
一括管理	file build log bat <duration>	/epas/trace/log_bat_*.tar.gz
同期 HTTP 上の Bidirectional-streams	file build log bosh <duration>	/epas/trace/log_bosh_*.tar.gz
証明書	file build log certificates <duration>	/epas/trace/log_certificates_ * gz
設定 エージェント コア	file build log cfg_agent_core <duration>	/epas/trace/log_cfg_agent_core_*.tar.gz
Customer Voice Portal	file build log cvp <duration>	/epas/trace/log_cvp_*.tar.gz
ディレクトリ グループ	file build log directory_groups <duration>	/epas/trace/log_directory_groups_*.tar.gz
ディザスタ リカバリ	file build log disaster_recovery <duration>	/epas/trace/log_disaster_recovery_*.tar.gz
柔軟なIM アドレス	file build log flexable_im_address <duration>	/epas/trace/log_flexible_im_address_*.tar.gz
汎用コア	file build log general_core <duration>	/epas/trace/log_general_core_*.tar.gz
高可用性	file build log ha <duration>	/epas/trace/log_ha_*.tar.gz

機能名	ログを作成するための CLI	CLI 出力ファイル
高いCPU使用率	file build log high_cpu <duration>	/epas/trace/log_high_cpu_*.tar.gz
ハイ メモリ	file build log 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	file build log imdb <duration>	/epas/trace/log_imdb_core_*.tar.gz
クラスタ間ピアリング	file build log inter_cluster <duration>	/epas/trace/log_inter_cluster_*.tar.gz
マネージド ファイル転送	ファイルビルドのログ managed_file_transfer < 期間 >	/epas/trace/log_managed_file_transfer_*.tar.gz
Microsoft Exchange	file build log msft_exchange <duration>	/epas/trace/log_msft_exchange_ * gz
メッセージ アーカイバ	file build log msg_archiver <duration>	/epas/trace/log_msg_archiver_*.tar.gz
プレゼンス エンジン コア	file build log pe_core <duration>	/epas/trace/log_pe_core_*.tar.gz
Presence and IM メッセージ交換	file build log presence_im_exchange <duration>	/epas/trace/log_presence_im_exchange_*.tar.gz
SIP ログインの問題	file build log pws <duration>	/epas/trace/log_pws_*.tar.gz
Remote Call Control（リモート呼制御）	file build log remote_call_control <duration>	/epas/trace/log_remote_call_control_*.tar.gz
セキュリティの脆弱性	file build log sec_vulnerability <duration>	/epas/trace/log_sec_vulnerability_*.tar.gz
サービスアビリティの GUI	ファイルビルドのログ serviceability_ui < 期間 >	/epas/trace/log_serviceability_ui_*.tar.gz
SIP ドメイン間フェデレーション	file build log sip_inter_federation <duration>	/epas/trace/log_sip_inter_federation_ * tar.gz
SIP パーティション ドメイン間 フェデレーション	file build log sip_partitioned_federation <duration>	/epas/trace/log_sip_partitioned_federation_ *.tar.gz
SIP プロキシ コア	file build log sipd_core <duration>	/epas/trace/log_sipd_core_*.tar.gz
常設チャットの高可用性	file build log 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	file build log text_conference <duration>	/epas/trace/log_text_conference_*.tar.gz
アップグレードの問題	file build log upgrade_issues <duration>	/epas/trace/log_upgrade_issues_*.tar.gz
□ユーザ接続	file build log user_connectivity <duration>	/epas/trace/log_user_connectivity_*.tar.gz
名簿	file build log user_rosters <duration>	/epas/trace/log_user_rosters_*.tar.gz
XCP ルータ コア	file build log xcp_core <duration>	/epas/trace/log_xcp_core_*.tar.gz
XMPP ドメイン間フェデレーション	file build log xmpp_inter_federation <duration>	/epas/trace/log_xmpp_inter_federation_*.tar.gz
展開情報	file build log deployment_info <duration>	/epas/trace/log_deployment_info_*.tar.gz

CLI 経由のトレースの実行

CLI（コマンドライン インターフェイス）を介してカスタマイズしたトレース ファイルを作成するには、次の手順を使用します。CLI で duration パラメータを使用して、トレースに含める過去にさかのぼる日数を指定することができます。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、ファイル転送にのみに使用してください。

始める前に

システムにトレースが設定されている必要があります。トレースを設定する方法の詳細は、*Cisco Unified Serviceability* 管理ガイド の「Traces」の章を参照してください。

実行可能なトレースのリストを CLIを介した共通トレース （382 ページ） で確認します。

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、`file build log <name of service> <duration>` CLI コマンドを実行します。duration には、トレースに含める日数を指定します。

たとえば、`file build log cisco_cluster_manager 7` では、Cisco Cluster Manager ログの過去 1 週間分を表示します。

ステップ 3 ログを取得するには、`file get activelog <log filepath>` CLI コマンドを実行します。

たとえば、**file get activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz** となります。

ステップ 4 システムの安定性を維持するために、取得後にログは削除します。ログを削除するには、`file delete activelog <filepath>` コマンドを実行します。

たとえば、`file delete activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz`となります。

RTMT を介した共通トレース

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 ファイルを表示することができます。

（注） CLI を使用すると、RTMT で表示可能であ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ことができ、単一の圧縮 zip ファイルにまとめて保存することが可能です。CLI トレースの詳細は、CLIを介した共通トレース （382 ページ）を参照してください。

表 *42 : IM and Presence Service* ノードに共通のトレースおよびトレース 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`
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`

サービス	トレース ログのファイル名
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

第 VI 部

参考情報

- Cisco Unified Communications Manager での TCP および UDP ポートの使用 （391 ページ）
- IM and Presence Service のポート使用状況の情報 （413 ページ）

第 27 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 （391 ページ）
- ポートの説明 （393 ページ）
- ポート参照 （411 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、以下のカテゴリに整理されます。

- Cisco Unified Communications Manager サーバがクラスタ間で使用するポート
- 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
- CCMAdmin 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、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もありますが、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） システムの一時的なポートの範囲は32768～61000であり、電話機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 への接続が開き、抑えられないように、ファイアウォールを設定します。IM and Presence サブスクライバ ノードのインストール中には、Cisco Unified Communications Manager パブリッシャ ノードへの複数の接続が次々と開かれます。これらの接続をスロットリングすると、インストールが失敗する可能性があります。

ポートの説明

Cisco Unified Communications Manager サーバがクラスタ間で使用するポート

表 *43 : Cisco Unified Communications Manager* サーバがクラスタ間で使用するポート

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、およびアラート向けの Cisco AMC Service
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 マスター 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	Unified Communications Manager	5005 / TCP	このポートは SOAP CDROnDemand2 サービスによって使用される
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（Gateway）	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 サブスクライバ	22 / TCP	Cisco SFTP サービス。サブスクラ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 *44 :* 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	マスターサーバとプロキシサーバ間の Trivial File Transfer Protocol（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 マスター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	ネイティブエージェント MIB 要求を処理するために、マスターエージェントとネイティブエージェントとの通信に使用されます。
Unified Communications Manager	Unified Communications Manager	6162 / UDP	ネイティブエージェントから生成された通知を転送するために、マスターエージェントとネイティブエージェントとの通信に使用されます。
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 マスター エージェントとサブエージェントと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 ～ 48198	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 *45 : 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 *46 : 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 *47 : 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 • 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 *48 :* 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	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。 （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。
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	Skinny Client Control Protocol（SCCP）
電話	Unified Communications Manager	2443 / TCP	Secure Skinny 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
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 *49* : 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（Gateway）	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		
ゲートウェイ（Gateway）	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 エクスチェンジ（IKE）
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（Gateway）	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（Gateway）	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（Gateway）	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		
ゲートウェイ（Gateway）	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		

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（Gateway）	Unified Communications Manager	2000 / TCP	Skinny Client Control Protocol（SCCP）
ゲートウェイ（Gateway）	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（Gateway）	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（Gateway）	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（Gateway）	Unified Communications Manager	2428 / TCP	Media Gateway Control Protocol（MGCP）バックホール
--	--	4000 ～ 4005 / TCP	Cisco Unified Communications Manager に音声、ビデオ、およびDチャ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（Gateway）	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間トランク（ICT）
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（Gateway）	Unified Communications Manager	5061 / TCP	Secure Session Initiation Protocol（SIPS）ゲートウェイおよびクラスタ間トランク（ICT）
Unified Communications Manager	ゲートウェイ		
ゲートウェイ（Gateway）	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 *50 :* 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

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
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。
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。

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	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。
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 add ime vapserver または set ime vapserver port 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 *51 : 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 *52 : 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
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 コンフィギュレーション ガイド』

http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html

『FWSM 3.1 Application Inspection コンフィギュレーション ガイド』

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_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 および IPCC Express）ポート活用ガイド』

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

『Cisco ICM/IPCC Enterprise および Hosted Editions ポート活用ガイド』

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

『Cisco Unified Communications Manager Express セキュリティ ベスト プラクティス ガイド』

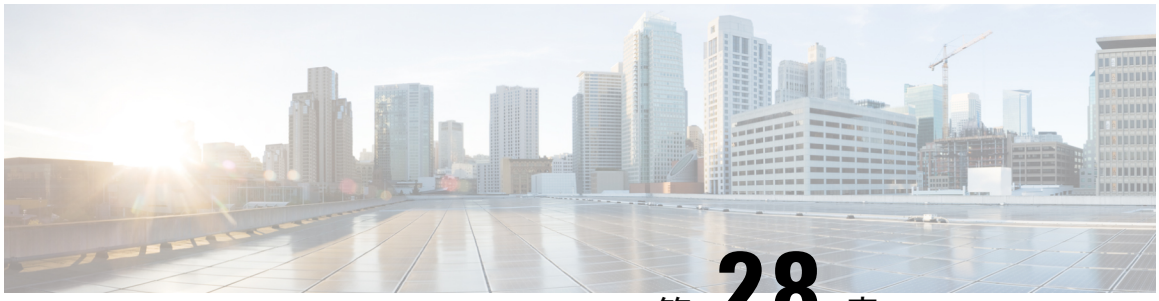
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

『Cisco Unity Express セキュリティ ベスト プラクティス ガイド』

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 28 章

IM and Presence Service のポート使用状況の情報

- IM and Presence Service ポートの使用方法の概要 （413 ページ）
- テーブルで照合する情報 （414 ページ）
- IM and Presence Service ポート リスト （414 ページ）

IM and Presence Service 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もありますが、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 *53* : 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	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（Transport Protocol）	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 Service 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 *54 : 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
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 *55 : 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
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 *56 : 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]	AXL/HTTPS	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。

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]	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 *57 : 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す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。

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	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 *58 : 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 *59 : 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 *60 : 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。

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]	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 *61 : IM and Presence* サービス ポート：*IPSec*マネージャからの要求

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 *62 : 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 *63 : 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（RTMT/AMC/SOAP）	IM and Presence（RIS）	[TCP]	[TCP]	2556	エフェメラル	Cisco RIS の 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 *64 : 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

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]	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の間の通信に使用します。
[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 *65 : 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（Gateway）] ---------- [IM and Presence]	[IM and Presence] ---------- [ゲートウェイ（Gateway）]	Ipsec	UDP	500	エフェメラル	Internet Security Association and the Key Management Protocol（ISAKMP）を有効にします。

表 *66 : 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 *67 : IM and Presence Service* 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 *68 : 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 *69 : 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 *70 : 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。サブスクライバ ノードが、パブリッシャ ノードと時刻を同期するために使用されます。

表 *71 : 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/IP 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 *72 : 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 *73 : 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 *74 : 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 *75 : IM and Presence* サービス ポート：外部データベース（*PostgreSQL*）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]	PostgreSQL データベース	[TCP]	[TCP]	5432 [2]	エフェメラル	PostgreSQL データベース リスニング ポート

[2] 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 *76 : 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 *77 : 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 *78 : 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。

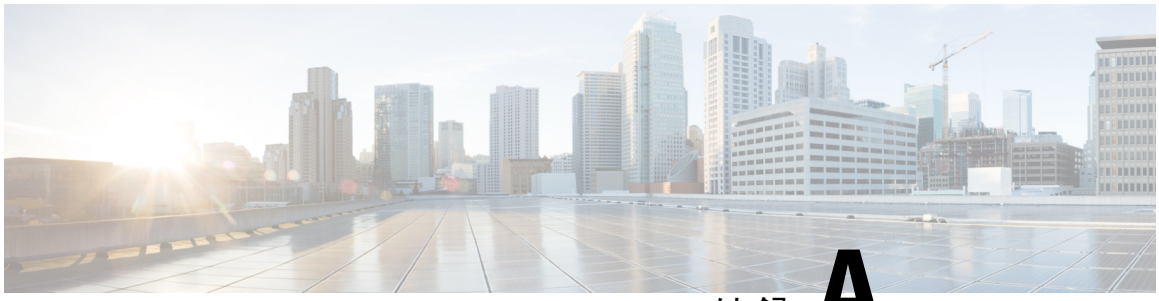
表 *79 : IM and Presence* サービス ポート：*In Memory* データベースの通知メッセージ

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 *80 : 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。

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。



付録 A

高可用性 クライアント ログイン プロファイル

- 高可用性ログイン プロファイル （431 ページ）
- 単一クラスタ コンフィギュレーション （434 ページ）

高可用性ログイン プロファイル

高可用性ログイン プロファイルに関する重要事項

- この項の高可用性ログイン 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（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。
- 高可用性クライアント 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、高可用性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高可用性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 Router 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期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 サイズおよび各高可用性展開タイプ（アクティブ/アクティブまたはアクティブ/スタンバイ）用に高可用性ログイン プロファイルを提供します。
- 高可用性ログイン 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、高可用性ログイン 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。

高可用性ログイン プロファイル テーブルの使用

高可用性ログイン 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高可用性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（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（Cisco Server Recovery Manager）] を選択して [重要なサービスの停止遅延（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、[重要なサービスの停止遅延（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 *81* : 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 *82* : 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 *83* : 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 *84 :* 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 *85 :* 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 *86 :* 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 *87 :* 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

表 *88 :* 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	137
500	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
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

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 *89 :* 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
3500	120	353
4000	120	387
4500	120	420
5000	120	453

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	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 *90* : 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	127
500	120	153
1000	120	187
1500	120	220
2000	120	253
2500	120	287
3000	120	320
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
8000	120	653
9000	120	720
10000	120	787
11000	120	853

アクティブ ユーザの予想数	再試行下限値	再試行上限値
12000	120	920
13000	120	987
14000	120	1053
15000	120	1120

25000ユーザフルUC（6vCPU16GB）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、シスコでは、少なくとも 2.8GHz の CPU クロック速度を推奨しています。

表 *91 :* 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
6000	120	787
7000	120	898
7500	120	953
8000	120	1009

アクティブ ユーザの予想数	再試行下限値	再試行上限値
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、シスコでは、少なくとも 2.8GHz の CPU クロック速度を推奨しています。

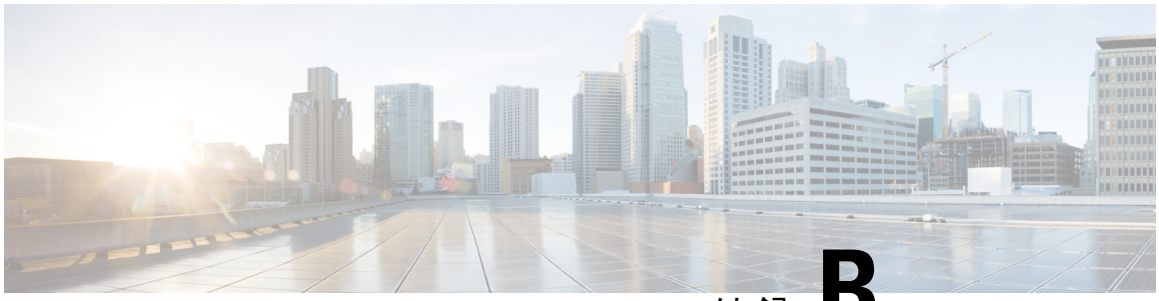
表 *92 :* アクティブ/スタンバイ プロファイルのログイン率：*16* ユーザが *80%* の *CPU* を使用

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	126
500	120	151
1000	120	183
1500	120	214
2000	120	245
2500	120	276
3000	120	308
3500	120	339
4000	120	370
4500	120	401
5000	120	433
6000	120	495
7000	120	558
8000	120	620

高可用性 クライアント ログイン プロファイル

アクティブ ユーザの予想数	再試行下限値	再試行上限値
9000	120	683
10000	120	745
11000	120	808
12000	120	870
13000	120	933
14000	120	995
15000	120	1058
16000	120	1120
17000	120	1183
18000	120	1245
19000	120	1308
20000	120	1370
21000	120	1433
22000	120	1495
23000	120	1558
24000	120	1620
25000	120	1683

高可用性 クライアント ログイン プロファイル



付録 B

追加の要件

- 高可用性ログイン プロファイル （443 ページ）
- 単一クラスタ コンフィギュレーション （446 ページ）
- XMPP 標準への準拠 （453 ページ）
- 設定変更通知およびサービス再起動通知 （454 ページ）

高可用性ログイン プロファイル

高可用性ログイン プロファイルに関する重要事項

- この項の高可用性ログイン 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（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。
- 高可用性クライアント 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、高可用性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高可用性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 Router 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期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 サイズおよび各高可用性展開タイプ（アクティブ/アクティブまたはアクティブ/スタンバイ）用に高可用性ログイン プロファイルを提供します。
- 高可用性ログイン 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、高可用性ログイン 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。

高可用性ログイン プロファイル テーブルの使用

高可用性ログイン 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高可用性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（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（Cisco Server Recovery Manager）] を選択して [重要なサービスの停止遅延（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、[重要なサービスの停止遅延（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 *93* : 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 *94* : 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 *95* : 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 *96 :* 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 *97 :* 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 *98 :* 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 *99 :* 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

表 *100 :* 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	137
500	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
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

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 *101* : 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
3500	120	353
4000	120	387
4500	120	420
5000	120	453

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	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 *102 :* 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	127
500	120	153
1000	120	187
1500	120	220
2000	120	253
2500	120	287
3000	120	320
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
8000	120	653
9000	120	720
10000	120	787
11000	120	853

アクティブ ユーザの予想数	再試行下限値	再試行上限値
12000	120	920
13000	120	987
14000	120	1053
15000	120	1120

25000ユーザフルUC（6vCPU16GB）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、シスコでは、少なくとも 2.8GHz の CPU クロック速度を推奨しています。

表 *103 :* 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
6000	120	787
7000	120	898
7500	120	953
8000	120	1009

アクティブ ユーザの予想数	再試行下限値	再試行上限値
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、シスコでは、少なくとも 2.8GHz の CPU クロック速度を推奨しています。

表 *104* : 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	126
500	120	151
1000	120	183
1500	120	214
2000	120	245
2500	120	276
3000	120	308
3500	120	339
4000	120	370
4500	120	401
5000	120	433
6000	120	495
7000	120	558
8000	120	620

アクティブ ユーザの予想数	再試行下限値	再試行上限値
9000	120	683
10000	120	745
11000	120	808
12000	120	870
13000	120	933
14000	120	995
15000	120	1058
16000	120	1120
17000	120	1183
18000	120	1245
19000	120	1308
20000	120	1370
21000	120	1433
22000	120	1495
23000	120	1558
24000	120	1620
25000	120	1683

XMPP 標準への準拠

IM and Presence Service 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 Router、Cisco SIP Proxy、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
グループ チャットと常設チャットの設定 （[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）]） 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

追加の要件

再起動を必要とする設定	再起動するサービス
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
Microsoft RCC 設定 （[アプリケーション（Application）] > [Microsoft RCC] > [設定（Settings）]） このページのいずれかの設定の編集	Cisco SIP Proxy
プレゼンス ゲートウェイ（Presence Gateway） （[プレゼンス（Presence）] > [ゲートウェイ（Gateways）]） プレゼンス ゲートウェイの追加、編集、削除 MS Exchange 証明書をアップロードした後	Cisco Presence Engine

再起動を必要とする設定	再起動するサービス
プレゼンス設定の構成 （[プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）]） [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 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 連絡先リストの最大サイズ（ユーザごと）（Maximum Contact List Size (per user)） [ウォッチャの最大数（Maximum Watchers）]	Cisco Presence Engine Cisco XCP Router
プレゼンス設定の構成 （[プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）]） [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	Cisco XCP Router
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 [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）]（チェックボックス） [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） 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 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	これらの設定を編集すると、Cisco SIP Proxy が自動的に再起動します さらに、XCP ルータを再起動する必要があります
プロキシ設定 （[プレゼンス（Presence）] > [ルーティング（Routing）] > [設定（Settings）]） プロキシ設定へのいずれかの編集	Cisco SIP Proxy

追加の要件

再起動を必要とする設定	再起動するサービス
セキュリティ設定 （[システム（System）] > [セキュリティ（Security）] > [設定（Settings）]） 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 いずれかのXMPP セキュリティ設定の編集	Cisco SIP Proxy（SIP セキュリティの編集の場合） Cisco XCP Router（XMPPセキュリティの編集の場合）
SIP フェデレーテッド ドメイン （[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）]） この設定の追加、編集、削除	Cisco XCP Router
サードパーティ製コンプライアンス サービス （[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）]） [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	Cisco XCP Router
TLS ピア サブジェクトの設定 （[システム（System）] > [セキュリティ（Security）] > [TLSピアサブジェクト（TLS Peer Subjects）]） このページでのいずれかの編集	Cisco SIP Proxy
TLS コンテキスト（TLS Context） （[システム（System）] > [セキュリティ（Security）] > [TLSコンテキスト設定（TLS Context Configuration）]） このページでのいずれかの編集	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。
XMPP フェデレーション （[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）]） （[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）]） XMPP フェデレーションへのいずれかの編集	Cisco XCP Router

再起動を必要とする設定	再起動するサービス
クラスタ間ピアリング （プレゼンス クラスタ間設定） クラスタ間ピア設定の編集	場合によっては、Cisco XCP Router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）。
イーサネット設定 （[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）]） いずれかのイーサネット設定の編集	システムが即時再起動されます
IPv6 設定（IPv6 Configuration） （[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]） [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	Cisco XCP Router Cisco SIP Proxy Cisco Presence Engine
トラブルシューティング 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 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	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 Proxy を再起動します。

再起動を必要とする設定	再起動するサービス
リモート監査ログの転送プロトコル utils remotesyslog set protocol * CLI コマンドのいずれかを実行した場合	ノードの再起動
次のアラートのいずれかを受け取った場合 • PEIDSQueryError • PEIDStoIMDBDatabaseSyncError • PEIDSSubscribeError • PEWebDAVInitializationFailure	Cisco Presence Engine を再起動することを推奨します。
次のアラートのいずれかを受け取った場合 • • XCPConfigMgrJabberRestartRequired • XCPConfigMgrR2RPasswordEncryptionFailed • XCPConfigMgrR2RRequestTimedOut • XCPConfigMgrHostNameResolutionFailed	Cisco XCP Router を再起動することを推奨します。
PWSSCBInitFailed	Cisco SIP Proxy 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 • 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 Service の再起動
新しい MSSQL 外部データベースの作成	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
次の Cisco SIP Proxy サービス パラメータの編集 • 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 Routerに影響するパラメータを編集する場合は、Cisco XCP Router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

再起動を必要とする設定	再起動するサービス
次のいずれかの [Cisco XCP File Transfer Manager] サービス パラメータの編集： • **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 Mulitple 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
外部データベース上の `install_dir /data/pg_hba.conf` または `install_dir /data/postgresql.conf` 設定ファイルの更新	Cisco XCP Router
移行ユーティリティ： • [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